damien.robert@inria.fr

Elliptic Curves

I) Introduction:

Let K be a field. An elliptic curve E/K is the projective curve in the projective plane $\mathbb{P}^2_K$ associated to the affine (short) Weierstrass equation: $E/K : y^2 = x^3 + ax + b$
by adding the "point at infinity", $O_E : (0:1:0)$

Then $E(K)$ has a group law given by algebra/geometric equations
$n \in \mathbb{Z}, P \in E(K) \longrightarrow n.P$ exponentiation
$P, nP \longrightarrow n$ Discrete log problem : DLP

If $K = \mathbb{F}_q$, the finite field with q elements, then $E(K)$ is a finite group
If E is well chosen, DLP is hard, while exponentiation is "easy".
$\Rightarrow$ Public Key Cryptography

Part 2: Pairings:

If $E/\mathbb{F}_q$ is an elliptic curve, the Weil and Tate pairing give bilinear non degenerate applications: $E[l] \times E[l] \to \mu_l \subset \mathbb{F}_{q^d}^*$
$\to$ Lots of cryptographic applications

II) Finite fields:

1) Euclidian ring:

If A is an euclidian ring then A is a principal domain, and if $f \in A, f \neq 0$ then $\Leftrightarrow$ - f is irreducible
- (f) is prime
- (f) is maximal
- $A/(f)$ is a field

Example 1: $\mathbb{Z}$ is euclidian so $\mathbb{Z}/n\mathbb{Z}$ is a field $\Leftrightarrow$ $n = p$ is a prime
$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ the field with p elements

Example 2: If k is a field, $k[x]$ the ring of polynomials is euclidian. So $k[x]/f[x]$ is a field $\Leftrightarrow$ f is irreducible.
And if $\deg f = n$, then $k[x]/f[x]$ is also a vector space over k of dimension n

Corollary: $k = \mathbb{F}_p$, if $f(x) \in \mathbb{F}_p[x]$ is irreducible of degree n, then $\mathbb{F}_p[x]/f(x)$ is a field, which is also a vector space of dimension n over $\mathbb{F}_p$, so has p^n elements. $\boxed{\mathbb{F}_{p^n} = \mathbb{F}_p[x]/f(x)}$

Arithmetic operations: If $\alpha, \beta \in \mathbb{F}_{p^n} = \mathbb{F}_p[x]/f(x)$
Represent α as $P \bmod f$ and β as $Q \bmod f$ then
$\alpha + \beta = P + Q \bmod f$, $\alpha \times \beta = P \times Q \bmod f$

How to compute $1/\alpha$ if $\alpha \neq 0$? Extended euclidian algorithm / Bézout
since f is prime, it is prime with P
$uf + vP = 1$, $\boxed{1/\alpha = v \bmod f}$

2) Abstract view of finite fields:

Theorem: If $\mathbb{F}_q$ is a field with q elements.
Then 1) $q = p^n$, where p is the characteristic and n is the dimension vector space over $\mathbb{F}_p$
2) $\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_q / x^q = x\}$

If Π_q is the Frobenius, $\Pi_q\{x\} = x^q$; $\mathbb{F}_q = \{x \in \overline{\mathbb{F}}_p / \Pi_q(x) = x\}$

Proposition: 1) $\mathbb{F}_{q_1} \subset \mathbb{F}_{q_2} \iff q_1 = p^{n_1}$, $q_2 = p^{n_2}$, and n_1 / n_2 in which case, $\mathbb{F}_{q_1} = \{x \in \mathbb{F}_{q_2} / \Pi_{q_1}(x) = x\}$

2) There always exists an irreducible polynomial f of degree $d = n/n_1$ over $\mathbb{F}_{q_1}$, so $\mathbb{F}_{q_2} \cong \mathbb{F}_{q_1}[x]/f(x)$

3) The structure of $\mathbb{F}_q^*$:

Remark: $(\mathbb{F}_q, +)$ is a vector space of dimension n over $\mathbb{F}_p$, so $(\mathbb{F}_q, +) \cong (\mathbb{F}_p^n, +)$
Proof $f = \sum_{i=0}^{n-1} a_i x^i \longrightarrow (a_0, \dots, a_{n-1})$

Theorem: $(\mathbb{F}_q^*, \times)$ is a cyclic group so is isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$
If $\alpha \in \mathbb{F}_q^*$ generates it as a multiplicative group, α is called a primitive element $\iff$ α has multiplicative order $q-1$

Corollary: If α is primitive, its minimal polynomial is of degree n, $\mathbb{F}_q \cong \mathbb{F}_p[\alpha]$

4) Squares in $\mathbb{F}_q^*$ ($q \neq 2$)

Recall that an elliptic curve has equation $y^2 = x^3 + ax + b$

Proposition: Since $\mathbb{F}_q^*$ is cyclic, there are exactly $\frac{q-1}{2}$ squares, $x \in \mathbb{F}_q^*$ is a square $\Leftrightarrow x^{\frac{q-1}{2}} = 1$

Remark: If $q = p$ and $x \in \mathbb{F}_p^*$

$x^{\frac{p-1}{2}} \begin{cases} \equiv 1 \bmod p & \text{if } x \text{ is a square} \\ \equiv -1 \bmod p & \text{if } x \text{ is not a square} \end{cases}$

$\left(\frac{x}{p}\right)$ the Legendre / Jacobi symbol

III) Exponentiation:

- $E/\mathbb{F}_q$ an elliptic curve, $P \in E(\mathbb{F}_q)$ ($P = (x_P, y_P)$, $x_P, y_P \in \mathbb{F}_q$ and $y_P^2 = x_P^3 + ax_P + b$ or $P = O_E$ the point at infinity)

Exponentiation: nP

For crypto: n has $\simeq 256$ bits

- $x \in \mathbb{F}_q^*$, this is also a group exponentiation: x^n

Naive method: $nP = \underbrace{P + P + \dots + P}_{n-1 \text{ additions}}$

$\Rightarrow$ Requires $\simeq 2^{256}$ additions (longer than time of universe)

Other method: Right to left method:

1) Write n in base 2: $n = b_r \dots b_0$, $n = \sum_{i=0}^{r} b_i \times 2^i$
2) Compute $P, 2P, 4P, \dots, 2^r P$
3) Compute $nP = \sum b_i \times 2^i P$

Total: $O(\log n)$ operations

Crypto: 256 operations

Left to Right method: $57P$: $57 = 111001_2$

$1P = P$ $11P = 3P = 2P + P$

$111P = 7P = 2(3P) + P$ $1110 = 14P = 2(7P)$ $11100P = 28P = 2(14)P$

$111001P = 57P = 2(28)P + P$

Algorithm: Each time we move to the right

1) Double the current point
2) Add P if the new bit is 1

Left to the right with a window:

Example with a window of size 2:

$11\,10\,01_2$ Precomputations: $00 \cdot P = O$ $01 \cdot P = P$ $10P = 2P$ $11P = 3P$

$11P = 3P$ $11\,10P = 14 = 4(3P) + 2P$ $11\,10\,01 = 57P = 4(14)P + P$

Sliding window method: Standard window of size 3: as size 2 but with 3

Sliding window: Slide to the right until there is a one at the leftmost part

$110\,001\,100\,111$ Precomputation: 100 101 110 111

6P Double x5 Add 111 Double x5 Add 111

Elliptic curves 2

I) Curves and projective plane:

1) Plane affine curves:

$\mathcal{C}/k$: curve in affine plane $\mathbb{A}^2_k$ is given by an equation : $f(x,y) = 0$ where $f(x,y) \in k[x,y]$.
$\mathcal{C}$ is irreductible / reduced when f is irreduced / reduced in $k[x,y]$
When $k \subset k'$, the k'-points of $\mathcal{C}$ $\mathcal{C}(k') = \{x,y \in k' \mid f(x,y) = 0\}$

Remark : $\mathcal{C}$ is determined by $\mathcal{C}(\bar{k})$ when $\mathcal{C}$ is reduced.

Example : $\mathcal{C}/\mathbb{R}$, $x^2 + y^2 + 1 = 0$, $\mathcal{C}(\mathbb{R}) = \emptyset$. So $\mathcal{C}$ is only determined by $\mathcal{C}(k)$.

2) Tangents:

Let $P \in \mathcal{C}(k)$, $P = (x_P, y_P)$. $\mathcal{C}$ is smooth at P if $\left(\frac{\partial f}{\partial x}(x_P, y_P), \frac{\partial f}{\partial y}(x_P, y_P)\right) \neq (0,0)$.

The equation of the tangent line $T_P \mathcal{C}$ is $\frac{\partial f}{\partial x}(x_P, y_P)(x - x_P) + \frac{\partial f}{\partial y}(x_P, y_P)(y - y_P) = 0$.

Definition: $\mathcal{C}$ is smooth if it is smooth at every point $P \in \mathcal{C}(\bar{k})$

Example $y^2+x^2+1=0$ is smooth, $y^2-x^3=0$ is not smooth at $(0,0)$

3) Elliptic curves:

Definition: An elliptic curve E/k, is the projective curve associated to an affine smooth plane curve given by a long Weierstrass equation:

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$$

Remark: If $\mathrm{char}\, k>3$ and $\Delta=0$, there always exists a linear change of variable such that E is isomorphic to a curve given by a short Weierstrass equation: $y^2=x^3+ax+b$

II) Projective curves:

1) Projective line: $\mathbb{P}^1_k$

Coordinates of $\mathbb{A}^1_k = x$.

Coordinates of $\mathbb{P}^1_k = (x:y)$ where $(x,y)\neq(0,0)$ and $(x:y)$ is the equivalence class of $(x_1,y_1)\sim(x_2,y_2)$ if there exists $k\in k^*$ such that $x_2=kx_1$, $y_2=ky_1$.

$$\mathbb{P}^1_k=(\mathbb{A}^2_k\setminus\{(0,0)\})/k^*$$

1) $\mathbb{P}^1_k \simeq$ the set of lines in $\mathbb{A}^2_k$ going through $(0,0)$

2) Define $i_1:\mathbb{A}^1_k\longrightarrow\mathbb{P}^1_k$ by $x\longrightarrow(x:1)$ this is an inclusion.

- If $(x:3)\in\mathbb{P}^1_k$, and $xy\neq0$, then $(x:y)=(\frac{x}{y}:1)$ so is in $i_1(\mathbb{A}_1)$
- If $y=0$, then $x\neq0$, so $(x:xy)=(1:0)=\infty$

$$\mathbb{P}^1_k=i_1(\mathbb{A}^1_k)\cup\{\infty\}$$

3) $i : \mathbb{A}^1_k \to \mathbb{P}^1_k$ by $x \to (1:x)$
$\mathbb{P}^1_k = \mathbb{A}^1 \cup \mathbb{A}^0$ glued through $x \leftrightarrow 1/x$ when $x \neq 0$

2) Projective plane $\mathbb{P}^2_k$:

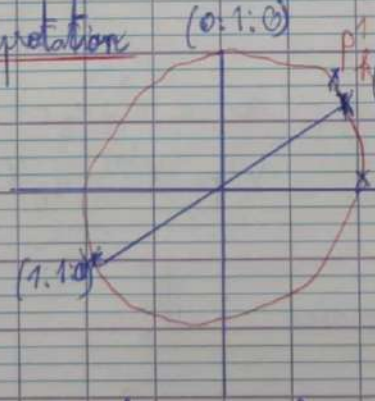
$\mathbb{A}^2_k$: coordinates (x, y)
$\mathbb{P}^2_k$: coordinates $(x:y:z)$ where $(x,y,z) \neq (0,0,0)$ and $(x:y:z)$ is the equivalence class under $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$ if $\exists k \in k^*$ / $x_2 = k x_1$, $y_2 = k y_1$, $z_2 = k z_1$

$\mathbb{P}^2_k = (\mathbb{A}^3_k \setminus (0,0,0)) / k^* =$ set of lines of $\mathbb{A}^3_k$ going through the origin.

Define $i : \mathbb{A}^2_k \hookrightarrow \mathbb{P}^2_k$ by $(x, y) \to (x:y:1)$
If $(x:y:z) \in \mathbb{P}^2_k$ and
- $z \neq 0$, $(x:y:z) = (\frac{x}{z} : \frac{y}{z} : 1)$ is in the image $i(\mathbb{A}^2_k)$
- $z = 0$, $(x:y:z) = (x:y:0)$

$\mathbb{P}^2_k = i(\mathbb{A}^2_k) \cup \mathbb{P}^1_k \simeq \mathbb{A}^2_k \cup \mathbb{A}^1_k \cup \mathbb{A}^0_k$

Geometric interpretation



* Change of variable: The projective plane around $P = (X:Y:Z)$ can be described using coordinates
- $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ when $Z \neq 0$
- $u = \frac{X}{Z}$, $v = \frac{Z}{Y}$ when $Y \neq 0$
- $p = \frac{Y}{X}$, $k = \frac{Z}{X}$ when $X \neq 0$

For instance: $u = \frac{x}{y}$, $v = \frac{1}{y}$

3) Projective curves:

A projective curve $\mathcal{C} \subset \mathbb{P}^2_k$ is a curve given by an equation $F(X,Y,Z) = 0$ where $F \in k[X,Y,Z]$ is a homogeneous polynomial (of degree d)
$F(X,Y,Z) = aX^d + bX^{d-1}Y + cX^{d-2}YZ + \dots$ all terms are of total degree d

$F(kX, kY, kZ) = k^d F(X,Y,Z)$ so "$F(X:Y:Z) = 0$" does not depend on the equivalence class of $(X:Y:Z)$

* If $\mathcal{C} \subset \mathbb{P}^2_k$ is a projective curve $F(X,Y,Z) = 0$ then $\mathcal{C} \cap i(\mathbb{A}^2_k)$ is an affine curve $f(x,y) = 0$ where $f(x,y) = F(x,y,1)$

* Conversely: if $\mathcal{C} \subset \mathbb{A}^2_k$ is the affine curve we associate to it the projective curve $\bar{\mathcal{C}} \subset \mathbb{P}^2_k$ the projective closure of $i(\mathcal{C})$ in $\mathbb{P}^2_k$ by

ie F is the homogenisation of f

Example: $E: y^2 = x^3 + ax + b$
$\bar{E}: Y^2Z = X^3 + aXZ^2 + bZ^3$

- $E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
$\bar{E}: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$

4) Elliptic curves in $\mathbb{P}^2_k$:

$E: y^2 = x^3 + ax + b$
$\bar{E}: Y^2Z = X^3 + aXZ^2 + bZ^3$

Pt $\bar{E}(\bar{k})$: $(X:Y:Z) \in \bar{E}(\bar{k})$

$Z \neq 0$, $(X:Y:Z) = \left(\frac{X}{Z}, \frac{Y}{Z}, 1\right) = (x, y, 1)$

$P \in E(k)$

$Z = 0 \Rightarrow Y^3 = 0 \Rightarrow Y = 0$

$P_\infty (0:1:0)$

$\overline{E}(k)$ only has one point "at infinity", $O_E = (0:1:0)$

$\mathbb{P}^2_k = \mathbb{A}^2_k \cup \mathbb{P}^1_k$ « At infinity, $y^2 = x^3$, $y = x^{\frac{3}{2}}$ »

$\overline{E} \quad E \quad \{O_E\}$

5) Lines in $\mathbb{P}^2_k$

$L : ax + by + c = 0$

$\overline{L} : aX + bY + cZ = 0$

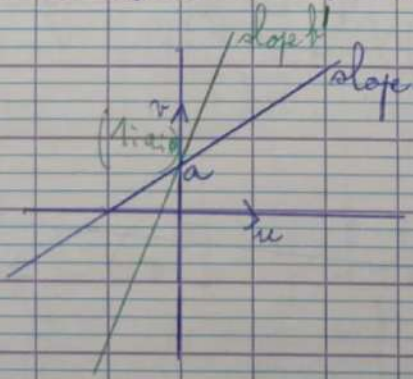
* $y = ax + b$

$Y = aX + bZ$

At infinity, $Z = 0$, $Y = aX$, one point $(1:a:0)$.

Change of variable : $v = \frac{Y}{X}$, $u = \frac{Z}{X}$

The equation becomes $v = a + bu$

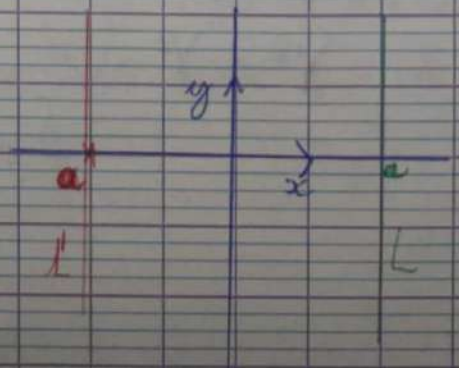


* $L : x = a$

$\overline{L} : X = aZ$

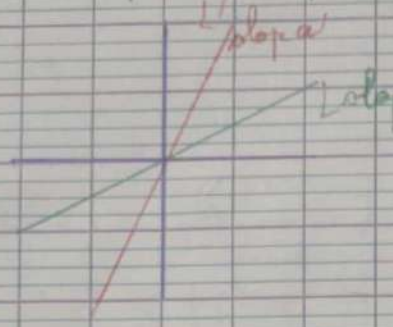
At infinity $Z = 0 \Rightarrow X = 0$

one point $(0:1:0)$

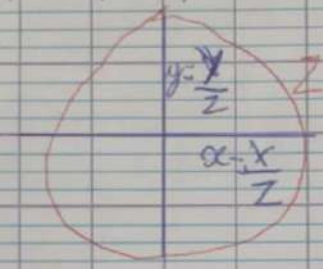


Change of variable:

$v = \frac{X}{Y}$, $u = \frac{Z}{Y}$ $\quad v = au$



* $Z = 0$ is the line at infinity



6) Tangents to projective curves

Let $\mathcal{C}/k \subset \mathbb{P}^2_k$ be the projective curve $F(X,Y,Z) = 0$.

Then $\mathcal{C}$ is smooth at P if $\left(\frac{\delta F}{\delta X}(P), \frac{\delta F}{\delta Y}(P), \frac{\delta F}{\delta Z}(P)\right) \neq (0,0,0)$

The equation of the tangent $T_P\mathcal{C}$ is given by

$$\frac{\delta F}{\delta X}(P)\,X + \frac{\delta F}{\delta Y}(P)\,Y + \frac{\delta F}{\delta Z}(P)\,Z = 0$$

Example: $E: y^2 = x^3 + ax + b$ $\quad \bar{E}: Y^2Z = X^3 + aXZ^2 + bZ^2$

$O_E = (0:1:0)$

Is $\bar{E}$ smooth at O_E?

$F(X,Y,Z) = Y^2Z - X^3 - aXZ^2 - bZ^2$

$\frac{\delta F}{\delta X}(0,1,0) = 0$ $\quad \frac{\delta F}{\delta Y}(0,1,0) = 0$ $\quad \frac{\delta F}{\delta Z}(0,1,0) = Y^2(0,1,0) = 1$

Corollary: $\bar{E}$ is always smooth at O_E, and the tagent line is $Z=0$

Corollary: $\bar{E}$ is smooth $\Leftrightarrow$ it is smooth at all points $P \in \bar{E}(\bar{k}) \Leftrightarrow E$ is smooth

Prop'ty: E is always smooth at O_E

E is not smooth at $P \Leftrightarrow$ 1) $P \in E(\bar{k}) \Rightarrow y_P^2 = x_P^3 + a_2 x_P + b = 0$
2) $y_P = 0$: dérivée en y
3) $3x_P^2 + a = 0$: dérivée en x

Write $h(x) = x^3 + ax + b$, $E: y^2 = h(x)$

1) $y_P = 0$
2) $h(x_P) = 0$ $\Big\} \Leftrightarrow x_P$ is a multiple root of $h(x)$ in $\bar{k}$
3) $h'(x_P) = 0$

Conclusion: E is not smooth $\Leftrightarrow h$ has multiple root in $\bar{k} \Leftrightarrow$ discrimant $= 0$ in k
Discriminant $h = 4a^3 + 27b^2$

Definition: discriminant $E = -16(4a^3 + 27b^2)$ written Δ_E

Theorem: E is smooth $\Leftrightarrow \Delta_E \neq 0$ in k
Note: the theorem is valid in any characteristic

Remark: Δ_E is also defined for a long Weierstrass equation, and the theorem is still true, but the expression of Δ_E is more complicated.

Change of variable for elliptic curves:

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

$$\boxed{y = y' - \frac{a_1 x}{2} - \frac{a_3}{2}}$$

$y^2 + a_1xy + a_3y = y^2 - a_1xy - a_3y + a_1xy + a_3y + \left(\frac{a_1x}{2} + \frac{a_3}{2}\right)^2 =$

$x^3 + a_2x^2 + a_4x + a_6$

So $y'^2 = x'^3 + a'_2x'^2 + a'_4x + a'_6$

$x = x' - \frac{a_2}{3}$

$x^3 = \left(x' - \frac{a'_2}{3}\right)^3 = x'^3 - a'_2x'^2 + 3x\left(\frac{-a_2}{3}\right)^2 - \left(\frac{a'_2}{3}\right)^3$

$\rightarrow y'^2 = x'^3 + a''_4x + a''_6$

Remark: 1) linear change of variable between long Weierstrass equation are of the form: $(x,y) \longrightarrow (u^2x + r, u^3y + su^2x + t)$

2) linear change of variable between short Weierstrass equation are of the form: $(x,y) \longrightarrow (u^2x, u^3y)$

$x = \frac{1}{u^2}x'$ and $y = \frac{1}{u^3}y'$ $\quad E_1 : y^2 = x^3 + ax + b$

$\left(\frac{y'}{u^3}\right)^2 = \left(\frac{x'}{u^2}\right)^3 + a\left(\frac{x'}{u^2}\right) + b$

$E_2 : y'^2 = x'^3 + u^4a + u^6b$

$j(E) = 1728 \times \frac{4a^3}{4a^3 + 27b^2}$

$E_1 \simeq E_2 \Longrightarrow j(E_1) = j(E_2)$

$E_1 \simeq E_2 \Longleftarrow j(E_1) = j(E_2)$ over k