Elliptic curves Cryptography

Francesco Pappalardi

#1 - First Lecture.

June 16^{th} 2019

WAMS School:
Introductory topics in Number Theory
and Differential Geometry
King Khalid University
Abha, Saudi Arabia

Three Lectures on Elliptic Curves Cryptography

Note (Program of the Lectures)

1. Generalities on Elliptic Curves over finite Fields
2. Basic facts on Discrete Logarithms on finite groups, generic attacks (Pohlig–Hellmann, BSGS, Index Calculus)
3. Elliptic curves Cryptography: pairing based Cryptography, MOV attacks, anomalous curves

Notations

Fields of characteristics 0

1. $\mathbb{Q}$ is the field of rational numbers
2. $\mathbb{R}$ and $\mathbb{C}$ are the fields of real and complex numbers
3. $K \subset \mathbb{C}$, $\dim_{\mathbb{Q}} K < \infty$ is a *number field*
   - $\mathbb{Q}[\sqrt{d}]$, $d \in \mathbb{Q}$
   - $\mathbb{Q}[\alpha]$, $f(\alpha) = 0$, $f \in \mathbb{Q}[X]$ irreducible

Finite fields

1. $\mathbb{F}_p = \{0, 1, \ldots, p-1\}$ is the prime field;
2. $\mathbb{F}_q$ is a finite field with $q = p^n$ elements
3. $\mathbb{F}_q = \mathbb{F}_p[\xi]$, $f(\xi) = 0$, $f \in \mathbb{F}_p[X]$ irreducible, $\partial f = n$
4. $\mathbb{F}_4 = \mathbb{F}_2[\xi]$, $\xi^2 = 1 + \xi$
5. $\mathbb{F}_8 = \mathbb{F}_2[\alpha]$, $\alpha^3 = \alpha + 1$ but also $\mathbb{F}_8 = \mathbb{F}_2[\beta]$, $\beta^3 = \beta^2 + 1$, $(\beta = \alpha^2 + 1)$
6. $\mathbb{F}_{101^{101}} = \mathbb{F}_{101}[\omega], \omega^{101} = \omega + 1$

Notations

Algebraic Closure of $\mathbb{F}_q$

- $\mathbb{C} \supset \mathbb{Q}$ satisfies that *Fundamental Theorem of Algebra*! (i.e. $\forall f \in \mathbb{Q}[x], \partial f > 1, \exists \alpha \in \mathbb{C}, f(\alpha) = 0$)
- We need a field that plays the role, for $\mathbb{F}_q$, that $\mathbb{C}$ plays for $\mathbb{Q}$. It will be $\overline{\mathbb{F}_q}$, called *algebraic closure of* $\mathbb{F}_q$

1. $\forall n \in \mathbb{N}$, we fix an $\mathbb{F}_{q^n}$
2. We also require that $\mathbb{F}_{q^n} \subseteq \mathbb{F}_{q^m}$ if $n \mid m$
3. We let $\overline{\mathbb{F}_q} = \bigcup_{n\in\mathbb{N}} \mathbb{F}_{q^n}$

- **Fact:** $\overline{\mathbb{F}_q}$ is *algebraically closed* (i.e. $\forall f \in \mathbb{F}_q[x], \partial f > 1, \exists \alpha \in \overline{\mathbb{F}_q}, f(\alpha) = 0$)

If $F(x, y) \in \mathbb{Q}[x, y]$ a *point of the curve* $F = 0$, means $(x_0, y_0) \in \mathbb{C}^2$ s.t. $F(x_0, y_0) = 0$.

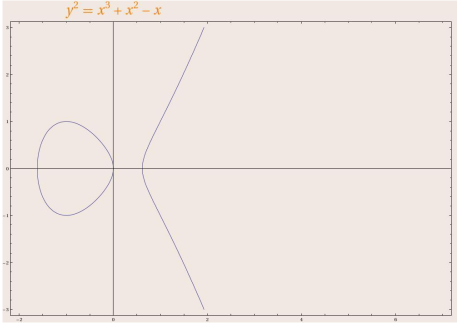
If $F(x, y) \in \mathbb{F}_q[x, y]$ a *point of the curve* $F = 0$, means $(x_0, y_0) \in \overline{\mathbb{F}_q}^2$ s.t. $F(x_0, y_0) = 0$.

The (general) Weierstraß Equation

An elliptic curve E over a $\mathbb{F}_q$ (finite field) is given by an equation

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

where $a_1, a_3, a_2, a_4, a_6 \in \mathbb{F}_q$



The equation should not be *singular*

The Discriminant of an Equation

The condition of absence of singular points in terms of a_1, a_2, a_3, a_4, a_6

Definition

The *discriminant* of a Weierstraß equation over $\mathbb{F}_q$, $q = p^n$, $p \geq 3$ is

$$D_E := \frac{1}{2^4}\Big(-a_1^5 a_3 a_4 - 8a_1^3 a_2 a_3 a_4 - 16a_1 a_2^2 a_3 a_4 + 36a_1^2 a_3^2 a_4 - a_1^4 a_4^2 - 8a_1^2 a_2 a_4^2 - 16a_2^2 a_4^2 + 96a_1 a_3 a_4^2 + 64a_4^3 + a_1^6 a_6 + 12a_1^4 a_2 a_6 + 48a_1^2 a_2^2 a_6 + 64a_2^3 a_6 - 36a_1^3 a_3 a_6 - 144a_1 a_2 a_3 a_6 - 72a_1^2 a_4 a_6 - 288a_2 a_4 a_6 + 432a_6^2\Big)$$

Note

E is *non singular* if and only if $D_E \neq 0$

Special Weierstraß equation of $E/\mathbb{F}_{p^\alpha}, p \neq 2$

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in \mathbb{F}_{p^\alpha}$$

If “complete the squares“ $\begin{cases} x \leftarrow x \\ y \leftarrow y - \frac{a_1x+a_3}{2} \end{cases}$

the Weierstraß equation becomes: $E' : y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$

where $a_2' = a_2 + \frac{a_1^2}{4}$, $a_4' = a_4 + \frac{a_1a_3}{2}$, $a_6' = a_6 + \frac{a_3^2}{4}$

If $p \geq 5$, we can also apply the transformation $\begin{cases} x \leftarrow x - \frac{a_2'}{3} \\ y \leftarrow y \end{cases}$ obtaining the equations: $E'' : y^2 = x^3 + a_4''x + a_6''$

where $a_4'' = a_4' - \frac{a_2'^2}{3}$, $a_6'' = a_6' + \frac{2a_2'^3}{27} - \frac{a_2'a_4'}{3}$

Definition

Two Weierstraß equations over $\mathbb{F}_q$ are said (affinely) equivalent if there exists a (affine) change of variables that takes one into the other

Note

The only affine transformation that take a Weierstrass equations in another Weierstrass equation have the form

$$\begin{cases} x \longleftarrow u^2 x + r \\ y \longleftarrow u^3 y + u^2 s x + t \end{cases} \quad r, s, t, u \in \mathbb{F}_q$$

The Weierstraß equation

Classification of simplified forms

After applying a suitable affine transformation we can always assume that $E/\mathbb{F}_q (q = p^n)$ has a Weierstraß equation of the following form

Example (Classification)

E	p	D_E
$y^2 = x^3 + Ax + B$	≥ 5	$4A^3 + 27B^2$
$y^2 + xy = x^3 + a_2x^2 + a_6$	2	a_6^2
$y^2 + a_3y = x^3 + a_4x + a_6$	2	a_3^4
$y^2 = x^3 + Ax^2 + Bx + C$	3	$4A^3C - A^2B^2 - 18ABC + 4B^3 + 27C^2$

Definition (Elliptic curve)

An elliptic curve is the data of a non singular Weierstraß equation (i.e. $D_E \neq 0$)

Note: If $p \geq 3$, $D_E \neq 0 \Leftrightarrow x^3 + Ax^2 + Bx + C$ has no double root

Elliptic curves over $\mathbb{F}_2$

All possible Weierstraß equations over $\mathbb{F}_2$ are:

Weierstraß equations over $\mathbb{F}_2$

1. $y^2 + xy = x^3 + x^2 + 1$
2. $y^2 + xy = x^3 + 1$
3. $y^2 + y = x^3 + x$
4. $y^2 + y = x^3 + x + 1$
5. $y^2 + y = x^3$
6. $y^2 + y = x^3 + 1$

However the change of variables $\begin{cases} x \leftarrow x + 1 \\ y \leftarrow y + x \end{cases}$ takes the sixth curve into the fifth.

Hence we can remove the sixth from the list.

Fact:

There are 5 affinely inequivalent elliptic curves over $\mathbb{F}_2$

Elliptic curves in characteristic 3

Via a suitable transformation ($x \to u^2x + r, y \to u^3y + u^2sx + t$) over $\mathbb{F}_3$, 8 inequivalent elliptic curves over $\mathbb{F}_3$ are found:

Weierstraß equations over $\mathbb{F}_3$

1. $y^2 = x^3 + x$
2. $y^2 = x^3 - x$
3. $y^2 = x^3 - x + 1$
4. $y^2 = x^3 - x - 1$
5. $y^2 = x^3 + x^2 + 1$
6. $y^2 = x^3 + x^2 - 1$
7. $y^2 = x^3 - x^2 + 1$
8. $y^2 = x^3 - x^2 - 1$

Fact: let $\left(\frac{a}{q}\right)$ be the Kronecker symbol. The number of non–isomorphic (i.e. inequivalent) classes of elliptic c. over $\mathbb{F}_q$ is

$$2q + 3 + \left(\frac{-4}{q}\right) + 2\left(\frac{-3}{q}\right)$$

The definition of $E(\mathbb{F}_q)$

Let $E/\mathbb{F}_q$ elliptic curve and consider a "symbol" ∞ (point at infinity). Set

$$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : \ y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\} \cup \{\infty\}$$

Hence

- $E(\mathbb{F}_q) \subset \mathbb{F}_q^2 \cup \{\infty\}$
- If $\mathbb{F}_q \subset \mathbb{F}_{q^n}$, then $E(\mathbb{F}_q) \subset E(\mathbb{F}_{q^n})$
- We may think that ∞ sits on the top of the y–axis ("vertical direction")

Definition (line through points $P, Q \in E(\mathbb{F}_q)$)

$$r_{P,Q} : \begin{cases} \text{line through } P \text{ and } Q & \text{if } P \neq Q \\ \text{tangent line to } E \text{ at } P & \text{if } P = Q \end{cases}$$

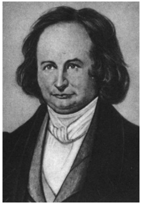
projective or affine

- if $\#(r_{P,Q} \cap E(\mathbb{F}_q)) \geq 2 \ \Rightarrow \ \#(r_{P,Q} \cap E(\mathbb{F}_q)) = 3$

  if tangent line, contact point is counted with multiplicity
- $r_{\infty,\infty} \cap E(\mathbb{F}_q) = \{\infty, \infty, \infty\}$

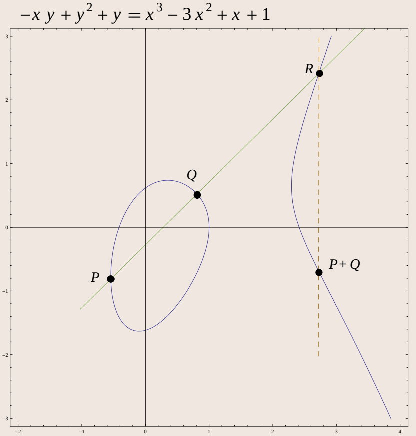
History (from WIKIPEDIA)

Carl Gustav Jacob Jacobi (10/12/1804 – 18/02/1851) was a German mathematician, who made fundamental contributions to elliptic functions, dynamics, differential equations, and number theory.



Some of His Achievements:

- Theta and elliptic function
- Hamilton Jacobi Theory
- Inventor of determinants
- Jacobi Identity $[A,[B,C]]+[B,[C,A]]+[C,[A,B]]=0$



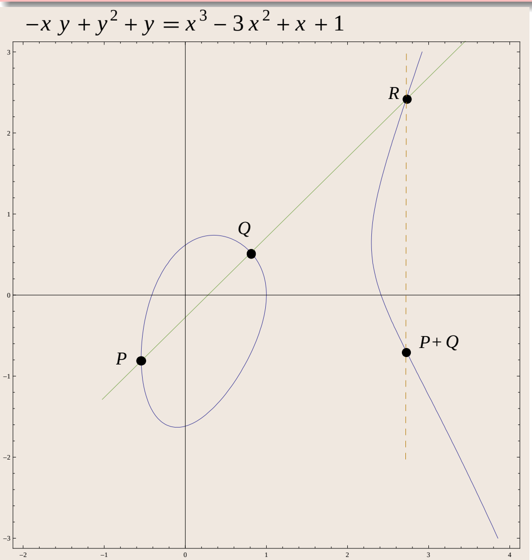
$r_{P,Q}\cap E(\mathbb{F}_q)=\{P,Q,R\}$

$r_{R,\infty}\cap E(\mathbb{F}_q)=\{\infty,R,R'\}$ $P+_E Q := R'$

$r_{P,\infty}\cap E(\mathbb{F}_q)=\{P,\infty,P'\}$ $-P := P'$

$E/\mathbb{F}_q$ elliptic curve ($D_E = D_E(a_1, a_2, a_3, a_4, a6) \neq 0$)

$E(\mathbb{F}_q) = \{(x, y) \in \mathbb{F}_q^2 : \; y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\} \cup \{\infty\}$



Properties of the operation "$+_E$"

Theorem

The addition law on $E(\mathbb{F}_q)$ has the following properties:

- (a) $P +_E Q \in E(\mathbb{F}_q)$ $\quad \forall P, Q \in E(\mathbb{F}_q)$
- (b) $P +_E \infty = \infty +_E P = P$ $\quad \forall P \in E(\mathbb{F}_q)$
- (c) $P +_E (-P) = \infty$ $\quad \forall P \in E(\mathbb{F}_q)$
- (d) $P +_E (Q +_E R) = (P +_E Q) +_E R$ $\quad \forall P, Q, R \in E(\mathbb{F}_q)$
- (e) $P +_E Q = Q +_E P$ $\quad \forall P, Q \in E(\mathbb{F}_q)$

- $\left(E(\mathbb{F}_q), +_E\right)$ commutative group
- All group properties are easy except associative law (d)
- Geometric proof of associativity uses *Pappo's Theorem*
- can substitute $\mathbb{F}_q$ with any field K; Theorem holds for $(E(K), +_E)$
- $-P = -(x_1, y_1) = (x_1, -a_1 x_1 - a_3 - y_1)$