Elliptic Curves, Construction using Complex Multiplication

Aristides Kontogeorgis

Department of Mathematics
University of Athens.

2/04/2014 Hellenic Army Academy

Contents

What is an elliptic curve?

Definition

An Elliptic Curve defined over a field k is the set E of points $(x, y) \in k^2$ satisfying a cubic equation of the form

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

so that the cubic polynomial $x^3 + ax + b$ has simple roots, together with a point $\mathcal{O}$ at infinity.

The points satisfying the above equation are equiped with an addition

$$E \times E \to E$$

$$(P, Q) \mapsto P + Q$$

such that $\mathcal{O}$ is the zero element and three colinear points sum to zero.

More on addition on Elliptic Curves

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on the elliptic curve E. The addition can be defined as:

Assume that $P_1, P_2 \neq \mathcal{O}$.

- If $x_1 = x_2$ and $y_1 = -y2$ we set: $P_1 + P_2 = \mathcal{O}$. Symmetric points with respect to the x axis sum to zero $\mathcal{O}$.
- In all other cases we set

$$\lambda = (3x_1 + a)/(2y_1) \text{ if } \quad P_1 = P_2$$

$$\lambda = (y_1 - y_2)/(x_1 - x_2) \text{ if } \quad P_1 \neq P_2$$

The point $P_1 + P_2$ has coordinates (x_3, y_3) given by:

$$(x_3, y_3) = (\lambda^2 - x_1 - x_2, -\lambda x_3 - y_1 + \lambda x_1)$$

Addition in a picture

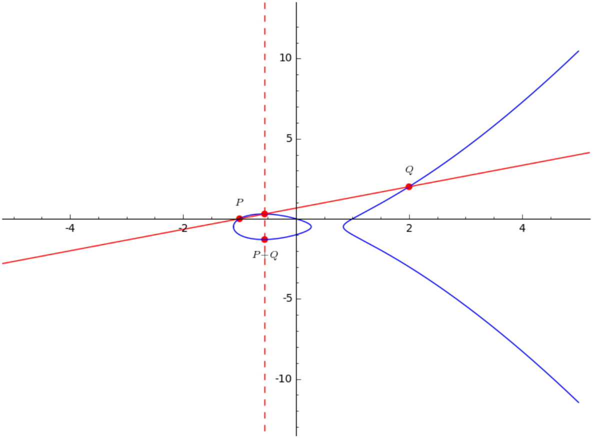


Figure : Adding points on $y^2 + y = x^3 - x$

Abelian Groups

The points in E together with the addition defined have the structure of an abelian group.
If the field k is a finite field $\mathbb{F}_p$, then the group $E(\mathbb{F}_p)$ is a finite group and has order $|E(\mathbb{F}_p)| \leq p^2 + 1$.

The Hasse Bound

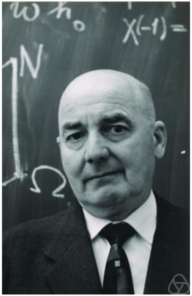


Figure : Helmut Hasse

H.Hasse proved that for an elliptic curve defined over the finite field $\mathbb{F}_{p^h}$ the following bound holds:

$$|E| = p^h + 1 \pm s,$$

Where $|s| \leq 2\sqrt{p^h}$. The number s is called the ``Frobenious trace".

Isomorphic Elliptic Curves

Consider the elliptic curve

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

The discriminant Δ of the elliptic curve is defined as $\Delta = -16(4a^3 + 27b^2)$. We also define the j-invariant by the formula:

$$j(E) = \frac{(4a)^3}{4a^3 + 27b^2} = -\frac{4a^3}{\Delta(E)}.$$

Theorem

If two curves are isomorphic they have the same j-invariant. Two elliptic curves with the same invariant become isomorphic after a quadratic extension of the field k.

Isomorphic Elliptic Curves

Consider the elliptic curve

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

The discriminant Δ of the elliptic curve is defined as $\Delta = -16(4a^3 + 27b^2)$. We also define the j-invariant by the formula:

$$j(E) = \frac{(4a)^3}{4a^3 + 27b^2} = -\frac{4a^3}{\Delta(E)}.$$

Theorem

If two curves are isomorphic they have the same j-invariant. Two elliptic curves with the same invariant become isomorphic after a quadratic extension of the field k.

Definition

A lattice L is the subset of $\mathbb{C}$ consisted of all $\mathbb{Z}$-linear combinations of two linear independed elements of $\mathbb{C}$. We usual consider lattices of the form $L = \langle 1, \tau \rangle$ where $\tau = a + ib$, $a \in \mathbb{R}$ and $b > 0$.

Weierstrass constructed a function $\wp : \mathbb{C} \to \mathbb{C}$ depending on L given by

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

Definition

A lattice L is the subset of $\mathbb{C}$ consisted of all $\mathbb{Z}$-linear combinations of two linear independed elements of $\mathbb{C}$. We usual consider lattices of the form $L = \langle 1, \tau \rangle$ where $\tau = a + ib$, $a \in \mathbb{R}$ and $b > 0$.

Weierstrass constructed a function $\wp : \mathbb{C} \to \mathbb{C}$ depending on L given by

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\lambda \in L - \{0\}} \left(\frac{1}{(z+\lambda)^2} - \frac{1}{\lambda^2} \right).$$

The function of Weierstrass satisfies the differential equation:

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(L)\wp(z) - g_3(L).$$

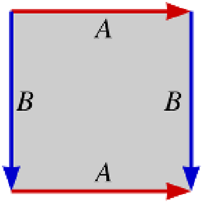
And it is periodic with respect to the lattice L, i.e.

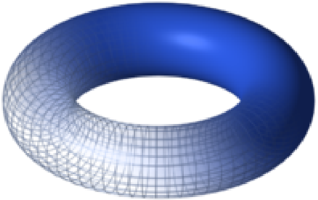
$$(\wp(z+\lambda), \wp'(z+\lambda)) = (\wp(z), \wp'(z)).$$

The points $(x, y) = (\wp(z), \wp'(z))$ satisfy the equation of the elliptic curve

$$y^2 = 4x^3 - g_2(L)x - g_3(L).$$

Elliptic curve over the complex numbers





Modular functions

Theorem

The functions g_2, g_3, Δ, j seen as functions of $\tau \in \mathbb{H}$ remain invariant under transformations of the form:

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

In particular these functions are periodic. This allows us to consider their Fourier expansions. The first terms of the Fourier expansion of the j-invariant is given by

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

where $q = e^{2\pi i\tau}$.

There is a lot of arithmetic information hidden in the above coefficients.

Modular functions

Theorem

The functions g_2, g_3, Δ, j seen as functions of $\tau \in \mathbb{H}$ remain invariant under transformations of the form:

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

In particular these functions are periodic. This allows us to consider their Fourier expansions. The first terms of the Fourier expansion of the j-invariant is given by

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

where $q = e^{2\pi i\tau}$.

There is a lot of arithmetic information hidden in the above coefficients.

Complex Multiplication of Elliptic Curves

Consider the ring of endomorphisms of the elliptic curve E, $\mathrm{End}(E)$ consisted of functions $f : E \to E$, $f(\mathcal{O}) = \mathcal{O}$. The ring $\mathbb{Z} \subset \mathrm{End}(E)$. If there is an endomorphism not in $\mathbb{Z}$ then it satisfies an equation:

$$\phi^2 + a\phi + b = 0, \text{ for some } a, b \in \mathbb{Z}, \text{ with } a^2 - 4b < 0.$$

In elliptic curves defined over $\mathbb{F}_p$ there is always an endomorphism of E not in $\mathbb{Z}$ namely the endomorphism of Frobenious defined by:

$$E \ni P = (x, y) \mapsto \phi(P) = (x^p, y^p).$$

The automorphism of Frobenious is related to the number of points of $E(\mathbb{F}_p)$ since this number equals to the number of its fixed points. This is true since $x \in \bar{\mathbb{F}}_p$ belongs to $\mathbb{F}_p$ if and only if $x^p = x$.

Complex Multiplication of Elliptic Curves

Consider the ring of endomorphisms of the elliptic curve E, $\mathrm{End}(E)$ consisted of functions $f : E \to E$, $f(\mathcal{O}) = \mathcal{O}$. The ring $\mathbb{Z} \subset \mathrm{End}(E)$. If there is an endomorphism not in $\mathbb{Z}$ then it satisfies an equation:

$$\phi^2 + a\phi + b = 0, \text{ for some } a, b \in \mathbb{Z}, \text{ with } a^2 - 4b < 0.$$

In elliptic curves defined over $\mathbb{F}_p$ there is always an endomorphism of E not in $\mathbb{Z}$ namely the endomorphism of Frobenious defined by:

$$E \ni P = (x, y) \mapsto \phi(P) = (x^p, y^p).$$

The automorphism of Frobenious is related to the number of points of $E(\mathbb{F}_p)$ since this number equals to the number of its fixed points. This is true since $x \in \bar{\mathbb{F}}_p$ belongs to $\mathbb{F}_p$ if and only if $x^p = x$.

Complex Multiplication of Elliptic Curves

Consider the ring of endomorphisms of the elliptic curve E, $\mathrm{End}(E)$ consisted of functions $f : E \to E$, $f(\mathcal{O}) = \mathcal{O}$. The ring $\mathbb{Z} \subset \mathrm{End}(E)$. If there is an endomorphism not in $\mathbb{Z}$ then it satisfies an equation:

$$\phi^2 + a\phi + b = 0, \text{ for some } a, b \in \mathbb{Z}, \text{ with } a^2 - 4b < 0.$$

In elliptic curves defined over $\mathbb{F}_p$ there is always an endomorphism of E not in $\mathbb{Z}$ namely the endomorphism of Frobenious defined by:

$$E \ni P = (x, y) \mapsto \phi(P) = (x^p, y^p).$$

The automorphism of Frobenious is related to the number of points of $E(\mathbb{F}_p)$ since this number equals to the number of its fixed points. This is true since $x \in \bar{\mathbb{F}}_p$ belongs to $\mathbb{F}_p$ if and only if $x^p = x$.

Complex Multiplication of Elliptic Curves

Consider the ring of endomorphisms of the elliptic curve E, $\mathrm{End}(E)$ consisted of functions $f : E \to E$, $f(\mathcal{O}) = \mathcal{O}$. The ring $\mathbb{Z} \subset \mathrm{End}(E)$. If there is an endomorphism not in $\mathbb{Z}$ then it satisfies an equation:

$$\phi^2 + a\phi + b = 0, \text{ for some } a, b \in \mathbb{Z}, \text{ with } a^2 - 4b < 0.$$

In elliptic curves defined over $\mathbb{F}_p$ there is always an endomorphism of E not in $\mathbb{Z}$ namely the endomorphism of Frobenious defined by:

$$E \ni P = (x, y) \mapsto \phi(P) = (x^p, y^p).$$

The automorphism of Frobenious is related to the number of points of $E(\mathbb{F}_p)$ since this number equals to the number of its fixed points. This is true since $x \in \bar{\mathbb{F}}_p$ belongs to $\mathbb{F}_p$ if and only if $x^p = x$.

Hasse bound

The Frobenious endomorphism ϕ satisfies the quadratic equation:

$$\phi^2 - t\phi + p = 0.$$

The coefficient t of ϕ equals the ``trace of Frobenious". Notice that the Hasse bound follows since the above quadratic equation should have negative discriminant.

In order to construct an elliptic curve with given number of points we should construct an elliptic curve with appropriate trace of Frobenious t.

Hasse bound

The Frobenious endomorphism ϕ satisfies the quadratic equation:

$$\phi^2 - t\phi + p = 0.$$

The coefficient t of ϕ equals the ``trace of Frobenious". Notice that the Hasse bound follows since the above quadratic equation should have negative discriminant.
In order to construct an elliptic curve with given number of points we should construct an elliptic curve with appropriate trace of Frobenious t.

Complex Multiplication

Idea: consider $\tau \in \mathbb{H}$ which satisfies the same equation

$$\phi^2 - t\phi + p.$$

and consider the complex Elliptic curve E_τ corresponding to the lattice $\langle 1, \tau \rangle$.

Then reduce E_τ to $\mathbb{F}_p$.

Idea: consider $\tau \in \mathbb{H}$ which satisfies the same equation

$$\phi^2 - t\phi + p.$$

and consider the complex Elliptic curve E_τ corresponding to the lattice $\langle 1, \tau \rangle$.
Then reduce E_τ to $\mathbb{F}_p$.

Gauss studied quadratic forms

$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, a, b, c \in \mathbb{Z} \ \ (a, b, c) = 1,$$

up to an equivalence.

A full set of representatives is given by (a, b, c) such that

$$|b| \leq a \leq \sqrt{\frac{D}{3}}, a \leq c, (a, b, c) = 1, b^2 - 4ac = -D$$

if $|b| = a$ or $a = c$ then $b \geq 0$.

Complex Multiplication

Gauss studied quadratic forms

$$ax^2 + bxy + cy^2; b^2 - 4ac = -D, a, b, c \in \mathbb{Z} \ \ (a, b, c) = 1,$$

up to an equivalence.
A full set of representatives is given by (a, b, c) such that

$$|b| \le a \le \sqrt{\frac{D}{3}}, a \le c, (a, b, c) = 1, b^2 - 4ac = -D$$

if $|b| = a$ or $a = c$ then $b \ge 0$.

Complex Multiplication

Consider $\tau \in \mathbb{H}$ which satisfies a monic quadratic polynomial in $\mathbb{Z}[x]$.
Consider the elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ which has j-invariant $j(\tau)$.
The number $j(\tau)$ satisfies a polynomial equation:

$$H_D(x) = \prod_{[a,b,c]\in \mathrm{CL(D)}} \left(x - j\left(\frac{-b+\sqrt{-D}}{2a} \right) \right) \in \mathbb{Z}[x].$$

Moreover a root of the reduction of the polynomial $H_D(x) \bmod p$ leads to an elliptic curve over $\mathbb{F}_p$ with Frobenious endomorphism that satisfies the same characteristic polynomial as τ.

Complex Multiplication

Consider $\tau \in \mathbb{H}$ which satisfies a monic quadratic polynomial in $\mathbb{Z}[x]$. Consider the elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ which has j-invariant $j(\tau)$. The number $j(\tau)$ satisfies a polynomial equation:

$$H_D(x) = \prod_{[a,b,c] \in \mathrm{CL(D)}} \left(x - j\left(\frac{-b + \sqrt{-D}}{2a} \right) \right) \in \mathbb{Z}[x].$$

Moreover a root of the reduction of the polynomial $H_D(x) \bmod p$ leads to an elliptic curve over $\mathbb{F}_p$ with Frobenious endomorphism that satisfies the same characteristic polynomial as τ.

Complex Multiplication

Consider $\tau \in \mathbb{H}$ which satisfies a monic quadratic polynomial in $\mathbb{Z}[x]$. Consider the elliptic curve $E_\tau = \mathbb{C}/(\mathbb{Z} + \tau\mathbb{Z})$ which has j-invariant $j(\tau)$. The number $j(\tau)$ satisfies a polynomial equation:

$$H_D(x) = \prod_{[a,b,c] \in \mathrm{CL(D)}} \left(x - j\left(\frac{-b + \sqrt{-D}}{2a} \right) \right) \in \mathbb{Z}[x].$$

Moreover a root of the reduction of the polynomial $H_D(x) \bmod p$ leads to an elliptic curve over $\mathbb{F}_p$ with Frobenious endomorphism that satisfies the same characteristic polynomial as τ.

Example CM

For $D = 491$ we compute

$$\mathrm{CL}(D) = [1, 1, 123], [3, \pm 1, 41], [9, \pm 7, 15], [5, \pm 3, 25], [11, \pm 9, 3].$$

For each $[a, b, c]$ we select the root

$$\rho = \frac{-b + i\sqrt{491}}{2s}, \text{ with positive imaginary part.}$$

$[a, b, c]$	Root	j-invariant
$[1, 1, 123]$	$\rho_1 = (-1 + i\sqrt{491})/2$	-1.7082855 E30
$[3, 1, 41]$	$\rho_2 = (-1 + i\sqrt{491})/6$	5.977095 E9 + 1.0352632 E10I
$[3, -1, 41]$	$\rho_3 = (1 + i\sqrt{491})/6$	5.9770957 E9 - 1.0352632 E10I
$[9, 7, 15]$	$\rho_4 = (-7 + i\sqrt{491})/18$	-1072.7816 + 1418.3793I
$[9, -7, 15]$	$\rho_5 = (7 + i\sqrt{491})/18$	-1072.7816 - 1418.3793I
$[5, 3, 25]$	$\rho_6 = (-3 + i\sqrt{491})/10)$	-343205.38 + 1058567.0I
$[5, -3, 25]$	$\rho_7 = (3 + i\sqrt{491})/10$	-343205.38 - 1058567.0I
$[11, 9, 13]$	$\rho_8 = (-9 + i\sqrt{491})/22$	6.0525190 + 170.50800I
$[11, -9, 13]$	$\rho_9 = (9 + i\sqrt{491})/22$	6.0525190 - 170.50800I

Example CM

Compute the polynomial

$$f(x) = \prod_{i=1}^{9} (x - j(\rho_i))$$

with 100 digits precision and arrive at

```
x^9+(170828551993829356071116505088 0.0000 + 0.E-105*I)*x^8 +
(-2041999594381474622455269141880290829926 4.0000 +
5.527147875260444561 E-76*I)*x^7 +
(24410449766543274815871531378358313021155670228992 0.00000
- 3.203247249195215313 E-66*I)*x^6 +
(168061099707176489267621705337969352389335280404863647744.0000 -
8.477642883414348322 E-61*I)*x^5 +
(302663406228710339993356777425938984884433281603698934574743552.0000 +
1.179755502567748528 2E-53*I)*x^4 +
(645485900085616784926354786035581108920923697188375949395393249280.0000+
 5.552991534850878913 E-50*I)*x^3 +
(957041138046397870965520808576552949198885665738183643750394920697856.0000
- 1.530756330080109172 1 E-47*I)*x^2 +
(732286287103378441923659612927325084552910850222176255650744547200204 8.0000+
4.458155165749933023 E-45*I)*x +
(278313659432538880431289772161069994442281398650557514572675822343075921 92.0000
 - 3.587324068671531702 E-43*I)
```

which is a polynomial is $\mathbb{Z}[x]$.

Construction

We now have at hand the polynomial

$$x^9 + 170828551993829356071116505088 0x^8 +$$

$$2041999594381474622455269141880290829926 4x^7 +$$

$$2441044976654327481587153137835831302115567022899 20x^6 +$$

$$16806109970717648926762170533796935238933528040486364774 4^5 +$$

$$302663406228710339993356777425938984884433281603698934574743552x^4 +$$

$$6454859000856167849263547860355811089209236971883759493953932492 80x^3 +$$

$$957041138046397870965520808576552949198885665738183643750394920697856x^2 +$$

$$7322862871033784419236596129273 2x +$$

$$278313659432538880431289772161069994442281398650557514572675822343075921 92$$

Construction

Reduce it modulo p and find a root of the reduced polynomial modulo p. This is the j invariant of a curve which has either $p+1-t$ or $p+1+t$ points. The curve is given by

$$y^2 = x^3 + 3kc^2x + 2kc^3, k = j/(1728-j), c \in \mathbb{F}_p.$$

For different values of c correspond two non-isomorphic curves $,'$ of orders $p+1\pm t$. One is

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

and the other is

$$y^2 = x^3 + ac^2x + bc^3,$$

where c is a non-quadratic residue in $\mathbb{F}_p$. Which of the two curves corresponds to which order can be computed by selecting one point in one of them and computing its order n such that $nP = \mathcal{O}$. The order n should divide either $p+1-t$ or $p+1+t$.

Construction

Reduce it modulo p and find a root of the reduced polynomial modulo p. This is the j invariant of a curve which has either $p + 1 - t$ or $p + 1 + t$ points. The curve is given by

$$y^2 = x^3 + 3kc^2x + 2kc^3, k = j/(1728 - j), c \in \mathbb{F}_p.$$

For different values of c correspond two non-isomorphic curves $,'$ of orders $p + 1 \pm t$. One is

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

and the other is

$$y^2 = x^3 + ac^2x + bc^3,$$

where c is a non-quadratic residue in $\mathbb{F}_p$. Which of the two curves corresponds to which order can be computed by selecting one point in one of them and computing its order n such that $nP = \mathcal{O}$. The order n should divide either $p + 1 - t$ or $p + 1 + t$.

Construction

Reduce it modulo p and find a root of the reduced polynomial modulo p. This is the j invariant of a curve which has either $p+1-t$ or $p+1+t$ points. The curve is given by

$$y^2 = x^3 + 3kc^2x + 2kc^3, k = j/(1728 - j), c \in \mathbb{F}_p.$$

For different values of c correspond two non-isomorphic curves $,'$ of orders $p+1 \pm t$. One is

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

and the other is

$$y^2 = x^3 + ac^2x + bc^3,$$

where c is a non-quadratic residue in $\mathbb{F}_p$. Which of the two curves corresponds to which order can be computed by selecting one point in one of them and computing its order n such that $nP = \mathcal{O}$. The order n should divide either $p+1-t$ or $p+1+t$.

Conclusion

This method has the disadvantage that the polynomials $H(t)$ constructed become very large for the discriminants D required for a secure implementation of the method.

Can we do better? Yes we can use instead of the modular function j other modular functions. For example using a class function constructed by Ramanujan the polynomials constructed are significantly smaller. For the $D = 491$ case the corresponding polynomial is given by:

$$x^9 + x^8 + 16x^7 + 2x^6 + 37x^5 - 31x^4 + 44x^3 - 40x^2 + 29x - 1.$$

An other approach in order to obtain small polynomials is to carefull select the discriminants. This will be explained in prof. Konstantinou talk.

Conclusion

This method has the disadvantage that the polynomials $H(t)$ constructed become very large for the discriminants D required for a secure implementation of the method.

Can we do better? Yes we can use instead of the modular function j other modular functions. For example using a class function constructed by Ramanujan the polynomials constructed are significantly smaller. For the $D = 491$ case the corresponding polynomial is given by:

$$x^9 + x^8 + 16x^7 + 2x^6 + 37x^5 - 31x^4 + 44x^3 - 40x^2 + 29x - 1.$$

An other approach in order to obtain small polynomials is to carefull select the discriminants. This will be explained in prof. Konstantinou talk.

Conclusion

This method has the disadvantage that the polynomials $H(t)$ constructed become very large for the discriminants D required for a secure implementation of the method.

Can we do better? Yes we can use instead of the modular function j other modular functions. For example using a class function constructed by Ramanujan the polynomials constructed are significantly smaller. For the $D = 491$ case the corresponding polynomial is given by:

$$x^9 + x^8 + 16x^7 + 2x^6 + 37x^5 - 31x^4 + 44x^3 - 40x^2 + 29x - 1.$$

An other approach in order to obtain small polynomials is to carefull select the discriminants. This will be explained in prof. Konstantinou talk.

Thanks

Thank you for your attention!