Chapter 5 Hoffstein: Elliptic Curves and Cryptography

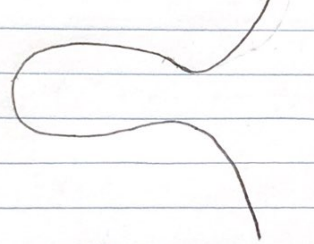
5.1 Elliptic Curves

Note: Elliptic Curves & ellipses are not the same thing

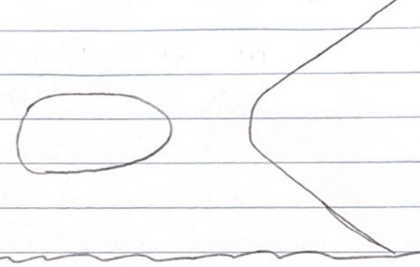
- An elliptic curve is the set of solutions to an equation of the form

$$Y^2 = X^3 + AX + B$$

① Ex. $Y^2 = X^3 - 3X + 3$



② Ex. $Y^2 = X^3 - 6X + 5$



- One feature of elliptic curves is that there is a natural way to take two points on an elliptic curve and "add" them to produce a third point.

- What is meant by "add"?

denoted: $P \oplus Q$: we draw a line L through points P & Q on the curve E. This line L intersects E at 3 points P, Q, and a new point we call R. we that point R and reflect it across the x-axis to get R' ← this new point is called "the sum of P and Q"

add

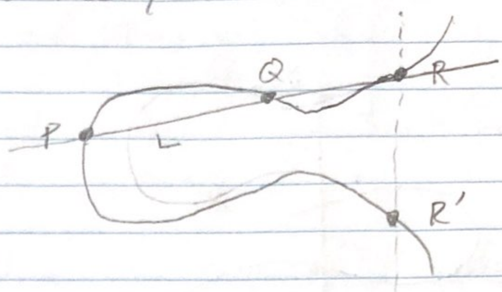
Ex. Let E be the elliptical curve

$$Y^2 = X^3 - 15X + 18 \quad (*)$$

Points $P = (7,16)$ and $Q = (1,2)$ are on the curve E. The line L going through both the points has the equation

$$L: Y = \frac{7}{3}X - \frac{1}{3} \quad (\circ)$$

So now, we substitute (*) into (•) and solve for X to find the point R. Thus



$$\left(\frac{7}{3}x - \frac{1}{3}\right)^2 = x^3 - 15x + 18 \,.$$

after lots of algebra we get the roots of X,

$$(x-7)(x-1)\left(x + \frac{29}{3}\right)$$

↑ x-coordinate of $R = -\frac{29}{3}$

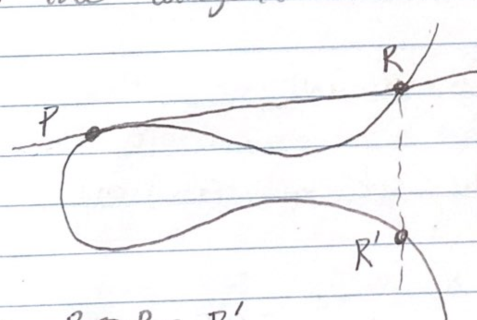
$\therefore \; Y = \frac{7}{3}\left(-\frac{29}{3}\right) - \frac{1}{3} \implies Y = \frac{170}{27}$

$R = \left(-\frac{29}{3}, \frac{170}{27}\right) \rightarrow R' = \left(-\frac{29}{3}, -\frac{170}{27}\right)$

reflect across X-axis

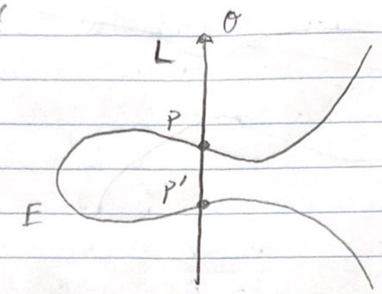
What about adding a point to itself?
- imagine sliding the point Q along the curve until it gets extremely close to point P. What happens to the line?

it becomes the tangent line at Point P



$2P = P \oplus P = R'$

What if the line between two points is vertical?
i.e, if we try to add $P=(a,b)$ to its reflection about the x-axis $P'=(a,-b)$. There is no third point of intersection!



The solution is to create an extra point $\mathcal{O}$ that lives "at infinity" ← $\mathcal{O}$ does not exist in the XY plane, rather it lies on every vertical line
We set
$$P \oplus P' = \mathcal{O}$$

We also need to know how to add $\mathcal{O}$ to an ordinary point $P=(a,b)$ on E. The line L that connects P to $\mathcal{O}$ is the vertical line through P, b/c $\mathcal{O}$ lies on vertical lines. To add P to $\mathcal{O}$, we reflect P' across the x axis which gets us back to P

Essentially, $P \oplus \mathcal{O} = P$, so $\mathcal{O}$ acts like a zero for elliptic curves addition

Definition

An elliptic curve E is the set of solutions to a Weierstrass equation
$$E: Y^2 = X^3 + AX + B$$
together with an extra point $\mathcal{O}$, where the constants A and B must satisfy
$$\boxed{4A^3 + 27B^2 \neq 0}$$

The addition law on E is defined as follows. Let P and Q be two points on E. Let L be the line connecting P & Q, or the tangent line to E at P if $P=Q$. Then the intersection of E and L consists of three points P, Q, and R, counted with appropriate multiplicities and with that $\mathcal{O}$ lies on every vertical line.

Writing $R=(a,b)$, the sum of P and Q is defined to be the reflection $R'=(a,-b)$ of R across the X-axis. The sum is denoted $P \oplus Q$ or $P+Q$

Also, if $P=(a,b)$, we denote the reflected point by $\ominus P=(a,-b)$ or simply by $-P$, and we define

$$P \ominus Q \text{ (or } P-Q)$$

as $P \oplus (\ominus Q)$

repeated addition is represented as multiplication of a point by an integer

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

what is the extra condition $4A^3+27B^2 \neq 0$?

$$\Delta_E = 4A^3+27B^2 \text{ is the discriminant of } E$$

$\Delta_E \neq 0$ is equivalent to the condition that cubic polynomial X^3+AX+B have no repeated roots

Theorem 5.5 Let E be an elliptic curve. Then the addition law on E has the following properties

abelian group

(a) $P+\mathcal{O}=\mathcal{O}+P=P$ for all $P \in E$ [Identity]

(b) $P+(-P)=\mathcal{O}$ for all $P \in E$ [Inverse]

(c) $(P+Q)+R=P+(Q+R)$ for all $P,Q,R \in E$ [Associative]

(d) $P+Q=Q+P$ for all $P,Q \in E$ [Commutative]

Theorem 5.6 (Elliptic Curve Addition Algorithm)

Let $E: Y^2 = X^3 + AX + B$

be an elliptic curve and let P_1 and P_2 be points on E

(a) If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$

(b) Otherwise, if $P_2 = \mathcal{O}$, then $P_1 + P_2 = P_1$

(c) Otherwise, write $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$

(d) If $x_1 = x_2$ and $y_1 = -y_2$, then $P_1 + P_2 = \mathcal{O}$

(e) Otherwise, define λ by

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \dfrac{3x_1^2 + A}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

and let

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{and} \quad y_3 = \lambda(x_1 - x_3) - y_1$$

Then $P_1 + P_2 = (x_3, y_3)$

Proof: Parts (a) and (b) are clear, and (d) is the case that the line through P_1, P_2 is vertical. For (e), we note that if $P_1 \neq P_2$, then λ is the slope of line through P_1 & P_2 and if $P_1 = P_2$, then λ is the slope of tangent line at $P_1 = P_2$. In either case the line L is given by the equation $Y = \lambda X + v$ with $v = y_1 - \lambda x_1$. Substituting the equation for L into the equation E gives

$$(\lambda X + v)^2 = X^3 + AX + B$$

$$\hookrightarrow \quad X^3 - \lambda^2 X^2 + (A - 2\lambda v)X + (B - v^2) = 0$$

we know that this cubic has x_1 and x_2 as two of its roots. If we calle the third root x_3, then its factors as

$$X^3 - \lambda^2 X^2 + (A\ 2\lambda v)X + (B - v^2) = (X - x_1)(X - x_2)(X - x_3)$$

If we expand this out and look at the coefficient of x^2 on each side

$$\underset{\text{coeff on left side}}{-\lambda^2} = \underbrace{-x_1 - x_2 - x_3}_{\text{coeff on right side after expanding}}$$

So now we can solve for $x_3 = \lambda^2 + x_1 - x_2$, and the Y-coordinate of the 3rd intersection point of E and L is given by $\lambda x_3 + v$. In order to get $P_1 + P_2$, we must reflect across the x-axis, which means flipping the sign of the Y-coordinate $\square$

5.2 Elliptic Curves over finite fields

In order to apply the theory of Elliptic Curves to cryptography we need to look at elliptic curves whose points have coordinate in a finite field $\mathbb{F}_p$

define an elliptic curve over $\mathbb{F}_p$ to be an equation of the form

$$E: Y^2 = X^3 + AX + B \quad \text{with } A, B \in \mathbb{F}_p \text{ satisfying } 4A^3 - 27B^2 \neq 0$$

and then we look at the points on E with coordinates in $\mathbb{F}_p$, which we denote by

$$E(\mathbb{F}_p) = \{(x,y) : x, y \in \mathbb{F}_p \text{ satisfy } y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}$$

we also require that $p \geq 3$

Consider the elliptic curve

$$E: Y^2 = X^3 + 3X + 8 \quad \text{over the field } \mathbb{F}_{13}$$

We can find the points of $E(\mathbb{F}_{13})$ by substituting in all possible values $X = 0, 1, 2, \ldots, 12$ and checking for which X values the quantity $X^3 + 3X + 8$ is a square modulo 13

for $X = 1 \rightarrow \quad 1 + 3 + 8 = 12$, 12 is a square modulo 13, and has two square roots

$$5^2 \equiv 12 \bmod 13 \quad \text{and} \quad 8^2 \equiv 12 \bmod 13$$

This gives two points $(1,5)$ and $(1,8)$ in $E(\mathbb{F}_{13})$

Continuing, we end up with

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}$$

Suppose we want to add two points P, Q in $E(\mathbb{F}_p)$ we use theorem 5.6

Theorem 5.9 Let E be an elliptic curve over $\mathbb{F}_p$ and let P and Q be points in $E(\mathbb{F}_p)$

(a) The elliptic curve addition algorithm applied to P and Q yields a point in $E(\mathbb{F}_p)$. we denote this point by $P+Q$

(b) This addition law on $E(\mathbb{F}_p)$ satisfies all of the properties listed in Theorem 5.5 i.e, this addition law makes $E(\mathbb{F}_p)$ into a finite group

Proof: The elliptic curve addition algorithm is derived from the equation for E by substituting the equation of a line & solving for X, so the resulting point has to be on E

Ex. $E: Y^2 = X^3 + 3X + 8$ over $\mathbb{F}_{13}$
add the points $P = (9,7)$ and $Q = (1,8)$ in $E(\mathbb{F}_{13})$

(e) $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1} = \dfrac{1}{-8} \equiv \dfrac{1}{5} \equiv 8 \pmod{13}$

Next we compute

$$v = y_1 - \lambda x_1 = 7 - 8 \cdot 9 = -65 = 0$$

$$x_3 = \lambda^2 - x_1 - x_2 = 64 - 9 - 1 = 54 \equiv 2 \pmod{13}$$
$$y_3 = -(\lambda x_3 + v) = -8 \cdot 2 + 0 = -16 \equiv 10 \pmod{13}$$

$$\therefore \; P + Q = (2, 10) \text{ in } E(\mathbb{F}_{13})$$

It is clear that the set of points $E(\mathbb{F}_p)$ is a finite set, since there are only finitely many possibilities for the X and Y coordinates. there are p possibilities for X, and the equation

$Y^2 = X^3 + AX + B$ shows that there are at most two possibilities for Y.
with $\mathcal{O}$ included

$\# E(\mathbb{F}_p)$ has at most $2p + 1$ points

When we plug in a value for X, there are three possibilities for the value of

$$X^3 + AX + B$$

① quadratic residue modulo p $\rightarrow$ 2 square roots and 2 points in $E(\mathbb{F}_p)$ $\approx 50\%$ of the time
② nonresidue modulo p, discard $X \rightarrow \approx 50\%$ time
③ equals 0 $\rightarrow$ one point in $E(\mathbb{F}_p) \rightarrow$ very rare

Thus we might approx

$$\# E(\mathbb{F}_p) \approx 50\% \cdot 2 \cdot p + 1 = p + 1$$

Theorem 5.11

Let E be an elliptic curve over $\mathbb{F}_p$. Then $\#E(\mathbb{F}_p) = p+1-t_p$ with t_p satisfying

$$|t_p| \leq 2\sqrt{p}$$

Definition The quantity

$$t_p = p+1 - \#E(\mathbb{F}_p)$$

is called the trace of Frobenius for $E/\mathbb{F}_p$

Ex. Let E be given by

$$E: Y^2 = X^3 + 4X + 6$$

Number of points and trace of Frobenius

p	$\#E(\mathbb{F}_p)$	t_p	$2\sqrt{p}$
3	4	0	3.46
5	8	-2	4.47
7	11	-3	5.29
11	16	-4	6.63
13	14	0	7.21
17	15	3	8.25