Elliptic Curves.

Elliptic curves are plane curves given by defining equation which (in standard form) is

$$E: F(x,y) = y^2 - (x^3 + ax + b) \text{ for } a, b \in K^\times \ (K = \mathbb{C}, \mathbb{R}, \mathbb{Q} \text{ or } \mathbb{F}_q \text{ with } q = p^n).$$

In mid 1980s Neal Koblitz and Victor Miller realized that the group law for points on elliptic curves can be effectively used for the purposes of cryptography.

Rmk. The presence of the group structure on E was noticed long before that. The first rigorous treatment (or verification) of the group law on elliptic curves appeared in a paper of H. Poincare dating back to 1901.

The subject of Elliptic Curves over $\mathbb{C}$ is arguably one of the most fascinating in Number Theory, if not mathematics in general. However to treat it properly would require a solid background in Complex Analysis and take us too far away from our 'crypto route'.

We will focus on elliptic curves over $\mathbb{R}$ and finite fields $\mathbb{F}_q$ ($q = p^n$, mostly, $q = p$, $p >> 0$).

Important agreement. If K is a finite field ($K = \mathbb{F}_q$, $q = p^n$), we assume char $K = p \neq 2, 3$ to avoid extra technicalities.

Def-n. A point $p \in E$ is called smooth if $p = (x, y)$ is not a sol-n of the system

$$\begin{cases} F'_x(x,y) = 0 \\ F'_y(x,y) = 0 . \end{cases} \quad (\star)$$

In other words, the partial derivatives of the defining eq-n of E do not simultaneously vanish at P.

Using that $F(x,y) = y^2 - (x^3 + ax + b)$, we simplify $(\star)$ into

$$\begin{cases} -(3x^2 + a) \\ y = 0 \end{cases} \Leftrightarrow \begin{cases} f'(x) = 0 \\ f(x) = 0 \end{cases}, \text{ where}$$

$f(x) = x^3 + ax + b$.

Prop-n. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ be a polynomial. The following 2 conditions are equivalent:

(1) $f(x)$ has a multiple zero c.

(2) $f(c) = f'(c) = 0$.

Proof. $f(c)=0 \underset{\uparrow \atop \text{Bezout's theorem}}{\Longleftrightarrow} f(x)=(x-c)g(x)$, hence, $f'(x)=-cg(x)+$ $+(x-c)g'(x)$ and

$f'(c)=0 \Longleftrightarrow g(c)=0 \Longleftrightarrow f(x)=(x-c)^2 \cdot h(x)$ ▨

Def-n. Let $f(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_0$ be a polynomial and $\{x_1,\dots,x_n\}$ the (not necessarily distinct) roots of $f(x)$. The *discriminant* of $f(x)$ is the function

$$D_f=\prod_{1\le i<j}(x_i-x_j)^2.$$

Rmk: $D_f=0 \Longleftrightarrow f(x)$ has multiple roots.

Example. $P(x)=x^2+bx+c$ (quadratic polynomial).

Then $D_P=(x_1-x_2)^2=b^2-4c$.

Exercise. Derive this formula using that

$P(x)=(x-x_1)(x-x_2)$ (Bezout's thm), so

$$\begin{cases} b=-(x_1+x_2) \\ c=x_1x_2. \end{cases}$$

Much more annoying exercise (but everyone with 'poisonous' enough poise for math should do it).

$$P(x)=x^3+ax+b.$$

(1) Using that $P(x)=(x-x_1)(x-x_2)(x-x_3)$, show that

$$\begin{cases} x_1+x_2+x_3=0 \\ x_1x_2+x_1x_3+x_2x_3=a \\ x_1x_2x_3=-b. \end{cases}$$

(2) Derive that $D_p=4a^3+27b^2$.

<u>Rmk.</u> For 'technical reasons' the formula $D_p=-16(4a^3+27b^2)$ is usually used, the factor of -16 does not change the vanishing locus of D_p.

The following statement is obvious and concludes the discussion.

<u>Obvious lemma.</u> $D_{f_E}\neq 0 \iff E$ is smooth, where $f_E=x^3+ax+b$ is the defining polynomial of E.

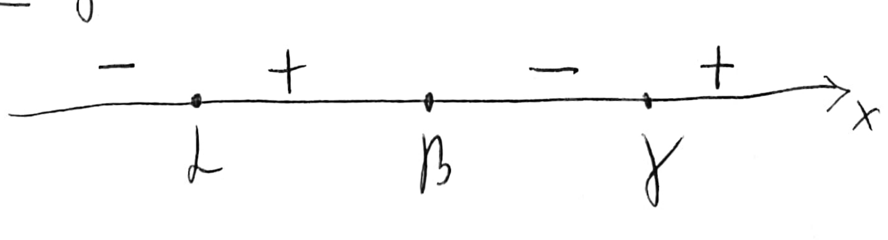
<u>$K=\mathbb{R}$.</u>

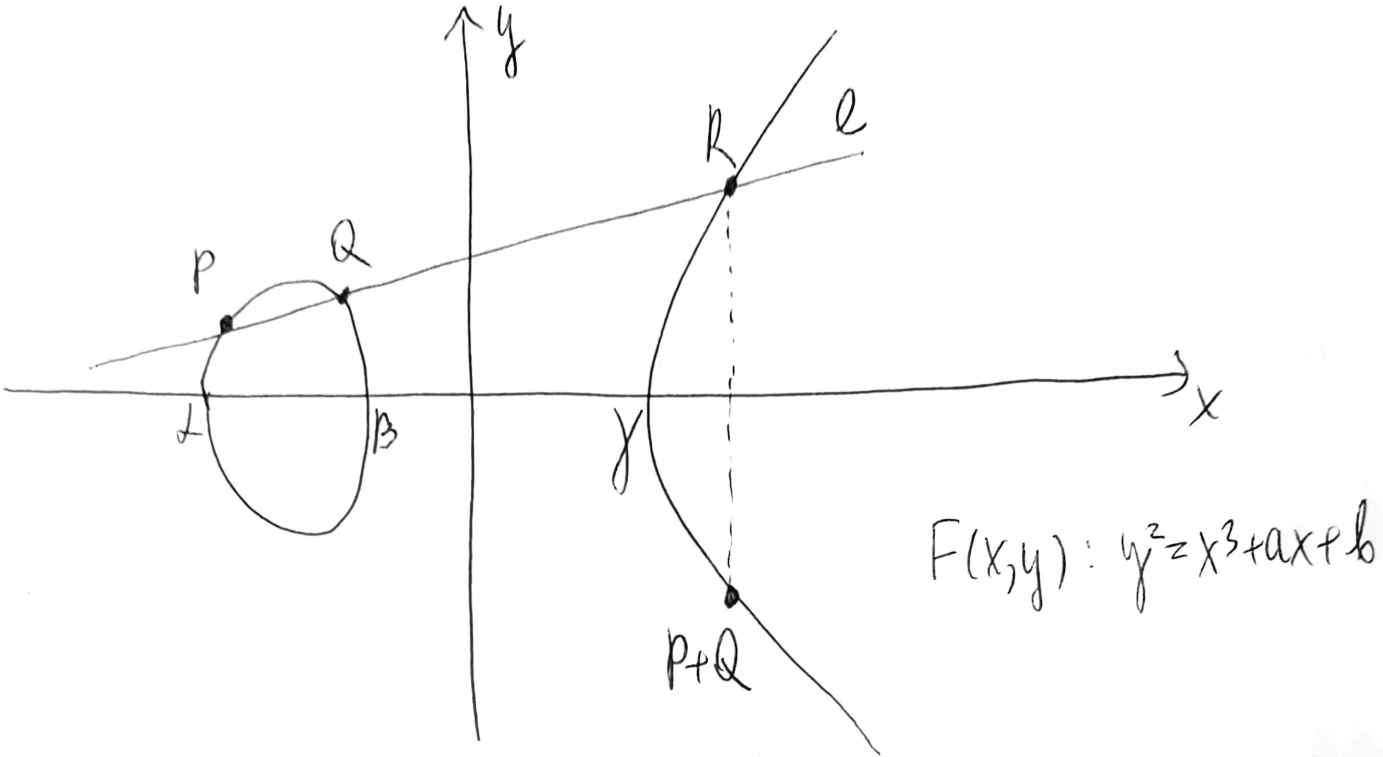
Consider a smooth elliptic curve E over $\mathbb{R}$ given by $y^2=(x-\alpha)(x-\beta)(x-\gamma)$ with $\alpha<\beta<\gamma\in\mathbb{R}$.

First we sketch the graph of E.

<u>Domain:</u> $y^2\geq 0$, so we must have $(x-\alpha)(x-\beta)(x-\gamma)\geq 0$

$x\in[\alpha,\beta]\cup[\gamma,\infty)$





Rmk. The graph of the correspondence $F(x,y)$ is symmetric w.r.t. the x-axis. It is not a f-n, as many values of x correspond to two values of y.

Group Law.

Idea: take two points $P \neq Q$ on E and draw a line l through them. The intersection $l \cap E$ is given by the zeros of the restr-n of $F(x,y)$ to l, which is a cubic polynomial in x. Concretely, l is given by an equation $y = mx + c$ (the case of ~~horiz~~ vertical lines will be treated separately). Then $l \cap E$ = zeros of $F(x,y)|_l = \{(x,y) \in \mathbb{R} \mid (mx+c)^2 = x^3 + ax + b\}$. Moreover, P and $Q \in l \cap E$, thus the x-coordinates of P and Q are zeros of $g(x)=x^3+ax+b-(mx+c)^2$ and dividing $g(x)$ by $(x-P_x)(x-Q_x)$, we obtain the x-coordinate of the third point of intersection. Let this point be $R=(R_x,R_y)$ (to find R_y simply plug R_x into $y^2=x^3+ax+b$, use that $R\in\ell$ to choose the right value of R_y).

Finally, define $P\oplus Q$ to be the point $\widetilde{R}=(R_x,-R_y)$, the reflection of R w.r.t. the x-axis.

Rmk. Clearly $P\oplus Q=Q\oplus P$.

But wait... What about (0) identity?

(1) inverses??

(2) $P\oplus P$???

Answers:

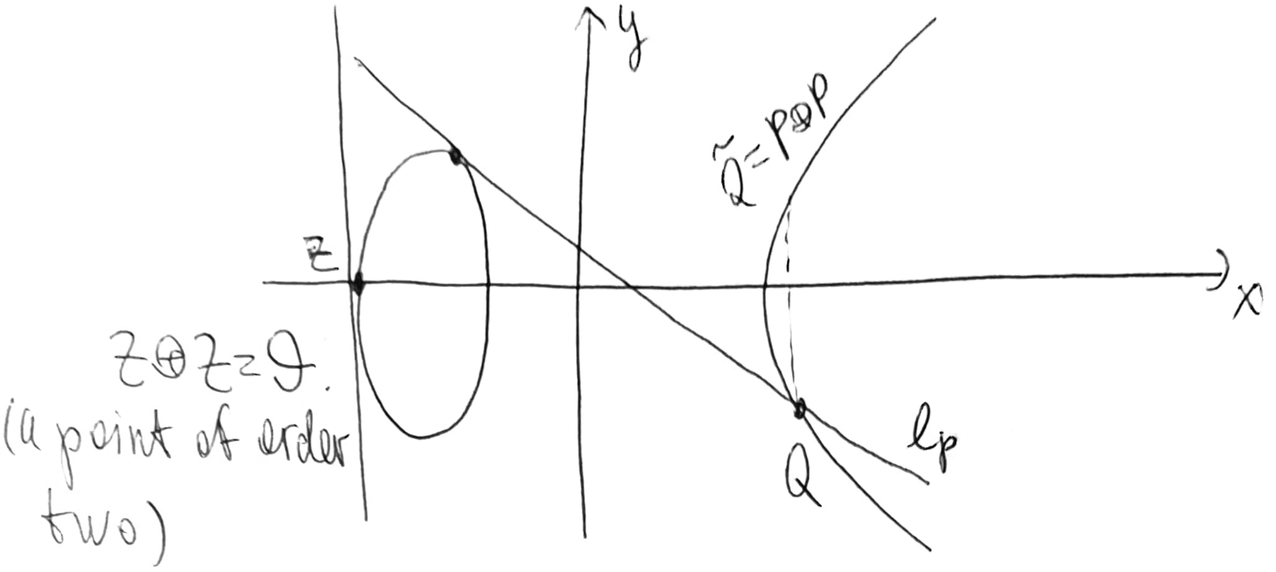
(0) Let's just artificially add the point at infinity ϑ and impose the rules: $\vartheta\oplus P=P\oplus\vartheta=P$ for any $P\in E$.

Rmk. Of course there is a way to get rid of the artificialness. Interested? Check out the 'Take-Home exam'.

(1) The inverse of a point $P\in E$ is the point Q on the vertical line through P: $Q=(P_x,-P_y)$.

Rmk. In case $P_y=0$, we get $P\oplus P=\vartheta$, so P has order 2.

(2) Draw a tangent line ℓ_P through P to E. Then ℓ_P will intersect E in one more point $Q=(Q_x,Q_y)$. Set $P\oplus P=\widetilde{Q}=(Q_x,-Q_y)$



Concrete formulas for the group operation.

Let's derive the actual formulas.

Step 1. Find the equation of the line l through $\underset{(P_x,P_y)}{\underset{\shortparallel}{P}}$ and $\underset{(Q_x,Q_y)}{\underset{\shortparallel}{Q}} \in E$.

$$l: y - y_P = \frac{y_Q - y_P}{x_Q - x_P} \cdot (x - x_P)$$, so l is given by

$y = mx + c$ with $m = \frac{y_Q - y_P}{x_Q - x_P}$, $c = y_P - m x_P$.

Step 2. Restrict the defining equation of E to l in order to find the x-coordinate of the third point of intersection $l \cap E$. (x_R)

$$g(x) := F(x,y)\big|_l = (mx+c)^2 - (x^3 + ax + b) =$$
$$= x^3 - m^2 x^2 + (a - 2mc)x + (b - c^2).$$

Notice that as P and $Q \in E \cap \ell$, we have $g(x_p)=g(x_q)=0$. Moreover, $x_p+x_q+x_R=m^2$ (Vieta's thm).

$$x_R=m^2-x_p-x_q.$$

<u>Step 3.</u> Find the y-coordinate of the third point of intersection $\ell \cap E$: $y_R=mx_R+C=m(m^2-x_p-x_q)+y_p-mx_p=$

$$=y_p+m(x_R-x_p).$$

<u>Step 4.</u> $P \oplus Q=(x_R,-y_R)=(m^2-x_p-x_q;-y_p-m(x_R-x_p))$.

<u>Exercise.</u> Derive the formula for $P\oplus P$, following exactly the same logic: draw the line ℓ_p', tangent to E at P, find the third point of intersection $\ell_p \cap E$. Notice that x_p will be a root of multiplicity two (of $g(x)=F(x,y)|_{\ell_p}$).

$$P\oplus P=(\underbrace{m^2-2x_p}_{\overset{\shortparallel}{x_R}};-y_p-m(x_R-x_p)) \text{ with } m=\frac{3x_p^2+a}{2y_p}.$$

<u>Rmk.</u> Looking at the formula for m above, you might guess why we would like to avoid the cases char p=2,3. Other than these two cases, the formulas for the group law derived above make perfect sense over finite fields! The pictures are quiet messy, though.

Elliptic curves over $K=\mathbb{F}_p$.

Let $K=\mathbb{F}_p$, $p\neq 2,3$. The 'graphs' get really awkward, but the formulas for the group law work just fine over $\mathbb{F}_p$!

Example. Consider the elliptic curve E given by the defining equation $y^2=x^3+x-3$ over the field $\mathbb{F}_5$.

First we check that $D_f\neq 0$: $4\cdot 1^3+27\cdot 3^2=4+243=247\equiv 2\neq 0$ ✓

Now let's find the points on E:

$x=0$: $y^2=-3\equiv 2$ - not a square ✗

$x=1$: $y^2=1+1-3\equiv 4$ - a square ⇝ points $(1,2)$ and $(1,3)$.

$x=2$: $y^2=8+2-3\equiv 2$ - not a square ✗

$x=3$: $y^2=27+3-3\equiv 2$ - not a square ✗

$x=4$: $y^2\equiv(-1)^3-1-3\equiv 0$ ⇝ point $(4,0)$.

Points (el-ts of $G(E)$): $\underset{\substack{\uparrow\\ \text{identity}}}{\mathcal{O}}$, $(4,0)$, $(1,2)$, $(1,3)$.

Rmk. The points $(1,2)$ and $(1,3)$ lie on a vertical line (have the same x-coordinate), hence $(1,2)\oplus(1,3)=\mathcal{O}$

The point $(4,0)$ lies on the x-axis, so it has order 2:
$(4,0)\oplus(4,0)=\mathcal{O}$.

Q: Which abelian group did we get?
Well, $|G(E)|=4$, so $G(E)$ must be $\mathbb{Z}_4$ or $\mathbb{Z}_2\times\mathbb{Z}_2$.
We also know that $(4,0)$ is an element of order 2.
Let's find $(1,2)\oplus(1,2)$. If $(1,2)\oplus(1,2)=\vartheta$, then $G(E)\simeq\mathbb{Z}_2\times\mathbb{Z}_2$, while $G(E)\simeq\mathbb{Z}_4$ otherwise.

Rmk. As the y-coordinate is not zero, $(1,2)\oplus(1,2)\neq\vartheta$, but, to practice withe the formulas, we will still find $(1,2)\oplus(1,2)=R=(x_R,y_R)$

$$m=\frac{3x_p^2+a}{2y_p}=\frac{3+1}{4}\equiv 1.$$

$$x_R=m^2-2x_p=1-2\cdot 1=-1\equiv 4$$

$$y_R=y_p+m(x_R-x_p)=2+1\cdot(4-1)\equiv 0.$$

$(1,2)\oplus(2,1)=(4,0)$ and $G(E)\simeq\mathbb{Z}_4$.

Here is an interesting question.

Q: How many points are there on E over $\mathbb{F}_q$?

Thm (Hasse). Let E be an elliptic curve over $\mathbb{F}_q$. The number of points on E satisfies the inequality

$$q+1-2\sqrt{q}\leq N\leq q+1+2\sqrt{q}.$$

Example. For $E/\mathbb{F}_5$ Hasse's thm asserts

$$5+1-2\sqrt{5} \leq N \leq 5+1+2\sqrt{5} \text{ or } 2 \leq N \leq 10.$$

Notice that $N=4$ satisfies the inequalities, so our answer is consistent with the theorem.