Complex multiplication

M. Jauch, G. Wolff

28.11.2023

Motivation

In this talk we will present some theory of elliptic curves with complex multiplication. Here is a non-conclusive list of reasons to be interested in the topic:

1. Cryptography. We will present a key exchange based on isogenies between elliptic curves.

2. Numerical phenomena. One of these phenomena:

$$e^{\pi\sqrt{163}} = 262537412640768743.9999999999992... \approx 640320^3 + 744.$$

One can explain this phenomenon with properties of the j-invariant and its connection to imaginary quadratic number fields.

Another one:

$$n^2 + n + 41$$

is prime for the first 40 integers $n = 0, 1, 2, ..., 39$. Here $163 = 4 \cdot 41 - 1$.

3. Study maps. As always one studies maps between the objects to understand the objects better and to discover more structure. As an example for a map from one curve to another, we already saw transformations from general forms into Weierstrass form. The first maps from a curve to itself on might come up with, could be translation by a point (not an isogeny) and multiplication by n. By playing around one might discover more maps that work for some elliptic curves but not for others. See example below.

4. Class field theory. Kronecker's Jugentraum, Hilbert's 12th problem. The theory of complex multiplication is used for an amazing (check choice of adjective) result in the study of number fields and their extensions: a proof of a special case of Kronecker's Jugendtraum. The final theorem of this talk (if enough time) will give an analogue to the Kronecker-Weber theorem for the more general case of allowing imaginary quadratic number fields as the base field. For a short recap of number fields and the statement of Kronecker-Weber, see appendix B.

1 Maps between elliptic curves

We want to understand the different maps there are between elliptic curves. This helps us to classify different kinds of curves. The structure and most of the content of this section were taken from [2].

1.1 Homomorphisms and Isogenies

We first want to study analytic homomorphisms $\phi : \mathbb{C} \to \mathbb{C}/L$. One can show that all homomorphisms can be characterized by a unique linear map:

Proposition 1.1. *Let L be a lattice in $\mathbb{C}$. For every analytic homomorphism ϕ like above, there exists a unique linear map $\lambda : \mathbb{C} \to \mathbb{C}$ which makes the following diagram commute:*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\lambda} & \mathbb{C} \\ & \searrow^{\phi} & \downarrow{\scriptstyle \pi_L} \\ & & \mathbb{C}/L \end{array}$$

Where π_L is the universal covering of any torus. (Recall: $\mathbb{C}/L$ is a complex torus.)

Proof. We want to show that $\phi(x) = \pi_L(\lambda x)$. We know that for π_L: $\pi_L(0) = 0$ and is continuous in 0 and therefore locally injective in a neighbourhood U of 0. Thus $\phi_L|U : U \to V$ is a bijection for any open set $V \subset \mathbb{C}/L$. Defining

$$f := (\pi_L|_U)^{-1} \circ \phi$$

which is analytic and preserves addition in a neighbourhood $W \subset \mathbb{C}$ of 0, for $x, y, x + y \in W$. Taking the derivative with respect to y gives that $f'(x + y) = f'(y)$. Setting $y = 0$ yields $f'(x) = f'(0) = \lambda$, i.e., the derivative is constant and thus $f(x) = \lambda x$ is linear (using $f(0) = 0$).

This means that $\phi(x) = \pi_L(\lambda x)$ locally. But since $\phi(x) - \pi_L(\lambda x)$ is analytic and vanishes in a neighbourhood of 0, it follows that $\phi(x) = \pi_L(\lambda x)$ everywhere. □

As a direct consequence we get the following.

Proposition 1.2. *Let now $f : \mathbb{C}/L \to \mathbb{C}/M$ be an analytic homomorphism. Then there exists a unique linear map such that the following diagram commutes. This means that f factors through a $\lambda \in \mathbb{C}$.*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\lambda} & \mathbb{C} \\ \downarrow{\scriptstyle \pi_L} & \overset{\phi}{\searrow} & \downarrow{\scriptstyle \pi_M} \\ \mathbb{C}/L & \xrightarrow{f} & \mathbb{C}/M \end{array}$$

Proof. To see this, notice that for the analytic homomorphism $\phi : \mathbb{C} \to \mathbb{C}/M$, $\phi = f \circ \pi_L$ factors through a $\lambda \in C$ via $\phi = \pi_M \circ \lambda$ which implies $\pi_M \circ \lambda = f \circ \pi_L$. □

This motivates us to have a closer look at analytic maps between elliptic curves. Record the following properties:

Proposition 1.3. *Let $f : E_1 \longrightarrow E_2$ be an analytic homomorphism of elliptic curves. Then*

i) $f(E_1) = \mathcal{O} \quad or \quad f(E_1) = E_2$.

ii) If f is not constant, $ker(f)$ is finite.

Proof. This is the idea of the proof:

i) If $\lambda = 0$, then $f(E) = \mathcal{O}$. Otherwise $\lambda \neq 0$ and $x + M$ is the image of $\lambda^{-1}x + L$.

ii) $ker(f) = \{z \in \mathbb{C}/L : \lambda z \in M\}$. This is a discrete set in a compactum. □

Definition 1.4. *We call an analytic map $f : \mathbb{C}/L \to \mathbb{C}/M$ as above an isogeny if it has finite kernel. The degree of an isogeny is defined via it's kernel:*

$$def(f) = \#ker(f)$$

for a non zero isogeny f and $deg(f) = 0$ else.

This immediately yields two properties about isogenies. With the Proposition above we get:

Proposition 1.5. *If $f : \mathbb{C}/L \to \mathbb{C}/M$ is an isogeny, then there exists a $\lambda \in \mathbb{C}$ such that $f(z) = \lambda z$ and $\lambda L \subset M$.*

Proposition 1.6. *Given two lattices such that $\lambda L \subset M$ with $\lambda \in \mathbb{C}$ there exists an isogeny $f : \mathbb{C}/L \to \mathbb{C}/M$, via $f(x + L) = \lambda x + M$.*

In this setting there also exists an isogeny $\mathbb{C}/M \to \mathbb{C}/L$ since $\mu M \subset L$ for some $\mu \in \mathbb{C}$ by property of latticies. We call this map the dual isogeny.

Definition 1.7. *In the case of the above to propositions, we say that $\mathbb{C}/L$ and $\mathbb{C}/M$ are isogenous.*

Note, that being isogenous defines an equivalence relation. Also, an isogeny does not need to be an isomorphism. The dual isogeny is not its inverse!

We want to state Tate's isogeny theorem.

Theorem 1.8. *Two elliptic curves over a finite field k are isogenous over k if and only if the have the same number of k-rational points.*

1.2 Isomorphisms

Now we let $f : \mathbb{C}/L \to \mathbb{C}/M$ be an analytic isomorphism. We have seen above, that f factors through a linear map $\mathbb{C} \to \mathbb{C}$, $x \mapsto \lambda x$ through the canonical surjective projections π_L and π_M and $\lambda L \subset M$. The inverse isomorphism f^{-1} factors through $x \mapsto \lambda^{-1}x$ and therefore $\lambda^{-1}M \subset L$. We conclude, that $\lambda L = M$.

This motivates the following definition.

Definition 1.9. *Two elliptic curves $\mathbb{C}/M$ and $\mathbb{C}/L$ are called isomorphic, if there exists an invertible isogeny between them, i.e., a map as described above.*

Note: an invertible isogeny has degree 1.

Theorem 1.10. *Let L and M be two lattices in $\mathbb{C}$. The corresponding elliptic curves $\mathbb{C}/M$, $\mathbb{C}/L$ are isomorphic if and only if their j-invariant agrees.*

In order to understand this theorem, we want to recall the the definition of the j-invariant corresponding to a lattice L.

Definition 1.11. *Given a lattice L, the j-invariant is defined as the function*

$$j(L) = \frac{1728 g_2^3(L)}{\Delta(L)}$$

Where Δ is the discriminant

$$\Delta(L) = g_2^3(L) - 27g_3^2(L)$$

defined with the Weierstrass invariants

$$g_2 = 60G_4(L) = 60 \sum_{w \in L^x} w^{-4}$$

$$g_3 = 140G_6(L) = 140 \sum_{w \in L^x} w^{-6}$$

We can show that for two isomorphic lattices M and L, i.e. when $M = \lambda L$ for $\lambda \in \mathbb{C}^x$. The j-invariant agrees:

Proposition 1.12. *$M = \lambda L$ if and only if $j(L) = j(M)$.*

This follows from the properties from g_2 and g_3 as one can show with easy calculations that

$$g_2(\lambda L) = \lambda^{-4} g_2(L)$$
$$g_3(\lambda L) = \lambda^{-6} g_3(L)$$

for any λ.

1.3 Endomorphisms

We have seen that an analytic homomorphism $\phi : E_1 \longrightarrow E_2$ of elliptic curves corresponds to multiplication by a complex number (when viewing the elliptic curves as $\mathbb{C}/L$ and $\mathbb{C}/M$ respectively). We call such a map an isogeny.

Remark 1.13. *I believe the reason we look at analytic homomorphisms is because $\mathbb{C}/L$ is a Riemann surface that has a group structure. Apparently we could have instead required the map ϕ to be a rational map of projective varieties that preserves $\mathcal{O}$, also a natural choice considering that elliptic curves are projective varieties with a specified point $\mathcal{O}$. Such a map is then automatically a morphism of varieties (because it is defined on smooth curves), and then automatically a homomorphism of groups, and then again multiplication by a complex number. The details of the latter way of arriving at isogenies are contained in [4], III.4.*

We now look at the case that $E_1 = E_2$; so isogenies from an elliptic curve $\mathbb{C}/L$ to itself; so the maps that correspond to $\lambda \in \mathbb{C}$, such that $\lambda L \subseteq L$.

Proposition 1.14. *If $\lambda L \subseteq L$, then*

i) λ is a rational integer or an algebraic integer in an imaginary quadratic number field.

ii) $\wp_L(\lambda z)$ is a rational function of $\wp_L(z)$ such that the degree of the numerator is λ^2 if $\lambda \in \mathbb{Z}$, and $N(\lambda)$ if λ is imaginary quadratic; the degree of the denominator is $\lambda^2 - 1$ and $N(\lambda)^2 - 1$, respectively.

Proof. i) If $\lambda L \subseteq L = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$, then

$$\begin{cases} \lambda\omega_1 = a\omega_1 + b\omega_2, \\ \lambda\omega_2 = c\omega_1 + d\omega_2, \end{cases}$$

with $a, b, c, d \in \mathbb{Z}$. This implies

$$\frac{\omega_1}{\omega_2} = \frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d}$$

or, by putting $\tau = \omega_1/\omega_2$:

$$c\tau^2 + (d-a)\tau - b = 0.$$

If λ is not a rational integer, then $c \neq 0$, and τ is a quadratic imaginary number (imaginary, since ω_1/ω_2 cannot be real). Since $\lambda = c\tau + d$, this shows that λ is an element of $\mathbb{Q}(\tau)$, an imaginary quadratic field. Now we confirm $\lambda^2 - (a + d)\lambda + ad - bc = 0$, so λ is an algebraic integer.

ii) Since $\lambda L \subseteq L$, $\wp_L(z)$ is elliptic with respect to L: $\wp_L(\lambda(z + \omega)) = \wp(\lambda z + \lambda\omega) = \wp(\lambda z)$ and it is even because $\wp$ is. The idea of the proof is as usual: to build a function with the same poles and zeroes as $\wp_L(\lambda z)$ out of building blocks of the form $(\wp(z) - \alpha)^{n_\alpha}$. I will not do it here but note that this strategy works for any even elliptic function over L and actually we have the following result: $\mathcal{E}_L = \mathbb{C}(\wp) + \wp'\mathbb{C}(\wp)$, (where $\mathcal{E}_L$ denotes the elliptic functions with respect to the lattice L.)

To arrive at the degrees of numerator and denominator, note that α is a pole of $\wp(\lambda z)$ iff $\lambda\alpha$ is a pole of $\wp$ iff $\alpha \in \frac{1}{\lambda}L$. The details can be found in [2]. □

Remark 1.15. *Part ii) of the previous proposition can be used to construct an explicit (yet by hand computationally unpleasant) algorithm to determine the curves with complex multiplication by a given λ.*

An example of an isogeny from an elliptic curve to itself (that exists for any curve), is multiplication by n:

$$[n] : E \longrightarrow E, \quad P \mapsto nP.$$

Since the addition is a rational map it is a morphism of curves and so is $[n]$. $[n]$ also preserves $\mathcal{O}$, so it is an isogeny. On the torus it corresponds to scaling by n. Actually we can say more:

Proposition 1.16. *$End(E)$ is a ring and the map*

$$[\ ] : \mathbb{Z} \hookrightarrow End(E), \quad n \mapsto [n]$$

is an injective group homomorphism.

If $End(E)$ is strictly larger than $\mathbb{Z}$ (so E has a non trivial isogeny to itself) we say that E has complex multiplication.

Proof. I will sketch the proof.

$End(E)$ is a ring: Define the addition as $(\phi + \psi)(P) = \phi(P) + \psi(P)$, where the latter addition is addition on E. Then $\phi + \psi$ is an isogeny, because the addition on E is defined by a rational map that preserves $\mathcal{O}$, and both ϕ and

ψ are rational maps that preserve $\mathcal{O}$. Define multiplication by composition of maps.

That $n \mapsto [n]$ is injective and a homomorphism can be seen when thinking about what $[n]$ does on $\mathbb{C}/L$. □

Corollary 1.17. *Let E be a CM-curve. Then $End(E)$ is an order $\mathcal{O}$ in an imaginary quadratic field.*

Example 1.18. *Take the elliptic curve $E : y^2 = x^3 - x$. Multiplication by n is an isogeny and this always works. But there is the extra map we denote $[i]$*

$$[i] : E \longrightarrow E, \quad (x, y) \mapsto (-x, iy).$$

Notice that

$$[i] \circ [i](x, y) = (x, -y) = -(x, y) = [-1](x, y)$$

Note for when the fundamentals are understood: This shows that if the base field contains i, $End(E)$ is strictly larger than $\mathbb{Z}$. Also

$$\mathbb{Z}[i] \longrightarrow End(E), \quad m + ni \mapsto [m] + [n]i$$

Is a ring homomorphism, that is an isomorphism in $char(K) = 0$. Then $Aut_K(E) = \mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

Which are the curves with complex multiplication by a given ring of integers?

Theorem 1.19. *Let K be imaginary quadratic.*

1. *$End(E) \cong \mathcal{O}_K \Rightarrow E \cong \mathbb{C}/\Lambda$, where $\Lambda \subseteq \mathcal{O}_K$ is an ideal.*
2. *$\Lambda \subseteq \mathcal{O}_K$ an ideal $\Rightarrow End(\mathbb{C}/\Lambda) \cong \mathcal{O}_K$.*
3. *$End(E) \cong \mathcal{O}_K \iff E \cong \mathbb{C}/\Lambda$, $\lambda \subseteq \mathcal{O}_K$ ideal.*
4. *If Λ_1, Λ_2 are in the same ideal class, then $\mathbb{C}/\Lambda_1 \cong \mathbb{C}/\Lambda_2$.*

Proof. Again, I sketch only the ideas.

1. E needs to be of the form $\mathbb{C}/L$, where L is a lattice that is closed under multiplication by $\mathcal{O}_K$.

2. If Λ is an ideal in $\mathcal{O}_K$, it is closed under multiplication by $\mathcal{O}_K$ and $End(\mathbb{C}/\Lambda) \cong \{\alpha \in \mathbb{C} : \alpha\Lambda \subseteq \Lambda\}$.

3. Restatement of 1. and 2.

4. If two ideals are in the same ideal class, they are related by a principal fractional ideal $\Lambda_1 = \mathfrak{a}\Lambda_2$, $\mathfrak{a}^{-1}\Lambda_1 = \Lambda_2$ (remember that non-zero fractional ideals are invertible in number fields). But Λ_1 and Λ_2 are lattices and these relations imply that each lattice can be obtained from the other by multiplication with a complex number. □

1.4 Auto

Automorphisms of an elliptic curve correspond to λ such that $\lambda L = L$.

If the curve does not have complex multiplication, then $End(E) \cong \mathbb{Z}$ and $\lambda = \pm 1$ are the only maps that are injective and they are indeed automorphisms.

If the curve has complex multiplication then we saw that $End(E) \cong \mathcal{O}$, for some order $\mathcal{O} \subseteq \mathcal{O}_K$ in an imaginary quadratic number field K. Then the automorphisms are the invertible elements of $\mathcal{O}$, i.e. the elements in $\mathcal{O}^\times \subseteq \mathcal{O}_K^\times$.

Remember (see B.12) that for an imaginary quadratic field K

$$\mathcal{O}_K^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if} \quad K = \mathbb{Q}(i), \\ \left\{\pm 1, \frac{\pm 1 \pm \sqrt{-3}}{2}\right\} & \text{if} \quad K = \mathbb{Q}(e^{2\pi i/3}), \\ \{\pm 1\} & \text{else.} \end{cases}$$

2 Class field theory

The following theorem is a classic result in a area that is now called class field theory.

Theorem 2.1 (Kronecker-Weber Theorem)**.** *Every finite abelian extension*[1] *of* $\mathbb{Q}$ *is contained in some cyclotomic field.*

Remark 2.2. *Note that a cyclotomic field is an extension of* $\mathbb{Q}$ *by a special value of the* exp *function.*

Kronecker's Jugendtraum (and Hilbert's twelfth problem) is the extension of the Kronecker-Weber theorem to any number field as a base field (instead of $\mathbb{Q}$*). Preferably one would like to find the maximal abelian extension of a number field* K*, or perhaps all abelian extension of* K*, by adjoining special values of some function to* K*. With the theory of complex multiplication one can show that this is possible in the case where the number field is an imaginary quadratic field.*

Example 2.3. *The quadratic number field* $K = \mathbb{Q}(\sqrt{5})$ *is galois since it is the splitting field of* $x^2 - 5$ *and the base field* $\mathbb{Q}$ *has characteristic 0. There are two embeddings: the identity and the one that swaps* $\sqrt{d}$ *and* $-\sqrt{d}$*, hence* $|Gal(K/\mathbb{Q})| = 2$ *and* $Gal(K/\mathbb{Q}) \cong C_2$*. Since* C_2 *is abelian,* K *is an abelian extension of* $\mathbb{Q}$ *and the Kronecker-Weber theorem tells us that* $K \subseteq \mathbb{Q}(\zeta_n)$ *for* ζ_n *some primitive* n*-th root of unity. It turns out that*

$$\sqrt{5} = e^{2\pi i/5} - e^{4\pi i/5} - e^{6\pi i/5} + e^{8\pi i/5},$$

so

$$\mathbb{Q}(\sqrt{5}) \subset \mathbb{Q}(\zeta_5) = \mathbb{Q}(e^{2\pi i/5}).$$

One can go one step further and remember from the beloved algebra class that $Gal(\mathbb{Q}(\zeta_5)) = C_4$ *which has only one subgroup:* C_2*.*

In general $\mathbb{Q}(\sqrt{d})) \subset \mathbb{Q}(\zeta_D)$*, where* D *is the absolute value of the discriminant of* $\mathbb{Q}(\sqrt{d})$*. So all quadratic fields are actually just subfields of cyclotomic fields, which are extensions of* $\mathbb{Q}$ *by special values of the* exp *function.*

Theorem 2.4 (Extension of Kronecker-Weber to imaginary quadratic base fields)**.** *Let* K *be an imaginary quadratic number field with class number* h *and let* $C_1, ..., C_h$ *denote the ideal classes in* $Cl(K)$*. Let* j *denote the* j*-invariant. Then*

[1] A galois extension is called abelian if the galois group is abelian.

i) The values $j(C_1), ...j(C_h)$ are distinct algebraic integers of degree h, they are called singular moduli.

ii) The field $H = K(j(C_i))$ does not depend on i; the values $j(C_i)$ are conjugated over K, and H is the Hilbert class field of K (the maximal unramified abelian extension of K; it has degree $[H : K] = h(K)$).

iii) There exists a bijection between the ideal class group $Cl(K)$ of K and the Galois group of H/K; this bijection is in fact an isomorphism given by $\mathfrak{a} \mapsto \sigma_{\mathfrak{a}} \in Gal(H/K)$, where $\sigma_{\mathfrak{a}}(j(C_i)) = j([\mathfrak{a}]^{-1}C_i)$.

iv) $j(\mathfrak{a})$ is real if and only if $\mathfrak{a}$ has order dividing 2 in $Cl(K)$; in particular, $j(\mathcal{O}_K)$ is real, and $[\mathbb{Q}(j(\mathcal{O}_K)) : \mathbb{Q}] = h$.

v) The maximal abelian extension of K is given by adjoining all elements of the form

$$\tau\left(\frac{1}{n}(a\omega_1 + b\omega_2)\right), \quad a, b \in \mathbb{Z},\ n \in \mathbb{N}$$

to the Hilbert class field H of K. Here ω_1 and ω_2 are the periods of the lattice $\mathbb{C}/\mathcal{O}_K$ and the function τ is an expression in $\wp, g_2, g_3$ and depends on $|\mathcal{O}_K^\times|$. The definition of tau follows this theorem.

Definition 2.5. *Let $e = |\mathcal{O}_K^\times|$ The function τ from the previous theorem is defined as*

$$\tau(u) = (-\wp(u))^{e/2} g^{(e)},$$

where one defines $g^{(e)}$ by

$$g^{(2)} = 2^7 3^5 g_2 g_3 \Delta^{-1}; \quad g^{(4)} = 2^8 3^4 g_2^2 \Delta^{-1}; \quad g^{(6)} = 2^9 3^6 g_3 \Delta^{-1}.$$

The reason that one has to distinguish the cases $e = 2, 4, 6$ in this definition ($e = 4, 6$ being the exceptional cases $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$), is somehow connected to the zeroes of the Eisenstein series:

$$g_2(\rho) = g_3(i) = 0.$$

Here $\rho = e^{2\pi i/3} = \frac{-1+\sqrt{3}}{2}$.

Now we are ready to understand why $e^{\pi\sqrt{163}}$ is almost an integer.

Example 2.6. *Let d be an integer such that $h(\mathbb{Q}(\sqrt{-d})) = 1$ and $-d \equiv 1$ mod 4. By the Stark-Heegner theorem we know this is the case when $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ and $d \geq 11$.*

By theorem 2.4, $j(\mathcal{O}_K) = j(\tau_K) = j(\frac{1+\sqrt{-d}}{2})$ is an algebraic integer of degree 1, i.e. an integer $m \in \mathbb{Z}$. Remember the Laurent expansion of the j-invariant

$$j(\tau) = q^{-1} + 744 + 196884q + \mathcal{O}(q^2).$$

Thus

$$\begin{aligned} m = j(\frac{1+\sqrt{-d}}{2}) &= e^{-\pi i(1+\sqrt{-d})} + 744 + 196884 \cdot e^{\pi i(1+\sqrt{-d})} + ... \\ &= -e^{\pi\sqrt{d}} + 744 + \mathcal{O}\left(e^{-\pi\sqrt{d}}\right). \end{aligned}$$

Now for example for $d = 163$ we have $j(\frac{1+\sqrt{-d}}{2}) = (-640320)^3$ and the linear error term is $196884 \cdot e^{-\pi\sqrt{-d}} \approx 0.00000000000075$.

3 Cryptography

We now want to take a look at isogenies that are relevant for cryptography. We consider elliptic curves over $\mathbb{F}_{p^n}$ where p is a prime larger than 3 and $n > 0$ an integer. We write the elliptic curve in short Weierstrass form

$$E : y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_{p^n}, \quad 4a^3 + 27b^2 \neq 0.$$

Recall that isomorphism classes of elliptic curves has the j-invariant as a unique representative for each class.

Definition 3.1. *An elliptic curve over $\mathbb{F}_{p^n}$ is called supersingular if it has $p^n + 1 - kp$ many points for some integer k such that $kp \in [-2p^{n/2}, 2p^{n/2}]$.*

Generally speaking, this definition implies that the elliptic curve has complex multiplication.

An isogeny of order l has as kernel a cyclic subgroup of order l. Important is, that each kernel uniquely defines an isogeny, which can be computed efficiently by Velu's formula with complexity growing linearly in l. Velu's formula gives an explicit equation of the image curve and the isogeny in terms of the coordinates of the points in the kernel.

Velu's formulas are as follows:

Theorem 3.2. *Given an elliptic curve E_A and a point P with prime order l on E_A. For $1 \leq ill$ let X_i be the X-coordinare of $[i]P$. And let*

$$\tau = \prod_{i=1}^{l-1} X_i, \quad \sigma = \sum_{i=1}^{l-1} \left(X_i - \frac{1}{X_i}\right), \quad f(x) = x \prod_{i=1}^{l-1} \frac{xX_i - 1}{x - X_i}.$$

Then the l-isogeny with kernel $\langle P \rangle$ is given by

$$\varphi_l : E_A \to E_{A'}, (X, Y) \mapsto (f(X), c_0 Y f'(X))$$

where $A' = \tau(A - 3\sigma)$, and $c_0^2 = \tau$.

3.1 Isogeny Graphs

We now specifically look at isomorphism classes of supersingular elliptic curves over extensions of $\mathbb{F}_{p^2}$. We now consider a graph $G = (V, E)$, where the vertices E are the isomorphism classes of elliptic curves and edges E are isogenies of degree l between elliptic curves. Notice that this graph is undirected because of the dual isogeny.

Again, a vertex in the graph corresponds to an isomorphism class uniquely characterized by its j-invariant. The isomorphisms are taken over field extensions of $\mathbb{F}_{419^2}$.

Choosing the parameters specifically over extensions of $\mathbb{F}_{p^2}$ gives us, that the graph of l isogenies is (almost) $l+1$ connected and Ramanujan. This essentially means that the graph is highly connected and any vertex in the graph can be reached by using only a few edges from any other vertex. When computing a path of isogenies, at each vertex one has a choice of l edges to go forward.

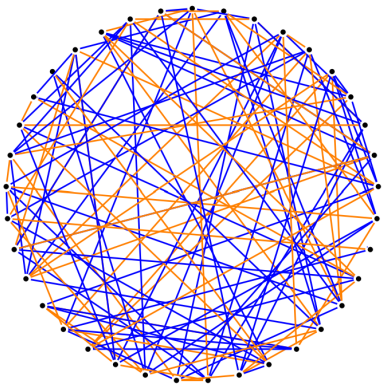

Figure 1: This figure shows an example of an isogeny graph: the supersingular elliptic curves over $\mathbb{F}_{419^2}$. Edges are 2 (orange) and 3 (blue) isogenies.

3.2 The SIDH system

The SIDH system is a key exchange protocol. In cryptography, key exchanges are needed, such that two parties that wish to communicate with each other using encrypted messages, can agree on a key under which encryption is performed. In the literature, these two paries are usually refered to as Alice and Bob. Key exchange protocols are useful, as using those Alice and Bob can agree on a key while communicating via a potentially corrupted channel but the key will still only be known by Alice and Bob. It is obviously a lot more convenient to agree to a mutual key via e.g. the internet instead of physically meeting up and agreeing on a key.

SIDH precisely uses isomorphism classes of supersingular curves over $\mathbb{F}_{p^2}$ to generate an isogeny graph like above. The general idea is to perform walks on the isogeny graph and that Alice and Bob can, starting at the same vertex V, then both perform different walks $\varphi_{A,B} : V \to W$ and end up at the same vertex W. The vertex W then corresponds to an isomorphism class with some j-invariant, which then is used as the input to a key-generation algorithm.

SIDH is a key exchange protocol based on the difficulty of computing isogenies between supersingular elliptic curves. Let E_0 be a supersingular elliptic curve over a finite field $\mathbb{F}_{p^2}$, where p is a prime. The SIDH protocol involves the following steps:

First, points P_A, Q_A and P_B, Q_B are chosen on the elliptic curve which both are a basis of points of a specific order.

1. **Key Generation + Isogeny Computation:**
    - Choose random secret keys a and b from a finite key space.
    - Alice computes $T_A = P_A + aQ_A$ and the isogeny ϕ_A with kernel $\langle T_A \rangle$ landing at curve E_A.
    - Bob computes $T_B = P_B + bQ_B$ and the isogeny ϕ_B with kernel $\langle T_B \rangle$ landing at curve E_B

- Bob computes and publishes $\phi_B(P_A)$ and $\phi_B(Q_A)$ likewise for Alice, she publishes $\phi_A(P_B)$ and $\phi_A(Q_B)$.

2. **Secret Agreement:**

   - Alice computes $T'_A = \phi_B(P_A) + a\phi_B(Q_A)$ and the isogeny ϕ'_B with kernel $\langle T'_A \rangle$, landing at E_{AB}.
   - Bob computes $T'_B = \phi_A(P_B) + b\phi_A(Q_B)$ and the isogeny ϕ'_A with kernel $\langle T'_B \rangle$, landing at E_{BA}.

The calculations to obtain isogenies and image curves are done using Velu's formula as described above.

The curves E_{AB} and E_{BA} are not necessarily the same curves, but they belong to the same isomorphism class of curves and thus share the same j-invariant.

To summarize Alice's secret key is a and her public key is $(E_A, \phi_A(P_B), \phi_A(Q_B))$ and similarly for Bob. This corresponds to the following diagram that commutes:

$$\begin{array}{ccc} E & \xrightarrow{\phi_A} & E_A \\ \downarrow{\scriptstyle \phi_B} & & \downarrow{\scriptstyle \phi'_B} \\ E_B & \xrightarrow{\phi'_A} & E_{AB} \end{array}$$

SIDH then uses the j-invariant of the resulting curve to compute a shared key. The security of this system relies on the hardness to compute E_{AB} given $E, E_A, E_B, \phi_B(P_A), \phi_B(Q_A), \phi_A(P_B), \phi_A(Q_B)$. It has long been considered to be hard, but in July of 2022 an efficient attack has been found using Torsion points that makes the scheme in this form useless.

References

[1] D.A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley (2013).

[2] M. Waldschmidt, *Complex Multiplication* (2003).

[3] S. Zerbes, *Lecture Notes of "Number Theory I"*, (Fall semester 2022 at ETH Zürich). Based partly on I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, CRC Press (2016).

[4] J.H. Silverman, *The Arithemtic of Elliptic Curves*, Springer (2016).

[5] L. Panny, *Elliptic curves and isogenies: The good bits*, Week 1 of the Isogeny-based Cryptography School, originally planned in 2020, Bristol, `https://yx7.cc/docs/misc/isog_bristol_notes.pdf`.

[6] T. Lange, *(C)SIDH - Isogeny school week 3*, July 18th 2021, `https://www.hyperelliptic.org/tanja/teaching/isogeny-school21/csidh-sidh-week-3.pdf`.

A Collection of previous results

The following summarizes the results of the seminar up to this point.

An elliptic curve E is a non-singular projective plane curve. Without loss of generality we may assume the elliptic curve to be given in Weierstrass form, i.e. we may think of $E(K)$ as the solutions in K of $y^2 = 4x^3 - g_2x - g_3$ together with a point $\mathcal{O}$ at infinity.

It turns out that $E(K)$ has a group structure. Mordell's theorem states that for an elliptic curve defined over $\mathbb{Q}$, $E(\mathbb{Q})$ is a finitely generated abelian group.

(We have also seen results about the torsion part of $E(\mathbb{Q})$ and the integer points, but these are not immediately relevant for this topic.)

Of greater importance to this talk: $E(\mathbb{C}) \cong \mathbb{C}/L$ where L is a lattice and the isomorphism is among other things an isomorphism of groups. One may picture addition on the elliptic curve as addition in the fundamental parallelogram $\mathbb{C}/L$.

B Recap number fields

The following results were not presented in the seminar but they are important to understand what the talk is about.

Definition B.1. *An algebraic integer is a complex root of a monic polynomial with coefficients in $\mathbb{Z}$. We denote the set of algebraic integers by $\mathbb{A}$. An algebraic number is a complex root of a polynomial (not necessarily monic) with coefficients in $\mathbb{Z}$ (or equivalently $\mathbb{Q}$). We denote the set of algebraic numbers by $\overline{\mathbb{Q}}$, as it is the algebraic closure of $\mathbb{Q}$.*

Definition B.2. *A number field K is a finite extension of $\mathbb{Q}$, i.e. a field extension of $\mathbb{Q}$ with $[K : \mathbb{Q}] < \infty$.*

Remember that the degree of an extension E/F is defined as the dimension of E as a vector space over F.

Proposition B.3. *Any number field K is a simple extension of $\mathbb{Q}$ by an algebraic number, that is $K = \mathbb{Q}(\alpha) \subset \mathbb{C}$, with $\alpha \in \overline{\mathbb{Q}}$.*

Definition B.4. *The ring of integers $\mathcal{O}_K$ of a number field K is the ring $\mathcal{O}_K = K \cap \mathbb{A}$, i.e. the elements of K that are roots of a monic polynomial in $\mathbb{Z}[X]$.*

Definition B.5. *The following definitions are equivalent and define an order $\mathcal{O}$ of a number field K. $\mathcal{O} \subset \mathcal{O}_K$ is a subring of the ring of integers that*

a) has rank $[K : \mathbb{Q}]$ when regarded as a $\mathbb{Z}$-module (so the largest possible rank);

b) has finite index in $\mathcal{O}_K$;

c) contains a $\mathbb{Q}$ basis of K;

d) has K as its field of fractions.

$\mathcal{O}_K$ is called the maximal order. The index $f = [\mathcal{O}_K : \mathcal{O}]$ is called the conductor of $\mathcal{O}$.

Definition B.6. *An integral basis is a $\mathbb{Q}$-basis of K that is also a $\mathbb{Z}$-basis of $\mathcal{O}_K$.*

Proposition B.7. *Every number field K has an integral basis of size $n = [K : \mathbb{Q}]$.*

Example B.8. *i) $K = \mathbb{Q}$ is a number field over $\mathbb{Q}$ of degree 1. Its ring of integers are the integers: $\mathcal{O}_K = \mathbb{Z}$. Any ring of the form $n\mathbb{Z}$ for $n \in \mathbb{N}$ is an order in $\mathbb{Q}$.*

ii) $K = \mathbb{Q}(i)$ is a number field since it is a field extension over $\mathbb{Q}$ of degree 2; in fact $\mathbb{Q}(i) = \{a + ib \ : \ a, b \in \mathbb{Q}\}$ is a vector space over $\mathbb{Q}$ of dimension 2. Its ring of integers is $\mathcal{O}_K = \mathbb{Z}[i] = \{a + ib \ : \ a, b \in \mathbb{Z}\} = \mathbb{Z} + i\mathbb{Z}$, a lattice. Notice that this implies that $\{1, i\}$ is an integral basis of $\mathbb{Q}(i)$. $Z[2i] = \mathbb{Z} + 2i\mathbb{Z}$ is an order in K, as it has conductor 2, and it is a sublattice of $\mathbb{Z} + i\mathbb{Z}$. $\mathbb{Z}$, $2\mathbb{Z} + 2i\mathbb{Z}$ and $2\mathbb{Z} + i\mathbb{Z}$ are not orders in $\mathbb{Z}[i]$, however the former two are ideals. Notice that ideals and orders of $\mathbb{Z}[i]$ are sublattices of $\mathbb{Z}[i]$: Both are certainly subsets of the lattice and both are additive subgroups.

Definition B.9. *A number field is called quadratic if it has degree two. It is called imaginary quadratic if it is not contained in $\mathbb{R}$.*

Proposition B.10. *A quadratic number field is of the form $\mathbb{Q}(\sqrt{d})$ for some square-free, non-zero integer d. It is imaginary quadratic if and only if $d < 0$.*

The number fields that are least difficult to study are imaginary quadratic number fields and cyclotomic fields ($\mathbb{Q}(\zeta_n)$, where ζ_n is a root of unity). For our talk it is helpful to understand imaginary quadratic number fields, particularly their rings of integers.

Theorem B.11. *The ring of integers in an imaginary quadratic number field $K = \mathbb{Q}(\sqrt{d})$ (i.e. for $d \in \mathbb{Z}_{<0}$ square-free) is $\mathcal{O}_K = \mathbb{Z}[\tau_d]$, where*

$$\tau_d = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \text{ mod } 4, \\ \dfrac{1 + \sqrt{d}}{2} & \text{if } d \equiv 1 \text{ mod } 4. \end{cases}$$

Theorem B.12. *Let $K = \mathbb{Q}(\sqrt{d})$ be imaginary quadratic. Then the units of the ring of integers are*

$$(\mathcal{O}_K)^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if } \ d = \text{-1}, \\ \left\{\pm 1, \dfrac{\pm 1 \pm \sqrt{-3}}{2}\right\} & \text{if } \ d = \text{-3}, \\ \{\pm 1\} & \text{else.} \end{cases}$$

In particular

$$|(\mathcal{O}_K)^\times| = \begin{cases} 4 & \text{if } \ d = \text{-1}, \\ 6 & \text{if } \ d = \text{-3}, \\ 2 & \text{else.} \end{cases}$$

Proposition B.13. *Let $K = \mathbb{Q}(\sqrt{d})$ be imaginary quadratic. An integral basis of K is given by $\{1, \tau_K\}$.*

Corollary B.14 (Orders are lattices)**.** *Let $K = \mathbb{Q}(\sqrt{d})$ be imaginary quadratic. By the previous proposition, $\mathcal{O}_K$ is the lattice $\mathbb{Z} + \tau_K\mathbb{Z}$. Since any order of K needs to contain 1, any order of K is of the form $\mathbb{Z} + f \cdot \tau_K\mathbb{Z}$ for some $f \in \mathbb{N}$.*

The following concept is used in proposition 1.14.

Definition B.15. *Let $K/\mathbb{Q}$ be a number field of degree n and $\sigma_1, ..., \sigma_n$ the complex embeddings[2] of K. Then the norm of an element $\alpha \in K$ is defined as*

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$$

In case $K = \mathbb{Q}(\sqrt{d})$ is imaginary quadratic, this reduces to

$$N(a + b\tau_K) = (a + b\tau_K)(a + b\sigma(\tau_K)) = \begin{cases} a^2 - db^2 & \text{if } d \equiv 2, 3 \bmod 4, \\ a^2 + \dfrac{1-d}{4}b^2 & \text{if } d \equiv 1 \bmod 4. \end{cases}$$

We see that in the case of an imaginary quadratic number field $N(\alpha) \in \mathbb{Z}$ for $\alpha \in \mathcal{O}_K$.

We need one more concept about number fields: the class group. Note that in general $\mathcal{O}_K$ is not a unique factorization domain however factorization of ideals into prime ideals is unique. In order to show this (we will not look at this here) one introduces the ideal class group of a number field. It turns out that this group is an important piece of information when handling number fields and it will occur in the talk about complex multiplication, hence we introduce it here.

Definition B.16. *A fractional ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is a $\mathcal{O}_K$-submodule of K such that $c\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ for some $0 \neq c \in \mathcal{O}_K$.*

A principal fractional ideal is an $\mathcal{O}_K$-submodule of K that is generated by a single element $x \in K$, i.e. a fractional ideal of the form $(x) \coloneqq \{xy : \ y \in \mathcal{O}_K\}$ for some $x \in K$.

Proposition B.17. *The fractional ideals of a number field form a group, denote it by $\mathcal{I}_K$. The principal fractional ideals form a subgroup, denote it by $\mathcal{P}_K$.*

Definition B.18. *For a number field K, the ideal class group $Cl(K)$ is defined as the quotient the fractional ideals by the principal fractional ideals, $Cl(K) = \mathcal{I}_K/\mathcal{P}_K$.*

Proposition B.19. *$Cl(K)$ is finite and we may define the class number of the number field as $h(K) \coloneqq |Cl(K)|$.*

Remark B.20. *Notice that the class group is trivial and the class number is 1 iff every fractional ideal is principal. If every fractional ideal is principal then in particular all ideals of $\mathcal{O}_K$ are principal and thus $\mathcal{O}_K$ is a unique factorization domain.*

[2]The homomorphisms $K \hookrightarrow \mathbb{C}$, i.e. the elements of the galois group.