Elliptic Curves

J. Jiménez Urroz, UPC

Benin, July, 16, 2014

Given an integer n let us consider $D(n) = \{d : b - a = d, ba = n\}$.

Problem

For any integer k, find k integers $n_1, \ldots, n_k$ such that

$$\left| \cap_{i=1}^{k} D(n_i) \right| \geq 3.$$

Given an integer n let us consider $D(n) = \{d : b - a = d, ba = n\}$.

Problem

For any integer k, find k integers $n_1, \dots, n_k$ such that

$$\left| \cap_{i=1}^{k} D(n_i) \right| \geq 3.$$

$b = x + d, a = x - d$ and so $n = x^2 - d^2$. Hence, we need to find three integers d_1, d_2, d_3 and k 3-tuples (x_i, y_i, z_i) integer solutions to

$$x^2 - y^2 = d_1^2 - d_2^2$$
$$x^2 - z^2 = d_1^2 - d_3^2$$

Given an integer n let us consider $D(n) = \{d : b - a = d, ba = n\}$.

Problem

For any integer k, find k integers $n_1, \ldots, n_k$ such that

$$\left| \cap_{i=1}^{k} D(n_i) \right| \geq 3.$$

$b = x + d, a = x - d$ and so $n = x^2 - d^2$. Hence, we need to find three integers d_1, d_2, d_3 and k 3-tuples (x_i, y_i, z_i) integer solutions to

$$x^2 - y^2 = d_1^2 - d_2^2$$
$$x^2 - z^2 = d_1^2 - d_3^2$$

Or two integers A, B and $k + 1$ 3-tuples (x, y, z) integer solutions to

$$x^2 - y^2 = A$$
$$x^2 - z^2 = B$$

Find two integers A, B and $k+1$ 3-tuples (x, y, z) integer solutions to

$$x^2 - y^2 = A,$$
$$x^2 - z^2 = B.$$

By denoting $X = x^2$, we get $X - A = y^2$ and $X - B = z^2$, and multiplying the equations this is the same as finding $k+1$ solutions to

$$Y^2 = X(X-A)(X-B) \tag{1}$$

with the three factors being squares.

Theorem

Equation (1) has a solutions with the three factors squares, if and only if, the point (X, Y) on the elliptic curve is the double of another point.

Problem

Given an integer n is there a right triangle with rational sides and area n?

Problem

Given an integer n is there a right triangle with rational sides and area n?

$$a^2 + b^2 = c^2$$

$$2ab = 4n.$$

Right triangles, of rational area come from Pythagorean tryples $X^2 + Y^2 = Z^2$.

Dividing by Z^2, we get $x^2 + y^2 = 1$, the equation of the circle with the trivial solution $(1, 0)$.

Right triangles, of rational area come from Pythagorean tryples $X^2 + Y^2 = Z^2$.

Dividing by Z^2, we get $x^2 + y^2 = 1$, the equation of the circle with the trivial solution $(1, 0)$.

Draw the line $y = t(x - 1)$ and substituting into the equation we get

$$x = \frac{1 - t^2}{1 + t^2}, \qquad y = \frac{-2t}{1 + t^2}.$$

Right triangles, of rational area come from Pythagorean tryples $X^2 + Y^2 = Z^2$.

Dividing by Z^2, we get $x^2 + y^2 = 1$, the equation of the circle with the trivial solution $(1, 0)$.

Draw the line $y = t(x - 1)$ and substituting into the equation we get

$$x = \frac{1 - t^2}{1 + t^2}, \qquad y = \frac{-2t}{1 + t^2}.$$

$t = \frac{a}{b}$ gives

$$X = D(a^2 - b^2), \qquad Y = D(2ab), \qquad Z = D(a^2 + b^2)$$

for $(a, b) = 1$ $a \not\equiv b \pmod 2$.

Right triangles, of rational area come from Pythagorean tryples $X^2 + Y^2 = Z^2$.

Dividing by Z^2, we get $x^2 + y^2 = 1$, the equation of the circle with the trivial solution $(1, 0)$.

Draw the line $y = t(x - 1)$ and substituting into the equation we get

$$x = \frac{1 - t^2}{1 + t^2}, \qquad y = \frac{-2t}{1 + t^2}.$$

$t = \frac{a}{b}$ gives

$$X = D(a^2 - b^2), \qquad Y = D(2ab), \qquad Z = D(a^2 + b^2)$$

for $(a, b) = 1$ $a \not\equiv b \pmod 2$.

How the program knows if there are solutions or not?

Problem

Given an integer n is there a right triangle with rational sides and area n?

Problem

Given an integer n is there a right triangle with rational sides and area n?

$$a^2 + b^2 = c^2$$

$$2ab = 4n.$$

Problem

Given an integer n is there a right triangle with rational sides and area n?

$$a^2 + b^2 = c^2$$
$$2ab = 4n.$$

$$(a+b)^2 = c^2 + 4n$$
$$(a-b)^2 = c^2 - 4n.$$

Problem

Given an integer n is there a right triangle with rational sides and area n?

$$a^2 + b^2 = c^2$$
$$2ab = 4n.$$

$$(a+b)^2 = c^2 + 4n$$
$$(a-b)^2 = c^2 - 4n.$$

$$y^2 = x(x-4n)(x+4n) = x^3 - 16n^2x$$

$n = 6$. Since $35^2 = 25 \times 1 \times 49 = 25^3 - 24^2 \times 25$, we see that $(3, 4, 5)$ form a right triangle with area 6.

$n = 6$. Since $35^2 = 25 \times 1 \times 49 = 25^3 - 24^2 \times 25$, we see that $(3, 4, 5)$ form a right triangle with area 6.

We can find the sides (a, b, c) from the solution, for example as follows: from the solution to the equation of the elliptic curve we know $c = 5$. Then

$$a^2 + b^2 = 25$$
$$ab = 12.$$

The first tells us that a, b are less than $\sqrt{25} = 5$ and since they are divisors of 12 the unique solution is $a = 3, b = 4$ or viceversa.

$n = 6$. Since $35^2 = 25 \times 1 \times 49 = 25^3 - 24^2 \times 25$, we see that $(3, 4, 5)$ form a right triangle with area 6.

We can find the sides (a, b, c) from the solution, for example as follows: from the solution to the equation of the elliptic curve we know $c = 5$. Then

$$a^2 + b^2 = 25$$
$$ab = 12.$$

The first tells us that a, b are less than $\sqrt{25} = 5$ and since they are divisors of 12 the unique solution is $a = 3, b = 4$ or viceversa.

What for other n, for example $n = 1/4$?

Problem

Is there an integer solution to $x^4 + y^4 = z^4$*?*

Problem

Is there an integer solution to $x^4 + y^4 = z^4$?

Multiply by z^2/x^6 and change $z/x = x^2$, $zy^2/x^3 = y$ to get

$$y^2 = x^3 - x$$

Problem

Is there an integer solution to $x^4 + y^4 = z^4$?

Multiply by z^2/x^6 and change $z/x = x^2$, $zy^2/x^3 = y$ to get

$$y^2 = x^3 - x$$

No points except $(0,0), (1,0), (-1,0)$ and so no nontrivial solutions to the equation.

Elliptic Curves

Given the field K, an Elliptic curve is a subset of $K \times K$ given by a cubic equation. The most simple is the **Weierstrass equation**.

$$E := \{(x, y) \in K \times K \,:\, y^2 = x^3 + Ax + B\} U \{O\}, \tag{2}$$

where O is an extra point at infinity and the coefficients $A, B \in K$.

Elliptic Curves

Given the field K, an Elliptic curve is a subset of $K \times K$ given by a cubic equation. The most simple is the **Weierstrass equation**.

$$E := \{(x, y) \in K \times K \; : \; y^2 = x^3 + Ax + B\} U \{O\}, \qquad (2)$$

where O is an extra point at infinity and the coefficients $A, B \in K$.

In order to call it an elliptic curve, we do not allow singular equations, which means that

$$((e_1 - e_2)(e_3 - e_2)(e_1 - e_3))^2 = -(4A^3 + 27B^2) \neq 0,$$

where e_1, e_2, e_3 are the roots of $x^3 + Ax + B$.

Elliptic Curves

Given the field K, an Elliptic curve is a subset of $K \times K$ given by a cubic equation. The most simple is the **Weierstrass equation**.

$$E := \{(x, y) \in K \times K \,:\, y^2 = x^3 + Ax + B\} U \{O\}, \tag{2}$$

where O is an extra point at infinity and the coefficients $A, B \in K$.

In order to call it an elliptic curve, we do not allow singular equations, which means that

$$((e_1 - e_2)(e_3 - e_2)(e_1 - e_3))^2 = -(4A^3 + 27B^2) \neq 0,$$

where e_1, e_2, e_3 are the roots of $x^3 + Ax + B$.

$E(L)$ denotes the solutions to the equation describing E in the field $K \subset L$.

$y^2 - 2y + 1 = x^3 + Ax + B$, is the same as $y^2 = x^3 + Ax + B$ adding 1 to the y coordinate.

In general we will consider E' to be "the same" elliptic curve as E if we can go from one to the other, and backwards, by a change of variables.

$y^2 - 2y + 1 = x^3 + Ax + B$, is the same as $y^2 = x^3 + Ax + B$ adding 1 to the y coordinate.

In general we will consider E' to be "the same" elliptic curve as E if we can go from one to the other, and backwards, by a change of variables.

If $\text{char}(K) \neq 2, 3$ then we can reduce the **generalized Weierstrass equation**

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{3}$$

with $a_1, a_2, a_3, a_4, a_6 \in K$ to

$$Y^2 = X^3 + AX + B$$

with $A, B \in K$.

Exercise: Many generalized Weierstrass equations correspond to the same Weierstrass equation. Which ones?

Exercise: Many generalized Weierstrass equations correspond to the same Weierstrass equation. Which ones?

Let $j = 1728\frac{4A^3}{4A^3+27B^2}$.

Theorem

Two elliptic curves are isomorphic over $\overline{K}$, if and only if they have the same j invariant. In fact, there exist $\mu \in \overline{K}$ so that the change of variables $(X, Y) = (\mu^2 x, \mu^3 y)$ brings one to the other.

Exercise: Many generalized Weierstrass equations correspond to the same Weierstrass equation. Which ones?

Let $j = 1728\frac{4A^3}{4A^3+27B^2}$.

Theorem

Two elliptic curves are isomorphic over $\overline{K}$, if and only if they have the same j invariant. In fact, there exist $\mu \in \overline{K}$ so that the change of variables $(X, Y) = (\mu^2 x, \mu^3 y)$ brings one to the other.

Remark. There are curves which are isomorphic, but they are not the same over their field of definition. For example $y^2 = x^3 - 25x$ has infinitely many rational points, while $y^2 = x^3 - x$ has only four. Both have j invariant 1728.

Exercise: Many generalized Weierstrass equations correspond to the same Weierstrass equation. Which ones?

Let $j = 1728\frac{4A^3}{4A^3+27B^2}$.

Theorem

Two elliptic curves are isomorphic over $\overline{K}$, if and only if they have the same j invariant. In fact, there exist $\mu \in \overline{K}$ so that the change of variables $(X, Y) = (\mu^2 x, \mu^3 y)$ brings one to the other.

Remark. There are curves which are isomorphic, but they are not the same over their field of definition. For example $y^2 = x^3 - 25x$ has infinitely many rational points, while $y^2 = x^3 - x$ has only four. Both have j invariant 1728.

Remark. $y^2 = x^3 + \frac{3j}{1728-j}x + \frac{2j}{1728-j}$ has j invariant j. $y^2 = x^3 + 1$ and $y^2 = x^3 + x$ have 0 and 1728 as j invariants. These curves have more automorphisms than the trivial $(x, y) \to (x, -y)$.

There are some other equations which can be reduced to Weierstrass form.

There are some other equations which can be reduced to Weierstrass form.

- **Legendre form** Transform $y^2 = (x - e_1)(x - e_2)(x - e_3)$ into $Y^2 = (X)(X - 1)(X - \lambda)$ where $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$. Not over K

There are some other equations which can be reduced to Weierstrass form.

- **Legendre form** Transform $y^2 = (x - e_1)(x - e_2)(x - e_3)$ into $Y^2 = (X)(X - 1)(X - \lambda)$ where $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$. Not over K
- **Cubic equations** Every cubic equation $C(x, y) = 0$ over K with $P \in E(K)$ and $\mathrm{char}(K) \neq 2, 3$, can be transformed into Weierstrass equation. Example $y^3 + x^3 = 1$ can be transformed into $y^2 = x^3 - 432$. Maybe singular

There are some other equations which can be reduced to Weierstrass form.

- **Legendre form** Transform $y^2 = (x - e_1)(x - e_2)(x - e_3)$ into $Y^2 = (X)(X - 1)(X - \lambda)$ where $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$. Not over K
- **Cubic equations** Every cubic equation $C(x, y) = 0$ over K with $P \in E(K)$ and $\mathrm{char}(K) \neq 2, 3$, can be transformed into Weierstrass equation. Example $y^3 + x^3 = 1$ can be transformed into $y^2 = x^3 - 432$. Maybe singular
- **Quartic equations** If $C := v^2 = au^4 + bu^3 + cu^2 + du + e$, $P \in C(K)$, and $\mathrm{char}(K) \neq 2$, it has Weierstrass form.

There are some other equations which can be reduced to Weierstrass form.

- **Legendre form** Transform $y^2 = (x - e_1)(x - e_2)(x - e_3)$ into $Y^2 = (X)(X - 1)(X - \lambda)$ where $\lambda = \frac{e_3 - e_1}{e_2 - e_1}$. Not over K
- **Cubic equations** Every cubic equation $C(x, y) = 0$ over K with $P \in E(K)$ and $\mathrm{char}(K) \neq 2, 3$, can be transformed into Weierstrass equation. Example $y^3 + x^3 = 1$ can be transformed into $y^2 = x^3 - 432$. Maybe singular
- **Quartic equations** If $C := v^2 = au^4 + bu^3 + cu^2 + du + e$, $P \in C(K)$, and $\mathrm{char}(K) \neq 2$, it has Weierstrass form.
- **Interserction of two Quadric surfaces** The intersection of the two surfaces $au^2 + bv^2 = e$ and $cu^2 + dw^2 = f$ is an elliptic curve, whenever the intersection is nonempty in a field K of $\mathrm{char}(K) \neq 2$.

Group Law

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ points on E and denote $P_3 = P_1 + P_2 = (x_3, y_3)$. Consider the equations given by $-P_1 = (x_1, -y_1)$.

$$\begin{aligned} x_3 &= m^2 - x_2 - x_1, \\ y_3 &= m(x_1 - x_3) - y_1, \end{aligned} \tag{4}$$

where

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2, \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0. \end{cases}$$

Observe that if $y_1 = 0$, then $P_1 = -P_1$ and then $2P_1 = O$.

Group Law

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ points on E and denote $P_3 = P_1 + P_2 = (x_3, y_3)$. Consider the equations given by $-P_1 = (x_1, -y_1)$.

$$\begin{aligned} x_3 &= m^2 - x_2 - x_1, \\ y_3 &= m(x_1 - x_3) - y_1, \end{aligned} \tag{4}$$

where

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2, \\ \frac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0. \end{cases}$$

Observe that if $y_1 = 0$, then $P_1 = -P_1$ and then $2P_1 = O$.

Theorem

Let $E := y^2 = x^3 + Ax + B$ be an elliptic curve. Then, the equations in (4) give structure of group to the curve E.

Endomorphisms

Definition

An endomorphism of an elliptic curve E defined over K is a map $\alpha : E(\overline{K}) \to E(\overline{K})$ such that $\alpha(P+Q) = \alpha(P) + \alpha(Q)$ and

$$\alpha(x,y) = (r_1(x), yr_2(x)) = \left(\frac{p_1(x)}{q_1(x)}, y\frac{p_2(x)}{q_2(x)} \right).$$

It is separable if one of $p_1'(x), q_1'(x)$ is not identically zero. Otherwise is inseparable.

We call **Degree** *of α to be $Max\{deg(p_1(x)), deg(q_1(x))\}$*

Endomorphisms

Definition

An endomorphism of an elliptic curve E defined over K is a map $\alpha : E(\overline{K}) \to E(\overline{K})$ such that $\alpha(P+Q) = \alpha(P) + \alpha(Q)$ and

$$\alpha(x,y) = (r_1(x), yr_2(x)) = \left(\frac{p_1(x)}{q_1(x)}, y\frac{p_2(x)}{q_2(x)}\right).$$

It is separable if one of $p_1'(x), q_1'(x)$ is not identically zero. Otherwise is inseparable.

We call **Degree** *of α to be $Max\{deg(p_1(x)), deg(q_1(x))\}$*

Remark. If $q_1(x) = 0$, then $\alpha(x,y) = O$. If $q_1(x) \neq 0$, then $q_2(x) \neq 0$.

Remark. If the characteristic is 0 there are no inseparable polynomials. If $\mathrm{char}(K) = p$ the inseparable polynomials are $g(x^p)$.

Examples. Multiplication by an integer n is an endomorphism for any elliptic curve, simply because its group structure. In the particular case of $n = 2$, the equations are given by the **Doubling equations**.

$$r_1(x) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)},$$
$$r_2(x) = \frac{-(8B^2 - 5Ax^4 + 5x^2A^2 + 4AxB - 20x^3B - x^6 + A^3)}{8(x^3 + Ax + B)^2}.$$

In the finite field F_q, with characteristic p and $q = p^r$ elements, the most important endomorphism is called the **Frobenius** endomorphism

$$\phi_q(x, y) = (x^q, y^q). \tag{5}$$

Theorem

Let E be an elliptic curve defined over the finite field F_q. The Frobenius map is an inseparable endomorphism of E of degree q.

Proof We need $\phi_q(E) \in E$ and $\phi_q(P + Q) = \phi_q(P) + \phi_q(Q)$. It follows from the identities $x^q = x$ and $(a + b)^q = a^q + b^q$. The degree and separability are consequences of the definition.

In the finite field F_q, with characteristic p and $q = p^r$ elements, the most important endomorphism is called the **Frobenius** endomorphism

$$\phi_q(x, y) = (x^q, y^q). \tag{5}$$

Theorem

Let E be an elliptic curve defined over the finite field F_q. The Frobenius map is an inseparable endomorphism of E of degree q.

Proof We need $\phi_q(E) \in E$ and $\phi_q(P + Q) = \phi_q(P) + \phi_q(Q)$. It follows from the identities $x^q = x$ and $(a + b)^q = a^q + b^q$. The degree and separability are consequences of the definition.

The set of endomorphisms of an elliptic curve has ring structure. In fact it is a $\mathbb{Z}$-module.

Proposition

Let E be and elliptic curve, and α a non trivial endomorphism of E. Then, if it is separable then deg$(\alpha) = |Ker(\alpha)|$ and deg$(\alpha) > |Ker(\alpha)|$ otherwise.

Proof. Let $\alpha = (r_1(x), yr_2(x))$ and $r_1(x) = p/q(x)$. Since it is an endomorphism it is enough to see that $|\alpha^{-1}(P)| =$deg(α) for any P in the image of α. Now it is enough to find a so that $r_1(x) = a$ and $r_1'(x) \neq 0$. This guaranties that $p - aq$ does not have multiple roots, and hence, with a suitable a it will have precisely deg(α) roots. For each of them, the second coordinate is fixed by the definition of the endomorphism.

For the proof, we need $r_1(x)$ to take infinitely many values. In fact, it takes them all.

Theorem

Let E be and elliptic curve, and α a non trivial endomorphism of E. Then, $\alpha(E(\overline{K})) = E(\overline{K})$.

Proof. If $p - aq$ is not constant the result is trivial. But it can only be constant for one value of a. Take another point, and add it to get a in the image.

For the proof, we need $r_1(x)$ to take infinitely many values. In fact, it takes them all.

Theorem

Let E be and elliptic curve, and α a non trivial endomorphism of E. Then, $\alpha(E(\overline{K})) = E(\overline{K})$.

Proof. If $p - aq$ is not constant the result is trivial. But it can only be constant for one value of a. Take another point, and add it to get a in the image.

We now state a condition on separability important for the applications.

Proposition

Let E be an elliptic curve over q a power of the prime p, and r, s integers not both zero. Then $r\phi + s$ is separable if and only if $p \nmid s$.

The proof is a direct application of the following results.

The proof is a direct application of the following results.

Lemma

Let $\alpha_1 = (R_1(x), yS_1(x))$, $\alpha_2 = (R_2(x), yS_2(x))$ *endomorphims and let* $\alpha_3 = \alpha_1 + \alpha_2 = (R_3(x), yS_3(x))$.*If*

$$R_1'(x)/S_1(x) = c_1 \qquad \textit{and} \qquad R_2'(x)/S_2(x) = c_2,$$

then $R_3'(x)/S_3(x) = c_1 + c_2$.

The proof is a direct application of the following results.

Lemma

Let $\alpha_1 = (R_1(x), yS_1(x))$*,* $\alpha_2 = (R_2(x), yS_2(x))$ *endomorphims and let* $\alpha_3 = \alpha_1 + \alpha_2 = (R_3(x), yS_3(x))$*.If*

$$R_1'(x)/S_1(x) = c_1 \qquad \text{and} \qquad R_2'(x)/S_2(x) = c_2,$$

then $R_3'(x)/S_3(x) = c_1 + c_2$*.*

This lemma is a consequence of the chain rule.

Corollary

Let $n(x, y) = (R_n(x), yS_n(x))$, *the multiplication by* n *in* E. *Then*

$$R_n'(x)/S_n(x) = n.$$

Corollary

Let $n(x,y) = (R_n(x), yS_n(x))$*, the multiplication by* n *in* E*. Then*

$$R_n'(x)/S_n(x) = n.$$

Proof. For positive n it is an straighforward application of the previous lemma and induction. For negative n recall that $-n(x,y) = (R_n(x), -yS_n(x))$.

Singular curves

Two results are important in case the discrimant of the curve vanishes.

Singular curves

Two results are important in case the discrimant of the curve vanishes.

Theorem

Let $E := y^2 = x^3$ be defined over K. Then, the map α from $E(K) - (0,0)$ to $(K,+)$ given by

$$\alpha(x,y) = \frac{x}{y}, \qquad \alpha(O) = 0,$$

is an isomorphism. The inverse is $\alpha^{-1}(t) = (\frac{1}{t^2}, \frac{1}{t^3})$.

Theorem

$E := y^2 = x^3 + a^2x^2$ over K. α from $E(K) - (0,0)$

$$\alpha(x,y) = \frac{y+ax}{y-ax}, \qquad \alpha(O) = 1.$$

i) if $a \in K^*$ then α is an isomorphism to $(K^*, \times)$.

$$\alpha^{-1}(t) = \left(\frac{4a^2t}{(t-1)^2}, \frac{4a^3t(t+1)}{(t-1)^3}\right).$$

ii) If $a \notin K$, then α is an isomorphism to the multiplicative group

$$\{u + av \,:\, (v,v) \in K \times K, u^2 - a^2v^2 = 1\},$$

$$\alpha^{-1}(u,v) = \left(\left(\frac{u+1}{v}\right)^2 - a, \frac{u+1}{v}x\right)$$

The proofs are consequences of the parametrizations exhibited and the addition laws. When the curve in the first theorem arises from reducing a curve modulo a prime, se say that the curve have **additive** reduction. If it is the case i) or ii) of the second theorem, we say that the reduction is **split** or **nonsplit multiplicative** respectively. If the reduction is non singular, we say **good reduction.**

Curves modulo composite integers.

The problem when working modulo composite integers is that we are working with rings that have divisors of zero. To avoid this problem, we have to work on the projective spaces so we can somehow forget about denominators. The notion of primitive is important.

Curves modulo composite integers.

The problem when working modulo composite integers is that we are working with rings that have divisors of zero. To avoid this problem, we have to work on the projective spaces so we can somehow forget about denominators. The notion of primitive is important.

Definition

Let R be a commutative ring. An n-tuple $(r_1, \dots, r_n)$ is primitive if there are elements $(x_1, \dots x_n)$of R so that $x_1 r_1 + \cdots + x_n r_n = 1$.

We say that two primitive triples (x, y, z) and (x', y', z') are equivalent if there exist $u \in R^*$ so that $(x', y', z') = u(x, y, z)$. P^2_R are the primitive triples modulo the equivalence relation, and we denote $(x : y : z)$ the class of the triple (x, y, z).

Definition

An elliptic curve E defined over R is an homogeneous equation $y^2z = x^3 + Axz^2 + Bz^3$ with $A, B \in R$ and so that $4A^3 + 27B^2 \in R^*$.

Definition

An elliptic curve E defined over R is an homogeneous equation $y^2z = x^3 + Axz^2 + Bz^3$ with $A, B \in R$ and so that $4A^3 + 27B^2 \in R^*$.

Theorem

Let $E := y^2z = x^3 + Axz^2 + Bz^3$ be an elliptic curve defined in P^2_R. There exist three sets of equation wich give group structure to $E(R)$.

Remark The equation are in the book of Washington. The theorem ensures that some of the equations in the set allow to define the addition of two points avoiding the problems in the denominators.

See Example 2.10 in the same book.

Corollary

Let $(n_1, n_2) = 1$ *odd and* E *over* $\mathbb{Z}/n_1 n_2\mathbb{Z}$. *Then, the CRT gives a group isomorphism* $E(\mathbb{Z}/n_1 n_2\mathbb{Z}) \simeq E(\mathbb{Z}/n_1\mathbb{Z}) \times E(\mathbb{Z}/n_2\mathbb{Z})$.

Corollary

Let $(n_1, n_2) = 1$ *odd and* E *over* $\mathbb{Z}/n_1 n_2\mathbb{Z}$. *Then, the CRT gives a group isomorphism* $E(\mathbb{Z}/n_1 n_2\mathbb{Z}) \simeq E(\mathbb{Z}/n_1\mathbb{Z}) \times E(\mathbb{Z}/n_2\mathbb{Z})$.

Corollary

Let , $E/\mathbb{Z}$, *and* n *an integer coprime with the discriminant. Then*

$$red_n : (x : y : z) \to (x : y : z) \pmod{n}$$

gives a group homomorphism between $E(\mathbb{Q})$ *and* $E(\mathbb{Z}/n\mathbb{Z})$.

Corollary

Let $(n_1, n_2) = 1$ *odd and* E *over* $\mathbb{Z}/n_1n_2\mathbb{Z}$. *Then, the CRT gives a group isomorphism* $E(\mathbb{Z}/n_1n_2\mathbb{Z}) \simeq E(\mathbb{Z}/n_1\mathbb{Z}) \times E(\mathbb{Z}/n_2\mathbb{Z})$.

Corollary

Let , $E/\mathbb{Z}$, *and* n *an integer coprime with the discriminant. Then*

$$red_n : (x : y : z) \to (x : y : z) \pmod{n}$$

gives a group homomorphism between $E(\mathbb{Q})$ *and* $E(\mathbb{Z}/n\mathbb{Z})$.

Corollary

Let R *a ring and* I *an ideal. Then,*

$$red_I : (x : y : z) \to (x : y : z) \pmod{I}$$

gives a group homomorphism between $E(R)$ *and* $E(R/I)$.

Corollary

Let $(n_1, n_2) = 1$ *odd and* E *over* $\mathbb{Z}/n_1n_2\mathbb{Z}$. *Then, the CRT gives a group isomorphism* $E(\mathbb{Z}/n_1n_2\mathbb{Z}) \simeq E(\mathbb{Z}/n_1\mathbb{Z}) \times E(\mathbb{Z}/n_2\mathbb{Z})$.

Corollary

Let , $E/\mathbb{Z}$, *and* n *an integer coprime with the discriminant. Then*

$$red_n : (x : y : z) \to (x : y : z) \pmod{n}$$

gives a group homomorphism between $E(\mathbb{Q})$ *and* $E(\mathbb{Z}/n\mathbb{Z})$.

Corollary

Let R *a ring and* I *an ideal. Then,*

$$red_I : (x : y : z) \to (x : y : z) \pmod{I}$$

gives a group homomorphism between $E(R)$ *and* $E(R/I)$.

The result needs mild conditions on R and I.

Elliptic Curves II

J. Jiménez Urroz, UPC

Benin, July, 17, 2014

Given $E := y^2 + Ax + B$ we are interested in the torsion part.

If $K = \mathbb{F}_q$ then $E(K) \simeq E_{\text{tors}}(K)$.

Given $E := y^2 + Ax + B$ we are interested in the torsion part.

If $K = \mathbb{F}_q$ then $E(K) \simeq E_{\text{tors}}(K)$.

In particular we will study

$$E[n] = \{P \in E(\overline{K}) \, : \, nP = O\}.$$

Given $E := y^2 + Ax + B$ we are interested in the torsion part.

If $K = \mathbb{F}_q$ then $E(K) \simeq E_{\text{tors}}(K)$.

In particular we will study

$$E[n] = \{P \in E(\overline{K}) \,:\, nP = O\}.$$

Example: $n = 2$.
• $\text{char}K \neq 2$. $2P = O$, $E := \{y^2 = P(x)\}$, with $\deg(P) = 3$.

$$E[2] = \{(e_1, 0), (e_2, 0), (e_3, 0), O\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

where $P(x) = (x - e_1)(x - e_2)(x - e_3)$

Given $E := y^2 + Ax + B$ we are interested in the torsion part.

If $K = \mathbb{F}_q$ then $E(K) \simeq E_{\text{tors}}(K)$.

In particular we will study

$$E[n] = \{P \in E(\overline{K}) \,:\, nP = O\}.$$

Example: $n = 2$.

• char$K \neq 2$. $2P = O$, $E := \{y^2 = P(x)\}$, with $\deg(P) = 3$.

$$E[2] = \{(e_1, 0), (e_2, 0), (e_3, 0), O\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

where $P(x) = (x - e_1)(x - e_2)(x - e_3)$

In characteristic 2, $E := \{y^2 + xy + x^3 + a_2x^2 + a_6 = 0\}$, $a_6 \neq 0$ or $E := \{y^2 + a_3y + x^3 + a_4x + a_6 = 0\}$, $a_3 \neq 0$ and $E[2] \simeq \mathbb{Z}/2\mathbb{Z}$ or $E[2] = O$.

Example $n = 3$.

• char$K \neq 2, 3$. $2P = -P$ This means that $2P$ and P has the same x coordinates.

$$m^2 - 2x = x, \text{ where } m = \frac{3x^2 + A}{2y}$$

Example $n = 3$.
• char$K \neq 2, 3$. $2P = -P$ This means that $2P$ and P has the same x coordinates.

$$m^2 - 2x = x, \text{ where } m = \frac{3x^2 + A}{2y}$$

Clearing denominators, we get

$$3x^4 + 6AX^2 + 12Bx - A^2 = 0$$

Example $n = 3$.

• char$K \neq 2, 3$. $2P = -P$ This means that $2P$ and P has the same x coordinates.

$$m^2 - 2x = x, \text{ where } m = \frac{3x^2 + A}{2y}$$

Clearing denominators, we get

$$3x^4 + 6AX^2 + 12Bx - A^2 = 0$$

The discriminant of the polynomial is $-6912(4A^3 + 27B^2)^2$

Example $n = 3$.

• char$K \neq 2, 3$. $2P = -P$ This means that $2P$ and P has the same x coordinates.

$$m^2 - 2x = x, \text{ where } m = \frac{3x^2 + A}{2y}$$

Clearing denominators, we get

$$3x^4 + 6AX^2 + 12Bx - A^2 = 0$$

The discriminant of the polynomial is $-6912(4A^3 + 27B^2)^2$

$$E[3] \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z},$$

• char$K = 3$. In this case we have
$E := y^2 = x^3 + a_2x^2 + a_4x + a_6$, and taking into account $3 = 0$, some terms dissapear in the addition equations. We get

$$\left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 3x = 0,$$

which simplifies to

$$a_2x^3 + a_2a_6 - a_4^2 = 0.$$

• char$K = 3$. In this case we have
$E := y^2 = x^3 + a_2x^2 + a_4x + a_6$, and taking into account $3 = 0$, some terms dissapear in the addition equations. We get

$$\left(\frac{2a_2x + a_4}{2y}\right)^2 - a_2 = 3x = 0,$$

which simplifies to

$$a_2x^3 + a_2a_6 - a_4^2 = 0.$$

If $a_2 = 0$ there are no solutions, and otherwise has a triple root. Hence, $E[3] = O$ or $E[3] \simeq \mathbb{Z}/3\mathbb{Z}$ in characteristic 3.

For given A, B, we define the **Division polynomial** $\psi_n(x, y)$ by the following recursive formula.

$$
\begin{aligned}
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6AX^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \qquad \text{for } m \geq 2 \\
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \qquad \text{for } m \geq 3.
\end{aligned}
$$

For given A, B, we define the **Division polynomial** $\psi_n(x, y)$ by the following recursive formula.

$$\begin{aligned}
\psi_1 &= 1\\
\psi_2 &= 2y\\
\psi_3 &= 3x^4 + 6AX^2 + 12Bx - A^2\\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \qquad \text{for } m \geq 2\\
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2), \qquad \text{for } m \geq 3.
\end{aligned}$$

From here, one can see that $\psi_{2n+1} \in \mathbb{Z}[x]$, $\psi_{2n} \in 2y\mathbb{Z}[x]$, and

$$\begin{aligned}
\varphi_m &= x\psi_m^2 - \psi_{m-1}\psi_{m+1},\\
\omega_m &= (4y)^{-1}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2),
\end{aligned} \tag{1}$$

are indeed polynomials and $\{\varphi_m, \omega_{2m}\} \subset \mathbb{Z}[x]$ while $\omega_{2m+1} \in y\mathbb{Z}[x]$.

Theorem

Let $P = (x, y)$ be a point on the elliptic curve $y^2 = x^3 + Ax + B$, and let n be a positive integer. Then,

$$nP = \left(\frac{\varphi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3} \right).$$

Theorem

Let $P = (x, y)$ be a point on the elliptic curve $y^2 = x^3 + Ax + B$, and let n be a positive integer. Then,

$$nP = \left(\frac{\varphi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3} \right).$$

Theorem

Multiplication by n is an endomorphism of degree n^2.

Theorem

Let $P = (x, y)$ be a point on the elliptic curve $y^2 = x^3 + Ax + B$, and let n be a positive integer. Then,

$$nP = \left(\frac{\varphi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3} \right).$$

Theorem

Multiplication by n is an endomorphism of degree n^2.

Proof.

$$\varphi_m(x) = x^{m^2} + \text{ lower degree terms},$$
$$\psi_m(x)^2 = m^2 x^{m^2-1} + \text{ lower degree terms}.$$

Theorem

Let E/K be an elliptic curve and $char(K) = p$.
a) If $p \nmid n$ then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
b)If $p|n$ then $E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$. or $E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, where n' is the greatest divisor of n coprime with p.

Theorem

Let E/K be an elliptic curve and $\mathrm{char}(K) = p$.
a) If $p \nmid n$ then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
b)If $p|n$ then $E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$. or $E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, where n' is the greatest divisor of n coprime with p.

Remark. When $E[p] = \mathbb{Z}/p\mathbb{Z}$ the curve is called **ordinary**. If $E[p] = O$ then it is **supersingular**.

Theorem

Let E/K be an elliptic curve and char$(K) = p$.
a) If $p \nmid n$ then $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.
b)If $p|n$ then $E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$. or $E[n] \simeq \mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, where n' is the greatest divisor of n coprime with p.

Remark. When $E[p] = \mathbb{Z}/p\mathbb{Z}$ the curve is called **ordinary**. If $E[p] = O$ then it is **supersingular**.

Proof. The degree of the multiplication by n is n^2, which is the size of the kernel when $p \nmid n$. Hence, by the clasification of finite abelian groups, it must be $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

If $p \nmid n$, then there exist $P, Q \in E[n]$ so that $R = aP + bQ$ for any $R \in E[n]$ and some $a, b \in \mathbb{Z}$. Moreover, if α is and homomorphism of E, then

$$\alpha(nP) = n\alpha(P),$$

so $\alpha : E[n] \to E[n]$. we can associate a 2 by 2 matrix in $M_2(\mathbb{Z}/n\mathbb{Z})$ to each homomorphism of the curve. (endomorphism or automorphism of the field $\overline{K}$)

If $p \nmid n$, then there exist $P, Q \in E[n]$ so that $R = aP + bQ$ for any $R \in E[n]$ and some $a, b \in \mathbb{Z}$. Moreover, if α is and homomorphism of E, then

$$\alpha(nP) = n\alpha(P),$$

so $\alpha : E[n] \to E[n]$. we can associate a 2 by 2 matrix in $M_2(\mathbb{Z}/n\mathbb{Z})$ to each homomorphism of the curve. (endomorphism or automorphism of the field $\overline{K}$)

Example: $E := y^2 = x^3 - x$. $p = 11, n = 3$

$\psi_3(x) = 3x^4 - 6x^2 - 1; \quad \psi_3(4) = 4^2(3 \cdot 4^2 - 6) - 1$

$E[3] =< (4,4), (7, 5\sqrt{2}) >=< P, Q >$

$\phi_{11}(4,4) = (4,4)$, $\phi_{11}(7, 5\sqrt{2}) = (7, 6\sqrt{2}) = -Q$, hence

$$\phi_{11} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Elliptic curves over $\mathbb{C}$.

Let $L = m\omega_1 + n\omega_2$ be a lattice in $\mathbb{C}$, and denote $\mathfrak{E}(L)$ the set of meromorphic functions on $\mathbb{C}/L$. In particular $f(z+\omega) = f(z)$ for all $\omega \in L$. Let F be a fundamental domain for $\mathbb{C}/L$

Elliptic curves over $\mathbb{C}$.

Let $L = m\omega_1 + n\omega_2$ be a lattice in $\mathbb{C}$, and denote $\mathfrak{E}(L)$ the set of meromorphic functions on $\mathbb{C}/L$. In particular $f(z+\omega) = f(z)$ for all $\omega \in L$. Let F be a fundamental domain for $\mathbb{C}/L$

Theorem

Any function in $\mathfrak{E}(L)$ without poles in F is constant.

Proof. Liouville's theorem

Elliptic curves over $\mathbb{C}$.

Let $L = m\omega_1 + n\omega_2$ be a lattice in $\mathbb{C}$, and denote $\mathfrak{E}(L)$ the set of meromorphic functions on $\mathbb{C}/L$. In particular $f(z+\omega) = f(z)$ for all $\omega \in L$. Let F be a fundamental domain for $\mathbb{C}/L$

Theorem

Any function in $\mathfrak{E}(L)$ without poles in F is constant.

Proof. Liouville's theorem

Theorem

For $f \in \mathfrak{E}(L)$ and $z_0 \in \mathbb{C}$, the sum of the residues of f in $z_0 + F$ is zero.

Proof Cauchy's theorem (The only condition needed is that f has no poles at the boundary of $z_0 + F$)

Corollary

For $f \in \mathfrak{E}(L)$ and $z_0 \in \mathbb{C}$, the sum of the orders of zeroes in $z_0 + \mathfrak{E}(L)$ is equal to the sum of the order of poles in $z_0 + \mathfrak{E}(L)$ counting multiplicities.

Proof Take $\frac{f'}{f}$.

Corollary

For $f \in \mathfrak{E}(L)$ and $z_0 \in \mathbb{C}$, the sum of the orders of zeroes in $z_0 + \mathfrak{E}(L)$ is equal to the sum of the order of poles in $z_0 + \mathfrak{E}(L)$ counting multiplicities.

Proof Take $\frac{f'}{f}$.

Example: $\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$

$$\mathcal{P}'(z) = -\sum_{\omega \in L} \frac{1}{(z-\omega)^3}.$$

Corollary

For $f \in \mathfrak{E}(L)$ and $z_0 \in \mathbb{C}$, the sum of the orders of zeroes in $z_0 + \mathfrak{E}(L)$ is equal to the sum of the order of poles in $z_0 + \mathfrak{E}(L)$ counting multiplicities.

Proof Take $\frac{f'}{f}$.

Example: $\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$

$$\mathcal{P}'(z) = -\sum_{\omega \in L} \frac{1}{(z-\omega)^3}.$$

$\mathcal{P}$ is even. $\mathcal{P}'$ is odd.

Corollary

For $f \in \mathfrak{E}(L)$ and $z_0 \in \mathbb{C}$, the sum of the orders of zeroes in $z_0 + \mathfrak{E}(L)$ is equal to the sum of the order of poles in $z_0 + \mathfrak{E}(L)$ counting multiplicities.

Proof Take $\frac{f'}{f}$.

Example: $\mathcal{P}(z) = \frac{1}{z^2} + \sum_{\substack{\omega\in L\\ \omega\neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$

$$\mathcal{P}'(z) = -\sum_{\omega\in L} \frac{1}{(z-\omega)^3}.$$

$\mathcal{P}$ is even. $\mathcal{P}'$ is odd.

Theorem

In the conditions above

- $\mathfrak{E}(L) = \mathbb{C}(\mathcal{P}, \mathcal{P}')$. *In fact,* $\mathfrak{E}(L)^+ = \mathbb{C}(\mathcal{P})$
- $\mathcal{P}'^2 = a\mathcal{P}^3 + b\mathcal{P}^2 + c\mathcal{P} + d$, *for some* $a, b, c, d \in \mathbb{C}$.

Corollary

For any integer n $\mathcal{P}(nz)$ *is a rational function of* $\mathcal{P}(z)$ *and* $\mathcal{P}'(z)$

Corollary

For any integer n $\mathcal{P}(nz)$ is a rational function of $\mathcal{P}(z)$ and $\mathcal{P}'(z)$

Theorem

The map $z \to (\mathcal{P}(z), \mathcal{P}'(z))$ is an analytic one to one correspondence between $\mathbb{C}/L$ and the elliptic curve $y^2 = 4x^3 + g_2(L)x + g_3(L)$.

Pairings

We call μ_n the group of n-th roots of unity in $\overline{K}$.

Theorem

Let E/K be an elliptic curve, and $char(K) \nmid n$. There exist a pairing

$$e_n : E[n] \times E[n] \to \mu_n,$$

which is bilinear, non-degenerate, Galois compatible, and such that $e_n(P,P) = 1$ and $e_n(\alpha(P), \alpha(Q)) = e_n(P,Q)^{deg(\alpha)}$.

Pairings

We call μ_n the group of n-th roots of unity in $\overline{K}$.

Theorem

Let E/K be an elliptic curve, and $\mathrm{char}(K) \nmid n$. There exist a pairing

$$e_n : E[n] \times E[n] \to \mu_n,$$

which is bilinear, non-degenerate, Galois compatible, and such that $e_n(P, P) = 1$ and $e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{deg(\alpha)}$.

$$1 = e_n(T+S, T+S) = e_n(T, T)e_n(T, S)e_n(S, T)e_n(S, S),$$

hence

$$e_n(T, S) = e_n(S, T)^{-1}$$

Corollary

If T_1, T_2 is a basis of $E[n]$, then $e_n(T_1, T_2)$ is a primitive n-th root of unity.

Corollary

If T_1, T_2 is a basis of $E[n]$, then $e_n(T_1, T_2)$ is a primitive n-th root of unity.

Corollary

If $E[n] \in E(K)$, then $\mu_n \in K$.

Corollary

If T_1, T_2 is a basis of $E[n]$, then $e_n(T_1, T_2)$ is a primitive n-th root of unity.

Corollary

If $E[n] \in E(K)$, then $\mu_n \in K$.

Corollary

Let E/Q be an elliptic curve. $E[n] \notin E(\mathbb{Q})$ for $n \geq 3$.

To any endomorphism α we can associate a 2×2 matrix α_n with entries in $Z/n\mathbb{Z}$.

Proposition

Let E be an elliptic curve over K with char$(K) = p$. Let α be an endomorphism of E and n an integer not divisible by p. Then $deg(\alpha) \equiv det(\alpha_n) \pmod{n}$.

Proof.

$$\begin{aligned} \zeta^{\deg\alpha} &= e_n(\alpha(T_1), \alpha(T_2)) = e_n(aT_1 + bT_2, cT_1 + dT_2) \\ &= e_n(T_1, T_2)^{ad-bc}. \end{aligned}$$

Proposition

$deg(a\alpha + b\beta) = a^2 deg\alpha + b^2 deg\beta + ab(deg(\alpha + \beta) - deg\alpha - deg\beta)$.

Finite Fields

Examples. $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$.

x	$x^3 + x + 1$	y	Points
0	1	± 1	$(0,1),(0,4)$
1	3		
2	1	± 1	$(2,1),(2,4)$
3	1	± 1	$(3,1),(3,4)$
4	4	± 2	$(4,2),(4,3)$

Therefore, $E(\mathbb{F}_5) =< (0,1) >$ has order 9.

Finite Fields

Examples. $y^2 = x^3 + x + 1$ over $\mathbb{F}_5$.

x	x^3+x+1	y	Points
0	1	± 1	$(0,1),(0,4)$
1	3		
2	1	± 1	$(2,1),(2,4)$
3	1	± 1	$(3,1),(3,4)$
4	4	± 2	$(4,2),(4,3)$

Therefore, $E(\mathbb{F}_5) =< (0,1) >$ has order 9.

$y^2 = x^3 + 2$ over $\mathbb{F}_7$. Then
$E(\mathbb{F}_7) = \{O, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}$.
Every point satisfy $3P = O$, so $E(\mathbb{F}_7) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve. Then, for some $n_1|n_2$.

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve. Then, for some $n_1|n_2$.

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

Theorem

(Hasse) Let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve. Then, for some $n_1 | n_2$.

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z},$$

Theorem

(Hasse) Let $E/\mathbb{F}_q$ be an elliptic curve. Then

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Proof $E(\mathbb{F}_q) =$Ker$(\phi_q - 1)$ and $\phi_q - 1$ is separable, hence, $\#E(\mathbb{F}_q) = \deg(\phi_q - 1)$.

$r^2 q + s^2 - rsa = \deg(r\phi_q - s) \geq 0$, where $a = q + 1 - \#E(\mathbb{F}_q)$. Since this is true for any r, s, we get $qx^2 - ax + 1 \geq 0$ for any real x. The result follows.

Corollary

Let $E(\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then, $q = n^2 + 1$, $q = n^2 \pm n + 1$ or $q = (n \pm 1)^2$.

Proof Observe that $E[n] \subset E(\mathbb{F}_q)$, and so $\mu_n \in \mathbb{F}_q$. Hence, $n|q-1$, and so $n^2 = q + 1 - a$ gives $a = 2 + kn$ for some integer k. Hasse's Theorem gives now the result.

Theorem

Let $q = p^n$ and $N = q + 1 - a$ There exist an elliptic curve over $E/\mathbb{F}_q$ with $N = \#E(\mathbb{F}_q)$ if and only if $a \leq 2\sqrt{q}$ and

- *$p \nmid a$.*
- *n is even and $a = \pm 2\sqrt{q}$*
- *n is even, $p \not\equiv 1 \pmod 3$ and $a = \pm\sqrt{q}$.*
- *n is odd, $p = 2, 3$ and $a = \pm p^{(n+1)/2}$*
- *n is even, $p \not\equiv 1 \pmod 4$ and $a = 0$*
- *n is odd and $a = 0$.*

Theorem

Let the conditions of the above theorem and $N = p^e n_1 n_2$ with $n_1 | n_2$ and $p \nmid n_1 n_2$. There is an elliptic curve $E/\mathbb{F}_q$ such that

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/p^e\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$$

if and only if,

- $n_1 | q - 1$ *and we are not in the second case of the previous theorem,*
- $n_1 = n_2$ *in the second case of the previous theorem.*

Group order

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve and $a = q + 1 - \#E(\mathbb{F}_q)$. Then, a is the unique integer so that

$$\phi_q^2 - a\phi_q + q = 0.$$

Group order

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve and $a = q + 1 - \#E(\mathbb{F}_q)$. Then, a is the unique integer so that

$$\phi_q^2 - a\phi_q + q = 0.$$

Moreover, $a \equiv Trace((\phi_q)_m) \pmod{m}$ for any $(m, q) = 1$.

Group order

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve and $a = q + 1 - \#E(\mathbb{F}_q)$. Then, a is the unique integer so that

$$\phi_q^2 - a\phi_q + q = 0.$$

Moreover, $a \equiv Trace((\phi_q)_m) \pmod{m}$ for any $(m, q) = 1$.

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$ and $x^2 - ax + q = (x - \alpha)(x - \beta)$. Then

$$\#E(\mathbb{F}_{q^n}) = q + 1 - s_n$$

where $s_n = \alpha^n + \beta^n$.

Group order

Theorem

Let $E/\mathbb{F}_q$ be an elliptic curve and $a = q + 1 - \#E(\mathbb{F}_q)$. Then, a is the unique integer so that

$$\phi_q^2 - a\phi_q + q = 0.$$

Moreover, $a \equiv Trace((\phi_q)_m) \pmod{m}$ for any $(m, q) = 1$.

Theorem

Let $\#E(\mathbb{F}_q) = q + 1 - a$ and $x^2 - ax + q = (x - \alpha)(x - \beta)$. Then

$$\#E(\mathbb{F}_{q^n}) = q + 1 - s_n$$

where $s_n = \alpha^n + \beta^n$.

Lemma

s_n is an integer

Proof. $s_{n+1} = as_n - qs_{n-1}$.

Example.

Compute $E(\mathbb{F}_{2^{101}})$, where $E := y^2 + xy = x^3 + 1$.

$\#E(\mathbb{F}_2) = 4$. Therefore, $a = -1$, and we obtain

$$x^2 + x + 2 = \left(x - \frac{-1+\sqrt{-7}}{2}\right)\left(x - \frac{-1-\sqrt{-7}}{2}\right)$$

Using the recurrence for s_n or using sufficiently high precision floating point arithmetic yields
$\left(\frac{-1+\sqrt{-7}}{2}\right)^{101} + \left(\frac{-1-\sqrt{-7}}{2}\right)^{101} = 2969292210605269.$
Therefore, $\#E(\mathbb{F}_{2^{101}}) = 2^{101} + 1 - 2969292210605269 =$
$2535301200456455833701195805484.$

Definition

$E/\mathbb{F}_q$ is said to be **supersingular** *if* $E[p] = O$.

However, we have an alternative definition which is the one we are interested on now.

Proposition

$E/\mathbb{F}_q$ es supersingular if and only if $|E(\mathbb{F}_q)| \equiv 1 \pmod p$ *which is the same as* $a = q + 1 - |E(\mathbb{F}_q)| \equiv 0 \pmod p$.

Proof. Consequence of the previous theorem, the recurrence relation of s_n, and Fermat's Little Theorem.

Example

The curve $y^2 = x^3 - x$ is supersingular for any prime $p \equiv 3 \pmod 4$.

Example

The curve $y^2 = x^3 - x$ is supersingular for any prime $p \equiv 3 \pmod 4$.

If $E/\mathbb{Z}$ has CM by $Q(\sqrt{-d})$, $E \pmod p$ is supersingular if and only if $-d$ is not a square modulo p. Therefore E, is supersingular for approximately half of the primes. If E has not CM complex multiplication, the set of primes for which is supersingular is infinite but for $p < x$ is less than $Cx/In^{2-\varepsilon}(x)$. It has been conjectured by Lang and Trotter that the truth would be $C\sqrt{x}/\log x$. This has been shown to be true "on average" by Fouvry and Murty.

But In general, how do we find the order?

But In general, how do we find the order?Trying points at random.

But In general, how do we find the order?Trying points at random. Suppose $E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with $n_1|n_2$. What is the chance that the least common multiple of the orders of random points is n_2?
Let $\operatorname{ord} P_1 = n_1$, $\operatorname{ord} P_2 = n_2$, generators. If $P \in E(\mathbb{F}_q)$ then $P = a_1P_1 + a_2P_2$ with $0 \le a_i < n_i$. Let $p^e || n_2$.
$\mathrm{Prob}(p \nmid a_2) = 1 - 1/p$ hence, $p^e | \operatorname{ord} P$. If p is large, it is very likely If p is small, say $p = 2$, then the probability is at least $1/2$.

Proposition

Let $E/\mathbb{F}_q$ be an elliptic curve. Write $E(\mathbb{F}_q) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ with $n_1|n_2$. Suppose that q is not one of the following:

$$3, 4, 5, 7, 9, 11, 13, 17, 19, 23, 25, 27, 29,$$

$$31, 37, 43, 61, 73, 181, 331, 547.$$

Then n_2 uniquely determines n_1.

If we can find a point of order greater than $4\sqrt{q}$, there can be only one multiple of this order in the correct interval, and it must be $\#E(\mathbb{F}_q)$. Even if the order of the point is smaller than $4\sqrt{q}$, we obtain a small list of possibilities for $\#E(\mathbb{F}_q)$. Using a few more points often shortens the list enough that there is a unique possibility for $\#E(\mathbb{F}_q)$.

If we can find a point of order greater than $4\sqrt{q}$, there can be only one multiple of this order in the correct interval, and it must be $\#E(\mathbb{F}_q)$. Even if the order of the point is smaller than $4\sqrt{q}$, we obtain a small list of possibilities for $\#E(\mathbb{F}_q)$. Using a few more points often shortens the list enough that there is a unique possibility for $\#E(\mathbb{F}_q)$.

Examples

$y^2 = x^3 + 7x + 1$ over $\mathbb{F}_{101}$. $\mathrm{ord}(0,1) = 116$.

$$101 + 1 - 2\sqrt{101} \leq |E(\mathbb{F}_{101})| \leq 101 + 1 + 2\sqrt{101},$$

hence

$|E(\mathbb{F}_{101})| = 116$. The group is cyclic.

$y^2 = x^3 - 10x + 21$ over $\mathbb{F}_{557}$. ord $(2,3) = 189$ and $511 \leq |E(\mathbb{F}_{557})| \leq 605$. Therefore $|E(\mathbb{F}_{557})| = 567 = 3 \cdot 189$.

$y^2 = x^3 - 10x + 21$ over $\mathbb{F}_{557}$. ord $(2,3) = 189$ and $511 \leq |E(\mathbb{F}_{557})| \leq 605$. Therefore $|E(\mathbb{F}_{557})| = 567 = 3 \cdot 189$.

$y^2 = x^3 + 7x + 12$ over $\mathbb{F}_{103}$. $\text{ord}(-1,2) = 13$ $\text{ord}(19,0) = 2$. Therefore $|E(\mathbb{F}_{103})|$ is a multiple of 26. But $84 \leq |E(\mathbb{F}_{103})| \leq 124$. So $|E(\mathbb{F}_{103})| = 104$

How do we find the order of a point?

How do we find the order of a point?
Baby Step Giant Step Algorithm We choose an integer $m > \sqrt{2}q^{1/4}$. Then, since $|a| < 2\sqrt{q}$, we can express it on base m as $a = u + vm$ with $0 \leq u \leq m$, $-m \leq v < m$. Observe that, if a positive integer $a = u + vm$, then $-a = -u - vm = m - u - (v+1)m$.

- Baby Step. From $P_j = jP$ compute $(j+1)P$ for $j = 1$ up to $(m-1)P$.
- Giant Step. From $Q_k = (q + 1 + km)P$ compute $q + 1 + (k+1)mP$ for $k = -m + 1$ up to m.
- Factor $N = q + 1 - j + km$ and let $p_1, \ldots, p_r$ its prime factors.
- Compute N/p_iP if it is O repeat with $N = N/p_i$. Otherwise $N = \mathrm{ord}(P)$.

There will be a match $P_u = Q_{-v}$ and we have done $3m \sim 3\sqrt{2}q^{1/4}$ additions and two multiplitacions $(q+1)P$ and mP.

Example.

$y^2 = x^3 - 10x + 21$ over $\mathbb{F}_{557}$, $P = (2,3)$. We follow the procedure above.

- $Q = 558P = (418, 33)$.
- Let $m = 5 > 557^{1/4}$.
  $jP = \{O, (2,3), (58,164), (44,294), (56,339), (132,364)\}$.
- When $k = 2$, we have $Q + kmP = (2,3) = P$.
- We have $(q + 1 + mk - j)P = 567P = O$.
- Factor $567 = 3^4 7$. Compute $(567/3)P = 189P = O$. We now have 189 as a candidate for the order of P.
- Factor $189 = 3^3 7$. Compute $(189/3)P = (38, 535) \neq O$ and $(189/7)P = (136, 360) \neq O$. Therefore $\operatorname{ord} P = 189$.

Schoof algorithm is the best to obtain the group of points on an elliptic curve. It works in polynomial time in the number of digits of q. It is based on computing the numer of points modulo enough prime factors. Each of those calculations can be done using the characteristic polynomial of the Frobenius and the division polynomials.

Schoof algorithm is the best to obtain the group of points on an elliptic curve. It works in polynomial time in the number of digits of q. It is based on computing the numer of points modulo enough prime factors. Each of those calculations can be done using the characteristic polynomial of the Frobenius and the division polynomials.

Choose a set of primes $S = \{2, 3, 5, ..., L\}$ (with $p \notin S$) such that $\prod_{l \in S} l > 4\sqrt{q}$.

If $l = 2$, we have $a \equiv 0 \pmod 2$ if and only if $\gcd(x^3 + Ax + B, x^q - x) \neq 1$.

For each odd prime $l \in S$ do the following.

1. (a) Let $q_l \equiv q \pmod{l})$ with $|q_l| < l/2$.
   (b) Compute the x-coordinate x' of
   $(x', y') = ((x^{q^2}, y^{q^2}) + q_l)(x, y) \pmod{\psi_l}$
   (c) For $j = 1, 2, ..., (l-1)/2$, do the following.
   i. Compute the x-coordinate x_j of $(x_j, y_j) = j(x, y)$.
   ii. If $x' - x_j^q \equiv 0 \pmod{\psi_l}$, go to step (iii). If not, try the next value of j (in step (c)). If all values been tried, go to step (d).
   iii. Compute y' and y_j . If $(y' - y_j^q)/y \equiv 0 \pmod{\psi_l}$ then $a \equiv j \pmod{l}$. If not, then $a \equiv -j \pmod{l}$.
   (d) Let $w^2 \equiv q \pmod{l}$. Otherwise $a \equiv 0 \pmod{l}$
   (e) If $\gcd(\text{numerator}(x^q - x_w), \psi_l) = 1$, then $a \equiv 0 \pmod{l})$. Otherwise, if $\gcd(\text{numerator}((y^q - y_w)/y), \psi_l) \neq 1$, $a \equiv 2w \pmod{l}$. Otherwise, $a \equiv -2w \pmod{l}$.
2. Compute $a \pmod{\prod_{l \in S} l}$ and choose the value of a that satisfies $|a| < 2\sqrt{q}$. The number of points in $E(\mathbb{F}_q)$ is $q + 1 - a$.

Example

$y^2 = x^3 + 2x + 1 \pmod{19}$. We will show $a \equiv 1, 2, 3$ modulo $2, 3, 5$ respectively. Then $a \equiv 23 \pmod{30}$ and since $|a| < 2\sqrt{19} < 9$, $a = -7$.

Example

$y^2 = x^3 + 2x + 1 \pmod{19}$. We will show $a \equiv 1, 2, 3$ modulo $2, 3, 5$ respectively. Then $a \equiv 23 \pmod{30}$ and since $|a| < 2\sqrt{19} < 9$, $a = -7$.

$\bullet l = 2$. $\quad x^{19} - x \equiv x^2 + 13x + 14 \pmod{x^3 + 2x + 1}$. Hence $gcd(x^{19} - x, x^3 + 2x + 1) = 1$.

Example

$y^2 = x^3 + 2x + 1 \pmod{19}$. We will show $a \equiv 1, 2, 3$ modulo $2, 3, 5$ respectively. Then $a \equiv 23 \pmod{30}$ and since $|a| < 2\sqrt{19} < 9$, $a = -7$.
$\bullet l = 2$. $x^{19} - x \equiv x^2 + 13x + 14 \pmod{x^3 + 2x + 1}$. Hence $gcd(x^{19} - x, x^3 + 2x + 1) = 1$.

$\bullet l = 3$. $q_l = 1$. We compute the x coordinate of $(x^{361}, y^{361}) + (x, y)$ which is $\left(\frac{y^{361}-y}{x^{361}-x}\right)^2 - x^{361} - x$ modulo ψ_3.

We cannot make the inverse, since $\gcd(x^{361} - x, 3x^4 + 12x^2 + 12x - 4) = x - 8$.

But then $|E(\mathbb{F}_{19})| \equiv 0 \pmod{3}$ or $a \equiv 2 \pmod{3}$.

$\bullet l = 5, \quad q_l = -1$
We get $\left(\frac{y^{361}-y}{x^{361}-x}\right)^2 - x^{361} - x \equiv \left(\frac{3x^{38}+2}{2y^{19}}\right)^2 - 2x^{19} \pmod{\psi_5(x)}$.
Hence $a \equiv \pm 2 \pmod 5$.

The y coordinate, y' of $(x^{361}, y^{361}) + (x, -y)$ is
$y(9x^{11} + 13x^{10} + 15x^9 + 15x^7 + 18x^6 + 17x^5 + 8x^4 + 12x^3 + 8x + 6)$
$\pmod{\psi_5}$.
The y coordinate, y'', of $2(x, y)$ is
$y(13x^{10} + 15x^9 + 16x^8 + 13x^7 + 8x^6 + 6x^5 + 17x^4 + 18x^3 + 8x + 18)$
$\pmod{\psi_5}$
and so
$(y' + y''^{19})/y \equiv 0 \pmod{\psi_5}$. Hence $a \equiv -2 \pmod 5$.

Elliptic Curves III

J. Jiménez Urroz, UPC

Benin, July ,18, 2014

In order to build secure cryptosystems, we need to have behind a difficult mathematical problem. Breaking the cryptosystem would means solve the problem. One of them is the Discrete logarithm problem, DLP.

Problem. (DLP) Given a multiplicative group $G =< g >$ and $a \in G$ find the integer k, so that $g^k = a$.

In order to build secure cryptosystems, we need to have behind a difficult mathematical problem. Breaking the cryptosystem would means solve the problem. One of them is the Discrete logarithm problem, DLP.

Problem. (DLP) Given a multiplicative group $G =< g >$ and $a \in G$ find the integer k, so that $g^k = a$.

The integer k shares properties with the logarithm.

$g^{L(h)} \equiv h \pmod{p}$. Then,

$g^{L(h1h2)} \equiv h1h2 \equiv g^{L(h1)+L(h2)} \pmod{p}$, Hence

$$L(h1h2) \equiv L(h1) + L(h2) \pmod{p-1}.$$

In order to build secure cryptosystems, we need to have behind a difficult mathematical problem. Breaking the cryptosystem would means solve the problem. One of them is the Discrete logarithm problem, DLP.

Problem. (DLP) Given a multiplicative group $G =< g >$ and $a \in G$ find the integer k, so that $g^k = a$.

The integer k shares properties with the logarithm.

$g^{L(h)} \equiv h \pmod{p}$. Then,

$g^{L(h1h2)} \equiv h1h2 \equiv g^{L(h1)+L(h2)} \pmod{p}$, Hence

$$L(h1h2) \equiv L(h1) + L(h2) \pmod{p-1}.$$

It is believed that it cannot be found in polynomial time. Recently there are good algorithms for small characteristic

Index Calculus: $\mathbb{F}_p^*$

Solve the DLP for small primes and find $g^j a$ to be smooth. End with linear algebra.

Remark. A number is B-smooth, if all its prime factors are bounded by B.

$$\psi(X; X^{1/u})/X \sim u^{-u}$$

Index Calculus: $\mathbb{F}_p^*$

Solve the DLP for small primes and find $g^j a$ to be smooth. End with linear algebra.

Remark. A number is B-smooth, if all its prime factors are bounded by B.

$$\psi(X; X^{1/u})/X \sim u^{-u}$$

Example. Let $p = 1217$ and $g = 3$. Solve $3^k \equiv 37 \pmod{1217}$.

Index Calculus: $\mathbb{F}_p^*$

Solve the DLP for small primes and find $g^j a$ to be smooth. End with linear algebra.

Remark. A number is B-smooth, if all its prime factors are bounded by B.

$$\psi(X; X^{1/u})/X \sim u^{-u}$$

Example. Let $p = 1217$ and $g = 3$. Solve $3^k \equiv 37 \pmod{1217}$.

$$\begin{aligned}
3^{24} &\equiv -2^2 \cdot 7 \cdot 13 \pmod{1217} \\
3^{25} &\equiv 5^3 \\
3^{30} &\equiv -2 \cdot 5^2 \\
3^{54} &\equiv -5 \cdot 11 \\
3^{87} &\equiv 13 \\
3^{16} \cdot 37 &\equiv 2^3 \cdot 7 \cdot 11
\end{aligned}$$

$3^{(p-1)/2} = -1$, so $L(-1) = 608$.

$$\begin{aligned}
24 &\equiv 608 + 2L(2) + L(7) + L(13) \pmod{1216} \\
25 &\equiv 3L(5) \\
30 &\equiv 608 + L(2) + 2L(5) \\
54 &\equiv 608 + L(5) + L(11) \\
87 &\equiv L(13) \\
16 + L(37) &\equiv 3L(2) + L(7) + L(11)
\end{aligned}$$

$3^{(p-1)/2} = -1$, so $L(-1) = 608$.

$$\begin{aligned}
24 &\equiv 608 + 2L(2) + L(7) + L(13) \pmod{1216}\\
25 &\equiv 3L(5)\\
30 &\equiv 608 + L(2) + 2L(5)\\
54 &\equiv 608 + L(5) + L(11)\\
87 &\equiv L(13)\\
16 + L(37) &\equiv 3L(2) + L(7) + L(11)
\end{aligned}$$

$L(37) = 588$, hence $3^{588} \equiv 37 \pmod{1217}$.

$3^{(p-1)/2} = -1$, so $L(-1) = 608$.

$$\begin{aligned}
24 &\equiv 608 + 2L(2) + L(7) + L(13) \pmod{1216} \\
25 &\equiv 3L(5) \\
30 &\equiv 608 + L(2) + 2L(5) \\
54 &\equiv 608 + L(5) + L(11) \\
87 &\equiv L(13) \\
16 + L(37) &\equiv 3L(2) + L(7) + L(11)
\end{aligned}$$

$L(37) = 588$, hence $3^{588} \equiv 37 \pmod{1217}$.

The expected running time is $O(\exp(\sqrt{2 \log p \log \log p}))$

Pollard's ρ method

Any function $f(P_i) = P_{i+1}$ has a periodic orbit in a finite group. Hence, there is a match.

Pollard's ρ method

Any function $f(P_i) = P_{i+1}$ has a periodic orbit in a finite group. Hence, there is a match.

$|G| = N$. We want to find $kP = Q$.

1. Split G into s sets S_i and choose randomly $M_i = a_i P + b_i Q$
2. Choose random $P_0 = a_0 P + b_0 Q$
3. If $P_i \in S_j$, then $P_{i+1} = P_i + M_j$
4. The match $P_l = P_m$ gives $u_l P + v_l Q = u_m P + v_m Q$
5. $k \equiv (v_m - v_l)^{-1}(u_l - u_m) \pmod N$

Remark. If $(v_m - v_l, N) = d$ the equation gives d possible values of k.

Example

Let $G = E(\mathbb{F}_{1093})$, $E := y^2 = x^3 + x + 1$. $s = 3$.

$P = (0, 1)$, $Q = (413, 959)$. Find $kP = Q$. $\mathrm{ord}(P) = 1067$.

$P_0 = 3P + 5Q$, $M_0 = 4P + 3Q$, $M_1 = 9P + 17Q$, $M_2 = 19P + 6Q$.

$f(x, y) = (x, y) + M_i$ if $x \equiv i \pmod 3$.

$f(P_0) = P_0 + M_2 = (727, 589)$, since $P_0 = (326, 69)$ and $326 \equiv 2 \pmod 3$.

$P_5 = P_{58}$. $P_5 = 88P + 46Q$ and $P_{58} = 685P + 620Q$.

Therefore, $O = P_{58} - P_5 = 597P + 574Q$.

$k \equiv (-574)^{-1} 597 \equiv 499 \pmod{1067}$.

MOV Attack

Reduce the DLP on the elliptic curve, to DLP on a finite field via the Weil pairing.

MOV Attack

Reduce the DLP on the elliptic curve, to DLP on a finite field via the Weil pairing.

Lemma

Let $E/\mathbb{F}_q$ and $ordP = N$ coprime with q. $Q \in E(\mathbb{F}_q)$. There exists k such that $Q = kP$ if and only if $NQ = O$ and the Weil paring $e_N(P, Q) = 1$.

One direction is trivial. For the other, take $\hat{P}$ so that $P, \hat{P}$ is a base of the N torsion. Recall that, since $(q, N) = 1$, $E[N] \simeq \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Then, $Q = aP + b\hat{P}$ for some integers a, b, and $1 = e_N(P, Q) = e_N(P, P)^a e_N(P, \hat{P})^b = \zeta^b$ for ζ some primitive N-th root of unity. In particular $N|b$ which finish the result.

1. Choose a random point $T \in E(F_{q^m})$.
2. Compute the order M of T.
3. Let $d = \gcd(M, N)$, and let $T_1 = (M/d)T$. Then T_1 has order d, which divides N, so $T_1 \in E[N]$.
4. Compute $\zeta_1 = e_N(P, T_1)$ and $\zeta_2 = e_N(Q, T_1)$. Then both ζ_1 and ζ_2 are in $\mu_d \subset \mathbb{F}^*_{q^m}$.
5. Solve the discrete log problem $\zeta_2 = \zeta_1^k$ in $\mathbb{F}^*_{q^m}$. This will give k modulo d.
6. Repeat with random points T until the least common multiple of the various d's obtained is N. This determines k modulo N.

Remark. With high probability d is big.

Remark. With high probability d is big.

Remark. We require $E[N] \in \mathbb{F}_{q^m}$ then $\mu_d \in \mathbb{F}_{q^m}$.

Remark. With high probability d is big.

Remark. We require $E[N] \in \mathbb{F}_{q^m}$ then $\mu_d \in \mathbb{F}_{q^m}$.

Proposition

Let E be an elliptic curve over $\mathbb{F}_q$ and suppose $a = q + 1 - \#E(\mathbb{F}_q) = 0$. Let N be a positive integer. If there exists a point P of $E(\mathbb{F}_q)$ of order N, then $E[N] \subset E(\mathbb{F}_{q^2})$.

Proof. The Frobenius endomorphism satisfies $\varphi_q^2 = -q$. Since there is a point of order N, we have $N|q+1$. Suposse now $S \in E[N]$. Then $S = -qS = \varphi_{q^2} S$ as we wanted to see.

Remark. With high probability d is big.

Remark. We require $E[N] \in \mathbb{F}_{q^m}$ then $\mu_d \in \mathbb{F}_{q^m}$.

Proposition

Let E be an elliptic curve over $\mathbb{F}_q$ and suppose $a = q + 1 - \#E(\mathbb{F}_q) = 0$. Let N be a positive integer. If there exists a point P of $E(\mathbb{F}_q)$ of order N, then $E[N] \subset E(\mathbb{F}_{q^2})$.

Proof. The Frobenius endomorphism satisfies $\varphi_q^2 = -q$. Since there is a point of order N, we have $N|q+1$. Suposse now $S \in E[N]$. Then $S = -qS = \varphi_{q^2} S$ as we wanted to see.

Remark. When E is supersingular but $a \neq 0$, $m = 3, 4$, or 6.

Elliptic curve Cryptography

Alice wants to send a message, often called the plaintext, to Bob. In order to keep the eavesdropper Eve from reading the message, she encrypts it to obtain the ciphertext. When Bob receives the ciphertext, he decrypts it and reads the message. In order to encrypt the message, Alice uses an **encryption key**. Bob uses a **decryption key** to decrypt the ciphertext. Clearly, the decryption key must be kept secret from Eve.

Elliptic curve Cryptography

Alice wants to send a message, often called the plaintext, to Bob. In order to keep the eavesdropper Eve from reading the message, she encrypts it to obtain the ciphertext. When Bob receives the ciphertext, he decrypts it and reads the message. In order to encrypt the message, Alice uses an **encryption key**. Bob uses a **decryption key** to decrypt the ciphertext. Clearly, the decryption key must be kept secret from Eve.

symmetric encryption, the encryption key and decryption key are the same, (DES)

public key encryption, or asymmetric encryption. Bob publishes a public encryption key, which Alice uses. He also has a private decryption key that allows him to decrypt ciphertexts. Since everyone knows the encryption key, it should be infeasible to deduce the decryption key from the encryption key. RSA

Generally, public key systems are slower than good symmetric systems.

Generally, public key systems are slower than good symmetric systems.

Diffie-Hellman key exchange

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete logarithm problem is hard in $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$ such that the subgroup generated by P has large prime.
2. Alice chooses a secret integer a, computes $P_a = aP$, and sends it to Bob.
3. Bob chooses a secret integer b, computes $P_b = bP$, and sends it to Alice.
4. Alice computes $aP_b = abP$.
5. Bob computes $bP_a = baP$.

The public information is E, q, P, P_a, P_b. From here to compute abP would be enough to solve the DLP on the elliptic curve E. It is not know if one can compute abP without solving DLP.

Decision Diffie-Hellman problem Given P, aP, and bP in $E(\mathbb{F}_q)$, and given a point $Q \in E(\mathbb{F}_q)$ determine whether or not $Q = abP$.

In other words, it is believed that P, aP, and bP do not lick a single bit of information about abP.

DDH problem can be asked in any group. In the case of elliptic curves, it is subtle since, in some cases, one could use the Weil pairing to solve the problem, as we did to solve the DLP.

Example Consider the curve $y^2 = x^3 + 1$ and $q \equiv 2 \pmod 3$. Then, $E(\mathbb{F}_q) = q + 1$.

$\beta(x, y) = (\omega x, y)$ where $\omega \notin \mathbb{F}_q$ is a third root of unity.

$$\tilde{e}_n(P_1, P_2) = e_n(P_1, \beta(P_2)),$$

Lemma

Assume $3 \nmid n$. If $P \in E(\mathbb{F}_q)$ has order exactly n, then $\tilde{e}_n(P, P)$ is a primitive n-th root of unity.

Proof. We see that it is impossible to have a relation between P and $\beta(P)$ unless $x = 0$, but the point $P = (0, \pm 1)$ has order $3|n$. Hence, they are independent, and hence the Weil pairing is a primitive root. $(\psi_3 = 3x^4 + 6AX^2 + 12Bx - A^2)$

Assume now that $Q = tP$. (one can check this) . Then $Q = abP$ if and only if $ab \equiv t \pmod n$. This is equivalent to $\tilde{e}_n(Q, P) = \tilde{e}_n(aP, bP)$, when $3 \nmid n$, by the previous lemma.

A Public Key Scheme Based on Factoring

$n = pq$, $ed \equiv 1 \pmod{\varphi(n)}$ n, e public, d, p, q secret. $c = m^e \pmod{n}$.

A Public Key Scheme Based on Factoring

$n = pq$, $ed \equiv 1 \pmod{\varphi(n)}$ n, e public, d, p, q secret. $c = m^e \pmod{n}$.
If Eve finds d, then finds $\varphi(n) = (p-1)(q-1) = n + 1 - (p+q)$ from here and $n = pq$, she can factor n.

A Public Key Scheme Based on Factoring

$n = pq$, $ed \equiv 1 \pmod{\varphi(n)}$ n, e public, d, p, q secret. $c = m^e \pmod{n}$.
If Eve finds d, then finds $\varphi(n) = (p-1)(q-1) = n + 1 - (p+q)$ from here and $n = pq$, she can factor n.

1. Bob chooses two distinct large primes p, q with $p \equiv q \equiv 2 \pmod{3}$ and computes $n = pq$.
2. Bob chooses integers e, d with $ed \equiv 1 \pmod{lcm(p+1, q+1)}$.
3. Bob makes n and e public and keeps d, p, q private.
4. Alice represents her message as a pair of integers $(m_1, m_2) \pmod{n}$. She regards (m_1, m_2) as a point M on the elliptic curve E given by $y^2 = x^3 + b \pmod{n}$, where $b = m_2^2 - m_1^3 \pmod{n}$ (she does not need to compute b).
5. Alice adds M to itself e times on E to obtain $C = (c1, c2) = eM$. She sends C to Bob.
6. Bob computes $M = dC$ on E to obtain M.

Remarks. The order of $E(\mathbb{Z}_n)$ is $|E(\mathbb{F}_p)||E(\mathbb{F}_q)| = (p+1)(q+1)$. Therefore, $(p+1)M \equiv O \pmod{p}$ and $(q+1)M \equiv O \pmod{q}$ This means that the decryption works.

Remarks. The order of $E(\mathbb{Z}_n)$ is $|E(\mathbb{F}_p)||E(\mathbb{F}_q)| = (p+1)(q+1)$. Therefore, $(p+1)M \equiv O \pmod{p}$ and $(q+1)M \equiv O \pmod{q}$ This means that the decryption works.

If Alice first chooses the x-coordinate as the message, then she is faced with the problem of computing square roots mod n. This is computationally equivalent to factoring n.

Remarks. The order of $E(\mathbb{Z}_n)$ is $|E(\mathbb{F}_p)||E(\mathbb{F}_q)| = (p+1)(q+1)$. Therefore, $(p+1)M \equiv O \pmod{p}$ and $(q+1)M \equiv O \pmod{q}$ This means that the decryption works.

If Alice first chooses the x-coordinate as the message, then she is faced with the problem of computing square roots mod n. This is computationally equivalent to factoring n.

If Eve factors n as pq, she can decrypt Alice's message. The opposite is also true with high probability.

1. Write $ed - 1 = 2^k v$ with v odd and with $k \geq 1$.
2. Pick a random pair of integers $R = (r_1, r_2) \pmod{n}$, and let $b' = r_2^2 - r_1^3$ and regards R as a point on the elliptic curve E' given by $y^2 = x^3 + b'$.
3. Compute $R_0 = vR$. If $R_0 = O \pmod{n}$, start over with a new R. On the other hand if $R_0 = O \mod p$ only, then Eve has factored n.
4. For $i = 0, 1, 2, ..., k$, computes $R_{i+1} = 2R_i$. If $R_{i+1} \equiv O \pmod{p}$ only or some i, then $R_i = (x_i, y_i)$ with $y_i \equiv 0 \pmod{p}$ and $\gcd(y_i, n) = p$.
5. If for some i, $R_{i+1} = O \pmod{n}$, then start over with a new random point.

Factoring Using Elliptic Curves

$p-1$ **method.** Choose random a. Compute $a_1 = a^{B!} \pmod{n}$ and $\gcd(a_1 - 1, n)$.

If $p-1$ is B-smooth, then $p|(a_1 - 1)$. If $l|(q-1)$ then there is $1/l$ chance that $q|(a_1 - 1)$ and we factor n with high probability.

If $p-1$ and $q-1$ have very large prime factors there is no way to succeed.

The elliptic curve method have the freedom of choosing another curve. Can factor numbers of about 60 digits.

The elliptic curve method have the freedom of choosing another curve. Can factor numbers of about 60 digits.

1. Choose several random elliptic curves $E_i : y^2 = x^3 + A_i x + B_i$ (usually around 10 to 20) and points $P_i \pmod{n}$.
2. Choose an integer B (perhaps around 108) and compute $(B!)P_i$ on E_i for each i.
3. If step 2 fails because some slope does not exist mod n, then we have found a factor of n.
4. If step 2 succeeds, increase B or choose new random curves E_i and points P_i and start over.

Factor 4453. Consider $y^2 = x^3 + 10x - 2 \pmod{4453}$ and $P = (1, 3)$. We try to compute $3P$.

Factor 4453. Consider $y^2 = x^3 + 10x - 2 \pmod{4453}$ and $P = (1, 3)$. We try to compute $3P$.
Compute $2P$.

$$m = \frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

$$2P = (4332, 3230).$$

Factor 4453. Consider $y^2 = x^3 + 10x - 2 \pmod{4453}$ and $P = (1, 3)$. We try to compute $3P$.
Compute $2P$.

$$m = \frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

$$2P = (4332, 3230).$$

Compute $3P$.

$$m = \frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

$\gcd(4331, 4453) = 61$, hence $4453 = 61 \cdot 73$.

Factor 4453. Consider $y^2 = x^3 + 10x - 2 \pmod{4453}$ and $P = (1, 3)$. We try to compute $3P$.
Compute $2P$.

$$m = \frac{3x^2 + 10}{2y} = \frac{13}{6} \equiv 3713 \pmod{4453}.$$

$$2P = (4332, 3230).$$

Compute $3P$.

$$m = \frac{3230 - 3}{4332 - 1} = \frac{3227}{4331}.$$

$\gcd(4331, 4453) = 61$, hence $4453 = 61 \cdot 73$.

$$E(Z_{4453}) \simeq E(\mathbb{F}_{61}) \times E(\mathbb{F}_{73}).$$

$$P = (1, 3), 2P = (1, 58), 3P = O, 4P = (1, 3), \ldots \pmod{61}.$$

However,

$$P = (1, 3), 2P = (25, 18), 3P = (28, 44), \ldots, 64P = O \pmod{73}.$$

Primality Testing

Theorem

Let $n > 1$ and let E be an elliptic curve modulo n. Suppose there exist distinct prime numbers $l_1, \ldots, l_k$ and finite points $P_i \in E(\mathbb{Z}/n\mathbb{Z})$ such that

$$l_i P_i = O \text{ for } 1 \leq i \leq k,$$

$$\prod_{i=1}^{k} l_i \geq (n^{1/4} + 1)^2.$$

Then n is prime.

Proof.

Since $l_i P_i = O \pmod{n}$, $l_i P_i = O \pmod{p}$ for any $p|n$. Hence, $l_i | E(\mathbb{F}_p)$ for $1 \leq i \leq k$. Hence, by Hasse's Theorem, for any prime $p|n$ we have

$$(n^{1/4} + 1)^2 \leq \prod_{i=1}^{k} l_i \leq |E(\mathbb{F}_p)| < (\sqrt{p} + 1)^2.$$

Hence, $p \geq \sqrt{n}$ for any prime $p|n$ and, in particular, n is prime.

Example Let $n = 907$. $y^2 = x^3 + 10x - 2 \pmod{n}$. Let $l = 71 > (907^{1/4} + 1)^2$.
$P = (819, 784)$ has $71P = O$. Hence, 907 is prime.

Example Let $n = 907$. $y^2 = x^3 + 10x - 2 \pmod{n}$. Let $l = 71 > (907^{1/4} + 1)^2$.
$P = (819, 784)$ has $71P = O$. Hence, 907 is prime.

How to find the curve E and the point P?

Example Let $n = 907$. $y^2 = x^3 + 10x - 2 \pmod{n}$. Let $l = 71 > (907^{1/4} + 1)^2$.
$P = (819, 784)$ has $71P = O$. Hence, 907 is prime.

How to find the curve E and the point P?

For that, we need to learn the theory of complex multiplication, in the next CIMPA school.

See you there!!!