§ 7 Elliptic Curves

Definition 7.1

Let F be a field.

An elliptic curve is a non-singular (i.e no cusps or self-intersections) curve given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad , \quad a_i \in F .$$

If the characteristic of $F \neq 2$, by a change of variable $y = y' - \frac{1}{2}(a_1x + a_3)$

$$\left[y' - \tfrac{1}{2}(a_1x+a_3)\right]^2 + a_1x\left[y' - \tfrac{1}{2}(a_1x+a_3)\right] + a_3\left[y' - \tfrac{1}{2}(a_1x+a_3)\right] = x^3 + a_2x^2 + a_4x + a_6$$

$$y'^2 - \tfrac{1}{4}a_1^2x^2 - \tfrac{1}{2}a_1a_3x - \tfrac{1}{4}a_3^2 = x^3 + a_2x^2 + a_4x + a_6$$

$$y'^2 = x^3 + (a_2 + \tfrac{a_1^2}{4})x^2 + (a_4 + \tfrac{a_1a_3}{2})x + (a_6 + \tfrac{a_3^2}{4})$$

$$y'^2 = x^3 + b_1x^2 + b_2x + b_3$$

If the characteristic of $F \neq 3$, by a change of variable $x = x' - \frac{b_1}{3}$,

$$y'^2 = (x' - \tfrac{b_1}{3})^3 + b_1(x' - \tfrac{b_1}{3})^2 + b_2(x' - \tfrac{b_1}{3}) + b_3$$

$$y'^2 = x'^3 + (-\tfrac{b_1^2}{3} + b_2)x' + (-\tfrac{2b_1^3}{27} - \tfrac{b_1b_2}{3} + b_3)$$

$$y'^2 = x'^3 + c_1x + c_2$$

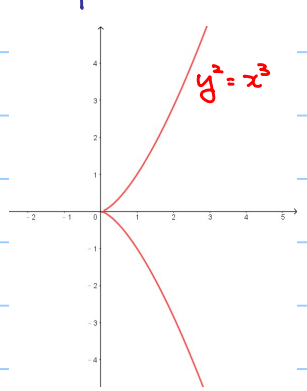
Therefore, if the characteristic of $F \neq 2, 3$, we only need to focus on

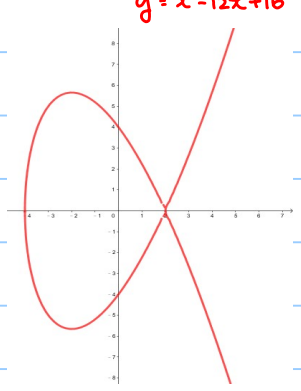
$$y^2 = x^3 + bx + c \quad \text{for } b, c \in F.$$

Fact : Let $\Delta = -16(4b^3 + 27c^2)$. If $\Delta \neq 0$, then $y^2 = x^3 + bx + c$ defines a non-singular curve

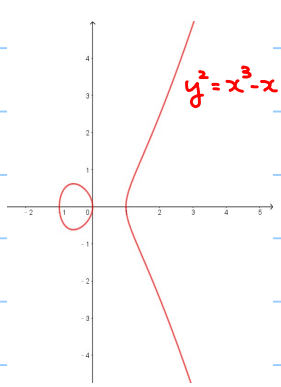
Elliptic Curve over $\mathbb{R}$

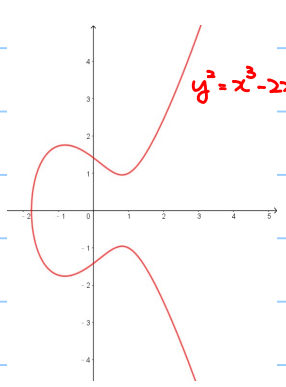
Example 7.1





$\Delta = 0$

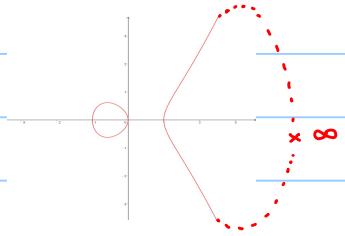




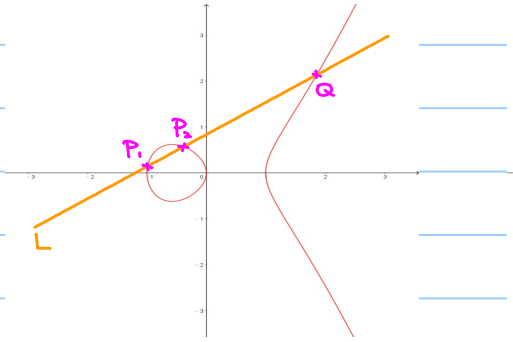
$\Delta \neq 0$

Usually, we add one more point ∞

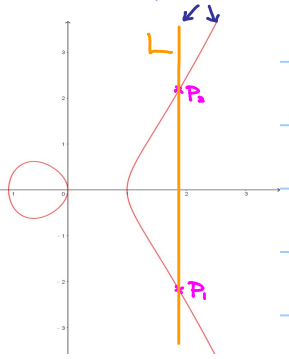
glue the two ends at ∞



Reason:



Intersect at $Q = \infty$



Fix two points P_1 and P_2, draw a line L, it must intersect E at another point Q.

Further study: Projective Geometry, Algebraic Geometry.

Main Goal: Define an addition on E.

One more observation: If $(x,y) \in E$, then $(x,-y) \in E$

Case 1. $P_1, P_2 \in E \setminus \{\infty\}$ and $P_1 \neq P_2$

Let L be the line passing through P_1 and P_2.

(a) If L is not vertical (i.e. $x_1 \neq x_2$)

$P_3 = P_1 + P_2$ is defined as the reflection of Q along the x-axis.

Equation of L:

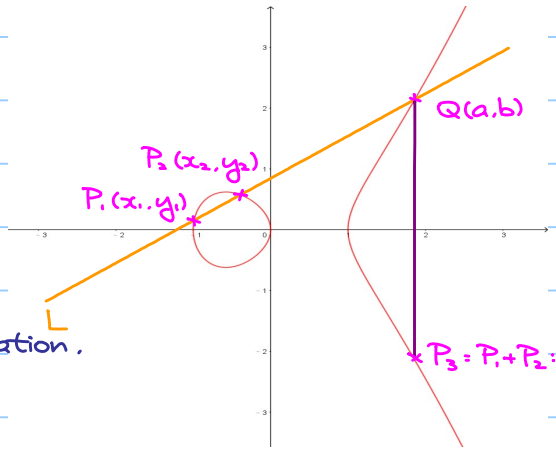
$$y = m(x-x_1) + y_1 \quad \text{where } m = \frac{y_2-y_1}{x_2-x_1}$$

Put it into the equation of E:

$$[m(x-x_1)+y_1]^2 = x^3 + bx + c$$

$$x^3 - m^2x^2 + (b+2mx_1)x + (c - mx_1^2 - y_1^2) = 0$$

Note that a, x_1, x_2 are roots of the above equation.



So $a + x_1 + x_2 = m^2$, i.e. $a = m^2 - x_1 - x_2$

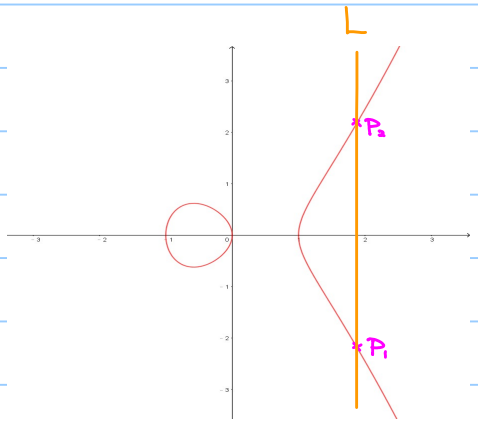
$$b = m(a-x_1) + y_1$$

$\therefore P_3 = (x_3, y_3) = (a, -b)$ where $x_3 = m^2 - x_1 - x_2$

$$y_3 = m(x_1 - x_3) - y_1$$

(b) If L is vertical (i.e. $x_1 = x_2$)

We simply define $P_1 + P_2 = \infty$

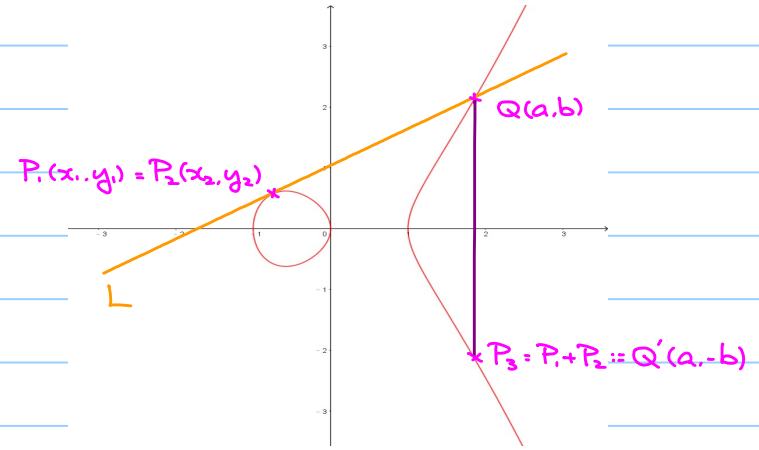


Case 2. $P_1 = P_2 \in E \setminus \{\infty\}$

$$y^2 = x^3 + bx + c$$

$$2y\frac{dy}{dx} = 3x^2 + b$$

$$\left.\frac{dy}{dx}\right|_{\substack{x=x_1 \\ y=y_1}} = \frac{3x_1^2 + b}{2y_1}$$



Equation of L:

$$y = m(x - x_1) + y_1 \quad \text{where } m = \frac{3x_1^2 + b}{2y_1}$$

Put it into the equation of E:

$$x^3 - m^2x^2 + (b + 2mx_1)x + (c - mx_1^2 - y_1^2) = 0$$

Note that a, x_1, x_2 are roots of the above equation. (in fact, $x_1 = x_2$ is a double root)

so $a + x_1 + x_2 = m^2$, i.e. $a = m^2 - x_1 - x_2$

$$b = m(a - x_1) + y_1$$

$\therefore P_3 = (x_3, y_3) = (a, -b)$ where $x_3 = m^2 - x_1 - x_2$

$$y_3 = m(x_1 - x_3) - y_1$$

Case 3. $P_1, P_2 \in E$ and $P_2 = \infty$

We simple define $P_1 + \infty = \infty + P_1 = P_1$

Remark: ∞ plays the role of additive identity.

Also, if $P = (x, y) \in E \setminus \{\infty\}$, then $-P = (x, -y) \in E \setminus \{\infty\}$ such that $P + (-P) = \infty$,

so $-P$ acts as an additive inverse of P.

(Caution: Here, $-P \neq (-x, -y)$)

Exercise 7.1

Let $P, Q, R \in E \setminus \{\infty\}$. Prove that $P + Q + R = \infty$ if and only if P, Q and R are collinear.

Now, we ignore the geometrical interceptation and borrow the formulas to define an addition on an elliptic curve over a field F with characteristic $\neq 2, 3$:

Let E be an elliptic curve given by $y^2 = x^3 + bx + c$ for $b, c \in F$.

1) $\infty + P = P + \infty$ for all $P \in E$

2) If $(x, y), (x, -y) \in E \setminus \{\infty\}$, then $(x, y) + (x, -y) = \infty$

3) Otherwise, let $P_1(x_1, y_1), P_2(x_2, y_2) \in E \setminus \{\infty\}$

$$P_3 = P_1 + P_2 = (x_3, y_3) \quad \text{where} \quad \begin{cases} x_3 = m^2 - x_1 - x_2 \\ y_3 = m(x_1 - x_3) - y_1 \end{cases} \quad \text{and} \quad m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq \pm P_2 \\ \dfrac{3x_1^2 + b}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

Exercise 7.2

Prove that $(E, +)$ is an abelian group

Elliptic Curve Mod $p \geq 5$

Example 7.2

Let E be an elliptic curve defined over $\mathbb{Z}_5$ defined by the equation

$$y^2 \equiv x^3 + 4x + 4 \pmod 5$$

Note:

x	0	1	2	3	4
$x^2 \pmod 5$	0	1	4	4	1

Then,

$x \equiv 0 \Rightarrow y^2 \equiv 4 \Rightarrow y \equiv 2$ or $3 \pmod 5$

$x \equiv 1 \Rightarrow y^2 \equiv 9 \equiv 4 \Rightarrow y \equiv 2$ or $3 \pmod 5$

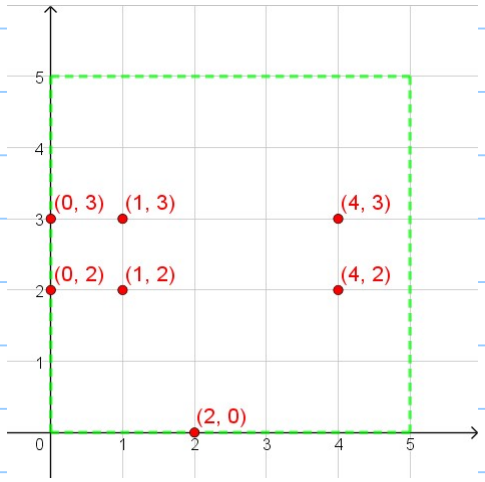
$x \equiv 2 \Rightarrow y^2 \equiv 20 \equiv 0 \Rightarrow y \equiv 0 \pmod 5$

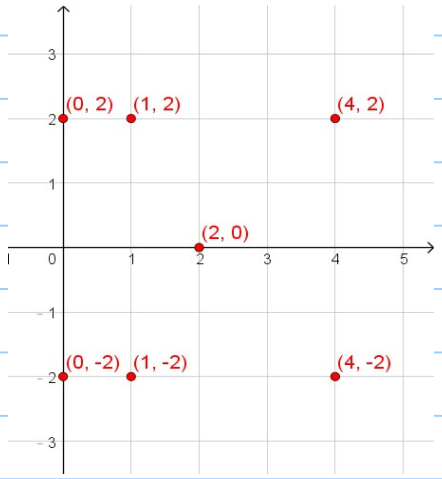
$x \equiv 3 \Rightarrow y^2 \equiv 43 \equiv 3 \Rightarrow$ no solution

$x \equiv 4 \Rightarrow y^2 \equiv 84 \equiv 4 \Rightarrow y \equiv 2$ or $3 \pmod 5$

We can list all the points of E:

$(0,2), (0,3), (1,2), (1,3), (2,0), (4,2), (4,3), \infty$





We have $(0,3) \equiv (0,-2) \pmod 5$ and etc. If we put down points of E as shown on the right, then it is easier to see that E is symmetric along the x-axis.

Let $P_1 = (x_1, y_1) = (1,2)$, $P_2 = (x_2, y_2) = (4,3)$

$$m \equiv \frac{y_2 - y_1}{x_2 - x_1} \equiv \frac{3-2}{4-1} \equiv \frac{1}{3} \equiv 1 \cdot 2 \equiv 2$$ (Note $3^{-1} = 2$ in $\mathbb{Z}_5$)

$P_1 + P_2 = (x_3, y_3)$ where $x_3 \equiv m^2 - x_1 - x_2 \equiv 2^2 - 1 - 4 \equiv -1 \equiv 4 \pmod 5$

$y_3 \equiv m(x_1 - x_3) - y_1 \equiv 2(1-4) - 2 \equiv -8 \equiv 2 \pmod 5$

$\therefore (1,2) + (4,3) = (4,2)$

Discrete Logarithms on Elliptic Curves

Recall:

Let p be a prime. $(\mathbb{Z}/p\mathbb{Z})^\times$ is a multiplicative group.

Discrete Logarithm problem: Give $\alpha, \beta \in (\mathbb{Z}/p\mathbb{Z})^\times$, find $n \in \mathbb{Z}^+$ such that $\beta = \alpha^n$

In general, discrete logarithm problem can also be done on a group $(G, *)$

Given $\alpha, \beta \in G$, find $n \in \mathbb{Z}$ such that $\beta = \alpha^n$.

In particular, we are interested in discrete logarithm problem on the group $(E, +)$, where E is an elliptic curve mod p (with $p \geq 5$)

Given points $P, Q \in E$, find $n \in \mathbb{Z}$ such that $Q = nP$ (E is an additive group)

If solving discrete logarithm problem on E is hard, we may use it to construct cryptosystems.

However, there are some technical problems.

Question : How do we list all the points of E ?

Of course, brute force ! (See example 7.2)

Fact : There is no known polynomial time algorithm for finding all points of an arbitrary E.

Even for brute force, there is a question:

Given x, how to find y such that $y^2 \equiv x^3+bx+c \pmod p$

(i.e. finding square root mod p)

If $p \equiv 3 \pmod 4$, it is easy ; if $p \equiv 1 \pmod 4$, it is more complicated.

Proposition 7.1

Let $p \equiv 3 \pmod 4$ be a prime and let y be an integer. Let $x \equiv y^{\frac{p+1}{4}} \pmod p$.

1) If y has a square root mod p, then the square roots of y mod p are $\pm x$.

2) If y does not have square root mod p, then $-y$ has a square root mod p, and the square roots of $-y$ mod p are $\pm x$.

proof:

If $y \equiv 0 \pmod p$, it is trivial

Assume $y \not\equiv 0 \pmod p$, let $x \equiv y^{\frac{p+1}{4}} \pmod p$ Then,

$$x^4 \equiv y^{p+1} \equiv y^{p-1} \cdot y^2 \equiv y^2 \pmod p$$

$$\Rightarrow (x^2-y)(x^2+y) \equiv 0 \pmod p$$

$$\Rightarrow x^2 \equiv y \text{ or } x^2 \equiv -y \pmod p$$

Therefore, at least one of y or $-y$ has square roots mod p.

However, if both of y and $-y$ have square roots mod p, say $y \equiv a^2$ and $-y \equiv b^2 \pmod p$

then $a^2 \equiv -b^2 \pmod p$

$$(a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} (b^2)^{\frac{p-1}{2}} \pmod p$$

$$1 \equiv a^{p-1} \equiv -b^{p-1} \equiv -1 \pmod p \quad \text{(Contradiction !)} \quad (p \equiv 3 \pmod 4 \Rightarrow \tfrac{p-1}{2} \text{ is odd})$$

Example 7.3

If $y \equiv 5 \pmod{11}$, let $x \equiv y^{\frac{p+1}{4}} \equiv 5^3 \equiv 4 \pmod{11}$.

Check : $x^2 \equiv 4^2 \equiv 16 \equiv 5 \pmod{11}$, so ± 4 are square roots of 5 mod 11.

If $y \equiv 2 \pmod{11}$, let $x \equiv y^{\frac{p+1}{4}} \equiv 2^3 \equiv 8 \pmod{11}$.

Check : $x^2 \equiv 8^2 \equiv 64 \equiv -2 \not\equiv 2 \pmod{11}$, so ± 8 are square roots of -2 mod 11.

Question: How many points does E have?

Rough idea: If we put $x = 0, 1, 2, \cdots, p-1$ into the equation $y^2 \equiv x^3 + bx + c \pmod p$, around half of the chance we have two square roots, we expect it it contributes p points. Together with ∞, an elliptic curve consists of around $p+1$ points

Theorem 7.1 (Hasse's Theorem)

Suppose that $E \pmod p$ has N points. Then, we have

$$|N - p - 1| < 2\sqrt{p} \qquad \text{(i.e. } p+1-2\sqrt{p} < N < p+1+2\sqrt{p}\text{)}$$

Example 7.4

Let $E: y^2 \equiv x^3 - 10 + 21 \pmod{p = 557}$ be an elliptic curve.

By Hasse's theorem, $\left||E| - 558\right| < 2\sqrt{557} \approx 47.2$

$$510.7 < |E| < 605.2 \quad \text{— (1)}$$

Check: $P = (2, 3)$ is a point on E.

(Computer needed) Compute $P, 2P, 3P, \cdots$ until we get $kP = \infty$.

Then k is the order of subgroup of E generated by P and so $k \mid |E|$ (Lagrange's Theorem).

It turns out $k = 189$ and we have $189 \mid |E|$ — (2).

$|E| = 567$ is the only possible integer which satisfies both (1) and (2).

Question: How do we represent a message by a point on E?

Idea: Suppose we represent a message by an integer m, we try to embed it in the x-coordinate of a point on E.

However, $y^2 \equiv m^3 + bm + c \pmod p$ may have no solution.

Method: Fix a positive integer K, suppose m satisfies $m(K+1) < p$,

put $x = mK + j$, for $j = 0, 1, 2, \cdots, K-1$, into the equation of E.

Since, there is about half the chance we get a solution for each x, the failure rate of getting no solution for all j (i.e. cannot generate a point on E) is around $(\frac{1}{2})^K$.

Example 7.5

Let $p = 179$ and E is given by $y^2 \equiv x^3 + 2x + 7 \pmod{179}$.

Take $K = 10$, since we need $m(K+1) < 179$, $0 \le m \le 16$

Suppose that $m = 5$, put $x = mK + j = 50 + j$ for $j = 0, 1, 2, \cdots, 9 \ (= K-1)$

For $x = 50$, (Exercise) $y^2 \equiv 50^3 + 2(50) + 7 \equiv 165 \pmod{179}$ has no solution.

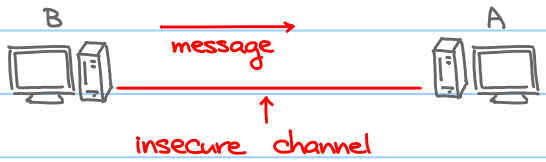
For $x = 51$, $y^2 \equiv 51^3 + 2(51) + 7 \equiv 121 \pmod{179} \Rightarrow y \equiv \pm 11 \pmod{179}$

The message can be represented by $P_m(51, 11)$ on E.

(Remark: We can also perform the above to generate a set of possible messages and corresponding points on E.)

If one gets $P_m(51, 11)$, he computes $m = \lfloor \frac{x}{K} \rfloor = \lfloor \frac{51}{10} \rfloor = 5$ and recovers the message.

The ElGamal Cryptosystem



Algorithm:

1) A chooses an elliptic curve E and a point $P \in E$

2) A chooses a secret integer d and compute $Q = dP$

3) A sends (E, P, Q) to B.

4) Suppose that the message is a point $M \in E$.

   B chooses a random integer k and computes $R = kP$ and $T = kQ + M$,

   then B sends (R, T) back to A.

5) A decryts by computing $T - dR = (kQ + M) - (dk)P$

$$= (dk)Q + M - (dk)Q$$

$$= M$$

If a person gets E, P, Q, R, T, in order to obtain M:

1) Solve d from $Q = dP$;

2) Solve k from $R = kP$, then $M = T - kQ$

However, both involve discrete logarithm problems (Assume to be difficult)