# Complex multiplication of elliptic curves

Andreas Enge

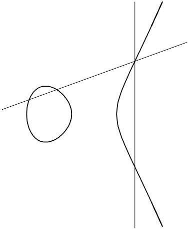
LFANT project-team
INRIA Bordeaux–Sud-Ouest
andreas.enge@inria.fr
http://www.math.u-bordeaux.fr/~aenge

FAST Workshop, Bordeaux, 6 September 2017

# Complex multiplication

# Elliptic curves

- $E : Y^2 = X^3 + aX + b, \quad a, b \in \mathbb{F}_p$
- Abelian variety of dimension 1 $\Rightarrow$ finite group



- Hasse 1934

$$|\#E(\mathbb{F}_p) - (p+1)| \leqslant 2\sqrt{p}$$

- Deuring 1941: All these cardinalities occur.

Literature: [Sch10]

# Primality proofs

If $P \in E(\mathbb{Z}/N_1\mathbb{Z})$ with $P$ of prime order $N_2$,

$$N_2 > \left(\sqrt[4]{N_1} + 1\right)^2,$$

then $N_1$ is prime.

Record: 25 050 decimal digits (Morain 2010)

# Cryptography

- Discrete logarithm based cryptography
  - Need prime cardinality
  - Prefer random curves
- Pairing-based cryptography Weil and (reduced) Tate pairing

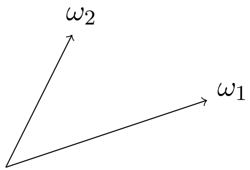
$$e : E(\mathbb{F}_p)[\ell] \times E(\mathbb{F}_{p^k})[\ell] \to \mathbb{F}_{p^k}^\times[\ell]$$

  - Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$
  - An exponential number of cryptographic primitives...
  - Need CM constructions for suitable curves.

## Definition 2.1

Let $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ with $\Im\left(\frac{\omega_2}{\omega_1}\right) > 0$ be a complex lattice. An *elliptic function* is a meromorphic function $f : \mathbb{C} \to \mathbb{C}$ with

$$f(z + \omega) = f(z) \quad \forall z \in \mathbb{C}, \omega \in L.$$




## Proposition 2.2

$\mathbb{C}/L$ is a compact Riemann surface of genus $1$.

## Definition 2.3

The Weierstraß $\wp$-function and its derivative are given by

$$\wp(z|L) = \frac{1}{z^2} + \sum_{\omega \in L}{}' \left( \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

$$\wp'(z|L) = -2 \sum_{\omega \in L} \frac{1}{(z-\omega)^3}$$

## Proposition 2.4

$\wp'$ is odd and elliptic, $\wp$ is even and elliptic. The field of elliptic functions is $\mathbb{C}(\wp, \wp')$.

## Definition 2.5

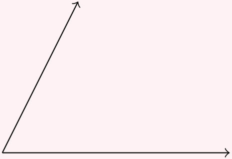
Let the *Eisenstein series* be defined by

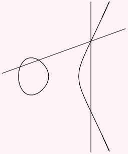
$$\begin{aligned} G_k(L) &= \sum_{\omega \in L}{}' \frac{1}{\omega^{2k}} \\ g_2(L) &= 60\, G_2(L) \\ g_3(L) &= 140\, G_3(L) \end{aligned}$$

## Proposition 2.6

The map

$$\mathbb{C}/L \;\to\; E : Y^2 Z = 4X^3 - g_2(L) X Z^2 - g_3(L) Z^3$$





$$z \;\mapsto\; \begin{cases} (\wp(z) : \wp'(z) : 1) & \text{for } z \notin L \\ \left( \frac{\wp(z)}{\wp'(z)} : 1 : \frac{1}{\wp'(z)} \right) & \text{in a neighbourhood of } 0 \end{cases}$$

$$0 \;\mapsto\; (0 : 1 : 0)$$

is a bijection between the additive group $\mathbb{C}/L$ and $E$.

The right hand side (in $Z = 1$) has discriminant

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

## Theorem 2.7 (Addition formula of $\wp$)

$$\wp(z_1 + z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1) - \wp'(z_2)}{\wp(z_1) - \wp(z_2)}\right)^2 \text{ for } z_1 \pm z_2 \notin L$$

$$\wp(2z) = -2\wp(z) + \frac{1}{4}\left(\frac{\wp''(z)}{\wp'(z)}\right)^2$$

$$= -2\wp(z) + \frac{1}{4}\left(\frac{12\wp(z)^2 - g_2}{2\wp'(z)}\right)^2 \text{ for } 2z \notin L$$

# Complex multiplication

## Definition 3.1

Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sl}_2(\mathbb{Z})$ and $k \in \mathbb{Z}$. We denote

$$\begin{aligned} (f \circ M)(z) &= f(Mz) = f\left(\frac{az+b}{cz+d}\right) \\ (f|_k M)(z) &= (cz+d)^{-k} f(Mz) \end{aligned}$$

Let $\Gamma = \mathrm{Sl}_2(\mathbb{Z})/\{\pm 1\}$ be the *modular group*. Let $\mathbb{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$. Then

$$\begin{aligned} M : \mathbb{H} &\to \mathbb{H} \\ \mathbb{Q} \cup \{i\infty\} &\to \mathbb{Q} \cup \{i\infty\}; \end{aligned}$$

the latter are called *cusps*. Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{i\infty\}$.

## Proposition 3.2

$$\Gamma = \langle T, S \rangle$$

with the *translation* $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : z \mapsto z + 1$ and the *inversion (Stürzung)* $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : z \mapsto \frac{-1}{z}$.

$\Gamma \backslash \mathbb{H}^*$ is a compact Riemann surface represented by the *fundamental domain*

$$\mathcal{F} = \left\{ z \in \mathbb{H} : -\frac{1}{2} \leqslant \Re(z) < \frac{1}{2}, |z| \geqslant 1, \Re(z) \leqslant 0 \text{ if } |z| = 1 \right\} \cup \{ i\infty \}$$

## Definition 3.3

A meromorphic function $f\colon \mathbb{H} \to \mathbb{C}$ is a *modular form* for $\Gamma$ of weight $k$ if

1. $f|_k M = f \quad \forall M \in G$
2. $f$ is meromorphic at $i\infty$: There are $\nu_0 \in \mathbb{Z}$ and $a_\nu \in \mathbb{C}$ with

$$f(z) = \sum_{\nu \geqslant \nu_0} a_\nu q^\nu \text{ with } q = e^{2\pi i z}.$$

$f$ is called a *modular function* if $k = 0$; the field of modular functions for $\Gamma$ is denoted $\mathbb{C}_\Gamma$.

## Definition 3.4

Two lattices $L$ and $L'$ are *homothetic* if $L' = \lambda L$ for some $\lambda \in \mathbb{C}^*$.

## Proposition 3.5

$$\begin{aligned} \wp(\lambda z | \lambda L) &= \lambda^{-2} \wp(z | L) \\ g_2(\lambda L) &= \lambda^{-4} g_2(L) \\ g_3(\lambda L) &= \lambda^{-6} g_3(L) \end{aligned}$$

The curves

$$\begin{aligned} E = \mathbb{C}/L &: \quad Y^2 = 4X^3 - g_2(L)X - g_3(L) \\ E' = \mathbb{C}/\lambda L &: \quad Y^2 = 4X^3 - \lambda^{-4} g_2(L)X - \lambda^{-6} g_3(L) = 4X^3 - g_2(\lambda L)X - g_3(\lambda \end{aligned}$$

are isomorphic under $(X, Y) \mapsto (\lambda^{-2} X, \lambda^{-3} Y)$; these are the only possible isomorphisms.

## Examples 3.6

Define $g_2(z) = g_2(\mathbb{Z} + z\mathbb{Z})$, and so on.
Then $g_2$, $g_3$, $\Delta$ are modular for $\Gamma$ of weight $4$, $6$, $12$.

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

is a modular function, holomorphic in $\mathbb{H}$ with a simple pole at $i\infty$:

$$j = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots;$$

precisely,

$$\mathbb{C}_\Gamma = \mathbb{C}(j).$$

## Theorem 3.7

$E = \mathbb{C}/L$ and $E' = \mathbb{C}/L'$ isomorphic
$\Leftrightarrow L$ and $L'$ homothetic
$\Leftrightarrow j(L) = j(L')$

# Complex multiplication

## Definition 4.1

An *isogeny* from $\mathbb{C}/L$ to $\mathbb{C}/L'$ is an $\alpha \in \mathbb{C}^*$ such that $\alpha L \subseteq L'$. It is a group homomorphism:

$$\alpha(z_1 + z_2) = \alpha z_1 + \alpha z_2,$$

with kernel

$$\ker \alpha = (\alpha^{-1} L')/L.$$

$L$ is a sublattice of $\alpha^{-1} L'$. Its index is

$$|\ker \alpha| = |\alpha|^2 \frac{\mathrm{covol}(L)}{\mathrm{covol}(L')}$$

If $L = L'$, then an isogeny is called *endomorphism* or *multiplier*.

## Theorem 4.2

Let $L = \mathbb{Z} + \tau\mathbb{Z}$ be a lattice and $\alpha \in \mathbb{C} \backslash \mathbb{Z}$. Are equivalent:

1. $\alpha L \subseteq L$
2. $L = \frac{1}{A}\left(A, \frac{-B+\sqrt{D}}{2}\right)_{\mathbb{Z}}$ is a proper fractional ideal of an imaginary quadratic order $\mathcal{O} = \left(1, \frac{D+\sqrt{D}}{2}\right)_{\mathbb{Z}}$, and $\alpha \in \mathcal{O}$.
3. $\wp(\alpha z | L)$ is a rational function in $\wp(z|L)$, $\wp'(\alpha z|L)$ equals $\wp'(z|L)$ times a rational function in $\wp(z|L)$.

## Corollary 4.3

An elliptic curve over $\mathbb{C}$ has endomorphism ring

- $\mathbb{Z}$ or
- $\mathcal{O}$, an imaginary-quadratic order of discriminant $D$ (*complex multiplication*).

In the latter case,

$$\begin{aligned} E &= \mathbb{C}/\mathfrak{a} \text{ for a proper ideal } \mathfrak{a} \text{ of } \mathcal{O} \\ \mathfrak{a} &= A\mathbb{Z} + \left(\frac{-B+\sqrt{D}}{2}\right)\mathbb{Z} \\ & \quad A, B, C \in \mathbb{Z}, A > 0, \gcd(A, B, C) = 1, \\ & \quad D = B^2 - 4AC; \text{ so } C > 0. \end{aligned}$$

There are $h(\mathcal{O}) = |\mathrm{Cl}(\mathcal{O})|$ non-isomorphic such curves, parameterised by the *singular values* $j(\mathfrak{a}) := j(\tau)$ with $\tau = \frac{-B+\sqrt{D}}{2A}$ a basis quotient of $\mathfrak{a}$.

**Theorem 5.1 (Deuring 1941)**

Every (ordinary) elliptic curve over a finite field $\mathbb{F}_q = \mathbb{F}_{p^m}$ is the reduction "modulo $p$" of an elliptic curve over $\mathbb{C}$ with the same endomorphism ring, called its *canonical lift*.

## Definition 5.2

The map $\pi : E \to E$, $(x, y) \mapsto (x^q, y^q)$, is called the *Frobenius endomorphism*.

## Theorem 5.3 (Hasse)

Let $\mathcal{O} = \left(1, \frac{1/0+\sqrt{D}}{2}\right)$ be the order of discriminant $D < -4$, and

$$4q = t^2 - v^2 D.$$

Then $|t| \leqslant 2\sqrt{q}$. Either the element $\pi = \frac{t+v\sqrt{D}}{2}$ or $-\pi$ is (reduced to) the Frobenius on the elliptic curves with complex multiplication by $\mathcal{O}$. They have minimal polynomials

$$\pi^2 - \mathrm{Tr}(\pi)\pi + \mathrm{N}(\pi) = \pi^2 \mp t\pi + q.$$

The associated elliptic curves have cardinality

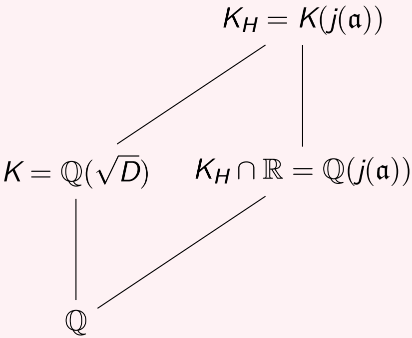
$$|\ker(\pi - 1)| = |\pi - 1|^2 = \mathrm{N}(\pi - 1) = q + 1 \mp t.$$

# Complex multiplication

**Theorem 6.1**

$j(\mathfrak{a})$ is an algebraic integer.

## Theorem 6.2




$K_H/K$ is Galois
with group $\mathrm{Cl}(\mathcal{O})$ via:

$$\sigma(\mathfrak{b}) : j(\mathfrak{a}) \mapsto j(\mathfrak{a}\mathfrak{b}^{-1})$$

If $D$ is fundamental, it is the *Hilbert class field*, the maximal abelian unramified extension, of $K$, and $\sigma$ is the Artin map from class field theory.

$\mathfrak{p}$ prime ideal of order $f$ in $\mathrm{Cl}(\mathcal{O})$
$\Leftrightarrow$ $\mathfrak{p}$ has inertia degree $f$ in $K_H$

## Definition 6.3

The irreducible polynomial

$$H_D(X) = \prod_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})} \big(X - j(\mathfrak{a})\big) \in \mathbb{Z}[X] \quad (1)$$

is called the *(Hilbert) class polynomial of* $\mathcal{O}$.

## Algorithm 7.1

**Input:** A problem

**Output:** An elliptic curve $E$ over $\mathbb{F}_q$ with known cardinality providing a solution to the problem

1. Choose $D$, $q = p^f$ such that $4p^f = t^2 - v^2 D$ for some $t, v \in \mathbb{Z}$ (and there is no solution with a smaller $f$), and suitable $|E| = q + 1 - t$ .
2. Compute
$$H_D(X) = \prod_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})} \big(X - j(\mathfrak{a})\big) \in \mathbb{Z}[X]$$
by Algorithm 7.2.
3. Compute a root $\bar{j} \in \mathbb{F}_q$ of $H_D \bmod p$.
4. $k = \frac{\bar{j}}{1728 - \bar{j}}$, $\gamma$ quadratic non-residue in $\mathbb{F}_q$
5. **return** the one of
$E: Y^2 = X^3 + 3kX + 2k \quad E' : Y^2 = X^3 + 3k\gamma^2 X + 2k\gamma^3$
with $|E| = q + 1 - t$ (for $D < -4$, otherwise, more twists)

## Algorithm 7.2

**Input:** $D < 0$ a quadratic discriminant
**Output:** $H_D \in \mathbb{Z}[X]$

1. Let $h = \#\mathrm{Cl}(\mathcal{O}_D)$.
2. Compute the reduced system of representatives $[A_k, B_k, C_k]$ of $\mathrm{Cl}(\mathcal{O}_D)$ for $k = 1, \ldots, h$:

$$D = B_k^2 - 4A_kC_k, \gcd(A_k, B_k, C_k) = 1, |B_k| \leqslant A_k \leqslant C_k$$

   and $B_k > 0$ if there is equality in one of the inequalities.
3. **for** $k = 1, \ldots, h_D$
4. $\quad \tau_k \leftarrow \frac{-B_k+\sqrt{D}}{2A_k} \in \mathbb{C}$
5. $\quad j_k \leftarrow j(\tau_k) \in \mathbb{C}$
6. $H_D \leftarrow \prod_{k=1}^{h_D}(X - j_k) \in \mathbb{C}[X]$
7. Drop the imaginary part of $H_D$, and round the coefficients to integers.

# Complex multiplication

## Theorem 8.1

$$h_D \in O\left(|D|^{1/2} \log |D|\right);$$

under GRH,

$$h_D \in O\left(|D|^{1/2} \log\log |D|\right), h_D \in \Omega\left(\frac{|D|^{1/2}}{\log\log |D|}\right).$$

## Theorem 8.2 ([Eng09, Sch91])

$$\mathrm{maxcoeff}(H_D) \leqslant C h_D + \pi \sqrt{|D|} \sum_{k=1}^{h_D} \frac{1}{A_k} \in O\left(|D|^{1/2} \log^2 |D|\right) \subseteq \tilde{O}\left(|D|^{1/2}\right)$$

with $C = 3.01\ldots$.

Andreas Enge.
The complexity of class polynomial computation via floating point approximations.
*Mathematics of Computation*, 78(266):1089–1107, 2009.

René Schoof.
The exponents of the groups of points on the reductions of an elliptic curve.
In G. van der Geer, F. Oort, and J. Steenbrink, editors, *Arithmetic Algebraic Geometry*, pages 325–335, Boston, 1991. Birkhäuser.

Reinhard Schertz.
*Complex Multiplication*, volume 15 of *New Mathematical Monographs*.
Cambridge University Press, Cambridge, 2010.