$$\begin{cases} x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)\cdot(x_1-x_3) \end{cases}$$

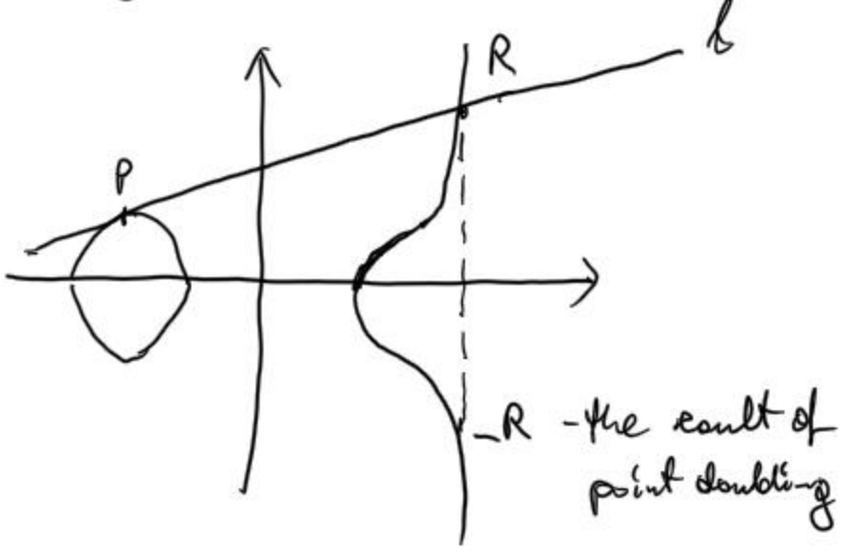
---

(2) $P=Q$,

if $y_1=0$ then $P=-P$, hence $2P=\mathcal{O}$

Let $\underline{y_1 \neq 0}$:

If $K=\mathbb{R}$ we can represent the situation graphically



To generalize this to the discrete case consider the line

$l: y = \alpha x + \beta$

$P \in l$, $P \in E$ so x_1 satisfies $\{P=(x_1,y_1)$

$$(**) \quad (\alpha x+\beta)^2 - (x^3+ax+b) = 0$$

However, since $P=Q$, x_1 is a double root of $(**)$, which means that x_1 is also a root of the formal derivative of $(**)$:

$$2(\alpha x+\beta)\cdot\alpha - 3x^2 - a = 0$$

That is

$$2\alpha y_1 - 3x_1^2 - a = 0 \Rightarrow \alpha = \frac{3x_1^2+a}{2y_1}$$

$$\begin{cases} x_3 = \alpha^2 - 2x_1 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -(\beta+\alpha x_3) = -y_1 + \left(\frac{3x_1^2+a}{2y_1}\right)\cdot(x_1-x_3) \end{cases}$$

DLP in $E_{a,b}(K)$:

define: $Y = s\cdot P = \underbrace{P+\ldots+P}_{s}$

DLP problem on $E_{a,b}(K)$:

Given a pair of points (Y, P), such that $Y \in \langle P \rangle$ find s, such that

$$Y = s \cdot P$$

For correctly chosen $E_{a,b}$ and P the DLP on E is hard.

Given s, P how to efficiently calculate

$$Y = s \cdot P \ ?$$

Double-and-add method:

P, $s = (11)_{10} = (1011)_2 = (1011)_2$ ($2^3\,2^2\,2^1\,2^0$)

$(1011)_2$

R – let it means "result"

$R := P$ $\quad R = (1)_2 \cdot P$

$(1011)_2$

$R := 2R = 2 \cdot (1)_2 P = (10)_2 P$

$(1011)_2$

$R := 2R = 2 \cdot (10)_2 P = (100)_2 P$

$R := R + P = (100)_2 \cdot P + (001)_2 \cdot P =$

$= (101)_2 P$

$(1011)_2$

$R := 2 \cdot R = 2 \cdot (101)_2 P = (1010)_2 P$

$R := R + P = (1010)_2 P + (0001)_2 \cdot P =$

$= (1011)_2 \cdot P$

return R

Point compression:

Note that for a given x we have at most two y satisfying:

$$(***) \quad y^2 = \underbrace{x^3 + ax + b}_{A}$$

$$y^2 - A = 0$$

For simplicity consider the case $K = \mathbb{F}_p$:

$$y, -y = p - y$$

if RHS of (***) is nonzero then only one number y, $p-y$ is even and only one is odd.

So to fully determine (x,y) it suffices to transfer x and the information about the value of the parity bit (lsb) of y.

Indeed, transmission and storage of the uncompressed encoding of $P = (x,y)$ is

$$C \| X \| Y, \text{ where}$$

$$C = 0_x 04$$

Whereas the compressed encoding is

$$C \| X \text{ where}$$

$$C = 0_x 02 \text{ if } lsb(Y) = 0$$

$$C = 0_x 03 \text{ if } lsb(Y) = 1$$

To decompress the point we have to calculate square roots $z, p-z$ from $x^3 + ax + b$ and take the one having the required lsb.

Square root algorithm for $\mathbb{F}_p^*$:

Preliminaries: $|\mathbb{F}_p^*| = p - 1$

See Neal Koblitz A Course in Number Theory and Cryptography Sec. Ed. pages 48-49

- for any $a \in G$, G - is a finite abelian group

  $\text{ord}\, a \mid |G|$

- $\mathbb{F}_p^*$ is cyclic, that is $\exists g \in \mathbb{F}_p^*$ such that $\langle g \rangle = \mathbb{F}_p^*$,

  so in other words:

$$\forall a \in \mathbb{F}_p^* \ \exists k \in \{0, 1, \ldots, (\text{ord}\, g) - 1\}$$
$$a = g^k \pmod p$$

- Quadratic residues: $a \in \mathbb{F}_p^*$ is a quadratic residue if $\exists x \in \mathbb{F}_p^*$ such that

$$a = x^2 \pmod p.$$

The x above is some power of the generator g of $\mathbb{F}_p^*$, that is $x = g^{\ell} \pmod p$,

the order of g is even (equal to $p-1$)

so:

$$a = g^{2\ell} \pmod p \equiv g^{2\ell \,(\text{mod } p-1)} \pmod p$$

$$= g^{2\ell - u(p-1)} \pmod p$$

even number $\in \{0, 1, \ldots, p-2\}$ — $p-1$ values

$u = 0$ if $2\ell < p-1$

$u = 1$ if $2\ell \geq p-1$

So it is easy to see that a is a quadratic residue iff a is an even power of some generator.