HAL open science

Cryptographic applications of modular curves

Sudarshan Shinde

▶ To cite this version:

Sudarshan Shinde. Cryptographic applications of modular curves. Number Theory [math.NT]. Sorbonne Université, 2020. English. NNT : . tel-03146424v2

HAL Id: tel-03146424

https://theses.hal.science/tel-03146424v2

Submitted on 26 Aug 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Sorbonne Université

École doctorale de sciences mathématiques de Paris centre

Thèse de doctorat

Discipline : Mathématiques

présentée par

Sudarshan Shinde

Cryptographic applications of modular curves

---

dirigée par Pierre-Vincent Koseleff et Razvan Barbulescu

Soutenue le 10 juillet 2020 devant le jury composé de :

M. Jean-Marc Couveignes	Université de Bordeaux	Rapporteur
M. David Zureick-Brown	Emory University	Rapporteur
M. Loïc Merel	Université de Paris	Examinateur
M. Benjamin Smith	École Polytechnique	Examinateur
Mme Annick Valibouze	Sorbonne Université	Examinatrice
M. Razvan Barbulescu	Université de Bordeaux	Directeur
M. Pierre-Vincent Koseleff	Sorbonne Université	Directeur

Institut de mathématiques de Jussieu-
Paris Rive gauche. UMR 7586.
Boîte courrier 247
4 place Jussieu
75 252 Paris Cedex 05

Sorbonne Université
École doctorale de sciences
mathématiques de Paris centre.
Boîte courrier 290
4 place Jussieu
75 252 Paris Cedex 05

To *Karmaveer* Bhaurao Patil, the founder of
Rayat Shikshan Sanstha.

bas ki dushvār hai har kaam kā āsāñ honā
aadmī ko bhī mayassar nahīñ insāñ honā

Mirza Ghalib

Acknowledgement

This long term project required several helping hands, visible and invisible. Let me thank as many of them as I can.

First and foremost, I would like to express my enormous gratitude towards my advisors Dr. Razvan Barbulescu and Dr. Pierre-Vincent Koseleff for their guidance, help and patience over last 4 years. This work would not have been possible without them.

Dr. Jean-Marc Couveignes and Dr. David Zureick-Brown took time to go through the manuscript and gave me positive feedback. I sincerely thank them as well. Furthermore, I appreciate that Dr. Annick Valibouze, Dr. Loïc Merel and Dr. Benjamin Smith accepted the invitation to participate my jury. I have had a few occasions to discuss with all of them during this PhD. Finally I extend my gratitude towards Dr. Andrew Sutherland and Dr. David Kohel who had accepted to be referees if required. I would like to mention that Dr. Sutherland's online notes and scripts helped me a lot.

I must thank to my teachers in India, notably, Acharya Sir, Kunjeer Sir and Kumaresan Sir for helping me out on multiple occasions when I was confused. I must mention that I decided to pursue mathematics thanks to MT&TS program!

ED386, INRIA and École Polytechnique financed my studies and stay in France for last 8 years, I express my gratitude towards them as well.

In what follows, I take the liberty of being informal!

Firstly, let me appreciate my friends in France! Manali and Neeraj for being my family away from home! Priyanka, Chaitanya and Dhruv for several socio-political discussions and watching cricket together! Pallavi and Thibaut for their time when they used to come to Paris! Abhishek and Nagarjun who are also my flatmates, for their patience and support! Irene for weekly meetings in Jussieu, Arnub, Sourabh for coffee breaks, Suraj for political debates although there was nothing *left*! Shalmali for windy dinner plans! A special thanks to Vlerë (Arthur) for several Irish times, a few small trips and of course Frasier! Mariagiulia for her humour and visits to MacDo! Cyrus and Iva for Indian film festivals! Iffat for picnics! Shambhavi for lockdown conversations! Mathieu for usual *taquinage* in *couloir des doctorants*! Sylvain and Yasya for BWV1052-1054, several concerts, lunches and dinners! Yash for teaching me "*Si je suis moi parce que je suis moi, et si tu es toi parce que tu es toi, je suis moi et tu es toi. Si, en revanche, je suis moi parce que tu es toi, et si tu es toi parce que je suis moi, alors je ne suis pas moi et tu n'es pas toi*". Jagruti, Ketan and Akash for Saturday morning *chai*s, countless dinners, (once in a while ;)) lamb curries and most importantly for their patience with me during the lockdown! I thank Parul, Kaustubh and Mandar for various (never-happening) trip plans and a few other things ;)! Sanika, Sagar Pandhare, Sagar Kalane, Chinmay for showing me good time in Paris! Rasika, we are yet to meet here! Finally, Christiane, Nelly, Jean-Pierre for their warm welcome in cold cherbourgeois winters!

Now, I will come to my awesome friends in India! I appreciate Nilesh and Disha for their patience whenever I visited Pune, Vinay for keeping me posted about almost

everything (from Covid cases in Barshi to the fact that Dada has renovated his bungalow and is not going anywhere anytime soon!), Kiran for heavy afternoon lunches and Mumbai times! Kabir, Shantanu, Swapnil, Sangram for several *Namaskar* evenings, a few trips to Sangola (not you Kabir)! Siddhesh for all his help in Pune and welcome in Kolhapur! Vijaya and Bharat for so many things, notably French food times in Pune with Kunjeer Sir!! Dhanashree, Omkar for impromptu plans, Bhagyesha and Shriranjan (+ Awate family) for interesting perspectives! Manasi for JM Road breakfasts, Shruthi for helping me in Mumbai! Madhura and Saloni for walks in Fergusson! Ira, Nutan and Pratik for their support whenever I was in India! Ajinkya, Aniket, Abhijeet, Prasad, Prashant, Pritam, Gajendra, Abhinav for some amazing moments in Pune! Uday for late night *chai*s at Niranjan!

A special thanks to Atul for everything! He is someone on whom I can always rely! Thank you Atul.

Finally, my friends from my village! Sandip (*Mahadu*), Vitthal, Abhijit (*Pithya*)!

I must thank my family, especially my mother who never said no to any of my academic decisions! Thank you *Aai*! I express my gratitude towards my late father for everything he provided. I also express my profound love towards my brother, my sister-in-law and a cute little nephew for being always there to cheer me up! My uncles, aunts, countless cousins and nephews and nieces, thank you all!

Last but not the least, I must thank Gabbar for his enormous patience and unconditional love! <3

Contents

Introduction **vii**

I Elliptic curves and Galois representations **1**

1 Elliptic curves **3**
1 Algebraic curves . . . 3
2 Elliptic curves . . . 7
3 Isogenies and torsion subgroups . . . 12
4 Elliptic curves over finite fields . . . 16
5 The torsion point field . . . 18
6 Galois representation . . . 22

2 Subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and Galois images **27**
7 Structure of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ . . . 28
8 Local-global study of Galois images . . . 32
9 Properties of Galois images . . . 35
10 Surjectivity of $\rho_{\mathrm{E},\ell}$ . . . 36
11 Comparison of two algorithms . . . 44

II ECM and finding ECM-friendly elliptic curves **47**

3 Elliptic curve method **49**
12 Factorization using elliptic curves . . . 49
13 Classical improvements of ECM . . . 52
14 What makes a curve ECM-friendly? . . . 56
15 Quantifying ECM-friendliness . . . 59

4 Resolvent and subfields **65**
16 Computing Galois groups . . . 65
17 Formal resolvent to find ECM-friendly curves . . . 72
18 The subfields approach . . . 79

5 Modular Curves **83**
19 Elliptic curves over $\mathbb{C}$ . . . 83
20 Modular curves . . . 86
21 Modular functions . . . 91
22 Computing modular curves . . . 96

6 Progress on Mazur's Program B **99**
23 Works of [RZB15] and [SZ17] 99
24 Non-prime-power level case 101
25 Local-global problems for elliptic curves 108
26 Comparison with Morrow's work 110

Conclusion and further topics **113**

Tables **115**

Bibliography **125**

Introduction

Simply speaking, cryptography is a way of sharing secrets. In this sense, humans have been using various cryptographical means since antiquity. Traditionally, people have used methods based on private key cryptography. In this method, two users agree upon a common key and the same key can be used for encryption and decryption. A major disadvantage is the security of key. If a third person gets access to the private key then any encrypted message can be deciphered. Whence the necessity of the public key cryptography, where not only the key but the encryption method also is public. The public key cryptography is based on the assumption of difficulty of some mathematical problems and the non-availability of short cuts to solve these problems. The idea is to devise a cryptosystem based on a "difficult" mathematical problem in such a way that breaking the cryptosystem would amount to solving the problem on which it is based. One such problem is factoring integers i.e. expressing an integer as a product of smaller numbers. One can convince oneself of its difficulty by trying to factor manually 5219. Needless to say, a machine can perform this task easily. However, nowadays cryptosystems are based on substantially large numbers which even modern computers cannot factor rapidly. To give the reader an idea, a single 2.2GHz processor would take about 1500 years to factor the number RSA-768 ([KAF+10]). An important cryptosystem called RSA (which stands for Rivest, Shamir and Adelman) is based on the difficulty of factorization.

The methods of factorization split into two classes.

1. Methods whose costs depend exclusively on the size of the integer n to factor, like the quadratic sieve and the number field sieve (NFS), see [Pol93, LLJMP93].

2. Methods whose costs depend on the size of the factors we are looking for, up to a polynomial factor in the logarithmic size of n, which is the case for the trial division and the elliptic curve method (ECM), see [LJ87].

At the first sight, only the first class is relevant in cryptography because the numbers to factor in an RSA cryptosystem are of the form $n = pq$ where p and q are two primes with equal bit size. The most efficient algorithm of the first class is NFS which uses ECM as a subroutine in its co-factorization step. This use of ECM takes a non-negligible fraction of the total cost of NFS, see [BGK+]. Another important problem in cryptography is that of computing discrete logarithms, i.e. given a cyclic group G with a generator g and an element h of G, find m such that $g^m = h$. For this problem as well, the best known algorithm is a variant of NFS and uses ECM. One can thus say that improving ECM would improve NFS and it is cryptographically relevant.

Roughly speaking, a rational elliptic curve E is a plane curve defined by the equation $y^2 = x^3 + ax + b$ where a and b are rational numbers (Def. 2.5, p. 8). It turns out that the set $\mathrm{E}(\mathbb{Q})$ of rational points on E admits an additive group law which can be given by explicit polynomial equations (Section 2.1, p. 9). The points of finite order

on E are called the torsion points of E. We say a point P on E is a m-torsion point if $m\mathrm{P} := \mathrm{P} + \mathrm{P} + \cdots + \mathrm{P}$ (m times) is the neutral element of the group E.

Let n be an integer to factor with at least two distinct prime factors. The idea of ECM is to consider E over the ring $\mathbb{Z}/n\mathbb{Z}$ and to perform various group theoretic computations on E. These operations require inversion in $\mathbb{Z}/n\mathbb{Z}$. However, as n is not a prime, $\mathbb{Z}/n\mathbb{Z}$ has zero divisors, and in this case, we expect to arrive at the "division by 0" situation at some point. This should yield a factor of n.

For example, let p be a prime factor of n. One first chooses a rational elliptic curve E and a point P on it. It is algorithmically convenient to work with the projective form of E which is defined by $y^2z = x^3 + axz^2 + bz^3$. We first reduce E and P modulo n. Clearly if the denominator d of a coordinate of P is not coprime to n, we consider $\gcd(d, n)$ to obtain a factor of n. One can thus suppose that the denominators of the coordinates of P are all coprime with n. One then computes $\mathrm{P}_m := m\mathrm{P}$, for a well-chosen value of m, while keeping the coordinates modulo n. If the order $\#\mathrm{E}(\mathbb{F}_p)$ of E over the finite field $\mathbb{F}_p$ divides m, then P_m is the neutral element $(0, 1, 0)$ of the group $\mathrm{E}(\mathbb{F}_p)$. As p divides the z-coordinate z_{P} of P_m, one considers $\gcd(z_{\mathrm{P}}, n)$ to obtain a factor of n. In ECM, one uses elliptic curves from parameterized sets. We shall refer to these parameterized sets as families of elliptic curves. For more details on ECM, the reader can refer to Section 12.

The choice of m varies from one implementation to another, but as a first approximation, we take $m = \mathrm{B}!^{\lceil \log_2 \mathrm{B} \rceil}$ for some integer B. The algorithm succeeds if $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth i.e. all its prime factors are less than B.

Our goal is to find ECM-*friendly elliptic curves* i.e. suitable elliptic curves for ECM. Clearly, what renders an elliptic curve ECM-friendly is not well-defined. There are two ways.

1. One way is to consider curves with good arithmetic properties. For these curves, adding two points is not expensive which makes ECM faster. Most of the curves proposed for ECM in the literature fall in this category (Section 13.1, p. 53), for example, the twisted Edwards' curves or Montgomery curves.

2. The second way is to consider curves with better smoothness properties i.e. the curves E such that $\#\mathrm{E}(\mathbb{F}_p)$ has several small factors for all but finitely many primes p (Section 13.2, p. 55).

In this thesis, we focus on the second criterion and test eventually if the families of curves with better smoothness properties intersect with the ones with better arithmetic properties.

Historically, there have been various improvements of ECM. Soon after ECM was published, Montgomery introduced the parameterization $\mathrm{B}y^2 = x^3 + \mathrm{A}x^2 + x$ in [Mon87], which speeds up the process of point addition and doubling in ECM. Montgomery also suggested to use elliptic curves with 12 and 16 rational torsion points. Because, the torsion subgroup $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$ embeds (Theorem 4.5, p. 17) in $\mathrm{E}(\mathbb{F}_p)$ for all but finitely many primes p. Thus, the torsion order $\#\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$ divides $\#\mathrm{E}(\mathbb{F}_p)$ for all but finitely many primes. Experimentally, this increases the proportion of primes p where $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth. In order to compare the performance of elliptic curves in ECM, Montgomery considered the average $v_\ell(\mathrm{E})$ of valuations of a prime ℓ at $\#\mathrm{E}(\mathbb{F}_p)$ with varying p. This average can rigorously be defined using Chebotarev density (Theorem 8.4, p. 33). We shall revisit it in Section 14. In this sense, an elliptic curve E is ECM-friendly if $v_\ell(\mathrm{E})$ is larger for some prime ℓ.

Mazur's theorem (Theorem 3.7, p. 14) states that there are 15 possible torsion structures over $\mathbb{Q}$ and there are infinitely many *distinct* elliptic curves with these torsion structures. Their corresponding families have been considered for ECM, see [AM93, BBLP13, BBL10].

Brier and Clavier in [BC10] consider families defined over $\mathbb{Q}$ with large torsion over $\mathbb{Q}(\zeta_n)$ where ζ_n is a primitive n-th root of unity for $n = 3, 4, 5$. Heer, McGuire and Robinson in [HMR16] presented more rational families with large torsion over $\mathbb{Q}(\zeta_3)$ and noted experimentally that they have better performance in ECM than the elliptic curves with the same torsion over $\mathbb{Q}$.

However, when it comes to improving $v_\ell(\mathrm{E})$, the torsion subgroup is not the complete story because two curves can have the same torsion subgroup yet different values of $v_\ell(\mathrm{E})$ for the same prime ℓ. In other words, they can have different proportions of primes p such that $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth. For example, the Suyama family [Mon87, p. 262] has 6 rational torsion points but has better performance in ECM than a generic curve with the same torsion. Also note that, if E is a Suyama curve, then 12 divides $\#\mathrm{E}(\mathbb{F}_p)$ for all primes p of good reduction, whereas only the divisibility by 6 is guaranteed for an arbitrary curve with the same torsion. Thus the average valuation $v_\ell(\mathrm{E})$ cannot be explained by the torsion structure alone.

Barbulescu, Bos, Bouvier, Kleinjung and Montgomery [BBB+13] analyzed this behaviour and noted that the torsion subgroup over $\mathbb{Q}$ (or for that matter over any number field) does not completely explain the behaviour of curves in ECM.

In fact, they proposed subfamilies Suyama-11 and Suyama-$9/4$ of the Suyama family with the following property. Over any number field K, $\#\mathrm{E}(\mathrm{K})_{\mathrm{tors}} = \#\mathrm{E}'(\mathrm{K})_{\mathrm{tors}}$, where E is a curve from Suyama-11 (or Suyama-$9/4$ family) and E′ is a generic curve from Suyama family. And yet, E has better smoothness properties than E′. They also found the families of elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ with better smoothness properties than the generic curves with the same torsion. They proved that this difference is due to the Galois group of the torsion point field for some non-trivial torsion, say $m > 1$ and this explains the behaviour of curves in ECM.

The *m-torsion point field* $\mathbb{Q}(\mathrm{E}[m])$ is the field generated by adjoining to $\mathbb{Q}$ the coordinates of the m-torsion points of E over $\overline{\mathbb{Q}}$. In particular, the group $\mathrm{E}(\overline{\mathbb{Q}})[m]$ of m-torsion points is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ (Section 3.1, p. 13). Let P_1 and $\mathrm{P}_2 \in \mathrm{E}(\overline{\mathbb{Q}})$ be such that $\mathrm{E}(\overline{\mathbb{Q}})[m] = (\mathbb{Z}/m\mathbb{Z})\,\mathrm{P}_1 + (\mathbb{Z}/m\mathbb{Z})\,\mathrm{P}_2$. We call the mod m *Galois representation* (Def. 6.1, p. 23) attached to E the following map.

$$\begin{array}{rccc} \rho_{\mathrm{E},m}: & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \to & \mathrm{Aut}(\mathrm{E}[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \\ & \rho & \mapsto & \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right), \end{array}$$

where $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ are such that $\sigma(\mathrm{P}_1) = a\mathrm{P}_1 + b\mathrm{P}_2$ and $\sigma(\mathrm{P}_2) = c\mathrm{P}_1 + d\mathrm{P}_2$. We refer to $\mathrm{Im}\rho_{\mathrm{E},m}$ as the mod m *Galois image of* E and the integer m as the *level of* $\mathrm{Im}\rho_{\mathrm{E},m}$. Furthermore, if $\rho_{\mathrm{E},m}$ is non-surjective, we say that the mod m Galois image of E is *exceptional*.

In a similar manner, for a prime ℓ, we define (Def 6.5, p. 24) the *ℓ-adic Galois representation* $\rho_{\mathrm{E},\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{E}[\ell^\infty]) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$ and *the adelic Galois representation* (Def. 6.10, p. 25) $\rho_{\mathrm{E}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{E}_{\mathrm{tors}}) \cong \mathrm{GL}_2(\hat{\mathbb{Z}})$.

Serre's open image theorem [Ser71] (Theorem 6.7, p. 25) states that, for a rational elliptic curve E without complex multiplication (Def. 3.12, p. 16), $\rho_{\mathrm{E},\ell}$ is surjective for all but finitely many primes ℓ and there exists an integer m such that $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \mathrm{Im}\rho_{\mathrm{E}}] = [\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) : \mathrm{Im}\rho_{\mathrm{E},m}]$. Serre in [Ser81] also conjectured that for all rational elliptic curves without complex multiplication, $\rho_{\mathrm{E},\ell}$ is surjective for all $\ell > 37$ and gave a criterion

to conclude the surjectivity of $\rho_{E,\ell}$ (Theorem 10.6, p. 39). Using the classification of Dickson (Prop. 7.5, p. 29) of subgroups of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$, we give an algorithm to conclude the surjectivity of $\rho_{E,\ell}$ (Algorithm 10.1, p. 37). We also analyse a previously known algorithm that uses Serre's criterion, based on *local* images i.e. mod ℓ Galois images over finite fields, to conclude the surjectivity of $\rho_{E,\ell}$ (Algorithm 10.2, p. 40). We also evaluate the average number of primes over which one needs to verify Serre's criterion in order to conclude the surjectivity of $\rho_{E,\ell}$.

For curves without complex multiplication, the authors of [BBB+13] analyzed the relationship between the average valuation $v_\ell(E)$ and the ℓ-adic Galois image $\mathrm{Im}\rho_{E,\ell^\infty}$ and proved that if two curves E_1 and E_2 have the same ℓ-adic Galois image, up to conjugacy, then $v_\ell(E_1) = v_\ell(E_2)$. They in fact gave a formula for computing the average valuation using the elements of the ℓ-adic Galois image (Theorem 14.4, p. 57).

As the curves E with higher values of $v_\ell(E)$ for some ℓ are better for ECM, the classification of ECM-friendly elliptic curves boils down to the classification of rational elliptic curves with exceptional mod m Galois image. It turns out that this question, without its relation to cryptography, had already been posed by Barry Mazur, see [SZ06, p. 109]. As far as we know, no link between Mazur's Program B and cryptography has been previously established in the literature except for finding explicit parameterizations of the 15 families of torsion over $\mathbb{Q}$. We now give the statement of Mazur's Program B.

Mazur's Program B: Given a subgroup H of $GL_2(\hat{\mathbb{Z}})$ and a field k, classify all elliptic curves E defined over k such that $\mathrm{Im}\rho_E \subset H$ up to conjugacy.

Shimura's theory [Shi71] states that these elliptic curves lie in a 1-parameter family and they can be parameterized by the *modular curve* X_H (Chapter 5, p. 83). Thus, finding ECM-friendly elliptic curves boils further down to computing modular curves X_H and deciding whether X_H results into an infinite family.

Plenty of work has been done in this direction starting with Mazur himself. There seem to have been two ways. Either one fixes a particular subgroup H of $GL_2(\hat{\mathbb{Z}})$ and a degree d of a number field and considers the modular curve X_H over varying degree d number fields. Another way is to fix a number field and a prime ℓ and considering X_H for $H \subset GL_2(\mathbb{Z}_\ell)$. For example, in the first way, choosing H in the subgroup of matrices $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$ amounts to considering possible torsion structures, as explained in Example 6.4.

Kenku and Momose in [KM88] and Kamienny in [K+86] proved that over varying quadratic number fields, there are 26 possible torsion structures. The case of cubic number fields was settled by Jeon, Kim, Schweizer ([JKS04]). For quartic number fields, Jeon, Kim, Park in [JKP06] and for quintic and sextic number fields, Derickx, Sutherland in [DS17] found out possible torsion structures that occur infinitely many times. Kohel used quaternions to compute modular curves, see [Koh99].

On the other hand, Sutherland and Zwyina in [SZ17] computed the equations of modular curves X_H for $H \subset GL_2(\mathbb{Z}/m\mathbb{Z})$ for prime-power m where $-I \in H$. Rouse and Zureick-Brown in [RZB15] obtained the complete classification of 2-adic Galois images associated to rational elliptic curves.

In this work, we discuss two methods of computing the equations of X_H. The first one (Section 18, p. 79) is based on the computations of subfields of a function field and is more suitable for smaller values of ℓ. The second method is proposed by [RZB15] and is based on the theory of modular curves (Section 22). We extend the works of Sutherland and Zywina to subgroups of odd prime-power level which do not contain $-I$ and give explicit parameterizations of corresponding elliptic curves (Section 23.1, p. 100, Table 26.1, 26.2). Based on this list of elliptic curves with exceptional Galois images of odd prime-power levels and the classification of [RZB15] for $\ell = 2$, we consider Mazur's

Program B for arbitrary levels. We focus on the subgroups H of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ for any integer m which are isomorphic to the cartesian product of their projections modulo prime-power divisors of m. We call such subgroups *cartesian products* (Def. 24.1, p. 101).

Recall that a smooth plane rational curve of genus 0 (Def. 1.1) with at least one rational point has infinitely many rational points. If the curve has genus 1 and a point on it then it is an elliptic curve ([Sil08, Prop. III.3.1]) and if its rank (Section. 3.3, p. 15) is positive then it has infinitely many rational points.

As we are interested in infinite families of ECM-friendly elliptic curves and as Faltings' theorem states the finiteness of rational points on curves of genus 2 and higher, we focus in this work only on genus 0 or genus 1 cases. In all the cases we encountered, we were able to prove the existence of infinitely many points in genus 0 cases and compute ranks in genus 1 cases. We summerize new families in Table 24.2. An important quantity attached to an elliptic curve E given by $y^2 = x^3 + ax + b$ is its j-invariant $j(\mathrm{E}) = -1728 \cdot 4a^3/-16(4a^3 + 27b^2)$. We now give our main result.

Theorem 24.7 *There are exactly* 1525 *subgroups of* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ *which are cartesian and occur as Galois images for infinitely many rational elliptic curves with distinct j-invariants.*

The explicit equations of these families are given in the online complement of this work, available at [BS19b]. We then look for previously known ECM-friendly families from the literature in our list. Even though, these families were not proposed as solutions to Mazur's Program B, we find them among our families (Table 26.3, p. 118).

Equipped with these families, we quantify their ECM-friendliness i.e. their efficiency in ECM. We mentioned that ECM succeeds if $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth. By Hasse's theorem (Theorem 4.6, p. 17), we have $\#\mathrm{E}(\mathbb{F}_p) \approx p$. In the version of ECM proposed by Lenstra [LJ87], one selects uniformly random integers x_0, y_0 and a in $[0, p-1]$ and sets $\mathrm{E} : y^2 = x^3 + ax + b$ such that $(x_0, y_0) \in \mathrm{E}(\mathbb{F}_p)$. Lenstra [LJ87, Prop 2.7] proved that the proportion of elliptic curves selected in this manner for which $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth equals, up to a factor $1/\mathcal{O}(\log p)$, to the proportion of B-smooth integers in $[p - \sqrt{p}, p + \sqrt{p}]$ (Theorem 12.2, p. 51). Thus, the ECM-friendly families are hidden in $1/\mathcal{O}(\log p)$ factor in Lenstra's analysis.

Inspired by the idea of [Mur99] and results of [BL17], we consider the proportion of primes p of size n for which $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth. We then look for $\alpha(\mathrm{E})$ that renders this proportion approximately equal to the proportion of integers of the "corrected" size $ne^{\alpha(\mathrm{E})}$ that are B-smooth. Similar to [BL17], we put up a suitable candidate (Def. 15.1, p. 60) for the correction factor $e^{\alpha(\mathrm{E})}$ using an infinite convergent series. With our definition, ECM-friendly curves have smaller values of $\alpha(\mathrm{E})$. We rank all the families with respect to their values of $\alpha(\mathrm{E})$. We perform various experiments with α and notice that α works experimentally quite well (Example 15.3). In Section 15.3, we discuss a few limitations of α and define some finer tools.

Finally, we note that the families with better arithmetic properties described in Section 13.1 intersect with some families in our list. It is known that a Montgomery curve with 16 torsion points can not be put in the *twisted Edwards' form* (Section 13.1, p. 54) with $a = -1$. However, we find 4 families (Section 24.5, p. 108) that can be put in the *twisted Edwards' form* (Section 13.1, p. 54) with $a = -1$ and which have the same success probabilities as Montgomery curves with 16 torsion points. Thus, these families are strictly better that the ones used previously: Montgomery and Suyama families.

A generic Montgomery curve has only 2 torsion points over $\mathbb{Q}$ however its order over $\mathbb{F}_p$ is always divisible by 4. We analyze this behaviour in Section 25 using a result of

[Kat80] and find other such families in Theorem 25.5 from the list of families given by Theorem 24.7.

Organization of this work: In this work, we make use of various computer algebra systems like SAGE, MAPLE and MAGMA. The manuscript contains examples of elementary SAGE commands. The reader can find all the relevant scripts in the online complement available at [BS19b].

Part 1:
This part consists of two chapters. In Chapter 1, in order to render this work accessible, we recall elliptic curves and discuss classical relevant objects related to them. The purpose of this chapter is to give a construction of torsion point fields on number fields and on finite fields and describe Galois representations attached to an elliptic curve.

In Chapter 2, we consider subgroups and conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. We analyze the relationship between *local-global Galois images* i.e. Galois images over finite fields and over $\mathbb{Q}$. We give some group-theoretic properties of a mod ℓ Galois image. As the mod ℓ Galois image of an ECM-friendly elliptic curves is exceptional, we discuss methods to conclude the surjectivity of $\rho_{\mathrm{E},\ell}$. We give an algorithm which concludes the surjectivity $\rho_{\mathrm{E},\ell}$, by considering local Galois images (Algorithm 10.1, p. 37). We also analyze a previously known algorithm (Algorithm 10.2, p. 40) implemented in SAGE.

Part 2:
In Chapter 3, we describe the elliptic curve method of factorization (ECM) and mention various historical improvements of ECM. We recall briefly the results of [BBB+13] and rigorously define the average valuation $\bar{v}_\ell(\mathrm{E})$. We also illustrate how one can compute the exact value of $\bar{v}_\ell(\mathrm{E})$ using $\mathrm{Im}(\rho_{\mathrm{E},\ell^\infty})$. We recall Mazur's program B and define $\alpha(\mathrm{E})$ in order to quantify ECM-friendliness of an elliptic curve. We define $\alpha(\mathrm{E})$ over number fields as well and give examples over cyclotomic fields.

In Chapter 4, we discuss the resolvent method of computing Galois groups of the splitting fields of polynomials and how it can be used to find ECM-friendly families. This section is motivated by a question asked in [BBB+13]. We answer this question and show a drawback of this method when it comes to finding ECM-friendly elliptic curves. Finally in this chapter, we describe a method which makes use of subfields of function fields. We apply this method to a family of twisted Edwards' curves first appearing in [BBB+13] and obtain two new families (Prop. 18.3, p. 82).

We then move on to the approach using modular curves in Chapter 5. We discuss the general theory of elliptic curves over $\mathbb{C}$ and relate them to the quotients of $\mathbb{C}$ with lattices. We describe classical congruence subgroups and modular curves like $\mathrm{X}_0(\mathrm{N})$, $\mathrm{X}_1(\mathrm{N})$, $\mathrm{X}(\mathrm{N})$ and $\mathrm{X}(1)$. We then review meromorphic functions on these modular curves. In Section 22, we discuss the method from [RZB15] to compute modular curves X_H.

Finally in Chapter 6, we build upon the works of [SZ17] and [RZB15] and compute modular curves for cartesian subgroups of arbitrary levels having genus 0 and 1. We give all the infinite families having larger prime-power torsion over $\mathbb{F}_p$ for all but finitely many primes p than over $\mathbb{Q}$. We then identify previously known ECM-friendly families and compare our work with recent results of [Mor19].

Part I

Elliptic curves and Galois representations

Chapter 1

Elliptic curves

We recall several objects related to elliptic curves. Starting from the generalities of plane curves, we proceed to defining Weierstrass curves and then elliptic curves. The goal of this chapter is to define the central object of this work: the Galois representation attached to an elliptic curve.

We shall follow Joseph Silverman's classical text [Sil08].

1 Algebraic curves

Let k be a field of characteristic $\neq 2, 3$ with a fixed algebraic closure $\bar{k}$.

1.1 Affine algebraic curves

The *affine 2-space* $\mathbb{A}^2(\bar{k})$ is the set $\{(x_1, x_2) \mid x_1, x_2 \in \bar{k}\}$. The set $\mathbb{A}^2(k)$ of k-rational points of $\mathbb{A}^2(\bar{k})$ is $\{(x_1, x_2) \mid x_1, x_2 \in k\}$. Recall that the polynomial rings $\bar{k}[\mathrm{X}, \mathrm{Y}]$ and $k[\mathrm{X}, \mathrm{Y}]$ are both unique factorization domains.

Definition 1.1. Let $\mathrm{I} \subset \bar{k}[\mathrm{X}, \mathrm{Y}]$ be an ideal.

1. The *affine algebraic set* associated to I is the set

$$\mathrm{V}(\mathrm{I}) = \{\mathrm{P} \in \mathbb{A}^2(\bar{k}) \mid f(\mathrm{P}) = 0, \forall f \in \mathrm{I}\}.$$

   If the ideal I is generated by polynomials defined over k, we say that $\mathrm{V}(\mathrm{I})$ is defined over k and denote it by $\mathrm{V}(\mathrm{I})/k$.

2. For an affine algebraic set V, consider the ideal $\mathrm{I}(\mathrm{V})$ of polynomials in $\bar{k}[\mathrm{X}, \mathrm{Y}]$ vanishing over V. If $\mathrm{I}(\mathrm{V})$ is an ideal generated by a single non-constant polynomial f which is irreducible over $\bar{k}$, we call V an *affine algebraic plane curve defined by* f. For a subfield $k' \subset \bar{k}$, the set $\mathrm{V}(k')$ of k'-rational points on V is equal to $\mathrm{V}(\mathrm{I}) \cap \mathbb{A}^2(k')$. When it is clear from the context, we simply refer to V as a curve.

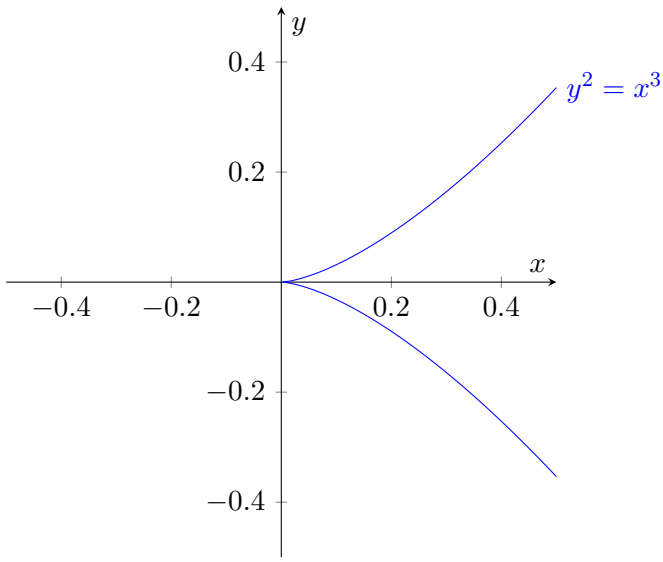
3. Let V be an affine algebraic plane curve defined by f and $\mathrm{P} \in \mathrm{V}$. We say that P is a *singular point* of V, if

$$\frac{\partial f}{\partial \mathrm{X}}(\mathrm{P}) = \frac{\partial f}{\partial \mathrm{Y}}(\mathrm{P}) = 0.$$

   If a point is not singular, we call it non-singular. If every point of V is non-singular, we say that V is non-singular or *smooth*.

4. For a smooth curve V defined by f, the genus $g(\mathrm{V})$ of V is equal to $\frac{(d-2)(d-1)}{2}$ where d is the degree of f. It is possible to define the genus of a singular curve, see [FH13]. We shall revisit it in the next section.

Example 1.2. Let V be defined by $y^2 - x^3 \in \mathbb{R}[x, y]$. The point $(0, 0)$ on V is singular and thus V is not smooth.



1.2 Projective curves

The *projective 2-space* $\mathbb{P}^2(\bar{k})$ is defined as the quotient of $\mathbb{A}^3(\bar{k}) \setminus \{(0, 0, 0)\}$ by the equivalence relation where we identify the points up to scalar multiplication. In other words, for $x = (x_0, x_1, x_2)$ and $y = (y_0, y_1, y_2) \in \mathbb{A}^3(\bar{k}) \setminus \{(0, 0, 0)\}$, we define the following equivalence relation,

$$x \sim y$$

if there exists $\lambda \in \bar{k}^*$ such that $x_i = \lambda y_i$ for all i. We denote the equivalence class of x by $[x_0, x_1, x_2]$. The set of k-rational points of $\mathbb{P}^2(\bar{k})$ is denoted by $\mathbb{P}^2(k)$.

A *projective algebraic set* and a *projective curve* can be defined in a similar manner as in Definition 1.1 via homogeneous polynomials and homogeneous ideals i.e. ideals generated by homogeneous polynomials in $\bar{k}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$. For more details, the reader can refer to [Sil08, Section I.2].

Example 1.3. Let $\mathcal{C}$ be the projective curve defined by $f = \mathrm{ZY} - \mathrm{X}^2 \in \mathbb{Q}[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$. We first look for singular points. Suppose $\mathrm{P} = [x_0, y_0, z_0]$ is a singular point of $\mathcal{C}$. Then we must have,

$$\begin{aligned}
\frac{\partial f}{\partial \mathrm{X}}(\mathrm{P}) &= -2x_0 &= 0 \\
\frac{\partial f}{\partial \mathrm{Y}}(\mathrm{P}) &= z_0 &= 0 \\
\frac{\partial f}{\partial \mathrm{Z}}(\mathrm{P}) &= y_0 &= 0
\end{aligned}$$

As $\mathrm{char}(k) \neq 2$, we must have $x_0 = y_0 = z_0 = 0$. This is not possible in $\mathbb{P}^2(\mathbb{Q})$. Thus $\mathcal{C}$ is smooth.

Furthermore, one can dehomogenize $\mathcal{C}$ with respect to Z by dividing by $\mathrm{Z}^{\deg f}$ (i.e. by letting $\mathrm{Z} = 1$). The change of variables $\mathrm{X}' = \frac{\mathrm{X}}{\mathrm{Z}}$ and $\mathrm{Y}' = \frac{\mathrm{Y}}{\mathrm{Z}}$ gives the affine curve $\mathcal{C}_1$ defined by $\mathrm{Y}' - \mathrm{X}'^2$. One can also dehomogenize with respect to X to get the affine curve $\mathcal{C}_2$ defined by $\mathrm{Z}'\mathrm{Y}' - 1$. We say that the affine curves $\mathcal{C}_1$ and $\mathcal{C}_2$ have the same *projective closure.*

We now discuss the function field of a projective curve $\mathcal{C}/k$. Let $\mathcal{C}$ be defined by a homogeneous polynomial $f \in k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$. Recall that f is absolutely irreducible i.e. irreducible over $\bar{k}$.

Definition 1.4. Let $\mathcal{C}$ be a projective curve defined by $f \in k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$. The function field $k(\mathcal{C})$ of $\mathcal{C}$ consists of fractions g/h where

1. g and h are homogeneous polynomials in $k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$ of the same degree.
2. $h \not\equiv 0 \mod f$
3. $\frac{g_1}{h_1} = \frac{g_2}{h_2}$ if, and only if, $g_1 h_2 \equiv g_2 h_1 \mod f$.

We require g and h to have the same degree so that one can evaluate $\frac{g}{h}$ at $\mathrm{P} \in \mathcal{C}$ in a unique way.

Example 1.5. Let $\mathcal{C}/k$ be defined by $\mathrm{X} + \mathrm{Y} + \mathrm{Z} \in k[\mathrm{X}, \mathrm{Y}, \mathrm{Z}]$. Clearly $f = \frac{\mathrm{Z}^2}{\mathrm{XY}} \in k(\mathcal{C})$ and one can evaluate f at $\mathrm{P} = [1, -1, 0] \in \mathcal{C}$ to get $f(\mathrm{P}) = 0$. However if one wishes to evaluate f at $\mathrm{P}_1 = [-1, 0, 1] \in \mathcal{C}$, the denominator vanishes. One can nonetheless define the value of f at P_1 by noting $\frac{\mathrm{Z}^2}{\mathrm{XY}} = \frac{\mathrm{Z}^2}{-\mathrm{X}^2 - \mathrm{XZ}}$ in $k(\mathcal{C})$. We then put $f(\mathrm{P}_1) = -1/2$.

Definition 1.6. Let $\mathcal{C}/k$ be a projective curve. Let $f \in k(\mathcal{C})$. We say f is *regular* at a point $\mathrm{P} \in \mathcal{C}$ if $f = \frac{g}{h}$ in $k(\mathcal{C})$ for some g and h such that $h(\mathrm{P}) \neq 0$.

We now define a rational map between two projective curves.

Definition 1.7. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two projective curves.

1. A *rational map* between $\mathcal{C}_1$ and $\mathcal{C}_2$ is

$$\begin{aligned} f \colon \mathcal{C}_1 &\to \mathcal{C}_2 \\ [x, y, z] &\mapsto [f_1(x, y, z), f_2(x, y, z), f_3(x, y, z)], \end{aligned}$$

   where f_1, f_2, f_3 are function in $\bar{k}(\mathcal{C}_1)$ such that whenever they are defined at a point in $\mathcal{C}_1$, the image lies in $\mathcal{C}_2$. We put $f = [f_1, f_2, f_3]$.

2. If there exists $\lambda \in \bar{k}(\mathcal{C}_1)^*$ such that λf_1, λf_2 and $\lambda f_3 \in k(\mathcal{C}_1)$, we say f is defined over k.
3. A rational map that is regular everywhere on its domain is called a *morphism.*

Equipped with the notion of morphisms between two curves, one can define an isomorphism between two curves.

Definition 1.8. Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two projective curves. Let $\phi : \mathcal{C}_1 \longrightarrow \mathcal{C}_2$ and $\psi : \mathcal{C}_2 \longrightarrow \mathcal{C}_1$ be morphisms (resp. rational maps). If $\psi \circ \phi$ and $\phi \circ \psi$ are identity over $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively, we say $\mathcal{C}_1$ and $\mathcal{C}_2$ are *isomorphic* (resp. *birationally equivalent*).

Example 1.9. Let $\mathcal{C}_1$ be the projective curve defined by $\mathrm{X}^2+\mathrm{Y}^2-\mathrm{Z}^2 \in \mathbb{Q}[\mathrm{X},\mathrm{Y},\mathrm{Z}]$ and let $\mathcal{C}_2$ defined by $\mathrm{T} \in \mathbb{Q}[\mathrm{S},\mathrm{T},\mathrm{R}]$. Consider the following rational map:

$$\begin{aligned} \phi\colon \mathcal{C}_1 &\to \mathcal{C}_2 \\ [x,y,z] &\mapsto [x+z,0,y]. \end{aligned}$$

One sees that ϕ is defined everywhere except at $[1,0,-1]$. One can however define ϕ at $[1,0,-1]$, by noting that modulo $\mathrm{X}^2+\mathrm{Y}^2=\mathrm{Z}^2$, we have,

$$\begin{aligned} \phi &\equiv [\mathrm{X}+\mathrm{Z},0,\mathrm{Y}] \\ &\equiv [(\mathrm{X}+\mathrm{Z})(\mathrm{X}-\mathrm{Z}),0,\mathrm{Y}(\mathrm{X}-\mathrm{Z})] \\ &\equiv [-\mathrm{Y}^2,0,\mathrm{Y}(\mathrm{X}-\mathrm{Z})] \\ &\equiv [-\mathrm{Y},0,\mathrm{X}-\mathrm{Z}]. \end{aligned}$$

We thus define $\phi([-1,0,1]) = [0,0,2] = [0,0,1]$. This implies ϕ is regular everywhere and hence a morphism from $\mathcal{C}_1$ to C_2. Let us now consider the following map:

$$\begin{aligned} \psi\colon \mathcal{C}_2 &\to \mathcal{C}_1 \\ [s,t,r] &\mapsto [s^2-r^2,2sr,s^2+r^2]. \end{aligned}$$

Clearly, this map is regular everywhere. Consider now $\psi\circ\phi$ modulo the relation $\mathrm{X}^2+\mathrm{Y}^2=\mathrm{Z}^2$,

$$\begin{aligned} \psi\circ\phi &\equiv [(\mathrm{X}+\mathrm{Z})^2-\mathrm{Y}^2,2(\mathrm{X}+\mathrm{Z})\mathrm{Y},(\mathrm{X}+\mathrm{Z})^2+\mathrm{Y}^2] \\ &\equiv [(\mathrm{X}^2+\mathrm{Z}^2+2\mathrm{XZ})-\mathrm{Y}^2,2(\mathrm{X}+\mathrm{Z})\mathrm{Y},(\mathrm{X}^2+\mathrm{Z}^2+2\mathrm{XZ})+\mathrm{Y}^2] \\ &\equiv [2\mathrm{X}^2+2\mathrm{XZ},2(\mathrm{X}+\mathrm{Z})\mathrm{Y},2\mathrm{Z}^2+2\mathrm{XZ}] \\ &\equiv [\mathrm{X},\mathrm{Y},\mathrm{Z}], \end{aligned}$$

and $\phi\circ\psi$ modulo the relation $\mathrm{T}=0$,

$$\begin{aligned} \phi\circ\psi &\equiv [(\mathrm{S}^2-\mathrm{R}^2)+(\mathrm{S}^2-\mathrm{R}^2),0,2\mathrm{SR}] \\ &\equiv [2\mathrm{S}^2,0,2\mathrm{SR}] \\ &\equiv [\mathrm{S},0,\mathrm{R}] \\ &\equiv [\mathrm{S},\mathrm{T},\mathrm{R}]. \end{aligned}$$

This proves that $\mathcal{C}_1$ and C_2 are isomorphic.

Example 1.10. Let V be from Example 1.2 in its projective form $\mathrm{Y}^2\mathrm{Z}-\mathrm{X}^3$. We saw that the point $(0,0,1)$ is singular and V is not smooth. We want to define the genus of V. Consider the curve $\mathcal{C}$ defined by $\mathrm{YZ}-\mathrm{X}^2$ and the following rational maps:

$$\begin{array}{cccc} f\colon & \mathrm{V} & \longrightarrow & \mathcal{C} \\ & [x,y,z] & \mapsto & [yz,x^2,xz] \end{array}$$

$$\begin{array}{cccc} g\colon & \mathcal{C} & \longrightarrow & \mathrm{V} \\ & [x,y,z] & \mapsto & [yz,xy,z^2] \end{array}$$

It is not difficult to see that $f\circ g$ and $g\circ f$ are identity over $\mathcal{C}$ and V respectively. Thus V and C are birationally equivalent and thus, by [Har77, Corollary 5.6], have the same genus which is 0. Note that V and C are not isomorphic as the map f is not defined at the point $[0,0,1]$.

Let us conclude this section with two classical results about maps between two curves.

Theorem 1.11 ([Sil08, Theorem II.2.1])**.** *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two curves and $\phi\colon \mathcal{C}_1 \to \mathcal{C}_2$ a rational map. If a point $\mathrm{P} \in \mathcal{C}_1$ is smooth i.e. non-singular then ϕ is regular at P_1. In particular, if $\mathcal{C}_1$ is smooth then ϕ is regular everywhere and thus is a morphism.*

Theorem 1.12 ([Har77, Theorem II.6.8])**.** *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two curves. Suppose $\mathcal{C}_1$ is smooth. Let $\phi\colon \mathcal{C}_1 \to \mathcal{C}_2$ be a morphism. Then ϕ is either constant or surjective.*

2 Elliptic curves

Having discussed the relevant objects related to algebraic curves, we shift our focus to a particular type of curves: *Weierstrass curves*. A projective Weierstrass equation over $\bar{k}$ is given by

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{1.1}$$

where a_1, a_2, a_3, a_4 and $a_6 \in \bar{k}$. One can dehomogenize it with respect to z to obtain,

$$\mathrm{E}_{\mathcal{W}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We denote the affine *Weierstrass polynomial* by

$$\mathcal{W}_a(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6,$$

and the projective Weierstrass polynomial by

$$\mathcal{W}_p(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3.$$

The curve in $\mathbb{P}^2(\bar{k})$ defined by $\mathcal{W}_p(x, y, z)$ is called a *projective Weierstrass curve* and it always has at least one k-rational point $\mathcal{O} = [0, 1, 0]$. It is the only point of intersection of the curve and the line at infinity $z = 0$ and we call it *the point at infinity*. One can see that $\mathcal{O}$ is non-singular.

In fact, any cubic curve with a point on it can be put in Weierstrass form. As k is supposed to be of characteristic $\neq 2, 3$, one can, using affine transformations of variables [Sil08, Section III.1], put $\mathrm{E}_{\mathcal{W}}$ in the following *short* Weierstrass form

$$y^2 = x^3 + ax + b.$$

Henceforth in this section, for the sake of brevity, we shall deal only with short Weierstrass forms. Let us now look for the form preserving transformations of variables x and y.

Proposition 2.1. *The only linear projective changes of variables that transform a curve E in short Weierstrass form to a curve E' in short Weierstrass form are*

$$x = u^2x', \quad y = u^3y', \quad \textit{for some } u \in k^*$$

Proof. Let $\mathcal{W}_a(x, y) = y^2 - x^3 - ax - b$. As the degrees of x and y in $\mathcal{W}_a(x, y)$ are 3 and 2 respectively, any form preserving affine change of variables must be of the following form,

$$\begin{aligned} x &= rx' + s \\ y &= ty' + vx' + w. \end{aligned}$$

Let $\mathcal{W}'_a(x', y')$ be the resulting polynomial after such a change of variables. We want to prove that $s = v = w = 0$ and $r = u^2$ and $t = u^3$ for some non-zero $u \in k$.

As the coefficient of x and y in $\mathcal{W}_a(x, y)$ are 1 and -1 respectively, we must have $r^3 = t^2$ and $rt \neq 0$. We put $u = \frac{t}{r}$ which ensures $u^2 = \frac{t^2}{r^2} = r$ and $u^3 = \frac{t^3}{r^3} = t$. The coefficients of $x'y', x'^2$ and y' in $\mathcal{W}'_a(x', y')$ are all 0. So we have $2tv = 0, v^2 - 3r^2 s = 0$ and $2tw = 0$. As $rt \neq 0$, we must have $s = v = w = 0$. □

Two Weierstrass curves related by the affine transformation of Prop. 2.1 are called *equivalent* Weierstrass curves and they are isomorphic as curves. One associates two important quantities to a Weierstrass curve E: its *discriminant* Δ_{E} and its *j-invariant* $j(\mathrm{E})$. These quantities have simple expressions when E is in short Weierstrass form $y^2 = x^3 + ax + b$. We have

$$\Delta_{\mathrm{E}} = -16(4a^3 + 27b^2), \quad j(\mathrm{E}) = -1728 \cdot 4a^3/\Delta_{\mathrm{E}}.$$

In fact, there exist curves with all possible j-invariants. If j is different than 0 and 1728 then the curve E_j defined by $y^2 = x^3 - 3j(j - 1728)x - 2j(j - 1728)^2$ is such that $j(\mathrm{E}_j) = j$. For $j = 0$ (resp. $j = 1728$), one can take the curve $y^2 = x^3 + d$ (resp. $y^2 = x^3 + dx$) for some non-zero d.

It is easy to see that two equivalent Weierstrass curves have the same j-invariant, however they are not necessarily isomorphic.

Proposition 2.2 ([Sil08, Section III.1, Prop. 1.4 (b)])**.** *Two elliptic curves are isomorphic over an algebraically closed field if, and only if, they have the same j-invariant.*

Proposition 2.3. *The Weierstrass curve* E *defined by $y^2 = x^3 + ax + b$ is smooth if, and only if, $\Delta_{\mathrm{E}} \neq 0$.*

Proof. Let us suppose that $\mathrm{P} = (x_0, y_0)$ is a singular point on E. Then, by taking partial derivatives we obtain

$$2y_0 = 0, \quad 3x_0^2 + a = 0, \quad y_0^2 = x_0^3 + ax_0 + b$$

Solving the above system for a and b, we obtain $a = -3x_0^2$ and $b = 2x_0^3$. This implies $\Delta_{\mathrm{E}} = -16(4a^3 + 27b^2) = 0$.

Conversely, if $\Delta_{\mathrm{E}} = 0$ then $x^3 + ax + b$ has a multiple root $x_0 = -3b/2a$ and the point $(x_0, 0)$ on E is singular. □

We now define an elliptic curve.

Definition 2.4. Let k be a field. An elliptic curve E over k is a smooth projective curve in $\mathbb{P}^2(k)$ defined by $\mathcal{W}_p(x, y, z) \in k[x, y, z]$.

Following Proposition 2.3, we have the following.

Definition 2.5. Let k be a field of characteristic $\neq 2$ and let $a, b \in k$ such that $4a^3 + 27b^2 \neq 0$. The projective curve E in $\mathbb{P}^2(k)$ defined by $zy^2 - x^3 - axz^2 - bz^3$ is an elliptic curve. Any curve isomorphic to E is also called an elliptic curve.

One can describe an elliptic curve using the genus of a curve.

Proposition 2.6 ([Sil08, Prop. III.3.1])**.** *Let k be a field and $\mathcal{C}$ be a smooth projective curve over k with at least one point in $\mathbb{P}^2(k)$. If the genus of $\mathcal{C}$ is 1 then $\mathcal{C}$ is an elliptic curve.*

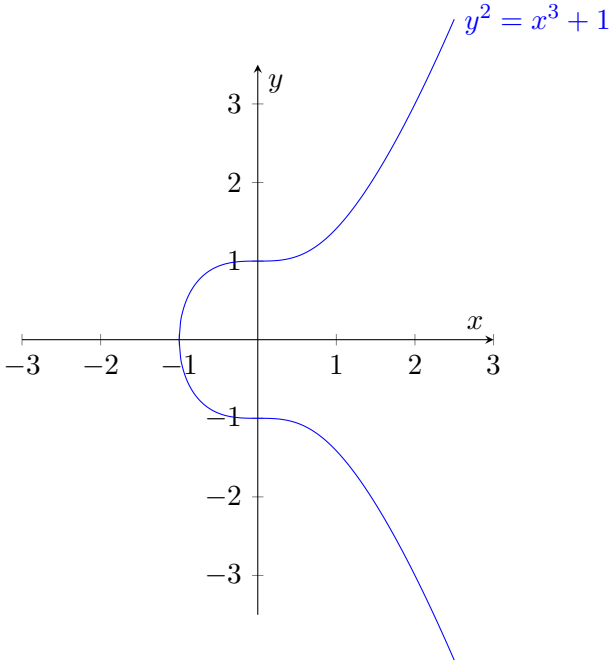
We mentioned in Definition 1.1 that the genus of a smooth curve of degree d is $\frac{(d-1)(d-2)}{2}$. Thus if the genus of a smooth curve is 1 then one sees that the curve is essentially of degree 3. Using an algorithm due to [vH95] implemented in MAPLE, one can transform a genus 1 curve into its Weierstrass form.

Keeping in mind, the point at infinity $\mathcal{O}$, we often denote an elliptic curve by its affine equation. In other words, if E/k is defined by $y^2 = x^3 + ax + b$ where $4a^3 + 27b^2 \neq 0$, the elliptic curve E is

$$\mathrm{E} = \{(x, y) \in \bar{k}^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}.$$

Let us take an example.

Example 2.7. Consider the curve $\mathrm{E} : y^2 = x^3 + 1$. As $\Delta_{\mathrm{E}} = -432 \neq 0$, E is smooth and thus is an elliptic curve.



One can create an elliptic curve in SAGE using its Weierstrass coefficients and compute its j-invariant and discriminant.

```
sage: E = EllipticCurve([3,5])
sage: E
Elliptic Curve defined by y^2 = x^3 + 3*x + 5 over Rational Field
sage: E.j_invariant()
6912/29
sage: E.discriminant()
-12528
```

2.1 Group law on an elliptic curve

The set of points on an elliptic curves admits a group law which we describe in this section. For more details, the reader can refer to [Sil08, Section III.2]. This group law can simply be described by stating that "the sum of three colinear point on an elliptic curve is the point at infinity $\mathcal{O}$".

Let E/k be an elliptic curve and P and Q $\in$ E. In order to compose P and Q, consider the line L in $\mathbb{P}^2(\bar{k})$ passing through P and Q. If P = Q, then L becomes the tangent to E at P. We shall see that L intersects E at a third point, say R. We then consider the line L′ passing through $\mathcal{O}$ and R. This line intersects E at a third point, say R′. We put R′ to be the composition of P and Q which we denote as $\mathrm{P} \bigoplus \mathrm{Q}$. One can see that for this composition law $\mathcal{O}$ is an identity element. It is easy to prove that (except the associative property!) this law turns E in an abelian group. [Sil08, Ch. III, Section III.2]. The reader can find a geometric proof of associativity in [ST92, Ch. 1]. If one is not afraid of computations, one can use the explicit formulae, which we shall now provide, to verify the associativity. Henceforth, as the group law over E is commutative, we shall simply denote it by + instead of $\bigoplus$.

Explicit group law

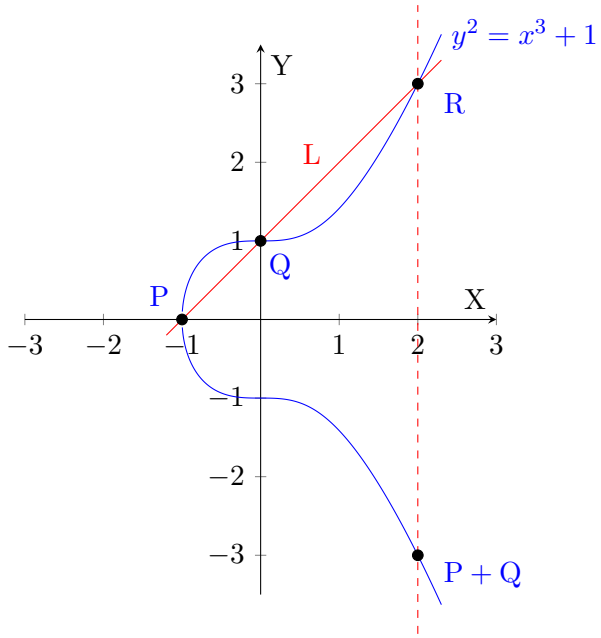
Let $\mathrm{E} : y^2 = x^3 + ax + b$ and $\mathrm{P} = (x_1, y_1)$ and $\mathrm{Q} = (x_2, y_2) \in \mathrm{E}$.

1. We have $-\mathrm{P} = (x_1, -y_1)$

2. Let $\mathrm{Q} \neq -\mathrm{P}$. Let $\mathrm{P} + \mathrm{Q} = \mathrm{R} = (x_3, y_3)$. Consider the equation of line L passing through P and Q. If $\mathrm{P} \neq \mathrm{Q}$, then the slope λ of L is $\frac{y_1 - y_2}{x_1 - x_2}$. However, if P = Q, L is tangent at P with the slope $\lambda = \frac{3x_1^2 + a}{2y_1}$. Then the equation of L is $y = \lambda x + \mu$ with $\mu = \frac{x_1 y_2 - y_1 x_2}{x_1 - x2}$, if $\mathrm{P} \neq \mathrm{Q}$ and $\mu = \frac{-x_1^3 + a x_1 + 2b}{2y_1}$, if P = Q. Finally, intersecting L with E yields the polynomial $\mathcal{W}_a(x, \lambda x + \mu) = (\lambda x + \mu)^2 - (x^3 + ax + b)$ which has three (not necessarily distinct) roots namely x_1, x_2 and x_3. Equating the coefficients in
$$\kappa(x - x_1)(x - x_2)(x - x_3) = (\lambda x + \mu)^2 - (x^3 + ax + b),$$
we obtain,
$$x_3 = \lambda^2 - x_1 - x_2 \text{ and } y_3 = -(\lambda x_3 + \mu).$$
Consequently, if two points are in $\mathrm{L} \cap \mathrm{E}(k)$, then the third one is also in $\mathrm{L} \cap \mathrm{E}(k)$.

Given a point P on E and a positive integer m, we define
$$[m] \cdot \mathrm{P} = \mathrm{P} + \cdots + \mathrm{P} \ (m \text{ times}).$$
If m is negative, we define
$$[m] \cdot \mathrm{P} = (-\mathrm{P}) + \cdots + (-\mathrm{P}) \ (|m| \text{ times}),$$
with convention $[0] \cdot \mathrm{P} = \mathcal{O}$. We shall often express $[m] \cdot \mathrm{P}$ by $m\mathrm{P}$.

Example 2.8. Let $\mathrm{E}/\mathbb{Q} : y^2 = x^3 + 1$. Let $\mathrm{P} = (-1, 0)$ and $\mathrm{Q} = (0, 1)$. The line L passing through P and Q intersects E at $\mathrm{R} = (2, 3)$. We then have $\mathrm{P} + \mathrm{Q} = (2, -3)$. One can also see that P is its own inverse as the tangent at P intersects curve at $\mathcal{O}$. One can find some points on E easily. For example, $(-1, 0), (0, 1), (0, -1), (2, 3), (2, -3) \in \mathrm{E}(\mathbb{Q})$. Clearly $(-1, 0)$ is the only point of order two as the y-coordinate is 0. Let $\mathrm{P}_1 = (0, 1)$. We compute, using the explicit group law, $[2] \cdot \mathrm{P}_1$. Here $\lambda = 0$ and $\mu = 1$ which gives $[2] \cdot \mathrm{P}_1 = (0, -1)$ and then we have $\mathrm{P}_1 + [2] \cdot \mathrm{P}_1 = [3] \cdot \mathrm{P}_1 = \mathcal{O}$. Thus the point P is of order 3. Now let $\mathrm{P}_2 = (2, 3)$. We first compute $[2] \cdot \mathrm{P}_2$. Here $\lambda = \frac{3 \times 2^2 + 0}{6} = 2$ and $\mu = \frac{-6}{6} = -1$. Then $[2] \cdot \mathrm{P}_2 = (0, 1) = \mathrm{P}_1$. Thus P_2 is of order 6.



One can create and add points in projective coordinates on an elliptic curve in SAGE.

```
sage: E = EllipticCurve([0,1])
sage: P1 = E.point((0,1,1))
sage: 3*P1
(0 : 1 : 0)
sage: P2 = E.point((2,3,1))
sage: P2.order()
6
```

2.2 $\mathbb{Q}$-isomorphism classes of elliptic curves

In this part, we restrict ourselves to elliptic curves over $\mathbb{Q}$, although the following arguments work over any number field. We saw in Prop. 2.2 that two elliptic curves E and E′ are isomorphic over $\mathbb{C}$ if, and only if, $j(\mathrm{E}) = j(\mathrm{E}')$. However, this criterion is not sufficient over $\mathbb{Q}$.

Example 2.9. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 = x^3 + 21x - 26$ and $\mathrm{E}_1/\mathbb{Q}$ be defined by $y^2 = x^3 + 21x + 26$. They have the same j-invariant however they are not isomorphic. In fact E has a point of order 3 whereas E_1 does not.

```
sage: E = EllipticCurve([21,-26])
sage: E1 = EllipticCurve([21,26])
sage: E.j_invariant() == E1.j_invariant()
True
sage: E.is_isomorphic(E1)
False
```

Let us assume that E and E′ have the same j-invariant and are not isomorphic. One can ask what stops E and E′ from being isomorphic over $\mathbb{Q}$. The answer lies in the notion of quadratic twists.

Definition 2.10. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve given by $y^2 = x^3 + ax + b$ and let $d \in \mathbb{Q}^*$. The *quadratic twist* E_d of E by d is the curve defined by the equation $dy^2 = x^3 + ax + b$. Here d is called the *twisting factor*.

One sees that E_d is not in Weierstrass form. We make the change of variable $x \mapsto \frac{x}{d}$ and $y \mapsto \frac{y}{d^2}$ to put E_d in its short Weierstrass form $y^2 = x^3 + d^2 \cdot ax + d^3 \cdot b$. One can verify that $j(\mathrm{E}_d) = j(\mathrm{E})$ and $\Delta_{\mathrm{E}_d} = 2^{12} d^6 \Delta_{\mathrm{E}}$. In fact, we have a stronger result.

Lemma 2.11. *Let* $\mathrm{E}/\mathbb{Q}$ *and* $\mathrm{E}'/\mathbb{Q}$ *be two elliptic curves in short Weierstrass form such that* $j(\mathrm{E}) = j(\mathrm{E}')$ *and* $j(\mathrm{E}) = j(\mathrm{E}') \notin \{0, 1728\}$. *Then* E *is a quadratic twist of* E'. *In other words, there exists* $d \in \mathbb{Q}^*$ *such that* $\mathrm{E} = \mathrm{E}'_d$.

Proof. Let E be defined by $y^2 = x^3 + ax + b$ and E' be defined by $y^2 = x^3 + a'x + b'$. As they have the same j-invariant, we have

$$\frac{a^3}{b^2} = \frac{a'^3}{b'^2}.$$

As $j(\mathrm{E}) = j(\mathrm{E}') \notin \{0, 1728\}$, none of a, b, a' and b' is zero. Then, as $\frac{a^3}{a'^3}$ is a square, we must have $\frac{a}{a'}$ a square. Let d be its square root. We then have $d^3 = \frac{b}{b'}$. Straightforward computations then show that E is a quadratic twist of of E' by d. □

We have another reformulation of Prop. 2.1.

Proposition 2.12. *Let* $\mathrm{E}/\mathbb{Q}$ *be defined by* $y^2 = x^3 + ax + b$ *and* $\mathrm{E}'/\mathbb{Q}$ *be defined by* $y^2 = x^3 + a'x + b'$. *Then* E *is isomorphic to* E' *if, and only if,* E *is quadratic twists of* E' *by* d^2 *for some* $d \in \mathbb{Q}^*$.

Proof. Let E be isomorphic to E'. Then by Prop. 2.1, E can be obtained from E' via the change of variable $x \mapsto u^2 x$ and $y \mapsto u^3 y$ for some non-zero $u \in \mathbb{Q}$. It suffices to put $d = \frac{1}{u}$ to see that E is quadratic twists of E' by d^2. Now consider that E is the quadratic twist of E' by d^2, i.e. E is defined by $y^2 = x^3 + d^4 a'x + d^6 b'$. One has an explicit isomorphism E' and E defined by $x \mapsto \frac{x}{d^2}$ and $y \mapsto \frac{y}{d^3}$. □

Remark 2.13. *If two elliptic curves are given in equivalent Weierstrass forms then they are isomorphic and have the same group structure.*

In SAGE,

```
sage: E = EllipticCurve([3,5])
sage: E1 = E.quadratic_twist(2)
sage: E1
Elliptic Curve defined by y^2 = x^3 + 12*x + 40 over Rational Field
sage: E2 = E.quadratic_twist(4)
sage: E.is_isomorphic(E1)
False
sage: E.is_isomorphic(E2)
True
```

Let us end this section by noting that $\mathrm{E}/\mathbb{Q}$ and $\mathrm{E}_d/\mathbb{Q}$ are isomorphic over $\mathbb{Q}(\sqrt{d})$.

3 Isogenies and torsion subgroups

We now consider morphisms, which preserve the point $\mathcal{O}$, between two elliptic curves.

Definition 3.1. Let E_1 and E_2 be two elliptic curves. An *isogeny* between E_1 and E_2 is a morphism $\phi : \mathrm{E}_1 \to \mathrm{E}_2$ such that $\phi(\mathcal{O}) = \mathcal{O}$.

Two elliptic curves are said to be *isogenous* if there is a non-constant, and thus by Theorem 1.12 surjective, isogeny between them. We now define the degree of an isogeny between two rational elliptic curves.

Definition 3.2. Let E_1 and E_2 be two rational elliptic curves and let $\phi : \mathrm{E}_1 \to \mathrm{E}_2$ be an isogeny. We define the degree $\deg \phi$ of ϕ to be $\# \ker \phi$.

By [Sil08, Cor.III.4.9], the degree of an isogeny is always finite.

Example 3.3. Let $\mathrm{E}_1/\mathbb{Q}$ and $\mathrm{E}_2/\mathbb{Q}$ be defined by $\mathrm{ZY}^2 = \mathrm{X}^3 + \mathrm{XZ}^2$ and $\mathrm{ZY}^2 = \mathrm{X}^3 - 4\mathrm{XZ}^2$ respectively. Consider the following rational map between them,

$$\begin{aligned} \phi\colon \mathrm{E}_1 &\to \mathrm{E}_2 \\ [x, y, z] &\mapsto [x(x^2 + z^2), y(x^2 - z^2), x^2 z] \end{aligned}$$

Let us verify that the image of $[x, y, z]$ lies on E_2. We evaluate $\mathrm{ZY}^2 - (\mathrm{X}^3 - 4\mathrm{XZ}^2)$ at the image.

$$\begin{aligned} x^2 z(y(x^2 - z^2))^2 - ((x(x^2 + z^2))^3 - 4x(x^2 + z^2)(x^2 z)^2) &= x^2(x^2 - z^2)^2(y^2 z - x^3 - xz^2) \\ &= 0 \end{aligned}$$

In order to claim that ϕ is an isogeny, one must check that $\phi([0, 1, 0]) = [0, 1, 0]$. However, $\phi([0, 1, 0]) = [0, 0, 0]$ which is not an element of a projective space. We thus need to find a suitable representative of $[x(x^2 + z^2), y(x^2 - z^2), x^2 z]$ in $\mathbb{P}^2(\mathbb{Q}(\mathrm{E}_1))$. We have modulo the equation defining E_1 the following,

$$\begin{aligned} [x(x^2 + z^2), y(x^2 - z^2), x^2 z] &\equiv [y(x^2 + z^2), \frac{y^2(x^2 - z^2)}{x}, xyz] \\ &\equiv [xy^2, y(y^2 - 2xz), x^3] \end{aligned}$$

With this equivalent representative, we have $\phi([0, 1, 0]) = [0, 1, 0]$.

Example 3.4. For a point P on an elliptic curve E and a positive integer m, we consider the following *multiplication by m* map.

$$\begin{aligned} [m]\colon \mathrm{E} &\longrightarrow \mathrm{E} \\ \mathrm{P} &\mapsto [m] \cdot \mathrm{P} \end{aligned}$$

Note that $[m]$ is a rational map. Indeed, as the addition of two points on an elliptic curve can be expressed using polynomial expressions. As E is smooth, by Theorem 1.11, $[m]$ is a morphism. Finally, as $[m] \cdot \mathcal{O} = \mathcal{O}$, $[m]$ is an isogeny.

If $m \neq 0$, the map $[m]$ is non-constant by [Sil08, Prop. III.4.2]. We denote the set of isogenies from an elliptic curve E to itself by End(E). It forms a ring under addition and composition of isogenies. For $\phi, \psi \in \mathrm{End}(\mathrm{E})$, we define $(\phi + \psi)(\mathrm{P}) = \phi(\mathrm{P}) + \psi(\mathrm{P})$ and $(\phi \times \psi)(\mathrm{P}) = \phi(\psi(\mathrm{P}))$.

3.1 Torsion subgroup

Let E be an elliptic curve and m a positive integer. The *m-torsion subgroup* $\mathrm{E}[m]$ of E is

$$\mathrm{E}[m] = \{\mathrm{P} \in \mathrm{E}(\overline{k}) \mid [m]\mathrm{P} = \mathcal{O}\}.$$

This is a very important object of this work and we will see it again on several occasions. If E is defined over k, we denote the m-torsion k-rational points of E by $\mathrm{E}(k)[m]$. The *torsion subgroup* of E is denoted as $\mathrm{E}_{\mathrm{tors}}$ and is defined as

$$\mathrm{E}_{\mathrm{tors}} = \bigcup_{m \geq 1} \mathrm{E}[m].$$

$\mathrm{E}_{\mathrm{tors}}(k)$ denotes the set of k-rational points in $\mathrm{E}_{\mathrm{tors}}$. The group $\mathrm{E}[m]$ has a simple structure.

Proposition 3.5 ([Sil08, Corr. III.6.4])**.** *Let* E/k *be an elliptic curve. If* $\mathrm{char}(k) = 0$ *or* $\mathrm{char}(k) = p$ *and* $\gcd(p, m) = 1$*, then* $\mathrm{E}[m]$ *is isomorphic to* $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$*.*

Example 3.6. Let E be defined by $y^2 = x(x+1)(x-1)$ over $\mathbb{Q}$. By the geometry of elliptic curves, the points of order 2 on E are precisely the ones where the tangent is parallel to the y-axis. Thus their x-coordinates correspond to the roots of the polynomial $x(x+1)(x-1)$. We obtain $\mathrm{E}[2] = \{(0,0), (1,0), (-1,0), \mathcal{O}\}$. We say E admits full 2-torsion over $\mathbb{Q}$.

One can naturally ask what group structures can occur as torsion subgroups over a field k. The answer depends on the field k and is known for several fields (see for example [Sut12b, KM88]). The first result of this kind is due to Barry Mazur.

Theorem 3.7 (Mazur's theorem, [Sil08, Theorem VIII.7.5], [SZ06, Theorem 1])**.** *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve. Then* $\mathrm{E}_{\mathrm{tors}}(\mathbb{Q})$ *is isomorphic to one of the following groups.*

1. $\mathbb{Z}/m\mathbb{Z}$ *for* $m \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$
2. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ *for* $m \in \{1, 2, 3, 4\}$.

Furthermore, every group in the above list occurs for infinitely many elliptic curves and the sets of these elliptic curves can be parameterized [Kub76, Table 3]. We shall visit it again in Chapter 5. One can compute the torsion subgroup over number fields using SAGE.

Example 3.8.
```
sage: E = EllipticCurve([0, -1, 1, -10, -20])
sage: E.torsion_subgroup()
Torsion Subgroup isomorphic to Z/5 associated to the Elliptic Curve
defined by y^2 + y = x^3 - x^2 - 10*x - 20 over Rational Field
sage: E = E.change_ring(CyclotomicField(5))
sage: E.torsion_subgroup().generator_orders()
(5, 5)
```
Here, E admits full 5-torsion over $\mathbb{Q}(\zeta_5)$ where ζ_5 is a primitive fifth root of unity.

3.2 Weil pairing

The torsion points are intrinsically related to the roots of unity via Weil pairing. Let E/k be an elliptic curve. Let m be a positive integer coprime to $p = \mathrm{char}(k)$ if $p > 0$. We mentioned that $\mathrm{E}[m]$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. There exists a natural way to associate a m-th root of unity in $\overline{k}$ to a pair of points in $\mathrm{E}[m]$. This is known as *Weil pairing*. As it is the case with the basis of $\mathrm{E}[m]$, the choice of the m-the root of unity is not canonical and depends upon the choice of the basis.

Definition - Theorem 3.1 ([Sil08, Prop. III.8.1])**.** *Let* E/k *be an elliptic curve and* $m > 0$ *be an integer coprime to* $p = \mathrm{char(k)}$ *if* $p > 0$*. Let* μ_m *be the* set of m-th roots of unity in $\overline{k}$*. Let* $(\mathrm{P}_1, \mathrm{P}_2) \in \mathrm{E}[m]^2$ *be an ordered basis of* $\mathrm{E}[m]$*. Then, there exists a pairing on* $\mathrm{E}[m]$ *i.e. a map* e_m *from* $\mathrm{E}[m] \times \mathrm{E}[m]$ *to* μ_m *such that*

$$e_m(a\mathrm{P}_1 + b\mathrm{P}_2, c\mathrm{P}_1 + d\mathrm{P}_2) = \zeta_m^{ad-bc} \text{ for all } a, b, c, d \in \mathbb{Z}/m\mathbb{Z},$$

where ζ_m *is a primitive* m*-th root of unity.*

In the above Definition - Theorem, the choice of ζ_m is not canonical as it depends on the basis P_1 and P_2. As an immediate consequence, we have the following.

Corollary 3.9 ([Sil08, Cor. III.8.1.1])**.** *If* $\mathrm{E}[m] \subset \mathrm{E}(k)$ *then* $\mu_m \subset k^*$*.*

On computes the Weil pairing using divisors on curve, see [Sil08, Section III.8]. It is implemented in SAGE. Let us take the curve from Example 3.8.

```
sage: E = EllipticCurve([0, -1, 1, -10, -20])
sage: E = E.change_ring(CyclotomicField(5))
sage: P1, P2 = E.torsion_subgroup().gens()
sage: P1 = E(P1); P2 = E(P2) #One needs to coerce points on E.
sage: P1.weil_pairing(P2,5)
zeta5^2
```

3.3 Mordell-Weil group

Mordell studied in 20's the structure of $\mathrm{E}(\mathbb{Q})$ and proved that $\mathrm{E}(\mathbb{Q})$ is finitely generated. Later, Weil generalized it to abelian varieties.

Theorem 3.10 (Mordell-Weil theorem [Sil08, Ch. VIII]))**.** *Let* k *be a number field and* E/k *be an elliptic curve. Then* $\mathrm{E}(k)$ *is finitely generated. In other words, there exist* $\mathrm{P}_1, \mathrm{P}_2, \ldots, \mathrm{P}_n \in \mathrm{E}(k)$ *such that for every point* $\mathrm{P} \in \mathrm{E}(k)$*, we have*

$$\mathrm{P} = c_1\mathrm{P}_1 + c_2\mathrm{P}_2 + \cdots + c_n\mathrm{P}_n,$$

for some $c_i \in \mathbb{Z}$*.*

By the classification of finitely generated abelian groups, we have

$$\mathrm{E}(k) = \mathrm{E}_{\mathrm{tors}}(k) + \mathbb{Z}^r,$$

where the integer r is called as the *rank* of E over k. Note that the rank depends on the number field k. It is conjectured (see [Sil08, Conjecture VIII.10.1]) that there exist rational elliptic curves of arbitrary ranks. Over $\mathbb{Q}$, there exists an elliptic curve with rank at least 28, see Elkies [Elk06].

Example 3.11. We compute the rank of E defined by $y^2 = x^3 + 3x + 5$ over $\mathbb{Q}$ and over $\mathbb{Q}(i)$.

```
sage: E = EllipticCurve([3,5]); E.rank()
1
sage: E.change_ring(CyclotomicField(4)).rank()
2
```

3.4 Complex multiplication

Let k be a field of characteristic 0 and let E/k be an elliptic curve. Consider the following map from Example 3.4.

$$\begin{aligned} [\ ]\colon \mathbb{Z} &\to \mathrm{End}(\mathrm{E}) \\ m &\mapsto [m]. \end{aligned}$$

Often, the above map is bijective. In other words, for most of the curves, the only isogenies are the multiplication maps by m.

Definition 3.12. Let E/k be an elliptic curve such that the endomorphism ring $\mathrm{End}(\mathrm{E})$ is strictly larger than $\mathbb{Z}$. We say E has *complex multiplication*.

We often say elliptic curve with CM or without CM to say if a curve has complex multiplication or not.

Example 3.13. Let E be defined by $y^2 = x^3 - x$. It has complex multiplication as $\mathrm{End}(\mathrm{E})$ is larger than $\mathbb{Z}$ as it contains the following map. Let i denote the usual square root of -1.

$$\begin{array}{rccc} [i]\colon & \mathrm{E} & \to & \mathrm{E} \\ & (x,y) & \mapsto & (-x, iy) \end{array}$$

Heilbronn (see [Hei34]) proved that there are only finitely many imaginary quadratic number fields with any given class number. By theory of complex multiplication, the j-invariants of elliptic curves with CM over any number field is also finite. In a letter to Tate, Serre, using work of Weber (see [Web98, p. 462]), mentions computing all 13 j-invariants of rational elliptic curves with complex multiplication (see [CS15, p. 178]).

Elliptic curves with CM have several special properties (see, for example, [Sil13, Ch. II], [Cox11b, Ch. 3]). However, their use in ECM is limited. Indeed, for an elliptic curve E with CM, the proportion of primes p such that $\#\mathrm{E}(\mathbb{F}_p) = p + 1$ is half (see [Sil08, Example V.4.5 and the discussion thereafter, Exercise 5.10(b)]). Practically in ECM, one uses the $p-1$ (see Section 12) and the $p+1$ method of factorization (see [Wil82]) as the first step. These methods use the smoothness of $p - 1$ and $p + 1$ respectively. Thus, using an elliptic curve with CM in ECM is not efficient as one ends up performing redundant computations 50% of the times. Therefore, we do not concern ourselves with them.

With SAGE, one can test whether a curve has complex multiplication. One can also obtain the list of CM j-invariants over any number field.

```
sage: EllipticCurve([3,5]).has_cm()
False
sage: EllipticCurve([-1,0]).has_cm()
True
sage: len(cm_j_invariants(QQ)) #len returns the length of a list.
13
sage: len(cm_j_invariants(CyclotomicField(5)))
31
```

4 Elliptic curves over finite fields

Given a rational elliptic curve $\mathrm{E} : y^2 = x^3 + \frac{a'}{a}x + \frac{b'}{b}$, there exists an isomorphic elliptic curve with coefficients in Z. Indeed, one can get rid of the denominators a and b using Prop. 2.1. So one can always suppose that E is defined by $y^2 = x^3 + mx + n$ for $m, n \in \mathbb{Z}$.

Let p be a prime which divides neither m nor n, one can reduce E to obtain the curve $\tilde{\mathrm{E}}$ defined by $y^2 = x^3 + \bar{m}x + \bar{n}$ where $\bar{m}$ and $\bar{n}$ are the reductions of m and n modulo p. Even if E is an elliptic curve, $\tilde{\mathrm{E}}$ is not necessarily an elliptic curve as it can have singular points. For example, if the discriminant Δ_{E} of E vanishes modulo a prime p, the reduction $\tilde{\mathrm{E}}$ will not necessarily define an elliptic curve over $\mathbb{F}_p$.

Example 4.1. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 = x^3 + 5$ of discriminant $\Delta_{\mathrm{E}} = -10800 = -2^4 \cdot 3^3 \cdot 5^2$. As 7 does not divide Δ_{E}, the reduction of E modulo 7 defines an elliptic curve over $\mathbb{F}_7$. Now consider the curve $\mathrm{E}_1/\mathbb{Q}$ defined by $y^2 = x^3 + 7^6 \cdot 5$ which, by Prop. 2.12, is isomorphic to E over $\mathbb{Q}$. One sees however that the reduction of E_1 modulo 7 does not produce an elliptic curve over $\mathbb{F}_7$.

In order to render the reduction of E dependent only on the isomorphism class of E, we define the *minimal discriminant* and the *minimal model* of an elliptic curve.

Definition 4.2. Let E be a rational elliptic curve. Let S be the set of rational elliptic curves E' that are isomorphic to E over $\mathbb{Q}$ with $\Delta'_{\mathrm{E}} \in \mathbb{Z}$. Then the *minimal discriminant* of E is the minimum of the following set.

$$\{|\Delta_{\mathrm{E}'}| : \mathrm{E}' \in \mathrm{S}\} \subset \mathbb{N}.$$

If E' is the curve with the minimal discriminant, we say E' is the *minimal model* of E.

As an immediate consequence of the above definition and Prop. 2.12, we have the following result.

Lemma 4.3. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve . Then, the minimal model of* E *is given by* $y^2 = x^3 + ax + b$ *with* $a, b \in \mathbb{Z}$ *such that*

$$\text{for all primes } p,\ p^4 \mid a \Rightarrow p^6 \nmid b.$$

Definition 4.4. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve with the minimal model E'. If a prime p does not divide $\Delta_{\mathrm{E}'}$, we say that E has *good reduction* at p, if not, we say E has *bad reduction* at p.

In Example 4.1, E_1 has good reduction at 7. Let us end this section with two important results. Recall that a rational polynomial with a rational root admits a root modulo every prime. Similar result holds for the points of finite order of an elliptic curve.

Theorem 4.5 ([Sil08, Ch. VII, Prop. 3.1])**.** *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve and* p *a prime of good reduction for* E*. Then we have the following reduction modulo* p *injective homomorphism of abelian groups*

$$\begin{array}{ccc} \mathrm{E}(\mathbb{Q})[m] & \hookrightarrow & \mathrm{E}(\mathbb{F}_p) \\ (x, y) & \mapsto & (x \bmod p, y \bmod p) \end{array}$$

Consequently, the order of $\mathrm{E}(\mathbb{Q})[m]$ *divides the order of* $\mathrm{E}(\mathbb{F}_p)$.

Finally we discuss briefly the size of elliptic curves over finite fields. Naturally they are finite groups. An important result about the size of an elliptic curve over a finite field is due to Hasse.

Theorem 4.6 ([Has36])**.** *Let* E *be an elliptic curve over a finite field* $\mathbb{F}_p$*. Then we have* $\#\mathrm{E}(\mathbb{F}_p) \in [(\sqrt{p} - 1)^2, (\sqrt{p} + 1)^2]$.

In SAGE, we can compute the minimal model of a rational elliptic curve, the order of an elliptic curve over a finite field.

```
sage: E = EllipticCurve([2*3^4, 3^6])
sage: E.minimal_model()
Elliptic Curve defined by y^2 = x^3 + 2*x + 1 over Rational Field
sage: E.has_good_reduction(3)
True
sage: E.change_ring(GF(53)).order()
59
```

5 The torsion point field

We now come to an important object of this work: the torsion point field. Recall that $\mathrm{E}[m] = \{\mathrm{P} \in \mathrm{E}(\overline{k}) \mid [m]\mathrm{P} = \mathcal{O}\}$.

Definition 5.1. Let E/k be an elliptic curve and $m > 0$ be an integer coprime to $p = \mathrm{char(k)}$ if $p > 0$. The *m-torsion point field* $k(\mathrm{E}[m])$ of an elliptic curve E is the extension of k obtained by adjoining the coordinates of $\mathrm{E}[m]$.

The torsion point fields can be seen as a generalization of cyclotomic fields. Their special properties enable us to study them further. For example, [Ade04] deals with the splitting of primes in torsion point fields.

Example 5.2. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 = x(x+1)(x-1)$ from Example 3.6. We have $\mathrm{E}[2] = \{(0,0),(1,0),(-1,0),\mathcal{O}\}$. Here $\mathbb{Q}(\mathrm{E}[2]) = \mathbb{Q}$. Let $\mathrm{E}_1/\mathbb{Q}$ be defined by $y^2 = x(x^2+1)$. We see that E_1 does not admit full 2-torsion over $\mathbb{Q}$. Over $\overline{\mathbb{Q}}$, the points of order 2 are $\{(0,0),(i,0),(-i,0),\mathcal{O}\}$ where i is a square root of -1 in $\overline{\mathbb{Q}}$. We obtain that $\mathbb{Q}(\mathrm{E}_1[2]) = \mathbb{Q}(i)$.

We end this section with the following lemma.

Lemma 5.3. *Let* E *be an elliptic curve over* $\mathbb{Q}$ *and* m *a positive integer. Then* $\mathbb{Q}(\mathrm{E}[m])$ *is a Galois extension of* $\mathbb{Q}$.

Proof. Let $\mathrm{E}[m] = \{\mathcal{O},(x_1,y_1),\ldots,(x_r,y_r)\}$. Then, by definition, $\mathbb{Q}(\mathrm{E}[m]) = \mathbb{Q}(x_1,y_1,\ldots,x_r,y_r)$. Let σ be a field homomorphism from $\mathbb{Q}(\mathrm{E}[m])$ to $\mathbb{C}$. It suffices to prove $\sigma(\mathbb{Q}(\mathrm{E}[m])) \subset \mathbb{Q}(\mathrm{E}[m])$. As $\mathbb{Q}(\mathrm{E}[m])$ is generated by x_i and y_i, σ can completely be determined by its action on x_i and y_i. Let us note that $\sigma(\mathcal{O}) = \mathcal{O}$ as $\mathcal{O}$ is a $\mathbb{Q}$-rational point. Let $\mathrm{P} = (x_i,y_i) \neq \mathcal{O}$ be a point of order dividing m then $\sigma(\mathrm{P}) = (\sigma(x_i),\sigma(y_i))$ is also a point of order dividing m. Indeed because,

$$\mathcal{O} = \sigma(\mathcal{O}) = \sigma([m]\mathrm{P}) = [m]\sigma(\mathrm{P}),$$

where the last equality follows because σ fixes $\mathbb{Q}$ and the addition law over E is defined using polynomials with coefficients from $\mathbb{Q}$. Consequently, $\sigma(\mathbb{Q}(\mathrm{E}[m])) \subset \mathbb{Q}(\mathrm{E}[m])$. □

Using SAGE, one can compute $\mathbb{Q}(\mathrm{E}[m])$ when m is a prime. These computations are quite expensive when $\mathbb{Q}(\mathrm{E}[m])$ is of large degree.

```
sage: E = EllipticCurve([1,1])
sage: time K.<alpha> = E.division_field(2)
CPU times: user 3.22 ms, sys: 1.32 ms, total: 4.54 ms
```

```
Wall time: 7.99 ms
sage: K.degree()
6
sage: K.defining_polynomial()
x^6 + 3*x^5 + 29*x^4 + 55*x^3 + 223*x^2 + 151*x + 379
sage: time K1.<beta> = E.division_field(3)
CPU times: user 874 ms, sys: 162 ms, total: 1.04 s
Wall time: 1.39 s
sage: K1.degree()
48
```

5.1 Division polynomials

Recall that, if E is given in a short Weierstrass form $y^2 = x^3 + ax + b$ and if $\mathrm{P} \in \mathrm{E}$ is a point of order 2 then the x-coordinate $x(\mathrm{P})$ of P is a root of $x^3 + ax + b$. Let us derive a similar condition for a point of order 3. If $\mathrm{P} = (x, y) \in \mathrm{E}$ is of order 3 then $-\mathrm{P} = [2]\mathrm{P}$. Then we have $x(-\mathrm{P}) = x([2]\mathrm{P})$. Using the group law, we have

$$\begin{aligned} x &= \left(\frac{3x^2 + a}{2y}\right)^2 - 2x \\ &= \frac{(3x^2 + a)^2}{4(x^3 + ax + b)} - 2x \end{aligned}$$

After simplifying, we obtain the condition

$$3x^4 + 6\,ax^2 + 12\,bx - a^2 = 0.$$

Thus the point P is of order 3 if, and only if, $x(\mathrm{P})$ is a root of the above polynomial. In fact, such polynomials exist in all cases.

Definition 5.4. Let a, b be variables. We define

$$\psi_1 = 1, \psi_2 = 2y,$$

$$\psi_3 = 3x^4 + 6\,ax^2 + 12\,bx - a^2,$$

$$\psi_4 = 2y(x^6 + 5\,ax^4 + 20\,bx^3 - 5\,a^2x^2 - 4\,abx - a^3 - 8\,b^2).$$

We further put recursively,

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \;\; m \geq 2,$$

$$\psi_{2m} = \frac{1}{2y}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \;\; m \geq 3.$$

ψ_m is called the *m-th division polynomial.*

Let us first see why they are polynomials.

Lemma 5.5. *If m is odd then $\psi_m \in \mathbb{Z}[a, b, x, y^2]$, and if m is even then $\psi_m \in 2y\mathbb{Z}[a, b, x, y^2]$.*

Proof. For $m < 5$, the lemma is true. Assume that $4y^2$ divides ψ_n for all $5 \leq n < 2m$. Then $m \geq 3$ and all polynomials used to define ψ_{2m} satisfy the induction hypothesis. Consider the following two cases depending on the parity of m:

1. If m is even then $m+2$ and $m-2$ are even. Thus ψ_m, ψ_{m+2} and ψ_{m-2} are in $2y\mathbb{Z}[a,b,x,y^2]$ and $4y^2$ divides $2y\psi_{2m}$. So we have $\psi_{2m} \in 2y\mathbb{Z}[a,b,x,y^2]$.

2. If m is odd then $m+1$ and $m-1$ are even. So ψ_{m+1} and ψ_{m-1} are in $2y\mathbb{Z}[a,b,x,y^2]$. As above, here too $4y^2$ divides $2y\psi_{2m}$. So again, $\psi_{2m} \in 2y\mathbb{Z}[a,b,x,y^2]$.

One can reason similarly for ψ_{2m+1}. □

The division polynomials have useful properties in relation to elliptic curves.

Proposition 5.6 ([Sil08, Ch. III, Exercise 3.7])**.** *Let* $\mathrm{E} : y^2 = x^3 + ax + b$ *be an elliptic curve and let* $\mathrm{P} \neq \mathcal{O} \in \mathrm{E}$*. Then we have,* P *is in* $\mathrm{E}[m]$ *if, and only if,* $\psi_m(\mathrm{P}) = 0$*.*

One can in fact use univariate polynomials obtained from ψ_m to characterise the points in $\mathrm{E}[m]$ (see [BSS99, Section III.4, p. 40]). Define

$$\bar{f}(m) = \begin{cases} \psi_m/\psi_2, & \text{if } m \text{ is even} \\ \psi_m, & \text{if } m \text{ is odd} \end{cases}$$

As we always evaluate division polynomials at a point on an elliptic curve $\mathrm{E} : y^2 = x^3 + ax + b$, we can replace y^2 by $x^3 + ax + b$ and see that $\bar{f}_m(n)$ is a polynomial in x. With this, we have the following.

Corollary 5.7 ([BSS99, Cor. III.7])**.** *Let* $\mathrm{E} : y^2 = x^3 + ax + b$ *be an elliptic curve and let* $\mathrm{P} \neq \mathcal{O} \in \mathrm{E}$*. Then we have,* P *is in* $\mathrm{E}[m]$*,* $m > 2$ *if, and only if,* $\bar{f}_m(x(\mathrm{P})) = 0$*.*

Remark 5.8. *Recall that there are* m^2 *points of* E *of order dividing* m*. Using this, we can compute the degree of* $\bar{f}_m$ *explicitly when* m *is odd. As each root of* $\bar{f}_m$ *gives exactly 2 points of order dividing* m *and as we do not take into account* $\mathcal{O}$*, we have* $\deg \bar{f}_m = \frac{m^2-1}{2}$*. For an even* m*, we have* $\deg \bar{f}_m = \frac{m^2-1-3}{2} = \frac{m^2-4}{2}$*. Here, the subtraction of* 3 *corresponds to the points of order 2.*

Henceforth, we shall, although it is an abuse of notation, treat $\bar{f}_m$ as the division polynomial ψ_m. In particular, we shall always consider them in one variable by replacing y^2 by $x^3 + ax + b$ whenever necessary.

Example 5.9. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 = x^3 + 21x - 26$. Here,

$$\begin{aligned} \psi_3(\mathrm{E}) &= 3x^4 + 126x^2 - 312x - 441 \\ &= 3(x-3)(x+1)(x^2+2x+49). \end{aligned}$$

We evaluate the equation defining E at $x = 3$ to see that $(3, \pm 8)$ is a point of order 3. At $x = -1$, we get $y^2 = -48$. So, E has another point of order 3 defined over $\mathbb{Q}(\sqrt{-3})$. In fact, $\mathbb{Q}(\mathrm{E}[3]) = \mathbb{Q}(\sqrt{-3})$. On the other hand, by Corollary 3.9, we have $\mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\sqrt{-3})$ where $\zeta_3 \in \overline{\mathbb{Q}}$ is a primitive cubic root of unity. As they both have the same degree of extension, we have $\mathbb{Q}(\mathrm{E}[3]) = \mathbb{Q}(\zeta_3)$.

Example 5.10. Let $\mathrm{E}'/\mathbb{Q}$ be defined by $y^2 = x^3 + 21x + 26$. Here, $\psi_3(\mathrm{E}')$ has the roots -1 and 3. Evaluating the equation defining E' at them gives $y^2 = 48$ and $y^2 = -64$. Thus $\mathrm{E}'(\mathbb{Q})[3] = \{\mathcal{O}\}$. However over the quartic extension $\mathbb{Q}(i, \sqrt{3})$, the points $(-1, 4\sqrt{3})$ and $(3, 8i)$ generate $\mathrm{E}[3]$.

The division polynomials can be quite cumbersome for bigger values of m. However as they are defined using a recurrence relation, it is easy to compute them. We would also like to define a polynomial describing the x-coordinates of points of order *exactly* m.

Definition 5.11. Let E/k be an elliptic curve and m a positive integer. Let

$$\psi_m^{\text{new}} = \prod_{\text{P of order m}} (x - x[\mathrm{P}]).$$

We call ψ_m^{new} the new m-th division polynomial.

One can see that ψ_m^{new} is in fact defined over $\mathbb{Q}$. Indeed, as it can be obtained by dividing ψ_m by ψ_d^{new} for all divisors $d \neq m$ of m.

Example 5.12. Let E be defined by $y^2 = x^3 + ax + b$. We have

$$\psi_4 = \underbrace{(2y)}_{\psi_2} \underbrace{\left(x^6 + 5\,ax^4 - 5\,a^2x^2 + 20\,bx^3 - a^3 - 4\,abx - 8\,b^2\right)}_{\psi_4^{\text{new}}}.$$

Using the recurrence relation from Definition 5.4, SAGE computes division polynomials quite rapidly.

```
sage: E = EllipticCurve([a,b])
sage: E.division_polynomial(3)
3*x^4 + 6*a*x^2 + 12*b*x - a^2
sage: E.division_polynomial(10).degree()
51
```

5.2 Construction of torsion point fields

One uses division polynomials ψ_m and ψ_m^{new} in order to explicitly construct torsion point fields. In order to construct the m-torsion point field $\mathbb{Q}(\mathrm{E}[m])$, we construct $\mathbb{Q}(\mathrm{E}[\ell^n])$ for all prime-power divisors ℓ^n of m and we then take the compositum of all of them. This method can be adapted to any number field. We then proceed to the construction of torsion point fields over finite fields. Let $\mathrm{E} : y^2 = x^3 + ax + b$ be a rational elliptic curve and ℓ a prime divisor of m. As $\mathrm{E}[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, it suffices to construct the field containing the coordinates of a basis $(\mathrm{P}_1, \mathrm{P}_2)$ of $\mathrm{E}[\ell]$. Let ψ_ℓ be the ℓ-th division polynomial. Put $\psi_2 = x^3 + ax + b$.

1. We first make an extension of $\mathbb{Q}$ by an irreducible non-linear factor of ψ_ℓ to obtain a number field K_1. If ψ_ℓ splits over $\mathbb{Q}$, we set $\mathrm{K}_1 = \mathbb{Q}$. By construction, K_1 contains the x-coordinate x_1 of a point P_1 of order ℓ.

2. We then check whether $\psi_2(x_1)$ is a square in K_1. If it is not, we make an extension K_2 of K_1 by adjoining $\sqrt{\psi_2(x_1)}$ to it. If $\psi_2(x_1)$ is a square in K_1, we set $\mathrm{K}_2 = \mathrm{K}_1$. By construction K_2 contains a point P_1 of order ℓ and also all its multiples.

3. We now need a point P_2 of order ℓ and which is not a scalar multiple of P_1. As K_2 contains all those scalar multiples, we have to factor ψ_ℓ over K_2 to see whether there is an irreducible non-linear factor. If there is one such factor, we extend K_2 by it to obtain K_3. If ψ_ℓ splits in K_2, we set $\mathrm{K}_3 = \mathrm{K}_2$. As in the first step, K_3 contains the x-coordinate x_2 of a point of order ℓ, say P_2 which is not a scalar multiple of P_1.

4. Finally, we check whether $\psi_2(x_2)$ is a square in K_3. If not, we adjoin $\sqrt{\psi_2(x_2)}$ to K_3 to obtain K_4. If $\psi_2(x_2)$ is a square in K_3, we set $\mathrm{K}_4 = \mathrm{K}_3$. By construction, the curve E admits two linearly independent points of order ℓ over K_4. Thus $\mathbb{Q}(\mathrm{E}[\ell]) = \mathrm{K}_4$.

One constructs $\mathbb{Q}(\mathrm{E}[\ell^n])$ recursively. Having constructed $\mathbb{Q}(\mathrm{E}[\ell^{n-1}])$, one can construct $\mathbb{Q}(\mathrm{E}[\ell^n])$ over it using the 4 extensions given above where we replace, ψ_ℓ by $\psi_{\ell^n}^{\mathrm{new}}$ and adjoin the square roots of $\psi_2(x)$ where x is not taken from the set $\{x(\mathrm{P}_1 + \mathrm{M}) \mid \mathrm{M} \in \mathrm{E}[\ell^{n-1}]\}$. Finally, $\mathbb{Q}(\mathrm{E}[m])$ is the compositum of $\mathbb{Q}(\mathrm{E}[\ell^n])$ for all prime-power divisors ℓ^n of m.

This method is computationally expensive and only practical for torsion point fields having smaller degrees, say less than 50.

Remark 5.13. *Alternatively, as $\mathbb{Q}(\mathrm{E}[\ell])$ contains all the roots of ψ_ℓ, one can compute the splitting field of ψ_ℓ and then make a quadratic extension if necessary to obtain the necessary y-coordinates. We will see in Lemma 9.4 that at most only one extension suffices to obtain $\mathbb{Q}(\mathrm{E}[\ell])$ over the splitting field of ψ_ℓ. In fact this method works for any integer, prime or not. This method too is computationally expensive.*

Unlike over number fields where we need at most 4 extensions to construct $\mathbb{Q}(\mathrm{E}[\ell])$, over finite fields, one can do it in 2 extensions as we shall see now.

Let $q = p^i$ be a prime-power where $p > 3$. Let $\mathbb{F}_q$ be the finite field with q elements and $\mathrm{E} : y^2 = x^3 + ax + b$ be an elliptic curve over $\mathbb{F}_q$. Let m be an integer coprime to p. Like over number fields, the main ingredient here is the division polynomial ψ_m. We put $\psi_2 = x^3 + ax + b$.

1. We first factor ψ_m over $\mathbb{F}_q$ and compute its splitting field $\mathbb{F}_{q'}$ (cf. [VZGG13, Ch. 14]).

2. We then compute the set X_1 of roots of ψ_m over $\mathbb{F}_{q'}$. For each $x \in \mathrm{X}_1$, we check whether $\psi_2(x)$ is a square in $\mathbb{F}_{q'}$. If for some $x \in \mathrm{X}_1$, $\psi_2(x)$ is not a square, we set $\mathbb{F} = \mathbb{F}_{q'^2}$. If for all $x \in \mathrm{X}_1$, $\psi_2(x)$ is a square in $\mathbb{F}_{q'}$ then we set $\mathbb{F} = \mathbb{F}_{q'}$. In both cases $\mathbb{F}$ contains every root of ψ_m and the corresponding values of y-coordinates and thus $\mathrm{E}(\mathbb{F})$ has 2 linearly independent points of order m and admits full m-torsion over $\mathbb{F}$.

Over finite fields, computations are rapid and one can construct torsion point fields for higher torsion.

Example 5.14. Let $\mathrm{E} : y^2 = x^3 + 3x + 5$ be a rational elliptic curve. In order to construct $\mathbb{Q}(\mathrm{E}[3])$, we follow the procedure and make 4 extensions. In fact one can see using the online complement of this work (available at [BS19b]) that all 4 extensions are required and they are of degree 4, 2, 3 and 2 respectively. This gives us the degree of $\mathbb{Q}(\mathrm{E}[3]) = 4 \times 2 \times 3 \times 2 = 48$. Over

6 Galois representation

We can now define the central object of this work: Galois representation attached to an elliptic curve. We shall define three types of representations.

6.1 mod m Galois representation

Let $\mathrm{E} : y^2 = x^3+ax+b$ be a rational elliptic curve. We use the notations of Serre [Ser71]. Let P_1 and P_2 be such that

$$\mathrm{E}[m] = \frac{\mathbb{Z}}{m\mathbb{Z}}\mathrm{P}_1 + \frac{\mathbb{Z}}{m\mathbb{Z}}\mathrm{P}_2.$$

Let $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and let $\mathrm{P} = (x, y) \in \mathrm{E}$. We define the action of σ on P using its action on the coordinates of P. In other words, $\sigma(\mathrm{P}) = (\sigma(x), \sigma(y))$. One can see that $(\sigma(x), \sigma(y))$ is indeed a point on E as

$$\begin{aligned}\sigma(y)^2 &= \sigma(x^3) + \sigma(a)\sigma(x) + \sigma(b)\\ &= \sigma(x^3) + a\sigma(x) + b,\end{aligned}$$

as σ fixes $\mathbb{Q}$. We put $\sigma(\mathcal{O}) = \mathcal{O}$ which makes sense as $\mathcal{O} = [0, 1, 0]$ is a $\mathbb{Q}$-rational point of E and σ fixes $\mathbb{Q}$. Furthermore if P is a point of order m, $\sigma(\mathrm{P})$ is also a point of order m. For, the equality $[m]\mathrm{P} = \mathcal{O}$ can be translated using polynomials defined over $\mathbb{Q}$.

Definition 6.1. The mod m Galois representation attached to E is the following map.

$$\begin{array}{rccc}\rho_{\mathrm{E},m}: & \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) & \to & \mathrm{Aut}(\mathrm{E}[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})\\ & \rho & \mapsto & \left(\begin{smallmatrix} a & c\\ b & d\end{smallmatrix}\right),\end{array}$$

where $a, b, c, d \in \mathbb{Z}/m\mathbb{Z}$ such that $\sigma(\mathrm{P}_1) = a\mathrm{P}_1 + b\mathrm{P}_2$ and $\sigma(\mathrm{P}_2) = c\mathrm{P}_1 + d\mathrm{P}_2$.

We refer to $\mathrm{Im}\rho_{\mathrm{E},m}$ as the mod m Galois image of E and the integer m as the *level of* $\mathrm{Im}\rho_{\mathrm{E},m}$.

Remark 6.2. 1. *Some authors (for example [RZB15]) consider the right action to define the mod m Galois image. The image they obtain is transposed with respect to the image obtained from the left action under the same basis.*

2. *Naturally the mod m Galois image is defined only up to conjugacy in* $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ *as it depends on the choice of basis of* $\mathrm{E}[m]$.

Some authors (for example [BBB+13, RV01]) define mod m Galois representation using $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q})$ in the similar manner as above. Both approaches yield the same representation as

$$\mathrm{Im}\rho_{\mathrm{E},m} \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\ker \rho_{\mathrm{E},m}} \cong \frac{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mathrm{E}[m]))} \cong \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q}).$$

This enables us to compute explicit mod m Galois images and we do want to compute many of them!

Note that the mod m Galois representation defined using $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q})$ is necessarily injective. Indeed, because any $\sigma \in \ker \phi_{\mathrm{E},m}$ which fixes P_1 and P_2 would fix all of $\mathbb{Q}(\mathrm{E}[m])$. We are particularly interested when $\rho_{\mathrm{E},m}$ is not surjective.

Definition 6.3. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve without complex multiplication and $m > 0$ an integer. We say that $\mathrm{Im}\rho_{\mathrm{E},m}$ is *exceptional* if $\rho_{\mathrm{E},m}$ is not surjective. In this case, we say m is exceptional for E.

Example 6.4. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 = x(x^2+1)$. We saw in Example 5.2 that $\mathbb{Q}(\mathrm{E}[2]) = \mathbb{Q}(i)$ and $\mathrm{E}[2] = \{(0,0),(i,0),(-i,0),\mathcal{O}\}$. Clearly any two points of order 2 would form a basis of $\mathrm{E}[2]$. Put $\mathrm{P}_1 = (0,0)$ and $\mathrm{P}_2 = (i,0)$. Furthermore the action of elements of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ over $\mathbb{Q}(i)$ is completely determined by their action on i. There are two types of elements: σ_i which is identity over $\mathbb{Q}(i)$ and σ_{-i} which sends i to $-i$. We then have

$$\begin{aligned}\sigma_i(\mathrm{P}_1) &= \mathrm{P}_1 = 1\cdot\mathrm{P}_1 + 0\cdot\mathrm{P}_2\\ \sigma_i(\mathrm{P}_2) &= \mathrm{P}_2 = 0\cdot\mathrm{P}_1 + 1\cdot\mathrm{P}_2.\end{aligned}$$

Thus $\rho_{\mathrm{E},2}(\sigma_i) = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$. Similarly for σ_{-i}, we have

$$\begin{aligned}\sigma_{-i}(\mathrm{P}_1) &= \mathrm{P}_1 = 1\cdot\mathrm{P}_1 + 0\cdot\mathrm{P}_2\\ \sigma_{-i}(\mathrm{P}_2) &= (-i,0) = 1\cdot\mathrm{P}_1 + 1\cdot\mathrm{P}_2.\end{aligned}$$

Here we have $\rho_{\mathrm{E},2}(\sigma_{-i}) = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$. Thus the mod 2 Galois image attached to E is the subgroup of order 2 generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ in $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. As $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ has 6 elements, $\mathrm{Im}\rho_{\mathrm{E},2}$ is exceptional.

One can obtain several details about the mod m Galois image attached to an elliptic curve using SAGE.

```
sage: E = EllipticCurve([9,18])
sage: G = E.galois_representation()
sage: G.non_surjective()
[3, 5]
sage: G.is_surjective(7)
True
```

6.2 ℓ-adic Galois representation

We often would like to consider several representations at a time. This is done using the Tate module which can be constructed in a similar way as p-adic numbers, see [Gou97].

Definition 6.5. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and $\ell \in \mathbb{Z}$ a prime. The ℓ-adic Tate module of E is

$$\mathrm{T}_\ell(\mathrm{E}) = \varprojlim_n \mathrm{E}[\ell^n],$$

where the inverse limit is with respect to the map $\mathrm{E}[\ell^{n+1}] \xrightarrow{[\ell]} \mathrm{E}[\ell^n]$.

Simply put, an element of $\mathrm{T}_\ell(\mathrm{E})$ is a sequence P_n of points in E where each P_n is of order dividing ℓ^n and $\mathrm{P}_n = [\ell]\mathrm{P}_{n+1}$. As in the case of $\mathrm{E}[\ell]$, the Tate module $\mathrm{T}_\ell(\mathrm{E})$ is isomorphic to $\mathbb{Z}_\ell\times\mathbb{Z}_\ell$, see [Sil08, Ch. III, Prop. 7.1] where $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers. We choose compatible basis for every $\mathrm{E}[\ell^n]$ and define the ℓ-adic Galois representation of E the following map,

$$\rho_{\mathrm{E},\ell^\infty} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{T}_\ell(\mathrm{E})) \cong \mathrm{GL}_2(\mathbb{Z}_\ell).$$

We refer to $\mathrm{Im}\rho_{\mathrm{E},\ell^\infty}$ as ℓ-adic Galois image.

Remark 6.6. *This is subtle. A priori, in order to give an ℓ-adic Galois image explicitly, one might have to give an infinite collection of generators of matrix groups. However, thanks to the following theorem, called the open image theorem, of Serre, only finitely many generators are sufficient.*

Theorem 6.7 ([Ser71, Theorem 3, p. 299])**.** *Let* E *be a rational elliptic curve without complex multiplication. Then,*

1. *For all primes ℓ outside a finite set $\mathcal{S}_{\mathrm{E}}$ depending on* E *and for all $k \geq 1$, $\rho_{\mathrm{E},\ell^k}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q})) = \mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$.*
2. *For a prime $\ell \in \mathcal{S}_{\mathrm{E}}$ and $k \geq 1$, the sequence*

$$\iota_k = [\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) : \rho_{\mathrm{E},\ell^k}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q}))]$$

is non-decreasing and eventually stationary.

By Serre's open image theorem, for *almost all* primes ℓ, $\rho_{\mathrm{E},\ell^\infty}$ is surjective and for the primes ℓ where $\rho_{\mathrm{E},\ell^\infty}$ is not surjective, one can determine the image of $\rho_{\mathrm{E},\ell^\infty}$ using $\rho_{\mathrm{E},\ell^k}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q}))$ for only finitely many values of k. We will use this theorem and its applications on several occasions in this work.

Remark 6.8. *When $\mathrm{E}/\mathbb{Q}$ has complex multiplication and $m > 2$, $\mathrm{Im}\rho_{\mathrm{E},m}$ is always exceptional. In fact, the extension $\mathbb{Q}(\mathrm{E}[m])$ is an abelian extension of a quadratic imaginary extension of $\mathbb{Q}$ (see [Sil13, Theorem 2.3]).*

6.3 Adelic Galois representation

Finally, we combine ℓ-adic Galois representations for all primes ℓ to define the adelic Galois representation of an elliptic curve. Put

$$\hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

As a consequence of the Chinese Remainder Theorem, we have $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$. Remark that $\hat{\mathbb{Z}} \neq \prod_n \mathbb{Z}/n\mathbb{Z}$, as the latter can contain any arbitrary sequence.

Example 6.9. $a = (\cdots, (0 \bmod 4), (1 \bmod 3), (1 \bmod 2), (1 \bmod 1)) \in \prod_n \mathbb{Z}/n\mathbb{Z}$, however $a \notin \hat{\mathbb{Z}}$.

We then define the following.

Definition 6.10. The adelic Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is induced by its action on $\mathrm{E}_{\mathrm{tors}}$, the points of finite order of $\mathrm{E}(\overline{\mathbb{Q}})$.

$$\rho_{\mathrm{E}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathrm{E}_{\mathrm{tors}}) \cong \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

When it is clear from the context, we will refer to it as the Galois representation of E and we call its image the Galois image of E.

Let us end this chapter by mentioning that over $\mathbb{Q}$, ρ_{E} is never surjective. Serre, while responding to a question of Tate, mentions in [CS15, p. 424] (and proves in [Ser71, Section 5]) that $\mathrm{E}/\mathbb{Q}$ defined by $y^2 + y = x^3 - x$ has surjective ℓ-adic Galois image for all primes ℓ. However, the image of ρ_{E} is contained an index 2 subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. This is indeed the case for all rational elliptic curves (see [Ser71, Prop. 22]).

Greicius in [Gre10] gives an example of a curve E defined over a cubic number field for which ρ_{E} is surjective.

Chapter 2

Subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and Galois images

In Chapter 1, we defined the mod ℓ Galois representation attached to an elliptic curve. As its image is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ up to conjugacy, it is not without interest to discuss the subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. In this chapter, we do so and establish various properties of Galois images. We also describe the local-global behaviour of Galois images. Finally, we shall describe two algorithms that test whether $\rho_{\mathrm{E},\ell}$ is surjective without explicitly constructing the ℓ-torsion point field.

Let us start with some definitions and results from group theory. These are classical objects and can readily be found in any standard algebra textbook, for example, [Her06, DF04].

Definition 6.11. Let G be a group and $\mathrm{S} \subset \mathrm{G}$, a subset of G. The *centralizer* $\mathrm{C}(\mathrm{S})$ of S is the set

$$\mathrm{C}(\mathrm{S}) = \{g \in \mathrm{G} \mid gs = sg \text{ for all } s \in \mathrm{S}\}.$$

And the *normalizer* $\mathrm{N}(\mathrm{S})$ of S is the set

$$\mathrm{N}(\mathrm{S}) = \{g \in \mathrm{G} \mid g\mathrm{S} = \mathrm{S}g\}.$$

Remark 6.12. *If* $\mathrm{S} = \{s\}$*, we denote* $\mathrm{C}(\mathrm{S})$ *by* C_s*. If* S *is a subgroup of* G*, then* $\mathrm{N}(\mathrm{S})$ *is the largest subgroup of* G *in which* S *is normal.*

Definition 6.13. Let G be a group and $g, h \in \mathrm{G}$. If there exists $s \in \mathrm{G}$ such that $g = shs^{-1}$, we say g is a G-*conjugate* of h via s (or h is a G-conjugate of g via s^{-1}). The set Cl_g of conjugates of g is called the *conjugacy class* of g.

When it is clear from the context, we omit the prefix G and just say g is a conjugate of h. Similarly, we say that two subgroups H_1 and H_2 of G are G-conjugates via $g \in \mathrm{G}$ if $\mathrm{H}_1 = g\mathrm{H}_2 g^{-1}$.

Example 6.14. Let $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ and consider $\mathrm{G}_1 = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle \subset \mathrm{G}$ and $\mathrm{G}_2 = \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \rangle \subset \mathrm{G}$. One can verify that G_1 and G_2 are not G-conjugate, however every element of G_1 is conjugated to an element of G_2 via an element of G, not necessarily unique.

Consider the action of G on itself via conjugation by $g \in \mathrm{G}$.

$$\begin{array}{rccc} c_g : & \mathrm{G} & \longrightarrow & \mathrm{G} \\ & h & \mapsto & ghg^{-1} \end{array}$$

Under this action, the orbit $\mathrm{Orbit}(h)$ of $h \in \mathrm{G}$ is the conjugacy class Cl_h of h and the stabilizer $\mathrm{Stab}(h)$ is the centralizer C_h of h. Thus by the orbit-stabilizer theorem, we have

$$\#\mathrm{Cl}_h = \frac{\#\mathrm{G}}{\#\mathrm{C}_h}.$$

7 Structure of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

This section is based on [Ser71] and [Sut16]. Let ℓ be an odd prime unless specified otherwise. We identify $\mathbb{Z}/\ell\mathbb{Z}$ with $\mathbb{F}_\ell$, the finite field with ℓ elements. Let ${\mathbb{F}_\ell}^*$ denote the multiplicative group of units in $\mathbb{F}_\ell$.

7.1 Subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Let ϵ be a non-square element in $\mathbb{F}_\ell$.

Definition 7.1. Put

$$\mathrm{C}_{sp}(\ell) := \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \;\middle|\; ab \neq 0 \right\},$$

$$\mathrm{C}_{nsp}(\ell) := \left\{ \left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right) \;\middle|\; (a,b) \neq (0,0) \right\},$$

$$\mathrm{B}(\ell) := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \;\middle|\; ad \neq 0 \right\}.$$

1. A *split Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is a subgroup $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$-conjugated to $\mathrm{C}_{sp}(\ell)$.
2. A *non-split Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is a subgroup $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$-conjugated to $\mathrm{C}_{nsp}(\ell)$.
3. A *Borel subgroup* of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is a subgroup $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$-conjugated to $\mathrm{B}(\ell)$.

When we say a Cartan subgroup, we mean either a split or a non-split Cartan subgroup.

Remark 7.2. *1. $\mathrm{C}_{sp}(\ell)$ is abelian, $\mathrm{C}_{nsp}(\ell)$ is isomorphic to ${\mathbb{F}_{\ell^2}}^*$ and thus cyclic and $\mathrm{B}(\ell)$ is non-abelian for $\ell \geq 3$. Note that $\mathrm{B}(2)$ is abelian.*

2. We have $\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) = (\ell^2-\ell)(\ell^2-1)$, $\#\mathrm{C}_s(\ell) = (\ell-1)^2$, $\#\mathrm{C}_{nsp}(\ell) = \ell^2-1$ and $\#\mathrm{B}(\ell) = \ell(\ell-1)^2$. In particular, an element of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of order ℓ cannot be in $\mathrm{C}_{sp}(\ell) \cup \mathrm{C}_{nsp}(\ell)$.

3. The center $\mathrm{Z}(\ell)$ of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ consists of scalar matrices $\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right)$ where $x \in (\mathbb{Z}/\ell\mathbb{Z})^*$.

4. $\mathrm{C}_{sp}(\ell) \cap \mathrm{C}_{nsp}(\ell) = \mathrm{Z}(\ell)$.

5. When it is clear from the context, we shall denote $\mathrm{C}_{sp}(\ell)$ and $\mathrm{C}_{nsp}(\ell)$ simply by C_{sp} and C_{nsp} respectively.

Let us describe the normalizers of split and non-split Cartan subgroups.

Proposition 7.3 ([Sut16, Section 3])**.** *Let* C_{sp} *and* C_{nsp} *as above. Then,* $\mathrm{N}(\mathrm{C}_{sp}) = \mathrm{C}_{sp} \cup \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right) \mathrm{C}_{sp}$ *and* $\mathrm{N}(\mathrm{C}_{nsp}) = \mathrm{C}_{nsp} \cup \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \mathrm{C}_{nsp}$*. Furthermore, for all* $g \in \mathrm{N}(\mathrm{C}_{sp}) - \mathrm{C}_{sp}$*, the trace* $\mathrm{tr}(g)$ *of* g *is* 0*.*

Example 7.4. Let $\ell = 3$ and fix $\epsilon = 2$. We have,

1. $\mathrm{C}_{sp}(3) = \left\langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right) \right\rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

2. $\mathrm{C}_{nsp}(3) = \left\langle \left(\begin{smallmatrix} 1 & 2 \\ 1 & 1 \end{smallmatrix}\right) \right\rangle \cong \mathbb{Z}/8\mathbb{Z}$.

3. $\mathrm{B}(3) = \left\langle \left(\begin{smallmatrix} 2 & 1 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle \cong \mathrm{D}_{12}$, the dihedral group with 12 elements.

The subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ can be classified in terms of their images in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) := \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/\mathrm{Z}(\ell)$.

Proposition 7.5 (Dickson's classification [Dic03])**.** *Let* ℓ *be an odd prime and let* G *be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *with image* H *in* $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$*. If* G *contains an element of order* ℓ *then either* G *is in a Borel subgroup or* $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{G}$*. Otherwise one of the followings holds:*

1. H *is cyclic and* G *is in a Cartan subgroup;*

2. H *is dihedral and* G *is in the normalizer of a Cartan subgroup, but not in any Cartan subgroup;*

3. H *is isomorphic to* A_4 *or* S_4 *or* A_5 *and* G *is not contained in the normalizer of any Cartan subgroup.*

Proof. We shall briefly discuss a proof given by Swinnerton-Dyer in [SD73, Lemma 2] and [Lan12, Theorem XI.2.3]. Let V denote the vector space $(\mathbb{Z}/\ell\mathbb{Z})^2$. Let us first suppose that G contains an element g of order ℓ. Then g is conjugate to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and there is a unique one dimensional eigenspace W of V fixed by g. If every element of G has W as an eigenspace then G is contained in a Borel subgroup. If not, there exists $f \in \mathrm{G}$ such that $f(\mathrm{W}) = \mathrm{W}'$ where W' is another one-dimensional subspace of V. Then fgf^{-1} is of order ℓ and admits a unique eigenspace W'. Considering W and W' as coordinate axis of V, one can write,

$$g = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \text{ and } fgf^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ c & 1 \end{smallmatrix}\right),$$

for some non-zero $b, c \in \mathbb{Z}/\ell\mathbb{Z}$. As these matrices generate $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we have that $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{G}$.

Let us now suppose that G does not contain an element of order ℓ. Then the same is true of H. So every non-trivial element (i.e. an element that is not scalar in G) of H has exactly two eigenvectors, possibly over $\mathbb{F}_{\ell^2}$. It can be shown that if two elements of H have one eigenvector in common then they have the same two eigenvectors. The set of eigenvectors of non-trivial elements of H is finite and invariant under H. Let $\omega_1, \ldots, \omega_n$ be representatives of the orbits under the action of H. For ω_i, let μ_i denote the number of elements of H which fix ω_i. Thus there are $\mu_i - 1$ non-trivial elements of H which fix ω_i. If h is the order of H, then the orbit of ω_i has exactly h/μ_i elements.

By counting the pairs formed by a non-trivial element of H and an eigenvector of it in two different ways, we obtain the following.

$$2h-2=\frac{h(\mu_1-1)}{\mu_1}+\cdots+\frac{h(\mu_n-1)}{\mu_n}.$$

We can rewrite this equality in the following form.

$$2\left(1-\frac{1}{h}\right)=\left(1-\frac{1}{\mu_1}\right)+\cdots+\left(1-\frac{1}{\mu_n}\right).$$

Recall that μ_i divides h. If $\mu_i=h$ for some i, then clearly $n=2$ and $\mu_1=\mu_2=h$. Furthermore we have $n\leq 3$. Indeed, if $n\geq 4$, the right hand side is at least 2. However the left hand side is strictly less 2.

Suppose now $n=3$. Then $\mu_i=2$ for some i. Indeed, if all three of them were ≥ 3, the right hand side would be ≥ 2. Thus h is even. Let $2=\mu_1\leq\mu_2\leq\mu_3$. If $\mu_3=h/2$, then we must have $\mu_1=\mu_2=2$.

Suppose now $\mu_3<h/2$. Then one can verify that $\mu_2=3$. Finally assuming $\mu_1=2$ and $\mu_2=3$, we must have $\mu_3\in\{3,4,5\}$.

We have the following 5 cases.

1. $n=2$, $\mu_1=\mu_2=h$.
2. $n=3$, h even, $\mu_1=\mu_2=2$, $\mu_3=h/2$.
3. $n=3$, $h=12$, $\mu_1=2$, $\mu_2=\mu_3=3$.
4. $n=3$, $h=24$, $\mu_1=2$, $\mu_2=3$, $\mu_3=4$.
5. $n=3$, $h=60$, $\mu_1=2$, $\mu_2=3$, $\mu_3=5$.

The first two cases correspond to the first two cases of the proposition and the last three cases above correspond to the third one. □

7.2 Conjugacy classes of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Let $g=\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Its characteristic polynomial is

$$\chi(g)=x^2-(a+d)x+(ad-bc)=x^2-\mathrm{tr}(g)+\det(g).$$

As conjugate matrices have the same characteristic polynomial, they have the same determinant and the trace. However, the converse is not true. For example, $\left(\begin{smallmatrix} 1 & 0\\ 0 & 1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1\\ 0 & 1\end{smallmatrix}\right)$ have the same trace and determinant but they are not conjugated. Albeit $\chi(g)$ does not determine g up to conjugacy in general, in dimension 2, it does except if it has a double root.

Consider the roots λ_1 and λ_2 of $\chi(g)$, possibly in $\mathbb{F}_{\ell^2}$. One then computes the centralizer C_g of g. Finally, by the orbit-stabilizer theorem, one determines the size of the conjugacy class Cl_g of g. Depending on λ_1 and λ_2, we have the following cases.

1. If $\lambda_1\neq\lambda_2$ and are in $\mathbb{F}_\ell$ then g is a conjugate of $\left(\begin{smallmatrix} \lambda_1 & 0\\ 0 & \lambda_2\end{smallmatrix}\right)$. Note that $\left(\begin{smallmatrix} \lambda_1 & 0\\ 0 & \lambda_2\end{smallmatrix}\right)$ is a conjugate of $\left(\begin{smallmatrix} \lambda_2 & 0\\ 0 & \lambda_1\end{smallmatrix}\right)$ via $\left(\begin{smallmatrix} 0 & 1\\ 1 & 0\end{smallmatrix}\right)$. Thus, as λ_1 and λ_2 are both non-zero and distinct, there are $\binom{\ell-1}{2}=\frac{(\ell-1)(\ell-2)}{2}$ such conjugacy classes. One can verify with

explicit calculations that the centralizer $\mathrm{C}_g = \left\{ \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \;\middle|\; a \neq 0, b \neq 0 \right\}$. In particular, $\#\mathrm{C}_g = (\ell-1)^2$. Finally, by the orbit-stabilizer theorem,

$$\#\mathrm{Cl}_g = \frac{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}{\#\mathrm{C}_g} = \frac{(\ell^2-1)(\ell^2-\ell)}{(\ell-1)^2} = \ell(\ell+1).$$

2. If $\lambda_1 = \lambda_2$ then g is a conjugate of $\left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_1 \end{smallmatrix}\right)$ or of $\left(\begin{smallmatrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{smallmatrix}\right)$ and in each case, there are $\ell-1$ choices for λ_1 and thus for the conjugacy classes. Clearly, in the first case, $\mathrm{C}_g = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and in the second case one obtains that $\mathrm{C}_g = \{\left(\begin{smallmatrix} x & t \\ 0 & x \end{smallmatrix}\right) \mid x \neq 0\}$. So $\#\mathrm{C}_g = (\ell^2-1)(\ell^2-\ell)$ in the first case and $\#\mathrm{C}_g = \ell(\ell-1)$ in the second. So in the first case,

$$\#\mathrm{Cl}_g = \frac{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}{\#\mathrm{C}_g} = \frac{(\ell^2-1)(\ell^2-\ell)}{(\ell^2-1)(\ell^2-\ell)} = 1,$$

and in the second case,

$$\#\mathrm{Cl}_g = \frac{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}{\#\mathrm{C}_g} = \frac{(\ell^2-1)(\ell^2-\ell)}{(\ell^2-\ell)} = \ell^2-1.$$

3. If λ_1 and λ_2 are not in $\mathbb{F}_\ell$ then they are in $\mathbb{F}_{\ell^2}$ and we have $\lambda_1 = \alpha + \sqrt{\epsilon}\beta$ and $\lambda_2 = \alpha - \sqrt{\epsilon}\beta$ for some α and $\beta \in \mathbb{F}_\ell$ with $\beta \neq 0$. Recall that ϵ is a non-square element in $\mathbb{F}_\ell$. So in this case, g is a conjugate of $\left(\begin{smallmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{smallmatrix}\right)$. As $\left(\begin{smallmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{smallmatrix}\right)$ is a conjugate of $\left(\begin{smallmatrix} \alpha & -\epsilon\beta \\ -\beta & \alpha \end{smallmatrix}\right)$ via $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, there are $\frac{\ell-1}{2}$ choices for β and ℓ for α. Thus there are $\binom{\ell}{2} = \frac{\ell(\ell-1)}{2}$ such conjugacy classes. By explicit computations, one verifies that $\mathrm{C}_g = \{\left(\begin{smallmatrix} t & \epsilon w \\ w & t \end{smallmatrix}\right) \mid (t,w) \neq (0,0)\}$ and $\#\mathrm{C}_g = \ell^2-1$. So by the orbit-stabilizer theorem,

$$\#\mathrm{Cl}_g = \frac{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}{\#\mathrm{C}_g} = \frac{(\ell^2-1)(\ell^2-\ell)}{(\ell^2-1)} = \ell^2-\ell.$$

We summarize the above discussion by a classical result.

Theorem 7.6. *Let $g \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, let C_g denote the centralizer of g and let Cl_g denote the conjugacy class of g. Then,*

1. *If g is conjugate to $\left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ for $\lambda_1 \neq \lambda_2$ then we have $\#\mathrm{C}_g = (\ell-1)^2$, $\#\mathrm{Cl}_g = \ell(\ell+1)$ and the number of such conjugacy classes is $\frac{(\ell-1)(\ell-2)}{2}$.*

2. *If g is conjugate to $\left(\begin{smallmatrix} \lambda & 0 \\ 0 & \lambda \end{smallmatrix}\right)$ for $\lambda \neq 0$ then we have $\#\mathrm{C}_g = (\ell-1)^2(\ell+1)\ell$, $\#\mathrm{Cl}_g = 1$ and the number of such conjugacy classes is $(\ell-1)$.*

3. *If g is conjugate to $\left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$ for $\lambda \neq 0$ then we have $\#\mathrm{C}_g = \ell(\ell-1)$, $\#\mathrm{Cl}_g = \ell^2-1$ and the number of such conjugacy classes is $\ell-1$.*

4. *If g is conjugate to $\left(\begin{smallmatrix} \alpha & \epsilon\beta \\ \beta & \alpha \end{smallmatrix}\right)$ for $\beta \neq 0$ then we have $\#\mathrm{C}_g = \ell^2-1$, $\#\mathrm{Cl}_g = \ell(\ell-1)$ and the number of such conjugacy classes is $\frac{\ell(\ell-1)}{2}$. Furthermore, the characteristic polynomial $\chi(g)$ is irreducible.*

8 Local-global study of Galois images

Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and let $p \in \mathbb{Z}$ be a prime of good reduction for E and let $\ell \neq p$ be a prime. If E is in its minimal model defined in Def. 4.2 and then p is such that p does not divide the discriminant Δ_{E}. Let $\mathbb{F}$ be the ℓ-torsion point field $\mathbb{F}_p(\mathrm{E}[\ell])$. Clearly, $\mathbb{F}$ is Galois and $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ is generated by the Frobenius automorphism. Considering the action of the Frobenius automorphism over $\mathrm{E}[\ell]$, one obtains a representation $\rho^p_{\mathrm{E},\ell}$ of $\mathrm{Gal}(\mathbb{F}/\mathbb{F}_p)$ in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. It is not difficult to see that $\mathrm{Im}\rho^p_{\mathrm{E},\ell}$ is always a cyclic subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

In this section, given the *global* mod ℓ Galois image $\mathrm{Im}\rho_{\mathrm{E},\ell}$, we are interested in knowing how the *local* image $\mathrm{Im}\rho^p_{\mathrm{E},\ell}$ varies with p.

8.1 Some results from number theory

Let us recall some classical results from algebraic number theory. For proofs and more details, the reader can refer to [Neu13], [Cox11b]. For the sake of brevity, we shall restrict ourselves to Galois extensions.

Let K be a finite Galois extension of $\mathbb{Q}$ with the ring of integers $\mathcal{O}_{\mathrm{K}}$. Note that $\mathcal{O}_{\mathrm{K}}$ is a Dedekind domain which means $\mathcal{O}_{\mathrm{K}}$ is not necessarily a unique factorization domain, however one can uniquely factor its ideals. We shall call a prime ideal of $\mathcal{O}_{\mathrm{K}}$ a prime in K. For any prime p in $\mathbb{Q}$, as K is Galois, the ideal $p\mathcal{O}_{\mathrm{K}}$ can be written as a product of distinct primes in K.

$$p\mathcal{O}_{\mathrm{K}} = (\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_r)^e.$$

We call the exponent e the *ramification index* of p. If $e = 1$, we say p is *unramified* in K, otherwise we say it is *ramified*. For every i, we say $\mathfrak{p}_i$ is an ideal above p.

Let $\mathfrak{p}$ be an ideal above an unramified prime p and $k_{\mathfrak{p}} := \mathcal{O}_{\mathrm{K}}/\mathfrak{p}$ denote its residue field. It is a finite extension of $\mathbb{F}_p$ of degree, say f. As K is Galois, this degree is independent of the choice of an ideal above p. We call f the *inertia degree* above p.

Definition 8.1. We say p is *totally split in* K, if $e = f = 1$.

Example 8.2. Let $\mathrm{K} = \mathbb{Q}(\zeta_5)$ defined by $\Phi_5 = x^4 + x^3 + x^2 + x + 1$. We know that $\mathrm{K}/\mathbb{Q}$ is Galois with Galois group isomorphic to $\mathbb{Z}/4\mathbb{Z}$. By the splitting of primes in cyclotomic fields, we know that a prime p splits completely in K if, and only if, $p \equiv 1 \mod 5$. These are essentially the primes modulo which Φ_5 splits completely.

We define the *decomposition group* $\mathrm{Dec}(\mathfrak{p})$ of $\mathfrak{p}$ as the subgroup of $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ which fixes $\mathfrak{p}$ as set i.e.

$$\mathrm{Dec}(\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}.$$

Each automorphism of $\mathrm{Dec}(\mathfrak{p})$ induces an automorphism of $k_{\mathfrak{p}}$ in a natural way. As elements of $\mathrm{Dec}(\mathfrak{p})$ fix $\mathfrak{p}$, one can, to each element of $\mathrm{Dec}(\mathfrak{p})$, associate an element of $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$. Let us call this map $\alpha^{(\mathfrak{p})}$. By [Neu13, Ch.1, Prop. 9.4], $\alpha^{(\mathfrak{p})}$ is a surjective homomorphism from $\mathrm{Dec}(\mathfrak{p})$ to $\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p)$. Its kernel is called the *inertia group* $\mathrm{Inert}(\mathfrak{p})$ of $\mathfrak{p}$. We have the following.

$$\mathrm{Inert}(\mathfrak{p}) = \{\sigma \in \mathrm{Gal}(\mathrm{K}/\mathbb{Q}) \mid \sigma(x) \equiv x \bmod \mathfrak{p} \text{ for all } x \in \mathcal{O}_{\mathrm{K}}\}.$$

Let $\phi_{\mathfrak{p}}$ be the Frobenius automorphism of the residue field $k_{\mathfrak{p}}$. We then define the Frobenius *element*[1] associated to p.

[1] It is an abuse of notation. This Frobenius is a conjugacy class.

Definition 8.3. In the above-given set up, we define the *Frobenius of* p as,

$$\mathrm{Frob}(p) = \bigcup_{\mathfrak{p} | p\mathcal{O}_{\mathrm{K}}} (\alpha^{(\mathfrak{p})})^{-1}(\phi_{\mathfrak{p}}).$$

Each element $(\alpha^{(\mathfrak{p})})^{-1}(\phi_{\mathfrak{p}}) \in \mathrm{Frob}(p)$ is characterized by the following property:

$$(\alpha^{(\mathfrak{p})})^{-1}(\phi_{\mathfrak{p}})(x) \equiv x^p \bmod \mathfrak{p} \text{ for all } x \in \mathrm{K}.$$

$\mathrm{Frob}(p)$ is a conjugacy class in $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$. At this point, one might ask whether every conjugacy class $\mathcal{C}$ in $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ occurs as the image of Frobenius for some prime p. The answer is given by the following *Chebotarev's density theorem.*

Theorem 8.4 ([Tsc26])**.** *Let* K *be a finite Galois extension of* $\mathbb{Q}$*. Let* $\mathcal{C}$ *be a conjugacy class in* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$*. Then* $\mathcal{C}$ *occurs as* $\mathrm{Frob}(p)$ *for some prime* p *and*

$$\mathrm{Prob}(\mathrm{Frob}(p) = \mathcal{C}) = \frac{\#\mathcal{C}}{\#\mathrm{Gal}(\mathrm{K}/\mathbb{Q})}.$$

The above probability is in the sense of natural density. We say that a set S of prime numbers admits a *natural density* δ if

$$\lim_{n\to\infty} \frac{\#(\mathrm{S} \cap \Pi(n))}{\#\Pi(n)} = \delta,$$

where $\Pi(n)$ is the set of primes less than n. We write $\mathrm{Prob}\,(\mathrm{S}) = \delta$. Clearly, adding or removing finitely many primes to S does not change the value of $\mathrm{Prob}\,(\mathrm{S})$.

Example 8.5. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 = x^3 + 3x + 5$. We saw in Example 5.14 that $\mathrm{Im}\rho_{\mathrm{E},3} = \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. On the other hand, it is not difficult to see that E admits full 3-torsion over $\mathbb{F}_p$ if, and only if, $\mathrm{Im}\rho^p_{\mathrm{E},3} = \{\mathrm{I}\}$, where $\mathrm{I} = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. By Chebotarev's theorem the density of such primes is

$$\mathrm{Prob}\left(\{p \mid \mathrm{E}(\mathbb{F}_p)[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\}\right) = \frac{\#\text{ conjugacy class of I}}{\#\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})} = \frac{1}{48} \approx 0.0208.$$

Experimentally, we compute this density over first 20000 primes of good reduction, to obtain 0.0203.

By Chebotarev's density theorem, every conjugacy class in $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$ appears as $\mathrm{Frob}(p)$ as we vary p. There exists an effective version of Chebotarev's density theorem due to Lagarias et al, see [LO79]. In other words, given a conjugacy class $\mathcal{C}$ of $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$, one can compute an upper bound on primes p to consider in order to obtain $\mathcal{C}$ as $\mathrm{Frob}(p)$.

Theorem 8.6 ([Ser81, Theorem 6])**.** *Assume the GRH. Let* K *be a Galois extension of* $\mathbb{Q}$ *of degree* n*. Let* $\mathcal{R}$ *be the finite set of primes in* $\mathbb{Q}$ *which are ramified in* K*. Then for all conjugacy classes* $\mathcal{C}$ *in* $\mathrm{Gal}(\mathrm{K}/\mathbb{Q})$*, there exists a prime* $p \notin \mathcal{R}$ *such that* $\mathrm{Frob}(p) = \mathcal{C}$ *and*

$$p \leq \kappa \cdot n^2 \left(\log n + \sum_{q \in \mathcal{R}} \log q \right)^2,$$

where κ *is an absolute constant.*

See [Bel13, PTBW17], for recent developments on the topic.

8.2 Local Galois images

We wish to apply the tools discussed in the previous section to a torsion point field. We borrow the notations of [BBB+13]. Recall that, by Lemma 5.3, a torsion point field is a Galois extension of $\mathbb{Q}$. Let $\mathrm{K} = \mathbb{Q}(\mathrm{E}[\ell])$ where ℓ is a prime. Let p be a an unramified prime of good reduction different than ℓ and let $\mathfrak{p}$ be a prime above p.

The residue field $k_{\mathfrak{p}}$ is precisely the ℓ-torsion point field $\mathbb{F}_p(\mathrm{E}[\ell])$. Indeed, the fact that $\mathbb{Q}(\mathrm{E}[\ell])$ contains $\mathrm{E}[\ell]$ can be restated by saying some rational polynomials have roots in $\mathbb{Q}(\mathrm{E}[\ell])$. The mod p reductions of these polynomials will also have roots in $k_{\mathfrak{p}}$.

Consider the following map:

$$\begin{array}{rccc} i_\ell : & \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell])/\mathbb{Q}) & \to & \mathrm{Aut}(\mathrm{E}(\overline{\mathbb{Q}})[\ell]) \\ & \rho & \mapsto & [\mathrm{P} \mapsto \rho(\mathrm{P})] \end{array}$$

Let $i_\ell^{(p)}$ be the similar map from $\mathrm{Gal}(\mathbb{F}_p(\mathrm{E}[\ell])/\mathbb{F}_p)$ to $\mathrm{Aut}(\mathrm{E}(\overline{\mathbb{F}}_p)[\ell])$. As E has good reduction at p and $p \neq \ell$, by [Sil08, Prop. VII.3.1], there exists an isomorphism $r_\ell^{(\mathfrak{p})}$ between the groups $\mathrm{Aut}(\mathrm{E}(\overline{\mathbb{Q}})[\ell])$ and $\mathrm{Aut}(\mathrm{E}(\overline{\mathbb{F}}_p)[\ell])$. So the following diagram commutes.

$$\begin{tikzcd} \mathrm{Dec}(\mathfrak{p}) \arrow[r, hook] \arrow[d, "\alpha^{(\mathfrak{p})}"] & \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell])/\mathbb{Q}) \arrow[r, hook, "i_\ell"] & \mathrm{Aut}(\mathrm{E}(\overline{\mathbb{Q}})[\ell]) \arrow[d, "r_\ell^{(\mathfrak{p})}"] \\ \mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p) \arrow[r, "\cong"] & \mathrm{Gal}(\mathbb{F}_p(\mathrm{E}[\ell])/\mathbb{F}_p) \arrow[r, hook, "i_\ell^{(p)}"] & \mathrm{Aut}(\mathrm{E}(\overline{\mathbb{F}}_p)[\ell]) \end{tikzcd}$$

Let $\mathrm{Im}\rho_{\mathrm{E},\ell}$ be the global mod ℓ Galois image constructed using a basis $(\mathrm{P}_1, \mathrm{P}_2)$ of $\mathrm{E}[\ell]$. With the compatible local basis $(\tilde{\mathrm{P}}_1, \tilde{\mathrm{P}}_2)$ of $\mathrm{E}(\overline{\mathbb{F}}_p)[\ell]$ i.e. the basis $(\tilde{\mathrm{P}}_1, \tilde{\mathrm{P}}_2)$ such that $\tilde{\mathrm{P}}_1 \equiv \mathrm{P}_1$ and $\tilde{\mathrm{P}}_2 \equiv \mathrm{P}_2$ modulo p, the local mod ℓ Galois image $\mathrm{Im}\rho^p_{\mathrm{E},\ell}$ is a cyclic subgroup of $\mathrm{Im}\rho_{\mathrm{E},\ell}$. Note that for an incompatible choice of local basis, one obtains a $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$-conjugate local Galois image.

Remark 8.7. *The image* $\mathrm{Im}\rho^p_{\mathrm{E},\ell}$ *is generated by* $\rho^p_{\mathrm{E},\ell}\left(\alpha^{(\mathfrak{p})}(\mathrm{Frob}(p))\right)$. *Henceforth, when it is clear from the context, we shall denote it simply by* $\mathrm{Frob}(p)$. *We shall only use it when the number field* K *is a torsion point field* $\mathbb{Q}(\mathrm{E}[\ell])$.

Let us take an example.

Example 8.8. We saw in Example 5.9 that $\mathrm{E}/\mathbb{Q}$ defined by $y^2 = x^3 + 21x - 26$ has full 3-torsion over $\mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive root of unity. Using SAGE, one can see that $\mathrm{E}[3]$ is generated by $\mathrm{P}_1 = (3, -8)$ and $\mathrm{P}_2 = (-1, 8 \cdot \zeta_3 + 4)$. Note that $\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q})$ has two elements: σ_1 defined by $\sigma_1(\zeta_3) = \zeta_3$ and σ_2 defined by $\sigma_2(\zeta_3) = -\zeta_3 - 1$. One can see that $\mathrm{Im}\rho_{\mathrm{E},3} \subset \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is generated by $\rho_{\mathrm{E},3}(\sigma_2) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right)$.

```
sage: K.<z> = NumberField(x^2+x+1)
sage: E = EllipticCurve(K,[21,-26])
sage: P1 = E.point([3,-8,1]); P2 = E.point([-1,8*z+4,1]);
sage: 2*P2
(-1 : -8*z - 4 : 1)
sage: sigma_2 = K.automorphisms()[1] #generator
sage: assert sigma_2(8*z+4)==-8*z - 4 #verification of Galois image
sage: Ok = K.ring_of_integers()
sage: five = Ok.ideal(5); K5 = five.residue_field();
sage: zeta^5== -zeta-1 #verification that sigma_2 is Frob(5)
True
```

Let us now consider it modulo $p = 5$. Over $\mathbb{F}_5$, $\#\mathrm{Im}\rho^5_{\mathrm{E},3} = 2$. We can suppose that $\mathbb{F}_5(\mathrm{E}[3])$ is defined by x^2+x+1 which is irreducible over $\mathbb{F}_5$. Let $\bar{x}$ be a root of x^2+x+1 in $\mathbb{F}_5(\mathrm{E}[3]) = \mathbb{F}_{5^2}$. Fixing the consistent basis $\tilde{\mathrm{P}}_1 = (3,3)$ and $\tilde{\mathrm{P}}_2 = (4, 3\bar{x}+4)$, we obtain the same image as $\mathrm{Im}\rho_{\mathrm{E},3}$.

Let us now change the basis to $\tilde{\mathrm{P}}_1 = (3,3)$ and $\tilde{\mathrm{P}}_3 = (2\bar{x}, 2\bar{x}+4)$. With this basis, we obtain that $\mathrm{Im}\rho^5_{\mathrm{E},3} \subset \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is generated by $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 2 \end{smallmatrix}\right)$. This image is $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$-conjugated to the global image via the matrix $\left(\begin{smallmatrix} 3 & 2 \\ 0 & 4 \end{smallmatrix}\right)$.

9 Properties of Galois images

One can ask what subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ can occur as mod ℓ Galois images for rational elliptic curves. A partial answer is provided by several properties of the torsion point fields. Note that the following results are classic. They are true over $\mathbb{Q}$ and do not hold in general over arbitrary number fields.

Proposition 9.1. *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve, let m be a positive integer and let $\mathrm{Im}\rho_{\mathrm{E},m} = \mathrm{G} \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. Then the application*

$$\det : \mathrm{G} \longrightarrow \mathbb{Z}/m\mathbb{Z}^*$$

is surjective. In particular, if $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z}) \subset \mathrm{G}$ then

$$\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Proof. Let us fix a basis P_1 and P_2 of $\mathrm{E}[m]$ and let e_m denote the Weil pairing over $\mathrm{E}[m]$. By Definition - Theorem 3.1, $e_m(\mathrm{P}_1, \mathrm{P}_2) = \zeta_m$ and by Corollary 3.9 we have $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(\mathrm{E}[m])$. Furthermore, as $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m]/\mathbb{Q})$ surjects onto $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ via the determinant map, we have the surjectivity of the determinant. Consequentially, if $\mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$ is the kernel of det, $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. □

As the image of any automorphism which fixes $\mathbb{Q}(\zeta_m)$ must have determinant 1 by Definition - Theorem 3.1 of Weil pairing, we have the following.

Lemma 9.2. *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and let $\mathrm{Im}\rho_{\mathrm{E},m} = \mathrm{G}$ over $\mathbb{Q}(\zeta_m)$. Then $\mathrm{G} \subset \mathrm{SL}_2(\mathbb{Z}/m\mathbb{Z})$.*

Remark 9.3. *Henceforth, we shall denote the identity element $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ of the group $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ by I.*

Lemma 9.4. *Let E/k be an elliptic curve over a field k and let m be a positive integer. Let K denote the splitting field of ψ_m over k and let $\mathrm{L} = k(\mathrm{E}[m])$. Then, if $-\mathrm{I} \in \mathrm{Im}\rho_{\mathrm{E},m}$ then L is a quadratic extension of K. Otherwise, $\mathrm{L} = \mathrm{K}$.*

Proof. We know that

$$\mathrm{Gal}(\mathrm{L}/\mathrm{K}) \subset \mathrm{Gal}(\mathrm{L}/k)$$

and $\mathrm{Gal}(\mathrm{L}/k)$ is isomorphic to $\mathrm{Im}\rho_{\mathrm{E},m}$. Let H be the subgroup of $\mathrm{Im}\rho_{\mathrm{E},m}$ corresponding to $\mathrm{Gal}(\mathrm{L}/\mathrm{K})$. Let P_1 and P_2 be a basis of $\mathrm{E}[m]$. Recall that the x-coordinates of P_1 and P_2 belong to K (see Proposition 5.6).

Let $\sigma \in \mathrm{Gal}(\mathrm{L}/\mathrm{K})$ be such that $\rho_{\mathrm{E},m}(\sigma) \in \mathrm{H}$. By definition, σ fixes K. So σ fixes the x-coordinate of every point in $\mathrm{E}[m]$. As $\mathrm{E}[m]$ is invariant under σ, we must have, $\sigma(\mathrm{P}_1) = \pm\mathrm{P}_1$, $\sigma(\mathrm{P}_2) = \pm\mathrm{P}_2$.

Similarly, we also have $\sigma(\mathrm{P}_1+\mathrm{P}_2) = \pm(\mathrm{P}_1+\mathrm{P}_2) \in \{\mathrm{P}_1+\mathrm{P}_2, -\mathrm{P}_1-\mathrm{P}_2\}$. On the other hand, as σ is linear over $\mathrm{E}[m]$, $\sigma(\mathrm{P}_1+\mathrm{P}_2) = \sigma(\mathrm{P}_1)+\sigma(\mathrm{P}_2)$. So $\rho_{\mathrm{E},m}(\sigma) \in \{\mathrm{I}, -\mathrm{I}\}$ and $\mathrm{H} \subset \{\mathrm{I}, -\mathrm{I}\}$.

If $-\mathrm{I} \in \mathrm{H}$ then H is of order 2 and L is a quadratic extension of K. If not, $\mathrm{H} = \{\mathrm{I}\}$ and $\mathrm{L} = \mathrm{K}$. □

The following result is valid over totally real fields.

Lemma 9.5 ([Zyw15b, Prop. 3.5])**.** *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve and let* m *be an integer. Then there exists a conjugate of* $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ *or* $\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right)$ *in* $\mathrm{Im}\rho_{\mathrm{E},m}$.

We conclude this section with a lemma.

Lemma 9.6. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve and let* $m > 2$ *be a positive integer. Let* K *denote the splitting field of* ψ_m. *Then* $\rho_{\mathrm{E},m}$ *is surjective if, and only if,*

$$[\mathrm{K}\colon \mathbb{Q}] = \frac{\#\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})}{2}.$$

Proof. If $\rho_{\mathrm{E},m}$ is surjective the $-\mathrm{I} \in \mathrm{Im}\rho_{\mathrm{E},m}$ and we conclude using Lemma 9.4. Reciprocally suppose $[\mathrm{K}\colon \mathbb{Q}] = \#\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})/2$ and $\rho_{\mathrm{E},m}$ is not surjective. By Lemma 9.4, $-\mathrm{I} \notin \mathrm{Im}\rho_{\mathrm{E},m}$. As $\mathrm{Im}\rho_{\mathrm{E},m}$ is an index 2 subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, it contains all the squares in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. But $-\mathrm{I}$ being the square of $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ belongs to $\mathrm{Im}\rho_{\mathrm{E},m}$. This yields a contradiction. □

10 Surjectivity of $\rho_{\mathrm{E},\ell}$

It is known that for all, but a set of density 0, rational elliptic curves E, $\rho_{\mathrm{E},\ell}$ is surjective for all primes ℓ, (see [Duk97, Theorem 1]). In this section, we are interested in certifying $\rho_{\mathrm{E},\ell}$ is surjective if it is the case. One way to do it is to explicitly construct the splitting field of the ℓ-th division polynomial ψ_ℓ using computer algebra systems such as SAGE or MAGMA and see whether its degree is equal to the order of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/2$. If it is the case then by Lemma 9.6, $\rho_{\mathrm{E},\ell}$ is surjective.

However, this construction is computationally expensive for large values of ℓ. For example, computing the splitting field of ψ_5 for the curve $y^2 = x^3+3x+5$ takes more than 4 hours in MAGMA. We thus look for methods which would rely on local data i.e. information of mod ℓ Galois images over finite fields. In this section, we present a probabilistic method to certify the surjectivity of $\rho_{\mathrm{E},\ell}$ which is based on Dickson's classification (Prop. 7.5). We shall see that this method has some limitations. We shall later analyse a previously known algorithm whose variant over number fields is given in [Sut16, Algorithm 6].

10.1 First algorithm

We now present our first algorithm which is due to our master thesis work to conclude the surjectivity of $\rho_{\mathrm{E},\ell}$ if it is the case. This algorithm is based on the following result, which is a straightforward consequence of Dickson's classification applied to Galois images.

Corollary 10.1. *Let* ℓ *be an odd prime and let* G *be a subgroup of* $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *which occurs as* $\mathrm{Im}\rho_{\mathrm{E},\ell}$ *for some rational elliptic curve* E. *If there exist* $g \in \mathrm{G}$ *of order* ℓ *and* $h \in \mathrm{G}$ *such that the discriminant* $\mathrm{tr}(h)^2 - 4\det(h)$ *of* $\chi(h)$ *is not a square then* $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$

Proof. As G contains an element of order ℓ, by Prop. 7.5, G is contained either in a Borel subgroup or $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{G}$. Furthermore, as G contains an element with irreducible characteristic polynomial, G cannot be a subgroup of a Borel subgroup. Thus, $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{G}$. By Prop. 9.1, $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. □

Algorithm 10.1 Surjectivity of $\rho_{\mathrm{E},\ell}$

Input: An elliptic curve $\mathrm{E}/\mathbb{Q}$ without complex multiplication and ℓ an odd prime.
Output: Certificate that $\rho_{\mathrm{E},\ell}$ is surjective if it is the case.

```
c_1, c_2 ← false.
while true do
    p ← a random prime ≠ ℓ of good reduction for E.        ▷ Definition 4.2
    Construct F_p(E[ℓ]).                                   ▷ Section 5.2.
    g ← (a b; c d) ∈ GL_2(Z/ℓZ) such that ⟨g⟩ = Im ρ^p_{E,ℓ}.   ▷ g = Frob(p) from Def. 8.3
and Remark 8.7.
    if c_1 is false then c_1 ← tr(g)^2 − 4 det(g) is not a square.
    end if
    if c_2 is false then c_2 ← g ≠ I and g^ℓ = I
    end if
    if c_1 and c_2 then return true
    end if
end while
```

Prima facie, it is not clear why Algorithm 10.1 should terminate. We know that by Chebotarev's density theorem, every conjugacy class in $\mathrm{Im}\rho_{\mathrm{E},\ell}$ appears as $\mathrm{Frob}(p)$ as we vary p.

When $\rho_{\mathrm{E},\ell}$ is surjective then two tests from Algorithm 10.1 return positive after testing finitely many primes and one can conclude that $\rho_{\mathrm{E},\ell}$ is surjective. The number of primes to test varies with curves E but it is always less than the bound estimated by the effective version of Chebotarev's theorem (Theorem 8.6).

If $\rho_{\mathrm{E},\ell}$ is not surjective, at least one of above tests fail for all primes. In particular, after testing for all primes up to the bound estimated by the effective version of Chebotarev's theorem, one can conclude that $\rho_{\mathrm{E},\ell}$ is not surjective. Thus, the algorithm terminates in both cases. The reader can find the script for this algorithm at [BS19b].

We now estimate the bound assured by the effective version Chebotarev's theorem when applied to torsion point fields.

Theorem 10.2. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve and* ℓ *be a prime. Let* $\mathcal{R}$ *be the set of primes of bad reduction and* ℓ*. Let* $\mathcal{C}$ *be a conjugacy class in* $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell])/\mathbb{Q})$*. Then* $\mathrm{Frob}(p) = \mathcal{C}$ *for some prime* p *less than* $\mathcal{B}_{\mathrm{E},\ell}$ *where*

$$\mathcal{B}_{\mathrm{E},\ell} := \kappa \cdot \ell^8 \cdot \left(\log \ell^4 + \sum_{q \in \mathcal{R}} \log q \right)^2,$$

for an explicit constant κ*.*

Proof. The torsion point field $\mathrm{K} = \mathbb{Q}(\mathrm{E}[\ell])$ is of degree at most ℓ^4 and the set of primes ramified in K consists of ℓ and the ones where E has bad reduction, see [DT02, Theorem 1]. It then suffices to apply Theorem 8.6. □

Complexity analysis of Algorithm 10.1

Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve such that $\rho_{\mathrm{E},\ell}$ is surjective for an odd prime ℓ. Algorithm 10.1 performs two tests to certify the surjectivity of $\rho_{\mathrm{E},\ell}$. We shall compute the density of primes over which each test comes positive, in other words we shall estimate the number of primes needed on average for each test to turn out positive.

1. In the first test, one looks for a prime p such that $f := \mathrm{Frob}(p) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is such that $\mathrm{tr}(f)^2 - 4\det(f)$ is a non-square i.e. f is conjugated to $\left(\begin{smallmatrix} a & eb \\ b & a \end{smallmatrix}\right)$. Thus by Chebotarev's theorem, we have,
$$\pi_1 = \mathrm{Prob}\left(\{p \mid \mathrm{Im}\rho^p_{\mathrm{E},\ell} \not\subset \mathrm{B}\}\right) = \frac{\ell(\ell-1)}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} \times \frac{\ell(\ell-1)}{2} = \frac{\ell}{2(\ell+1)}.$$
2. In the second test, one looks for a prime p such that $f := \mathrm{Frob}(p) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is of order ℓ. We saw in the proof of Prop. 7.5 that an element of order ℓ in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is conjugated to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Thus by Chebotarev's theorem, we have,
$$\pi_2 = \mathrm{Prob}\left(\{p \mid \#\mathrm{Im}\rho^p_{\mathrm{E},\ell} = \ell\}\right) = \frac{(\ell^2-1)}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} = \frac{1}{\ell^2-\ell}.$$

Theorem 10.3. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve and* ℓ *a prime. Then,*

1. *If* $\rho_{\mathrm{E},\ell}$ *is surjective then the average number of primes one tests in Algorithm 10.1 is* $O(\ell^2)$.
2. *Independently of surjectivity, the algorithm decides the surjectivity of* $\rho_{\mathrm{E},\ell}$ *after testing* $\mathcal{B}_{\mathrm{E},\ell}$ *primes, where* $\mathcal{B}_{\mathrm{E},\ell}$ *is the bound given by Theorem 10.2.*

Proof. In Algorithm 10.1, let π_i be the density of primes for which the i-th test comes positive. Then, the average number of primes needed is $O\left(\frac{1}{\pi_1} + \frac{1}{\pi_2}\right) = O(\ell^2)$. The second point is a straightforward reformulation of Theorem 10.2. □

Example 10.4. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 = x^3 + 3x + 5$ and let $\ell = 5$. It is known that $\rho_{\mathrm{E},5}$ is surjective. We are interested in seeing how many local images we need, to certify the surjectivity of $\rho_{\mathrm{E},5}$ using Algorithm 10.1. Note that E has bad reduction at $p = 2, 3, 29$. In Table 10.1, we prove that $\rho_{\mathrm{E},5}$ is surjective using 13 random primes up to 1000 of good reduction different than 5.

Example 10.5. Consider $\mathrm{E}/\mathbb{Q}$ defined by $y^2 = x^3 + 9x - 18$ of discriminant $-2^8 \times 3^6$ and let $\ell = 5$. For this curve, we obtain, using $\kappa = 280$ (see [Ser81]) that $\mathcal{B}_{\mathrm{E},\ell}$ is 2×10^{10}. Using SAGE, we check for primes below this bound and fail to prove that $\rho_{\mathrm{E},5}$ is surjective. Thus, one can conclude that $\rho_{\mathrm{E},5}$ is not surjective.

```
sage: E = EllipticCurve([9,-18])
sage: rho = E.galois_representation()
sage: p_bound = prime_pi(2*10^10)
sage: time rho.is_surjective(5,p_bound)
CPU times: user 1h 27min 41s, sys: 31.3 s, total: 1h 28min 12s
Wall time: 1h 32min 53s
```

In the next section, we shall discuss another algorithm based on [Ser71, Prop. 19, p. 283] which is implemented in SAGE. Sutherland in [Sut16] proposed a local-global algorithm which not only proves the surjectivity if it is the case but also computes the image when $\rho_{\mathrm{E},\ell}$ is not surjective. Note that in some cases, his algorithm cannot distinguish between two images.

p	$\mathrm{Im}\rho^{p}_{\mathrm{E},5}$	Test 1	Test 2
41	$\langle\left(\begin{smallmatrix}4&0\\4&4\end{smallmatrix}\right)\rangle$	false	false
557	$\langle\left(\begin{smallmatrix}2&1\\4&3\end{smallmatrix}\right)\rangle$	true	false
271	$\langle\left(\begin{smallmatrix}2&1\\3&2\end{smallmatrix}\right)\rangle$	-	false
389	$\langle\left(\begin{smallmatrix}4&1\\2&4\end{smallmatrix}\right)\rangle$	-	false
577	$\langle\left(\begin{smallmatrix}4&1\\2&1\end{smallmatrix}\right)\rangle$	-	false
677	$\langle\left(\begin{smallmatrix}2&2\\1&2\end{smallmatrix}\right)\rangle$	-	false
127	$\langle\left(\begin{smallmatrix}2&2\\1&2\end{smallmatrix}\right)\rangle$	-	false
431	$\langle\left(\begin{smallmatrix}3&4\\3&1\end{smallmatrix}\right)\rangle$	-	false
79	$\langle\left(\begin{smallmatrix}1&1\\0&4\end{smallmatrix}\right)\rangle$	-	false
383	$\langle\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right)\rangle$	-	false
877	$\langle\left(\begin{smallmatrix}2&2\\1&2\end{smallmatrix}\right)\rangle$	-	false
167	$\langle\left(\begin{smallmatrix}4&0\\0&3\end{smallmatrix}\right)\rangle$	-	false
251	$\langle\left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right)\rangle$	-	false

Table 10.1: Local images for $y^2 = x^3 + 3x + 5$ and tests from Corollary 10.1.

10.2 Second algorithm

Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve without CM and ℓ a prime. Let $\mathrm{G} = \mathrm{Im}\rho_{\mathrm{E},\ell}$. By Prop. 7.5, one sees that the following conditions suffice to conclude that $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

1. G is not contained in any Borel subgroup.
2. G is not contained in the normalizer of any Cartan subgroup (split or non-split).
3. The image of G in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is not $\mathrm{A}_4, \mathrm{S}_4$ or A_5.

In fact, if the above conditions are satisfied then by Prop. 7.5, $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{G}$ and then by Prop. 9.1, $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. As the elements of local Galois images can be determined only up to conjugacy, one transforms the above conditions into computational matrix properties, which are preserved under conjugation, and these properties then give us the tests in order to certify the surjectivity of $\rho_{\mathrm{E},\ell}$.

Theorem 10.6 ([Ser71, Prop. 19])**.** *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and $\ell > 3$ a prime. Let $\mathrm{G} = \mathrm{Im}\rho_{\mathrm{E},\ell}$. Then if,*

1. *$\exists\ f \in \mathrm{G}$ such that $\mathrm{tr}(f) \neq 0$ and $\mathrm{tr}(f)^2 - 4\det(f)$ is a non-square in $\mathbb{F}_\ell$.*
2. *$\exists\ g \in \mathrm{G}$ such that $\mathrm{tr}(g) \neq 0$ and $\mathrm{tr}(g)^2 - 4\det(g)$ is a non-zero square in $\mathbb{F}_\ell$.*
3. *$\exists\ h \in \mathrm{G}$ such that $u(h) := \frac{\mathrm{tr}(h)^2}{\det(h)} \notin \{0, 1, 2, 4\}$ and $u(h)^2 - 3u(h) + 1 \neq 0$.*

Then $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Proof. Recall that a Borel subgroup B is conjugated to the subgroup of upper triangular matrices. In particular, the characteristic polynomial $\chi(f)$ splits over $\mathbb{F}_\ell$ for all $f \in \mathrm{B}$. By 1., there exists $f \in \mathrm{G}$ such that $\mathrm{tr}(f)^2 - 4\det(f)$, which is the discriminant of $\chi(f)$, is a non-square in $\mathbb{F}_\ell$. So $\chi(f)$ does not split over $\mathbb{F}_\ell$ and G is not contained in a Borel subgroup.

Let us now see why G is not contained in the normalizer $\mathrm{N(C)}$ of a Cartan subgroup C. Suppose $\mathrm{G} \subset \mathrm{N(C)}$ where C is a split Cartan subgroup. Then for all $g \in \mathrm{G}$, $\mathrm{tr}(g)^2 - 4\det(g)$ is a square or $\mathrm{tr}(g) = 0$ depending on whether $g \in \mathrm{C}$ or $g \in \mathrm{N(C)} - \mathrm{C}$

respectively (Prop. 7.3). By 1., G is not contained in the normalizer of a split Cartan subgroup. Similarly, using 2., one can show that G is not contained in the normalizer of a non-split Cartan subgroup.

Finally, we claim that the image H in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of G is not isomorphic to A_4 or S_4 or A_5. Note that the possible orders of elements in these three groups are $1, 2, 3, 4$ and 5. An element $g \in \mathrm{G}$ with order 1 in H is scalar. For such an element $u(g) = 4$. If the order of g in H is 2 then g^2 is scalar, say $\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$. Then the eigenvalues of g are in $\{\sqrt{a}, -\sqrt{a}\}$. As g is not scalar, we have $\mathrm{tr}(g) = 0$ and so $u(g) = 0$. Similarly one can show that if the order of g in H is 3 (respectively 4 or 5) then $u(g) = 1$ (respectively $u(g) = 2$ or $u(g)$ satisfies $x^2 - 3x + 1$). So, using 3. we conclude that the image H in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of G is not isomorphic to A_4 or S_4 or A_5. Thus $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subset \mathrm{G}$. Then, by Prop. 9.1, $\mathrm{G} = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. □

We now present an algorithm based on the above theorem, which certifies the surjectivity of $\rho_{\mathrm{E},\ell}$ when $\ell > 3$.

Remark 10.7. *When $\ell = 3$, the second and the third test from Theorem 10.6 are never satisfied for any prime so the following algorithm never terminates despite the surjectivity. In this case, considering Lemma 9.6, one can compute the splitting field of ψ_3 and verify whether it has degree 24.*

Algorithm 10.2 Surjectivity of $\rho_{\mathrm{E},\ell}$ ([Sut16, Algorithm 6])

Input: An elliptic curve $\mathrm{E}/\mathbb{Q}$ without complex multiplication and a prime $\ell > 3$.
Output: Certificate that $\rho_{\mathrm{E},\ell}$ is surjective if it is the case.

$c_1, c_2, c_3 \leftarrow$ false.
while true **do**
  $p \leftarrow$ a random prime $\neq \ell$ of good reduction for E. ▷ Definition 4.2
  Construct $\mathbb{F}_p(\mathrm{E}[\ell])$. ▷ Section 5.2.
  $g \leftarrow \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $\langle g \rangle = \mathrm{Im}\rho^p_{\mathrm{E},\ell}$. ▷ $g = \mathrm{Frob}(p)$ from Def. 8.3 and Remark 8.7.
  if c_1 is false **then** $c_1 \leftarrow \mathrm{tr}(g) \neq 0$ **and** $\mathrm{tr}(g)^2 - 4\det(g)$ is not a square.
  end if
  if c_2 is false **then** $c_2 \leftarrow \mathrm{tr}(g) \neq 0$ **and** $\mathrm{tr}(g)^2 - 4\det(g)$ is a non-zero square.
  end if
  if c_3 is false **then** $c_3 \leftarrow u(g) = \frac{\mathrm{tr}(g)^2}{\det(g)} \notin \{0, 1, 2, 4\}$ **and** $u(g)^2 - 3u(g) + 1 \neq 0$.
  end if
  if c_1 **and** c_2 **and** c_3 **then return** true
  end if
end while

Following the discussion after Algorithm 10.1, the algorithm above terminates if $\rho_{\mathrm{E},\ell}$ is surjective. Clearly, if $\rho_{\mathrm{E},\ell}$ is not surjective then the above algorithm does not terminate on itself. Indeed, $\mathrm{Im}\rho_{\mathrm{E},\ell}$ is contained in either a Borel subgroup or in the normalizer of a Cartan subgroup or the image H of $\mathrm{Im}\rho_{\mathrm{E},\ell}$ in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is A_4 or A_5 or S_4. Thus the associated test fails modulo any prime. However, in such a case, on can use the effective version of Chebotarev's theorem to certify that $\rho_{\mathrm{E},\ell}$ is not surjective. So in any case, one either proves the surjectivity or disproves it.

The reader can find the script for this algorithm at [BS19b].

Complexity analysis of Algorithm 10.2

Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve such that $\rho_{\mathrm{E},\ell}$ is surjective for some prime $\ell > 3$. Algorithm 10.2 performs three tests to certify the surjectivity of $\rho_{\mathrm{E},\ell}$. We shall compute the density of primes over which each test comes positive, in other words we shall estimate the number of primes needed on average for each test to turn out positive.

1. In the first test, one looks for a prime p such that $f := \mathrm{Frob}(p) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is such that $\mathrm{tr}(f)^2 - 4\det(f)$ is a non-square and $\mathrm{tr}(f) \neq 0$ i.e. f is conjugated to $\left(\begin{smallmatrix} a & \epsilon b \\ b & a \end{smallmatrix}\right)$ with $a \neq 0$. Thus by Chebotarev's theorem, we have,

$$\pi_1 = \mathrm{Prob}\left(\{p \mid \mathrm{Im}\rho^p_{\mathrm{E},\ell} \not\subset \mathrm{B}\}\right) = \frac{(\ell-1)(\ell-1)}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} \times \frac{\ell(\ell-1)}{2} = \frac{\ell-1}{2(\ell+1)}.$$

2. In the second test, we look for a prime p such that $g := \mathrm{Frob}(p) \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is such that $\mathrm{tr}(g) \neq 0$ and $\mathrm{tr}(g)^2 - 4\det(g)$ is a non-zero square. Such a g is conjugated to $\left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$ where $\lambda_1 \neq \lambda_2$ and $\lambda_1 \neq -\lambda_2$. So, we have

$$\pi_2 = \mathrm{Prob}\left(\{p \mid \mathrm{Im}\rho^p_{\mathrm{E},\ell} \not\subset \mathrm{N(C)}\}\right) = \frac{(\ell-1)(\ell-3)}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} \times \frac{\ell(\ell+1)}{2} = \frac{(\ell-3)}{2(\ell-1)}.$$

3. Finally, one certifies that the image H in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$ of $\rho_{\mathrm{E},\ell}$ is not isomorphic to A_4 or S_4 or A_5. Let m denote $\mathrm{Frob}(p)$ i.e. $\mathrm{Im}\rho^p_{\mathrm{E},\ell}$ is generated by m in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Put $u_p := u(m) = \frac{\mathrm{tr}(m)^2}{\det(m)}$. Here we wish to compute the following.

$$\mathrm{Prob}\left(\left\{p \,\middle|\, \begin{array}{l} u_p \notin \{0,1,2,4\} \text{ and} \\ u_p^2 - 3u_p + 1 \neq 0 \end{array}\right\}\right).$$

We make 5 cases.

(a) Suppose $u_p = 0$ for some prime p. This can occur only in Case 1 and Case 4 of Theorem 7.6. In Case 1, there are $\frac{\ell-1}{2}$ choices for λ_1 and thus for conjugacy classes. Each of them contains $\ell(\ell+1)$ elements. In Case 4, one must have $\alpha = 0$ so there are $\frac{\ell-1}{2}$ choices for β and thus for conjugacy classes. Each of them contains $\ell(\ell-1)$ elements. Thus we have,

$$\begin{aligned}\mathrm{Prob}\left(\{p \,|\, u_p = 0\}\right) &= \frac{1}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}\left(\frac{\ell-1}{2}\ell(\ell+1) + \frac{\ell-1}{2}\ell(\ell-1)\right) \\ &= \frac{\ell}{\ell^2-1}.\end{aligned}$$

(b) Now suppose $u_p = 1$. As above, this is possible only in Case 1 and Case 4 of Theorem 7.6. For Case 1, we have the equation $(\lambda_1+\lambda_2)^2 = \lambda_1\lambda_2$. If we fix λ_1, we can solve for λ_2 if and only if -3 is a square modulo ℓ. i.e. $\ell \equiv 1 \mod 3$.

Furthermore, if $\ell \equiv 1 \mod 3$, Case 4 does not occur otherwise we would have, $\epsilon = \square$. So if we let $m = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$. There are two choices for λ_2 which are

roots of $x^2 + \lambda_1 x + \lambda_1^2$. Thus there are $\ell - 1$ distinct conjugacy classes each containing $\ell(\ell+1)$ elements. We thus have,

$$\text{if } \ell \equiv 1 \mod 3, \quad \mathrm{Prob}\Big(\{p \,|\, u_p = 1\}\Big) = \frac{1}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}\left((\ell-1)\ell(\ell+1)\right) = \frac{1}{\ell-1}.$$

When $\ell \equiv 2 \mod 3$, the Case 1 does not occur and Case 4 does. In Case 4, we have $\frac{\ell-1}{2}$ choice for β and each choice gives 2 values of α, thus there are $\ell - 1$ distinct conjugacy classes each containing $\ell(\ell-1)$ elements. So,

$$\text{if } \ell \equiv 2 \mod 3, \quad \mathrm{Prob}\Big(\{p \,|\, u_p = 1\}\Big) = \frac{1}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}\left((\ell-1)\ell(\ell-1)\right) = \frac{1}{\ell+1}.$$

(c) Now suppose $u_p = 2$. Again only Case 1 and Case 4 can occur. In Case 1, we have the equation $(\lambda_1 + \lambda_2)^2 = 2(\lambda_1\lambda_2)$. This gives $\lambda_1^2 + \lambda_2^2 = 0$. If we fix λ_1, we can solve for λ_2 if and only if -1 is a square modulo ℓ. i.e. $\ell \equiv 1 \mod 4$. Furthermore, if $\ell \equiv 1 \mod 4$, Case 4 does not occur otherwise we would have, $\epsilon = \square$. Suppose $\ell \equiv 1 \mod 4$ then there are $\ell - 1$ distinct conjugacy classes each containing $\ell(\ell+1)$ elements. We thus have, as above,

$$\text{if } \ell \equiv 1 \mod 4, \quad \mathrm{Prob}\Big(\{p \,|\, u_p = 2\}\Big) = \frac{1}{\ell-1}.$$

On the other hand, if $\ell \equiv 3 \mod 4$ then Case 4 occurs and Case 1 does not. And similar to (b), we have,

$$\text{if } \ell \equiv 3 \mod 4, \quad \mathrm{Prob}\Big(\{p \,|\, u_p = 2\}\Big) = \frac{1}{\ell+1}.$$

(d) Note that $u_p = 4$ for all matrices from Case 2 and Case 3 of Theorem 7.6. We thus have,

$$\mathrm{Prob}\Big(\{p \,|\, u_p = 4\}\Big) = \frac{1}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})}\Big(1 \cdot (\ell-1) + (\ell^2-1)(\ell-1)\Big) = \frac{\ell}{\ell^2-1}.$$

(e) Put $m = \mathrm{Frob}(p)$ and $u_p = \frac{\mathrm{tr}(m)^2}{\det(m)}$. Suppose that $u_p^2 - 3u_p + 1 = 0$. In particular $u_p \neq 0, 1, 2$. If $u_p = 4$ then $\ell = 5$. And this case occurs for all matrices from Case 2 and 3 and only for them. Thus, we have,

$$\text{if } \ell = 5, \quad \mathrm{Prob}\left(\left\{p \,\middle|\, u_p^2 - 3u_p + 1 = 0\right\}\right) = \frac{\ell^2(\ell-1)}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} = \frac{\ell}{\ell^2-1} = \frac{5}{24}.$$

Suppose henceforth $\ell \neq 5$. The condition $u_p^2 - 3u_p + 1 = 0$ implies

$$\left(\frac{2\det(m)}{\mathrm{tr}(m)^2} - 3\right)^2 = 5.$$

So 5 is a square modulo ℓ i.e. $\ell \equiv \pm 1 \mod 5$. So only Case 1 and Case 4 are possible.

In Case 1, m is conjugated to $\left(\begin{smallmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{smallmatrix}\right)$, $\lambda_1 \neq \lambda 2$ then $u_p = 0$ implies

$$\lambda_1^4 + \lambda_1^3\lambda_2 + \lambda_1^2\lambda_2^2 + \lambda_1\lambda_2^3 + \lambda_2^4 = 0.$$

Putting $\lambda = \frac{\lambda_1}{\lambda_2}$, one sees that the above equation is solvable if, and only if, $\ell \equiv 1 \mod 5$. So Case 1 occurs if, and only if, $\ell \equiv 1 \mod 5$. Hence Case 4 occurs if, and only if, $\ell \equiv -1, \mod 5$.

In Case 1, we have $\frac{\lambda_1}{\lambda 2} \in \{\zeta, \zeta^2, \zeta^3, \zeta^4\}$ where ζ is a fixed fifth primitive root of unity. Thus there are *a priori* $4(\ell-1)$ choices. However as $\zeta^4 = \frac{1}{\zeta}$ and $\left(\begin{smallmatrix}\lambda_1 & 0\\ 0 & \lambda_2\end{smallmatrix}\right)$ is conjugated to $\left(\begin{smallmatrix}\lambda_2 & 0\\ 0 & \lambda_1\end{smallmatrix}\right)$, we have only $2(\ell-1)$ choices which give,

$$\text{if } \ell \equiv 1 \bmod 5, \quad \mathrm{Prob}\left(\left\{p \,\middle|\, u_p^2 - 3u_p + 1 = 0\right\}\right) = \frac{2(\ell-1)\ell(\ell+1)}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} = \frac{2}{\ell-1}.$$

In Case 4, m is conjugated to $\left(\begin{smallmatrix}\alpha & \epsilon\beta\\ \beta & \alpha\end{smallmatrix}\right)$ and $\beta \neq 0$. As $u_p \neq 0$, we also have $\alpha \neq 0$ and

$$\alpha^2 = -\epsilon\beta^2\left(1 \pm \frac{2\theta}{5}\right),$$

where θ is a square root of 5 modulo ℓ. There are $\ell - 1$ choices for α and 2 choices for θ. As $\left(\begin{smallmatrix}\alpha & \epsilon\beta\\ \beta & \alpha\end{smallmatrix}\right)$ is conjugated to $\left(\begin{smallmatrix}\alpha & -\epsilon\beta\\ -\beta & \alpha\end{smallmatrix}\right)$, β can be chosen uniquely. Then,

$$\text{if } \ell \equiv -1 \bmod 5, \quad \mathrm{Prob}\left(\left\{p \,\middle|\, u_p^2 - 3u_p + 1 = 0\right\}\right) = \frac{2(\ell-1)\ell(\ell-1)}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} = \frac{2}{\ell+1}.$$

Using $(a), (b), (c)$ and (d), we compute $\pi_3 = \mathrm{Prob}\left(\left\{p \,\middle|\, \begin{array}{l} u_p \notin \{0,1,2,4\} \text{ and} \\ u_p^2 - 3u_p + 1 \neq 0 \end{array}\right\}\right)$

$$\pi_3 = \begin{cases} \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell-1}\right)\left(1 - \frac{1}{\ell+1}\right) = \frac{1805}{4608}, \text{ if } \ell = 5 \\ \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell\mp1}\right)^2\left(1 - \frac{2}{\ell\mp1}\right), \text{ if } \ell \equiv \pm 1 \mod 60 \\ \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell-1}\right)\left(1 - \frac{1}{\ell+1}\right), \text{ if } \ell \equiv \pm 7, \pm 17 \mod 60 \\ \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell\pm1}\right)^2\left(1 - \frac{2}{\ell\mp1}\right), \text{ if } \ell \equiv \pm 11 \mod 60 \\ \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell\mp1}\right)^2, \text{ if } \ell \equiv \pm 13 \mod 60 \\ \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell\mp1}\right)\left(1 - \frac{1}{\ell\pm1}\right)\left(1 - \frac{2}{\ell\pm1}\right) \text{ if } \ell \equiv \pm 19 \mod 60 \\ \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell\pm1}\right)^2, \text{ if } \ell \equiv \pm 23 \mod 60 \\ \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{1}{\ell\pm1}\right)\left(1 - \frac{1}{\ell\mp1}\right)\left(1 - \frac{2}{\ell\pm1}\right), \text{ if } \ell \equiv \pm 29 \mod 60 \end{cases}$$

Corollary 10.8. *In Algorithm 10.2, let π_i be the Chebotarev density of primes over which i-th test comes positive. Then, we have the following.*

$$\pi_1 \geq \frac{(\ell-1)}{2(\ell+1)}, \quad \pi_2 \geq \frac{(\ell-3)}{2(\ell-1)}, \quad \pi_3 \geq \left(1 - \frac{\ell}{\ell^2-1}\right)^2\left(1 - \frac{4}{\ell}\right).$$

p	$\mathrm{Im}\rho^p_{\mathrm{E},5}$	Test 1	Test 2	Test 3
307	$\langle\left(\begin{smallmatrix}3&0\\0&4\end{smallmatrix}\right)\rangle$	false	true	false
521	$\langle\left(\begin{smallmatrix}1&0\\4&1\end{smallmatrix}\right)\rangle$	false	-	false
967	$\langle\left(\begin{smallmatrix}2&0\\0&1\end{smallmatrix}\right)\rangle$	false	-	false
883	$\langle\left(\begin{smallmatrix}4&0\\0&2\end{smallmatrix}\right)\rangle$	false	-	false
839	$\langle\left(\begin{smallmatrix}0&4\\4&3\end{smallmatrix}\right)\rangle$	true	-	false
383	$\langle\left(\begin{smallmatrix}2&0\\0&4\end{smallmatrix}\right)\rangle$	-	-	false
757	$\langle\left(\begin{smallmatrix}2&2\\1&2\end{smallmatrix}\right)\rangle$	-	-	true

Table 10.2: Local images for $y^2 = x^3 + 3x + 5$ and tests from Theorem 10.6.

Average number of trials

Let T be the random variable of number of trials until the success in Algorithm 10.2. The i-th test fails for first n trials with probability $(1-\pi_i)^n$. So,

$$\mathrm{Prob}\,(\mathrm{T} > \mathrm{n}) \leq (1-\pi_1)^n + (1-\pi_2)^n + (1-\pi_3)^n$$

So, the expected value of T satisfies

$$\mathbb{E}(\mathrm{T}) = \sum_{n\geq 0} \mathrm{Prob}(\mathrm{T} > n) \leq \frac{1}{\pi_1} + \frac{1}{\pi_2} + \frac{1}{\pi_3}$$

Thus using Corollary 10.8, we have

$$\mathbb{E}(\mathrm{T}) \leq \frac{1}{\pi_1} + \frac{1}{\pi_2} + \frac{1}{\pi_3} \leq 5 + \frac{50}{\ell}.$$

Note that the above bound decreases rapidly as ℓ increases. As $\ell > 3$, we have $\mathbb{E}(\mathrm{T}) \leq 15$.

Theorem 10.9. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve and* ℓ *a prime. Then,*

1. *If* $\rho_{\mathrm{E},\ell}$ *is surjective then the average number of primes one tests in Algorithm 10.2 at most 15.*

2. *Independently of surjectivity, the algorithm decides the surjectivity of* $\rho_{\mathrm{E},\ell}$ *after testing* $\mathcal{B}_{\mathrm{E},\ell}$ *primes, where* $\mathcal{B}_{\mathrm{E},\ell}$ *is the bound given by Theorem 10.2.*

Proof. The proof is similar to that of Theorem 10.3. □

The reader can find more refined bounds in [Sut16, Section 4].

Example 10.10. Reconsider the curve E from Example 10.4. In Table 10.2, we prove the surjectivity using 8 random primes less than 1000.

11 Comparison of two algorithms

In this last part, we compare the performances of Algorithm 10.1 and 10.2 using 5000 rational non-isomorphic elliptic curves and primes $\ell = 5$ and 7. The curves used can be found at [BS19b].

ℓ	Algorithm 10.1	Algorithm 10.2
5	19.79	6.31
7	43.99	4.22

Table 11.1: Average of consecutive primes of good reduction needed

One sees that Algorithm 10.2 is way more efficient than Algorithm 10.1.

Part II

ECM and finding ECM-friendly elliptic curves

Chapter 3

Elliptic curve method

So far, we have discussed elliptic curves and mod ℓ Galois images attached to them. In this chapter, we shall describe the elliptic curve method (ECM) of factoring integers and its classical improvements. We then give a criterion for ECM-friendly curves i.e. suitable curves for ECM. Following [BBB+13], we shall see that for ECM-friendly curves the mod ℓ Galois image is exceptional for some prime ℓ. We shall conclude with a tool which allows us to compare ECM-friendly curves and its limitations.

12 Factorization using elliptic curves

The elliptic curve method of factorization (ECM) was originally proposed by Lenstra in [LJ87] and is similar to the $p-1$ method of Pollard [Pol74]. Let n be an integer with a prime factor p. We further suppose that $p-1$ is sufficiently B-smooth, for $\mathrm{B} \ll n$.

The main ingredient of Pollard's $p-1$ method is Fermat's little theorem.

Algorithm 12.1 Pollard's $p-1$ method

Input: An odd non-prime-power integer n and a bound $\mathrm{B} > 2$

Output: A non-trivial factor of n less than B if it exists or FAIL.

$a \leftarrow$ a random integer between 2 and $n-1$ such that $\gcd(a,n)=1$.
$g \leftarrow \gcd(a^{\mathrm{B}!}-1, n)$
if $g \notin \{1, n\}$ **then return** g
end if
return FAIL

Pollard's method has two versions. The Monte Carlo version is used to remove small prime factors of n with probability 1/2 before factoring n completely using NFS. In the Las Vegas version, one increases B until one obtains a factor. Let us now see why and when this method works and consider its limitations. We know by Fermat's little theorem that $a^{p-1} \equiv 1 \bmod p$.

As $p-1$ is supposed to be B-smooth, it is likely that $p-1$ divides B!, except if a small prime divides $p-1$ with large exponent, for example if p is a Fermat number of form $2^{2^i}+1$. So we further suppose that $p-1$ has only small prime factors with small multiplicities and that $p-1$ divides B!. In this case, one can see that the algorithm succeeds. In case the value of g is 1 or n in the second step, one can change the value of in the first step a and restart.

So Pollard's method works almost surely if the group $(\mathbb{Z}/p\mathbb{Z})^*$ has small exponent i.e. the ppcm of order of its elements. When it comes to large primes p, it is almost impossible for the condition above to be satisfied. This is a major limitation of Pollard's method.

Lenstra's idea was to replace the group $(\mathbb{Z}/p\mathbb{Z})^*$ by the group $\mathrm{E}(\mathbb{F}_p)$ where E is an elliptic curve. Indeed, it has approximately the same order as $(\mathbb{Z}/p\mathbb{Z})^*$ by Hasse's theorem (Theorem 4.6). The advantage of ECM is that $\#\mathrm{E}(\mathbb{F}_p)$ varies around p as we vary E.

In Chapter 1, we saw that the group law on an elliptic curve requires computing inverses of non-zero elements which is always possible over a field. However, if one considers the equation of an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ for a non-prime N and applies the addition formulae modulo N, one must be careful as there do not always exist multiplicative inverses modulo N. While computing multiples of a point on an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$, if we end up "inverting" a non-invertible element of $\mathbb{Z}/n\mathbb{Z}$, we may find a factor. We now present ECM in its original form below.

Note that for any triple of integers (x_0, y_0, a) in a ring, one can set $b = y_0^2 - (x_0^3 + ax_0)$ and, if $4a^3 + 27b^2 \neq 0$, consider the projective curve $\mathrm{E}_{a,b} : zy^2 = x^3 + axz^2 + bz^3$. This curve has a point $(x_0, y_0, 1)$ on it. Throughout this section $\mathrm{E}_{a,b}$ will be constructed in this manner.

Algorithm 12.2 The elliptic curve method: Lenstra's version

Input: Integer N an odd non-prime-power and a bound $\mathrm{C} > 2$

Output: A non-trivial factor of N if it exists.

$x_0, y_0, a \leftarrow$ random integers $\in [0, n-1]$
$b \leftarrow y_0^2 - (x_0^3 + ax_0)$
$\mathrm{E}_{a,b} \leftarrow zy^2 = x^3 + axz^2 + bz^3$ and $\mathrm{P} \leftarrow (x_0, y_0, 1)$.
$\mathrm{B} \leftarrow \mathrm{L}_{\mathrm{C}}(1/2, \sqrt{2})$ $\triangleright$ $\mathrm{L}_{\mathrm{C}}(a, c) = e^{c(\log \mathrm{C})^a (\log\log \mathrm{C})^{1-a}}$
$\mathrm{M} \leftarrow [\mathrm{B}!] \cdot \mathrm{P} = (x_{\mathrm{M}}, y_{\mathrm{M}}, z_{\mathrm{M}})$.
$g \leftarrow \gcd(z_{\mathrm{M}}, n)$
if $g \notin \{1, n\}$ **then return** g
end if
return FAIL

Remark 12.1. *We shall discuss the curious choice of* B *soon.*

Let $\tilde{\mathrm{P}}$ be the image of P in $\mathrm{E}_{a,b}(\mathbb{F}_p)$. If the order of $\tilde{\mathrm{P}}$ divides B!, we have $[\mathrm{B}!] \cdot \mathrm{P} \equiv \mathcal{O} \equiv [0, 1, 0] \bmod p$. We thus obtain a factor of N by checking $\gcd(z_{\mathrm{P}}, n)$. Like in the case of Pollard's $p-1$ method, here the algorithm succeeds if the order of $\tilde{\mathrm{P}}$ is B-smooth. As the order of an element in a finite group divides the order of the group, ECM succeeds whenever $\#\mathrm{E}_{a,b}(\mathbb{F}_p)$ is B-smooth.

Note that two points can be different modulo N but equal modulo p. In this case, one obtains the triple $(0, 0, 0)$ and a factor can be obtained nonetheless computing the greatest common divisor of N and a coordinate.

Average case complexity

By Hasse's theorem [Has36], we have $\#\mathrm{E}(\mathbb{F}_p) \in [(\sqrt{p}-1)^2, (\sqrt{p}+1)^2]$. We also saw that ECM succeeds if $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth. The following theorem of Lenstra relates the proportion of elliptic curves E over $\mathbb{F}_p$ such that $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth to the proportion of B-smooth integers in a subset of $[(\sqrt{p}-1)^2, (\sqrt{p}+1)^2]$.

Theorem 12.2 (Lenstra, [LJ87]). *There is a positive effectively computable constant c such that for every prime number $p > 3$ and every subset S of $\{s \in \mathbb{Z} \mid p+1-\sqrt{p} \leq s \leq p+1+\sqrt{p}\}$, the number of triples $(x, y, a) \in (\mathbb{Z}/p\mathbb{Z})^3$ for which $\Delta(\mathrm{E}_{a,b}) \not\equiv 0 \bmod p$ and $\#(\mathrm{E}_{a,b}) \in \mathrm{S}$ is at least $\frac{cp^3}{\log p} \cdot \frac{\#\mathrm{S}-2}{2\sqrt{p}}$.*

If S is taken to be the set of smooth numbers then the success probability of one curve in ECM depends on the proportion B-smooth integers in the interval $[p+1-\sqrt{p}, p+1+\sqrt{p}]$.

Choosing the parameter B

We shall make use of the classical L notation:

$$\mathrm{L}_{\mathrm{N}}(\alpha, c) = \exp(c(\log \mathrm{N})^{\alpha}(\log\log \mathrm{N})^{1-\alpha}).$$

We mentioned that the success of ECM depends on the proportion B-smooth integers in the interval $[p+1-\sqrt{p}, p+1+\sqrt{p}]$. As this proportion is difficult to estimate, we heuristically suppose that this proportion is similar to the proportion of B-smooth integers in the interval $[1, p]$. This latter can be estimated using Dickman ρ function (see [Dic30, HT93]). Then choosing $\mathrm{B} = \mathrm{L}_{\mathrm{C}}(1/2, \sqrt{2})$ and assuming both the proportions above are equal, it can be shown that the success probability of ECM is $1/2$ after at most $\mathrm{B} \times (\log n)^3$ operations.

12.1 Practical use of ECM

In cryptology, ECM is used as an algorithm to test B-smoothness i.e. to find all prime factors less than B of an integer N. Under a conjecture about the existence of smooth integers in short intervals [Cro07, Conj 1], H. Lenstra Jr. proved that, if N has a prime factor less than B, ECM will find it with probability at least $1/2$ in time $\mathrm{M}(\mathrm{N})\mathrm{L}_{\mathrm{B}}(1/2, \sqrt{2})^{1+o(1)}$, where $\mathrm{M}(\mathrm{N}) = \mathcal{O}((\log \mathrm{N})^2)$ is the cost of the arithmetic operations in $\mathbb{Z}/\mathrm{N}\mathbb{Z}$.

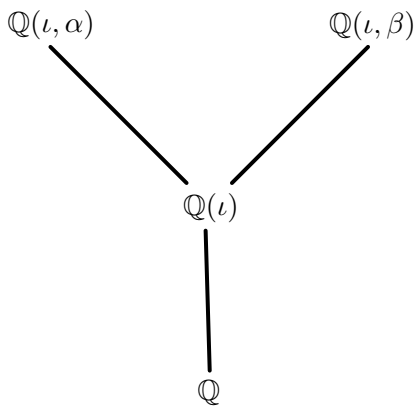
Smoothness tests play a key role in cryptology. Indeed, when factoring integers with NFS, one selects two distinct number fields $\mathbb{Q}[x]/f(x)$ and $\mathbb{Q}[x]/g(x)$ such that f and g have a common root m modulo N; we call α (resp. β) a root of f (resp. g) in its number field. The next stage of NFS consists of enumerating polynomials $\phi(x) \in \mathbb{Z}[x]$ and collecting all but a negligible proportion of those ϕ such that the norms $\mathrm{N}_{\mathbb{Q}(\alpha)}(\phi(\alpha))$ and $\mathrm{N}_{\mathbb{Q}(\beta)}(\phi(\beta))$ are B-smooth for $\mathrm{B} = \mathrm{L}_{\mathrm{N}}(1/3, \sqrt[3]{8/9})$.

The textbook implementation of NFS is without ECM as a subroutine. However in practice, one uses a hybrid version. The smoothness tests are done using ECM both in the complexity analysis and in practice, e.g. in the open source implementation CADO-NFS [BGK+].

The next stage of NFS consists in solving a linear system to find a tuple $(u_\phi)_{\phi \text{ collected}}$ such that $x_1 := \prod_\phi \phi(\alpha)^{u_\phi}$ and $x_2 := \prod_\phi \phi(\beta)^{u_\phi}$ are squares. Finally, one computes two polynomials r_1 and r_2 in $\mathbb{Z}[x]$ such that $r_1(\alpha)^2 = x_1$ and $r_2(\beta)^2 = x_2$ and obtain the solution $y_1^2 \equiv y_2^2 \pmod{N}$ where $y_1 = r_1(m) \bmod \mathrm{N}$ and $y_2 = r_2(m) \bmod \mathrm{N}$, where m is the common root of f and g modulo N. If $\gcd(y_1 - y_2, \mathrm{N}) \notin \{1, \mathrm{N}\}$, one finds a factor, otherwise one goes back to the beginning of the algorithm (in practice one computes many solutions (y_1, y_2) simultaneously).

When computing discrete logarithms in the multiplicative group of $\mathbb{F}_{p^n}$ for a prime p, the best asymptotic complexity is obtained by the extended tower number field sieve [KB16], which is a variant of NFS. The first step is to select a factor η of N and a polynomial $h(t) \in \mathbb{Z}[t]$ of degree η which is irreducible modulo p. Let ι be a

root of h in its number field. Then one selects two polynomials f and g in $\mathbb{Z}[t,x]$ such that, if ω is a root of H in $\mathbb{F}_p[t]/\langle h\rangle$, the polynomial $f(\omega,x)$ and $g(\omega,x)$ have a common irreducible factor $\varphi \in \mathbb{F}_p(\omega)[x]$ of degree $\kappa := \mathrm{N}/\eta$. If we call α and β roots of f and g respectively in their number fields, we obtain the following diagram:



Once h, f and g have been selected, the algorithm continues by enumerating a large number of pairs $a(t), b(t) \in \mathbb{Z}[t]$ and collecting all but a negligible proportion of the pairs a and b for which $\mathrm{N}_{\mathbb{Q}(\iota,\alpha)}(a(\iota)-\alpha b(\iota))$ and $\mathrm{N}_{\mathbb{Q}(\iota,\beta)}(a(\iota)-\beta b(\iota))$ are B-smooth for $\mathrm{B} = L_{p^n}(1/3, \sqrt[3]{8/9})$. In the next step, one factors $a(\iota)-\alpha b(\iota)$ and respectively $a(\iota)-\beta b(\iota)$ into prime ideals and writes a linear system whose coefficients are the valuations of prime ideals and the unknowns are in bijection with the prime ideals of norm less than B. The solution allows us to obtain the discrete logarithm of any element in a time which is negligible with respect to the cost of collecting the pairs $a(t)$ and $b(t)$.

As in the factoring variant of NFS, the smoothness tests are done with ECM. We note that in the case of discrete logarithm we have a larger number of methods to select the polynomials f and g. For example, in the case of the generalized Joux and Lercier method [JL03, BGGM15], one can set f to be any irreducible polynomial in $\mathbb{Z}[x]$ having an irreducible factor φ of degree κ. For example, in [BGGM14], the authors used $f(x) = \phi_8(x)$ so that for any pair (a,b), $\mathrm{N}_{\mathbb{Q}(\alpha)}(a-\alpha b) = a^4+b^4$, so half of the integers to factor in NFS can be tackled with elliptic curves defined over $\mathbb{Q}(\zeta_8)$, where ζ_8 is a primitive 8th root of unity. Moreover, when $h = h_0 + h_1 t + h_2 x^t$ for $h_0, h_1, h_2 \in \mathbb{Z}$, $\mathrm{N}_{\mathbb{Q}(\iota,\alpha)}(a(\iota)-\alpha b(\iota)) = N_{\mathbb{Q}(\iota)}(a'-\iota b') = h_0 v^2 + h_1 uv + h_2 u^2$, where $u - \iota v = N_{\mathbb{Q}(\iota,\alpha)/\mathbb{Q}(\iota)}(a(\iota)-\alpha b(\iota))$.

To sum up, an improvement of ECM adapted to integers of the form $h_2u^2 + h_1uv + h_0v^2$ would translate in an improvement of the relation collection of NFS and this can change the systems based on discrete logarithm in fields $F_{p^{2n}}$. An improvement on ECM in the general case would have consequences on the system based on factoring and discrete logarithm. Hence, for cryptologic applications, it is then important to find all the infinite families of elliptic curves defined over given number fields which have exceptional Galois images for some torsion, and to verify experimentally if they can bring a speed-up of ECM.

13 Classical improvements of ECM

Soon after ECM was proposed, Montgomery [Mon92] modified the version of Lenstra's algorithm which we present below. It is the practical version of ECM.

Algorithm 13.1 The elliptic curve method: Montgomery's version

INPUT: Integers n a non-prime-power and $\mathrm{B} > 2$
OUTPUT: a non-trivial factor of n less than B if it exists.

1: $\mathrm{E}/\mathbb{Q} \leftarrow$ an elliptic curve *from a family* and $\mathrm{P} \in \mathrm{E}(\mathbb{Q})$ of infinite order.
2: $\mathrm{M} \leftarrow [\mathrm{B}!] \cdot \mathrm{P} = (x_{\mathrm{M}}, y_{\mathrm{M}}, z_{\mathrm{M}})$.
3: $g \leftarrow \gcd(z_{\mathrm{M}}, n)$
4: **if** $g \notin \{1, n\}$ **then return** g
5: **end if**
6: **return** FAIL

A second stage to ECM was proposed by Brent and the reader can find it in [Bre10]. As performing group theoretical operations in ECM can be expensive, one prefers curves from a *suitable* family where these operations are less expensive. If an elliptic curve E is such that adding two points on it is less expensive or E has smaller coefficients, we say E has *better arithmetic properties*. On the other hand, if E is such that $\#\mathrm{E}(\mathbb{F}_p)$ has small factors for almost all primes p, we say E has *better smoothness properties*.

All the recent improvements of ECM deal with improving arithmetic and smoothness properties. Earlier, one considered curves with positive rank in order to have a ready-made point modulo n. However, this requirement is no longer enforced today, see [BI]. In this part, we shall discuss several classical and recent improvements of ECM considering well-chosen families of elliptic curves.

13.1 Curves with better arithmetic properties

Montgomery curves

Definition 13.1. Let k be a field of characteristic $\neq 2$ and $\mathrm{A}, \mathrm{B} \in k$ such that $\mathrm{B}(\mathrm{A}^2 - 4) \neq 0$. A *Montgomery curve* is the curve defined by the following equation.

$$\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}} : \mathrm{B}y^2 = x^3 + \mathrm{A}x^2 + x.$$

The discriminant of $\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}$ is $16(\mathrm{A}^2 - 4)$ which explains why we require that the characteristic of k be different than 2. Note that $\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}$ is the quadratic twist (Def. 2.10) of the curve $y^2 = x^3 + \mathrm{A}x^2 + x$ by B and it always has the point $(0, 0)$ of order 2. Montgomery curves have better arithmetic properties in the sense that the cost of doubling a point is 4 multiplications as opposed to curves in Weierstrass form where it takes 11 multiplications, see [LB]. Here we ignore the cost of addition.

Note that at this point, we do not know whether Montgomery curves also correspond to a family with better smoothness properties.

Lemma 13.2. *Let $\mathbb{F}_q$ be a finite field and $\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}$ be a Montgomery curve over $\mathbb{F}_q$. Then $4 \mid \#\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}(\mathbb{F}_q)$.*

Proof. Since the irreducible quadratic factor $x^2 + \mathrm{A}x + 1$ of the division polynomial Ψ_2 has discriminant $\mathrm{A}^2 - 4$, $\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}$ admits full 2 torsion over $\mathbb{F}_q$ if $\mathrm{A}^2 - 4$ is a square in $\mathbb{F}_q$. On the other hand, Ψ_4^{new} (see Example 5.12) is

$$(x-1)(x+1)\left(x^4 + 2\mathrm{A}x^3 + 6x^2 + 2\mathrm{A}x + 1\right).$$

As 1 and -1 are roots of Ψ_4^{new}, they are the x-coordinates of 2 points of order 4. Evaluating Ψ_2 at these roots, we obtain that $\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}(\mathbb{F}_q)$ has a point of order 4, if $\frac{\mathrm{A}+2}{\mathrm{B}}$

or $\frac{\mathrm{A}-2}{\mathrm{B}}$ is a square in $\mathbb{F}_q$. However, as $\mathbb{F}_q$ is a finite field, either $\frac{\mathrm{A}+2}{\mathrm{B}}$ or $\frac{\mathrm{A}-2}{\mathrm{B}}$ or their product $\frac{\mathrm{A}^2-4}{\mathrm{B}^2}$ must be a square. This ensures that $4 \mid \#\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}(\mathbb{F}_q)$. □

Note that not all curves E for which $4 \mid \#\mathrm{E}(\mathbb{F}_p)$ are Montgomery. One can even wonder whether there more curves. Using [Kat80, Theorem 1], we answer this question in Chapter 6.

Suyama curves

A Suyama curve (see [Mon87, p. 262],[Suy85]) is a Montgomery curve $\mathrm{E}_{\mathcal{M},\mathrm{A}(s,t),\mathrm{B}(s,t)}$ with

$$\mathrm{A}(s,t) = \frac{-3s^4 - 6s^2 + 1}{4s^3}$$
$$\mathrm{B}(s,t) = \frac{(s^2-1)^2}{4st^2}$$

with $s, t \in \mathbb{Q}$ and $st(s^2-1)(9s^2-1) \neq 0$. Suyama Noted than on this curve (s,t) is a point of order 3 which ensures divisibility by 12 over finite fields (see Theorem 4.5). Furthermore, Suyama also gave a positive rank subfamily $\mathrm{E}_{\mathcal{M},\mathrm{A}(\sigma),\mathrm{B}(\sigma)}$. The reader can find it in [Bar09, Section 3].

Twisted Edwards curves

Gauss and Euler studied the real solutions of $x^2 + y^2 = 1 - x^2y^2$. Edwards [Edw07] generalized it to study the equations of the form $x^2 + y^2 = c^2(1 + x^2y^2)$. Bernstein *et al* [BBJ+08] defined the twisted Edwards curves as following.

Definition 13.3. Let k be a field of characteristic $\neq 2$ and a, d be two distinct non-zero elements of k. A twisted Edwards curve defined by the following equation,

$$\mathrm{E}_{\mathcal{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2.$$

When $a = 1$, we refer it to simply as Edwards curves.

As suggested by the name, twisted Edwards curves are quadratic twists of Edwards curves. Indeed, $\mathrm{E}_{\mathcal{E},a,d}$ is a quadratic twist of $\mathrm{E}_{\mathcal{E},1,\frac{d}{a}}$ by a with the morphism $(x,y) \mapsto (\frac{x}{\sqrt{a}}, y)$. Furthermore, twisted Edwards curves are birationally equivalent to Montgomery curves.

Proposition 13.4 ([BBJ+08, Theorem 3.2])**.** *Let k be a field of characteristic $\neq 2$.*

1. *$\mathrm{E}_{\mathcal{E},a,d}$ is birationally equivalent to $\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}$ for $\mathrm{A} = 2\frac{a+d}{a-d}$ and $\mathrm{B} = \frac{4}{a-d}$ via the morphism $(x,y) \mapsto (x,y) = (\frac{1+y}{1-y}, \frac{1}{x} \cdot \frac{1+y}{1-y})$ and the inverse map is given by $(x,y) \mapsto (\frac{x}{y}, \frac{x-1}{x+1})$.*

2. *Conversely, for $\mathrm{A}, \mathrm{B} \in k$ be such that $\mathrm{B}(\mathrm{A}^2 - 4) \neq 0$, $\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}$ is birationally equivalent to $\mathrm{E}_{\mathcal{E},a,d}$ for $a = \frac{A+2}{B}$ and $d = \frac{A-2}{B}$.*

In ECM, the twisted Edwards curves with $a = 1$ and $a = -1$ are preferred as they have better arithmetic properties, see [LB]. For more details about twisted Edwards curves, the reader can refer to [BL07], [BBJ+08] and [Edw07].

Twisted Hessian curves

To put simply, twisted Hessian curves are precisely the elliptic curves isogenous to a curve with a point of order 3. They are named after Hesse [Hes44]. He considered curves defined by equations of the form $x^3 + y^2 + 1 = -6dxy$. They are used in ECM, see [HMR16], in their twisted forms which we define, following [BCKL15], as below.

Definition 13.5. Let k be a field and let $a, d \in k$ such that $a(27a - d^3) \neq 0$. A twisted Hessian curve is the curve defined by the following equation.

$$\mathrm{E}_{\mathcal{H},a,d} : ax^3 + y^3 + 1 = dxy.$$

When $a = 1$, we call the resulting curves as Hessian curves.

Like Montgomery, or equivalently, twisted Edwards curves, twisted Hessian curves have better arithmetic and better smoothness properties. Indeed, the cost of doubling a point is 8 multiplications and these curves always have a point of order 3 over every *finite* field, see [BCKL15, Theorem 5.2].

13.2 Curves with better smoothness properties

Theorem 4.5 says that $\#\mathrm{E}(k)_{\mathrm{tors}}$ divides $\#\mathrm{E}(\mathbb{F}_p)$ for all but finitely many primes p. Thus the smoothness of $\#\mathrm{E}(\mathbb{F}_p)$ depends on the smoothness of $\#\mathrm{E}(\mathbb{F}_p)/\#\mathrm{E}(k)_{\mathrm{tors}}$ which is of smaller size and thus heuristically has more chances of being smooth. So Montgomery proposed to choose curves E for ECM with larger torsion group $\mathrm{E}(k)_{\mathrm{tors}}$ where k is a number field. In this section, we discuss several such cases from the literature where curves with higher torsion over a number field are considered for ECM.

Torsion over $\mathbb{Q}$

Mazur's theorem (Theorem 3.7) gives 15 possible structures for $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$. Kubert [Kub76, Table 3, p. 217] parameterized families of elliptic curves having all these torsion structures. Atkin and Morain in [AM93] considered the curves E with $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z}$. There methods can be extended to the other torsion structures coming from Theorem 3.7 as well but those cases have already been dealt with Montgomery and Suyama parameterizations. Atkin and Morain also gave subfamilies with positive rank as it is preferred by some authors.

Torsion over other number fields

Brier and Clavier [BC10] considered curves defined over $\mathbb{Q}$ with bigger torsion over number fields. For example, they considered parameterized families of curves with full 4-torsion over $\mathbb{Q}(i)$ ([BC10, Section 3.5]), curves with full 3-torsion over $\mathbb{Q}(\zeta_3)$ ([BC10, Section 3.1]), curves with the torsion structure $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}(\zeta_3)$ [BC10, Section 3.2] and the curves with full 5-torsion over $\mathbb{Q}(\zeta_5)$ [BC10, Section 3.7]. The curves with torsion structure $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}(\zeta_3)$ were also considered in [BCKL15] in their twisted Hessian forms.

Going beyond torsion!

Kruppa in [Kru10] noted that the Suyama curve from Section 13.1 corresponding to $s = 11$ has better smoothness properties than a generic Suyama curve while having the same torsion. Barbulescu in [Bar09] extended this curve to an infinite family. Later,

Barbulescu *et al* in [BBB+13] proved that the torsion structure is not a complete story when it comes to finding suitable curves for ECM. One in fact has to consider the Galois image $\mathrm{Im}\rho_{\mathrm{E}}$. Their work motivated this thesis. We shall in Chapter 6 describe the families corresponding to the Galois representations.

14 What makes a curve ECM-friendly?

This section is heavily based on [BBB+13]. For a prime ℓ and an integer n, let $\mathrm{val}_\ell(n)$ denote the valuation of ℓ at n i.e. the highest power of ℓ dividing n.

Definition 14.1. Let E be a non-CM elliptic curve and ℓ a prime. Let Prob be Chebotarev density. We define the *average valuation* at ℓ of $\#\mathrm{E}(\mathbb{F}_p)$, where p is a random prime of good reduction by

$$\overline{v}_\ell(\mathrm{E}) = \sum_{n\geq 1} n \cdot \mathrm{Prob}(\{p \text{ prime } \mid \mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p)) = n\}).$$

The convergence of the series defining $\overline{v}_\ell(\mathrm{E})$ is proven in [BBB+13, Th 2.16]. If Chebotarev density Prob is a probability then one can consider $\mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p))$ as a random variable taking non-negative values. With this, $\overline{v}_\ell(\mathrm{E})$ is the expected value i.e. the average of the random variable $\mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p))$.

The proof of [BBB+13, Th 2.16] allows us to compute $\overline{v}_\ell(\mathrm{E})$ explicitly using $\mathrm{Im}\rho_{\mathrm{E},\ell^\infty}$. As E does not have complex multiplication, one can apply Serre's open image theorem (Theorem 6.7) to determine $\mathrm{Im}\rho_{\mathrm{E},\ell^\infty}$ using only finitely many images $\mathrm{Im}\rho_{\mathrm{E},\ell^i}$ for $i \leq n(\mathrm{E},\ell)$, where $n(\mathrm{E},\ell)$ is Serre's exponent which we define below.

Definition 14.2. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve without complex multiplication. Let us put $i(\mathrm{E},\ell,k) = [\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z}) : \rho_{\mathrm{E},\ell^k}(\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[\ell^k])/\mathbb{Q}))]$. We call *Serre's exponent* the integer $n(\mathrm{E},\ell) = \min\{n \in \mathbb{N}^* \mid \forall k \geq n, i(\mathrm{E},\ell,k+1) = i(\mathrm{E},\ell,k)\}$. In other words, Serre's exponent is the smallest integer n such that $\mathrm{Im}\rho_{\mathrm{E},\ell^\infty} = \pi^{-1}\left(\mathrm{Im}\rho_{\mathrm{E},\ell^n}\right)$, where π is the reduction map.

Serre's open image theorem ensures the existence of $n(\mathrm{E},\ell)$ as the sequence of indices is eventually constant when E does not have complex multiplication. With the above definition of average valuation, we can say that a curve E with higher value of $\overline{v}_\ell(\mathrm{E})$ for some ℓ is better for ECM.

14.1 Determining $\overline{v}_\ell(\mathrm{E})$

As $\overline{v}_\ell(\mathrm{E})$ can be considered as the average of the random variable $\mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p))$, the following estimation is its approximate value.

$$\overline{v}_\ell(\mathrm{E}) \approx \frac{\sum_{p\leq m} (\mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p))}{\#\Pi(m)},$$

where $\Pi(m)$ denotes the set of primes less than m for a large number m. We mentioned that one can compute the exact value of $\overline{v}_\ell(\mathrm{E})$ using the ℓ-adic Galois image associated to E, using the results of [BBB+13]. Let us now see how. In the theorem below, $\mathrm{Fix}(g)$ denotes the subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ which is fixed by $g \in \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Theorem 14.3 ([BBB+13, Theorem 2.7(1)]). *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and $m \geq 2$ be an integer. Let T be a subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Then,*

$$\mathrm{Prob}(\{p \text{ prime} \mid \mathrm{E}(\mathbb{F}_p)[m] \simeq \mathrm{T}\}) = \frac{\#\{g \in \mathrm{Im}\rho_{\mathrm{E},m} \mid \mathrm{Fix}(g) \simeq \mathrm{T}\}}{\#\mathrm{Im}\rho_{\mathrm{E},m}}.$$

Proof. Put $\mathrm{K} = \mathbb{Q}(\mathrm{E}(m))$ and let p be such that $\gcd(p, m) = 1$. Let $\mathfrak{p}$ be an ideal above p in K. Consider the following commutative diagram from Section 8.2.

$$\begin{tikzcd}
\mathrm{Dec}(\mathfrak{p}) \arrow[r, hook] \arrow[d, two heads, "\alpha^{(\mathfrak{p})}"] & \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q}) \arrow[r, hook, "\rho_{\mathrm{E},m}"] & \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \arrow[d, two heads] \\
\mathrm{Gal}(k_{\mathfrak{p}}/\mathbb{F}_p) \arrow[r, "\cong"] & \mathrm{Gal}(\mathbb{F}_p(\mathrm{E}[m])/\mathbb{F}_p) \arrow[r, hook, "\rho^p_{\mathrm{E},m}"] & \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})
\end{tikzcd}$$

Let $\mathrm{H} \subset \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m]/\mathbb{Q}))$ corresponding to $\{g \in \mathrm{Im}\rho_{\mathrm{E},m} \mid \mathrm{Fix}(g) \simeq \mathrm{T}\}$ i.e.

$$\mathrm{H} = \{\rho^{-1}_{\mathrm{E},m}(g) \mid g \in \mathrm{Im}\rho_{\mathrm{E},m} \text{ such that } \mathrm{Fix}(g) \simeq \mathrm{T}\}.$$

The only elements of the field $\mathbb{F}_p(\mathrm{E}[m])$ fixed by the Frobenius ϕ_p of $\mathrm{Gal}(\mathbb{F}_p(\mathrm{E}[m])/\mathbb{F}_p)$ are the ones in $\mathbb{F}_p$. Thus the only points of $\mathrm{E}[m]$ over $\mathbb{F}_p(\mathrm{E}[m])$ fixed by ϕ_p are $\mathbb{F}_p$-rational i.e. $\mathrm{E}(\mathbb{F}_p)[m] \simeq \mathrm{Fix}(\rho^p_{\mathrm{E},m}(\phi_p))$.

On the other hand, corresponding to ϕ_p, we have $\mathrm{Frob}(p) \subset \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[m])/\mathbb{Q})$ such that $\mathrm{Frob}(p) = (\alpha^{(\mathfrak{p})})^{-1}(\phi_p)$. So $\mathrm{E}(\mathbb{F}_p)[m] \simeq \mathrm{Fix}(\rho_{\mathrm{E},m}(\mathrm{Frob}(p)))$.

So we decompose H as a disjoint union of conjugacy classes $\mathcal{C}_1, \ldots, \mathcal{C}_r$. Then $\mathrm{Fix}(\rho_{\mathrm{E},m}(\mathrm{Frob}(p))) \simeq \mathrm{T}$ is equivalent saying $\mathrm{Frob}(p) = \mathcal{C}_i$ for some i. Thus from Chebotarev's density theorem (Theorem 8.4),

$$\begin{aligned}
\mathrm{Prob}(\{p \text{ prime} \mid \mathrm{E}(\mathbb{F}_p)[m] \simeq \mathrm{T}\}) &= \sum_{i=1}^{r} \mathrm{Prob}(\{p \text{ prime} \mid \mathrm{Frob}(p) = \mathcal{C}_i)\} \\
&= \sum_{i=1}^{r} \frac{\#\mathcal{C}_i}{\#\,\mathrm{Gal}(K/\mathbb{Q})} = \frac{\#H}{\#\,\mathrm{Gal}(K/\mathbb{Q})}.
\end{aligned}$$

□

Let $i, j, k \in \mathbb{N}$ with $i \leq j$. Put $\mathrm{T}_{i,j} = \mathbb{Z}/\ell^i\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z} \subset \mathbb{Z}/\ell^k\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z}$ and

$$p_{\ell,k}(i,j) = \mathrm{Prob}(\{p \text{ prime} \mid \mathrm{E}(\mathbb{F}_p)[\ell^k] \simeq \mathrm{T}_{i,j}\}).$$

The following result enables us to compute explicitly $\overline{v}_\ell(\mathrm{E})$.

Theorem 14.4 ([BBB+13, Theorem 2.20]). *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and ℓ a prime then*

$$\overline{v}_\ell(\mathrm{E}) = 2\sum_{i=1}^{n-1} p_{i,\ell}(i,i) + \frac{\ell}{\ell-1}\sum_{i=0}^{n-1} p_{n,\ell}(i,n) + \sum_{i=0}^{n-2}\sum_{j=i+1}^{n-1} p_{j,\ell}(i,j) + \frac{\ell(2\ell+1)}{(\ell-1)(\ell+1)} p_{n,\ell}(n,n).$$

Let us reformulate it below.

Corollary 14.5. *Let E_1 and E_2 be two elliptic curves without complex multiplication and ℓ a prime. If for all $n \in \mathbb{N}$, $\mathrm{Im}\rho_{\mathrm{E}_1,\ell^n}$ and $\mathrm{Im}\rho_{\mathrm{E}_2,\ell^n}$ are $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$-conjugates then $\overline{v}_\ell(\mathrm{E}_1) = \overline{v}_\ell(\mathrm{E}_2)$.*

In practice, to compute $\overline{v}_\ell(\mathrm{E})$, we first compute Serre's exponent $n = n(\mathrm{E}, \ell)$ by computing successive mod ℓ^i Galois images $\mathrm{Im}\rho_{\mathrm{E},\ell^i}$. Using [SZ17, Lemma 3.7], one can certify the computations of $n = n(\mathrm{E}, \ell)$.

Theorem 14.4 gives $\overline{v}_\ell(\mathrm{E})$ as a linear combination of $p_{1,\ell}(0,1)$, $p_{1,\ell}(1,1)$, $p_{2,\ell}(0,2)$, $p_{2,\ell}(1,2)$, $p_{2,\ell}(2,2)$ up to $p_{n,\ell}(0,n), \cdots, p_{n,\ell}(n,n)$. We compute each of $p_{j,\ell}(i,j)$ using $\mathrm{Im}\rho_{\mathrm{E},\ell^j}$ via Theorem 14.3.

Example 14.6. Let $\mathrm{E}/\mathbb{Q}$ be defined by $y^2 + xy + y = x^3 + x^2 - 284x - 1924$ of Cremona label 231a3. For this curve $n(\mathrm{E}, 2) = 2$. One can verify with SAGE that E admits full 2-torsion over $\mathbb{Q}$ and $\mathbb{Q}(\mathrm{E}[4])$ is a quartic extension of $\mathbb{Q}$. We furthermore have,

$$\mathrm{Im}\rho_{\mathrm{E},2} = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \rangle \subset \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

and

$$\mathrm{Im}\rho_{\mathrm{E},4} = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right) \rangle \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}).$$

Let us compute $\overline{v}_2(\mathrm{E})$. Here we have to compute $p_{1,2}(0,1)$, $p_{1,2}(1,1)$ using $\mathrm{Im}\rho_{\mathrm{E},2}$ and $p_{2,2}(0,2)$, $p_{2,2}(1,2)$ and $p_{2,2}(2,2)$ using $\mathrm{Im}\rho_{\mathrm{E},4}$. We clearly have $p_{1,2}(0,1) = 0$ and $p_{1,2}(1,1) = 1$ and $p_{2,2}(0,2) = 0$.

Out of 4 elements of $\mathrm{Im}\rho_{\mathrm{E},4}$, 3 matrices have fixed subspace $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Thus by Theorem 14.3, $p_{2,2}(1,2)$ is $\frac{3}{4}$. Finally, $p_{2,2}(2,2) = \frac{1}{4}$ which corresponds to the identity matrix. We thus have, using Theorem 14.4,

$$\overline{v}_2(\mathrm{E}) = 2(p_{1,2}(1,1)) + 2(p_{2,2}(0,2) + p_{2,2}(1,2)) + p_{1,2}(0,1) + \frac{10}{3}p_{2,2}(2,2) = \frac{13}{3}.$$

14.2 $\overline{v}_\ell(\mathrm{E})$ when $\rho_{\mathrm{E},\ell^\infty}$ is surjective

Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve without complex multiplication and ℓ be a prime. Let us further suppose that ρ_{E,ℓ^i} is surjective for all i, that is, $\rho_{\mathrm{E},\ell}$ is surjective and Serre's exponent $n(\mathrm{E}, \ell) = 1$. We mentioned (see [Duk97]) that this is the case for almost all elliptic curves. Let us compute $\overline{v}_\ell(\mathrm{E})$ for such curves. By Theorem 14.4,

$$\overline{v}_\ell(\mathrm{E}) = \frac{\ell}{\ell - 1}p_{1,\ell}(0,1) + \frac{\ell(2\ell+1)}{(\ell^2-1)}p_{1,\ell}(1,1).$$

Clearly,

$$p_{1,\ell}(1,1) = \frac{1}{\#\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})} = \frac{1}{(\ell^2-\ell)(\ell^2-1)}.$$

On the other hand, $p_{1,\ell}(0,1)$ is the proportion of matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with a fixed subspace of dimension 1. Let m be one such matrix. Then, up to conjugacy, $m = \left(\begin{smallmatrix} 1 & 0 \\ 0 & a \end{smallmatrix}\right)$ with $a \neq 1$ or $m = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ with $a \neq 0$. By Theorem 7.6, there are $\ell(\ell+1)(\ell-2)$ matrices of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ in the first case and $\ell^2 - 1$ in the second. So,

$$\begin{aligned}
\overline{v}_\ell(\mathrm{E}) &= \frac{\ell}{\ell-1}p_{1,\ell}(0,1) + \frac{\ell(2\ell+1)}{(\ell^2-1)}p_{1,\ell}(1,1) \\
&= \frac{\ell}{\ell-1}\frac{\ell(\ell+1)(\ell-2)+\ell^2-1}{(\ell^2-\ell)(\ell^2-1)} + \frac{\ell(2\ell+1)}{(\ell^2-1)}\frac{1}{(\ell^2-\ell)(\ell^2-1)} \\
&= \frac{\ell(\ell^3+\ell^2-2\ell-1)}{(\ell+1)^2(\ell-1)^3} = \frac{1}{\ell-1} + \frac{1}{(\ell-1)^2} + o\left(\frac{1}{(\ell-1)^2}\right)
\end{aligned}$$

One sees that for large values of ℓ, the generic valuation $\overline{v}_\ell(\mathrm{E})$ decreases rapidly.

B \ $\log_2 n$	25	29	33	37	40
1000	-2.03	-1.37	-1.81	-1.79	-1.73
2000	-1.94	-1.65	-1.75	-1.6	-1.68
3000	-1.94	-1.51	-1.62	-1.61	-1.63
4000	-1.82	-1.45	-1.55	-1.53	-1.59
5000	-1.8	-1.41	-1.57	-1.45	-1.61

Table 15.1: Values of $\beta(\mathrm{E}, n, \mathrm{B})$ for $\mathrm{E} : y^2 = x^3 + 3x + 5$ and various values of $\log n$ and B.

14.3 Mazur's program B

By Corollary 14.5, an ECM-friendly elliptic curve has an exceptional Galois image. Thus, the search of ECM-friendly elliptic curves boils down to finding curves with exceptional Galois images.

Mazur's program B, 1976 [SZ06]:[1] Given a number field K, a subgroup $\mathrm{H} \subset \mathrm{GL}_2(\hat{\mathbb{Z}}) = \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell)$, classify all elliptic curves E/K such that $\mathrm{Im}\rho_{\mathrm{E}}$ is contained in H up to conjugacy.

To put simply, over $\mathbb{Q}$, Mazur's program B asks, given a prime power ℓ^n and a subgroup $\mathrm{H} \subset \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, classify all rational elliptic curves E such that $\mathrm{Im}\rho_{\mathrm{E},\ell^n} \subset \mathrm{H}$ up to conjugacy. We shall see in Section 23 that the list of families of such curves is finite and the families of ECM-friendly elliptic curves in the sense of Corollary 14.5 appear in that list.

Before this work, the quest of ECM-friendly curves and Mazur's program B were seen as two independent problems. As discussed in Section 12.1, an important application of ECM consists in using the same elliptic curve to test smoothness of many integers. In this context, several articles [BBL10], [HMR16], [GKL17],[Mon87] measure the quality of a curve E for the ECM algorithm as the proportion of primes p less than a bound X for which $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth, where X and B are given parameters. In the rest of this section we study whether one can compare this proportion for two elliptic curves, regardless of the two parameters X and B. The next section thus quantifies the efficiency of elliptic curves for ECM. We shall refer to this quantification as the ECM-*friendliness* of a curve.

15 Quantifying ECM-friendliness

Given an elliptic curve E and two integers n and B, let $\beta(\mathrm{E}, n, \mathrm{B})$ be a real number such that

$$\frac{\#\{p \sim n \,|\, \#\mathrm{E}(\mathbb{F}_p) \textit{ is } \text{B-smooth}\}}{\#\{p \,|\, p \sim n\}} \approx \frac{\#\{x \sim ne^{\beta(\mathrm{E},n,\mathrm{B})} \,|\, x \textit{ is } \text{B-smooth}\}}{\#\{x \,|\, x \sim ne^{\beta(\mathrm{E},n,\mathrm{B})}\}},$$

where $p \sim n$ denotes that $p \in [n - 2\sqrt{n}, n + 2\sqrt{n}]$ and the sign $\approx$ denotes the equality up to a difference of $1/\#\{x \mid x \sim ne^{\beta(\mathrm{E},n,\mathrm{B})}\}$. This notation comes to correct a common heuristic which states that a cardinality of $\mathrm{E}(\mathbb{F}_p)$ is as smooth as a random integer of the same size. Table 15.1 shows the values of $\beta(\mathrm{E}, n, \mathrm{B})$ for the curve E of equation $y^2 = x^3 + 3x + 5$ and various values of $\log_2 n$ and B.

[1] One might believe that there is a Program A of Mazur however it is not the case. There is Conjecture A, Program B and Question C in the same paper of Mazur.

In Theorem 24.7, we list 1525 families of rational elliptic curves with distinct Galois images. In the sense of Theorem 14.5, ECM-friendly families belong to this list. A similar experiment for all of them suggests that $\beta_{\mathrm{E},n,\mathrm{B}}$ converges uniformly when n and B go to infinity.

Open question 15.1. *Let* E *be an elliptic curve without complex multiplication. Decide whether there exists a real number* $\beta(\mathrm{E})$ *such that*

$$\mathrm{Prob}(\#\mathrm{E}(\mathbb{F}_p) \text{ is B-smooth} \mid p \sim n) \sim_n \mathrm{Prob}(m \text{ is B-smooth} \mid m \sim ne^{\beta(\mathrm{E})}),$$

where $\sim_n$ *denotes the asymptotic equivalence,* $p \sim n$ *denotes that* $p \in [n-2\sqrt{n}, n+2\sqrt{n}]$, Prob *on the left side denotes the Chebotarev density and* Prob *on the right side denotes the proportion of* B*-smooth integers in the interval.*

Answering the above question goes beyond the scope of this thesis. Nevertheless, this offers a new point of view on a tool that Peter Montgomery used in experiments to compare elliptic curves. Indeed, Montgomery [Mon92, pages 75-76] considered the value

$$\log(2) \cdot \overline{\mathrm{val}_2}(\mathrm{E}) + \log(3) \cdot \overline{\mathrm{val}_3}(\mathrm{E}),$$

where $\overline{\mathrm{val}_2}$ and $\overline{\mathrm{val}_3}$ denote the average value of $\mathrm{val}_2(\#\mathrm{E}(\mathbb{F}_p))$ and $\mathrm{val}_3(\#\mathrm{E}(\mathbb{F}_p))$ when p runs through all the primes of good reduction up to a bound n. These are similar to the first terms of a numeric series that rigorously defines $\alpha(\mathrm{E})$, a candidate for $\beta(\mathrm{E})$ in Open question 15.1 as we explain in the next subsection.

Murphy in [Mur99] introduced a tool $\alpha(\mathrm{P})$ which answers the above question for the values taken by polynomials P:

$$\alpha(\mathrm{P}) = \sum_{\ell \text{ prime}} \log(\ell) \cdot \left(\frac{1}{\ell - 1} - \overline{\mathrm{val}_\ell} \right),$$

where $\overline{\mathrm{val}_\ell}$ is the average of valuations of ℓ at the elements of the set of integers that we study, the average being defined rigorously in the sequel of this section. Barbulescu and Lachand in [BL17, Theorem 1.1] proved that $\beta(\mathrm{F}) = \alpha(\mathrm{F})$ for any quadratic polynomial F with primitive fundamental negative discriminant.

15.1 Formal definition of $\alpha(\mathrm{E})$

Definition 15.1. Given an elliptic curve E and a prime ℓ, we put

$$\alpha_\ell(\mathrm{E}) = \log(\ell)(\overline{v}_\ell(n) - \overline{v}_\ell(\mathrm{E}))$$

and

$$\alpha(\mathrm{E}) = \sum_{\ell \text{ prime}} \alpha_\ell(\mathrm{E}).$$

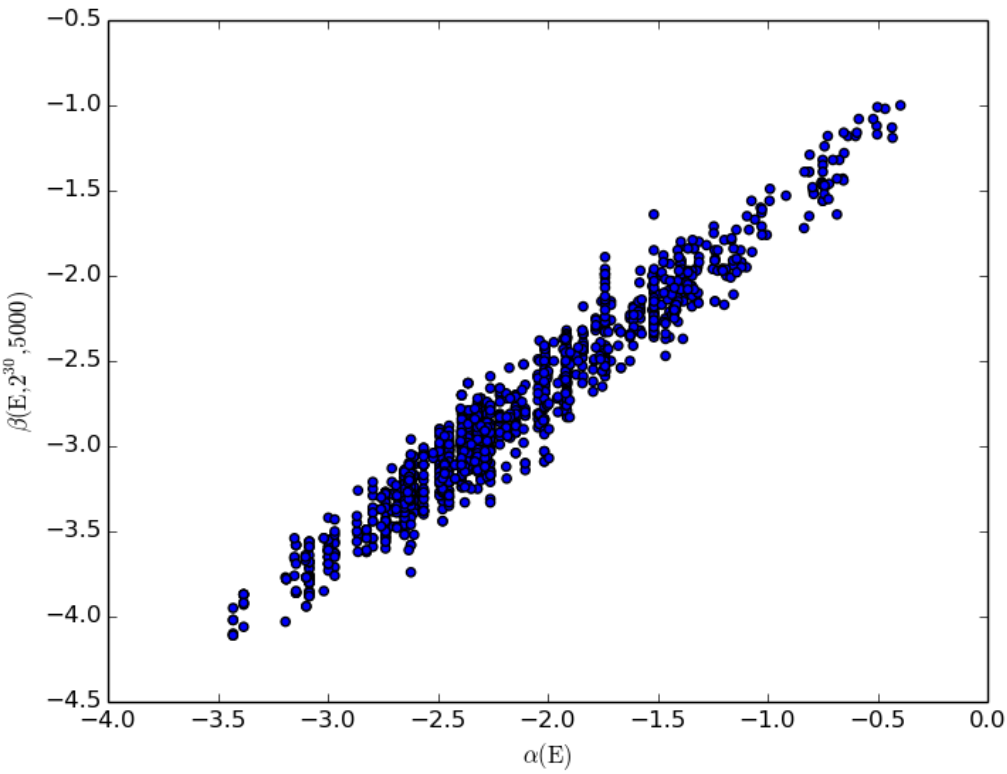
Let us prove the convergence of this series.

Theorem 15.2. *For any elliptic curve* $\mathrm{E}/\mathbb{Q}$ *without complex multiplication, the series* $\sum_\ell \alpha_\ell(\mathrm{E})$ *converges.*

Proof. By Serre's open image theorem, any elliptic curve E without complex multiplication has a finite set of primes ℓ such that the $\rho_{\mathrm{E},\ell^\infty}$ is not surjective. Hence, the series which defines α has the same nature of convergence as the series corresponding to a curve E for which $\rho_{\mathrm{E},\ell^\infty}$ is surjective. From Section 14.2, we have $\overline{v}_\ell(\mathrm{E}) = \frac{\ell(\ell^3+\ell^2-2\ell-1)}{(\ell+1)^2(\ell-1)^3}$. Hence, $\alpha_\ell(\mathrm{E}) = \log(\ell)\left(\frac{1}{\ell-1} - \overline{v}_\ell(\mathrm{E})\right) = \mathcal{O}\left(\frac{\log(\ell)}{\ell^2}\right)$, which is the term of a convergent series. $\square$

Note that, if $\rho_{\mathrm{E},\ell^\infty}$ is surjective for a curve E then $\alpha(\mathrm{E}) \approx -0.8119977339443$, which is negative and suggests that the cardinality of an elliptic curve has slightly more chances of being smooth than a random integer of the same size.

Comparing $\alpha(\mathrm{E})$ to $\beta(\mathrm{E}, 2^{30}, 5000)$ for 1525 families coming from Theorem 24.7, we get the following graph which suggests that $\beta_{\mathrm{E},n,\mathrm{B}}$ converges uniformly to $\alpha(\mathrm{E})$ when n and B go to infinity.



Let us take a few examples.

Example 15.3. 1. Let us consider a curve E from the family from [Kub76] which has $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Here, the value of $\overline{v}_2(\mathrm{E})$ changes from the value when $\rho_{\mathrm{E},2^\infty}$ is surjective, i.e. $\frac{14}{9}$, to $\frac{16}{3}$. Furthermore, for any generic curve in this family, for all primes ℓ different than 2, $\rho_{\mathrm{E},\ell^\infty}$ is surjective. Thus,

$$\alpha_{\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}} = \alpha_{generic} + \left(\frac{14}{9} - \frac{16}{3}\right)\log 2 \approx -3.4355.$$

2. Consider now a curve E from the Suyama-11 family parameterized in [BBB+13, Sec. 3.5.1]. Here $\overline{v}_2(\mathrm{E})$ changes from $\frac{14}{9}$ to $\frac{11}{3}$ and $\overline{v}_3$ changes from $\frac{87}{128}$ to $\frac{27}{16}$. And, for any generic curve in Suyama-11 family, for all primes different than 2 and 3, the corresponding Galois representation is surjective. Thus,

$$\alpha_{\mathrm{Suyama-11}} = \alpha_{generic} + \left(\frac{14}{9} - \frac{11}{3}\right)\log 2 + \left(\frac{87}{128} - \frac{27}{16}\right)\log 3 \approx -3.3825.$$

We can now test the efficiency of α by comparing the smoothness probabilities of $\#\mathrm{E}(\mathbb{F}_p)$ when p is a random prime of a given size n and that of a random integer of size $ne^{\alpha(\mathrm{E})}$.

Example 15.4. In the following tables, the first two columns give the proportions of B-smooth integers of size $n = 2^{25}$ and respectively ne^{α}. We compare them with the proportion of primes $p \sim n$ i.e. $p \in [n - 2\sqrt{n}, n + 2\sqrt{n}]$ for which $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth. The last two columns indicate relative errors, where the relative error of a with respect to b is $\frac{|a-b|}{|b|}$.

1. Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

	n	ne^{α}	$\#\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	0.000518	0.005753	0.005126	889 %	10.89 %
$\mathrm{B}_2 = 100$	0.008892	0.03883	0.042573	378.8 %	9.63 %

2. Suyama-11

	n	ne^{α}	$\#\mathrm{E}(\mathbb{F}_p)$	error_n	$\mathrm{error}_{ne^{\alpha}}$
$\mathrm{B}_1 = 30$	0.000518	0.005133	0.005743	1008 %	11.89 %
$\mathrm{B}_2 = 100$	0.008892	0.04013	0.04101	361%,	2.19%

15.2 $\alpha(\mathrm{E})$ over number fields

So far, we have considered rational elliptic curves E and their values of $\alpha(\mathrm{E})$. These curves fare better when we try to factor a random integer n. However, if more information is available about n, one might want to use it in order to factor n. For example, if we know that $n = 2^{2a} + 3$ for some a then -3 is a square modulo N, we consider families with better values of α over $\mathbb{Q}(\sqrt{-3})$. Indeed these family can be defined over $\mathbb{Q}(\sqrt{-3})$, however we restrict ourselves to the families defined over $\mathbb{Q}$. In this case, one must modify the definition of α from its original version of Section 15.1.

Let K be a number field, E a rational elliptic curve and ℓ a prime. We define the average valuation at ℓ of $\#\mathrm{E}(\mathbb{F}_p)$ when p is a random prime which splits completely in K by

$$\overline{v}_{\ell,\mathrm{K}}(\mathrm{E}) = \sum_{n \geq 1} n \,\mathrm{Prob}(\{p \text{ prime which splits completely in K} \mid \mathrm{val}_{\ell}(\#\mathrm{E}(\mathbb{F}_p) = n)\}).$$

The existence and the computation of $\overline{v}_{\ell,\mathrm{K}}(\mathrm{E})$ follow from Theorem 14.4. We now define α relative to K.

Definition 15.5. Given an elliptic curve $\mathrm{E}/\mathbb{Q}$, a prime ℓ and a number field K, we put

$$\alpha_{\ell,\mathrm{K}}(\mathrm{E}) = \log(\ell)(\overline{v}_{\ell}(n) - \overline{v}_{\ell,\mathrm{K}}(\mathrm{E}))$$

and

$$\alpha_{\mathrm{K}}(\mathrm{E}) = \sum_{\ell \text{ prime}} \alpha_{\ell,\mathrm{K}}(\mathrm{E}).$$

Example 15.6. Let $\mathrm{E} : y^2 + xy + y = x^3 + 9481x + 89898842$ and $\mathrm{K} = \mathbb{Q}(\zeta_3)$, the cyclotomic field of degree 3. For E, $\mathrm{Im}\rho_{\mathrm{E},2}$ and $\mathrm{Im}\rho_{\mathrm{E},3}$ both have order 2. On the other hand, p splits completely in K if, and only if, $p \equiv 1 \bmod 3$.

So in this case, $\overline{v}_{2,\mathrm{K}}$ changes from $\frac{14}{9}$ (generic value) to $\frac{8}{3}$ and $\overline{v}_{3,\mathrm{K}}$ changes from $\frac{87}{128}$ (generic value) to $\frac{21}{8}$. Thus,

$$\alpha_{\mathrm{K}}(\mathrm{E}) = \alpha_{generic} + \left(\frac{14}{9} - \frac{8}{3}\right)\log 2 + \left(\frac{87}{128} - \frac{21}{8}\right)\log 3 \approx -3.7193.$$

15.3 Going beyond α

Although α is very easy to compute, one can define more precise tools, e.g.

$$\mathbb{E}(\mathrm{E}) = \sum_{m\text{B-smooth integer} \leq n} \mathrm{Prob}\Big(m \text{ divides } \#\mathrm{E}(\mathbb{F}_p)\Big) \cdot \mathrm{Prob}\Big(x \text{ is } m\text{B-smooth}\Big),$$

where x denotes a random integer of the size of n. A key difference between α and $\mathbb{E}$ is that α depends on the probabilities of $\#\mathrm{E}(\mathbb{F}_p)$ being divisible by prime-powers but not on that of being divisible by composite numbers.

Indeed, it can happen (cf. example below) that two curves can have the same mod 2 and mod 3 Galois images and thus the same value of α yet have different probabilities that 6 divides $\#\mathrm{E}(\mathbb{F}_p)$. We describe this fact by saying E admits an entanglement at level 6 and we shall revisit it in Section 26.

Example 15.7. Let us consider the curves $\mathrm{E}_1 : y^2 = x^3 - 75x - 2950$ and $\mathrm{E}_2 : y^2 = x^3 + 45x - 366$ which have conjugate mod 2 and mod 3 Galois images. The following table gives compares probabilities of divisibility by 2, 3 and 6 for E_1 and E_2. These probabilities are computed using mod 6 Galois images for E_1 and E_2 and then using Theorem 14.3.

Curve	$\mathbb{P}(2\|\#(\mathrm{E}(\mathbb{F}_p))$	$\mathbb{P}(3\|\#(\mathrm{E}(\mathbb{F}_p))$	$\mathbb{P}(6\|\#(\mathrm{E}(\mathbb{F}_p))$	α
E_1	2/3	3/4	1/2	-1.39
E_2	2/3	3/4	**7/12**$>$ **2/3**$\cdot$ **3/4**	-1.39

If the Chebotarev density were a probability, one would say that the fact of being divisible by 2 and that of being divisible by 3 are correlated.

Chapter 4

Resolvent and subfields

The present chapter has a single purpose: finding solutions to Mazur's Program B as they correspond to ECM-friendly families of elliptic curves in the sense of Theorem 14.5. We consider two methods. The first one makes use of the resolvent method of computing Galois groups. We recall transitive subgroups of S_n and then apply the resolvent method to well-chosen torsion point fields. The second one is elementary and relies upon the computations of subfields of function fields. Some families we find in this chapter were previously known and some are new.

We start by describing the resolvent method of computing Galois groups. All that we shall say about Galois groups and their computations can be found in standard textbooks on Galois theory, see, for example, [Cox11a, Pra09]. We then answer the following question asked in [BBB+13].
Question: Is it possible to effectively use the resolvent method in order to compute equations (of elliptic curves) which improve the torsion properties?

Indeed, we establish that the resolvent method has its limitations when applied to torsion point fields.

16 Computing Galois groups

Let $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ be an irreducible, monic polynomial of degree n. Let us denote the Galois group of the splitting field of P by Gal(P). Considering the action of Gal(P) over an ordering of the roots of P, one can inject Gal(P) in the symmetric group S_n. A different ordering of roots would give a S_n-conjugate subgroup. We identify Gal(P) to its image in S_n up to conjugacy. As P is irreducible, Gal(P) is *transitive* i.e. for $i, j \in \{1, \ldots, n\}$, there exists $\sigma \in \mathrm{Gal(P)}$ such that $\sigma(i) = j$. We briefly recall the transitive subgroups of S_n for $n = 4, 5$ and 6. The list of transitive subgroups of S_n for $n \leq 32$ is known, see [CH08, Hul05].

16.1 Transitive subgroups

For the sake of completeness, note that S_1 and S_2 do not have any proper transitive subgroups. For S_3, the only proper transitive subgroup is the alternating group A_3.

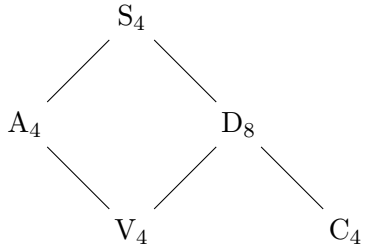


Figure 16.1: Transitive subgroups of S_4

Transitive subgroups of S_4

Let $G \neq S_4$ be transitive. As $\#S_4 = 24$, the possible orders of G are $1, 2, 3, 4, 6, 8$ and 12. Consider the natural action of G on $(1, 2, \ldots, 24)$. As G is transitive, the unique orbit of its action has length 4. Since this length divides the order of G, we must have $\#G = 4, 8$ or 12. If $\#G = 12$ then $G = A_4$ as A_n is the unique index 2 subgroup of S_n. The subgroups of order 8 are Sylow and thus conjugated. One of them is $\{(), (1234), (1432), (13)(24), (12)(34), (14)(23), (13), (24)\}$. This subgroup is isomorphic to the dihedral group D_8. Finally we consider the subgroups of order 4. There are two possibilities for a subgroup of order 4. It is isomorphic either to the cyclic group C_4 or to $V_4 := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Up to conjugacy in S_4, there is a unique possibility for C_4. Explicitly, we have $C_4 \simeq \{(), (1234), (13)(24), (1432)\}$ which is transitive. For V_4, we have two choices up to conjugacy in S_4. The first one is generated by $(12)(34)$ and $(13)(24)$ and the second one is generated by (12) and $(12)(34)$. One can see that only the first subgroup is transitive. Explicitly, we have $V_4 \simeq \{(), (12)(34), (13)(24), (14)(23)\}$.

Transitive subgroups of S_5

This part is reproduced from [Cox11a, Section 13.2].

Theorem 16.1 ([Cox11a, Theorem 13.2.2])**.** *The followings are the only transitive subgroups of* S_5 *up to conjugacy.*

1. S_5
2. A_5
3. $C_5 := \langle (12345) \rangle$
4. *A subgroup isomorphic to the following group of affine linear maps.*

$$\{f \mid f(i) = ai + b \text{ where } i, a, b \in \mathbb{F}_5, a \neq 0\}.$$

   For example, we identify the map $i \mapsto 2i$ *with the permutation* (1243) *or* $i \mapsto i + 1$ *with the permutation* (12345)*. As there are* $(5 - 1) \times 5$ *choices to choose* a *and* b*, the order of this subgroup is 20. We denote this subgroup by* $\mathrm{AGL}(\mathbb{F}_5)$*.*

5. $D_{10} := \mathrm{AGL}(\mathbb{F}_5) \cap A_5$.

Furthermore, every subgroup of order 20 (resp. 10) is S_5*-conjugated to* $\mathrm{AGL}(\mathbb{F}_5)$ *(resp.* D_{10}*).*

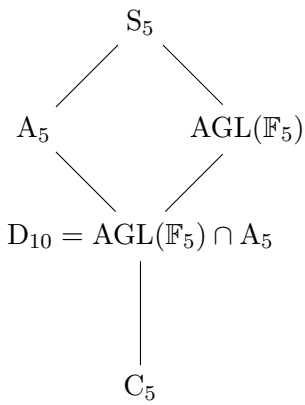


Figure 16.2: Transitive subgroups of S_5

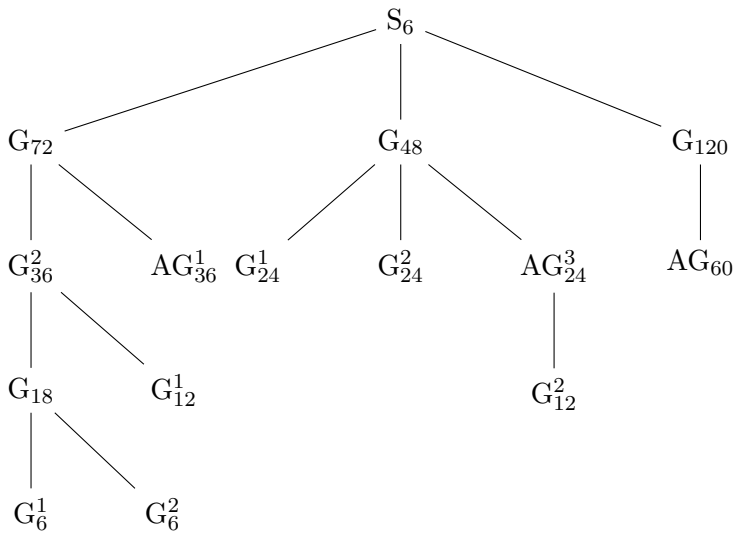


Figure 16.3: Transitive subgroups of S_6

Transitive subgroups of S_6

This section is reproduced from [Sta73].

Theorem 16.2 ([Sta73, Table 1])**.** *Up to conjugacy,* S_6 *has 15 transitive subgroups different than* A_6 *which are given in Figure 16.3, where* G_n^i *denotes the* i*-th subgroup of order* n *and the prefix* A *means that the subgroup is contained in* A_6*. A list of generators for each of these subgroups is in Table 16.1.*

Let us now discuss the *resolvent method* of computing Gal(P) described in [Sta73].

16.2 Resolvent method

Lagrange (see [Lag70]), in 1770's, analyzed methods of solving polynomial equations of degree less than 4 using permutations but his methods could not be extended to higher degrees (see [Cox11a, Section 12.1]). The resolvent method follows from Lagrange's analysis.

Throughout this section, $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ denotes a monic, irreducible polynomial of degree n. Let $(\theta_1, \ldots, \theta_n)$ be a fixed ordering of its complex roots.

Definition 16.3. Let G be a subgroup of S_n containing $\mathrm{Gal}(\mathrm{P})$. Let H be a subgroup of G and $\mathrm{F}(\mathrm{X}_1, \ldots, \mathrm{X}_n) \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_n]$ such that H is the stabilizer $\mathrm{Stab}_{\mathrm{G}}(\mathrm{F})$ of F in G. In other words,

$$\mathrm{H} = \{\sigma \in \mathrm{G} \mid \sigma\mathrm{F} := \mathrm{F}(\mathrm{X}_{\sigma(1)}, \ldots, \mathrm{X}_{\sigma(n)}) = \mathrm{F}(\mathrm{X}_1, \ldots, \mathrm{X}_n)\}.$$

We define the *resolvent polynomial* $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ as

$$\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P}) = \prod_{\sigma \in \mathrm{G}/\mathrm{H}} (\mathrm{X} - \mathrm{F}(\theta_{\sigma(1)}, \ldots, \theta_{\sigma(n)})).$$

Remark 16.4. *The degree of* $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ *is the index* $[\mathrm{G} : \mathrm{H}]$ *and one can see that* $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ *does not depend on the choice of coset representatives of* H *in* G*. Indeed, if* $\{\sigma_1, \ldots, \sigma_k\}$ *is a system of coset representatives of* H *in* G*. Then for* $\tau \in \mathrm{G}$*,* $\{\tau\sigma_1, \ldots, \tau\sigma_k\}$ *is also a system of coset representatives. Finally,* $\mathrm{R}_{\mathrm{G}}(\tau\mathrm{F}, \mathrm{P}) = \mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ *for all* $\tau \in \mathrm{G}$*.*

If $\mathrm{G} = \mathrm{S}_n$ then we call $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F}, \mathrm{P})$ the *absolute resolvent.* If G is a proper subgroup of S_n, we call the corresponding resolvent the *relative resolvent.*

Lemma 16.5. $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P}) \in \mathbb{Z}[\mathrm{X}]$.

Proof. As the coefficients of $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ are combinations of $\theta_1, \ldots, \theta_n$, they are algebraic integers. Furthermore, by Remark 16.4, they are fixed by G. As $\mathrm{Gal}(\mathrm{P}) \subset \mathrm{G}$, they are fixed by $\mathrm{Gal}(\mathrm{P})$ and hence are rational integers. □

Now we state the main theorem which gives us a technique to compute $\mathrm{Gal}(\mathrm{P})$.

Theorem 16.6 ([Cox11a, Prop 13.3.2])**.** *Let* G *be a subgroup of* S_n *and let* H *be a subgroup of* G*. Let* $\mathrm{F}(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ *be such that* $\mathrm{H} = \mathrm{Stab}_{\mathrm{G}}(\mathrm{F})$*. Then,*

1. *If* $\mathrm{Gal}(\mathrm{P})$ *is* G*-conjugated to a subgroup of* H *then* $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ *has a root in* $\mathbb{Z}$*.*
2. *if* $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ *has a simple root in* $\mathbb{Z}$ *then* $\mathrm{Gal}(\mathrm{P})$ *is* G*-conjugated to a subgroup of* H*.*

Proof. Suppose $\mathrm{Gal}(\mathrm{P})$ is G-conjugated to a subgroup N of H i.e. $\mathrm{Gal}(\mathrm{P}) = \tau^{-1}\mathrm{N}\tau$ for some $\tau \in \mathrm{G}$. Let $\sigma \in \mathrm{Gal}(\mathrm{P})$. Then $\sigma = \tau^{-1}\gamma\tau$ for some $\gamma \in \mathrm{N}$. As $\tau^{-1} \in \mathrm{G}$ is a coset representative of $\tau^{-1}\mathrm{H} \in \mathrm{G}/\mathrm{H}$, one of the roots of $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ is $\mathrm{F}(\theta_{\tau^{-1}(1)}, \ldots, \theta_{\tau^{-1}(n)})$. As $\gamma \in \mathrm{H} = \mathrm{Stab}_{\mathrm{G}}(\mathrm{F})$, we have

$$\begin{aligned}
\sigma\mathrm{F}(\theta_{\tau^{-1}(1)}, \ldots, \theta_{\tau^{-1}(n)}) &= \tau^{-1}\gamma\tau\mathrm{F}(\theta_{\tau^{-1}(1)}, \ldots, \theta_{\tau^{-1}(n)}) \\
&= \tau^{-1}\gamma\mathrm{F}(\theta_1, \ldots, \theta_n) \\
&= \mathrm{F}(\theta_{\tau^{-1}(1)}, \ldots, \theta_{\tau^{-1}(n)})
\end{aligned}$$

So, $\mathrm{F}(\theta_{\tau^{-1}(1)}, \ldots, \theta_{\tau^{-1}(n)})$ is fixed by $\mathrm{Gal}(\mathrm{P})$ so it must be rational and as θ_i are algebraic integers, it must be an integer.

On the other hand, suppose $\mathrm{R}_{\mathrm{G}}(\mathrm{F}, \mathrm{P})$ has a simple root in $\mathbb{Z}$, say $\mathrm{F}(\theta_{\rho(1)}, \ldots, \theta_{\rho(n)})$ for some $\rho \in \mathrm{G}$. Furthermore, for any $\sigma \in \mathrm{Gal}(\mathrm{P})$,

$$\sigma\mathrm{F}(\theta_{\rho(1)}, \ldots, \theta_{\rho(n)}) = \mathrm{F}(\theta_{\rho(1)}, \ldots, \theta_{\rho(n)}).$$

The above equality can also be written as,

$$\sigma\rho\mathrm{F}(\theta_1,\ldots,\theta_n) = \rho\mathrm{F}(\theta_1,\ldots,\theta_n).$$

As $\mathrm{F}(\theta_{\rho(1)},\ldots,\theta_{\rho(n)})$ is a simple root of $\mathrm{R_G}(\mathrm{F},\mathrm{P})$, we have $\sigma\rho\mathrm{F} = \rho\mathrm{F}$. Indeed, otherwise $\sigma\rho$ would belong to a different coset than that of ρ and hence the roots $\sigma\rho\mathrm{F}(\theta_1,\ldots,\theta_n)$ and $\rho\mathrm{F}(\theta_1,\ldots,\theta_n)$ would correspond to two *different* cosets. This cannot be the case as we have assumed that $\mathrm{F}(\theta_{\rho(1)},\ldots,\theta_{\rho(n)})$ is a simple root. So necessarily, $\sigma \in \mathrm{Stab_G}(\rho\mathrm{F})$. Finally, it is not difficult to see that $\mathrm{Stab_G}(\rho\mathrm{F}) = \rho\mathrm{Stab_G}(\mathrm{F})\rho^{-1} = \rho\mathrm{H}\rho^{-1}$. We conclude that $\mathrm{Gal}(\mathrm{P})$ is G-conjugated to a subgroup of H. □

In practice, one can get a resolvent having multiple roots. In such cases, one can either change P using a Tschirnhausen transformation ([Coh13, Alg. 6.3.4]) which leaves $\mathrm{Gal}(\mathrm{P})$ unchanged or one can change F. It is known that there exists F' such that if $\mathrm{Gal}(\mathrm{P}) \subset \mathrm{H} \subset \mathrm{G}$ then $\mathrm{R_G}(\mathrm{F}',\mathrm{P})$ has simple roots, see [Pra09, Theorem 5.4.4]. Constructing simpler polynomial $\mathrm{F}(\mathrm{X}_1,\ldots,\mathrm{X}_n)$ which are invariant under prescribed subgroups of S_n is an interesting problems, see [Val08, Abd99, KM00].

One can also consider non-linear factors of a resolvent as they provide information about $\mathrm{Gal}(\mathrm{P})$, see [Val95] for more details.

Determination of Gal(P)

Equipped with resolvents, we can determine $\mathrm{Gal}(\mathrm{P})$. This section is reproduced from [Sta73]. The reader can also refer to [Ber29]. We continue to suppose that $\mathrm{P} \in \mathbb{Z}[\mathrm{X}]$ is a monic, irreducible polynomial of degree n. Let us suppose that we know n complex roots of P with high precision and the lattice of transitive subgroups of S_n.

Algorithm 16.7.

1. Choose a maximal transitive subgroup $\mathrm{H} \neq \mathrm{A}_n$ of index k in S_n and a function $\mathrm{F} \in \mathbb{Z}[\mathrm{X}_1,\ldots,\mathrm{X}_n]$ such that $\mathrm{Stab}_{\mathrm{S}_n}(\mathrm{F}) = \mathrm{H}$. Then compute $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F},\mathrm{P})$ numerically. By Theorem 16.5, we know that this resolvent has integer coefficients. Round the coefficients of $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F},\mathrm{P})$ to the nearest integers in order to get the *exact* value of $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F},\mathrm{P})$.

2. If $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F},\mathrm{P})$ has multiple roots, apply the Tschirnhausen transformation (see [Coh13, Alg. 6.3.4]) to P or change F, till one obtains simple roots or no roots at all. If $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F},\mathrm{P})$ has no simple roots then move on to another maximal subgroup of S_n and start again. If $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F},\mathrm{P})$ does not have simple roots for any maximal subgroup H of S_n then conclude $\mathrm{Gal}(\mathrm{P}) = \mathrm{S}_n$, if $\mathrm{Disc}(\mathrm{P}) \neq \square$. If $\mathrm{Disc}(\mathrm{P}) = \square$, conclude $\mathrm{Gal}(\mathrm{P}) = \mathrm{A}_n$.

3. If for some maximal subgroup H, $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F},\mathrm{P})$ has simple roots, then by Theorem 16.6, $\mathrm{Gal}(\mathrm{P}) \subset \mathrm{H}$ up to conjugacy. Then continue the method using the maximal subgroups of H until we obtain the minimal subgroup H' containing $\mathrm{Gal}(\mathrm{P})$ up to conjugacy.

4. Finally, conclude $\mathrm{Gal}(\mathrm{P}) = \mathrm{H}'$, if $\mathrm{Disc}(\mathrm{P}) \neq \square$. If $\mathrm{Disc}(\mathrm{P}) = \square$, conclude $\mathrm{Gal}(\mathrm{P}) = \mathrm{A}_n \cap \mathrm{H}'$

List of invariant polynomial

Here we give a list of invariant polynomials $\mathrm{F} \in \mathbb{Z}[x_1,\ldots,x_n]$ corresponding to different transitive subgroups of S_n from [Sta73].

Label	$\subset$	Invariant polynomial	Generators
D_8	S_4	$x_1x_3 + x_2x_4$	$\langle(1234),(13)\rangle$
C_4	D_8	$x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_1^2$	$\langle(1234)\rangle$
V_4	A_4	-	$\langle(12)(34),(13)(24)\rangle$
$AGL(\mathbb{F}_5)$	S_5	F_1	$\langle(12345),(2354)\rangle$
D_{10}	$AGL(\mathbb{F}_5) \cap A_5$	-	$\langle(12345),(25)(34)\rangle$
C_5	D_{10}	$x_1x_2^2 + x_2x_3^2 + x_3x_4^2 + x_4x_5^2 + x_5x_1^2$	$\langle(12345)\rangle$
G_{72}	S_6	$x_1x_2x_3 + x_4x_5x_6$	$\langle(123),(456),(12),(45),(14)(25)(36)\rangle$
AG_{36}^1	$G_{72} \cap A_6$	-	$\langle(123),(456),(12)(45),(1425)(36)\rangle$
G_{36}^2	G_{72}	F_2	$\langle(123),(456),(12)(45),(14)(25)(36)\rangle$
G_{18}	G_{36}^2	F_3	$\langle(123),(456),(14)(25)(36)\rangle$
G_{12}^1	G_{36}^2	$x_1x_4 + x_2x_5 + x_3x_6$	$\langle(123)(456),(12)(45),(14)(25)(36)\rangle$
G_6^1	G_{18}	$x_1x_4 + x_2x_6 + x_3x_5$	$\langle(123)(465),(14)(25)(36)\rangle$
G_6^2	G_{18}	$x_1x_2^2 + x_2x_3^2 + x_3x_4^2 +$ $x_4x_5^2 + x_5x_6^2 + x_6x_1^2$	$\langle(123)(456),(14)(25)(36)\rangle$
G_{48}	S_6	$x_1x_2 + x_3x_4 + x_5x_6$	$\langle(12),(34),(56),(135)(246),(13)(24)\rangle$
G_{24}^1	G_{48}	F_4	$\langle(12)(34),(34)(56),(12)(56),$ $(135)(246),(14)(23)(56)\rangle$
G_{24}^2	G_{48}	F_5	$\langle(12)(34)(56),(34)(56),(56),(135)(246)\rangle$
AG_{24}^3	$G_{48} \cap A_6$	-	$\langle(135)(246),(13)(24),(12)(34),(34)(56)\rangle$
G_{12}^2	AG_{24}^3	F_5	$\langle(12)(34),(34)(56),(12)(56),(135)(246)\rangle$
G_{120}	S_6	F_6	$\langle(126)(354),(12345),(2354)\rangle$
AG_{60}	$G_120 \cap A_6$	-	$\langle(126)(354),(12345),(25)(34)\rangle$

Table 16.1: Transitive groups and invariant polynomials

$$
\begin{aligned}
F_1 &= (x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 - x_1x_3 - x_3x_5 - x_5x_2 - x_2x_4 - x_4x_1)^2 \\
F_2 &= (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)(x_4 - x_5)(x_5 - x_6)(x_6 - x_4) \\
F_3 &= (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) + (x_4 - x_5)(x_5 - x_6)(x_6 - x_4) \\
F_4 &= (x_1 + x_2 - x_3 - x_4)(x_3 + x_4 - x_5 - x_6)(x_5 + x_6 - x_1 - x_2)(x_1 - x_2)(x_3 - x_4)(x_5 - x_6) \\
F_5 &= (x_1 + x_2 - x_3 - x_4)(x_3 + x_4 - x_5 - x_6)(x_5 + x_6 - x_1 - x_2) \\
F_6 &= (x_1x_2 + x_3x_5 + x_4x_6)(x_1x_3 + x_4x_5 + x_2x_6)(x_3x_4 + x_1x_6 + x_2x_5) \\
&\quad (x_1x_5 + x_2x_4 + x_3x_6)(x_1x_4 + x_2x_3 + x_5x_6)
\end{aligned}
$$

Remark 16.8. *Table 16.1 gives various transitive subgroups, their generators and corresponding invariant polynomials. At some occasions we do not provide a polynomial, as one can certify whether* $\mathrm{Gal}(P) \subset G$ *by eliminating other possibilities.*

Examples

1. Let $P = x^4 + 3x^2 + 1 \in \mathbb{Q}[x]$ with discriminant $\mathrm{Disc}(P)$ is 20^2. So $\mathrm{Gal}(P) \subset A_4$. It remains to verify whether $\mathrm{Gal}(P) \subset V_4 = A_4 \cap D_8$ (see Figure 16.1). So we compute $R_{S_n}(F, P)$ where $F = x_1x_3 + x_2x_4$ is invariant under D_8 in S_n (see Table 16.1). If $R_{S_n}(F, P)$ has a simple root then $\mathrm{Gal}(P) \subset V_4$. Let $D_8 = \langle(1234),(12)(34)\rangle$ and

let $\{(), (123), (132)\}$ be coset representatives of D_8 in S_4. We also have complex θ_i roots of P up to precision of 3 decimal places. They are $\theta_1 = 1.618i$, $\theta_2 = -1.618i$, $\theta_3 = 0.618i$ and $\theta_4 = 0.618i$. Then we obtain,

$$\mathrm{R}_{\mathrm{S}_4}(x_1x_3 + x_2x_4, x^4 + 3x^2 + 1) = x^3 - 2.999x^2 - 3.999x + 11.998.$$

We round it to $x^3 - 3x^2 - 4x + 12 = (x+2)(x-2)(x-3)$. Thus, $\mathrm{Gal}(\mathrm{P}) = \mathrm{V}_4$.

2. Let $\mathrm{E} : y^2 = x^3 + ax + b$ be a rational elliptic curve. Let us assume that $x^3 + ax + b$ is irreducible. Note that the torsion point field $\mathbb{Q}(\mathrm{E}[2])$ is the splitting field of $x^3 + ax + b$. As A_3 is the only proper transitive subgroup of S_3, to conclude that $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[2])/\mathbb{Q}) \subset \mathrm{A}_3$ if, and only if, $\Delta_{\mathrm{E}} = \square$.

We now consider resolvents over the field of *formal* coefficients. We shall see it soon in an example. This idea was proposed by Bill Allombert during a discussion and the reader can find similar results in [Cox11a, Section 13.1, 13.2].

16.3 Formal resolvents

Let P be defined by $x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Q}[x_1, \ldots, x_n]$ where the coefficients a_i are indeterminates. Let $\theta_1, \ldots, \theta_n$ be formal roots of P. We know by Vieta's relations that the coefficients a_i can be expressed as symmetric polynomials in θ_i. Let us further consider a subgroup H of S_n and F such that $\mathrm{H} = \mathrm{Stab}_{\mathrm{S}_n}(\mathrm{F})$. One can formally compute $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F}, \mathrm{P})$ to determine whether $\mathrm{Gal}(\mathrm{P})$ is contained in H up to conjugacy.

As the resolvent $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F}, \mathrm{P})$ is defined using the cosets of H in S_n, one can see that the coefficients of $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F}, \mathrm{P})$, which are combinations of θ_i, are invariant under the action of S_n. Thus, by the fundamental theorem of symmetric polynomials ([Pra09, Theorem 3.1.1]), one can decompose the coefficients of $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F}, \mathrm{P})$ using the elementary symmetric functions. This gives us the resolvent $\mathrm{R}_{\mathrm{S}_n}(\mathrm{F}, \mathrm{P})$ defined using only the coefficients a_i. Let us illustrate it with an example.

Example 16.9. Let $\mathrm{P} = x^4 + ax^3 + bx^2 + cx + d$ defined over $\mathbb{Q}(a, b, c, d)$. Put $\theta_1, \ldots, \theta_4$ for its roots. By Vieta's relations, we have,

$$\begin{aligned}
a &= -(\theta_1 + \theta_2 + \theta_3 + \theta_4) \\
b &= \theta_1\theta_2 + \theta_1\theta_3 + \theta_1\theta_4 + \theta_2\theta_3 + \theta_2\theta_4 + \theta_3\theta_4 \\
c &= -(\theta_1\theta_2\theta_3 + \theta_1\theta_2\theta_4 + \theta_1\theta_3\theta_4 + \theta_2\theta_3\theta_4) \\
d &= \theta_1\theta_2\theta_3\theta_4
\end{aligned}$$

Let us consider $\mathrm{D}_8 \subset \mathrm{S}_4$ generated by $\langle (1234), (12)(34) \rangle$. Let $\{(), (123), (132)\}$ be its coset representatives in S_4. With these generators, we have $\mathrm{D}_8 = \mathrm{Stab}_{\mathrm{S}_n}(\mathrm{F})$ for $\mathrm{F} = x_1x_3 + x_2x_4$ (see Table 16.1). We have,

$$\begin{aligned}
\mathrm{R}_{\mathrm{S}_n}(\mathrm{F}, \mathrm{P}) &= \prod_{\sigma \in \mathrm{S}_n/\mathrm{D}_8} (\mathrm{X} - \mathrm{F}(\theta_{\sigma(1)}, \theta_{\sigma(2)}, \theta_{\sigma(3)}, \theta_{\sigma(4)})). \\
&= (\mathrm{X} - (\theta_1\theta_3 + \theta_2\theta_4)) \cdot (\mathrm{X} - (\theta_2\theta_1 + \theta_3\theta_4)) \cdot (\mathrm{X} - (\theta_3\theta_2 + \theta_1\theta_4)) \\
&= \mathrm{X}^3 + \Theta_2\mathrm{X}^2 + \Theta_1\mathrm{X} + \Theta_0 \quad \text{where,}
\end{aligned}$$

$$\begin{aligned}
\Theta_0 &= -(\theta_1^2\theta_2^2\theta_3^2 + \theta_1^3\theta_2\theta_3\theta_4 + \theta_1\theta_2^3\theta_3\theta_4 + \theta_1\theta_2\theta_3^3\theta_4 + \theta_1^2\theta_2^2\theta_4^2 + \theta_1^2\theta_3^2\theta_4^2 + \theta_2^2\theta_3^2\theta_4^2 + \theta_1\theta_2\theta_3\theta_4^3) \\
\Theta_1 &= \theta_1^2\theta_2\theta_3 + \theta_1\theta_2^2\theta_3 + \theta_1\theta_2\theta_3^2 + \theta_1^2\theta_2\theta_4 + \theta_1\theta_2^2\theta_4 + \theta_1^2\theta_3\theta_4 + \theta_2^2\theta_3\theta_4 + \theta_1\theta_3^2\theta_4 + \theta_2\theta_3^2\theta_4 \\
&\quad + \theta_1\theta_2\theta_4^2 + \theta_1\theta_3\theta_4^2 + \theta_2\theta_3\theta_4^2 \\
\Theta_2 &= -(\theta_1\theta_2 + \theta_1\theta_3 + \theta_2\theta_3 + \theta_1\theta_4 + \theta_2\theta_4 + \theta_3\theta_4)
\end{aligned}$$

The expressions defining Θ_0, Θ_1 and Θ_2 are S_4 invariant and thus one can decompose them in terms of the elementary symmetric polynomials to get

$$\begin{aligned}\Theta_0 &= 4bd - a^2d - c^2\\ \Theta_1 &= ac - 4d\\ \Theta_2 &= -b\end{aligned}$$

Thus, $\mathrm{Gal}(P) \subset D_8$ if $X^3 - bX^2 + (ac - 4d)X + (4bd - a^2d - c^2)$ has a simple root in $\mathbb{Q}(a, b, c, d)$.

As the degree of a resolvent is equal to the index of the subgroup in S_n, a subgroup of small order gives a complicated resolvent. In order to avoid it, note that if P is given by $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, one can make a change of variable by putting $x - \frac{a_{n-1}}{n}$ to get rid of $a_{n-1}x^{n-1}$ in P. This change of variable leaves Gal(P) unaffected. With this, one can obtain relatively simpler expressions for resolvents.

We compute resolvents for other transitive subgroups of S_4 to obtain the following.

Theorem 16.10. *Let* $P = x^4 + bx^2 + cx + d$ *be an irreducible rational polynomial. Then,*

1. $\mathrm{Gal}(P) \subset D_8$ *if* $x^3 - bx^2 - 4dx - c^2 + 4bd$ *has a simple rational root.*

2. $\mathrm{Gal}(P) \subset V_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *if* $x^6 - 6bx^5 + (13b^2 - 24d)x^4 - (12b^3 - 96bd)x^3 + (4b^4 - 120b^2d + 144d^2)x^2 + (48b^3d - 288bd^2)x + 4b^3c^2 - 16b^4d + 27c^4 - 144bc^2d + 272b^2d^2 - 256d^3$ *has a simple rational root.*

3. $\mathrm{Gal}(P) \subset C_4 = \mathbb{Z}/4\mathbb{Z}$ *if* $x^6 - 6cx^5 + (2b^3 + 24c^2 - 8bd)x^4 - (8b^3c + 56c^3 - 32bcd)x^3 + (b^6 + 22b^3c^2 - 12b^4d + 96c^4 - 120bc^2d + 48b^2d^2 - 64d^3)x^2 - (2b^6c + 28b^3c^3 - 24b^4cd + 96c^5 - 176bc^3d + 96b^2cd^2 - 128cd^3)x + b^6c^2 + 16b^3c^4 - 28b^4c^2d + 64c^6 - 224bc^4d + 176b^2c^2d^2 - 320c^2d^3$ *has a simple rational root.*

Remark 16.11. *In order to test whether the roots of a polynomial* P *are simple, it suffices to test* $\mathrm{Disc}(P) \neq 0$.

Example 16.12. Consider the polynomial $T = x^4 + tx^3 + tx + 1 \in \mathbb{Z}(t)$.[1] We evaluate the resolvent from Theorem 16.10 corresponding to D_8 at the coefficients of T to get $R_{S_n}(F, T) = (x - 2)\left(x^2 + t^2 + 2x\right)$. Thus, $\mathrm{Gal}(T) \subset D_8$. Here, one can even specialize a, b, c and d at different rational values i.e. replace them with rational numbers a_0, b_0, c_0 and d_0, respectively. Let P_0 be the resulting polynomial. It is known (see [VdWAN50, Section 61]) that, $\mathrm{Gal}(P_0)$ is S_n-conjugated to a subgroup of Gal(P).

17 Formal resolvent to find ECM-friendly curves

Recall that our objective is to find infinite families of rational elliptic curves E such that $\rho_{E,m}$ is not surjective for some m. Let us start with an example.

Example 17.1. Let E be defined by $y^2 = (x - a)(x^2 + bx + c)$ over the function field $\mathbb{Q}(a, b, c)$ where a, b and c are indeterminates. The point $(a, 0)$ has order 2 and $E(\mathbb{Q}(a, b, c))[2] = \mathbb{Z}/2\mathbb{Z}$. We are interested in knowing what happens if we specialize at a, b, c i.e. replace them by rational numbers $a = a_0, b = b_0$ and $c = c_0$. Let us denote

[1] This polynomial is from [Smi93].

the resulting curve by E_0. If $b_0^2 = 4c_0$ then E_0 is singular. If $b_0^2 - 4c_0 = \square \neq 0$ then $\mathrm{E}_0(\mathbb{Q})[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Clearly, for *almost all* (read *generic*) values of b_0 and c_0,

$$\mathrm{E}_0(\mathbb{Q})[2] = \mathrm{E}(\mathbb{Q}(a, b, c))[2].$$

Here, we say, E is an infinite family of rational elliptic curves with a point of order 2.

Let us explore the usage of *generic* in the example above. Let $\mathrm{K} = \mathbb{Q}(t)$ and consider $\mathrm{P} := x^2 - t \in \mathrm{K}[x]$. By Hilbert's irreducibility, (see [Lan83, Cor. 2.5]), P is irreducible for infinitely many rational specializations. Let K_1 be the extension of K obtained by adjoining a root of P. Note that K_1 is Galois over K and its Galois group does not change for most of the specializations of t and changes to the trivial group for a sparse set of rationals t.

Before applying the method of formal resolvents to torsion point fields, let us briefly recall a few classical results about plane curves. Let $\mathcal{C}$ be a smooth plane curve of genus g defined over a number field K. If $g \geq 2$, Faltings' theorem says that the set $\mathcal{C}(\mathrm{K})$ of K-rational points of $\mathcal{C}$ is finite. If $g = 1$ and C has one K-rational point then $\mathcal{C}$ is an elliptic curve. We use an algorithm from [vH95] (implemented in MAPLE's "algcurves" package) to put it in Weierstrass form. Note that, the algorithm can fail to find a K-rational point on $\mathcal{C}$ even if there exist such points. In this case, the user must provide a point. We succeed in doing so in all the computations in this work.

Cremona's algorithm from [Cre01] (implemented in SAGE) enables one to compute the rank of an elliptic curve E and the generators of the Mordell-Weil group of E. The search bounds of the algorithm can make the computations impractical; however, in this work, we succeed in either certifying that the rank is 0 or in finding the generators.

If $g = 0$, we use an algorithm from [vH97] (implemented in MAPLE's "algcurves" package) to parameterize it. The algorithm succeeds in all the cases we encounter.

Example 17.2 (Computations with MAPLE)**.** Let $\mathcal{C}_1$ be defined by $x^2 + y^2 - 3$ and $\mathcal{C}_2$ be defined by $y^2 - x^4 - 1$. We compute various objects related to these curves using MAPLE.

```
>with(algcurves):
>C1:=y^2+x^2-2: C2:=y^2-x^4-1:
>genus(C1,x,y); genus(C2,x,y);
0
1
>parametrization(C1,x,y,t);
[(-t^2+2t+1)/(t^2+1), (t^2+2t-1)/(t^2+1)]
>W:=Weierstrassform(C2,x,y,x0,y0):
>W[1];
x0^3+y0^2-4x0
>W[2],W[3];
2(y-1)/x^2, -4(y-1)/x^3
>W[4],W[5];
2y0/(x0^2-4),-(2x0^2+8)/(2(x0^2-4))
```

In the output of parameterization, we obtain $[x(t), y(t)]$ the parameterizations of variables x and y in $\mathcal{C}_1$. The curve $\mathcal{C}_2$ has genus 1 and we ask to puts it on Weierstrass form E_2. MAPLE searches for a point and put in a Weierstrass form. The first output is the elliptic curve E_2. The second and the third output defines a mapping $\mathcal{C}_2 \longrightarrow \mathrm{E}_2$ and the fourth and fifth output gives the inverse map from $\mathrm{E}_2 \longrightarrow \mathcal{C}_2$.

17.1 Formal resolvent: $\ell = 3$

Let $\mathrm{K} = \mathbb{Q}(a, b)$ and let E be an elliptic curve defined by $y^2 = x^3 + ax + b$ over K. Generically, in the sense of Example 17.1, the degree of $\mathrm{K}(\mathrm{E}[3])$ is 48; the order of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. Let $\psi_3 = x^4 + 2ax^2 + 4bx - \frac{1}{3}a^2$ be the 3-division polynomial of E. Over K, ψ_3 is irreducible. By Lemma 9.4, the splitting field of ψ_3 has degree 24. In other words, $\mathrm{Gal}(\psi_3)$ is generically S_4. We are interested in the parameterization $a = a(t)$ and $b = b(t)$ which would result in a smaller size of the corresponding Galois group over $\mathbb{Q}(t)$.

We first prove the following and then proceed to parameterizations.

Proposition 17.3. *Let* $\mathrm{E} : y^2 = x^3 + ax + b$ *be a rational elliptic curve. Suppose* ψ_3 *is irreducible and* $\mathrm{Gal}(\psi_3)$ *is not of order 24. Then*

1. $\mathrm{Gal}(\psi_3)$ *is isomorphic to a subgroup of either* D_8 *or* C_4.

2. $\mathrm{Gal}(\psi_3)$ *is isomorphic to a subgroup of* D_8 *if the polynomial* $3x^3 - 6ax^2 + 4a^2x - (8a^3 + 48b^2)$ *has a simple rational root.*

3. $\mathrm{Gal}(\psi_3)$ *is isomorphic to a subgroup of* C_4 *if the polynomial* R_4 *from [BS19b] has a simple rational root.*

Proof. Our strategy is to apply Theorem 16.10 to ψ_3. Consider first the discriminant of ψ_3 which is $-\frac{256}{27}\left(4\,a^3 + 27\,b^2\right)^2 = -3\square$. As this discriminant can never be a rational square, the Galois group can only be D_8 or C_4, see Figure 16.1. We then compute the formal resolvents for D_8 and C_4 to obtain the result. $\square$

We now choose to parameterize the coefficients $a = a(t)$ and $b = b(t)$ in such a way that the resolvent polynomials coming from the proposition above have rational roots.

1. $\mathrm{Gal}(\psi_3) \subset \mathrm{D}_8$ if
$$3x^3 - 6ax^2 + 4a^2x - (8a^3 + 48b^2)$$
has a simple root. Let us put $a = a(s) = s$ and $b = b(s) = s$. The resulting plane curve $\mathcal{C}$ is defined by
$$3x^3 - 6sx^2 + 4s^2x - (8s^3 + 48s^2).$$
This curve has genus 0 and can be parameterized by setting
$$x(t) = \frac{48t}{(t-2)(3t^2+4)}$$
$$s(t) = \frac{48}{(t-2)(3t^2+4)}.$$
Thus, for all $t \in \mathbb{Q}/\{2\}$, the 3-torsion point field of the elliptic curve defined by $y^2 = x^3 + s(t)x + s(t)$ has degree at most 16.

2. For C_4, we obtain a polynomial R_4 in x, a, b of degree 6 in x. However no simple parameterization $a = a(s)$ and $b = b(s)$ gives a curve of genus 0 or 1. We give up on this for now but we will come back to it soon in the next section.

We have proved the following.

Proposition 17.4. *Let* $\mathrm{E} : y^2 = x^3 + ax + b$ *be a rational elliptic curve where*

$$a = b = \frac{48}{(t-2)(3t^2+4)}, \qquad \textit{for some } t \neq 2.$$

Then $\mathrm{Gal}(\psi_3)$ *is of order at most 8. In particular,* $\mathrm{Im}\rho_{\mathrm{E},3}$ *is of order at most 16.*

Proof. The parameterization is evident from the discussion above. And using Lemma 9.4, the order of $\mathrm{Im}\rho_{\mathrm{E},3}$ is at most twice of the degree of the splitting field ψ_3. □

One can also use j-invariants instead of the coefficients a and b of E. The major advantage of using j-invariants is one would obtain curves, and not surfaces, and we can apply Faltings' theorem.

17.2 Using j-invariants

We saw that there exists an elliptic curve with any prescribed j-invariant. For example, the curve E_j defined by $y^2 = x^3 - 3(j-1728)jx - 2(j-1728)^2 j$ has the j-invariant j. In order to avoid three variables, we can work with E_j and expect to obtain families parameterized by j.[2] Let us take an example.

Example 17.5. Let E_j be defined by $y^2 = x^3 - 3(j-1728)jx - 2(j-1728)^2 j$ over $\mathbb{Q}(j)$. Let ψ_3 be the 3-division polynomial of E_j. We have

$$\psi_3 = x^4 - 6j(j-1728)x^2 - 8j(j-1728)^2 x - 3j^2(j-1728)^2.$$

We look for parameterizations $j = j(t)$ such that $\mathrm{Gal}(\psi_3)$ has order less than 24. As $\Delta_{\psi_j} = -3\square$, $\mathrm{Gal}(\psi_3)$ can only be contained in D_8 or C_4.

1. Considering the resolvent polynomial associated to D_8, we see that, $\mathrm{Gal}(\psi_3) \subset \mathrm{D}_8$, if

   $$\mathcal{C}_j = x^3 + 6(j-1728)jx^2 + 12(j-1728)^2 j^2 x - 64(j-1728)^4 j^2 + 72(j-1728)^3 j^3$$

   has a simple root. The plane curve defined by $\mathcal{C}_j$ has genus 0 and can be parameterized by setting

   $$j = j(t) = t^3, \quad x = x(t) = -2t^2(t^4 + 24t^3 - 1728t - 41472).$$

   Thus for any rational elliptic curve E with $j = t^3$ for some $t \in \mathrm{Q}$, the order of $\mathrm{Gal}(\psi_3)$ is at most 8 and using Lemma 9.4, $\mathbb{Q}(\mathrm{E}[3])$ has the degree at most 16.

2. For C_4, the curve defined by the resolvent has genus 22 and thus has only finitely many points.

Using the j-invariants, we can also consider the situation when ψ_3 is irreducible. As ψ_3 has degree 4, we have the following cases: 1. ψ_3 has one root, 2. ψ_3 has two roots, 3. ψ_3 splits completely, and, 4. ψ_3 has two irreducible quadratic factors. We shall treat all of these cases.

[2] As it turns out, this is the right approach which we shall consider in the next chapter.

1. Let $\mathcal{C}_3$ be the plane curve defined by $\psi_3 = x^4 - 6j(j-1728)x^2 - 8j(j-1728)^2x - 3j^2(j-1728)^2$. It has genus 0 and we parameterize it by setting

$$j = j(t) = -\frac{t^3(t-24)}{t+3}, \quad x = x(t) = \frac{t(t-24)(t^2-12t-72)}{t+3}.$$

With the substitution $j = j(t)$, ψ_3 has a root in $\mathbb{Q}(t)$. Let ψ_3' denote the irreducible cubic factor of ψ_3. Put E_j' for the elliptic curve with the j-invariant $j(t)$. For $t_0 \in \mathbb{Q}/\{-3\}$, let E_{t_0} be the curve defined by the specialization $\mathrm{E}_{j,t=t_0}'$. For all but finitely many specializations $t = t_0$, $\mathrm{E}_{j,t=t_0}'$ is an elliptic curve for which the order of $\mathrm{Gal}(\psi_3)$ at most 6 i.e. the order of the torsion point field $\mathbb{Q}(\mathrm{E}_{j,t=t_0}'[3])$ is at most 12, by Lemma 9.4.

2. We work on E_j'. If ψ_3 has 2 roots then ψ_3' must have a root. Let $\mathcal{C}_3'$ denote the plane curve defined by ψ_3'. This curve is also of genus 0 and we can further parameterize it by setting

$$t(s) = -\frac{3(s^3+216)}{s^3-27}.$$

Note that the expressions given by MAPLE are quite complicated and one needs to simplify them with suitable transformations. We use this expression of $t(s)$ from Chapter 5. Finally, the 3-division polynomial of the elliptic curve with j-invariant

$$j'(s) = -\frac{t(s)^3(t(s)-24)}{t(s)+3}$$

has two roots over $\mathbb{Q}(s)$. Let ψ_3'' be the remaining quadratic factor and let E_j'' be the elliptic curve with the j-invariant $j'(s)$. For all but finitely many rational specializations of s, the resulting curve E is such $\mathbb{Q}(\mathrm{E}[3])$ has order at most 4.

3. We work on E_j''. Let Δ_s be the discriminant of ψ_3''. We verify that $\Delta_t = -3\square \in \mathbb{Q}(s)$. So, no rational specialization of s would be such that ψ_3 would split completely.

4. Let us now suppose that ψ_3 has two irreducible quadratic factors. Let $a(j) = -3\,(j-1728)j$ and $b(j) = -2\,(j-1728)^2 j$; the coefficients of E_j. We write,

$$\psi_3 = x^4 + 2a(j)x^2 + 4b(j)x - \frac{a(j)^2}{3} = (x^2 + e_2x + e_1)(x^2 + f_2x + f_1)$$

and equate the coefficients on both sides. We get the following system of polynomial equations.

$$\begin{cases} e_2 + f_2 & = & 0 \\ e_2f_2 + e_1 + f_1 & = & 2a(j) \\ e_1f_2 + e_2\,f_1 & = & 4b(j) \\ e_1f_1 & = & \frac{-a(j)^2}{3} \end{cases}$$

We replace f_2 by $-e_2$ to get the equivalent system,

$$\begin{cases} -{e_2}^2 + e_1 + f_1 & = & 2a(j) \\ -e_1e_2 + e_2\,f_1 & = & 4b(j) \\ e_1f_1 & = & \frac{-a(j)^2}{3} \end{cases}$$

We then replace f_1 by $2a(j) + e_2^2 - e_1$ to get the following non-equivalent system,

$$\begin{cases} -e_1e_2 + e_2(2a(j) + e_2^2 - e_1) & = & 4b(j) \\ e_1(2a(j) + e_2^2 - e_1) & = & \frac{-a(j)^2}{3} \end{cases}$$

Finally, we eliminate e_1 by computing the resultant of two equations. Let $\mathcal{C}_6$ be the curve defined by this resultant. We have,

$$\begin{aligned} \mathcal{C}_6 &= 3\,x^6 + 12a(j)x^4 + 16a(j)^2x^2 - 48b(j)^2 \\ &= 3x^6 - 36(j-1728)jx^4 + 144\,(j-1728)^2j^2x^2 - 192(j-1728)^4j^2 \end{aligned}$$

We find the genus of $\mathcal{C}_6$ to be 0 and we can parameterize it, by setting,

$$j(t) = -\frac{27\,(t+3)^3(t-1)^3}{t^3}.$$

Even though we lost the equivalence, one can verify explicitly using MAPLE that ψ_3 of a curve with j-invariant $j(t)$ has two irreducible quadratic factors over $\mathbb{Q}(t)$. Thus, for any curve E obtained by a specialization of t, the order of $\mathrm{Gal}(\psi_3)$ is less at most 2.

We have proved the following result.

Theorem 17.6. *Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve with j-invariant j. Let d be the degree of the splitting field of the 3-division polynomial ψ_3. Then,*

1. *if $j = t^3$ for some $t \in \mathbb{Q}$ then $d \leq 8$.*
2. *if $j = -\frac{t^3(t-24)}{t+3}$ for some $t \in \mathbb{Q}$ then $d \leq 6$.*
3. *if $j = -\frac{27\,(t+3)^3(t-1)^3}{t^3}$ for some $t \in \mathbb{Q}$ then $d \leq 4$.*
4. *if $j = -\frac{t(s)^3(t(s)-24)}{t(s)+3}$ where $t(s) = -\frac{3(s^3+216)}{s^3-27}$ for some $s \in \mathbb{Q}$ then $d \leq 2$.*

17.3 Formal resolvent: Montgomery curves

Let $\mathrm{E}_{\mathcal{M},a,b}$ be the Montgomery curve defined by $by^2 = x^3 + ax^2 + x$ over $\mathbb{Q}(a,b)$ from Section 13.1 . We can rewrite it as $\mathrm{E}_{\mathcal{M},a,b} : y^2 = x^3 + bax^2 + b^2x$. The 4-torsion point field of $\mathrm{E}_{\mathcal{M},a,b}$ has degree 16. Let ψ_4 be its 4-division polynomial. We factor ψ_4 over $\mathbb{Q}(a,b)$,

$$\psi_4 = 8\,\underbrace{x(x^2+abx+b^2)}_{\psi_2}\,\underbrace{(x-b)(x+b)(x^4+2abx^3+6b^2x^2+2ab^3x+b^4)}_{\psi_4^{\mathrm{new}}}.$$

We discard two linear factors and denote the irreducible quartic factor $x^4+2abx^3+6b^2x^2+2ab^3x+b^4$ by ψ_4^{new}. We are interested in applying Theorem 16.10 to this quartic factor. Similarly to the previous example, we would like to parameterize $a = a(t), b = b(t)$ which would reduce the size of $\mathrm{Gal}(\psi_4^{\mathrm{new}})$ which would naturally reduce the degree of 4-torsion point field.

Let us first compute the resolvent associated with D_8. Note that the coefficient of x^3 in ψ_4^{new} is not zero so we first transform it by replacing x by $x - \frac{2ab}{4}$ to eliminate the term involving x^3.

We have $\mathrm{Gal}(\psi_4^{\mathrm{new}}) \subset \mathrm{D}_8$, if the resolvent associated with D_8,

$$8x^3 + \left(12a^2b^2 - 48b^2\right)x^2 + \left(6a^4b^4 - 16a^2b^4 - 32b^4\right)x + a^6b^6 + 4a^4b^6 - 80a^2b^6 + 192b^6$$

has a simple root in $\mathbb{Q}(a,b)$. One verifies with MAPLE that $-\frac{1}{2}a^2b^2 + 2b^2$ is indeed a root in $\mathbb{Q}(a,b)$. Furthermore, if $\mathrm{Gal}(\psi_4^{\mathrm{new}})$ is a proper subgroup of D_8 then we have either $\mathrm{Gal}(\psi_4^{\mathrm{new}}) \subset \mathrm{V}_4$ or $\mathrm{Gal}(\psi_4^{\mathrm{new}}) \subset \mathrm{C}_4$. We shall make two cases.

1. We have $\mathrm{Gal}(\psi_4^{\mathrm{new}}) \subset \mathrm{V}_4$ if, and only if, the discriminant $-(a^2-4)$ of ψ_4^{new} is a square. Thus, we consider the plane curve defined by $x^2 + a^2 - 4$. It has genus 0 and can be parameterized by putting

$$a(t) = \frac{4t}{t^2+1}.$$

   Thus $\mathrm{Gal}(\psi_4^{\mathrm{new}}) \subset \mathrm{V}_4$ for $\mathrm{E}_{\mathcal{M},a(t),b}$ over $\mathbb{Q}(t,b)$.

2. We have $\mathrm{Gal}(\psi_4^{\mathrm{new}}) \subset \mathrm{C}_4$ if the resolvent associated with it has a simple root. We compute this resolvent and check that it has an irreducible quadratic and quartic factor. The quadratic factor has discriminant $-\square$ which gives us no parameterization of a and b. The quartic factor has 3 variables x, a and b. We put $b = a$ to eliminate b. The resulting plane curve has genus 0 and can be parameterized by putting

$$a(t) = -\frac{2\left(t^4-4\right)}{t^4+4}.$$

   For the resulting curve $\mathrm{E}_{\mathcal{M},a(t),a(t)}$, $\mathrm{Gal}(\psi_4^{\mathrm{new}}) \subset \mathrm{C}_4$. In fact, for $\mathrm{E}_{\mathcal{M},a(t),a(t)}$, ψ_4^{new} factors into two quadratic factors each of which has discriminant $-\square$. Thus over $\mathbb{Q}(t)(i)$, they both split and $\mathrm{Gal}(\psi_4^{\mathrm{new}}) = \mathbb{Z}/2\mathbb{Z}$.

We summarize this discussion in the following theorem.

Theorem 17.7. *Let $\mathrm{E}_{\mathcal{M},a,b}$ be a rational Montgomery curve defined by $by^2 = x^3+ax^2+x$. Let d be the degree of the splitting field of ψ_4^{new}. Then,*

1. $d \leq 8$
2. *if $a = \frac{4t}{t^2+1}$ for some $t \in \mathbb{Q}$, then $d \leq 4$.*
3. *if $a = b = -\frac{2\left(t^4-4\right)}{t^4+4}$ for some $t \in \mathbb{Q}$, then $d \leq 2$.*

One can ask if the bounds of Theorem 17.6 and Theorem 17.7 are sharp. The answer is negative as we shall see below.

Example 17.8. Consider E defined by $y^2 = x^3 + 21x - 26$ from Ex. 5.9. E has a point of order 3 and we have $\mathbb{Q}(\mathrm{E}[3])$ of degree 2. Consider E′ the quadratic twist of E by 11. Following Def. 2.10, $j(\mathrm{E}) = j(\mathrm{E}')$ i.e. E and E′ have the same j-invariant. But the degree of $\mathbb{Q}(\mathrm{E}'[3])$ is 4. This makes a difference in ECM as the average valuation $\overline{v}_3(\mathrm{E}) = \frac{43}{16}$ whereas $\overline{v}_3(\mathrm{E}') = \frac{55}{32}$.

Thus, to classify ECM-friendly elliptic curves, we need to parameterize the the coefficients of elliptic curves, and not just j-invariants. In other words, following Section 2.2, we need to classify $\mathbb{Q}$-isomorphism classes of elliptic curves.

Efficiency of formal resolvents

In general, using resolvents to solve Mazur's Program B (partially) requires us to compute Galois groups of division polynomials. For an odd prime ℓ, the division polynomial ψ_ℓ has degree $\frac{\ell^2-1}{2}$. The resolvent method gives us tests to check the Galois group of ψ_ℓ in the symmetric group $\mathrm{S}_{\frac{\ell^2-1}{2}}$. By Lemma 9.4, this splitting field has degree at most $\frac{(\ell^2-1)(\ell^2-\ell)}{2}$. Thus the degree of the resolvent we need to compute, which is the index in the symmetric group, as at least of magnitude

$$\frac{\frac{\ell^2-1}{2}!}{\frac{(\ell^2-1)(\ell^2-\ell)}{2}},$$

which increases rapidly with ℓ rendering the computations ineffective.

18 The subfields approach

Let us take a motivating example.

Example 18.1. Let $\mathrm{P} = x^4 + tx^2 + 1$ over $\mathbb{Q}(t)$. One can verify using Theorem 16.10 that $\mathrm{Gal}(\mathrm{P})$ over $\mathbb{Q}(t)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is known that for infinitely many rational specializations of t, the resulting polynomial $\mathrm{P}_0 := \mathrm{P}_{t=t_0}(x) \in \mathbb{Q}[x]$ is irreducible and has the same Galois group.

We are interested in knowing whether for some specializations, this Galois group has smaller size, i.e., in this case of order 2 or of order 1. And if it is the case, whether there are infinitely many such specializations. Put $t = t_0 \in \mathbb{Q}$ and let $\mathrm{P}_0 = x^4 + t_0x^2 + 1$. If $t_0 = -\frac{s^4+1}{s^2}$ then P_0 has a rational root and thus splits completely over $\mathbb{Q}$. Thus infinitely many rational specializations of t result into a smaller Galois group of order 1.

Similarly, considering the discriminant $t_0^2 - 4$ of $x^2 + t_0x + 1$, if $t_0^2 - 4 = \square$ then P_0 factors in two quadratic factors of the same discriminant and the Galois group of its splitting field is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. The curve defined by $t^2-4 = y^2$ has genus 0 and can be parameterized by $t(s) = \frac{s^2+4}{2s}$. So, there are infinitely many rational specializations of t which result into a smaller Galois group of order 2.

Note that specializing at $t = 1$ factors P into two quadratic factors, however, $\frac{s^2+4}{2s} \neq 1$ for any $s \in \mathbb{Q}$. Are there infinitely many such cases?

In order to answer this question, we compute the subfields of splitting field of P. These computations can be done using MAGMA or MAPLE which use algorithms from [Klü02], [VHKN13]. We obtain three quadratic subfields defined by $x^2 - (t^2 - 4), x^2 - (t + 2)$ and $x^2 - (t - 2)$. The plane curves defined by these polynomials are all of genus 0 and admit infinitely many rational points. And these are all possible specializations of t yielding into a smaller Galois group.

Remark 18.2. *Note that MAGMA computes subfields only over the function fields with one indeterminate. However MAPLE can work with two indeterminates.*

In this section, we give a solution to Mazur's Program B based on the computation of the subfields of a function field. We shall see that it is simple and feasible (For example, level 8 of Montgomery curves).

Let $\mathrm{K} = \mathbb{Q}(a, b)$ (resp. $\mathbb{Q}(t)$) and let E be an elliptic curve over K. Let L be the m-torsion field of E. One first computes a defining polynomial f of L over K. One then computes $\mathrm{G} = \mathrm{Gal}(\mathrm{L}/\mathrm{K})$. For each subgroup H of G, one computes a defining polynomial f_H of the fixed subfield L^H. Let us now consider rational specialization of

pairs (a, b) (resp. t). After specialization, the resulting Galois group $\mathrm{G}_{a,b}$ (resp. G_t) is a subgroup of G.

$$\begin{tikzcd}
\mathrm{L} \arrow[dr, dash, "\mathrm{H}"] \arrow[dd, dash, "\mathrm{G}"'] & \\
& \mathrm{L}^{\mathrm{H}} = \mathrm{K}[\mathrm{X}]/f_{\mathrm{H}} \\
\mathrm{K} \arrow[ur, dash] &
\end{tikzcd}$$

The pairs $(a, b) \in \mathbb{Q}^2$ such that $\mathrm{G}_{a,b} \subset \mathrm{H}$ are such that $\exists\, r \in \mathrm{K},\ f_{\mathrm{H}}(a, b, r) = 0$. (resp. the parameters $t \in \mathbb{Q}$ for which $\mathrm{G}_t \subset \mathrm{H}$ are such that $\exists\, r \in \mathrm{K},\ f_{\mathrm{H}}(t, r) = 0$.)

Let us illustrate this method with the following example.

18.1 The case of twisted Edwards' curves

We consider a subfamily of twisted Edwards' curves from Section 3.4.1 of [BBB+13] defined by $\mathrm{E}_{\mathcal{E},a,d} : ax^2 + y^2 = 1 + dx^2y^2$ given by $a = -1$ and $d = -e^4$ over $\mathbb{Q}(e)$. We set $\mathrm{L} = \mathbb{Q}(e)(\mathrm{E}_{\mathcal{E},,-1}{-e^4}[8])$. Using MAPLE, we obtain that $[\mathrm{L} : \mathbb{Q}(e)] = 32$. We are interested in finding all subfamilies of $\mathrm{E}_{\mathcal{E},-1,-e^4}$ i.e. all parameterizations $e = e(t)$ for which the degree of L is less than 32. By the existence of Weil pairing (Cor. 3.9), $\mathbb{Q}(\zeta_8) \subset \mathrm{L}$. Thus to simplify the computations, we proceed in two steps: first we compute equations for the subfields containing $\mathrm{K} = \mathbb{Q}(\zeta_8) = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$ and then we consider arbitrary subfields. Using MAPLE's implementation of an algorithm in [VHKN13], we compute the quadratic subfields between K and L as shown in the following diagram.

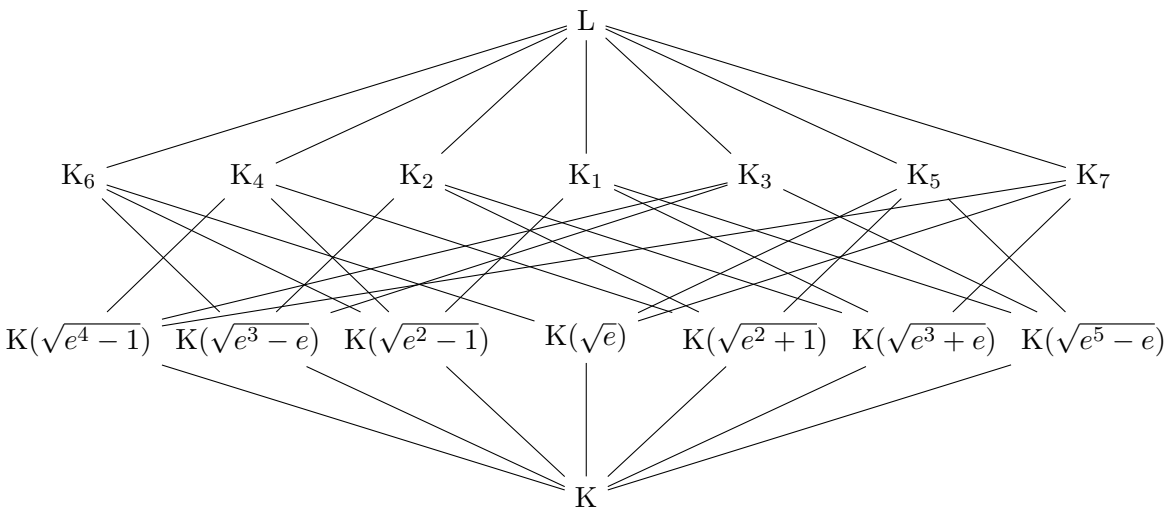


Figure 18.1: Subfields of $\mathrm{L} = \mathbb{Q}(e)(\mathrm{E}_e[8])$ over $\mathrm{K} = \mathbb{Q}(\zeta_8)(e)$ where $\mathrm{E}_e : y^2 - x^2 = 1 - e^4x^2y^2$. The fields $\mathrm{K}_1, \ldots \mathrm{K}_7$ are the compositums of pairs of quadratic fields.

We then consider the curves $\mathcal{C}$ that define these quadratic subfields. For each of them, we note the genus of the associated plane curve. One of the curves has genus 2 so there are only finitely many points. For the curves with genus 1, we compute their

Weierstrass forms. However, using MAGMA, we see that all genus 1 curves have rank 0 so the corresponding families are finite. We summarize it in the table below.

defining polynomial of $\mathcal{C}$	genus	$\#\mathcal{C}(\mathbb{Q}(\zeta_8))$ is infinite ?
$x^2 - e$	0	yes
$x^2 - (e^2 + 1)$	0	yes
$x^2 - (e^2 - 1)$	0	yes
$x^2 - (e^4 - 1)$	1	no
$x^2 - (e^3 + e)$	1	no
$x^2 - (e^3 - e)$	1	no
$x^2 - (e^5 - e)$	2	no

We are thus left with three curves of genus 0. For each curve, we start by finding a parameterization, then by computing the subfamilies.

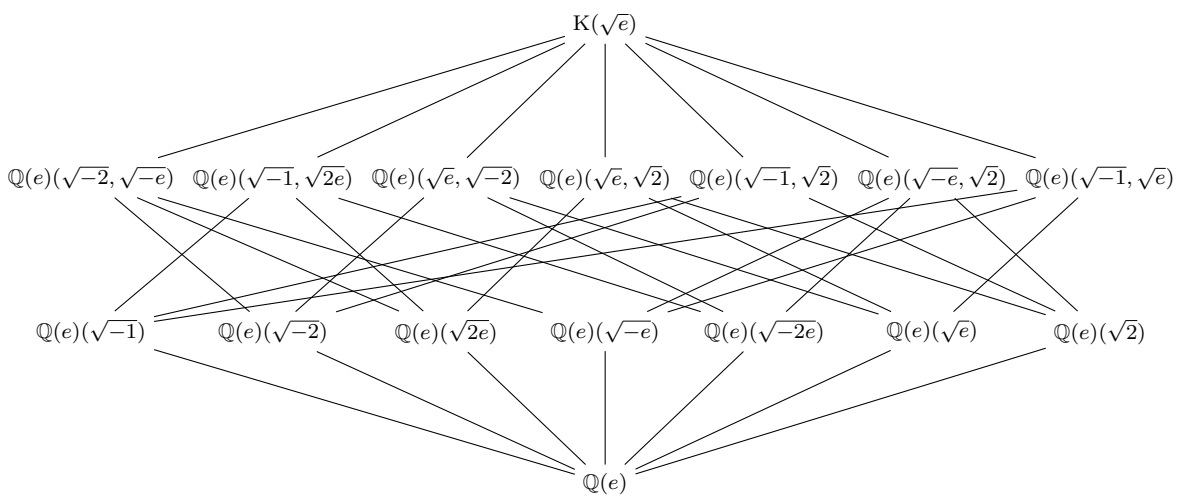
1. We parameterize the curve of equation $x^2 - e = 0$ by $e(t) = t^2$. The fields of above $\mathbb{Q}(\sqrt{e})$ are defined by the relative polynomials $x^2 - (t^4 + 1)$, $x^2 - (t^4 - 1)$ and $x^2 - (t^8 - 1)$. The first two define elliptic curves with rank 0 and the last one has genus 3.

2. We parameterize the curve of equation $x^2 - (e^2 + 1) = 0$ by $e(t) = \frac{t^2-1}{2t}$. The fields of above $\mathbb{Q}(\sqrt{e^2 + 1})$ are defined by the relative polynomials $x^2 - t(t^2 + 1)$, $x^2 - (t^4 + 6t^2 + 1)$ and $x^2 - t(t^2 + 1)(t^4 + 6t^2 + 1)$. Once again, the first two define elliptic curves of rank 0 and the last one has genus 3.

3. We parameterize the curve of equation $x^2 - (e^2 - 1) = 0$ by $e(t) = \frac{t^2+1}{2t}$. The fields of above $\mathbb{Q}(\sqrt{e^2 - 1})$ are defined by the relative polynomials $x^2 - t(t^2 - 1)$, $x^2 - (t^4 - 6t^2 + 1)$ and $x^2 - t(t^2 - 1)(t^4 - 6t^2 + 1)$. Here too, the first two define elliptic curves of rank 0 and the last one has genus 3.

We deduce that the only fields between K and L corresponding to families are $\mathrm{K}(\sqrt{e})$, $\mathrm{K}(\sqrt{e^2 + 1})$ and $\mathrm{K}(\sqrt{e^2 - 1})$.

Thus if a field F between $\mathbb{Q}(e)$ and L correspond to a rational family then the field $\langle \mathrm{F}, \mathrm{K} \rangle$ also correspond to a rational family. So, in order to compute the families defined over $\mathbb{Q}(e)$, we consider the subfields of $\mathrm{K}(\sqrt{e})$, $\mathrm{K}(\sqrt{e^2 + 1})$ and $\mathrm{K}(\sqrt{e^2 - 1})$. For the first one, we consider the subfield between $\mathbb{Q}(e)$ and $\mathrm{K}(\sqrt{e})$), as represented in the following subfields diagram.



Three of the defining polynomials of the quadratic subfields in the diagram correspond to curves with no rational points and the others are parameterized by $e = t^2$, $e = -t^2$, $e = 2t^2$ and $e = -2t^2$. As the degree of e in $\mathrm{E}_{\mathcal{E},-1,-e^4}$ is even, there is only one family for $e = t^2$ and $e = -t^2$. Thus in this case, we have 2 distinct subfamilies. We need not consider the fields of degree 4 because they contain at least one of $\sqrt{-1}$, $\sqrt{-2}$ and $\sqrt{2}$ which lead to polynomials systems without rational solutions.

Similarly, for the fields $\mathrm{K}(\sqrt{e^2+1})$ and $\mathrm{K}(\sqrt{e^2-1})$, each gives 2 subfamilies given by $e^2+1 = t^2$, $e^2+1 = 2t^2$ and $e^2-1 = t^2$, $e^2-1 = 2t^2$. We summarize this discussion below.

Proposition 18.3. *There are exactly* 6 *rational subfamilies of the family* $\mathrm{E}_{\mathcal{E},-1,-e^4}$.

Out of these families, four were presented in [BBB+13] and the two described by $2(e^2 \pm 1) = t^2$ are new.

Chapter 5

Modular Curves

We saw that solving Mazur's program B for $\mathrm{K} = \mathbb{Q}$ would yield a complete classification of ECM friendly rational elliptic curves in the sense of Corollary 14.5. Shimura proved that such curves lie on a modular curve. More precisely, given a subgroup $\mathrm{H} \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$ with some technical hypothesis, the set of elliptic curves E such that $\rho(\mathrm{E}) \subset \mathrm{H}$ up to conjugacy is characterised by the modular curve X_{H}. Recent progress on the Diophantine equations made it possible to give a complete list of possible Galois images and to find explicit models.

In this chapter, we first consider elliptic curves over the field $\mathbb{C}$ of complex numbers and recall a few classical results. We then define modular curves and describe their moduli interpretation. For further details, the reader can refer to [LR11, Sil08, Sil13, DS05, Shi71].

19 Elliptic curves over $\mathbb{C}$

Definition 19.1. A lattice Λ is an additive discrete subgroup of $\mathbb{C}$ containing a $\mathbb{R}$-basis of $\mathbb{C}$.

Given two non-zero complex numbers $z_1 = s_1 + t_1 i$ and $z_2 = s_2 + t_2 i$ such that the vectors (s_1, t_1) and $(s_2, t_2) \in \mathbb{R}^2$ are linearly independent, one can construct the lattice $\langle z_1, z_2 \rangle$ generated by them,

$$\langle z_1, z_2 \rangle := z_1\mathbb{Z} + z_2\mathbb{Z} = \{az_1 + bz_2 \mid a, b \in \mathbb{Z}\}.$$

Although $\langle z_1, z_2 \rangle = \langle z_2, z_1 \rangle$, we sometimes consider a "positively oriented" basis i.e. we require that the imaginary part $\mathrm{Im}(z_1/z_2)$ of z_1/z_2 be positive. The set $\mathbb{H}$ of complex numbers with positive imaginary part plays an important role in the theory of modular curves and is often referred to as *Poincaré half plane*.

Example 19.2. $\mathbb{Z}[i]$ is a lattice in $\mathbb{C}$ generated by $\langle i, 1 \rangle$. On the other hand, $\mathbb{Q}[i]$ is not a lattice even though it is an additive subgroup containing a $\mathbb{R}$-basis of $\mathbb{C}$, because it is not discrete.

Remark 19.3. *It can be shown ([LR11, Cor. 3.1.7 and the discussion thereafter]) that any lattice admits a basis of the form $\langle \tau, 1 \rangle$ with $\tau \in \mathbb{H}$ and two lattices $\langle \tau_1, 1 \rangle$ and $\langle \tau_2, 1 \rangle$ are isomorphic if, and only if, there exists $\mathrm{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tau_1 = \mathrm{M} \cdot \tau_2 := \frac{a\tau_2 + b}{c\tau_2 + d}$. This is called a* fractional linear transformation.

Definition 19.4. An *elliptic function* relative to a lattice Λ is a meromorphic function f on $\mathbb{C}$ invariant under Λ i.e.

$$f(z+w) = f(z) \text{ for all } \ (z,w) \in \mathbb{C} \times \Lambda.$$

As an elliptic function is invariant under Λ, it induces a function on the quotient $\mathbb{C}/\Lambda$. The set $\mathbb{C}(\Lambda)$ of all such functions forms a field. The quotient of $\mathbb{C}$ by a lattice can be described using the fundamental parallelogram of a lattice.

Definition 19.5. A *fundamental parallelogram* for $\Lambda = \langle z_1, z_2 \rangle$ is the set

$$\mathrm{D}_\Lambda := \{sz_1 + tz_2 \mid s,t \in [0,1)\}.$$

As an elliptic function is Λ invariant, its values on D_Λ determine its values over the entire complex plane. Let us now consider an example of an elliptic function.

Definition 19.6. The *Weierstrass $\wp$-function* relative to a lattice Λ is defined by the series

$$\wp(z;\Lambda) = \frac{1}{z^2} + \sum_{0 \neq w \in \Lambda} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right).$$

The series defining $\wp(z;\Lambda)$ is normally convergent over compact subsets of $\mathbb{C}$ not intersecting with Λ. It is an even function of z i.e. $\wp(z;\Lambda) = \wp(-z;\Lambda)$. Let $\wp'(z;\Lambda)$ be the derivative of $\wp(z;\Lambda)$. We have,

$$\wp'(z;\Lambda) = -2 \sum_{w \in \Lambda} \frac{1}{(z-w)^3}.$$

$\wp'(z;\Lambda)$ is an odd function of z i.e. $\wp'(-z;\Lambda) = -\wp'(z;\Lambda)$. It can be shown that $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ are elliptic function relative to Λ ([Sil08, Theorem VI.3.1]) and the field $\mathbb{C}(\Lambda)$ of elliptic functions relative to Λ is generated by $\wp(z;\Lambda)$ and $\wp'(z;\Lambda)$ ([Sil08, Theorem VI.3.2]). The Laurent series expansion of $\wp(z)$ at $z = 0$ is given using the Eisenstein series.

Definition 19.7. Let $k > 1$. The *Eisenstein series of weight* $2k$ relative to Λ is defined by the series

$$\mathrm{G}_{2k}(\Lambda) = \sum_{0 \neq w \in \Lambda} w^{-2k}.$$

The series defining $\mathrm{G}_{2k}(\Lambda)$ is absolutely convergent ([Sil08, Theorem VI.3.1]).

Remark 19.8. *Henceforth, when the lattice Λ is fixed, we omit Λ and write $\wp(z)$, $\wp'(z)$ and G_{2k}, respectively for $\wp(z;\Lambda)$, $\wp'(z;\Lambda)$ and $\mathrm{G}_{2k}(\Lambda)$.*

Theorem 19.9 ([Sil08, Theorem VI.3.5])**.** *Let $\Lambda \subset \mathbb{C}$ be a lattice.*

1. *The Laurent series for $\wp(z)$ at $z = 0$ is*

$$\wp(z) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)\mathrm{G}_{2k+2} z^{2k}.$$

2. *Let $\wp'$ be the derivative of $\wp$. Then, for all $z \in \mathbb{C} \setminus \Lambda$,*

$$\left(\frac{\wp'(z)}{2} \right)^2 = \wp(z)^3 - 15\mathrm{G}_4 \wp(z) - 35\mathrm{G}_6.$$

It can be shown ([Sil08, Prop. VI.3.6]) that the polynomial $x^3 - 15\mathrm{G}_4 x - 35\mathrm{G}_6$ has simple roots. Thus the curve $\mathrm{E}_\Lambda : y^2 = x^3 - 15\mathrm{G}_4(\Lambda)x - 35\mathrm{G}_6(\Lambda)$ defines a complex elliptic curve depending on the underlying lattice Λ. The second point of the above theorem means that $\left(\wp(z), \frac{\wp'(z)}{2}\right)$ is a point on E_Λ.

Remark 19.10. *It is customary to write* E_Λ *as* $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ *where*

$$g_2(\Lambda) = 60\mathrm{G}_4(\Lambda) \text{ and } g_3(\Lambda) = 140\mathrm{G}_6(\Lambda).$$

The j-invariant $j(\Lambda)$ of E_Λ is called the *modular j-invariant* and is equal to

$$j(\Lambda) = 1728\frac{20\mathrm{G}_4^3}{20\mathrm{G}_4^3 - 49\mathrm{G}_6^2} = 1728\frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27g_3(\Lambda)^2}.$$

And the discriminant $\Delta(\Lambda)$ of E_Λ is equal to

$$\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2.$$

By Theorem 19.9, every lattice in $\mathbb{C}$ gives rise to an elliptic curve and furthermore one can show that every complex elliptic curve comes from a lattice. It is the so called *uniformisation theorem* ([Sil08, Theorem VI.5.1]).

Example 19.11. Given an elliptic curve E, one can compute the corresponding lattice Λ, the series defining $\wp(z)$ at $z = 0$ using SAGE.

```
sage: E = EllipticCurve([3,5])
sage: L = E.period_lattice().basis()
sage: L
(2.85801308761229, 1.42900654380614 + 1.01215590531558*I)
sage: w = E.weierstrass_p()
sage: w1 = w.derivative()
sage: (w1/2)^2-(w^3+3*w+5)
O(z^16)
```

The last command verifies that $\left(\wp(z), \frac{\wp'(z)}{2}\right)$ is indeed a point on E. If $\Lambda =< \tau, 1 >$ then the value of $j(\tau) := j(\Lambda)$ can be computed using SAGE.

```
sage: elliptic_j(CC(I))
1728.00000000000
sage: elliptic_j(sqrt(-2))
7999.99999999999 - 3.91764589529391e-12*I
```

The exact values of $j(i)$ and $j(\sqrt{2}i)$ are 1728 and 8000 respectively.

19.1 Correspondence between $\mathbb{C}/\Lambda$ and E_Λ

Let us discuss the correspondence between a complex lattice Λ and the complex elliptic curve E_Λ associated to it. Fix a basis (w_1, w_2) of Λ.

1. The natural group structure of $\mathbb{C}/\Lambda$ is transferred to E via the map $(\wp, \wp')$ which makes E an abelian group. It is the same group structure as the one defined in Section 2.1.

2. Let us consider $[m]$ the multiplication by m map over E. There exists the corresponding map, which we again denote by $[m]$, over $\mathbb{C}/\Lambda$. Thus the points of $\mathrm{E}[m]$ correspond to the following set.

$$\begin{aligned}\{z \in \mathbb{C}/\Lambda \,|\, mz \in \Lambda\} &= \{z \in \mathbb{C}/\Lambda \,|\, \exists\, a, b \in \mathbb{Z} \text{ such that } mz = aw_1 + bw_2\} \\ &= \left\langle \frac{w_1}{m} \mod \Lambda, \frac{w_2}{m} \mod \Lambda \right\rangle\end{aligned}$$

In other words, the points of $\mathrm{E}[m]$ correspond to the *superlattice* of Λ defined by the basis $\left(\frac{w_1}{m}, \frac{w_2}{m}\right)$.

Clearly, two isomorphic lattices give isomorphic complex elliptic curves. By Proposition 2.2, two complex elliptic curves are isomorphic if, and only if, they have the same j-invariant.

20 Modular curves

Roughly speaking, modular curves characterize elliptic curves with extra torsion related data. We follow [DS05, p. 38] and call such elliptic curves *enhanced elliptic curves*. Recall that we are interested in modular curves as they pave a way to solve Mazur's program B.

Example 20.1. Let E be a complex elliptic curve. Let C be a finite cyclic subgroup of E then the pair (E, C) is an enhanced elliptic curve. If P and Q generate $\mathrm{E}[n]$ for some n then the pair $(\mathrm{E}, (\mathrm{P}, \mathrm{Q}))$ is also an enhanced elliptic curve.

We shall later see in Theorem 20.8 that such enhanced elliptic curves are classified by suitable modular curves. Simply put, a modular curve is the upper half complex plane $\mathbb{H}$ quotiented by a well-chosen subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We start by describing the simplest among them.

20.1 Modular curve X(1)

Let τ_1, $\tau_2 \in \mathbb{H}$. We mentioned in Remark 19.3 that two lattices $\langle \tau_1, 1\rangle$ and $\langle \tau_2, 1\rangle$ are isomorphic if, and only if, τ_1 is a fractional linear transformation of τ_2 by an element of $\mathrm{SL}_2(\mathbb{Z})$. This suggests considering the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ by fractional linear transformations. Under this action, $z_1, z_2 \in \mathbb{H}$ are equivalent if, and only if, there exists $\mathrm{M} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $z_1 = \mathrm{M} \cdot z_2 := \frac{az_2+b}{cz_2+d}$. As $-\mathrm{I} = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ acts trivially over $\mathbb{H}$, we consider the action of $\mathrm{SL}_2(\mathbb{Z})/\{\pm\mathrm{I}\}$ over $\mathbb{H}$. The group $\mathrm{SL}_2(\mathbb{Z})/\{\pm\mathrm{I}\}$ is called the *modular group* and is denoted by $\Gamma(1)$. It is generated ([Sil08, Prop. C.12.1]) by the following two matrices,

$$\mathrm{S} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \quad \text{and} \quad \mathrm{T} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right).$$

In practice, we consider the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$ while keeping in mind that $-\mathrm{I}$ acts as I. We are interested in the orbits of this action.

Theorem 20.2 ([Sil13, Prop. 1.5])**.** *Let $\mathcal{F} \subset \mathbb{H}$ be the following set,*

$$\mathcal{F} = \{z \in \mathbb{H} \mid |z| \geq 1 \text{ and } |\Re(z)| \leq \frac{1}{2}\}.$$

Then,

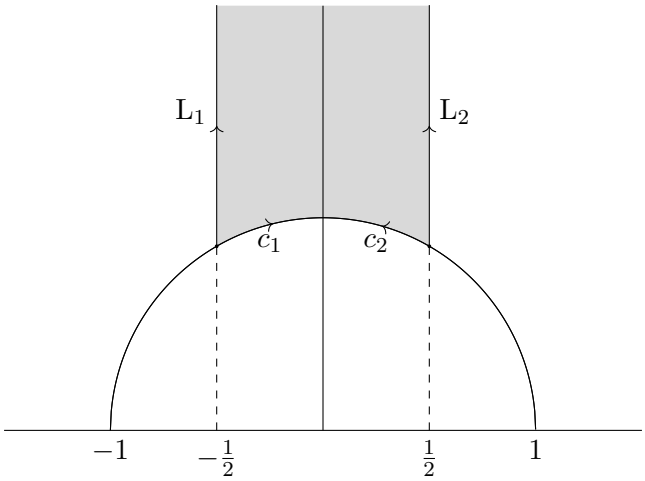


Figure 20.1: Fundamental domain of $\mathbb{H}/\Gamma_1$

1. *for every $z \in \mathbb{H}$, there is $\gamma \in \Gamma(1)$ such that $\gamma \cdot z \in \mathcal{F}$.*

2. *for all z in the interior of $\mathcal{F}$, the action of $\Gamma(1)$ is faithful.*

Consider Figure 20.1 depicting $\mathcal{F}$. Let us see how $\Gamma(1)$ acts on the boundary of $\mathcal{F}$. Clearly $\mathrm{T} \cdot \mathrm{L}_1 = \mathrm{L}_2$ and $\mathrm{T}^{-1} \cdot \mathrm{L}_2 = \mathrm{L}_1$. On the other hand, S fixes i and sends $x + iy$ from the arc c_1 to $-x + iy$ to the arc c_2. Thus under the action of $\Gamma(1)$, we identify L_1 and L_2 and c_1 and c_2. Let us call the resulting object $\mathrm{Y}(1)$. Topologically, $\mathrm{Y}(1)$ is the complex plane and lacks a point to be compact. One compactifies $\mathrm{Y}(1)$ by considering the action of $\Gamma(1)$ on the extended upper half plane $\mathbb{H}^*$. We put

$$\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}.$$

The points of $\mathbb{P}^1(\mathbb{Q})$ are called the *cusps* of $\mathbb{H}^*$. An element of $\Gamma(1)$ acts in the same way on a rational number as on a complex number. For ∞, we put *formally*

$$\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot \infty := \frac{a}{c}.$$

One can verify that under the action of $\Gamma(1)$, $\mathbb{P}^1(\mathbb{Q})$ forms a single orbit ([LR11, Prop. 3.4.3]). Adding this point to $\mathrm{Y}(1)$, we get a compact topological object called the *modular curve* $\mathrm{X}(1)$. We call $\mathrm{Y}(1)$ the *affine part* of $\mathrm{X}(1)$.

What does $\mathrm{X}(1)$ classify?

Recall that isomorphic lattices give isomorphic complex elliptic curves and isomorphic complex elliptic curves have the same j-invariant. On the other hand, every lattice admits a basis of the form $(\tau, 1)$ where $\tau \in \mathbb{H}$. Thus we have the following bijections.

$$\begin{array}{ccccc} \mathrm{Y}(1) & \longleftrightarrow & \mathbb{H}/\mathrm{SL}_2(\mathbb{Z}) & \longleftrightarrow & \{\text{Isomorphic complex lattices}\} \\ & & & & \updownarrow \\ \mathbb{C} & \longleftrightarrow & \{j \in \mathbb{C}\} & \longleftrightarrow & \{\text{Isomoprhic complex elliptic curves}\} \end{array}$$

Thus each point of the affine part $\mathrm{Y}(1)$ corresponds to the j-invariant of a complex elliptic curve. We associate to the point $\tau \in \mathrm{Y}(1)$, the complex elliptic curve associated to the lattice $\langle \tau, 1 \rangle$. More precisely, we have the following.

Theorem 20.3 ([Sil13, Theorem 4.1])**.** *There exists an isomorphism j of projective curves*

$$j\colon \mathrm{X}(1) \xrightarrow{\sim} \mathbb{P}^1(\mathbb{C}).$$

Remark 20.4. *Recall that* $\mathrm{X}(1)$ *has only one cusp. For example, choose* $x = 1 = [1,1] \in \mathbb{P}^1(\mathbb{Q})$ *as a representative of the orbit of* $\mathbb{P}^1(\mathbb{Q})$*. Then,*

$$\mathbb{C}/(\mathbb{Z} + x\mathbb{Z}) = \mathbb{C}/\mathbb{Z}.$$

Topologically, it is a cylinder. It is an elliptic curve minus a point. In general, the cusps on a modular curve do not characterize elliptic curves and thus we do not concern ourselves with it. The reader can find more details in [Sil13] or [DR73].

In this section, we presented a *very* brief description of the modular curve $\mathrm{X}(1)$. The reader can find more details in [Sil08, Section C.12], [LR11, Chapter 3] and [Shi71, Chapter 1].

20.2 Modular curves $\mathrm{X}(\mathrm{N})$, $\mathrm{X}_0(\mathrm{N})$ and $\mathrm{X}_1(\mathrm{N})$

We saw that $\mathbb{H}^*/\Gamma(1)$ classifies isomorphism classes of complex elliptic curves thus all complex j-invariants. One can restate it, albeit redundantly, by saying $\mathrm{X}(1)$ characterizes elliptic curves with a point of order 1. This interpretation is consistent with what follows.

Similar to the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$, one can consider the action of a congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{H}$. We denote the resulting curve by $\mathrm{Y}(\Gamma)$ and it can be compactified by extending the action of Γ to $\mathbb{H}^*$. We note the resulting curve $\mathrm{X}(\Gamma)$.

Congruence subgroups

Definition 20.5. Let $\mathrm{N} > 0$ be an integer. The *principle congruence subgroup* $\Gamma(\mathrm{N})$ of *level* N is the following subgroup of $\mathrm{SL}_2(\mathbb{Z})$,

$$\Gamma(\mathrm{N}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \bmod \mathrm{N} \right\}.$$

With this definition in mind, one can denote $\mathrm{SL}_2(\mathbb{Z})$ by $\Gamma(1)$ while keeping in mind that $-\mathrm{I}$ and I act the same over $\mathbb{H}$. As $\Gamma(\mathrm{N})$ is the kernel of the reduction modulo N map from $\mathrm{SL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$, it is normal in $\mathrm{SL}_2(\mathbb{Z})$. Since this map is surjective ([DS05, Ex. 1.2.2]), it induces the following isomorphism of groups.

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(\mathrm{N}) \cong \mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z}).$$

We now define arbitrary congruence subgroups.

Definition 20.6. Let Γ be a subgroup of $\mathrm{SL}_2(\mathbb{Z})$. We say Γ is a *congruence subgroup* if $\Gamma(\mathrm{N}) \subset \Gamma$ for some N. The level of Γ is the smallest such N.

Apart from $\Gamma(\mathrm{N})$, there are two other important congruence subgroups.

$$\Gamma_0(\mathrm{N}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \bmod \mathrm{N} \right\}$$

and

$$\Gamma_1(\mathrm{N}) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \bmod \mathrm{N} \right\}.$$

We have the following inclusions of groups.

$$\Gamma(\mathrm{N}) \subset \Gamma_1(\mathrm{N}) \subset \Gamma_0(\mathrm{N}) \subset \Gamma(1).$$

Similar to the previous section, we consider the actions of $\Gamma(\mathrm{N})$, $\Gamma_0(\mathrm{N})$ and $\Gamma_1(\mathrm{N})$ over $\mathbb{H}$. Let us call the resulting curves $\mathrm{Y}(\mathrm{N}), \mathrm{Y}_0(\mathrm{N})$ and $\mathrm{Y}_1(\mathrm{N})$ respectively. One compactifies them by extending the action of corresponding congruence subgroup to $\mathbb{H}^*$, equivalently, by adding the representatives of the orbits of cusps $\mathbb{P}^1(\mathbb{Q})$. We denote the resulting curves by $\mathrm{X}(\mathrm{N}), \mathrm{X}_0(\mathrm{N})$ and $\mathrm{X}_1(\mathrm{N})$ respectively.

Example 20.7. One can construct $\Gamma(\mathrm{N})$, $\Gamma_0(\mathrm{N})$ and $\Gamma_1(\mathrm{N})$ with SAGE.

```
sage: G = Gamma(3); G0 = Gamma0(3); G1 = Gamma1(3)
sage: G.generators()
[
[1 3]  [-8  3]  [ 4 -3]
[0 1], [-3  1], [ 3 -2]
]
sage: G.cusps()
[0, 1, 2, Infinity]
sage: G.index()
24
sage: G0.generators()
[
[1 1]  [-1  1]
[0 1], [-3  2]
]
sage: G0.cusps()
[0, Infinity]
sage: G0.index()
4
sage: G1.generators()
[
[1 1]  [ 1 -1]
[0 1], [ 3 -2]
]
sage: G1.cusps()
[0, Infinity]
sage: G1.index()
8
```

What do $\mathrm{X}(\mathrm{N})$, $\mathrm{X}_0(\mathrm{N})$ and $\mathrm{X}_1(\mathrm{N})$ classify?

Considering Remark 20.4, we ignore the cusps. So let us see what $\mathrm{Y}_1(\mathrm{N})$ classifies. Let $\tau \in \mathrm{Y}_1(\mathrm{N}) = \mathbb{H}/\Gamma_1(\mathrm{N})$ and $\Lambda = \langle \tau, 1 \rangle$. Let E_τ be the elliptic curve associated to Λ. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $\tau' = \gamma \cdot \tau = \frac{a\tau+b}{c\tau+d}$. Let $\Lambda' = \langle \tau', 1 \rangle$ and $\mathrm{E}_{\tau'}$ be the elliptic curve associated to the lattice $\langle \gamma \cdot \tau, 1 \rangle$.

Consider the following homomorphism of additive groups,

$$\begin{array}{rccc} f\colon & \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\Lambda' \\ & z & \mapsto & \frac{z}{c\tau+d} \end{array}$$

One can verify that the above map is well defined. Considering Remark 19.3, f is actually an isomorphism. Thus, E_τ and $\mathrm{E}_{\gamma\cdot\tau}$ are isomorphic complex elliptic curves.

Let $\mathrm{P}_\tau \in \mathrm{E}_\tau$ be associated to $\frac{1}{\mathrm{N}} \in \mathbb{C}/\Lambda$. Recall that P_τ can be obtained via Weierstrass $\wp$-function and its derivative (Theorem 19.9). One can see that $\mathrm{P}_\tau \in \mathrm{E}_\tau[\mathrm{N}]$ and is of order N. Under f, $\frac{1}{\mathrm{N}}$ gets mapped to $\frac{1}{\mathrm{N}(c\tau+d)}$. Consider the following difference.

$$\begin{aligned}\frac{1}{\mathrm{N}} - \frac{1}{\mathrm{N}(c\tau+d)} &= \frac{(c\tau+d)-1}{\mathrm{N}(c\tau+d)} \\ &= \frac{\frac{c}{\mathrm{N}}\tau + \frac{d-1}{\mathrm{N}}}{c\tau+d}\end{aligned}$$

If $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ belongs to $\Gamma_1(\mathrm{N})$, then by definition,

$$c \equiv 0 \bmod \mathrm{N} \text{ and } d \equiv 1 \bmod \mathrm{N}.$$

In particular, $\frac{c}{\mathrm{N}}$ and $\frac{d-1}{\mathrm{N}} \in \mathbb{Z}$ and thus

$$\frac{1}{\mathrm{N}} - \frac{1}{\mathrm{N}(c\tau+d)} \in f(\Lambda) = \Lambda'.$$

In other words, $\frac{1}{\mathrm{N}}$ is invariant under the base change of Λ induced by an element of $\Gamma_1(\mathrm{N})$. So each $\tau \in \mathrm{Y}_1(\mathrm{N})$ not only gives an elliptic curve E_τ but also specifies a point $\mathrm{P}_\tau \in \mathrm{E}_\tau$ of exact order N. Furthermore, for any elliptic curve E and a point $\mathrm{P} \in \mathrm{E}$ of order N, there exists $\tau \in \mathrm{Y}_1(\mathrm{N})$ such that the isomorphism from E_τ to E sends P_τ to P. We define an equivalence relation $\sim$ on the set of pairs (E, P) where E is a complex elliptic curve and $\mathrm{P} \in \mathrm{E}$ is a point of exact order N:

$$(\mathrm{E}, \mathrm{P}) \sim (\mathrm{E}', \mathrm{P}') \text{ if, and only if, } \exists \text{ isomorphism } \phi\colon \mathrm{E} \longrightarrow \mathrm{E}' \text{ such that } \phi(\mathrm{P}) = \mathrm{P}'.$$

Put $[\mathrm{E}, \mathrm{P}]$ for the equivalence class. Equipped with this, we can say that Y_1 characterizes the equivalence classes of enhanced elliptic curves (E, P) where $\mathrm{P} \in \mathrm{E}$ is a point of order N. Following the terminology of [DS05, Section 1.5], we say that the set

$$\mathrm{S}_1(\mathrm{N}) := \{[\mathrm{E}, \mathrm{P}] \mid \mathrm{E} \text{ a complex elliptic curve and } \mathrm{P} \in \mathrm{E} \text{ of order } \mathrm{N}\}$$

is a *moduli space* for $\Gamma_1(\mathrm{N})$. Following [Sil08, Section C.13], one can say $\mathrm{Y}_1(\mathrm{N})$ is a *moduli space* for the *moduli problem* of determining the set $\mathrm{S}_1(\mathrm{N})$.

It turns out that, even $\mathrm{Y}_0(\mathrm{N})$ and $\mathrm{Y}(\mathrm{N})$ also appear as moduli spaces of isomorphism classes of enhanced elliptic curves.

Theorem 20.8 ([Sil08, Theorem 13.1], [DS05, Theorem 1.5.1])**.** *Let* $\mathrm{N} > 1$ *be an integer.*

1. *There exists a smooth projective curve* $\mathrm{X}_0(\mathrm{N})$ *defined over* $\mathbb{Q}$ *and a complex analytic isomorphism of curves*

   $$j_{\mathrm{N},0}\colon \mathbb{H}^*/\Gamma_0(\mathrm{N}) \longrightarrow \mathrm{X}_0(\mathrm{N})(\mathbb{C})$$

   such that the following holds:

   Let $\tau \in \mathbb{H}/\Gamma_0(\mathrm{N})$ *and let* $\mathrm{K} = \mathbb{Q}(j_{\mathrm{N},0}(\tau))$*. Then* τ *corresponds to an equivalence class of pairs* (E, C) *where* $\mathrm{C} \subset \mathrm{E}$ *is a cyclic subgroup of order* N *and this equivalence class contains a pair such that* E *is defined over* K *and* $\mathrm{C} \subset \mathrm{E}(\mathrm{K})$*.*

2. *There exists a smooth projective curve* $X_1(N)$ *defined over* $\mathbb{Q}$ *and a complex analytic isomorphism of curves*

$$j_{N,1}\colon \mathbb{H}^*/\Gamma_1(N) \longrightarrow X_1(N)(\mathbb{C})$$

such that the following holds:

Let $\tau \in \mathbb{H}/\Gamma_1(N)$ *and let* $K = \mathbb{Q}(j_{N,1}(\tau))$. *Then* τ *corresponds to an equivalence class of pairs* (E, P) *where* $P \in E$ *is a point of exact order* N *and this equivalence class contains a pair such* E *is defined over* K *and* $P \in E(K)$.

3. *Fix a primitive* N*-th root of unity* $\zeta \in \mathbb{C}$. *There exists a smooth projective curve* $X(N)$ *defined over* $\mathbb{Q}$ *and a complex analytic isomorphism of curves*

$$j_N\colon \mathbb{H}^*/\Gamma(N) \longrightarrow X(N)(\mathbb{C})$$

such that the following holds:

Let $\tau \in \mathbb{H}/\Gamma(N)$ *and let* $K = \mathbb{Q}(\zeta, j_N(\tau))$. *Then* τ *corresponds to an equivalence class of pairs* $(E, (P, Q))$ *where* $P, Q \in E$ *generate* $E[N]$ *and are such that* $e_N(P, Q) = \zeta$ *where* e_N *is the* Weil pairing *(Definition - Theorem 3.1) and this equivalence class contains a pair such* E *is defined over* K *and* $P, Q \in E(K)$.

For arbitrary congruence subgroups Γ, one can consider the curve $Y(\Gamma) := \mathbb{H}/\Gamma$ and $X(\Gamma) := \mathbb{H}^*/\Gamma$. Note that $X(\Gamma)$ is a smooth projective curve and is called the *modular curve* associated to Γ. Our goal is to compute modular curves associated to a congruence subgroup.

Let us end this section by noting that it is possible to compute the genera of modular curves, without explicitly computing their models, see [DS05, Theorem 3.1.1]. In fact, we call the genus of $X(\Gamma)$ the genus of Γ. For classical congruence subgroups, one can compute the genus using SAGE.

```
sage: G = Gamma(3); H = Gamma(7)
sage: G.genus()
0
sage: H.genus()
3
```

21 Modular functions

We continue to follow [Sil08, Appendix C], [DS05]. We shall first define modular functions for $SL_2(\mathbb{Z})$ and then for arbitrary congruence subgroups. Roughly speaking, modular functions are meromorphic functions on a modular curve.

Modular functions for $SL_2(\mathbb{Z})$

Let us consider the case of $\Gamma(1) = SL_2(\mathbb{Z})/\pm I$. We first discuss meromorphic functions on Y_1 and then consider the meromorphicity at the only cusp ∞ of $\Gamma(1)$.

The main ingredient is the q-expansions of $\mathbb{Z}$-periodic functions. Let $\mathcal{D}$ be the open unit disc in the complex plane and let $\mathcal{D}'$ be $\mathcal{D}$ punctured at the origin. Consider the following map,

$$\begin{array}{rccc} q\colon & \mathbb{H} & \longrightarrow & \mathcal{D} \\ & \tau & \mapsto & e^{2\pi i\tau} \end{array}$$

Put $\tau = a + bi$. One can then rewrite

$$\begin{aligned} q(\tau) = e^{2\pi i\tau} &= e^{2\pi i(a+ib)} \\ &= e^{-2\pi b} \cdot (\cos 2\pi a + i \sin 2\pi a) \end{aligned}$$

Clearly, $q(\tau)$ is bounded and

$$\lim_{\mathrm{Im}(\tau)\longrightarrow\infty} q(\tau) = 0.$$

Now consider a $\mathbb{Z}$-periodic meromorphic function $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ i.e. f is meromorphic and $f(\tau+1) = f(\tau)$. Putting q as a variable over $\mathcal{D}'$ then f induces a function $\tilde{f}$ on $\mathcal{D}'$ defined below.

$$\begin{array}{rcl} \tilde{f}\colon \mathcal{D}' & \longrightarrow & \mathbb{C} \\ q & \mapsto & f\left(\frac{\log q}{2\pi i}\right) \end{array}$$

As the complex logarithm is defined up to $2\pi i\mathbb{Z}$, $\tilde{f}$ is well defined. We call the *q-expansion* of f the Laurent series expansion of $\tilde{f}$ at 0 treating q as a variable.

One can write,

$$f(\tau) = \tilde{f}(q(\tau)) = \sum_{n=-\infty}^{\infty} c(n)q^n.$$

Let $g\colon \mathbb{H} \longrightarrow \mathbb{C}$ be a $\mathrm{SL}_2(\mathbb{Z})$-invariant meromorphic function. As $\mathrm{SL}_2(\mathbb{Z})$ is generated by

$$\mathrm{S} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \quad \text{and} \quad \mathrm{T} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right),$$

we have,

$$g(z) = g(\mathrm{T} \cdot z) = g(z+1).$$

So g is $\mathbb{Z}$-invariant and therefore admits a q-expansion. In order to *meromorphically* extend g to X_1, we need to consider the meromorphicity of g at the cusp ∞ of $\Gamma(1)$. Recall that as $\mathrm{Im}(\tau)$ goes to infinity, $q(\tau)$ tends to 0. Thus we say that g is meromorphic at infinity, if $\tilde{g}$ is meromorphic at 0. In this case, the q-expansion of g has only finitely many negatively indexed terms i.e.

$$f(\tau) = \sum_{n=-n_0}^{\infty} c(n)q^n, \text{ for some } n_0 \geq 0 \text{ with } c(n_0) \neq 0.$$

The q-expansion is also called Fourier expansion.

Definition 21.1. A meromorphic function f on $\mathbb{H}$ is called a *modular function of weight k* for $\mathrm{SL}_2(\mathbb{Z})$ if

1. $f(\tau) = (c\tau + d)^{-k} f(\gamma \cdot \tau) = (c\tau + d)^{-k} f\left(\frac{az+b}{cz+d}\right) \ \forall\, \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$.

2. There exists an integer $n_0(f)$ such that the Fourier expansion of f in the variable $q = e^{2\pi i\tau}$ has the form

$$f(\tau) = \sum_{n=n_0(f)}^{\infty} c(n)q^n.$$

Furthermore if f is holomorphic on $\mathbb{H}$ and at ∞, in which case $n_0(f) = 0$, we say that f is a *modular form of weight k*. If furthermore $c(0) = 0$, we say f is a *cusp form*.

The set of modular forms of weight k is denoted by $\mathcal{M}_k(\Gamma(1))$. The coefficients of modular forms can be computed efficiently using [CE11, Chapter 15].

Example 21.2 (Eisenstein series)**.** Let $k > 1$ be an integer. Consider the Eisenstein series G_{2k} defined in Def. 19.7. It can be shown that G_{2k} is a modular form of weight $2k$ for $\mathrm{SL}_2(\mathbb{Z})$ ([DS05, p. 5]).

Example 21.3 (Modular j-invariant)**.** For $\tau \in \mathbb{H}$, consider the lattice $\Lambda = \langle \tau, 1 \rangle$ and the j-invariant

$$j(\Lambda) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}$$

associated to it. Then the following function defines a modular function of weight 0 for $\mathrm{SL}_2(\mathbb{Z})$.

$$\begin{array}{rcl} j\colon \mathbb{H} & \longrightarrow & \mathbb{C} \\ \tau & \mapsto & j(\Lambda) \end{array}$$

Furthermore, every other modular function of weight 0 for $\mathrm{SL}_2(\mathbb{Z})$ is a rational function of $j(\tau)$. See [Sil08, Theorem C.12.8] or [Ser12, Prop. 5]. The modular j-invariant admits the following q-expansion.

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \cdots$$

One sees that the modular j-invariant is not a modular form as $n_0(j) = -1$.

A modular function f of weight 0 for $\mathrm{SL}_2(\mathbb{Z})$ such that f is also meromorphic at ∞ i.e. $\tilde{f}$ is meromorphic at 0 induces a meromorphic function on the modular curve $\mathrm{X}(1)$.

Arbitrary modular functions

Similar to $\mathrm{SL}_2(\mathbb{Z})$, one can consider other congruence subgroups Γ and construct modular functions and forms. Let Γ be a congruence subgroup of level N. Then by definition $\Gamma(\mathrm{N}) \subset \Gamma$. In particular, $\mathrm{T}_\mathrm{N} = \left(\begin{smallmatrix} 1 & \mathrm{N} \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma$. If $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ is a $\mathrm{N}\mathbb{Z}$-periodic meromorphic function then

$$f(\tau) = f(\mathrm{T}_\mathrm{N} \cdot \tau) = f(\tau + \mathrm{N}).$$

Assuming f is also meromorphic at infinity, the q-expansion of f can be written as

$$f(\tau) = \sum_{n=-n_0}^{\infty} c(n) q^{\frac{n}{\mathrm{N}}}, \text{for some integer } n_0.$$

Definition 21.4. Let $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ be a meromorphic function. For $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, we define the function $f\gamma$ as below.

$$\begin{array}{rcl} f\gamma\colon \mathbb{H} & \longrightarrow & \mathbb{C} \\ \tau & \mapsto & f(\gamma \cdot \tau) = f\left(\frac{a\tau+b}{c\tau+d}\right) \end{array}$$

We can now define modular forms of weight k for Γ.

Definition 21.5. Let Γ be a congruence subgroup of level N and k be an integer. A meromorphic function f on $\mathbb{H}$ is called a *modular function of weight* k for Γ if

1. $f(\tau) = (c\tau + d)^{-k} f(\gamma \cdot \tau) = (c\tau + d)^{-k} f\left(\frac{az+b}{cz+d}\right) \ \forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$.

2. There exists an integer $n_0(f)$ such that the Fourier expansion of f in the variable $q = e^{2\pi i\tau}$ has the form
$$f(\tau) = \sum_{n=n_0(f)}^{\infty} c(n) q^{\frac{n}{\mathrm{N}}}.$$
Furthermore if f is holomorphic on $\mathbb{H}$ and if $f\gamma$ is holomorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we say that f is a *modular form of weight* k for Γ. If furthermore $c(0) = 0$ in the q-expansion of $f\gamma$ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, we say f is a *cusp form* for Γ.

The set of modular forms of weight k for Γ is denoted by $\mathcal{M}_k(\Gamma)$ and the set of cusp forms of weight k for Γ is denoted by $\mathcal{S}_k(\Gamma)$.

Note that $\mathcal{M}_k(\Gamma)$ is a vector spaces over C and $\mathcal{S}_k(\Gamma)$ is a subspace.

Definition 21.6. The Eisenstein space of weight k is the quotient
$$\mathcal{E}_k(\Gamma) := \mathcal{M}_k(\Gamma) \big/ \mathcal{S}_k(\Gamma).$$

Example 21.7 ([DS05, Section 4.2])**.** Let $\mathrm{N} > 2$ and $k \geq 3$ be positive integers. Let $(c', d') \in (\mathbb{Z}/\mathrm{N}\mathbb{Z})^2$ of order N. Put
$$\mathcal{I} := \{(c, d) \in \mathbb{Z}^2 \mid (c, d) \equiv (c', d') \bmod \mathrm{N} \text{ and } \gcd(c, d) = 1\}.$$
Define
$$\mathrm{E}_k^{(c',d')}(\tau) = \sum_{(c,d)\in\mathcal{I}} \frac{1}{(c\tau + d)^k}.$$
We call $\mathrm{E}_k^{(c',d')}(\tau)$ the *Eisenstein series of weight k for* $\Gamma(\mathrm{N})$ and it can be shown that $\mathcal{M}_k(\Gamma(\mathrm{N}))$ is spanned by $\mathrm{E}_k^{(c',d')}(\tau)$ as a complex vector space.

Definition 21.8 (Modular function for Γ)**.** Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. A *modular function* $f\colon \mathbb{H} \longrightarrow \mathbb{C}$ for Γ is a modular function of weight 0 for Γ such that f is also meromorphic at the cusps of Γ or equivalently, $f\gamma$ is meromorphic at ∞ for all $\gamma \in \mathrm{SL}_2(\mathbb{Z})$

A modular function f for Γ induces a meromorphic function on the modular curve $\mathrm{X}(\Gamma)$. The set of modular functions for a fixed congruence subgroup Γ forms a field which we denote as $\mathbb{C}(\Gamma)$. This is a transcendental extension of $\mathbb{C}$. If Γ' is another congruence subgroup contained in Γ then a modular function for Γ is also a modular function for Γ'. In other words, we have,
$$\Gamma' \subset \Gamma \implies \mathbb{C}(\Gamma) \subset \mathbb{C}(\Gamma').$$
So by Example 21.3, we have the following inclusion of fields,
$$\mathbb{C}(j) = \mathbb{C}(\Gamma(1)) \subset \mathbb{C}(\Gamma).$$

Modular functions for $\Gamma(\mathrm{N})$

This part is based on [Lan87, Ch. 6], [Shi71, Ch. 6] and [DS05, Section 7.5]. Recall that $\mathrm{X}(\mathrm{N})$ classifies isomorphism classes of elliptic curves E with a basis of $\mathrm{E}[\mathrm{N}]$. Let $\mathbb{C}(\Gamma(\mathrm{N}))$ be the field of modular functions for $\Gamma(\mathrm{N})$. One can explicitly find a generating set for $\mathbb{C}(\Gamma(\mathrm{N}))$.

Let $\tau \in \mathbb{H}$ and $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$. Let E_τ be the complex elliptic curve associated to Λ. Let us fix a vector $a := \begin{bmatrix} a_0 & a_1 \end{bmatrix}$ of $\mathbb{Q}^2$ and consider the following function,

$$f_a(\tau) = \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp\left(\begin{bmatrix} a_0 & a_1 \end{bmatrix} \cdot \begin{bmatrix} \tau \\ 1 \end{bmatrix}; \Lambda\right) = \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp\left(a_0\tau + a_1; \Lambda\right).$$

From Section 19.1, $\wp\left(a_0\tau + a_1; \Lambda\right)$ is the x-coordinate of a point of finite order. An element of $\mathrm{SL}_2(\mathbb{Z})$ acts in a natural way on f_a given in Def. 21.4. More precisely, we have the following, see [Shi71, Section 6.1]. If $a \in \mathbb{Q}^2/\mathbb{Z}^2$,

$$f_a \circ \gamma = f_{a\cdot\gamma} \text{ for all } \gamma \in \mathrm{SL}_2(\mathbb{Z}).$$

The main result about the generating set of $\mathbb{C}(\Gamma(\mathrm{N}))$ is the following.

Theorem 21.9 ([Shi71, Prop. 6.1])**.** *For every positive integer* N*,*

$$\mathbb{C}(\Gamma(\mathrm{N})) = \mathbb{C}(j, f_a \mid a = \begin{bmatrix} a_0 & a_1 \end{bmatrix} \in \frac{\mathbb{Z}^2}{\mathrm{N}} \text{ and } a \notin \mathbb{Z}^2).$$

As $\wp$ is an even function, $f_a(\tau) = f_{-a}(\tau)$. Furthermore, one sees that f_a is of weight 0. Consider the following sum where $\Lambda = \langle \tau, 1\rangle$ and $a \in \frac{\mathbb{Z}^2}{\mathrm{N}}$ and $a \notin \mathbb{Z}^2$ i.e. a has order N in $(\mathbb{Z}/\mathrm{N}\mathbb{Z})^2$:

$$\sum_a f_a(\tau)\frac{\Delta(\Lambda)}{g_2(\Lambda)g_3(\Lambda)}.$$

This sum is invariant under $\mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ and defines a modular form of weight 2. As there are no non-zero modular forms of weight 2, we must have $\sum_a f_a = 0$. Thus the set $\{f_{\pm a}\}$ is linearly dependent. Hecke ([Hec27, RZB15]) proved that removing one f_a for some a gives a $\mathbb{Q}(\zeta_\mathrm{N})$-linearly independent set.

f_a algebraic over $\mathbb{Q}(j)$

Shimura proved that f_a is algebraic over $\mathbb{Q}(j)$ where j is the modular j-invariant i.e. there exists a polynomial $\mathrm{T} \in \mathbb{Q}(j)[\mathrm{X}]$ such that $\mathrm{T}(f_a) = 0$. More precisely, we have the following,

Theorem 21.10 ([Shi71, Theorem 6.6])**.** *Let*

$$\mathcal{F}_\mathrm{N} = \mathbb{Q}\left(j, f_a \mid a \in \frac{\mathbb{Z}^2}{\mathrm{N}} \text{ and } a \notin \mathbb{Z}^2\right).$$

Then,

1. *$\mathcal{F}_\mathrm{N}$ is a Galois extension of $\mathbb{Q}(j)$.*
2. *For every $\beta \in \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$, the application $f_a \mapsto f_{a\beta}$ is an element, say $\tau(\beta)$, of $\mathrm{Gal}(\mathcal{F}_\mathrm{N}/\mathbb{Q}(j))$. Then, we have the following isomorphism,*

$$\begin{array}{rcl} \tau\colon \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})/\{\pm\mathrm{I}\} & \longrightarrow & \mathrm{Gal}(\mathcal{F}_\mathrm{N}/\mathbb{Q}(j)) \\ \beta & \mapsto & \tau(\beta) \end{array}$$

3. *If ζ is a primitive* N*-th root of unity, then $\zeta \in \mathcal{F}_\mathrm{N}$, and $\tau(\beta)(\zeta) = \zeta^{\det\beta}$.*

4. *$\mathbb{Q}(\zeta)$ is algebraically closed in $\mathcal{F}_\mathrm{N}$ i.e. $\overline{\mathbb{Q}} \cap \mathcal{F}_\mathrm{N} = \mathbb{Q}(\zeta)$.*

5. *$j \circ \alpha \in \mathcal{F}_\mathrm{N}$ for all $\alpha \in \mathrm{M}_2(\mathbb{Z})$ with determinant* N.

The field $\mathcal{F}_\mathrm{N}$ corresponds to the elements of $\mathbb{C}(\Gamma(\mathrm{N}))$ whose q-expansions are defined over $\mathbb{Q}(\zeta_\mathrm{N})$, where ζ_N is a N-th primitive root of unity. The 2. of the above theorem says that an element $\beta \in \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ acts on $\mathcal{F}_\mathrm{N}$ via the automorphism $\tau(\beta)$. We note that $-\mathrm{I}$ acts trivially. This action can be used to compute modular curves as we explain in next sections.

Let us conclude this section with a q-expansion of $\wp\left(\frac{c\tau+d}{\mathrm{N}}; \langle\tau, 1\rangle\right)$, see [Shi71, p. 141, Eq. 6.2.1]. Let $\tau \in \mathbb{H}$, $(c, d) \in (\mathbb{Z}/\mathrm{N}\mathbb{Z})$ be of order N and ζ be a primitive N-th root of unity. Then,

$$\frac{1}{4\pi^2}\wp\left(\frac{c\tau+d}{\mathrm{N}}; \langle\tau, 1\rangle\right) = \frac{-1}{12} - \frac{\zeta^d q^{\frac{c}{\mathrm{N}}}}{\left(1-\zeta^d q^{\frac{c}{\mathrm{N}}}\right)^2} + 2\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n} + \sum_{n=1}^{\infty}\left(\left(\zeta^{nd}q^{\frac{nc}{\mathrm{N}}} + \zeta^{-nd}q^{\frac{-nc}{\mathrm{N}}}\right)\cdot\frac{nq^n}{1-q^n}\right). \quad (5.1)$$

22 Computing modular curves

Let N be a positive integer and ζ be a primitive N-th root of unity. Let $\mathrm{G} \subset \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ be such that $-\mathrm{I} \in \mathrm{G}$ and $\det(\mathrm{G}) = (\mathbb{Z}/\mathrm{N}\mathbb{Z})^*$. Let $\mathcal{F}_\mathrm{N}^\mathrm{G}$ be the fixed subfield by G under the action defined in Theorem 21.10 (see Def. 21.4). One sees that $\mathcal{F}_\mathrm{N}^\mathrm{G}$ is an algebraic extension of $\mathbb{Q}(j)$. If $\mathrm{X}_\mathrm{G} \in \mathbb{Q}(j)[\mathrm{X}]$ is a defining polynomial of $\mathcal{F}_\mathrm{N}^\mathrm{G}$, we can consider $\mathcal{F}_\mathrm{N}^\mathrm{G}$ as the function field of the curve (viewed in two variables j and X) X_G which is called a modular curve associated to G. The field extension $\mathbb{Q}(j) \subset \mathcal{F}_\mathrm{N}^\mathrm{G}$ induces the following morphism of curves,

$$\pi_\mathrm{G}\colon \mathrm{X}_\mathrm{G} \longrightarrow \mathbb{P}^1(\mathbb{Q}).$$

Similar to the modular curves we saw earlier, X_G also has a moduli interpretation.

Theorem 22.1 ([Shi71, Ch. 6], [Zyw15a, Prop. 3.3])**.** *Let $\mathrm{G} \subset \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ be such that $-\mathrm{I} \in \mathrm{G}$ and $\det(\mathrm{G}) = (\mathbb{Z}/\mathrm{N}\mathbb{Z})^*$. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve such that $j(\mathrm{E}) \notin \{0, 1728\}$. Then the mod* N *Galois image $\mathrm{Im}(\rho_{\mathrm{E},\mathrm{N}})$ is $\mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$-conjugate of a subgroup of* G *if, and only if, $j(\mathrm{E}) \in \pi_\mathrm{G}(\mathrm{X}_\mathrm{G}(\mathbb{Q}))$.*

Another way of looking at the modular curve X_G is the following, see [CSS13, Ch. 3]. Consider the rational function field $\mathbb{Q}(j)$. Here we consider j as an indeterminate and *not* the modular j-invariant. Let E_j be an elliptic curve such that $j(\mathrm{E}_j) = j$. One such curve is

$$\mathrm{E}_j : y^2 = x^3 - 3(j-1728)jx - 2(j-1728)^2 j.$$

One constructs the N-torsion point field K over $\mathbb{Q}(j)$ by adjoining the coordinates of the points of $\mathrm{E}_j[\mathrm{N}]$ from $\overline{\mathbb{Q}(j)}$. Then $\mathrm{K}/\mathbb{Q}(j)$ is a Galois extension and

$$\mathrm{Gal}(\mathrm{K}/\mathbb{Q}(j)) \cong \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z}).$$

We have $\mathrm{G} \subset \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$. Consider the subfield $\mathrm{K}^\mathrm{G} \subset \mathrm{K}$ which is fixed by G. It is a function field of a smooth curve defined over $\mathbb{Q}$, which we call X_G. In other words,

consider a defining polynomial $\mathcal{P}_{\mathrm{G}} \in \mathbb{Q}(j)[\mathrm{X}]$ of the field K^{G}. The curve X_{G} has the same set of zeros as $\mathcal{P}_{\mathrm{G}}$. Despite the simplicity of this description of X_{G}, it is difficult to compute the preimage of G in $\mathrm{Gal}(\mathrm{K}/\mathbb{Q}(j))$. It can be however done if one uses the theory of modular curves as one can describe the action of an element of G on f_a. For computational aspects of modular curves, the reader can refer to [CE11].

22.1 Computing primitive elements

Let $\mathrm{G} \subset \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ be such that X_{G} has genus 0. We want to find a primitive element h of $\mathcal{F}_{\mathrm{N}}^{\mathrm{G}}$ over $\mathbb{Q}(j)$. Having computed such a primitive element for G, one can consider a subgroup G' of G. In this section, we discuss a method given in [RZB15, Section 4] to compute relative primitive elements.

Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ containing $-\mathrm{I}$ and with surjective determinant. Choose $\tilde{\mathrm{H}}$ containing H such that H is maximal in it. Let us suppose that we have computed a primitve element $\tilde{h}$ for $\tilde{\mathrm{H}}$. We want to compute an element $h \in \mathcal{F}_{\mathrm{N}}$ which generates the subfield of $\mathcal{F}_{\mathrm{N}}$ fixed by H over the function field $\mathbb{Q}(\mathrm{X}_{\tilde{\mathrm{H}}})$. In other words, we are looking for a root of a defining polynomial of the function field $\mathbb{Q}(\mathrm{X}_{\mathrm{H}})$ over $\mathbb{Q}(\mathrm{X}_{\tilde{\mathrm{H}}})$. For that, we first consider the function field $\mathbb{Q}(\zeta, \mathrm{X}_{\tilde{\mathrm{H}}})$ and then move on to $\mathbb{Q}(\mathrm{X}_{\tilde{\mathrm{H}}})$.

Let V be the $\mathbb{Q}(\zeta)$-subspace of $\mathcal{F}_{\mathrm{N}}$ spanned by the functions f_a defined in Section 21. We first look for h in the subspace V^{H} of V fixed by H under the action coming from Theorem 21.10. If we find an element $h \in \mathrm{V}^{\mathrm{H}}$ which has $[\tilde{\mathrm{H}} : \mathrm{H}]$ distinct images under the action of the representative of right cosets of H in $\tilde{\mathrm{H}}$, or equivalently if we find an $h \in \mathrm{V}^{\mathrm{H}}$ which is not invariant under $\tilde{\mathrm{H}}$ i.e. h such that $h \notin \mathrm{V}^{\tilde{\mathrm{H}}}$, we have found a primitive element for H. This approach can only succeed when the dimension of V^{H} is strictly bigger than that of $\mathrm{V}^{\tilde{\mathrm{H}}}$.

By [DS05, Section 4.6], the space of weight 2 Eisenstein series for $\Gamma(\mathrm{N})$ with coefficients in $\mathbb{Q}(\zeta)$ is isomorphic to V and the dimension of the space of weight 2 Eisenstein series for H is the number of cusps of X_{H} minus 1 (cf. [DS05, p. 111]). If X_{H} and $\mathrm{X}_{\tilde{\mathrm{H}}}$ have the same number of cusps, the fixed subspaces $\mathrm{V}^{\tilde{\mathrm{H}}}$ and V^{H} will have the same dimension and as $\mathrm{V}^{\tilde{\mathrm{H}}} \subset \mathrm{V}^{\mathrm{H}}$, we will have $\mathrm{V}^{\tilde{\mathrm{H}}} = \mathrm{V}^{\mathrm{H}}$. In this case, we do not find a primitive element for H in V^{H}.

So we instead consider a subgroup $\mathrm{K} \subset \mathrm{H}$ such that X_{K} has more cusps than X_{H}. Note that such a subgroup always exists. Indeed as the number of cusps of K is equal to the number of orbits of infinity under the action of the lift of $\mathrm{K} \cap \mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ in $\mathrm{SL}_2(\mathbb{Z})$. If K is chosen to be the singleton group then the lift of $\mathrm{K} \cap \mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ is $\Gamma(\mathrm{N})$. It has the maximum number of cusps which is equal to the cardinality of $\mathbb{P}^1(\mathbb{Z}/\mathrm{N}\mathbb{Z})$.

Once we have K, we compute the fixed subspace of V by $\mathrm{K} \cap \mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$. It is important to consider the intersection with $\mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ as by Theorem 21.10, the only matrices which fix the scalars in $\mathbb{Q}(\zeta)$ are the ones with determinant 1. Let $w_1, w_2, \cdots, w_n$ be the generators of the subspace fixed by $\mathrm{K} \cap \mathrm{SL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$.

We then consider the basis $\{\zeta^i w_j \mid 1 \leq i \leq \mathrm{N}, 1 \leq j \leq n\}$ and the action of an element of K on ζ in order to compute the fixed $\mathbb{Q}$-subspace V^{K} of V by K. Let V^{K} be generated by vectors $v_1, \cdots, v_m \in \mathrm{V}$. We take a random element v in V^{K}, for example one can take $v = \sum_{i=1}^{m} i v_i$, such that v has as many distinct images under the action of H as the index $[\mathrm{H} : \mathrm{K}]$.

We then compute the q-expansion of v using the q-expansions of f_a using Equation 5.1. Let $k_1, k_2, \cdots k_r$ be the representatives of right cosets of K in H. We define

$$h_s = e_s(k_1(v), k_2(v), \cdots, k_r(v)),$$

where e_s is the elementary symmetric polynomial of degree s in r variables. If for some s, h_s has as many distinct images as the index $[\tilde{\mathrm{H}} : \mathrm{H}]$ under the action of the representatives of right cosets of H in $\tilde{\mathrm{H}}$, we put $h = h_s$. It is a primitive element as it is stabilized by H and not by $\tilde{\mathrm{H}}$ and as the map $\mathrm{X}_{\mathrm{H}} \longrightarrow \mathrm{X}_{\tilde{\mathrm{H}}}$ has minimal degree.

In order to explicitly compute the equation of X_{H} over $\mathbb{Q}(j)$, one computes the minimal polynomial of h over $\mathbb{Q}(j)$ using the q-expansion of h and linear algebra. We consider the q-expansion of the following combination for m the index of H in $\tilde{\mathrm{H}}$,

$$\sum_{i=0}^{m}\sum_{k=0}^{m} c_{i,k} h^i j^k.$$

Equating this to 0 and collecting the coefficients of each power of q, one obtains a system of equations. Using enough terms of the q-expansion of h and j, one can determine the coefficients $c_{i,j}$.

Example

Let $\mathrm{H} = \langle \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1 \\ 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right) \rangle \subset \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. It is a maximal subgroup of order 16 of $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and they have the same number of cusps which is 1. Put $\mathrm{K} = \langle \left(\begin{smallmatrix} 0 & 1 \\ 2 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right) \rangle \subset \mathrm{H}$ of index 2, note that K has 2 cusps. The fixed subspace of V by $\mathrm{K} \cap \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ is 1-dimensional and is generated by $f = f_{(0,1)} + f_{(1,0)}$. We put ignoring $g_2(\Lambda)g_3(\Lambda)/\Delta(\Lambda)$, $f_a = \wp(a_0\tau + a_1; \Lambda)$ for $a = (a_0, a_1)$. We choose We then consider the fixed subspace of V by K using the basis $\{f, \omega f, \omega^2 f\}$ where ω is a primitive cube root of 1. We obtain that $\mathrm{V}^{\mathrm{K}} = \langle f \rangle$ and f has distinct 2 images under the action of coset representatives of H/K. The symmetric combination we consider is

$$\begin{aligned} h_2 &= e_2(f_{(0,1)} + f_{(1,0)}, f_{(1,1)} + f_{(1,2)}) \\ &= (f_{(0,1)} + f_{(1,0)}) \times (f_{(1,1)} + f_{(1,2)}) \end{aligned}$$

At this stage, we compute the Fourier expansion. As h_2 is a modular form of weight 4, we multiply it by $\mathrm{G}_4^2(\tau)/\Delta(\tau)$ to obtain a modular form of weight 0. The q-expansion of $f := \mathrm{G}_4^2(\tau)/\Delta(\tau) \times h_2$ is

$$-36q^{-1} + 432q^{-2/3} - 26784 + 214272q^{1/3} - 7087824q + 30132864q^{4/3} - 773775360q^2 + O(q^3).$$

Collecting enough terms of f and the q-expansion of modular j invariant defined in Example 21.3, we obtain the following modular curve.

$$46656j^3 + 3888j^2 f + 108jf^2 + f^3 - 80621568j^2 = 0.$$

This is a genus 0 curve and it can be parameterized by setting $j = j(t) = t^3$. In conclusion, for a rational elliptic curve E such that $j(\mathrm{E})$ is a rational cube, $\mathrm{Im}\rho_{\mathrm{E},3}$ is contained in H.

Chapter 6

Progress on Mazur's Program B

In this chapter, we start with a discussion on the recent progress on Mazur's Program B and then move on to modular curves associated to composite levels. We find all infinite ECM-friendly families and point out the ones having larger torsion over all finite fields than over $\mathbb{Q}$. Finally, we compare our results with those of [Mor19] in the section that deals with entanglement.

23 Works of [RZB15] and [SZ17]

In 2015, J. Rouse and D. Zureick-Brown in [RZB15] classified all possible 2-adic Galois images for rational elliptic curves. They proved that there are 1208 *proper* subgroups G of $\mathrm{GL}_2(\mathbb{Z}_2)$ for which $\mathrm{X_G}(\mathbb{Q})$ is non-empty. Out of these, for 8 subgroups, the modular curve has genus at least 2 and for the remaining 1200 subgroups, $\mathrm{X_G}(\mathbb{Q})$ is infinite. Among these, 194 subgroups contain the matrix $-\mathrm{I}$ and the remaining ones do not. They proved the following.

Theorem 23.1 ([RZB15, Cor. 1.3])**.** *Let* E *be an elliptic curve over* $\mathbb{Q}$ *without complex multiplication. Then the image of* $\rho_{\mathrm{E},2^\infty}$ *in* $\mathrm{GL}_2(\mathbb{Z}_2)$ *is* $\pi^{-1}(\mathrm{Im}\rho_{\mathrm{E},32})$*. For non-CM elliptic curves* $\mathrm{E}/\mathbb{Q}$ *there are precisely 1208 possible images for* $\rho_{\mathrm{E},2^\infty}$*.*

Contemporaneously, A. Sutherland and D. Zywina in [SZ17] considered groups G of prime power levels containing $-\mathrm{I}$. They computed explicit models of modular curves $\mathrm{X_G}$ which admit *infinitely many* rational points and gave parameterizations of these curves. For each subgroup H containing $-\mathrm{I}$, they found the list of subgroups H', with surjective determinant such that $-\mathrm{I} \notin \mathrm{H}$ and $\mathrm{H} = \langle -\mathrm{I}, \mathrm{H}' \rangle$.

An argument that we will see below in Lemma 23.4 guarantees that, for each j-invariant whose curves have the mod N Galois image contained in H, there exists exactly one elliptic curve, up to isomorphism over $\mathbb{Q}$ whose mod N Galois image is contained in H', up to conjugacy in H. Hence, without computing parameterizations of the elliptic curves whose Galois images do not contain $-\mathrm{I}$, they concluded that there are exactly 46 (resp. 22, 14, 1, 10) *proper* subgroups of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for $\ell = 3$ (resp. $5, 7, 11, 13$) which can occur as Galois images for infinitely many elliptic curves with distinct j-invariants, and none for other odd primes. They proved the following.

Theorem 23.2 ([SZ17, Cor. 1.6])**.** *For* $\ell = 2, 3, 5, 7, 11, 13$*, there are respectively* $1200, 46, 22, 14, 1, 10$ proper *subgroups* H *of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *that arise as the image of* $\rho_{\mathrm{E},\ell^\infty}$ *for infinitely many elliptic curves* $\mathrm{E}/\mathbb{Q}$ *with distinct* j*-invariants. For* $\ell > 13$*, the only such subgroup is* $\mathrm{H} = \mathrm{GL}_2(\mathbb{Z}_\ell)$*.*

Remark 23.3. *Theorem 3.3 of [SZ17] is applicable to all totally real number fields and generalizes to arbitrary number fields with a uniform bound on subgroups of genus 0 and 1. Thus, over any number field, one can make a similar classification.*

23.1 Parameterizations when $-\mathrm{I} \notin \mathrm{H}$

Two curves with the same j-invariant can have different Galois images. For example, an elliptic curve has a rational point P of order 3 if, and only if, its mod 3 Galois image is contained, up to conjugacy, in the group of matrices $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. Indeed, one can choose a basis of $\mathrm{E}[m]$ containing P. Then, as P is rational, it is fixed by every automorphism. This ensures that the first column of the image of any automorphism is $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$. Consider the set of pairs $(a, b) \in \mathbb{Q}^2$ such that for $\mathrm{E} : y^2 = x^3 + ax + b$, there exists a rational x_3 such that $\Psi_3(x_3) = 0$, where Ψ_3 is the 3-division polynomial of E. Then, among the set of curves $dy^2 = x^3 + ax + b$, which have the same j-invariant, only those such that $(x_3^3 + ax_3 + b)/d$ is a rational square, have a rational point of order 3. Hence, when $-\mathrm{I} \notin \mathrm{H}$, we have to parameterize the pairs (a, b) rather than just the j-invariants.

The following result gives a method to parameterize the set of curves whose Galois image is in a subgroup H which does not contain $-\mathrm{I}$. We put $\tilde{\mathrm{H}} = \langle -\mathrm{I}, \mathrm{H} \rangle$. If $\mathrm{X}_{\tilde{\mathrm{H}}}$ is a conic with a rational point then we parameterize it as $j = j(t)$ and apply the following lemma for $\mathrm{K} = \mathbb{Q}(t)$, $a = -3j(j - 1728) \in \mathrm{K}$ and $b = -2j(j - 1728)^2 \in \mathrm{K}$. If $\mathrm{X}_{\tilde{\mathrm{H}}}$ is an elliptic curve or a higher genus curve, we generate rational points on it and apply the following lemma for $\mathrm{K} = \mathbb{Q}$.

Lemma 23.4 ([RZB15, Section 5])**.** *Let* $\mathrm{K} = \mathbb{Q}(t)$ *(resp.* $\mathbb{Q}$*). Let* $\tilde{\mathrm{H}} \subset \mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ *such that* $-\mathrm{I} \in \tilde{\mathrm{H}}$*. Let* $\mathrm{H} \subset \tilde{\mathrm{H}}$ *such that* $-\mathrm{I} \notin \mathrm{H}$ *and* $\tilde{\mathrm{H}} = \langle -\mathrm{I}, \mathrm{H} \rangle$*. Let* $\mathrm{E} : y^2 = x^3 + ax + b$ *be an elliptic curve over* K *such that* $\mathrm{Im}\rho_{\mathrm{E},\mathrm{N}} = \tilde{\mathrm{H}}$*. Then there exists a unique squarefree* d *in* $\mathbb{Z}[x]$ *(resp. in* $\mathbb{Z}$*) such that* $\mathrm{Gal}(\mathrm{K}(\mathrm{E}_d[\mathrm{N}])/\mathrm{K}) \subset \mathrm{H}$*, where* $\mathrm{E}_d : dy^2 = x^3 + ax + b$*. Furthermore, the value of* d *is in the finite set of squarefree elements of* $\mathbb{Z}[t]$ *(resp.* $\mathbb{Z}$*) whose prime factors divide either the numerator or the denominator of* $\mathrm{N} \cdot (4a^3 + 27b^2)$*.*

In the light of the above lemma, there is a method, presented in [RZB15], which allows us to parameterize the curves corresponding to the subgroups of a group $\tilde{\mathrm{H}}$ containing $-\mathrm{I}$ whose modular curve is a conic i.e. has genus 0 and a rational point. Once we parameterize the pairs $(a = a(t), b = b(t))$ such that $y^2 = x^3 + ax + b$ has the Galois image in $\tilde{\mathrm{H}}$, we proceed in two steps:

1. We compute the list of irreducible factors $p_1, \ldots, p_k$ of $\mathrm{N} \cdot (4a^3 + 27b^2)$ in $\mathbb{Z}[t]$ and enumerate the products $d = (-1)^{e_0} \prod_{i=1}^{k} p_i^{e_i}$ where $e_0, \ldots, e_k \in \{0, 1\}$. We then test if the field $\mathrm{K}(\mathrm{E}[\mathrm{N}])$ contains a root of $x^2 - d$ to obtain the list of its quadratic subfields.

2. We make the list of subgroups H of $\mathrm{GL}_2(\mathbb{Z}/\mathrm{N}\mathbb{Z})$ such that $\langle \mathrm{H}, -\mathrm{I} \rangle = \tilde{\mathrm{H}}$ and $\det \mathrm{H} = (\mathbb{Z}/\mathrm{N}\mathbb{Z})^*$ and $-\mathrm{I} \notin \mathrm{H}$. For each $d(t)$ corresponding to quadratic subfields, we eliminate all but one subgroup H by giving numerical values to t and computing the Galois image of $d(t)y^2 = x^3 + ax + b$.

Example 23.5. Consider the case of $\mathrm{H} = \langle \left(\begin{smallmatrix} 0 & 1 \\ 2 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 \\ 0 & 2 \end{smallmatrix}\right) \rangle \subset \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. According to [SZ17, Tab. 1], the set of rational triples (d, a, b) such that for $\mathrm{E} : dy^2 = x^3 + ax + b$, $\mathrm{Im}\rho_{\mathrm{E},3}$ contained in H are such that there exist rationals t and λ such that $a = -3\lambda^2 (t + 27)(t + 3)$ and $b = -2\lambda^3(t^2 + 18t - 27)(t + 27)$. The prime factors of $3(4a^3 + 27b^2)$ are 2, 3, t and $(t + 27)$. Out of the 32 squarefree possible values of d, the only squares in $\mathbb{Q}(t)(\mathrm{E}[3])$ are $d = (t + 27)$, $d = -3(t + 27)$ and $d = -3$.

There are three index 2 subgroups of H, out of which two have surjective determinant and do not contain $-\mathrm{I}$: $\mathrm{H}_1 = \langle \left(\begin{smallmatrix} 2 & 1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 2 \end{smallmatrix}\right) \rangle$ and $\mathrm{H}_2 = \langle \left(\begin{smallmatrix} 1 & 2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 2 \\ 1 & 2 \end{smallmatrix}\right) \rangle$.

For numerical values t_0 of t (e.g. $t_0 = 5$), we compute the images of $\rho_{\mathrm{E}_{d_1(t=t_0)},3}$ and $\rho_{\mathrm{E}_{d_2(t=t_0)},3}$ using the scripts in the online complement ([BS19b]) and obtain that $d_1 = t + 27$ corresponds to H_1 and $d_2 = -3(t + 27)$ to H_2. Lemma 23.4 allows to conclude that, if the Galois image of E_{d_1} is not contained in H_2 for one numerical value it is not contained for any $t \in \mathbb{Q}$.

The work of Zywina in [Zyw15a] presents parameterizations corresponding to the groups which do not contain $-\mathrm{I}$, but only for prime levels. We completed the classification for the remaining prime-power cases ℓ^k where ℓ is odd. It is summarized in the following theorem. Note that two subgroups of H, corresponding to different quadratic subfields, can be conjugated.

Theorem 23.6. *Let ℓ be an odd prime. The set of subgroups $\mathrm{H} \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ which occur as Galois image for infinitely many j-invariants such that $-\mathrm{I} \in \mathrm{H}$ are the ones given in Tables 26.1 and 26.2, p. 116.*

It is remarkable that, for any prime-power, the subgroups that do not contain $-\mathrm{I}$ which occur as Galois images for infinitely many j-invariants have genus 0 and have rational parameterizations so one can apply Lemma 23.4 to $\mathrm{K} = \mathbb{Q}(t)$. The method in this section applies to subgroups of arbitrary genera and levels using Lemma 23.4 for $\mathrm{K} = \mathbb{Q}$.

24 Non-prime-power level case

A theorem of Cox and Parry [CP84] gives an explicit upper bound on the level of a congruence subgroup in terms of its genus. This allowed Cummins and Pauli [CP03] to obtain the complete list of subgroups of $\mathrm{PSL}_2(\mathbb{Z})$ of genus $g \leq 24$.

For each such subgroup Γ, one can compute the list of subgroups Γ' of $\mathrm{GL}_2(\mathbb{Z})$ such that $\Gamma' \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma$. (see the proof of [SZ17, Prop. 3.6].) The method in the previous section permits to compute X_H for any H. In this section, we propose an elementary method which is restricted to a certain class of subgroups which plays an important role in ECM.

Definition 24.1. Given a tuple of matrices $(\mathrm{M}_i)_{i\in\mathrm{I}}$ of $\prod_{i\in\mathrm{I}} \mathrm{GL}_2(\mathbb{Z}/\ell_i^{k_i}\mathbb{Z})$, we define their cartesian product $\times_{i\in\mathrm{I}}\mathrm{M}_i$ as the matrix M of $\mathrm{GL}_2(\mathbb{Z}/\prod_{i\in\mathrm{I}} \ell_i^{k_i}\mathbb{Z})$ whose coefficients are the lifts of corresponding coefficients of M_i. A subgroup H of $\mathrm{GL}_2(\mathbb{Z}/\prod_{i\in\mathrm{I}} \ell_i^{k_i}\mathbb{Z})$ is called cartesian if it is equal to $\times_{i\in\mathrm{I}}\mathrm{H}_i = \{\times_{i\in\mathrm{I}}\mathrm{M}_i | \mathrm{M}_i \in \mathrm{H}_i\}$, where H_i is the projection of H modulo $\ell_i^{k_i}$. A non-cartesian subgroup is called an *entanglement* subgroup.

An example of an entanglement subgroup is $\{\mathrm{I}, -\mathrm{I}\} \subset \mathrm{GL}_2(\mathbb{Z}/15\mathbb{Z})$. We shall revisit it in Section 26.

Remark 24.2. *Henceforth, We shall denote an even level subgroup by X_i from [RZB15]. When it is clear from the context we shall denote the corresponding modular curves also by X_i. In order to maintain the consistency, we consider these groups in their transposed forms. If the level is odd, we use the notations from [SZ17]. For $\mathrm{G} \subset \mathrm{GL}_2(\hat{\mathbb{Z}})$, its label in [SZ17] is $\mathrm{M}\mathrm{Z}^g$-$\mathrm{N}z$ where M, N and g are integers and Z and g are letters. The integers N and g correspond to the level and the genus of G and the integer M corresponds to the level of a congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ whose image modulo N is in the image*

of G *modulo* N. *the letter* Z *determines* Γ *up to conjugacy in* $\mathrm{SL}_2(\mathbb{Z})$ *and the letter* z *determines* G *up to conjugacy in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$. *The label* MZ^g-$\mathrm{N}z\mathrm{T}i$ *for* $i = 1, 2$ *denotes a quadratic twist in the case above, if it exists.*

Example 24.3. It is possible for a group MZ^g-$\mathrm{N}z$ to have different values of M and N. Consider the group $\mathrm{X}_4 \subset \mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ from [RZB15]. Its label in [SZ17] is $2\mathrm{A}^0$-$8a$. The intersection of the mod 2 (resp. 4) projection of X_4 with $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$) is the full group $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$).

24.1 The case $\mathrm{H}_1 \times \mathrm{H}_2$

Let $\mathrm{H}_1 \subset \mathrm{GL}_2(\mathbb{Z}/\ell_1^m)$ and $\mathrm{H}_2 \subset \mathrm{GL}_2(\mathbb{Z}/\ell_2^n)$ with $\ell_1 \neq \ell_2$. We consider three cases depending on whether $-\mathrm{I}$ belongs to both, either or neither of H_1 and H_2.

The case where $-\mathrm{I} \in \mathrm{H}_1$ and $-\mathrm{I} \in \mathrm{H}_2$ There are 17 possible maximal subgroups of $1\mathrm{A}^0$-$1a$ which is $\mathrm{GL}_2(\hat{\mathbb{Z}})$ which appear as Galois images infinitely often.

$$\mathrm{X}_2, \mathrm{X}_3, \mathrm{X}_4, \mathrm{X}_5, \mathrm{X}_6, \mathrm{X}_7 \subset \mathrm{GL}_2(\mathbb{Z}_2),$$
$$3\mathrm{A}^0\text{-}3a, 3\mathrm{B}^0\text{-}3a, 9\mathrm{F}^0\text{-}9a \subset \mathrm{GL}_2(\mathbb{Z}_3),$$
$$5\mathrm{A}^0\text{-}5a, 5\mathrm{B}^0\text{-}5a, 5\mathrm{C}^0\text{-}5a \subset \mathrm{GL}_2(\mathbb{Z}_5),$$
$$7\mathrm{B}^0\text{-}7a, 7\mathrm{D}^0\text{-}7a, 7\mathrm{F}^0\text{-}7a \subset \mathrm{GL}_2(\mathbb{Z}_7),$$
$$13\mathrm{A}^0\text{-}13a \subset \mathrm{GL}_2(\mathbb{Z}_{13}), 11\mathrm{C}^1\text{-}11a \subset \mathrm{GL}_2(\mathbb{Z}_{11}).$$

Note that the only maximal subgroup of genus 1 is $11\mathrm{C}^1$-$11a$. So for any pair of maximal subgroups H_1 and H_2, at least one of them has genus 0, say H_1. Let $j = j_1(t_1)$ be a parameterization of $\mathrm{X}_{\mathrm{H}_1}$. Then $\mathrm{X}_{\mathrm{H}_2}(j_1(t_1), t_2)$ is a plane curve which characterizes elliptic curves with mod ℓ_1^m Galois image in H_1 and mod ℓ_2^n Galois image in H_2.

Example 24.4. Let $\mathrm{H}_1 = \mathrm{X}_6$ and $\mathrm{H}_2 = 3\mathrm{A}^0$-$3a$ with $j_1(t) = \frac{(t-256)^3}{t^2}$ and $j_2(t) = t^3$. We consider the curve $\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2}$ defined by the numerator of $j_1(x) - j_2(y)$ which is $-x^2y^3 - x^3 + 768\,x^2 - 196608\,x + 16777216$. This is the modular curve X_6-$3\mathrm{A}^0$-$3a$. It has genus 0 and can be parameterized by setting

$$x = t^3 \text{ and } y = -\frac{t^3 - 256}{t^2}.$$

Thus, if the j-invariant of an elliptic curve $\mathrm{E}/\mathbb{Q}$ is of the form $\frac{-(t^3-256)^3}{t^6}$ for some $t \in \mathbb{Q}$, we have that $\mathrm{Im}\rho_{\mathrm{E},2} \subset \mathrm{H}_1$ and $\mathrm{Im}\rho_{\mathrm{E},3} \subset \mathrm{H}_2$. In this case, we say that E is parameterized by the modular curve X_6-$3\mathrm{A}^0$-$3a$.

For the 17 maximal subgroups, there are 112 possible cartesian products $\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2}$. Out of them, 17 have genus 0, 28 have genus 1 and others have higher genera. We do not concern ourselves with the last case as we are looking for infinite families.

If for some H_1 and H_2, we succeed in parameterizing the curve $\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2}$, then we proceed in the similar manner, by taking the maximal subgroups of H_1 and H_2. We obtain 163 products of genus 1 and 46 products of genus 0. Out of them, all the products of genus 0 have infinitely many rational points whereas 35 products of genus 1 have positive rank. Thus there are in total $46+35 = 81$ products of subgroups containing $-\mathrm{I}$ whose modular curves admit infinitely many rational points.

The case where $-\mathrm{I} \in \mathrm{H}_1$ and $-\mathrm{I} \notin \mathrm{H}_2$. We first consider the group $\mathrm{H}_2' = \langle \mathrm{H}_2, -\mathrm{I}\rangle$ and compute $\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2'}$. As above, we consider the genus of this curve and parameterize it to get a model $\mathrm{E}_{\mathrm{H}_1\times\mathrm{H}_2'}$. By Lemma 23.4, there exists a quadratic twist of $\mathrm{E}_{\mathrm{H}_1\times\mathrm{H}_2'}$ such that its mod ℓ_2^m Galois image is contained in H_2. From 81 possibilities of products, we find 110 such families. Out of them, 85 are of genus 0 and 25 are of genus 1.

The case where $-\mathrm{I} \notin \mathrm{H}_1$ and $-\mathrm{I} \notin \mathrm{H}_2$. Let $\mathrm{H}_1' = \langle \mathrm{H}_1, -\mathrm{I}\rangle$ and $y^2 = x^3 + a(t)x + b(t)$ be its model of j-invariant $j_1(t)$. Also let $d_1(t)y^2 = x^3 + a(t)x + b(t)$ be a model for H_1. We define H_2', $d_2(t)$ in a similar manner. For $(t_1, t_2) \in \mathrm{X}_{\mathrm{H}_1'\times\mathrm{H}_2'}$, Lemma 23.4, applied to a curve of j-invariant $j_1(t_1)$ and $\mathrm{K} = \mathbb{Q}$, gives the existence of a unique elliptic curve up to isomorphism over $\mathbb{Q}$ whose Galois image is contained in H_1. Equivalently, there exists a unique rational δ up to a square such that the curve $\delta y^2 = x^3 + a(t)x + b(t)$ has Galois image contained in H_1. As δ is unique, we have $d_1(t_1) = \delta$ up to a square. Similarly we have $d_2(t_2) = \delta\square$. This shows that

$$\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2} := \{(t_1, t_2) \in \mathrm{X}_{\mathrm{H}_1'\times\mathrm{H}_2'} \mid \frac{d_1(t_1)}{d_2(t_2)} = \square\},$$

corresponds to the pair $\mathrm{H}_1 \times \mathrm{H}_2$.

We thus consider the equation $d_1(t)/d_2(t) = x^2$. If the plane curve defined by this equation has infinitely many points then we obtain a required model. Out of 60 pairs, there are 48 curves of genus 0, none of genus 1 and 12 curves of genus greater than 1. Let us illustrate it with an example.

Example 24.5. Let $\mathrm{H}_1 = \mathrm{X}_3 \subset \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\mathrm{H}_2 = 7\mathrm{B}^0\text{-}7a \subset \mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$. Consider

$$\mathrm{H}_1' = \langle \left(\begin{smallmatrix} 2 & 3 \\ 3 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 3 \\ 0 & 3 \end{smallmatrix}\right)\rangle \subset \mathrm{H}_1 \text{ and } \mathrm{H}_2' = \langle \left(\begin{smallmatrix} 4 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 5 & 1 \end{smallmatrix}\right)\rangle \subset \mathrm{H}_2.$$

Note that neither H_1' nor H_2' contains $-\mathrm{I}$. We first compute a model for $\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2}$ using the case where $-\mathrm{I}$ is in both the groups. As both of them contain $-\mathrm{I}$, only j-invariant suffices. We get the following parameterization of the j-invariant.

$$j(t) = \frac{-\left(1494501t^4 + 1198050t^3 + 359905t^2 + 48020t + 2401\right)^3\left(30301t^4 + 24370t^3 + 7337t^2 + 980t + 49\right)}{(5t+1)^2 t^{14}}.$$

We then fix a model E_t with this j-invariant and then compute $d_1(t)$ and $d_2(t)$ by the method as explained in Example 23.5. We obtain $d_1(t) = 2t(5t+1)$ and $d_2(t) = -1$. Note that, these twists are not unique and they depend on the model E_t. In order to compute a model for $\mathrm{E}_{\mathrm{H}_1'\times\mathrm{H}_2'}$, we cannot twist E_t by $d_1(t)$ and $d_2(t)$, as the ratio of $d_1(t)$ and $d_2(t)$ is not a square. So, we consider the curve $2t(5t+1)+x^2$ defined by the equation $d_1(t)/d_2(t) = x^2$. This is a genus 0 curve which we parameterize by $t(s) = -\frac{s^2}{5\,s^2+50}$. Finally, we specialize E_t at $t = -\frac{s^2}{5\,s^2+50}$ and then twist it by -1 to obtain the model.

24.2 Curious cases when the genus is 1

Let $\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2}$ be of genus 1 such that there are infinitely many elliptic curves with distinct j-invariants with Galois image contained in $\mathrm{H}_1 \times \mathrm{H}_2$. One can then ask whether the Galois image is actually *equal* to $\mathrm{H}_1 \times \mathrm{H}_2$ for infinitely many of those curves. In the prime-power case, this is not necessarily true [RZB15, Remark 6.3]. We find 8 similar cases when the level is non-prime-power:

X_5-$3\mathrm{A}^0$-$3a$,	X_5-$3\mathrm{C}^0$-$3a$,	X_5-$3\mathrm{D}^0$-$3a$,	X_5-$3\mathrm{D}^0$-$3a\mathrm{T}1$
$3\mathrm{A}^0$-$3a$-$5\mathrm{A}^0$-$5a$,	X_5-$9\mathrm{B}^0$-$9a$,	X_5-$9\mathrm{B}^0$-$9a\mathrm{T}1$,	X_5-$9\mathrm{B}^0$-$9a\mathrm{T}2$.

The subtlety lies in the fact that Hilbert's irreducibility principle holds in the genus 0 case and does not necessary hold when the genus is 1.

We prove it for X_5-$3\mathrm{A}^0$-$3a$ below. The other cases have similar proofs. The codes of verification can be found at [BS19b].

Theorem 24.6. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve such that* $\mathrm{Im}\rho_{\mathrm{E},2} \subset \mathrm{X}_5$ *and* $\mathrm{Im}\rho_{\mathrm{E},3} \subset 3\mathrm{A}^0$-$3a$. *Then* $\mathrm{Im}\rho_{\mathrm{E},2} \subset \mathrm{X}_{17}$ *and* $\mathrm{Im}\rho_{\mathrm{E},3} \subset 3\mathrm{C}^0$-$3a$ *where* $\mathrm{X}_{17} \subset \mathrm{X}_5$ *and* $3\mathrm{C}^0$-$3a \subset 3\mathrm{A}^0$-$3a$.

Proof. Let j_{E} be the j-invariant of E. As $\mathrm{Im}\rho_{\mathrm{E},2} \subset \mathrm{X}_5$, there exists $t \in \mathbb{Q}$ such that $j_{\mathrm{E}} = 2t^2 + 1728$ and as $\mathrm{Im}\rho_{\mathrm{E},3} \subset 3\mathrm{A}^0$-$3a$, there exists $s \in \mathbb{Q}$ such that $j_{\mathrm{E}} = s^3$. Let E' be the curve defined by $2y^2 = x^3 - 1728$. Note that (s,t) is a point on E'. One sees from [SZ17] that the modular curve X_{17} can be parameterized by setting

$$j = \frac{32\left(\theta^2+6\right)^3}{\left(\theta^2-2\right)^2},$$

where θ is a rational parameter. Thus in order to prove that $\mathrm{Im}\rho_{\mathrm{E},2} \subset \mathrm{X}_{17}$, it suffices to prove that

$$2t^2 + 1728 = s^3 = \frac{32\left(\theta^2+6\right)^3}{\left(\theta^2-2\right)^2}$$

for some $\theta \in \mathbb{Q}$, or equivalently, that there exists $\theta \in \mathbb{Q}$ such that

$$t = \frac{4\theta(\theta^2-18)}{\theta^2-2}.$$

Let E'' be the elliptic curve defined by $4y^2 = x^3 + 8$ and consider the following map.

$$\begin{array}{rcl} f\colon \mathrm{E}'' & \longrightarrow & \mathrm{E}' \\ (x,y) & \mapsto & \left(\frac{2(x^3+32)}{x^2}, \frac{4y(y^2-18)}{y^2-2}\right) \end{array}$$

One sees that f is a rational map defined over E'' and $f(x,y) \in \mathrm{E}'$ for all $(x,y) \in \mathrm{E}''$. So using Theorem 1.11, f is a morphism. As f is non-constant, using Theorem 1.12, f is surjective. In particular, as $(s,t) \in \mathrm{E}'$, there exists $\theta \in \mathbb{Q}$ such that

$$t = \frac{4\theta(\theta^2-18)}{\theta^2-2}.$$

This forces $\mathrm{Im}\rho_{\mathrm{E},2}$ to be in the group X_{17}.

Now we prove that $\mathrm{Im}\rho_{\mathrm{E},3} \subset 3\mathrm{C}^0$-$3a$ in a similar way as above. In this case, it suffices to prove that

$$2t^2 + 1728 = s^3 = \frac{(\mu+3)^3(\mu-9)^3}{\mu^3}$$

for some $\mu \in \mathbb{Q}$, or equivalently, that there exists $\mu \in \mathbb{Q}$ such that

$$s = \frac{(\mu+3)(\mu-9)}{\mu}.$$

Let E''' be the elliptic curve defined by $2y^2 = x^3 - 18x^2 - 27x$ and consider the following map.

$\mathrm{H}_1 \times \mathrm{H}_2$	$\mathrm{H}'_1 \times \mathrm{H}'_2$
X_5-3A^0-3a	X_{17}-3C^0-3a
X_5-3C^0-3a	X_{17}-3C^0-3a
X_5-3D^0-3a	X_{17}-3D^0-3a
X_5-3D^0-3aT1	X_{17}-3D^0-3aT1
3A^0-3a-5A^0-5a	3A^0-3a-5E^0-5a
X_5-9B^0-9a	X_{17}-9B^0-9a
X_5-9B^0-9aT1	X_{17}-9B^0-9aT1
X_5-9B^0-9aT2	X_{17}-9B^0-9aT2

Table 24.1: $\mathrm{H}_1 \times \mathrm{H}_2$ and the subgroup $\mathrm{H}'_1 \times \mathrm{H}'_2$ such that the points on the modular curve $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_2}$ exist on the modular curve $\mathrm{X}_{\mathrm{H}'_1 \times \mathrm{H}'_2}$.

$$\begin{array}{rcc} g\colon \mathrm{E}''' & \longrightarrow & \mathrm{E}' \\ (x,y) & \mapsto & \left(\frac{(x+3)(x-9)}{x}, \frac{y(x^2+27)}{x^2}\right) \end{array}$$

Using a similar argument as above, we obtain the result. We represent the maps f and g below.

$$\begin{tikzcd} 4y^2 = x^3 + 8 \arrow[dr, "y \mapsto \frac{4y(y^2-18)}{y^2-2}"'] & & 2y^2 = x^3 - 18x^2 - 27x \arrow[dl, "x \mapsto \frac{(x+3)(x-9)}{x}"] \\ & 2y^2 + 1728 = x^3 & \end{tikzcd}$$

□

24.3 The case $\mathrm{H}_1 \times \mathrm{H}_2 \times \mathrm{H}_3$

According to the results in the tables of Cummins and Pauli [CP03], we must have $\{\ell_1, \ell_2, \ell_3\} = \{2, 3, 5\}$ or $\{2, 3, 7\}$. Since we consider first the case of maximal subgroups, we have to test only the case where the levels of $\mathrm{H}_1, \mathrm{H}_2$ and H_3 are equal to 2, 3, 5 respectively or 2, 3, 7 respectively. In each case, we consider only those triples of groups $\mathrm{H}_1, \mathrm{H}_2, \mathrm{H}_3$ where the genus of $\mathrm{X}_{\mathrm{H}_i \times \mathrm{H}_j}$ is either 0 or 1.

- The case of levels 2, 3 and 5: We start with triples $\mathrm{H}_1, \mathrm{H}_2$ and H_3 of levels 2, 3 and 5 respectively such that each H_i is maximal and all three curves defined by $\mathrm{X}_{\mathrm{H}_i \times \mathrm{H}_j}$ for all distinct i, j have infinitely many rational points. There are precisely 3 such triples: (X_6, 3A^0-3a, 5B^0-5a), (X_5, 3A^0-3a, 5A^0-5a) and (X_5, 3A^0-3a, 5C^0-5a).
  - The first two cases are simple to treat as there is at least a pair $(\mathrm{H}_1, \mathrm{H}_2)$ such that $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_2}$ has genus 0. In this case, let $j = j_{1,2}(t)$ be its parameterization and $j_3(s)$ be a parameterization of $\mathrm{X}_{\mathrm{H}_3}$. We consider the curve defined by $j_{1,2}(t) - j_3(s) = 0$ and verify that it is of genus higher than 1.
  - In the third case, all the curves $\mathrm{X}_{\mathrm{H}_i \times \mathrm{H}_j}$, with $1 \leq i \neq j \leq 3$ have genus 1 and rank 1. We consider the j-invariant associated with $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_3}$ which is $j_{1,3}(x,y) = -\frac{8000\left(40\,x^2-10\,xy+y^2\right)^3(2\,x+y)y^3}{\left(20\,x^2-y^2\right)^5}$, where (x,y) are points on the

Level N	$-\mathrm{I} \in \mathrm{H}$	$-\mathrm{I} \notin \mathrm{H}$	Total	Reference
$\mathrm{N} \in \{2, 4, 8, 16, 32\}$	194	1006	1200	[RZB15]
$\mathrm{N} \in \{3, 9, 27\}$	21	25	46	[SZ17], [Zyw15a] and Table 26.1
$\mathrm{N} \in \{5, 25\}$	12	10	22	[SZ17], [Zyw15a] and Table 26.2
7	6	8	14	[SZ17], [Zyw15a]
11	1	0	1	[SZ17], [Zyw15a]
13	6	4	10	[SZ17], [Zyw15a]
$\mathrm{N} \in \{6, 12, 18, 24, 36, 48, 72\}$	50	114	164	[BS19a]
$\mathrm{N} \in \{10, 20, 40\}$	19	20	39	[BS19a]
$\mathrm{N} \in \{14, 28, 56\}$	4	20	24	[BS19a]
104	3	4	7	[BS19a]
15	4	0	4	[BS19a]
21	1	0	1	[BS19a]
Total	321	1211	1532	

Table 24.2: Families with exceptional cartesian Galois images

elliptic curve $\mathrm{E} : y^2 - 5xy + \frac{125}{4}y = x^3 + \frac{15}{2}x^2 + \frac{2625}{16}x$. On the other hand, $\mathrm{X}_{\mathrm{H}_2}$ is also of genus 0 and its j-invariant can be parameterized by $j_3(s) = s^3$. If there are infinitely many points on $\mathrm{X}_{\mathrm{H}_1 \times \mathrm{H}_2 \times \mathrm{H}_3}$ then $j_{1,3}(x, y)$ must be a cube infinitely many often. It is equivalent to saying $\left(20\,x^2 - y^2\right)(2\,x + y)$ must be a cube infinitely often when (x, y) vary on E. We thus consider $\mathrm{Res}_x\left(t^3 - \left(20\,x^2 - y^2\right)(2\,x + y), \mathrm{E}\right)$. This curve is of genus 5.

Thus in all these case, we have the resulting curves of higher genus. Thus there are no new families, and we do not need to consider non-maximal subgroups.

- In the case of levels 2, 3 and 7, for each triple of maximal subgroups, at least two families intersect in a finite number of points, hence the intersection of three families is always finite.

We describe these families in Table 24.2. There are 1532 with exceptional cartesian Galois images. Thus adding 1 for $\mathrm{GL}_2(\hat{\mathbb{Z}})$ and removing 8 families which lift from Section 24.2, we obtain 1525 possible distinct cartesian images.

Theorem 24.7. *There are exactly* 1525 *subgroups of* $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ *which are cartesian and occur as Galois images* $\mathrm{Im}\rho_{\mathrm{E}}$ *for infinitely many rational elliptic curves* E *with distinct* j*-invariants.*

The list of these models is available at [BS19b].

24.4 Identifying previously known families

In the set of 1525 families from Theorem 24.7, we find previously known families from the literature. These families with their labels are given in Table 26.3. The scripts of verifications are available at [BS19b]. We describe Table 26.3.

row 1. The Montgomery and the twisted Edwards form are birationally equivalent due to Theorem 3.2 in [BBJ+08].

row 2. One can directly compute the function field of 4-torsion points as an extension of $\mathbb{Q}(d)$ and obtain the the Galois image is contained in that of X_{13f}. Conversely, any curve of X_{13f} can be put in twisted Edwards form with $a = -1$.

row 3. The group corresponding to X_{13h} is $\{\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})\}$, which corresponds to the elliptic curves having a rational point of order 4. Theorem 3.3 of [BBJ+08] states that an elliptic curve can be put in twisted Edwards' form such that $a = \square$ if, and only if, it has a rational point of order 4. X_{13h} does have a point of order 4 and can be put in twisted Edwards' form with $a = \square$.

row 4. Theorem 5.4 of [BCKL15] ensures that a curve is isogenous to a twisted Hessian curve if, and only if, it is isogenous to a curve having a point of order 3. The family $3\mathrm{B}^0$-$3a$ corresponds to the group $\{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})\}$, which characterizes curves isogenous to a curve with a point of order 3.

row 5. On page 262 of [Mon87], we have a description of the Suyama family as Montgomery curves $\mathrm{M}_{\mathrm{A,B}}$ for which there exist $x_3, y_3 \in \mathbb{Q}$ such that $\mathrm{A} = (-x_3^3 - 6x_3^3 + 1)/(4x_3^3)$ and $\mathrm{B} = (x_3 - 1)^2/(4x_3y_3^2)$. These equations force $\mathrm{M}_{\mathrm{A,B}}$ to have a point of order 3. Hence, the Suyama family is equivalent to the intersection of X_{13} (Montgomery form) and $3\mathrm{B}^0$-$3a\mathrm{T}2$ (point of order 3).

rows 6. to 11. These rows consider families which parameterize the elliptic curves having a point of order n for $n = 5, 7, 8, 9, 10, 11, 12$.

row 12. To our knowledge, this family is not reported to be used in ECM, it is listed here for reference in the following rows.

row 13. Montgomery noted that every elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ can be put in Montgomery form, and can therefore be put in twisted Edwards form. This shows that the parameterizations of [AM93], [Mon92] and [BBLP13] describe the same set of elliptic curves. We also have that the family of Section 2.3.2 in [HMR16] is the same family in disguise.

rows 14. In Sections 3.1 (resp. 3.5, 3.7) of [BC10], we have parameterizations of the curves E such that $\mathrm{E}[n](\mathbb{Q}(\zeta_n)) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ for $n = 3$ (resp. 4, 5). The Galois image in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ has order $\varphi(n)$ and surjective determinant, so the corresponding group is $\{\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \mid a \in (\mathbb{Z}/n\mathbb{Z})^*\}$. We identify these groups as corresponding to $3\mathrm{D}^0$-$3a\mathrm{T}1$, X_{58i} and respectively $5\mathrm{H}^0$-$5a\mathrm{T}1$.

row 15. In the previous paragraph, we explained how to identify the Galois image. We obtain that the family in Section 3.2 of [BC10] and the family in Section 3.5.1 of [HMR16] coincide.

row 16. The family of Section 3.5 of [BC10] and Section 3 of [BBL10] are the same. It is interesting to note that this family is not equal to that of row 12. Indeed, the condition $a = -\square$ which was imposed in order to improve the arithmetic cost, also improved the smoothness properties.

row 17. Section 3.7 of [HMR16] and Table 26.2 give the same parameterization:

$$a(t) = -27t^{20} - 6156t^{15} - 13338t^{10} + 6156t^5 - 27$$

$$b(t) = 54t^{30} - 28188t^{25} - 540270t^{20} - 540270t^{10} + 28188t^5 + 54.$$

rows 18. and 19. The families Suyama-11 and Suyama-9/4 are obtained from Suyama by imposing additional conditions. For Suyama-11 the condition on a Montgomery curve $\mathrm{M}_{\mathrm{A,B}}$ is $(\mathrm{A}+2)/\mathrm{B} = -\square$, which in Edwards coordinates $\mathrm{E}_{\mathcal{E},,a,d}$ is $a = -\square$. Hence, Suyama-11 is the intersection of X_{13f} and $3\mathrm{B}^0$-$3a\mathrm{T}2$. Similarly, the family Suyama-9/4 is obtained from Suyama by the additional condition on $\mathrm{M}_{\mathrm{A,B}}$ is $\mathrm{B} = \square$, or equivalently in Edwards coordinates $\mathrm{E}_{\mathcal{E},,a,d}$ the condition is $a - d = \square$. The unique twist of X_{13} such that $a-d$ is a square for all elements of the parameterization is X_{13d}. Hence, Suyama-9/4 is the intersection of X_{13d} and $3\mathrm{B}^0$-$3a\mathrm{T}2$.

rows 20. to 23. Section 18.1 identified the families of these rows as corresponding to parameterizations of some subgroups H. to identify the label we tested several numerical curves in the families of [BBB+13] and computed the Galois group of $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[8])/\mathbb{Q})$.

24.5 New families with better arithmetic

We mentioned that in ECM, one uses curves with better arithmetic properties. We consider intersecting the families with better values of α with the ones with better arithmetic.

Example 24.8 (A new family)**.** It is known that the family of elliptic curves with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and the family of twisted Edwards' curves with $a = -1$ do not intersect. There are however four families which have the same value of α as the one with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and which are also of the form twisted Edwards' with $a = -1$. One of them is X_{192i} in [RZB15] and can be transformed into twisted Edwards' form by choosing

$$a = -1, \qquad d = -\frac{\left(t^2+4\right)^4}{64\left(t^2-4\right)^2 t^2}.$$

The other families are X_{189d}, X_{207n} and X_{211m}.

25 Local-global problems for elliptic curves

Some local-global problems for elliptic curves have been considered by various authors. For example, in [Kat80], Katz considers the local-global problem for torsion.
Problem K: Let E be a rational elliptic curve and let $m \geq 2$ be an integer. Suppose that the congruence

$$\#\mathrm{E}(\mathbb{F}_p) \equiv 0 \mod m$$

holds for all but finitely many primes p. Does there exist a rational elliptic curve E' isogenous to E such that

$$\#\mathrm{E}(\mathbb{Q})_{\mathrm{tors}} \equiv 0 \mod m?$$

Sutherland in [Sut12a] considers the problem for isogenies.
Problem S: Let E be a rational elliptic curve and let ℓ be a prime. Suppose that E

admits an isogeny of degree ℓ over $\mathbb{F}_p$ for all but finitely many primes p. Does E admits an isogeny of degree ℓ over $\mathbb{Q}$?

We are interested in these problems as they are pertinent to ECM. Indeed, its the local smoothness properties of a curve E determine whether E is ECM-friendly or not. Furthermore, Problem K also explains why some curves E have large values of $v_\ell(\mathrm{E})$ without having large torsion over $\mathbb{Q}$.

Katz himself answered Problem K affirmatively in the same paper, [Kat80, Theorem 1]. Sutherland proved that Problem S admits an affirmative answer if $\ell < 7$ or $\ell \equiv 1 \bmod 4$. He found the only counter example for $\ell = 7$. Later, Anni in [Ann14] solved Problem S over number fields.

Example 25.1. Let E be an elliptic curve from [Sut12a] of j-invariant $\frac{2268945}{128}$. Then E admits an isogeny of degree 7 over $\mathbb{F}_p$ for all primes of good reduction for E. However E does not admit an isogeny over $\mathbb{Q}$.

In this section, we look for infinite families of elliptic curves which satisfy the condition of Problem K for prime power values of m.

Definition 25.2. Let $\mathrm{E}/\mathbb{Q}$ be an elliptic curve and ℓ a prime. We say the pair (E, ℓ) is Katzian if the valuation $v_\ell(\#\mathrm{E}(\mathbb{F}_p)) \geq i$ for all but finitely many primes p and $v_\ell(\#\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}) \leq j$ for some integers $j < i$.

Example 25.3. We proved in Lemma 13.2, a generic Montgomery curve E has a point of order 2 over $\mathbb{Q}$ however $\#\mathrm{E}(\mathbb{F}_p)$ is always a multiple of 4. Thus, Montgomery curves are Katzian for $\ell = 2$.

In order to find Katzian curves, it suffices look at possible mod m Galois images as we illustrate now.

25.1 Finding Katzian curves

For an elliptic curve E and $m \geq 2$, let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ such that $\mathrm{Im}\rho_{\mathrm{E},m}$ is conjugated to H. We denote the subgroup of $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ fixed by $h \in \mathrm{H}$ by $\mathrm{Fix}(h)$. Consider the minimum μ of the following set.

$$\mathcal{F}_{\mathrm{H}} := \{\#\mathrm{Fix}(h) \mid h \in \mathrm{H}\}.$$

By the arguments presented in the proof of Theorem 14.3, μ divides $\#\mathrm{E}(\mathbb{F}_p)$ for all primes p where E has good reduction. The essential idea is the fact that the Galois group of $\mathbb{F}_p(\mathrm{E}[m])$ fixes the base field $\mathbb{F}_p$.

Example 25.4. Consider the curve $\mathrm{E} : y^2 = x^3 - 37179x - 2794986$. Note that E does not admit any torsion over $\mathbb{Q}$. Let $m = 9$. We have that $\rho_{\mathrm{E},9}$ is contained in $\mathrm{H} = 9\mathrm{I}^0\text{-}9a\mathrm{T}2$ which is of order 54. We consider fixes of matrices in H. For 45 of them, $\mathrm{Fix}(h)$ is isomorphic to $\mathbb{Z}/9\mathbb{Z}$, for 8 of them it is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and for the identity element, it is $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. As the mod 9 Galois image over $\mathbb{F}_p$ is always contained in H up to conjugacy, $\mathrm{E}(\mathbb{F}_p)$ will always have a subgroup isomorphic to $\mathbb{Z}/9\mathbb{Z}$. Thus $\#\mathrm{E}(\mathbb{F}_p) \equiv 0 \bmod 9$ for all but finitely many primes p. We say the pair $(\mathrm{E}, 3)$ is Katzian. As dictated by [Kat80, Theorem 1], E is indeed isogenous to a curve $\mathrm{E}' : y^2 = x^3 - 17739x + 1205766$ with $\#\mathrm{E}'(\mathbb{Q})_{\mathrm{tors}} = 9$.

We look for infinite families of Katzian curves in the list of 1525 families from Theorem 24.7 to obtain the following.

Theorem 25.5. *Among 1525 families from Theorem 24.7, there are 618 (resp. 11, 2, 1) Katzian families for $\ell = 2$ (resp. $3, 5, 7$). Furthermore, all 618 Katzian curves for $\ell = 2$ are Montgomery.*

These families and the scripts of computations can be found at [BS19b].

26 Comparison with Morrow's work

After the works of [RZB15] and [SZ17], there are only two more steps to solving Mazur's Program B under Serre's conjecture.

1. Finding rational points on the modular curves with odd prime power levels.

2. Considering intersections of modular curves of different prime-power levels.

Motivated by the second step and its applications to ECM, we computed all explicit equations for all the infinite families.

Independently, Morrow computed the list of possible groups in [Mor19] which was published after we completed our computations. Our results corroborate with those of [Mor19]. Theorem A of [Mor19] says that at level 6, there are 6 possible images of $\rho_{\mathrm{E},6}$. Starting with these 6 images, the author considers the subgroups of these images of level 12, 24 and 48 and finds that there are 5, 6 and 4 infinite families of these levels respectively (cf. [Mor19, Table 1]). In each case, the author provides the equations of modular curves. The author also considers modular curves having higher genera and computes rational points on some of them using different methods.

Naturally the subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell_1^m\ell_2^n\mathbb{Z})$ having surjective projection mod ℓ_1 or mod ℓ_2 are not considered. For example, the family X_3-$3\mathrm{B}^0$-$3a$ does not appear in [Mor19] as its mod 2 projection is surjective on $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

We on the other hand consider all possible combinations of maximal subgroups of $1\mathrm{A}^0$-$1a$ and compute the modular curves of possible cartesian products having genera 0 or 1.

Dictionary between two works

For a group coming from [Mor19, Theorem A], we give the corresponding group from [BS19a] in Table 26.8. The equivalence of models can be verified using the scripts available at [BS19b].

Equipped with his results, Morrow considers non-cartesian i.e. entanglement subgroups (see Def. 24.1) which can occur as Galois images and proves that there are only 2 non-abelian entanglement at level 6.

Entanglement

Consider the curve $\mathrm{E}/\mathbb{Q}$ defined by $y^2 = x^3 - 36x + 84$. For this curve $\rho_{\mathrm{E},2}$ and $\rho_{\mathrm{E},3}$ are both surjective. One might expect $\rho_{\mathrm{E},6}$ to be surjective as well. However it is not the case, as the discriminant of E is of form $-3 \cdot \square$. Then as $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3) \subset \mathbb{Q}(\mathrm{E}[2]) \cap \mathbb{Q}(\mathrm{E}[3])$, $\rho_{\mathrm{E},6}$ is not surjective. In this case the mod 6 Galois image $\mathrm{Im}\rho_{\mathrm{E},6}$ is an entanglement subgroup in the sense of Def. 24.1. In fact, E belongs to a family presented by [BJ16]. They proved that for every non-CM elliptic curve with j-invariant of the form $2^{10}3^3t^3(1-4t^3)$, $\mathrm{Im}\rho_{\mathrm{E},6}$ is an entanglement subgroup.

Lemma 26.1. *Let* $\mathrm{E}/\mathbb{Q}$ *be an elliptic curve without complex multiplication. Let* m, n *be two coprime integers. Then* $\mathrm{Im}\rho_{\mathrm{E},mn} \subset \mathrm{GL}_2(\mathbb{Z}/mn\mathbb{Z})$ *is an entanglement subgroup if, and only if,*

$$\mathbb{Q}(\mathrm{E}[m]) \cap \mathbb{Q}(\mathrm{E}[n]) \neq \mathbb{Q}.$$

Proof. It is straightforward as $[\mathrm{GL}_2(\mathbb{Z}/mn\mathbb{Z})\colon \mathrm{Im}\rho_{\mathrm{E},mn}] = [\mathbb{Q}(\mathrm{E}[mn]) : \mathbb{Q}]$ and as $\mathbb{Q}(\mathrm{E}[mn])$ is the compositum of $\mathbb{Q}(\mathrm{E}[m])$ and $\mathbb{Q}(\mathrm{E}[n])$. □

Generally, the Galois images, which are non-abelian entanglement subgroups, are interesting. In this work, we came across two families of curves whose mod 6 Galois images are abelian entanglement subgroups.

Abelian entanglement at level 6

Consider $\mathrm{H}_1 = \mathrm{X}_6$ and $\mathrm{H}_2 = 3\mathrm{D}^0\text{-}3a$. The both contain $-\mathrm{I}$ and the modular curve $\mathrm{X}_{\mathrm{H}_1\times\mathrm{H}_2}$ can be parameterized by setting

$$j(t) = \frac{\left(t^6 - 6\,t^5 + 36\,t^4 + 8\,t^3 - 24\,t^2 + 16\right)^3\left(t^3 + 6\,t^2 + 4\right)^3\left(t^3 + 4\right)^3}{\left(t^2 + 2\,t + 4\right)^6\left(t^2 - t + 1\right)^3(t+1)^3(t-2)^6t^6}.$$

Let E_t be an elliptic curve with the j-invariant $j(t)$. We have that $\mathrm{Im}\rho_{\mathrm{E}_t,2} \subset \mathrm{X}_6$ and $\mathrm{Im}\rho_{\mathrm{E}_t,3} \subset 3\mathrm{D}^0\text{-}3a$.

Now consider the lift H of $\mathrm{H}_1 \times \mathrm{H}_2$ in $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$. With the choice of generators in [BS19b], H can be generated by $\left(\begin{smallmatrix}5&0\\0&5\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}4&3\\3&2\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}2&3\\3&2\end{smallmatrix}\right)$. So $\mathrm{Im}\rho_{\mathrm{E}_t,6} \subset \mathrm{H}$.

There are four index 2 subgroups H with surjective determinant, say $\mathrm{G}_1, \mathrm{G}_2, \mathrm{G}_3$ and G_4, of H which do not contain $-\mathrm{I}$. We verify that G_1 is conjugated to G_2 and G_3 is conjugated to G_4. On the other hand, by Lemma 23.4, there exist 4 quadratic twists of E_t, say $\mathrm{E}_{t,1}$, $\mathrm{E}_{t,2}$, $\mathrm{E}_{t,3}$ and $\mathrm{E}_{t,4}$ such that $\mathrm{Im}\rho_{\mathrm{E}_{t,i},6} \subset \mathrm{G}_i$ for all $i \in \{1,2,3,4\}$.

We further observe that G_3 and G_4 are not cartesian and correspond to a curves which admit abelian entanglement at level 6. For example, the following curve admits an entanglement at level 6,

$$y^2 = x^3 - x^2 - 2273x - 33439.$$

The explicit models and generators of subgroups can be found in [BS19b]. We summarize.

Proposition 26.2. *Let* $t \neq -1, 2$ *be a rational number. Let* E *be the elliptic curve defined by* $y^2 = x^3 + a(t) + b(t)$, *where*

$$\begin{aligned}
a(t) &= -3\left(t^3+1\right)^2\left(t^6 - 6\,t^5 + 36\,t^4 + 8\,t^3 - 24\,t^2 + 16\right)\left(t^3 + 6\,t^2 + 4\right)\left(t^3 + 4\right),\\
b(t) &= -2\left(t^3+1\right)^3\left(t^8 + 8\,t^7 + 64\,t^6 - 16\,t^5 - 56\,t^4 + 128\,t^3 + 64\,t^2 - 64\,t + 64\right)\left(t^4 - 2\,t^3 + 6\,t^2 + 4\,t + 4\right)\\
&\quad\left(t^4 - 8\,t^3 - 8\,t - 8\right)\left(t^2 + 2\,t - 2\right).
\end{aligned}$$

Let E_3 *be the quadratic twist of* E *by 3. Then*

$$\mathbb{Q}(\mathrm{E}[2]) \subset \mathbb{Q}(\mathrm{E}[3]) \text{ and } \mathbb{Q}(\mathrm{E}_3[2]) \subset \mathbb{Q}(\mathrm{E}_3[3])$$

Proof. We shall prove it for E. The proof for E_3 is similar. Let ψ_2 and ψ_3 be the second and the third division polynomial respectively of E. Note that ψ_3 has two linear factors

and a quadratic factor which splits on $\mathbb{Q}(\zeta_3)$ where ζ_3 is a primitive third root of unity. We have the following 4 roots of ψ_3 over $\mathbb{Q}(\zeta_3)$.

$$\begin{aligned}
\theta_1 &= -\left(t^3+1\right)\left(t^3+6\,t^2+4\right)^2 \\
\theta_2 &= 3\left(t^3+1\right)\left(t^3+4\right)^2 \\
\theta_3 &= \left(t^3+1\right)\left(t^3-6\,(\zeta_3+1)\,t^2+4\right) \\
\theta_4 &= -\left(t^3+1\right)\left(t^3+6\,\zeta_3 t^2+4\right)^2
\end{aligned}$$

For each root θ_i, we obtain that $\psi_2(\theta_i) = \left(t^3+1\right)\cdot s^2$ for some $s \in \mathbb{Q}(\zeta_3)$. So we deduce that

$$\mathbb{Q}(\mathrm{E}[3]) = \mathbb{Q}(\zeta_3, \sqrt{t^3+1}).$$

On the other hand, ψ_2, whose roots correspond to the x-coordinates of points in $\mathrm{E}[2]$, has a quadratic factor with discriminant $(t^3+1)\cdot\square$. So ψ_2 splits completely in $\mathbb{Q}(\mathrm{E}[3])$ and we have

$$\mathbb{Q}(\mathrm{E}[2]) \subset \mathbb{Q}(\mathrm{E}[3]).$$

$\square$

Conclusion and further topics

The purpose of this project was to classify ECM-friendly families of rational elliptic curves and compare their efficiencies. We first discussed methods to prove the surjectivity of the mod ℓ Galois representation $\rho_{\mathrm{E},\ell}$ attached to an elliptic curve E as it permits to eliminate the curve in ECM. We then considered the resolvent method of computing Galois groups and the subfields of function fields approach. These approaches produced a few new families and allowed us to rediscover some previously known.

The powerful theory of modular curves allows us to treat the problem of finding ECM-friendly curves in its generality. We continued in this direction using recent progress on Mazur's Program B and proved, with a technical hypothesis, that there are 1525 possible infinite families of ECM-friendly rational elliptic curves. As this work attempts at bridging the gap between the worlds of cryptography and modular curves and as we believe that the ultimate solution to Mazur's Program B would be an algorithmic one, we dedicated a substantial portion of this work in giving explicit, ready to use, equations of ECM-friendly families which can be found in the online complement of this work.

Equipped with these families, we defined a tool α that enables us compare the efficiency of these families in ECM. We perform several experiments with α and noticed that α, even though it does not take into account the entanglement, is a reliable tool when it comes to assess the ECM-friendliness of a curve. We also give the values of α for these families over chosen number fields and decide whether they admit good arithmetic properties known so far.

Concretely speaking, we have answered the following questions.

1. Given a rational elliptic curve E, is there a fast algorithm to determine the image of $\rho_{\mathrm{E},\ell}$? If $\rho_{\mathrm{E},\ell}$ is surjective, we give a new algorithm and analyse an old one to prove surjectivity in Chapter 2. Sutherland has proposed a fast local-global algorithm to compute Galois images, but in some cases it cannot decide between two possible images. Thanks to the complete classification in Chapter 6, we finally have a fast algorithm which works in all cases.

2. Is there an algorithm to compute all families of ECM-friendly curves? For theoretical purposes, one can answer affirmatively thanks to Chapter 4. For practical reasons, one can compute a complete (and finite) list of modular curves by the algorithm described in Chapter 5. In the case of the field of rational numbers, we find the complete list of infinite families. In the case of number fields, it remains the question of finding rational points on the modular curves, which is easy in practice but it is not known to be algorithmic (Hilbert's 10th problem).

3. Is there a model governing the smoothness probability in ECM, i.e. given an elliptic curve E and parameters B and $\log_2 p$, predict the probability that $\#\mathrm{E}(\mathbb{F}_p)$ is B-smooth? We propose such a model in Chapter 3 and test it experimentally.

4. Is it possible that the probabilities of $\#\mathrm{E}(\mathbb{F}_p)$ being divisible by m and m' are correlated ? We answer this question in Chapter 6.

5. Montgomery curves have 2 rational torsion points but 4 over any finite field. Are there other such families? We answer this in Chapter 6.

In future, one could consider the following directions.

1. Solve Mazur's Program B over well-chosen number fields of smaller degree.

2. Consider curves having the torsion point fields with the smallest degree possible. This idea is inspired by the works (see [GJLR15]) of Enrique and Álvaro.

3. Consider not only the average but the variance of $\mathrm{val}_\ell(\#\mathrm{E}(\mathbb{F}_p))$ for varying primes p. This idea is proposed by Paul Zimmerman. One could also consider how the exponent of $\#\mathrm{E}(\mathbb{F}_p)$ varies with p. It is inspired by the works by Bernstein.

4. Consider the splitting of primes in torsion point fields as it contains information about the structure of $\mathrm{E}(\mathbb{F}_p)$.

5. We obtain a new family better suitable to find primes $p \equiv 1 \bmod 5$. We believe this family can be put into a special form for which the multiplication by 5 would be substantially less expensive. One would consider finding that parameterization.

6. Define finer tools than α which would take into account entanglements.

Tables

label	parameterization
3B0-3aT1 3B0-3aT2	$a = -3(t+3)(t-27)^3,$ $b = -2(t^2+18t-27)(t-27)^4$
3D0-3aT1	$a = -3(t^2-6t+36)(t+6)t,$ $b = -2(t^2-6t-18)(t^4+6t^3+54t^2-108t+324)$
9B0-9aT1 9B0-9aT2	$a = -3(t^3+9t^2+27t+3)(t+3),$ $b = (-2t^6-36t^5-270t^4-1008t^3-1782t^2-972t+54)$
9C0-9aT1 9C0-9aT2	$a = -3(t^3+3)(t^2-3t+9)^3(t+3)^3,$ $b = -2(t^6+18t^3-27)(t^2-3t+9)^4(t+3)^4$
9H0-9aT1	$a = -3(t^3+9)(t^3+3)(t^2+3t+3)(t^2-3t+3)(t^2+3),$ $b = -2(t^{12}+18t^9+162t^6+486t^3+729)(t^4+3t^2+9)(t^2-3)$
9H0-9bT1 9H0-9bT2	$a = -3(t^6-18t^5+171t^4+180t^3-297t^2-162t+189)(t^3+9t^2-9t-9)(t^3-3t^2-9t+3),$ $b = -2(t^{12}+126t^{10}-1944t^9+6723t^8+23328t^7-21708t^6-58320t^5+34263t^4+54432t^3$ $-24786t^2-17496t+9477)(t^6-18t^5-45t^4+180t^3+135t^2-162t-27)$
9H0-9cT1	$a = 144(t^6+9t^5+9t^4-90t^3+27t^2+81t+27)(t+3)(t+1)(t-1)(t-3)t,$ $b = 16(t^{12}+18t^{11}+126t^{10}-18t^9-2025t^8-972t^7+13284t^6-2916t^5-18225$ $t^4-486t^3+10206t^2+4374t+729)(t^2+6t-3)(t^2-6\,t-3)(t^2-3)$
9I0-9aT1 9I0-9aT2	$a = -3(17t^9+9t^8-144t^6-918t^5+810t^4-3672t^3-648t^2-4131t-27)(t^3+3t^2-9t-3),$ $b = 142t^{18}+684t^{17}-162t^{16}-10944t^{15}-10152t^{14}+24624t^{13}$ $-131976t^{12}+393984t^{11}+834948t^{10}-1128600t^9+1628100t^8-7978176t^7+$ $12435768t^6-4210704t^5+14154264t^4+12410496t^3+8314974t^2+498636t-1458$
9I0-9bT1 9I0-9bT2	$a = -144(t^3+9t^2-9t+15)(t^3+9t+6)(t^3-3)(t+1)(t-1),$ $b = 16(t^6+12t^5+27t^4+48t^3-9t^2-108t-99)$ $(t^6+12t^5-9t^4+12t^3-9t^2+9)(t^6-6t^5+63t^4-132t^3+207t^2-54t-207)$
9I0-9cT1 9I0-9cT2	$a = -3(t^9-9t^8+27t^7-48t^6+54t^5-45t^4+27t^3-9t^2+1)(t^3-3t^2+1),$ $b = -2t^{18}+36t^{17}-270t^{16}+1140t^{15}-3114t^{14}+5940t^{13}-8256t^{12}+8460t^{11}$ $-6480t^{10}+4064t^9-2718t^8+2160t^7-1470t^6+612t^5-54t^4-84t^3+36t^2-2$
9J0-9aT1 9J0-9aT2	$a = -3(t^9-9t^7+6t^6+18t^5-9t^4-27t^3+27t^2-9t+1)(t^3+3t^2-6t+1)^3(t^2-t+1),$ $b = -2(t^{18}-18t^{16}+24t^{15}+81t^{14}-198t^{13}-30t^{12}+540t^{11}-828t^{10}+884t^9-729t^8$ $-180t^7+1491t^6-1944t^5+1341t^4-552t^3+135t^2-18t+1)(t^3+3t^2-6t+1)^4$
9J0-9bT1 9J0-9bT2	$a = -3(t^9-9t^8-1800t^6-54t^5+5022t^4-216t^3-5184t^2-243t+1971)$ $(t^3-9t^2-9t+9)^3(t^2+3),$ $b = -2(t^{18}-18t^{17}+81t^{16}+4176t^{15}-37692t^{14}-12312t^{13}-559980t^{12}-208656t^{11}$ $+2381886t^{10}-184140t^9-4348242t^8+1154736t^7+6764148t^6+635688t^5-8021916t^4$ $-2321136t^3+5447817t^2+931662t-1363959)(t^3-9t^2-9t+9)^4$
9J0-9cT1 9J0-9cT2	$a = -3(5t^3-9t^2-9t-3)(t^3+9t^2+27t+3)(t^3-9t+12)(t^2+3)(t+3)^3(t-3)^3t^3,$ $b = 2(11t^6-6t^5-63t^4+156t^3-99t^2-54t-9)(t^6+6t^5-9t^4-12t^3-225t^2+486t+9)$ $(t^6+6t^5-48t^3-63t^2-54t-18)(t+3)^4(t-3)^4t^4$
27A0-27aT1 27A0-27aT2	$a = -3(t^9+9t^6+27t^3+3)(t^3+3),$ $b = -2t^{18}-36t^{15}-270t^{12}-1008t^9-1782t^6-972t^3+54$

Table 26.1: Curves with exceptional Galois images in $\mathrm{GL}_2(\mathbb{Z}_3)$ associated to groups which do not contain $-\mathrm{I}$. For each subgroup H containing $-\mathrm{I}$ we call $\langle$label H$\rangle$T1, $\langle$label H$\rangle$T2, ... the subgroups of H of index 2, up to conjugacy, which do not contain $-\mathrm{I}$. The parameterization (a,b) corresponds to T1 and the parameterization $(9a, -27b)$ corresponds to T2. If H has a unique index two subgroup, up to conjugacy, then the parameterization $(9a, -27b)$ is a second family of Galois group T1.

label	parameterization
5D0-5aT1 5D0-5aT2	$a = -27t^4 - 6156t^3 - 13338t^2 + 6156t - 27,$ $b = 54(t^4 - 522t^3 - 10006t^2 + 522t + 1)(t^2 + 1)$
5D0-5bT1 5D0-5bT2	$a = -27t^4 + 324t^3 - 378t^2 - 324t - 27,$ $b = 54(t^4 - 18t^3 + 74t^2 + 18t + 1)(t^2 + 1)$
5H0-5aT1 5H0-5aT2	$a = -27(t^8 + t^7 + 7t^6 - 7t^5 + 7t^3 + 7t^2 - t + 1)$ $(t^8 - 4t^7 + 7t^6 - 2t^5 + 15t^4 + 2t^3 + 7t^2 + 4t + 1)(t^4 + 3t^3 - t^2 - 3t + 1),$ $b = 54(t^8 + 6t^7 + 17t^6 + 18t^5 + 25t^4 - 18t^3 + 17t^2 - 6t + 1)$ $(t^8 - 4t^7 + 17t^6 - 22t^5 + 5t^4 + 22t^3 + 17t^2 + 4t + 1)$ $(t^8 - t^6 + t^4 - t^2 + 1)(t^4 - 2t^3 - 6t^2 + 2t + 1)(t^2 + 1)$
25B0-25aT1 25B0-25aT2	$a = -27t^{20} - 324t^{15} - 378t^{10} + 324t^5 - 27,$ $b = 54(t^{20} + 18t^{15} + 74t^{10} - 18t^5 + 1)(t^8 - t^6 + t^4 - t^2 + 1)(t^2 + 1)$
25B0-25bT1 25B0-25bT2	$a = -27t^{20} - 6480t^{19} - 58320t^{18} - 181440t^{17} - 473040t^{16} - 816156t^{15} - 1561680t^{14}$ $-1645920t^{13} - 2157840t^{12} - 1121040t^{11} - 1633338t^{10} + 1121040t^9 - 2157840t^8$ $+1645920t^7 - 1561680t^6 + 816156t^5 - 473040t^4 + 181440t^3 - 58320t^2 + 6480t - 27,$ $b = -54(t^{20} - 510t^{19} - 13590t^{18} - 32280t^{17} - 82230t^{16} - 153522t^{15}$ $-302910t^{14} - 273540t^{13} - 412830t^{12} - 268230t^{11} - 262006t^{10} + 268230t^9$ $-412830t^8 + 273540t^7 - 302910t^6 + 153522t^5 - 82230t^4 + 32280t^3 - 13590t^2 + 510t + 1)$ $(t^8 + 6t^7 + 17t^6 + 18t^5 + 25t^4 - 18t^3 + 17t^2 - 6t + 1)(t^2 + 1)$
7B0-7aT1 7B0-7aT2	$a = -27(t^2 + 13t + 49)^3(t^2 + 5t + 1),$ $b = 54(t^4 + 14t^3 + 63t^2 + 70t - 7)(t^2 + 13t + 49)^4$
7E0-7aT1 7E0-7aT2	$a = -27(t^6 + 229t^5 + 270t^4 - 1695t^3 + 1430t^2 - 235t + 1)(t^2 - t + 1),$ $b = 54t^{12} - 28188t^{11} - 483570t^{10} + 2049300t^9 - 3833892t^8 + 7104348t^7$ $-13674906t^6 + 17079660t^5 - 11775132t^4 + 4324860t^3 - 790074t^2 + 27540t + 54$
7E0-7bT1 7E0-7bT2	$a = -432(t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)(t^2 - t + 1),$ $b = 3456t^{12} - 62208t^{11} + 404352t^{10} - 1223424t^9 + 1969920t^8 - 1679616t^7$ $+943488t^6 - 767232t^5 + 601344t^4 - 158976t^3 - 51840t^2 + 20736t + 3456$
7E0-7cT1 7E0-7cT2	$a = -189(5t^2 - t - 1)(3t^2 - 9t + 5)(t^2 - t + 1)(t^2 - 3t - 3),$ $b = -2646(9t^4 - 12t^3 - t^2 + 8t - 3)(3t^4 - 4t^3 - 5t^2 - 2t - 1)(t^4 - 6t^3 + 17t^2 - 24t + 9)$
13B0-13aT1 13B0-13aT2	$a = -3(t^8 + 235t^7 + 1207t^6 + 955t^5 + 3840t^4 - 955t^3 + 1207t^2 - 235t + 1)$ $(t^4 - t^3 + 5t^2 + t + 1)^3,$ $b = -2(t^{12} - 512t^{11} - 13079t^{10} - 32300t^9 - 104792t^8 - 111870t^7$ $-419368t^6 + 111870t^5 - 104792t^4 + 32300t^3 - 13079t^2$ $+512t + 1)(t^4 - t^3 + 5t^2 + t + 1)^4(t^2 + 1)$
13B0-13bT1 13B0-13bT2	$a = -27(t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1)(t^4 - t^3 + 5t^2 + t + 1)^3,$ $b = 54(t^{12} - 8t^{11} + 25t^{10} - 44t^9 + 40t^8 + 18t^7 - 40t^6 - 18t^5 + 40t^4 + 44t^3 + 25t^2 + 8t + 1)$ $(t^4 - t^3 + 5t^2 + t + 1)^4(t^2 + 1)$

Table 26.2: Curves with exceptional Galois image in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for $\ell = 5, 7, 13$ corresponding to groups which do not contain $-\mathrm{I}$. For each subgroup H containing $-\mathrm{I}$ we call ⟨label H⟩T1, ⟨label H⟩T2, ... the subgroups of H of index 2, up to conjugacy, which do not contain $-\mathrm{I}$. Set $\epsilon = 1$ if -1 is a square mod ℓ, -1 otherwise. The parameterization (a,b) corresponds to T1 and the parameterization $(\ell^2 a, \epsilon\ell^3 b)$ corresponds to T2. If H has a unique index two subgroup, up to conjugacy, then the parameterization $(\ell^2 a, \epsilon\ell^3 b)$ is a second family of Galois group T1.

#	Family	label in our tables	comment	$\subset$
1	Section 10.3.1 of [Mon87] Section 2.1 of [BBLP13]	X_{13}	Montgomery form twisted Edwards	
2	Section 1.1 of [BBL10]	X_{13f}	$a = -\square$ twisted Edwards	1
3	Section 2.1 of [BBLP13]	X_{13h}	$E(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ Edwards curves $a = \square$ twisted Edwards	1
4	Section 2 of [BCKL15]	$3B^0$-$3a$	isogenous to a curve with a point of order 3	
5	Section 10.3.2 of [Mon87] and [Suy85]	X_{13}-$3B^0$-$3a$T2	Suyama	$1 \cap 4$
6	Section 3.2 of [AM93]	$5D^0$-$5b$T1	$E(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$	
7	Section 3.3 of [AM93]	$7E^0$-$7b$T1	$E(\mathbb{Q}) \simeq \mathbb{Z}/7\mathbb{Z}$	
8	Section 4. of [BBL10]	X_{195l}	$E(\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$	3
9	Section 3.4 of [AM93]	$9I^0$-$9c$T2	$E(\mathbb{Q}) \simeq \mathbb{Z}/9\mathbb{Z}$	4
10	Section 3.5 of [AM93]	X_6-$5D^0$-$5b$T1	$E(\mathbb{Q}) \simeq \mathbb{Z}/10\mathbb{Z}$	6
11	Section 6.1 of [Mon92] Section 6.1 of [BBLP13]	X_{13h}-$3B^0$-$3a$T2	$E(\mathbb{Q}) \simeq \mathbb{Z}/12\mathbb{Z}$	$3 \cap 4$
12	page 217 of [Kub76]	X_{25n}	$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	3
13	Section 6.2 of [Mon92] Section 3.1 of [AM93] Section 6.5 of [BBLP13] Section 3.5.2 of [HMR16]	X_{193n}	$E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	$8 \cap 12$
14	Section 3.1 of [BC10]	$3D^0$-$3a$T1	$E(\mathbb{Q}(\zeta_3)) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$	4
15	Section 3.2 of [BC10] Section 3.5.1 of [HMR16]	X_6-$3D^0$-$3a$T1	$E(\mathbb{Q}(\zeta_3)) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	14
16	Section 3.5 of [BC10] Section 3 of [BBL10]	X_{58i}	$E(\mathbb{Q}(i)) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	12
17	Section 3.7 of [BC10]	$5H^0$-$5a$T1	$E(\mathbb{Q}(\zeta_5)) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$	6
18	Section 5 of [BBL10] Section 3.5.1 of [BBB+13]	X_{13f}-$3B^0$-$3a$T2	Suyama-11 exceptional Galois	$5 \cap 2$
19	Section 3.5.3 of [BBB+13]	X_{13d}-$3B^0$-$3a$T2	Suyama-9/4 exceptional Galois	5
20	Section 3.4.1 of [BBB+13], $e = g^2$	X_{183d}	exceptional Galois	16
21	Section 3.4.1 of [BBB+13], $e = \frac{2g^2+2g+1}{2g+1}$	X_{183i}	exceptional Galois	16
22	Section 3.4.1 of [BBB+13], $e = \frac{g^2}{2}$	X_{187d}	exceptional Galois	16
23	Section 3.4.1 of [BBB+13], $e = \frac{g^2-1}{2g}$	X_{189d}	exceptional Galois	16

Table 26.3: Correspondence between ECM-friendly families in the literature and the families in Theorem 24.7.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
X189d	-3.4305	✓	✓	✓	✗
X192i	-3.4305	✓	✗	✓	✗
X193n	-3.4305	✓	✓	✗	✗
X207n	-3.4305	✓	✓	✓	✗
X211m	-3.4305	✓	✗	✓	✗
X235l	-3.4305	✓	✓	✗	✗
X13d-3B0-3aT1	-3.3825	✓	✗	✗	✓
X13d-3B0-3aT2	-3.3825	✓	✗	✗	✓
X13f-3B0-3aT1	-3.3825	✓	✗	✓	✓
X13f-3B0-3aT2	-3.3825	✓	✗	✓	✓
X13h-3B0-3aT1	-3.3825	✓	✓	✗	✓
X13h-3B0-3aT2	-3.3825	✓	✓	✗	✓
X8d-3B0-3aT1	-3.3825	✗	✗	✗	✓
X8d-3B0-3aT2	-3.3825	✗	✗	✗	✓
X6-5D0-5aT1	-3.1922	✗	✗	✗	✗
X6-5D0-5bT1	-3.1922	✗	✗	✗	✗
X15-5D0-5aT1	-3.1886	✗	✗	✗	✗
X15-5D0-5bT1	-3.1886	✗	✗	✗	✗
X19-5D0-5aT1	-3.1886	✗	✗	✗	✗
X19-5D0-5bT1	-3.1886	✗	✗	✗	✗
X13-3B0-3aT1	-3.1514	✓	✗	✗	✓
X13-3B0-3aT2	-3.1514	✓	✗	✗	✓
X8-3B0-3aT1	-3.1514	✗	✗	✗	✓
X8-3B0-3aT2	-3.1514	✗	✗	✗	✓
X13c-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13c-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT2	-3.1442	✓	✗	✗	✓
X8c-3B0-3aT1	-3.1442	✗	✗	✗	✓
X8c-3B0-3aT2	-3.1442	✗	✗	✗	✓
X6-3D0-3aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT2	-3.1013	✗	✗	✗	✓
X16-3D0-3aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT2	-3.0977	✗	✗	✗	✓
X17-3D0-3aT1	-3.0977	✗	✗	✗	✓
X17-9B0-9aT1	-3.0977	✗	✗	✗	✓
X17-9B0-9aT2	-3.0977	✗	✗	✗	✓
X183d	-3.0839	✓	✓	✓	✗
X183i	-3.0839	✓	✓	✓	✗
X185g	-3.0839	✓	✓	✗	✗
X185h	-3.0839	✓	✗	✓	✗
X187d	-3.0839	✓	✓	✓	✗
X187k	-3.0839	✓	✓	✓	✗
X189e	-3.0839	✓	✓	✓	✗
X192g	-3.0839	✓	✓	✗	✗
X193i	-3.0839	✓	✗	✓	✗

Table 26.4: Best 50 families characterized by α(E) over $\mathbb{Q}$.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
X6-3D0-3aT1	-3.7193	✗	✗	✗	✓
X6-9B0-9aT1	-3.7193	✗	✗	✗	✓
X6-9B0-9aT2	-3.7193	✗	✗	✗	✓
X16-3D0-3aT1	-3.7156	✗	✗	✗	✓
X16-9B0-9aT1	-3.7156	✗	✗	✗	✓
X16-9B0-9aT2	-3.7156	✗	✗	✗	✓
X17-3D0-3aT1	-3.7156	✗	✗	✗	✓
X17-9B0-9aT1	-3.7156	✗	✗	✗	✓
X17-9B0-9aT2	-3.7156	✗	✗	✗	✓
X13d-3B0-3aT1	-3.5884	✓	✗	✗	✓
X13d-3B0-3aT2	-3.5884	✓	✗	✗	✓
X13f-3B0-3aT1	-3.5884	✓	✗	✓	✓
X13f-3B0-3aT2	-3.5884	✓	✗	✓	✓
X13h-3B0-3aT1	-3.5884	✓	✓	✗	✓
X13h-3B0-3aT2	-3.5884	✓	✓	✗	✓
X8d-3B0-3aT1	-3.5884	✗	✗	✗	✓
X8d-3B0-3aT2	-3.5884	✗	✗	✗	✓
X189d	-3.4305	✓	✓	✓	✗
X192i	-3.4305	✓	✗	✓	✗
X193n	-3.4305	✓	✓	✗	✗
X207n	-3.4305	✓	✓	✓	✗
X211m	-3.4305	✓	✗	✓	✗
X235l	-3.4305	✓	✓	✗	✗
X13-3B0-3aT1	-3.3574	✓	✗	✗	✓
X13-3B0-3aT2	-3.3574	✓	✗	✗	✓
X8-3B0-3aT1	-3.3574	✗	✗	✗	✓
X8-3B0-3aT2	-3.3574	✗	✗	✗	✓
X13c-3B0-3aT1	-3.3502	✓	✗	✗	✓
X13c-3B0-3aT2	-3.3502	✓	✗	✗	✓
X13e-3B0-3aT1	-3.3502	✓	✗	✗	✓
X13e-3B0-3aT2	-3.3502	✓	✗	✗	✓
X13g-3B0-3aT1	-3.3502	✓	✗	✗	✓
X13g-3B0-3aT2	-3.3502	✓	✗	✗	✓
X8c-3B0-3aT1	-3.3502	✗	✗	✗	✓
X8c-3B0-3aT2	-3.3502	✗	✗	✗	✓
9H0-9bT1	-3.2237	✗	✗	✗	✓
9H0-9bT2	-3.2237	✗	✗	✗	✓
9I0-9aT1	-3.2237	✗	✗	✗	✓
9I0-9aT2	-3.2237	✗	✗	✗	✓
9I0-9cT1	-3.2237	✗	✗	✗	✓
9I0-9cT2	-3.2237	✗	✗	✗	✓
X6-5D0-5aT1	-3.1922	✗	✗	✗	✗
X6-5D0-5bT1	-3.1922	✗	✗	✗	✗
X15-5D0-5aT1	-3.1886	✗	✗	✗	✗
X15-5D0-5bT1	-3.1886	✗	✗	✗	✗
X19-5D0-5aT1	-3.1886	✗	✗	✗	✗
X19-5D0-5bT1	-3.1886	✗	✗	✗	✗
X183d	-3.0839	✓	✓	✓	✗
X183i	-3.0839	✓	✓	✓	✗
X185g	-3.0839	✓	✓	✗	✗

Table 26.5: Best 50 families characterized by α(E) over $\mathbb{Q}(\zeta_3)$.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
X183d	-3.6616	✓	✓	✓	✗
X183i	-3.6616	✓	✓	✓	✗
X185g	-3.6616	✓	✓	✗	✗
X185h	-3.6616	✓	✗	✓	✗
X187d	-3.6616	✓	✓	✓	✗
X187k	-3.6616	✓	✓	✓	✗
X189d	-3.6616	✓	✓	✓	✗
X189e	-3.6616	✓	✓	✓	✗
X192g	-3.6616	✓	✓	✗	✗
X192i	-3.6616	✓	✗	✓	✗
X193i	-3.6616	✓	✗	✓	✗
X193n	-3.6616	✓	✓	✗	✗
X194k	-3.6616	✓	✗	✓	✗
X194l	-3.6616	✓	✓	✗	✗
X195h	-3.6616	✓	✓	✓	✗
X195l	-3.6616	✓	✓	✓	✗
X205h	-3.6616	✓	✓	✓	✗
X205i	-3.6616	✓	✓	✓	✗
X207l	-3.6616	✓	✓	✓	✗
X207n	-3.6616	✓	✓	✓	✗
X208a	-3.6616	✓	✗	✓	✗
X208c	-3.6616	✓	✓	✗	✗
X211m	-3.6616	✓	✗	✓	✗
X211s	-3.6616	✓	✓	✗	✗
X212h	-3.6616	✓	✗	✓	✗
X212i	-3.6616	✓	✓	✗	✗
X213h	-3.6616	✓	✗	✓	✗
X213i	-3.6616	✓	✓	✗	✗
X215c	-3.6616	✓	✓	✗	✗
X215l	-3.6616	✓	✗	✓	✗
X225g	-3.6616	✓	✗	✓	✗
X225h	-3.6616	✓	✓	✗	✗
X227i	-3.6616	✓	✓	✗	✗
X227k	-3.6616	✓	✗	✓	✗
X235i	-3.6616	✓	✗	✓	✗
X235l	-3.6616	✓	✓	✗	✗
X240h	-3.6616	✓	✗	✓	✗
X240l	-3.6616	✓	✓	✗	✗
X243d	-3.6616	✓	✓	✗	✗
X243g	-3.6616	✓	✗	✓	✗
X10d-3B0-3aT1	-3.4980	✗	✗	✗	✓
X10d-3B0-3aT2	-3.4980	✗	✗	✗	✓
X13d-3B0-3aT1	-3.4980	✓	✗	✗	✓
X13d-3B0-3aT2	-3.4980	✓	✗	✗	✓
X13f-3B0-3aT1	-3.4980	✓	✗	✓	✓
X13f-3B0-3aT2	-3.4980	✓	✗	✓	✓
X13h-3B0-3aT1	-3.4980	✓	✓	✗	✓
X13h-3B0-3aT2	-3.4980	✓	✓	✗	✓
X8d-3B0-3aT1	-3.4980	✗	✗	✗	✓
X8d-3B0-3aT2	-3.4980	✗	✗	✗	✓

Table 26.6: Best 50 families characterized by α(E) over $\mathbb{Q}(i)$.

label	α(E)	Montgomery	$a = 1$	$a = -1$	Hessian
25B0-25aT1	-4.0148	✗	✗	✗	✗
25B0-25aT2	-4.0148	✗	✗	✗	✗
25B0-25bT1	-4.0148	✗	✗	✗	✗
25B0-25bT2	-4.0148	✗	✗	✗	✗
5H0-5aT1	-4.0148	✗	✗	✗	✗
5H0-5aT2	-4.0148	✗	✗	✗	✗
X6-5D0-5aT1	-3.4437	✗	✗	✗	✗
X6-5D0-5aT2	-3.4437	✗	✗	✗	✗
X6-5D0-5bT1	-3.4437	✗	✗	✗	✗
X6-5D0-5bT2	-3.4437	✗	✗	✗	✗
X15-5D0-5aT1	-3.4401	✗	✗	✗	✗
X15-5D0-5aT2	-3.4401	✗	✗	✗	✗
X15-5D0-5bT1	-3.4401	✗	✗	✗	✗
X15-5D0-5bT2	-3.4401	✗	✗	✗	✗
X19-5D0-5aT1	-3.4401	✗	✗	✗	✗
X19-5D0-5aT2	-3.4401	✗	✗	✗	✗
X19-5D0-5bT1	-3.4401	✗	✗	✗	✗
X19-5D0-5bT2	-3.4401	✗	✗	✗	✗
X189d	-3.4305	✓	✓	✓	✗
X192i	-3.4305	✓	✗	✓	✗
X193n	-3.4305	✓	✓	✗	✗
X207n	-3.4305	✓	✓	✓	✗
X211m	-3.4305	✓	✗	✓	✗
X235l	-3.4305	✓	✓	✗	✗
X13d-3B0-3aT1	-3.3825	✓	✗	✗	✓
X13d-3B0-3aT2	-3.3825	✓	✗	✗	✓
X13f-3B0-3aT1	-3.3825	✓	✗	✓	✓
X13f-3B0-3aT2	-3.3825	✓	✗	✓	✓
X13h-3B0-3aT1	-3.3825	✓	✓	✗	✓
X13h-3B0-3aT2	-3.3825	✓	✓	✗	✓
X8d-3B0-3aT1	-3.3825	✗	✗	✗	✓
X8d-3B0-3aT2	-3.3825	✗	✗	✗	✓
X13-3B0-3aT1	-3.1514	✓	✗	✗	✓
X13-3B0-3aT2	-3.1514	✓	✗	✗	✓
X8-3B0-3aT1	-3.1514	✗	✗	✗	✓
X8-3B0-3aT2	-3.1514	✗	✗	✗	✓
X13c-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13c-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13e-3B0-3aT2	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT1	-3.1442	✓	✗	✗	✓
X13g-3B0-3aT2	-3.1442	✓	✗	✗	✓
X8c-3B0-3aT1	-3.1442	✗	✗	✗	✓
X8c-3B0-3aT2	-3.1442	✗	✗	✗	✓
X6-3D0-3aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT1	-3.1013	✗	✗	✗	✓
X6-9B0-9aT2	-3.1013	✗	✗	✗	✓
X16-3D0-3aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT1	-3.0977	✗	✗	✗	✓
X16-9B0-9aT2	-3.0977	✗	✗	✗	✓

Table 26.7: Best 50 families characterized by α(E) over $\mathbb{Q}(\zeta_5)$.

Theorem in [Mor19]	Label in [Mor19]	Label in [BS19b]
Theorem A(1)	$G_{3,2} \times G_{3,3}$	X_2-$3B^0$-$3a$
Theorem A(1)	$G_{2,2} \times G_{2,3}$	X_6-$3C^0$-$3a$
Theorem A(1)	$G_{2,2} \times G_{1,3}$	X_6-$3D^0$-$3a$
Theorem A(1)	$G_{2,2} \times G_{3,3}$	X_6-$3B^0$-$3a$
Theorem A(1)	$G_{2,2} \times G_{4,3}$	X_6-$3A^0$-$3a$
Theorem A(1)	$G_{1,2} \times G_{3,3}$	X_8-$3B^0$-$3a$
Theorem A(2)	$H_9 \times G_{3,3}$	X_9-$3B^0$-$3a$
Theorem A(2)	$H_{10} \times G_{3,3}$	X_{10}-$3B^0$-$3a$
Theorem A(2)	$H_{11} \times G_{4,3}$	X_{11}-$3A^0$-$3a$
Theorem A(2)	$H_{12} \times G_{4,3}$	X_{12}-$3A^0$-$3a$
Theorem A(2)	$H_{13} \times G_{3,3}$	X_{13}-$3B^0$-$3a$
Theorem A(3)	$H_{30} \times G_{4,3}$	X_{30}-$3A^0$-$3a$
Theorem A(3)	$H_{31} \times G_{4,3}$	X_{31}-$3A^0$-$3a$
Theorem A(3)	$H_{39} \times G_{4,3}$	X_{39}-$3A^0$-$3a$
Theorem A(3)	$H_{45} \times G_{4,3}$	X_{45}-$3A^0$-$3a$
Theorem A(3)	$H_{47} \times G_{4,3}$	X_{47}-$3A^0$-$3a$
Theorem A(3)	$H_{50} \times G_{4,3}$	X_{50}-$3A^0$-$3a$
Theorem A(4)	$H_{103} \times G_{4,3}$	X_{103}-$3A^0$-$3a$
Theorem A(4)	$H_{104} \times G_{4,3}$	X_{104}-$3A^0$-$3a$
Theorem A(4)	$H_{105} \times G_{4,3}$	genus > 1
Theorem A(4)	$H_{107} \times G_{4,3}$	genus > 1
Theorem A(4)	$H_{110} \times G_{4,3}$	genus > 1
Theorem A(4)	$H_{112} \times G_{4,3}$	genus > 1
Theorem A(4)	$H_{113} \times G_{4,3}$	X_{113}-$3A^0$-$3a$
Theorem A(4)	$H_{114} \times G_{4,3}$	X_{114}-$3A^0$-$3a$
Theorem A(4)	$H_{150} \times G_{4,3}$	genus > 1
Theorem A(4)	$H_{153} \times G_{4,3}$	genus > 1
Theorem A(4)	$H_{165} \times G_{4,3}$	genus > 1
Theorem A(4)	$H_{166} \times G_{4,3}$	genus > 1
Theorem C(1)	$G_{3,2} \times G_{9,5}$	X_2-$5A^0$-$5a$
Theorem C(2)	$G_{3,2} \times G_{7,7}$	X_2-$7B^0$-$7a$
Theorem C(3)	$G_{3,2} \times G_{3,11}$	genus > 1
Theorem C(4)	$G_{3,2} \times G_{7,13}$	genus > 1

Table 26.8: We translate labels from [Mor19] in our labels. A group in [Mor19] of form $G_{i,p} \times \mathrm{j}, \mathrm{q}$ for primes p and q correspond to product of the i-th group in the list of subgroups of level p and the j-th group in the list of subgroups of level q in [Mor19, Appendix A]. A group of form $H_i \times G_{j,q}$ means the product of the i-th group in the file "newsublist" of [RZB15] and the j-th group in the list of subgroups of level q in [Mor19, Appendix A].

Bibliography

[Abd99] Ines Abdeljaouad. Calculs d'invariants primitifs de groupes finis. *Theor. Inform. Appl.*, 33(1):59–77, 1999. https://www.gap-system.org/Gap3/Contrib3/contrib.html. 69

[Ade04] Clemens Adelmann. *The decomposition of primes in torsion point fields*. Springer, 2004. 18

[AM93] A Oliver L Atkin and Francois Morain. Finding suitable curves for the elliptic curve method of factorization. *Mathematics of Computation*, 60(201):399–405, 1993. ix, 55, 107, 118

[Ann14] Samuele Anni. A local–global principle for isogenies of prime degree over number fields. *Journal of the London Mathematical Society*, 89(3):745–761, 2014. 109

[Bar09] Razvan Barbulescu. Familles de courbes adaptées à la factorisation des entiers. Rapport de stage M1, 2009. 54, 55

[BBB+13] Razvan Barbulescu, Joppe Bos, Cyril Bouvier, Thorsten Kleinjung, and Peter Montgomery. Finding ECM-friendly curves through a study of galois properties. *The Open Book Series*, 1(1):63–86, 2013. ix, x, xii, 23, 34, 49, 56, 57, 61, 65, 80, 82, 108, 118

[BBJ+08] Daniel J Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards curves. In *Progress in Cryptology – AFRICACRYPT*, pages 389–405, 2008. 54, 106, 107

[BBL10] Daniel J Bernstein, Peter Birkner, and Tanja Lange. Starfish on strike. In *International Conference on Cryptology and Information Security in Latin America*, pages 61–80. Springer, 2010. ix, 59, 107, 118

[BBLP13] Daniel Bernstein, Peter Birkner, Tanja Lange, and Christiane Peters. Ecm using edwards curves. *Mathematics of Computation*, 82(282):1139–1179, 2013. ix, 107, 118

[BC10] Éric Brier and Christophe Clavier. New families of ecm curves for cunningham numbers. In *International Algorithmic Number Theory Symposium*, pages 96–109. Springer, 2010. ix, 55, 107, 118

[BCKL15] Daniel J Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange. Twisted Hessian curves. In *Progress in cryptology – LATINCRYPT 2015*, volume 9230 of *Lecture notes in computer science*, pages 269–294. Springer, 2015. 55, 107, 118

[Bel13] Joël Bellaïche. Théorème de chebotarev et complexité de littlewood. *arXiv preprint arXiv:1308.1022*, 2013. 33

[Ber29] WEH Berwick. On soluble sextic equations. *Proceedings of the London Mathematical Society*, 2(1):1–28, 1929. 69

[BGGM14] R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain. Discrete logarithms in GF(p^2) — 160 digits, 2014. Announcement available at the NMBRTHRY archives, item 004706. 52

[BGGM15] R. Barbulescu, P. Gaudry, A. Guillevic, and F. Morain. Improving NFS for the discrete logarithm problem in non-prime finite fields. In *Advances in Cryptology - EUROCRYPT 2015*, volume 9056 of *Lecture notes in computer science*, pages 129–155, 2015. 52

[BGK+] Shi Bai, Pierrick Gaudry, Alexander Kruppa, François Morain, Emmanuel Thomé, and Paul Zimmermann. Crible algébrique: Distribution, optimisation—number field sieve (cado-nfs). vii, 51

[BI] Cyril Bouvier and Laurent Imbert. Faster cofactorization with ecm using mixed representations. Available online as the Cryptology ePrint as report 669 of 2018. 53

[BJ16] Julio Brau and Nathan Jones. Elliptic curves with 2-torsion contained in the 3-torsion field. *Proceedings of the American Mathematical Society*, 144(3):925–936, 2016. 110

[BL07] Daniel J Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. In *Advances in cryptology – ASIACRYPT 2007*, volume 4833 of *Lecture notes in computer science*, pages 29–50, 2007. 54

[BL17] Razvan Barbulescu and Armand Lachand. Some mathematical remarks on the polynomial selection in nfs. *Mathematics of Computation*, 86(303):397–418, 2017. xi, 60

[Bre10] Richard P Brent. Some integer factorization algorithms using elliptic curves. *arXiv preprint arXiv:1004.3366*, 2010. 53

[BS19a] Razvan Barbulescu and Sudarshan Shinde. A classification of ECM-friendly families using modular curves. 2019. 106, 110

[BS19b] Razvan Barbulescu and Sudarshan Shinde. Online complement, 2019. Available at `https://webusers.imj-prg.fr/~sudarshan.shinde/ECMfriendly.html`. xi, xii, 22, 37, 40, 44, 74, 101, 104, 106, 110, 111, 123

[BSS99] Ian Blake, Gadiel Seroussi, and Nigel Smart. *Elliptic curves in cryptography*, volume 265. Cambridge university press, 1999. 20

[CE11] Jean-Marc Couveignes and Bas Edixhoven. *Computational aspects of modular forms and Galois representations*. 2011. 93, 97

[CH08] John J Cannon and Derek F Holt. The transitive permutation groups of degree 32. *Experimental Mathematics*, 17(3):307–314, 2008. 65

[Coh13] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013. 69

[Cox11a] David A Cox. *Galois theory*, volume 61. John Wiley & Sons, 2011. 65, 66, 67, 68, 71

[Cox11b] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011. 16, 32

[CP84] David A Cox and Walter R Parry. Genera of congruence subgroups in q-quaternion algebras. *J. Reine Angew. Math*, 351(66):112, 1984. 101

[CP03] C.J. Cummins and S. Pauli. Congruence subgroups of $psl(2, \mathbb{Z})$ of genus less than or equal to 24. *Experimental Mathematics*, 12(2):243–255, 2003. 101, 105

[Cre01] JE Cremona. Classical invariants and 2-descent on elliptic curves. *Journal of Symbolic Computation*, 31(1-2):71–87, 2001. 73

[Cro07] Ernie Croot. Smooth numbers in short intervals. *International Journal of Number Theory*, 3(01):159–169, 2007. 51

[CS15] Pierre Colmez and Jean-Pierre Serre. *Correspondance Serre-Tate (Volume I)*. Société Mathématique de France, 2015. 16, 25

[CSS13] Gary Cornell, Joseph H Silverman, and Glenn Stevens. *Modular forms and Fermat's last theorem*. Springer Science & Business Media, 2013. 96

[DF04] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004. 27

[Dic30] Karl Dickman. On the frequency of numbers containing prime factors of a certain relative magnitude. *Arkiv for matematik, astronomi och fysik*, 22(10):1–14, 1930. 51

[Dic03] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory*. Courier Corporation, 2003. 29

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable II*, pages 143–316. Springer, 1973. 88

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228. Springer, 2005. 83, 86, 88, 90, 91, 93, 94, 95, 97

[DS17] Maarten Derickx and Andrew Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proceedings of the American Mathematical Society*, 145(10):4233–4245, 2017. x

[DT02] W Duke and Árpad Tóth. The splitting of primes in division fields of elliptic curves. *Experimental Mathematics*, 11(4):555–565, 2002. 37

[Duk97] William Duke. Elliptic curves with no exceptional primes. *Comptes rendus de l'Académie des sciences. Série 1, Mathématique*, 325(8):813–818, 1997. 36, 58

[Edw07] Harold Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44(3):393–422, 2007. 54

[Elk06] N Elkies. $\mathbb{Z}^{28} \in \mathrm{E}(\mathbb{Q})$. *Number Theory Listserver*, 2006. 15

[FH13] William Fulton and Joe Harris. *Representation theory: a first course*, volume 129. Springer Science & Business Media, 2013. 4

[GJLR15] Enrique González-Jiménez and Álvaro Lozano-Robledo. On the minimal degree of definition of p-primary torsion subgroups of elliptic curves. *arXiv preprint arXiv:1511.08057*, 2015. 114

[GKL17] Alexandre Gélin, Thorsten Kleinjung, and Arjen K Lenstra. Parametrizations for families of ECM-friendly curves. In *International Symposium on Symbolic and Algebraic Computation – ISSAC 2017*, pages 165–171, 2017. 59

[Gou97] Fernando Q Gouvêa. p-adic numbers. In *p-adic Numbers*, pages 43–85. Springer, 1997. 24

[Gre10] Aaron Greicius. Elliptic curves with surjective adelic galois representations. *Experimental Mathematics*, 19(4):495–507, 2010. 25

[Har77] Robin Hartshorne. *Algebraic geometry*, volume 52. Springer-Verlag, New York, 1977. 6, 7

[Has36] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper i. die struktur der gruppe der divisorenklassen endlicher ordnung. *Journal für die reine und angewandte Mathematik*, 175:55–62, 1936. 17, 50

[Hec27] E. Hecke. Theorie der eisensteinschen reihen höherer stufe und ihre anwendung auf funktionentheorie und arithmetik. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 5(1):199–224, Dec 1927. 95

[Hei34] Hans Heilbronn. On the class-number in imaginary quadratic fields. *The Quarterly Journal of Mathematics*, (1):150–160, 1934. 16

[Her06] Israel N Herstein. *Topics in algebra*. John Wiley & Sons, 2006. 27

[Hes44] Otto Hesse. Über die elimination der variabeln aus drei algebraischen gleichungen vom zweiten grade mit zwei variabeln. *Journal für die reine und angewandte Mathematik*, 28:68–96, 1844. 55

[HMR16] Henriette Heer, Gary McGuire, and Oisin Robinson. JKL-ECM: an implementation of ECM using hessian curves. *LMS Journal of Computation and Mathematics*, 19(A):83–99, 2016. ix, 55, 59, 107, 108, 118

[HT93] Adolf Hildebrand and Gérald Tenenbaum. Integers without large prime factors. *Journal de théorie des nombres de Bordeaux*, 5(2):411–484, 1993. 51

[Hul05] Alexander Hulpke. Constructing transitive permutation groups. *Journal of Symbolic Computation*, 39(1):1–30, 2005. 65

[JKP06] Daeyeol Jeon, Chang Heon Kim, and Euisung Park. On the torsion of elliptic curves over quartic number fields. *Journal of the London Mathematical Society*, 74(1):1–12, 2006. x

[JKS04] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arithmetica*, 113:291–301, 2004. x

[JL03] A. Joux and R. Lercier. Improvements to the general number field for discrete logarithms in prime fields. *Mathematics of Computation*, 72(242):953–967, 2003. 52

[K+86] Sheldon Kamienny et al. Torsion points on elliptic curves over all quadratic fields. *Duke Mathematical Journal*, 53(1):157–162, 1986. x

[KAF+10] Thorsten Kleinjung, Kazumaro Aoki, Jens Franke, Arjen K Lenstra, Emmanuel Thomé, Joppe W Bos, Pierrick Gaudry, Alexander Kruppa, Peter L Montgomery, Dag Arne Osvik, et al. Factorization of a 768-bit rsa modulus. In *Annual Cryptology Conference*, pages 333–350. Springer, 2010. vii

[Kat80] Nicholas M Katz. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae*, 62(3):481–502, 1980. xii, 54, 108, 109

[KB16] T. Kim and R. Barbulescu. The extended tower number field sieve: A new complexity for the medium prime case. In *Advances in Cryptology – CRYPTO 2016*, volume 9814 of *Lecture notes in computer science*, pages 543–571, 2016. 51

[Klü02] Jürgen Klüners. Algorithms for function fields. *Experimental mathematics*, 11(2):171–181, 2002. 79

[KM88] Monsur A Kenku and Fumiyuki Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125–149, 1988. x, 14

[KM00] Jürgen Klüners and Gunter Malle. Explicit galois realization of transitive groups of degree up to 15. *Journal of Symbolic Computation*, 30(6):675–716, 2000. 69

[Koh99] David R Kohel. Computing modular curves via quaternions, 1999. x

[Kru10] Alexander Kruppa. *Speeding up Integer Multiplication and Factorization*. PhD thesis, Université Henri Poincaré - Nancy I, January 2010. 55

[Kub76] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society*, 3(2):193–237, 1976. 14, 55, 61, 118

[Lag70] J.-L. Lagrange. Réflexions sur la résolution algébrique des équations. *Prussian Academy*, 1770. 67

[Lan83] Serge Lang. *Hilbert's Irreducibility Theorem*, pages 225–246. Springer New York, New York, NY, 1983. 73

[Lan87] Serge Lang. Elliptic functions. In *Elliptic Functions*, pages 5–21. Springer, 1987. 95

[Lan12] Serge Lang. *Introduction to modular forms*, volume 222. Springer Science & Business Media, 2012. 29

[LB] Tanja Lange and Daniel Bernstein. The classical groups and k-theory. Available at http://hyperelliptic.org/EFD/g1p/index.html. 53, 54

[LJ87] Hendrik W Lenstra Jr. Factoring integers with elliptic curves. *Annals of mathematics*, pages 649–673, 1987. vii, xi, 49, 51

[LLJMP93] Arjen K Lenstra, Hendrik W Lenstra Jr, Mark S Manasse, and John M Pollard. The number field sieve. In *The development of the number field sieve*, pages 11–42. Springer, 1993. vii

[LO79] Montgomery Hugh L Lagarias, Jeffrey C and Andrew M Odlyzko. A bound for the least prime ideal in the chebotarev density theorem. 1979. 33

[LR11] Álvaro Lozano-Robledo. *Elliptic curves, modular forms, and their* L-*functions*. American Mathematical Society, 2011. 83, 87, 88

[Mon87] Peter L Montgomery. Speeding the pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243–264, 1987. viii, ix, 54, 59, 107, 118

[Mon92] Peter Lawrence Montgomery. *An FFT extension of the elliptic curve method of factorization*. PhD thesis, UNIVERSITY OF CALIFORNIA Los Angeles, 1992. 52, 60, 107, 118

[Mor19] Jackson Morrow. Composite images of galois for elliptic curves over $\mathbb{Q}$ and entanglement fields. *Mathematics of Computation*, 88(319):2389–2421, 2019. xii, 99, 110, 123

[Mur99] Brian Antony Murphy. *Polynomial selection for the number field sieve integer factorisation algorithm*. PhD thesis, The Australian National University, 1999. xi, 60

[Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013. 32

[Pol74] John M Pollard. Theorems on factorization and primality testing. In *Mathematical Proceedings of the Cambridge Philosophical Society*, volume 76, pages 521–528. Cambridge University Press, 1974. 49

[Pol93] John M Pollard. The lattice sieve. In *The development of the number field sieve*, pages 43–49. Springer, 1993. vii

[Pra09] Victor V Prasolov. *Polynomials*, volume 11. Springer Science & Business Media, 2009. 65, 69, 71

[PTBW17] Lillian Pierce, Caroline Turnage-Butterbaugh, and Melanie Wood. An effective chebotarev density theorem for families of number fields, with an application to ℓ-torsion in class groups. *Inventiones mathematicae*, 09 2017. 33

[RV01] Amadeu Reverter and Nuria Vila. Images of mod p galois representations associated to elliptic curves. *Canadian Mathematical Bulletin*, 44(3):313–322, 2001. 23

[RZB15] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of galois. *Research in Number Theory*, 1(1):1–34, 2015. iv, x, xii, 23, 95, 97, 99, 100, 101, 102, 103, 106, 108, 110, 123

[SD73] H. P. F. Swinnerton-Dyer. On ℓ-adic representations and congruences for coefficients of modular forms. In Willem Kuijk and Jean-Pierre Serre, editors, *Modular Functions of One Variable III*, pages 1–55, Berlin, Heidelberg, 1973. Springer Berlin Heidelberg. 29

[Ser71] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1971. ix, 23, 25, 28, 38, 39

[Ser81] Jean-Pierre Serre. Quelques applications du théoreme de densité de chebotarev. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 54(1):123–201, 1981. ix, 33, 38

[Ser12] Jean-Pierre Serre. *A course in arithmetic*, volume 7. Springer Science & Business Media, 2012. 93

[Shi71] Gorō Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 1. Princeton university press, 1971. x, 83, 88, 95, 96

[Sil08] Joseph H Silverman. *The Arithmetic of Elliptic Curves*, volume 106. Springer, 2008. xi, 3, 4, 7, 8, 9, 10, 13, 14, 15, 16, 17, 20, 24, 34, 83, 84, 85, 86, 88, 90, 91, 93

[Sil13] Joseph H Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151. Springer Science & Business Media, 2013. 16, 25, 83, 86, 88

[Smi93] Gene Ward Smith. Some polynomials over $\mathbb{Q}(t)$ and their galois groups. In *Preprint. Laboratoire A2X, Université BordeauxI, 351coursdelaLibération, 33405 Talence Cedex*. Citeseer, 1993. 72

[ST92] Joseph H Silverman and John Torrence Tate. *Rational points on elliptic curves*, volume 9. Springer, 1992. 10

[Sta73] Richard P Stauduhar. The determination of galois groups. *Mathematics of computation*, 27(124):981–996, 1973. 67, 69

[Sut12a] Andrew V Sutherland. A local-global principle for rational isogenies of prime degree. *Journal de théorie des nombres de Bordeaux*, 24(2):475–485, 2012. 108, 109

[Sut12b] Andrew V Sutherland. Torsion subgroups of elliptic curves over number fields. *Avalaible on* `https://math.mit.edu/drew/MazursTheoremSubsequentResults.pdf`, 1, 2012. 14

[Sut16] Andrew V Sutherland. Computing images of galois representations attached to elliptic curves. In *Forum of Mathematics, Sigma*, volume 4. Cambridge University Press, 2016. 28, 29, 36, 38, 40, 44

[Suy85] Hiromi Suyama. Informal preliminary report (8), 1985. Letter to Richard P. Brent. 54, 118

[SZ06] Jean-Pierre Serre and Don Bernard Zagier. *Modular functions of one variable V: proceedings international conference, University of Bonn, Sonderforschungsbereich Theoretische Mathematik, July 2-14, 1976*, volume 601. Springer, 2006. x, 14, 59

[SZ17] Andrew V Sutherland and David Zywina. Modular curves of prime-power level with infinitely many rational points. *Algebra & Number Theory*, 11(5):1199–1229, 2017. iv, x, xii, 58, 99, 100, 101, 102, 104, 106, 110

[Tsc26] N. Tschebotareff. Die bestimmung der dichtigkeit einer menge von primzahlen, welche zu einer gegebenen substitutionsklasse gehören. *Mathematische Annalen*, 95(1):191–228, Dec 1926. 33

[Val95] Annick Valibouze. Computation of the galois groups of the resolvent factors for the direct and inverse galois problems. In *International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes*, pages 456–468. Springer, 1995. 69

[Val08] Annick Valibouze. Sur les relations entre les racines d'un polynôme. *Acta Arithmetica*, 131(1):1–27, 2008. 69

[VdWAN50] Bartel Leendert Van der Waerden, Emil Artin, and Emmy Noether. *Moderne algebra*, volume 31950. Springer, 1950. 72

[vH95] Mark van Hoeij. An algorithm for computing the weierstrass normal form. In *Proceedings of the 1995 international symposium on Symbolic and algebraic computation*, pages 90–95. ACM, 1995. 9, 73

[vH97] Mark van Hoeij. Rational parametrizations of algebraic curves using a canonical divisor. *Journal of Symbolic Computation*, 23(2-3):209–227, 1997. 73

[VHKN13] Mark Van Hoeij, Jürgen Klüners, and Andrew Novocin. Generating subfields. *Journal of Symbolic computation*, 52:17–34, 2013. 79, 80

[VZGG13] Joachim Von Zur Gathen and Jürgen Gerhard. *Modern computer algebra*. Cambridge university press, 2013. 22

[Web98] Heinrich Weber. Lehrbuch der algebra: volume iii. *Braunschweig (Viehweg)*, 1898. 16

[Wil82] Hugh C Williams. A $p+1$ method of factoring. *Mathematics of computation*, 39(159):225–234, 1982. 16

[Zyw15a] David Zywina. On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07660*, 2015. 96, 101, 106

[Zyw15b] David Zywina. Possible indices for the galois image of elliptic curves over $\mathbb{Q}$. *arXiv preprint arXiv:1508.07663*, 2015. 36

Index

$\mathrm{E}[m]$, 13
E_d, 11
$\mathrm{E}_{\mathrm{tors}}$, 14
$\Gamma(1)$, 86
$\Gamma(\mathrm{N})$, 88
$\Gamma_0(\mathrm{N}$, 88
$\Gamma_1(\mathrm{N}$, 88
$\mathrm{E}_{\mathcal{M},\mathrm{A},\mathrm{B}}$, 53
$\Pi(n)$, 33
$\alpha^{(\mathfrak{p})}$, 32
$\bar{f}(m)$, 19, 20
$\mathbb{H}$, 83
$\mathcal{D}$, 91
$\mathcal{D}'$, 91
$\mathcal{B}_{\mathrm{E},\ell}$, 37
$\mathrm{Dec}(\mathfrak{p})$, 32
$\mathrm{Gal}(\mathrm{P})$, 65
$\mathrm{R}_{\mathrm{G}}(\mathrm{F},\mathrm{P})$, 68
$\mathrm{V}(\mathrm{I})/k$, 3
$\mathrm{X}(\Gamma)$, 91
$\mathrm{B}(\ell)$, 28
$\mathrm{C}_{nsp}(\ell)$, 28
$\mathrm{C}_{sp}(\ell)$, 28
μ_m, 15
ψ_m^{new}, 21
$\rho_{\mathrm{E},\ell^\infty}$, 24
$\rho_{\mathrm{E},m}$, 23
ρ_{E}, 25
$\mathrm{Frob}(p)$, 33
$\mathrm{Stab}_{\mathrm{G}}(\mathrm{F})$, 68
Cl_g, 27
$\mathrm{Im}(\tau)$, 92
I, 35
$\mathrm{Z}(\ell)$, 28
$\mathrm{val}_\ell(n)$, 56
e_{N}, 15, 91
$g_2(\Lambda)$, 85
$g_3(\Lambda)$, 85
$j(\mathrm{E})$, 8
$k(\mathrm{E}[m])$, 18
$n(\mathrm{E},\ell)$, 56
$p-1$ method, 49
q-expansion, 92
$\mathbb{A}^2(\bar{k})$, 3
$\mathbb{A}^2(k)$, 3

multiplication by m, 13

affine, 3
    2-space, 3
    algebraic plane curve, 3
    algebraic set, 3
    part of a modular curve, 87
    Singular point, 3
average valuation, 56

birationally equivalent, 5
Borel subgroup, 28

Centralizer, 27
complex multiplication, 16, 25
congruence subgroup, 88
    genus, 91
    level, 88
Conjugacy class of a group element, 27
cusp form, 92, 94
cusps, 87

decomposition group, 32
division polynomial, 19
    degree of, 20
    new, 21

Eisenstein series, 84
    of weight k for $\Gamma(\mathrm{N})$, 94
elliptic
    function, 84
elliptic curve, 8
    m-torsion subgroup, 13
    method, 49

rank, 15
average valuation at a prime, 56
enhanced, 86
group law, 9
minimal discriminant, 17
minimal model, 17
quadratic twist of, 11
torsion subgroup, 14
entanglement, 101

fractional linear transformation, 83
Frobenius element, 33
fundamental parallelogram, 84

Galois image
ℓ-adic Galois image, 24
adelic Galois image, 25
exceptional, 23
global, 32
level, 23
local, 32, 34
mod m Galois image, 23
genus, 4
of a singular curve, 4
of an elliptic curve, 8

homogeneous, 4
ideal, 4

inertia degree, 32
inertia group, 32
isogeny, 12
isogenous, 13
isomorphism
between curves, 5

modular j-invariant, 85
modular curve, 91
X(N), 89
$X_0(N)$, 89
$X_1(N)$, 89
X(1), 87
genus, 91
modular form of weight k, 92, 94
modular function of weight k, 92, 93
modular group, 86
moduli problem, 90
moduli space, 90
Montgomery curve, 53
morphism
between curves, 5

natural density, 33
Non-split Cartan subgroup, 28
normalizer, 29
Normalizer, 27

Poincaré half plane, 83
principle congruence subgroup, 88
Projective, 4
algebraic set, 4
closure, 5
curve, 4
n-space, 4

Quadratic twist, 11

ramification index, 32
ramified, 32
unramified, 32
rational map, 5
between projective curves, 5
reduction
bad reduction at a prime, 17
good reduction at a prime, 17
regular at a point, 5
residue field, 32
resolvent method, 67

Serre's exponent, 56
Split Cartan subgroup, 28
normalizer, 29
Suyama curves, 54

Theorem
Chebotarev's density, 33
Dickson's classification, 29
Hasse, 17
Serre's open image, 25
torsion point field, 18
construction of, 21
Transitive subgroup of S_n, 65
Twisted Edwards curves, 54
twisted Hessian curves, 55
twisting factor, 11

Weierstrass, 7
$\wp$-function, 84
j-invariant of a Weierstrass curve, 8
affine polynomial, 7
discriminant of a Weierstrass curve, 8
equation, 7

equivalent Weierstrass curves, 8
projective curve, 7
projective polynomial, 7
short Weierstrass form, 7
Weil pairing, 14, 35, 91

Abstract

This work is aimed at finding and classifying all the families of ECM-friendly rational elliptic curves and quantifying their ECM-friendliness. We establish a link between the classification of ECM-friendly curves and Mazur's program B, which consists in classifying all the elliptic curves with the adelic Galois image contained in H, a subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Building upon recent works which compute the models of modular curves associated to congruence subgroups of prime-power level, we prove that there are exactly 1525 distinct families of rational elliptic curves with distinct Galois images which are cartesian products of subgroups of prime-power level. This makes an *exhaustive* list of families of ECM-friendly rational elliptic curves, out of which less than 25 were previously known. Equipped with these families, we quantify their ECM-friendliness by improving a common heuristic which says that $\#\mathrm{E}(\mathbb{F}_p)$ is as smooth as a random integer of the same size.

Keywords. Factorization, Cryptography, elliptic curve method, modular curve, Mazur's program B.

Résumé

Ce travail a pour but de chercher des familles infinies de courbes elliptiques rationnelles les mieux adaptées pour l'algorithme ECM de factorisation d'un nombre, en utilisant des courbes elliptiques et de quantifier cette adaptabilité. On établit un lien entre cette classification et le "Programme B" de Mazur, dont le but est de classifier toutes les courbes elliptiques ayant une image de Galois adélique contenu en H, un sous-groupe donné de $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

En se basant sur des travaux récents qui calculent des modèles explicites de courbes modulaires pour des sous-groupes de congruences de niveau une puissance d'un nombre premier, nous montrons qu'il existe exactement 1525 familles distinctes de courbes elliptiques rationnelles dont l'image de Galois adélique est un produit cartésien de sous-groupes de niveau une puissance d'un nombre premier. Ceci fournit une liste *exhaustive* de courbes elliptiques mieux adaptées pour l'algorithme ECM dont moins de 25 étaient connues dans la littérature. On quantifie l'adaptabilité de ces familles à l'algorithme ECM en améliorant une heuristique commune qui dit que $\#\mathrm{E}(\mathbb{F}_p)$ est autant friable qu'un entier quelconque de même taille.

Mots clés. Factorisation, cryptographie, méthode de la courbe elliptique, courbe modulaire, programme B de Mazur