Computational Class Field Theory

for constructing cryptographic elliptic curves

Aristides Kontogeorgis

Department of Mathematics
University of Athens.

SSE Athens 6 April 2012

[1] This work was supported by the Project "*Thalis, Algebraic modeling of topological and Computational structures*". The Project "THALIS" is implemented under the Operational Project "Education and Life Long Learning is co-funded by the European Union (European Social Fund) and National Resources (ESPA)

Constructing Elliptic Curves

Modular functions

Galois Cohomology

Examples

Contents

1. Constructing Elliptic Curves
2. Modular functions
3. Galois Cohomology
4. Examples

- Elliptic curves defined over finite fields have applications in cryptography.

- Elliptic curves defined over finite fields have applications in cryptography.
- Produce cryptosystems that are difficult to decode.

- Elliptic curves defined over finite fields have applications in cryptography.
- Produce cryptosystems that are difficult to decode.
- Construct elliptic curves of large prime order.

- Elliptic curves defined over finite fields have applications in cryptography.
- Produce cryptosystems that are difficult to decode.
- Construct elliptic curves of large prime order.

The CM-method

- An elliptic curve is an algebraic curve that has an extra group structure.

The CM-method

- An elliptic curve is an algebraic curve that has an extra group structure.
- Elliptic curves are described in terms of their j-invariant.

The CM-method

- An elliptic curve is an algebraic curve that has an extra group structure.
- Elliptic curves are described in terms of their j-invariant.
- If we know the j-invariant we can construct the elliptic curve.

Elliptic curves

An *elliptic curve* over a finite field $\mathbb{F}_p$, p a prime larger than 3, is denoted by $E(\mathbb{F}_p)$ and it is comprised of all the points $(x, y) \in \mathbb{F}_p$ (in affine coordinates) such that

$$y^2 = x^3 + ax + b, \tag{1}$$

with $a, b \in \mathbb{F}_p$ satisfying $4a^3 + 27b^2 \neq 0$. These points, together with a special point denoted by $\mathcal{O}$ (the *point at infinity*) and a properly defined addition operation form an Abelian group. This is the *Elliptic Curve group* and the point $\mathcal{O}$ is its zero element

Elliptic curves II

Important quantities defined for an elliptic curve $E(\mathbb{F}_p)$ are

- *curve discriminant* $\Delta = -16(4a^3 + 27b^2)$
- *j-invariant* $j = j = -1728(4a)^3/\Delta$.

Elliptic curves II

Important quantities defined for an elliptic curve $E(\mathbb{F}_p)$ are

- *curve discriminant* $\Delta = -16(4a^3 + 27b^2)$
- *j-invariant* $j = j = -1728(4a)^3/\Delta$.

Given a j-invariant $j_0 \in \mathbb{F}_p$ (with $j_0 \neq 0, 1728$) *two* ECs can be constructed. If $k = j_0/(1728 - j_0)$ mod p, one of these curves is given by Eq. (1) by setting $a = 3k$ mod p and $b = 2k$ mod p. The second curve (the *twist* of the first) is given by the equation $y^2 = x^3 + ac^2x + bc^3$

Elliptic curves II

Important quantities defined for an elliptic curve $E(\mathbb{F}_p)$ are

- *curve discriminant* $\Delta = -16(4a^3 + 27b^2)$
- *j-invariant* $j = j = -1728(4a)^3/\Delta$.

Given a j-invariant $j_0 \in \mathbb{F}_p$ (with $j_0 \neq 0, 1728$) *two* ECs can be constructed. If $k = j_0/(1728 - j_0)$ mod p, one of these curves is given by Eq. (1) by setting $a = 3k$ mod p and $b = 2k$ mod p. The second curve (the *twist* of the first) is given by the equation $y^2 = x^3 + ac^2x + bc^3$

One of the curves has order $p + 1 - t$, then its twist has order $p + 1 + t$, or vice versa

CM-curves

Set $m = \#E$.

- Hasse's theorem, $Z = 4p - (p + 1 - m)^2 > 0$

CM-curves

Set $m = \#E$.

- Hasse's theorem, $Z = 4p - (p + 1 - m)^2 > 0$
- there is a unique factorization $Z = Dv^2$, with D a square free positive integer.

CM-curves

Set $m = \#E$.

- Hasse's theorem, $Z = 4p - (p+1-m)^2 > 0$
- there is a unique factorization $Z = Dv^2$, with D a square free positive integer.
- $4p = u^2 + Dv^2$ where $m = p + 1 \pm u$.

Given a prime p, choose the smallest D is chosen for which there exists some integer u for which $4p = u^2 + Dv^2$ holds.

CM-curves

Set $m = \#E$.

- Hasse's theorem, $Z = 4p - (p + 1 - m)^2 > 0$
- there is a unique factorization $Z = Dv^2$, with D a square free positive integer.
- $4p = u^2 + Dv^2$ where $m = p + 1 \pm u$.

Given a prime p, choose the smallest D is chosen for which there exists some integer u for which $4p = u^2 + Dv^2$ holds. Are $p + 1 \pm u$ suitable? If not start with a new D.

Complex analytic viewpoint

- Consider elliptic curves over $\mathbb{C}$.

Complex analytic viewpoint

- Consider elliptic curves over $\mathbb{C}$.
- These are abelian groups of the form $\mathbb{C}/L$, where L is a discrete subgroup.

Complex analytic viewpoint

- Consider elliptic curves over $\mathbb{C}$.
- These are abelian groups of the form $\mathbb{C}/L$, where L is a discrete subgroup.
- The j invariant becomes a complex meromorphic function $j : \mathbb{H} \to \mathbb{C}$.

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \cdots$$

where $q = \exp(2\pi i\tau)$.

CM-curves II

Now having the D at hand we consider the number field $\mathbb{Q}(\sqrt{-D})$.

CM-curves II

Now having the D at hand we consider the number field $\mathbb{Q}(\sqrt{-D})$. CM-theory: The Hilbert class field is generated by j. Thus, j satisfies a polynomial equation. The action of the class group can be effectively generated by Gauss theory of quadratic forms.

CM-curves II

Now having the D at hand we consider the number field $\mathbb{Q}(\sqrt{-D})$. CM-theory: The Hilbert class field is generated by j. Thus, j satisfies a polynomial equation. The action of the class group can be effectively generated by Gauss theory of quadratic forms.
Compute the Hilbert polynomial $\mathbb{Z}[t] = \prod(x - j^{[a,b,c]})(\theta)$ using floating point approximations of $j^{[a,b,c]}(\theta)$, where $\mathcal{O}_K = \mathbb{Z}[\theta]$.

Theorem

The elliptic curve defined over $\mathbb{F}_p$ with j invariant a root of the Hilbert polynomial modulo p has order $p + 1 \pm u$.

Hilbert class polynomial for $D = -299$

$$
\begin{gathered}
x^{8} + 391086320728105978429440x^{7} - 28635280874816126174326167699456x^{6} + \\
2094055410006322146651491130721133658112x^{5} - \\
186547260770756829961971675685151791296544768x^{4} + \\
6417141278133218665289808655954275181523718111232x^{3} - \\
19207839443594488822936988943836177115227877227364352x^{2} + \\
45797528808215150136248975363201860724351225694802411520x - \\
18273883965326272223717626628647422907813731016193733558272
\end{gathered}
$$

Hilbert class field of imaginary quadratic fields

Problem: The Hilbert polynomials constructed by this method has very big coefficients. Is there a better method to construct CM-elliptic curves?
Answer: Yes, we can use other class functions. These generate the Hilbert class field.

Examples of Class functions for $D = -299$

$$M_{299,13}(x) = x^8 + 78x^7 + 793x^6 + 5070x^5 + 20956x^4 + 65910x^3 + 134017x^2 + 171366x + 28561$$

$$M_{299,5,7}(x) = x^8 - 8x^7 + 31x^6 - 22x^5 + 28x^4 - 2x^3 - 19x^2 + 8x - 1$$

$$M_{299,3,13}(x) = x^8 - 6x^7 + 16x^6 + 12x^5 - 23x^4 + 12x^3 + 16x^2 - 6x + 1$$

$$T_{299}(x) = x^8 + x^7 - x^6 - 12x^5 + 16x^4 - 12x^3 + 15x^2 - 13x + 1$$

Modular functions of level N

- Complex functions $\mathbb{H} \to \mathbb{C}$

Modular functions of level N

- Complex functions $\mathbb{H} \to \mathbb{C}$
- Invariant under the action of

$$\Gamma(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \mod N, c \equiv b \equiv 0 \mod N, \det A = 1 \right\}.$$

- Some analytic conditions at the cusps.

Modular functions of level N

- Complex functions $\mathbb{H} \to \mathbb{C}$
- Invariant under the action of

$$\Gamma(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \mod N, c \equiv b \equiv 0 \mod N, \det A = 1 \right\}.$$

- Some analytic conditions at the cusps.

Remarks:

1. Modular functions are periodic and have Fourier expansions with coefficients in $\mathbb{Q}(\zeta_N)$.

Modular functions of level N

- Complex functions $\mathbb{H} \to \mathbb{C}$
- Invariant under the action of

$$\Gamma(N) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \bmod N, c \equiv b \equiv 0 \bmod N, \det A = 1 \right\}.$$

- Some analytic conditions at the cusps.

Remarks:

1. Modular functions are periodic and have Fourier expansions with coefficients in $\mathbb{Q}(\zeta_N)$.
2. All above examples are modular functions.

Shimura reciprocity law

- Gee-Stevenhagen provided us with a method in order to check if a modular function is a class invariant that can be used for the elliptic curve generation.
- They gave an explicit matrix action of the group $G_N := (\mathbb{O}/N\mathbb{O})^*$ on modular forms (Shimura Reciprocity) and they were able to prove that a modular function is a class invariant if and only if this function is invariant under the action of G_N.

Find new invariants

Assume that we can find a finite dimensional vector space V consisted of modular functions of level N so that $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ acts on V.

Find new invariants

Assume that we can find a finite dimensional vector space V consisted of modular functions of level N so that $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ acts on V.

We can always find such a vector space. We simple have to consider the orbit of f under the action of the finite group $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

Find new invariants

Assume that we can find a finite dimensional vector space V consisted of modular functions of level N so that $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ acts on V.
We can always find such a vector space. We simple have to consider the orbit of f under the action of the finite group $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$.

Every element $a \in \mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ can be written as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$.

Find new invariants

Assume that we can find a finite dimensional vector space V consisted of modular functions of level N so that $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ acts on V.

We can always find such a vector space. We simple have to consider the orbit of f under the action of the finite group $\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$.

Every element $a\in\mathrm{GL}(2,\mathbb{Z}/N\mathbb{Z})$ can be written as $b\cdot\begin{pmatrix}1 & 0\\ 0 & d\end{pmatrix}$, $d\in\mathbb{Z}/N\mathbb{Z}^*$ and $b\in\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$.

The group $\mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})$ is generated by the elements $S=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$ and $T=\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$.

Find new invariants

Assume that we can find a finite dimensional vector space V consisted of modular functions of level N so that $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ acts on V.
We can always find such a vector space. We simple have to consider the orbit of f under the action of the finite group $\mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$.

Every element $a \in \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z})$ can be written as $b \cdot \begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$, $d \in \mathbb{Z}/N\mathbb{Z}^*$ and $b \in \mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$.
The group $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ is generated by the elements $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
The action of S on functions $g \in V$ is defined to be $g \circ S = g(-1/z) \in V$ and the action of T is defined $g \circ T = g(z+1) \in V$.

Actions

The action of the matrix $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ is given by the action of the elements $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on the Fourier coefficients of the expansion at the cusp at infinity.

Actions

The action of the matrix $\begin{pmatrix} 1 & 0 \\ 0 & d \end{pmatrix}$ is given by the action of the elements $\sigma_d \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on the Fourier coefficients of the expansion at the cusp at infinity.

Since every element in $\mathrm{SL}(2, \mathbb{Z}/N\mathbb{Z})$ can be written as a word in S, T we obtain a function ρ

$$\begin{tikzcd} \left(\frac{\mathcal{O}}{N\mathcal{O}}\right)^* \arrow[r, "\phi"] \arrow[rr, bend left, "\rho"] & \mathrm{GL}(2, \mathbb{Z}/N\mathbb{Z}) \arrow[r] & \mathrm{GL}(V), \end{tikzcd} \tag{2}$$

where ϕ is the natural homomorphism

Cocylces

The map ρ defined in eq. (2) in previous section is not a homomorphism.

Cocylces

The map ρ defined in eq. (2) in previous section is not a homomorphism.

Proposition

The map ρ defined in eq. (2) satisfies the cocycle condition

$$\rho(\sigma\tau) = \rho(\tau)\rho(\sigma)^{\tau} \tag{3}$$

and gives rise to a class in $H^1(G, \mathrm{GL}(V))$, where $G = (\mathcal{O}/N\mathcal{O})^*$. The restriction of the map ρ in the subgroup H of G defined by

$$H := \{x \in G : \mathrm{det}(\phi(x)) = 1\}$$

is a homomorphism.

Invariant Theory

Select a basis $e_1, \ldots, e_m$ of V

Invariant Theory

Select a basis $e_1, \ldots, e_m$ of V
Classical invariant theory provides us with effective methods (Reynolds operator method,linear algebra method) in order to compute the ring of invariants $\mathbb{Q}(\zeta_N)[e_1, \ldots, e_m]^H$.
Select the vector space V_n of invariant polynomials of given degree n.

Invariant Theory

Select a basis $e_1, \dots, e_m$ of V
Classical invariant theory provides us with effective methods (Reynolds operator method,linear algebra method) in order to compute the ring of invariants $\mathbb{Q}(\zeta_N)[e_1, \dots, e_m]^H$.
Select the vector space V_n of invariant polynomials of given degree n.
The action of G/H on V_n gives rise to a cocycle

$$\rho' \in H^1(\mathrm{Gal}(\mathbb{Q}(\zeta_N))/\mathbb{Q}), V_n).$$

The multidimensional Hilbert 90 theorem asserts that there is an element $P \in \mathrm{GL}(V_n)$ such that

$$\rho'(\sigma) = P^{-1} P^{\sigma}. \tag{4}$$

Computation of P

Use a version of Glasby-Howlett probabilistic algorithm

Computation of P

Use a version of Glasby-Howlett probabilistic algorithm

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^{\sigma}. \tag{5}$$

If we manage to find a 2 × 2 matrix in $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ such that B_Q is invertible then $P := B_Q^{-1}$.

Computation of P

Use a version of Glasby-Howlett probabilistic algorithm

$$B_Q := \sum_{\sigma \in G/H} \rho(\sigma) Q^{\sigma}. \tag{5}$$

If we manage to find a 2×2 matrix in $\mathrm{GL}(2, \mathbb{Q}(\zeta_N))$ such that B_Q is invertible then $P := B_Q^{-1}$.
Non invertible matrices are rare (they form a Zariski closed subset in the space of matrices) our first random choice of Q always worked!

Example

Generalised Weber functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$

Example

Generalised Weber functions $\mathfrak{g}_0, \mathfrak{g}_1, \mathfrak{g}_2, \mathfrak{g}_3$

$$\mathfrak{g}_0(\tau) = \frac{\eta(\frac{\tau}{3})}{\eta(\tau)},\ \mathfrak{g}_1(\tau) = \zeta_{24}^{-1}\frac{\eta(\frac{\tau+1}{3})}{\eta(\tau)},$$

$$\mathfrak{g}_2(\tau) = \frac{\eta(\frac{\tau+2}{3})}{\eta(\tau)},\ \mathfrak{g}_3(\tau) = \sqrt{3}\frac{\eta(3\tau)}{\eta(\tau)},$$

where η denotes the Dedekind eta function:

$$\eta(\tau) = e^{2\pi i\tau/24}\prod_{n\geq 1}(1-q^n)\ \ \tau \in \mathbb{H}, q = e^{2\pi i\tau}.$$

These are modular functions of level 72.

Example

For $n = -571$ the group H has order 144 and G has order 3456. We find that the polynomials

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^{6})\mathfrak{g}_1\mathfrak{g}_2$$

are invariants of the action of H.

Example

For $n = -571$ the group H has order 144 and G has order 3456. We find that the polynomials

$$I_1 := \mathfrak{g}_0\mathfrak{g}_2 + \zeta_{72}^{6}\mathfrak{g}_1\mathfrak{g}_3, \qquad I_2 := \mathfrak{g}_0\mathfrak{g}_3 + (-\zeta_{72}^{18} + \zeta_{72}^{6})\mathfrak{g}_1\mathfrak{g}_2$$

are invariants of the action of H.

$$e_{\mathbf{1}} := (-12\zeta_{\mathbf{72}}^{\mathbf{18}} + 12\zeta_{\mathbf{72}}^{\mathbf{6}})\mathfrak{g}_{\mathbf{0}}\mathfrak{g}_{\mathbf{3}} + 12\zeta_{\mathbf{72}}^{\mathbf{6}}\mathfrak{g}_{\mathbf{0}}\mathfrak{g}_{\mathbf{3}} + 12\mathfrak{g}_1\mathfrak{g}_{\mathbf{2}} + 12\mathfrak{g}_{\mathbf{1}}\mathfrak{g}_{\mathbf{3}},$$

$$e_{\mathbf{2}} := 12\zeta_{\mathbf{72}}^{\mathbf{6}}\mathfrak{g}_{\mathbf{1}}\mathfrak{g}_{\mathbf{2}} + (-12\zeta_{\mathbf{72}}^{\mathbf{18}} + 12\zeta_{\mathbf{72}}^{\mathbf{6}})\mathfrak{g}_{\mathbf{0}}\mathfrak{g}_{\mathbf{3}} + (-12\zeta_{\mathbf{72}}^{\mathbf{12}} + 12)\mathfrak{g}_{\mathbf{1}}\mathfrak{g}_{\mathbf{3}} + 12\zeta_{\mathbf{72}}^{\mathbf{12}}\mathfrak{g}_{\mathbf{1}}\mathfrak{g}_3$$

Examples

Invariant	polynomial
Hilbert	$t^5 + 400497845154831586723701480652800t^4 +$ $818520809154613065770038265334290448384t^3 +$ $4398250752422094811238689419574422303726895104t^2$ $-16319730975176203906274913715913862844512542392320t$ $+15283054453672803818066421650036653646232315192410112$
$\mathfrak{g}_0^{12}\mathfrak{g}_1^{12} + \mathfrak{g}_2^{12}\mathfrak{g}_3^{12}$	$t^5 - 5433338830617345268674t^4 + 90705913519542658324778088t^3$ $-3049357177530030535811751619728t^2$ $-390071826912221442431043741686448t$ - 12509992052647780072147837007511456
e_1	$t^5 - 936t^4 - 60912t^3 - 2426112t^2 - 40310784t - 3386105856$
e_2	$t^5 - 1512t^4 - 29808t^3 + 979776t^2 + 3359232t - 423263232$

Questions:

1. Select the most efficient class invariants.

Questions:

1. Select the most efficient class invariants.This is equivalent to minimizing a height function on a lattice. Out of reach for now.

Questions:

1. Select the most efficient class invariants.This is equivalent to minimizing a height function on a lattice. Out of reach for now.
2. By computations we see that the best invariants occur when the class invariants are monomials of the Weber functions.

Questions:

1. Select the most efficient class invariants.This is equivalent to minimizing a height function on a lattice. Out of reach for now.
2. By computations we see that the best invariants occur when the class invariants are monomials of the Weber functions.
3. There are classes $n \bmod 24$ where no monomial invariants of the Weber functions exists. Then our method provides the best invariants.

Thank you!