AWS 2021: Modular Groups
Problem Set 6

Lecturer: Lori Watson
Written by: Tyler Genao, Hyun Jong Kim, Zonia Menendez and Sam Mundy (Assistants)

Last updated: March 1, 2021

1 Definitions and Notations

1. For an integer $N \in \mathbb{Z}^+$, let us write the reduction map for $\mathrm{SL}_2(\mathbb{Z})$ modulo N as $\mathrm{red} : \mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

2. Recall that for a modular curve $X(\Gamma)$, we write $Y(\Gamma) := \Gamma\backslash\mathcal{H}$ for its set of noncuspidal points. It is a non-compact Riemann surface, and can be interpreted as an affine algebraic curve over a suitable extension of $\mathbb{Q}$.

3. For a field k, we let $\overline{k}$ denote its *algebraic closure*.

4. Given a field extension $F/\mathbb{Q}$, if $\overline{F}$ denotes an algebraic closure of F over $\mathbb{Q}$ then the extension $\overline{F}/F$ is normal and separable. In particular, $\overline{F}/F$ is a Galois extension of infinite degree. Its automorphism group $G_F := \mathrm{Gal}(\overline{F}/F)$ is called the *absolute Galois group of* F.[1]

5. Recall that an *algebraic elliptic curve* over a field k is a nonsingular curve with a k-rational point. Via algebraic geometry, such a curve will have a defining equation in *general Weierstrass form*, $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_3x + a_6$; see Problem 19 from Problem Set 5. See also Chapter III [6].

6. Given an elliptic curve $E : y^2 = x^3 + Ax + B$ with $A, B \in F$ and an integer $N \in \mathbb{Z}^+$, the absolute Galois group G_F acts on the N-torsion subgroup $E[N]$ in the natural way, $\sigma \cdot (x, y) := (\sigma(x), \sigma(y))$. This group action is a homomorphism from G_F into the automorphism group of $E[N]$, which will be written as
$$\rho_{E,N} : G_F \to \mathrm{Aut}(E[N]).$$
This action/homomorphism is called the *mod-N Galois representation of E.*

7. $E[N]$ is a rank two $\mathbb{Z}/N\mathbb{Z}$-module. Fixing a basis $\{P, Q\}$ for $E[N]$, we can represent our action via 2×2 matrices. In this case, we may write our mod-N Galois representation as
$$\rho_{E,N,P,Q} : G_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

2 Introductory Problems

Problem 1. Let E be the elliptic curve defined by
$$E : y^2 = x^3 - 11x + 14.$$
Check directly that it has a rational point $(1, 2)$. Show that this point has order 4 by calculating its multiples.

Problem 2. Given an elliptic curve over defined by a Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Q}$, show that its 2-torsion points are exactly those points of the form $(x_0, 0)$ for $x_0 \in \overline{\mathbb{Q}}$ a root of $y^2 = x^3 + Ax + B$.

[1] For more on infinite Galois theory, see Keith Conrad's CTNT 2020 notes [1].

Problem 3.

a. Let $E_{/\mathbb{Q}}$ be the elliptic curve[2] defined by $y^2 = x^3 + 1$. Can you come up with an automorphism of E other than $[\pm 1]$? (*Hint:* it should be of order 3.)

b. Let $E/\mathbb{Q}$ be the elliptic curve[3] defined by $y^2 = x^3 + x$. Can you come up with an automorphism of E other than $[\pm 1]$? (*Hint:* it should be of order 4.)

Problem 4. Show that the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Q}$ can be transformed via a change of coordinates into the form

$$y^2 = x^3 + Ax + B$$

for some $A, B \in \mathbb{Q}$. (*Hint:* see Section III.1 [6].)

Problem 5.

a. Show that for all $A, B \in \mathbb{Q}$ the equation

$$E : y^2 = x^3 + Ax + B \tag{1}$$

defines a nonsingular curve iff $x^3 + Ax + B$ has no repeated roots. (*Hint:* to have a singular point (x_0, y_0), the polynomial $F(x, y) := y^2 - (x^3 + Ax + B)$ must have a solution (x_0, y_0) where both of its partial derivatives vanish at (x_0, y_0).)

b. One can homogenize the affine algebraic equation given in (1) to get a projective algebraic curve defined by

$$E_h : y^2z = x^3 + Axz^2 + Bz^3.$$

This curve lies in projective 2-space,

$$\mathbb{P}^2 := \{(a, b, c) \in \mathbb{C}^3 : (a, b, c) \neq (0, 0, 0)\}/\{(a, b, c) \sim (\lambda a, \lambda b, \lambda c) : \lambda \in \mathbb{C}^\times\}.$$

Show that E_h has a $\mathbb{Q}$-rational point, i.e., a point in $\mathbb{P}^2$ with an equivalence class representative which lies in $\mathbb{Q}$.

c. Conclude that an equation of the form given in (1) where $x^3 + Ax + B$ has no repeated roots will define an elliptic curve as per Definition 5.

Problem 6. Let us recall *Mazur's theorem* (originally known as *Ogg's conjecture*): any elliptic curve $E_{/\mathbb{Q}}$ will have a torsion subgroup

$$E(\mathbb{Q})[\text{tors}] \cong \begin{cases} \mathbb{Z}/N\mathbb{Z} & \text{for } N = 1, 2, \ldots, 10, 12; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{for } N = 1, 2, 3, 4 \end{cases}$$

This was first proven in [2] and [3], and then again in [4].

A key part of the proof in [2] was to show that for any prime $\ell \geq 11$ there are no elliptic curves with a $\mathbb{Q}$-rational ℓ-torsion point. Find an equivalent formulation of this fact in terms of modular curves.

Problem 7. Another result of Barry Mazur classifies rational isogenies of prime degree for elliptic curves over $\mathbb{Q}$ [4]. He shows that if an elliptic curve $E_{/\mathbb{Q}}$ admits a rational isogeny of prime degree ℓ, then

$$\ell \in \{2, 3, 5, 7, 11, 13, 17, 19, 37, 43, 67, 163\}.$$

Find an equivalent formulation of this in terms of modular curves.

[2] This elliptic curve has j-invariant 0.
[3] This elliptic curve has j-invariant 1728.

3 Intermediate Problems

Problem 8. Following Problem 2, construct infinitely many noncuspidal rational points on $Y_1(2)$ (Note that this will require infinitely many distinct j-invariants).

Problem 9 (There are no $\mathbb{Q}$-rational torsion points of order 11 on any elliptic curve)**.** The aim of this exercise is to show that

$$X_1(11)(\mathbb{Q}) = \{\text{cusps}\}.$$

Since the noncuspidal points of $X_1(11)(\mathbb{Q})$ will correspond to $\Gamma_1(11)$-isomorphism classes of elliptic curves with a $\mathbb{Q}$-rational torsion point of order 11, this exercise will show there are no elliptic curves over $\mathbb{Q}$ with a $\mathbb{Q}$-rational torsion point of order 11.

a. Prove that the genus $g(X_1(11)) = 1$. Noting that the cusp at infinity on $X_1(N)$ is always $\mathbb{Q}$-rational, conclude that $X_1(11)$ is an elliptic curve defined over $\mathbb{Q}$. (For a genus formula for $X_1(N)$, see Problem 18 on Problem Set 5.)

b. By part a., there is a model for $E := X_1(11)$ over $\mathbb{Q}$. One such model is

$$E : y^2 - y = x^3 - x^2.$$

By the Mordell-Weil theorem, we know that $E(\mathbb{Q})$ is a finitely generated abelian group. Therefore, it has a decomposition

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})[\text{tors}].$$

Here, r is the *rank* of E over $\mathbb{Q}$, and $E(\mathbb{Q})[\text{tors}]$ is its *torsion subgroup* over $\mathbb{Q}$.

Via a computer algebra system or otherwise, show that E has rank 0 over $\mathbb{Q}$.

c. By part b., $E(\mathbb{Q}) = E(\mathbb{Q})[\text{tors}]$ is a finite group. In particular, E has finitely many $\mathbb{Q}$-rational points.

Via a computer algebra system or otherwise, show that $\#E(\mathbb{Q})[\text{tors}] = 5$.

d. By Problem 12 on Problem Set 5, we know that $X_1(11)$ has ten cusps. Let us take for granted that exactly five cusps are $\mathbb{Q}$-rational. Conclude that $X_1(11)$ has no noncuspidal $\mathbb{Q}$-rational points. In particular, there do not exist $\mathbb{Q}$-rational torsion points of order 11 on any elliptic curve.

Problem 10. This problem assumes some basic algebraic geometry, but read the conclusion anyways!

Let $C/\mathbb{Q}$ be a smooth curve of genus $g(C) = 0$. There is a notion of divisors on curves which is similar to the notion of divisors on Riemann surfaces. There are also "rational" functions on C – analogous to meromorphic functions on a compact Riemann surface – which can be interpreted as algebraic maps $C \to \mathbb{P}^1$. There is also a notion of a Riemann Roch space for a divisor on C, $L(D) := \{f \text{ a rational function on } C : \operatorname{div} f + D \geq 0\}$. As it turns out, its dimension over $\mathbb{Q}$ is finite; we set $l(D) := \dim_{\mathbb{Q}} L(D)$.

A corresponding Riemann-Roch theorem holds and says the following: there is a divisor K (of degree $2g - 2$, compare to Problem 17 on Problem Set 5) on C such that for all divisors D on K, one has

$$l(D) - l(K - D) = \deg D - g + 1.$$

Suppose that C has a rational point $P \in C(\mathbb{Q})$. Apply this Riemann-Roch theorem to the divisor $D := (P)$ to show that C is actually isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$.

Problem 11. It is a fact that for $N \in \mathbb{Z}^+$ the modular curves $X_1(N)$ and $X_0(N)$ can be defined over $\mathbb{Q}$, and will have at least one $\mathbb{Q}$-rational point: the cusp at infinity. It is also a fact that any algebraic curve $C_{/\mathbb{Q}}$ with genus $g(C) > 1$ will have finitely many $\mathbb{Q}$-rational points (see Falting's Theorem).

Use these facts and the previous exercise to determine all primes $\ell \in \mathbb{Z}^+$ for which either $X_1(\ell)$ or $X_0(\ell)$ has infinitely many $\mathbb{Q}$-rational points. (Let us assume the genus one modular curves $X_1(\ell)$ and $X_0(\ell)$ all have rank zero, i.e., $\#X_1(\ell)(\mathbb{Q}) < \infty$ and $\#X_0(\ell)(\mathbb{Q}) < \infty$. Let us also assume that $g(X_0(2)) = g(X_0(3)) = g(X_1(2)) = g(X_1(3)) = 0$.)

Problem 12 (GL_2-modular curves, I)**.** This generalization of modular curves comes up more naturally when studying mod$-N$ Galois representations of elliptic curves. These five exercises on GL_2-modular curves will closely follow Samir Siksek's notes [5] (which itself follows [2]).

Fix an integer $N \in \mathbb{Z}^+$. Recall that for a primitive N'th root of unity $\zeta_N \in \mathbb{C}$, one has that $\mathbb{Q}(\zeta_N)/\mathbb{Q}$ is a Galois extension with Galois group

$$\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times. \tag{2}$$

Consider a subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We can define its *determinant subgroup* as

$$\det(H) := \{\det(\gamma) : \gamma \in H\}.$$

Observe that $\det(H) \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$, and so $\det(H)$ acts on $\mathbb{Q}(\zeta_N)$. By Galois theory, it has a corresponding fixed field of $\mathbb{Q}(\zeta_N)$, which we will denote by $\mathbb{Q}(\zeta_N)^{\det(H)}$.

a. Show that $\det(H) = (\mathbb{Z}/N\mathbb{Z})^\times$ iff $\mathbb{Q}(\zeta_N)^{\det(H)} = \mathbb{Q}$.

b. Define the *Borel subgroup of* $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ as

$$B_0(N) := \left\{ \begin{bmatrix} a & b \\ 0 & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) \right\}.$$

Show that $B_0(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{red}(\Gamma_0(N))$, and that $\mathbb{Q}(\zeta_N)^{\det(B_0(N))} = \mathbb{Q}$.

c. Define the $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ subgroup

$$B_1(N) := \left\{ \begin{bmatrix} 1 & b \\ 0 & d \end{bmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}.$$

Show that $B_1(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{red}(\Gamma_1(N))$, and that $\mathbb{Q}(\zeta_N)^{\det(B_1(N))} = \mathbb{Q}$.

d. Define the $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ subgroup

$$B(N) := \{I\}.$$

Show that $B(N) \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = \mathrm{red}(\Gamma(N))$, and that $\mathbb{Q}(\zeta_N)^{\det(B(N))} = \mathbb{Q}(\zeta_N)$.

Problem 13 (GL_2-modular curves, II)**.** Fix an integer $N \in \mathbb{Z}^+$ and a subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Taking the preimage of $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ under the reduction map $\mathrm{red} : \mathrm{SL}_2(\mathbb{Z}) \twoheadrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ gives a congruence subgroup Γ_H of level N, whence we have a corresponding modular curve $X_H := X(\Gamma_H)$. This algebraic curve has a nice[4] model over $\mathbb{Q}(\zeta_N)^{\det(H)}$. See Problem 12 for examples of Γ_H and the fixed fields $\mathbb{Q}^{\det(H)}$.

As it turns out, such modular curves X_H will be moduli spaces for H-isomorphism classes of elliptic curves with "level N structure". Such an H-isomorphism is as follows: suppose that E and E' are two elliptic curves with bases $\{P, Q\}$ and $\{P', Q'\}$ for $E[N]$ and $E'[N]$, respectively. For a vector $v := \begin{bmatrix} x \\ y \end{bmatrix} \in \mathrm{Mat}_{2\times 1}(\mathbb{Z}/N\mathbb{Z})$, let us write $R_v := xP + yQ$ and $R'_v := xP' + yQ'$. Then the elliptic curves E and E' are *H-isomorphic* with respect to $\{P, Q\}$ and $\{P', Q'\}$ if there exists an isomorphism $\phi : E \xrightarrow{\sim} E'$ and an element $h \in H$ so that for all column vectors $v \in \mathrm{Mat}_{2\times 1}(\mathbb{Z}/N\mathbb{Z})$, one has

$$\phi(R_v) = R'_{hv}.$$

What this means: since ϕ is an isomorphism from E to E', it is also an isomorphism from $E[N]$ to $E'[N]$. Both are isomorphic as $\mathbb{Z}/N\mathbb{Z}$-modules. Picking a basis for each $(\mathbb{Z}/N\mathbb{Z})$-module, it has a matrix representation M_ϕ by taking one basis to the other. Then ϕ is an H-isomorphism (w.r.t. these bases) iff $M_\phi \in H$.

For H-isomorphic elliptic curves, we will write $(E, P, Q) \sim_H (E', P', Q')$.

a. Show that H-isomorphism is an equivalence relation.

b. Show that each equivalence class $[(E, P, Q)]_H$ has a well-defined j-invariant.

[4]Smooth, projective, geometrically integral.

c. Based on the previous exercise, show that $\Gamma_{B_0(N)} = \Gamma_0(N)$, $\Gamma_{B_1(N)} = \Gamma_1(N)$ and $\Gamma_{B(N)} = \Gamma(N)$.

d. Show that when $H := B_0(N)$, one has $(E, P, Q) \sim_H (E', P', Q')$ iff there exists an isomorphism $\phi : E \xrightarrow{\sim} E'$ so that the subgroups $\langle \phi(P) \rangle = \langle P \rangle$. Conclude that the "data" of a $B_0(N)$-isomorphism is an elliptic curve E with a cyclic subgroup of order N.

e. Show that when $H := B_1(N)$, one has that $(E, P, Q) \sim_H (E', P', Q')$ iff there exists an isomorphism $\phi : E \xrightarrow{\sim} E'$ so that $\phi(P) = P'$. Conclude that the "data" of a $B_1(N)$-isomorphism is an elliptic curve E with a torsion point of order N.

f. Show that when $H := B(N)$, one has that $(E, P, Q) \sim_H (E', P', Q')$ iff there exists an isomorphism $\phi : E \xrightarrow{\sim} E'$ so that $\phi(P) = P'$ and $\phi(Q) = Q'$. Conclude that the "data" of a $B(N)$-isomorphism is an elliptic curve E with a basis for its N-torsion.

4 Advanced Problems

Problem 14 (GL_2-modular curves, III)**.** This problem concerns rational points on GL_2-modular curves, and their moduli space interpretation.

Fix an integer $N \in \mathbb{Z}^+$, and let $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be a subgroup. As noted in the previous exercise on GL_2-modular curves, X_H is a nice curve over $\mathbb{Q}(\zeta_N)^{\det(H)}$. In fact, the points on X_H may be regarded as H-isomorphism classes of elliptic curves with fixed level N structure. We will write such points as (E, P, Q), suppressing notation for H.

For each algebraic extension $F/\mathbb{Q}(\zeta_N)^{\det(H)}$, there is an action of the absolute Galois group G_F on the set $Y_H(\overline{F})$ of noncuspidal algebraic points as follows. For each $\sigma \in G_F$, let us define

$$(E, P, Q)^\sigma := (E^\sigma, P^\sigma, Q^\sigma).$$

Then one says that a point $(E, P, Q) \in Y_H(\overline{F})$ is F-rational iff $\forall \sigma \in G_F$ one has

$$(E, P, Q)^\sigma \sim_H (E, P, Q).$$

In such a case, let us write $(E, P, Q) \in Y_H(F)$.

a. Show that if $-I \in H$, then for a point $x \in Y_H(\overline{F})$ with j-invariant $\neq 0, 1728$, one has $x \in Y_H(F)$ iff there is a representative $x = (E, P, Q)$ with E defined over F and its mod-N Galois representation $\rho_{E,N,P,Q}(G_F) \subseteq H$. In such a case, any representative (E, P, Q) with E defined over F will also have $\rho_{E,N,P,Q}(G_F) \subseteq H$.

b. Show that if $-I \notin H$, then for a point $x \in Y_H(\overline{F})$ with j-invariant $\neq 0, 1728$, one has $x \in Y_H(F)$ iff there is a representative $x = (E, P, Q)$ with E defined over F and its mod-N Galois representation $\rho_{E,N,P,Q}(G_F) \subseteq H$. In such a case, any representative (E, P, Q) with E defined over F will also have $\rho_{E,N,P,Q}(G_F) \subseteq \{\pm I\}H$. (*Hint:* replace a representative $x = (E, P, Q)$ with a quadratic twist of E.)

Problem 15 (GL_2-modular curves, IV)**.** Let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

a. Suppose $-I \in H$. Show that Y_H is a *coarse moduli space* away from j-invariants $0, 1728$: for any finite extension $F/\mathbb{Q}$, an F-rational point $x \in Y_H$ with $j(x) \neq 0, 1728$ has infinitely many representatives (E, P, Q) with E defined over F which are not H-isomorphic over F. (*Hint:* use quadratic twists.)

b. Suppose $-I \notin H$. Show that Y_H is a *fine moduli space* away from j-invariants $0, 1728$: for any algebraic extension $F/\mathbb{Q}$, an F-rational point $x \in Y_H$ with $j(x) \neq 0, 1728$ will have a unique representative (E, P, Q) with E defined over F, up to H-isomorphism. (*Hint:* show that any H-isomorphism between two representatives of x is F-rational.)

Problem 16 (GL_2-modular curves, V)**.**

a. Pick your favorite subgroup H of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ for some $N \in \mathbb{Z}^+$. Try and determine both $\mathbb{Q}^{\det(H)}$ and Γ_H, and the "data" of a point on Y_H. Also determine if Y_H is a coarse or fine moduli space.

b. Many number theorists are interested in classifying Galois representations of elliptic curves over various fields, especially over $\mathbb{Q}$. This classification is at the core of *Mazur's Program B*, introduced in [2]. Read [7] for a survey on progress towards Mazur's Program B over $\mathbb{Q}$. Studying $\mathbb{Q}$-rational points on modular curves has helped make significant progress towards this program.

The next two problems assume basic knowledge of complex multiplication.

Problem 17 (CM points of bounded degree on $X_0(N)$)**.** Let K be an imaginary quadratic number field, and let $\mathcal{O}_K \subseteq K$ be its ring of integers. Let $N \in \mathbb{Z}^+$, and suppose that the pair $(N, \mathcal{O}_K)$ satisfies the *Heegner hypothesis,* i.e., each prime $p \mid N$ splits in $\mathcal{O}_K$.

a. Show there exists an ideal $I \subseteq \mathcal{O}_K$ of norm N.

b. Deduce that there exists a $K^{(1)}$-rational cyclic N-isogeny between $\mathcal{O}_K$-CM elliptic curves, $[I] : E \to E'$.[5]

c. Conclude that we have a noncuspidal point $(E, [I]) \in X_0(N)(K^{(1)})$ whose degree over $\mathbb{Q}$ is at most $2h_K$, where the class number $h_K := \#\mathrm{Cl}(\mathcal{O}_K)$.

d. Redo parts a., b. and c. after replacing $\mathcal{O}_K$ with an arbitrary order $\mathcal{O} \subseteq K$, $K^{(1)}$ with the *ring class field* $K(\mathcal{O})$, and h_K with the class number $h_{\mathcal{O}} := \#\mathrm{Cl}(\mathcal{O})$.

e. * What is the least degree of a CM point on $X_0(N)$?

Problem 18. Let K be an imaginary quadratic number field.

a. Show that for infinitely many primes $\ell \in \mathbb{Z}^+$, the modular curves $X_0(\ell)$ have a noncuspidal $K^{(1)}$-rational point.

b. Show that $X_0(\ell)$ has a noncuspidal $\mathbb{Q}$-rational point when $\ell \in \{2, 3, 7, 11, 19, 43, 67, 163\}$. (*Hint:* which fields $\mathbb{Q}(\sqrt{-\ell})$ have class number one?)

References

[1] K. Conrad, *Infinite Galois theory*, `https://ctnt-summer.math.uconn.edu/wp-content/uploads/sites/1632/2020/06/CTNT-InfGaloisTheory.pdf`.

[2] B. Mazur, *Rational points on modular curves*, Modular functions of one variable, V, Lecture notes in Math., Vol. 601 (1977), 107–148.

[3] B. Mazur, *Modular curves and the Eisenstein ideal,* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977).

[4] B. Mazur, *Rational isogenies of prime degree.* Invent. Math. Vol. 44 (1978), 129–162.

[5] S. Siksek, *Explicit arithmetic of modular curves*, `http://homepages.warwick.ac.uk/~maseap/teaching/modcurves/lecturenotes.pdf`.

[6] J. Silverman, *The arithmetic of elliptic curves*, 2nd Ed., Graduate Texts in Mathematics, vol. 106, Springer (2009).

[7] D. Zureick-Brown, *Progress on Mazur's Program B*, `http://www.math.emory.edu/~dzb/slides/DZB-JMM-program-B.pdf`.

[5] $K^{(1)}$ denotes the *Hilbert class field* of K. It is the maximal unramified abelian extension of K. By the theory of CM, one has $K^{(1)} = K(j(E))$ for any $\mathcal{O}_K$-CM elliptic curve E.