A Concrete Introduction to Number Theory and Algebra–Elliptic Curve.

Libin Wang

Shool of Computer Science, South China Normal University

November 2, 2022

Elliptic Curve.(椭圆曲线)

What exactly is an elliptic curve?

- Elliptic curves are number theoretic objects that are central to both pure and applied number theory.
- In particular, elliptic curves are widely believed to be useful in many applications.
- An elliptic curve is a point set of an Abelian group. The group law is constructed geometrically.
- Elliptic curves have (almost) nothing to do with ellipses.

Elliptic Curve.

Definition

(Elliptic Curve.) Let $a, b \in \mathbb{R}$ *be constants such that* $4a^3 + 27b^2 \neq 0$. *A non-singular elliptic curve is the set* E *of solutions* $(x, y) \in \mathbb{R} \times \mathbb{R}$ *to the equation:* $y^2 = x^3 + ax + b$ *together with a special point* $\mathcal{O}$ *called the point at infinity. The solution set* E *forms an Abelian group with identity* $\mathcal{O}$.

Play with EC using Sage.

Listing 1: "Play with EC using Sage."

```
## Play with EC using Sage.
# The elliptic curve y^2 = x^3 - 5x + 4 over R.
E0 = EllipticCurve(RR, [-5, 4])
show(plot(E0, hue=.9))
# The elliptic curve over F_p.
p = 137
F = FiniteField(p)
E1 = EllipticCurve(F, [F.random_element(), F.random_element()])
print E1
E1.points()
show(plot(E1, hue=.9))
```

Graphical Representation of EC over $\mathbb{R}$.

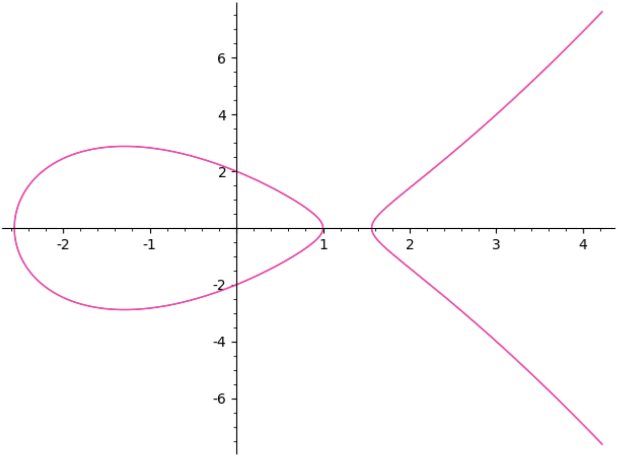

Figure: Elliptic Curve defined by $y^2 = x^3 - 5 * x + 4$ over $\mathbb{R}$.

Graphical Representation of EC over a finite field.

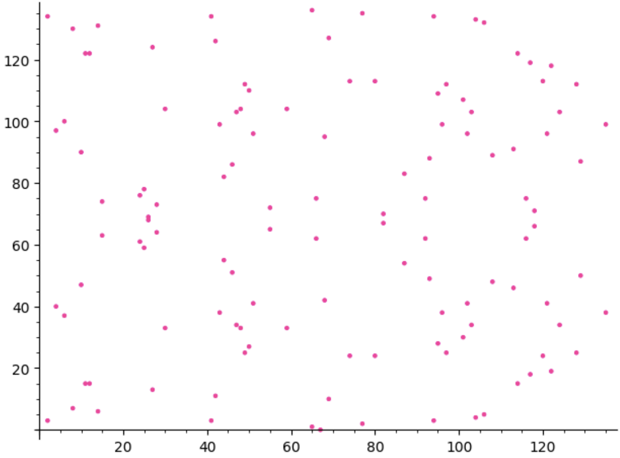

Figure: Elliptic Curve over $\mathbb{F}_{137}$.

Group Operations of Elliptic Curves.

Let E be an elliptic curve over a field $\mathbb{F}$, given by an equation $y^2 = x^3 + ax + b$. We begin by defining a binary operation $+$ on $E(\mathbb{F})$.

Group Operation.

- $P + \mathcal{O} = \mathcal{O} + P = P$;
- $P + (-P) = \mathcal{O}$, when $P = (x, y)$, $-P = (x, -y)$;
- $P + (Q + R) = (P + Q) + R$;
- $P + Q = Q + P$;

Graphical Representation of Negtive and the Point at Infinity.

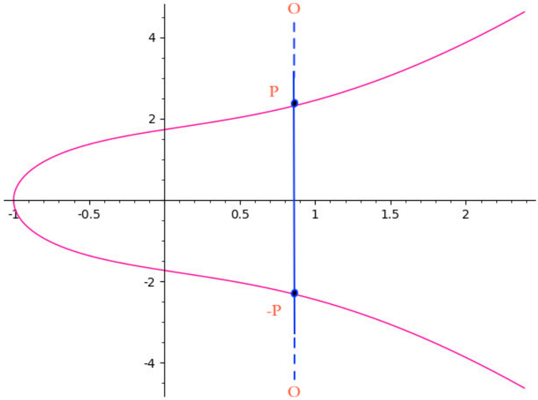

Figure: 椭圆曲线群的逆元与无穷远点

Group Operations of Elliptic Curves.

Given $P, Q \in E(\mathbb{F})$, computes a third point $R = P + Q \in E(\mathbb{F})$.

Addition of the Group $E(\mathbb{F})$.

Let $P = (x_1, y_1)$, and $Q = (x_2, y_2)$, $R = (x_3, y_3)$.

- $P = Q$.
  - compute $\lambda = (3x_1^2 + a)/2y_1$
  - compute $x_3 = \lambda^2 - 2x_1$, $y_3 = \lambda(x_1 - x_3) - y_1$.
- $P \neq Q$.
  - compute $\lambda = (y_2 - y_1)/(x_2 - x_1)$
  - compute $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$.

Graphical Representation of Addtion.

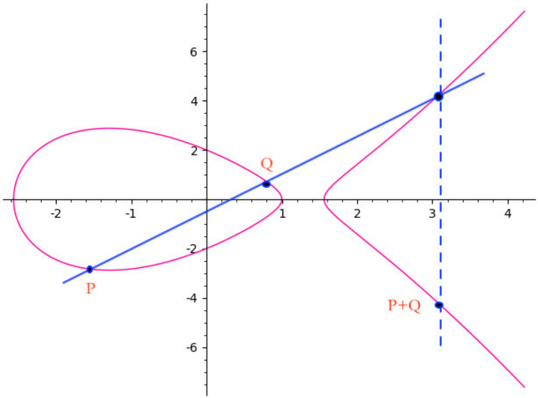

Figure: Add two different points in Elliptic Curve.

Graphical Representation of Addtion.

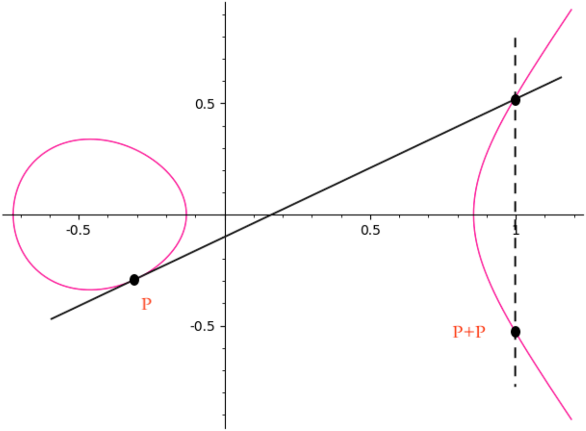

Figure: Add two same points in Elliptic Curve.

To Explain the Group Operations of Elliptic Curves-1.

Addition of two distinct points.

Given distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, computes $R = (x_3, y_3)$.

- $\lambda = (y_2 - y_1)/(x_2 - x_1)$ is the slope of the line L through P and Q. L can be written as:

$$y = \lambda(x - x_1) + y_1;$$

- The intersection of L and E is

$$(\lambda(x - x_1) + y_1)^2 = x^3 + ax + b,$$

and it can be rearranged to the form

$$0 = x^3 - \lambda^2 x^2 + \cdots ;$$

To Explain the Group Operations of Elliptic Curves-2.

Addition of two distinct points.

Given distinct points $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, computes $R = (x_3, y_3)$.

- Since we know the three roots of this cubic equation, thus:

$$x^3 - \lambda^2 x^2 + \cdots = (x - x_1)(x - x_2)(x - x_3) =$$
$$x^3 - (x_1 + x_2 + x_3)x^2 + \cdots = 0$$

- We obtain $x_3 = \lambda^2 - x_1 - x_2$;
- Hence $y_3 = \lambda(x_1 - x_3) - y_1$.

To Explain the Group Operations of Elliptic Curves-3.

Addition of points when $P = Q$.

Given distinct points $P = (x_1, y_1)$, computes $R = 2P = (x_3, y_3)$.

- The slope of the tangent line L through P is given by implicit differentiation
$$2y\frac{dy}{dx} = 3x^2 + a,$$
hence
$$\lambda = \frac{3x_1^2 + a}{2y_1}$$
- The previous analysis is general, thus we obtain $x_3 = \lambda^2 - 2x_1$ and $y_3 = \lambda(x_1 - x_3) - y_1$.

EC over a finite field.

Definition

Let $p > 3$ be prime. The elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$ is the set of solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ to the congruence: $y^2 \equiv x^3 + ax + b \pmod{p}$ where $a \in \mathbb{F}_p$, $b \in \mathbb{F}_p$, are constants such that $4a^3 + 27b^2 \neq 0 \pmod{p}$, together with a special point $\mathcal{O}$ called the point at infinity.

EC over a finite field.

Example: an EC over finite field.

Let's examine the elliptic curve $E: y^2 = x^3 + x + 6$ over $\mathbb{F}_{11}$ as an example. List all the points of the E:

x	0	1	2	3	4	5	6	7	8	9	10
E	6	8	5	3	8	4	8	4	9	7	4
y			4,7	5,6		2,9		2,9	3,8		2,9

The order of E is 13, a prime number.

EC over a finite field.

Example: an EC over finite field.

Since the oder of E is prime, the group is cyclic. We can generate the group by choosing any point other than the point at infinity. Let our generator be $g = (2, 7)$. Generate the group by using the rules of addition we defined earlier where $2g = g + g$. We know $\lambda = (3x_1^2 + a)/2y_1 = (12 + 1)/(2 * 7) = 8$, please check it!

g	2g	3g	4g	5g	6g	7g
(2, 7)	(5, 2)	(8, 3)	(10, 2)	(3, 6)	(7, 9)	(7, 2)
8g	9g	10g	11g	12g	13g	
(3, 5)	(10, 9)	(8, 8)	(5, 9)	(2, 4)	(0, 6)	

EC over a finite field.

Example: an EC over finite field.

Let generator be $g = (2, 7)$. $a = 1$, $b = 6$. We know $\lambda = (3x_1^2 + a)/2y_1 = (12 + 1)/(2 * 7) = 8$.

1. $2g = (x_3, y_3)$ while $x_3 = \lambda^2 - x_1 - x_2 = 5$, $y_3 = \lambda(x_1 - x_3) - y_1 = 2$.
2. $3g = g + 2g$. Check it yourself!

EC over a finite field.

How to compute ng?

Given $P \in E(\mathbb{F}_p)$, we can compute nP by using $O(n)$ additions, namely:

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}}.$$

EC over a finite field.

How to compute ng?

Given $P \in E(\mathbb{F}_p)$, we can compute nP by using $O(n)$ additions, namely:

$$nP = \underbrace{P + P + \cdots + P}_{n \text{ times}}.$$

Can we do it better?

EC over a finite field.

How to compute nP?

We can compute nP in $O(logn)$ steps by the usual *Double-and-Add Method*. First write

$$n = n_0 + n_1 \cdot 2 + n_2 \cdot 2^2 + \cdots + n_r \cdot 2^r$$

with $n_0, \cdots, n_r \in \{0, 1\}$.
Then nP can be computed as

$$nP = n_0 P + n_1 \cdot 2P + n_2 \cdot 2^2 P + \cdots + n_r \cdot 2^r P,$$

where $2^k g = 2 \cdot 2 \cdots 2P$ requires only k doublings.

EC over a finite field.

An important question.

Can we do even better?

To Explain the Elliptic Curves over $GF(2^n)$-1.

The Elliptic Curves over $GF(2^n)$

Why the Elliptic Curves over $GF(2^n)$ can't be $y^2 = x^3 + ax + b$?

- The slope of the tangent line L through P is given by implicit differentiation and
$$\lambda = \frac{3x_1^2 + a}{2y_1}$$
- What is $2y_1$ in $GF(2^n)$? 0 !

To Explain the Elliptic Curves over $GF(2^n)$-2.

The Elliptic Curves over $GF(2^n)$

The Elliptic Curves over $GF(2^n)$ may be $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Two problems should consider.

- The slope of the tangent line L through P.
- The negation of a point is given by

$$-(x, y) = (x, -a_1x - a_3 - y)).$$

To Explain the Elliptic Curves over $GF(2^n)$-3.

Why the negation of a point is not the same as the previous curves?

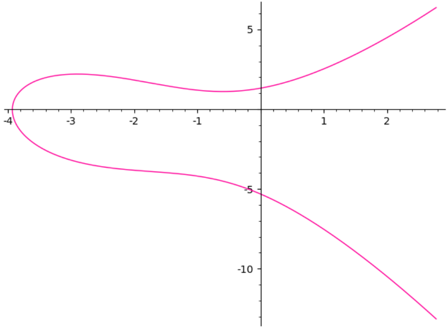

Figure: An Elliptic Curve defined by generalized Weierstrass equation.

Elliptic Curve Factorization Method.

Given a large number N, and a bound B

Basic Idea.

- Choose a random a and a point in $P \in E(\mathbb{F}_N)$;
- Compute compute $m = lcm(1, 2, \cdots, B)$;
- If at some point we cannot compute a sum of points because some denominator the computation is not coprime to N, we compute the greatest common divisor g of this denominator with N. If g is a nontrivial divisor, output it.

Elliptic Curve Factorization Method.

Listing 2: "Elliptic Curve Factorization Method."

```
def ecm(N, B=10^3, trials=10):
    m, R= lcm(1,2,...,B), Integers(N)
    R.is_field = lambda : True #Make Sage think that R is a field.
    for _ in range(trials):
        a = ChooseRandomA()
        try:
            m * EllipticCurve([a, 1])([0,1])
        except ZeroDivisionError as msg:
            # msg: "Inverse of <int> does not exist"
            return gcd(Integer(str(msg).split()[2]), N)
    return 1
```

Elliptic Curve Factorization Method.

Remark

Note that, actually $\mathbb{F}_N$ is not necessary a finite field , thus $E(\mathbb{F}_N)$ is not a well-formed elliptic curve;

Why we need ECC?

Why we need ECC?

- More efficiency.
- More security.
- More functional properties.

The Elliptic Curve Discrete Logarithm Problem.

Definition

(Elliptic Curve Discrete Log Problem) Suppose E is an elliptic curve over finit field $\mathbb{F}$ and $P \in E(\mathbb{F})$. Given a multiple Q of P, the elliptic curve discrete log problem (ECDLP) is to find $n \in \mathbb{F}$ such that $nP = Q$.

We believe ECDLP is hard.

Elliptic Curve Analogs of Diffie-Hellman.

Listing 3: "Elliptic Curve Diffie-Hellman."

```
p = next_prime(randrange(10^40))
F = FiniteField(p)
E = EllipticCurve(F, [F.random_element(), F.random_element()])
P = E.random_element()
b = randrange(1000); b
B = b*P
a = randrange(1000); a
A = a*P
if(a*B == b*A): print "We share a common secret."
```

Public Key Summary.

Table 4.5: Public Key Summary

Primitive	Parameters	Legacy System Minimum	Future System Minimum
RSA Problem	N, e, d	$\ell(n) \geq 1024$, $e \geq 3$ or 65537, $d \geq N^{1/2}$	$\ell(n) \geq 3072$ $e \geq 65537$, $d \geq N^{1/2}$
Finite Field DLP	p, q, n	$\ell(p^n) \geq 1024$ $\ell(p), \ell(q) > 160$	$\ell(p^n) \geq 3072$ $\ell(p), \ell(q) > 256$
ECDLP	p, q, n	$\ell(q) \geq 160$, $\star$	$\ell(q) > 256$, $\star$

Figure: Public Key Summary.