Elliptic Curve Cryptography

an introduction which is entirely too short

by Giacomo Fenzi (ETH Zurich)
on 6 January 2022

» Motivation

'It is possible to write endlessly on elliptic curves.
(This is not a threat.)' Serge Lang

*

» Outline

* Historical Notes
* Mathematical Background
* Addition on Elliptic Curves
* Discrete Logarithm and Diffie Hellman
* Pairings
* Isogenies

» History

Historically originated in the context of solving Diophantine equations such as

$$X^n + Y^n = Z^n, \;\; X, Y, Z \in \mathbb{Z}$$

or equivalently

$$x^n + y^n = 1, \;\; x, y \in \mathbb{Q}$$

Often very hard, and in general undecidable[1]!
Let us see what we can do...

[1] In fact, already undecidable with 11 integers variables!

» History: One variable

$$a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a = 0$$

Quite easy! We can show that:

Theorem

Let $\frac{p}{q} \in \mathbb{Q}$ be a solution of the above equation. Then q divides a_n and p divides a_0.

Check the finite list of candidates.
Alternatively, solve numerically and find candidate of form $\frac{b}{a_n}$

» History: Linear and Quadratic

$$ax + by = c$$

Theorem

Has infinitely many rational solution. If $\gcd(a, b)$ does not divide c, then no integers solutions. Else, infinitely many.

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

These are rational points on a conic.

* Given a rational point, all of them can be found geometrically
* Hasse principle allows us to test if a rational point exists

» History: Cubics

What about:

$$ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\ ?$$

This is the general form of an elliptic curve! We have that

Theorem (Mordell)

If the curve is non singular, and it has a rational point then the group of rational points is finitely generated

But no equivalent of Hasse principle!

Elliptic Curves $\neq$ Ellipse

» Background: Fields

Definition

A field $\mathbb{F}$ is set together with two operations $+, \cdot$ such that

* $\mathbb{F}$ is an abelian group under $+$ with identity 0
* $\mathbb{F} - \{0\}$ is an abelian group under multiplication with identity 1.
* For every $a, b, c \in \mathbb{F}$ we have that $a(b + c) = ab + ac$
* $0 \neq 1$

Informally, we can add, subtract, multiply and divide non zero elements.

» Background: Finite Fields

We are mostly interested in finite fields. We have that:

Theorem

For every prime p, and every $n \in \mathbb{Z}^+$ there is an unique field of size p^n, which we denote by either $\mathbb{GF}(p^n)$ or $\mathbb{F}_{p^n}$

If $n = 1$, then $\mathbb{F}_p = \mathbb{Z}_p$, if not we can write them as

$$\mathbb{F}_{p^n} = \frac{\mathbb{F}_p[X]}{(f(x))}$$

where $f(x)$ is an irreducible polynomial of degree n.

» Background: Characteristic

For any field, $\mathrm{char}(\mathbb{F})$ is the least integer[2] ℓ such that

$$\underbrace{1 + \ldots 1}_{\ell \text{ times}} = 0$$

We have that $\mathrm{char}(\mathbb{F}_{p^n}) = p$.

[2] Or ∞ if no such integer exists

» Background: Field Extensions

Let k, K be two fields. If there is an homomorphism $k \to K$, we can identify k with a subfield of K. In that case, K is a **field extension** of k which we denote by $k \subseteq K$.
Given any field K we can construct the algebraic closure $\overline{K}$ which is the smallest algebraically closed extension containing K.
Some examples:

* $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
* $\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^3} \cdots \subseteq \overline{\mathbb{F}}_p$

» Weierstrass Form

$$
\begin{array}{c}
ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \\
\downarrow \\
y^2 + axy + by = x^3 + cx^2 + dx + e \\
\Big\downarrow \ \mathrm{char}(\mathbb{F}) \neq 2, 3 \\
y^2 = x^3 + ax + b
\end{array}
$$

Much easier to manage!

» Elliptic Curves

Definition

Let $\mathbb{F}$ be a field. An elliptic curve E defined over a field $\mathbb{F}$ is given by

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

for $a, b \in \mathbb{F}$. For any extension $\mathbb{F} \subseteq \mathbb{E}$ we define

$$E(\mathbb{E}) = \left\{(x, y) \in \mathbb{E} \times \mathbb{E} \mid y^2 = x^3 + ax + b\right\} \cup \{\infty\}$$

Mathematicians are often interested with $E(\mathbb{Q}) \subseteq E(\mathbb{R}) \subseteq E(\mathbb{C})$ but we mostly consider the finite case.

» Some elliptic curves (In $E(\mathbb{R})$ since they look better...)

TODO: One singular with cusp, one node and three non singular

» Fundamental Quantities

Definition

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve.
The **discriminant** of E is

$$\Delta = -16(4a^3 + 27b^2)$$

A curve is **singular** if $\Delta = 0$.
If E is non-singular the j-**invariant** of E is

$$j(E) = -1728 \frac{(4A)^3}{\Delta}$$

Theorem

Let E, E' be two elliptic curves over K. Then $E \cong E'$ if and only if $j(E) = j(E')$.

» The Group Law

TODO: Picture group law

» The Group Law: Formulae

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve. Let $P_i = (x_i, y_i) \in E(K)$. Define

$$-P_0 = (x_0, -y_0)$$

Now, for $P_1 + P_2$:

* If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \infty$
* If $P_1 = \infty$ then $P_1 + P_2 = P_2$, and viceversa.
* Let $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ where λ is defined as:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, \ x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1}, \ \text{otherwise} \end{cases}$$

» Resources

* J.H. Silverman, The Arithmetic of Elliptic Curves
* J.H. Silverman, J.T. Tate, Rational Points on Elliptic Curves
* D.A. Cox, Primes of the form $x^2 + ny^2$
* P. Aluffi, Algebra: Chapter 0