Let K be a field of characteristic $\neq 2,3$ and let the polynomial x^3+ax+b (where $a, b \in K$) has no multiple roots (equivalent to the condition $4a^3+27 \cdot b^2 \neq 0$).

An elliptic curve over K is the set of points (x,y) with $x, y \in K$ such that:

(1) $\underline{y^2 = x^3+ax+b}$

short Weierstrass form

complete Weierstrass equation:

$$y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$$

$a_i \in K$

together with a single element $\mathcal{O}$ called the "~~point~~ zero at infinity".

$$E_{a,b}(K) = \{(x,y) : x, y \in K \wedge y^2 = x^3+ax+b \text{ where } a, b \in K\} \cup \{\mathcal{O}\}$$

Note that if $(x,y) \in E_{a,b}(K)$ then $(x,-y) \in E_{a,b}(K)$

To belong to $E_{a,b}(K)$ the point (x,y) must give X^3+aX+b being a square in K.

That is $\exists \alpha \in K$ such that

$$\alpha^2 = (X^3+aX+b)$$

For a finite field K we have (char $K \neq 2$)

0 is a square,

and half of the elements in $K \setminus \{0\}$ are the squares.

$K \setminus \{0\} = K^*$

For each finite field K^* is cyclic!

which means that

$\exists g \in K^*$ such that

$\langle g \rangle = K^*$.

$$\{g^0, g^1, g^2, \dots, g^{(\operatorname{ord} g)-1}\}$$

$g^0 = 1$

$g^{\operatorname{ord} g} = 1 = g^0$

$\langle g \rangle = K^* \Rightarrow \operatorname{ord} g = |K^*|$

So even powers of a generator are squares.

Odd powers of a generator are not squares (Why?)

If $\operatorname{char}(K) \neq 2$.

$|K|$ - odd number

$|K^*| = |K \setminus \{0\}|$ - even number

$$\dots, g^2, g^4, g^6, \dots, g^{|K^*|}$$

those elements are squares

$g^{|K^*|} = g^0$

square roots

$$g^1, g^2, g^3, \dots, g^{|K^*|/2}$$

$$-g^1, -g^2, -g^3, \dots, -g^{|K^*|/2}$$

$|K^*|/2$ ~~elements~~ we pointed elements having square roots

Let us consider the mapping

$$h(x) = x^2 \quad \text{in } K^*$$

It is easy to see that h is homomorphism

$\operatorname{Im}(h)$ are elements being the squares in K^*, $\operatorname{Ker}(h) = \{1, -1\}$

$x^2 - 1 \Rightarrow x^2 = 1$

From the first theorem of isomorphism

$$\mathrm{Im}(h) \cong K^*/\ker(h)$$

$$|\mathrm{Im}(h)| = \frac{|K^*|}{|\ker(h)|} = \frac{|K^*|}{2}$$

So there are no more than $\frac{|K^*|}{2}$ elements in K^* that have square roots.

$$X^3+aX+b \in K$$

$$x \in K$$

$$X^3+aX+b \in K^*$$

x if is not ~~an element~~ ~~being~~ a square

then $(x,\_) \notin E_{a,b}(K)$

K-finite:

$$\#E_{a,b}(K) = |E_{a,b}(K)| \leq 2\cdot|K|+1$$

$\cancel{\leq 2|K|+1}$

Hasse theorem:

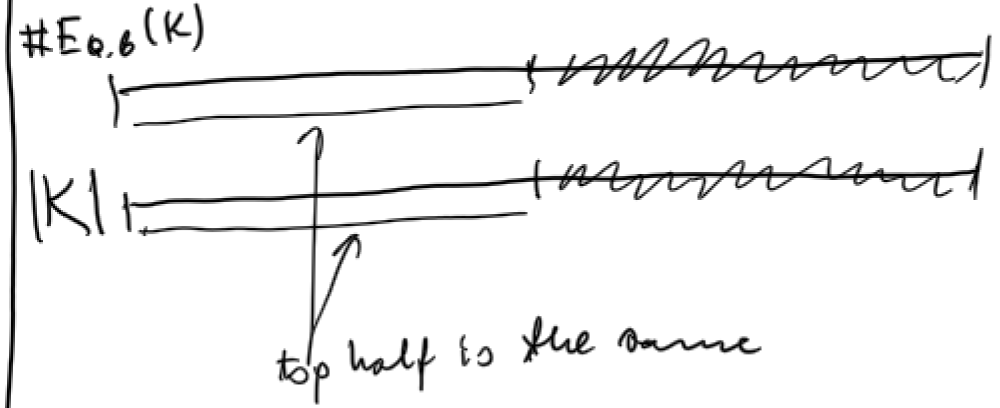
$K = \mathbb{F}_{p^r} \quad r \geq 1, p > 3$

$$(\sqrt{|K|}-1)^2 \leq \#E_{a,b}(K) \leq (\sqrt{|K|}+1)^2$$

$$|K| - 2\sqrt{|K|} + 1 \leq \#E_{a,b}(K) \leq |K| + 2\sqrt{|K|} + 1$$

length of the interval

$4\sqrt{|K|} \quad \} \; 2\sqrt{|K|}+1$



$(E_{a,b}(K), +)$ forms an abelian group.

special operation

"point addition" defined below.

Define $\underbrace{P+Q}$, $-P$:

two cases: (1) $P+Q$ $\quad P, Q$ are different

(2) $P+P$

$\underline{-P}$: if $P=\Theta$ then $-P=\Theta$

otherwise $P=(x,y)$ and

$-P=(x,-y)$ see that

if $P\in E_{a,b}(K)$

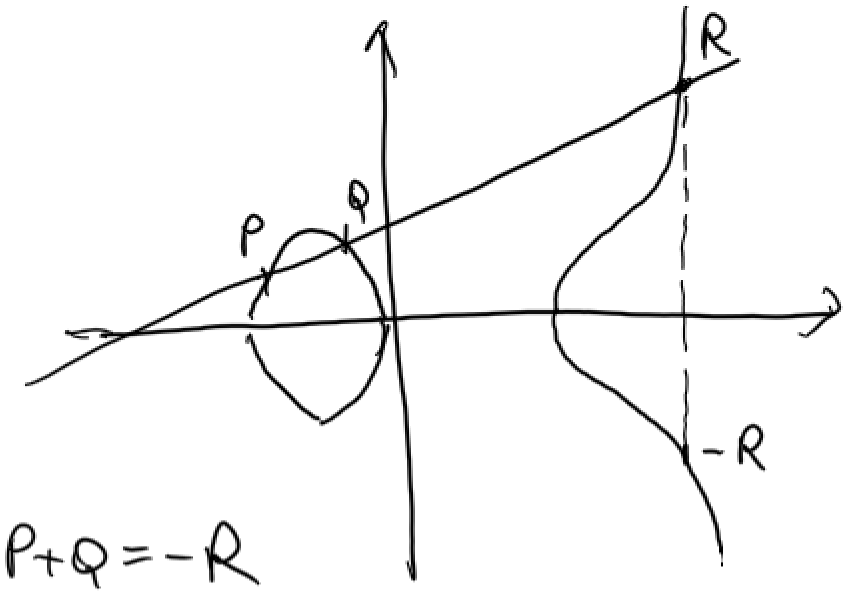
then $-P\in E_{a,b}(K)$.

(1) $P+Q$, P, Q are different.

Let $P=(x_1,y_1)$

$Q=(x_2,y_2)$

if $K=\mathbb{R}$ we can represent the process graphically:



$P+Q=-R$

Let generalize the picture also for the case of ~~K~~ a finite field.

$x_1=x_2$, but $y_1\neq y_2$

From the curve definition we have that

$y_2=-y_1$ (the only option)

because Y^2-A has no more than two roots.

$\underline{A=x_1^3+ax_1+b}$

Hence $Q=-P$

$P+(-P)\equiv\Theta$

$x_1 \neq x_2$

Let $l: y = \alpha x + \beta$ be a "straight line" passing through the points P and Q.

So P, Q satisfy the line equation:

$$\begin{cases} y_1 = \alpha x_1 + \beta \\ y_2 = \alpha x_2 + \beta \end{cases}$$

$$y_2 - y_1 = \alpha(x_1 - x_2)$$

$$\alpha = \frac{y_2 - y_1}{x_2 - x_1} \qquad \beta = y_1 - \alpha x_1 = = y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1$$

note that $x_1 \neq x_2$

Any point (x, y) of the straight line l belongs to E iff

$$(\alpha X + \beta)^2 = X^3 + aX + b$$

$$\underbrace{X^3 - (\alpha X + \beta)^2 + aX + b}_{P(X)} = 0$$

$P(X)$ we know that this polynomial of degree 3 has at least two different roots x_1, x_2.

$$P(X) = (X - x_1)(X - x_2)\underline{\qquad}$$

it must be a linear factor in $K[X]$

So $P(X)$ must have also a third root: x_3.

$$P(X) = (X - x_1)(X - x_2)(X - x_3) =$$

$$= X^3 - (x_1 + x_2 + x_3)X^2 + \dots$$

From Viète's formulas we learn:

$$x_1 + x_2 + x_3 = \alpha^2$$

$$x_3 = \alpha^2 - (x_1 + x_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2$$

$$y_3 = -(\beta + \alpha x_3) = -\left[y_1 - \frac{y_2 - y_1}{x_2 - x_1} \cdot x_1 + \frac{y_2 - y_1}{x_2 - x_1} \cdot x_3\right]$$