⊙ $(f \cap g)_p \geq m_p(f) m_p(g)$

$p = (0,0)$

$f(x,y) = f_{m_f} + f_{m_f+1} + \cdots$

$= x^{m_f} p_{m_f}(x) + x^{m_f-1} p_{m_f-1}(x) y + \cdots$

$$R_{f,g}(x) = \pm \det \begin{bmatrix} x^{m_f} p_{m_f} & x^{m_f-1} p_{m_f-1} & \cdots \\ 0 & x^{m_f} p_{m_f} & \cdots \\ & \vdots & \end{bmatrix}$$

$\rightarrow x^{m_f m_g} \mid R_{f,g}$

Criptography

a b c d

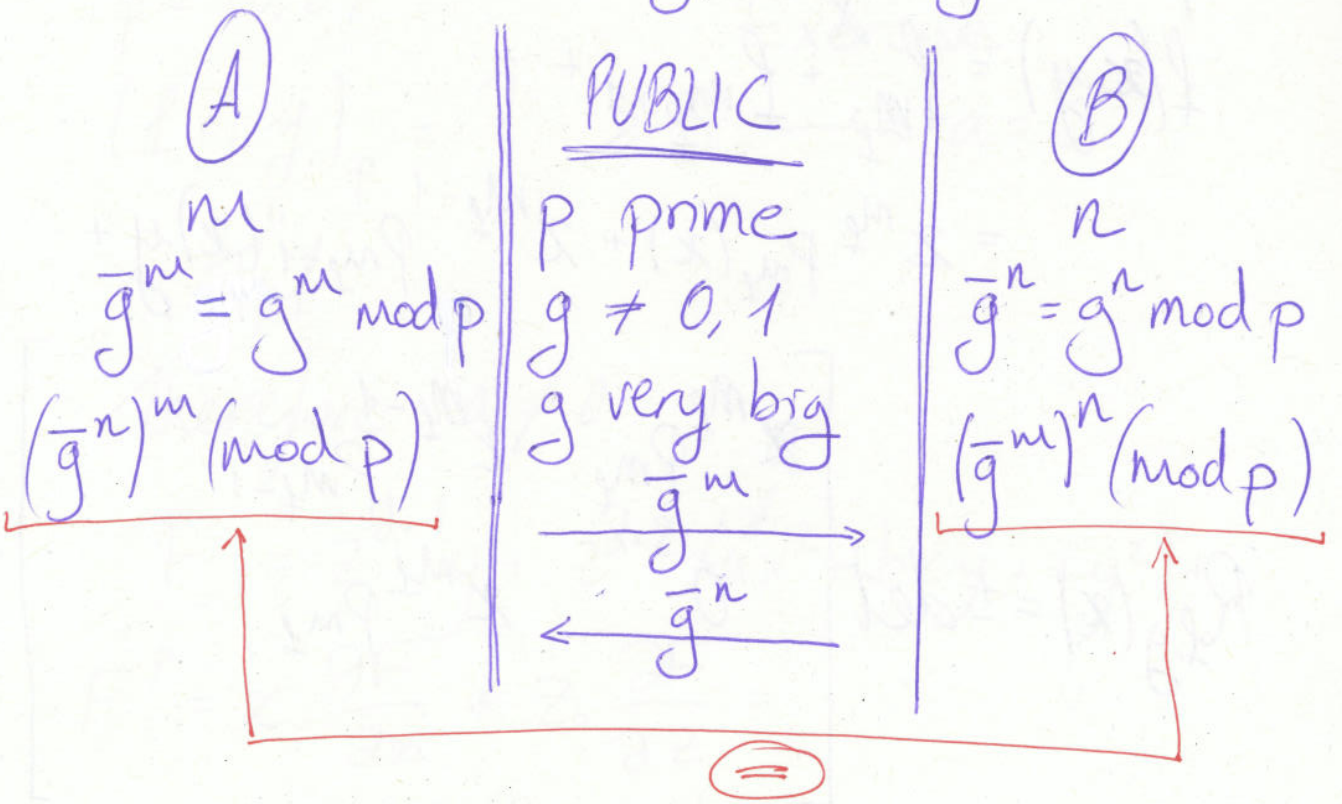
↓ ↓ ↓ ↓

d e f ...

easily solved

Public Key:

Diffie-Hellman key exchange method



$g \cdot g^m \xrightarrow{\log} m$

Discrete logarithm problem

When we choose p prime we have

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, $G = \mathbb{F}_p \setminus \{0\}$

G is a group with multiplication

(A) PUBLIC (B)

G finite group

$g \in G \setminus \{1\}$

m $\qquad$ n

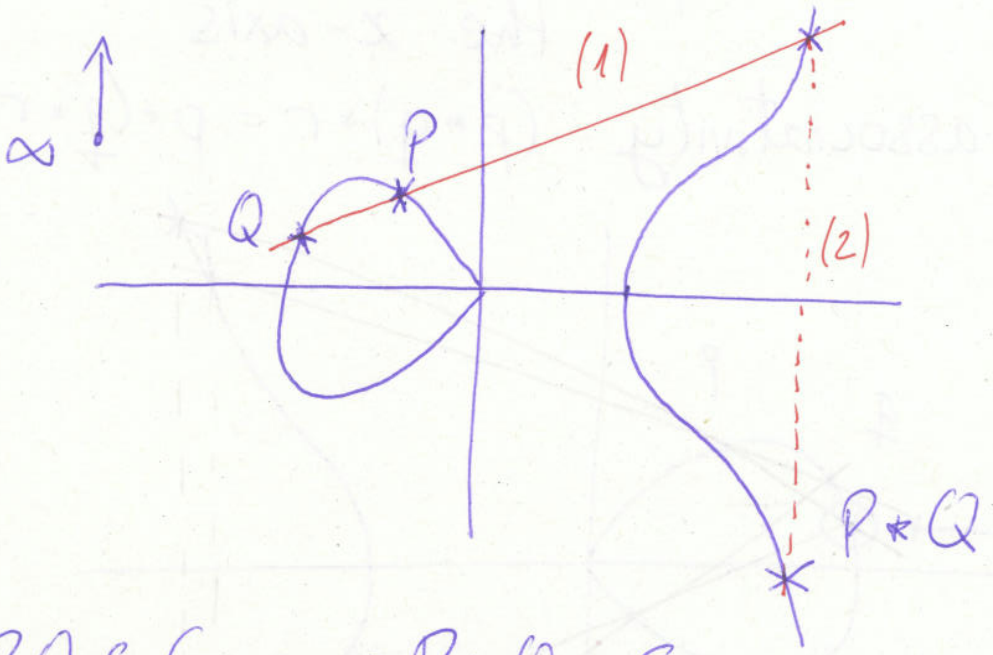
$x = (g^n)^m$ $\qquad$ $x = (g^m)^n$

$G \uparrow$ $\qquad$ $\xrightarrow{\quad g^m \quad}$ $\qquad$ $\xleftarrow{\quad g^n \quad}$

$F(x,y,z) = y^2z - x^3 + xz^2 \in \mathbb{F}_p[\mathbb{P}^2]$

elliptic curve $\qquad$ $\mathbb{F}_p\mathbb{P}^2$

We will define a group structure on this curve



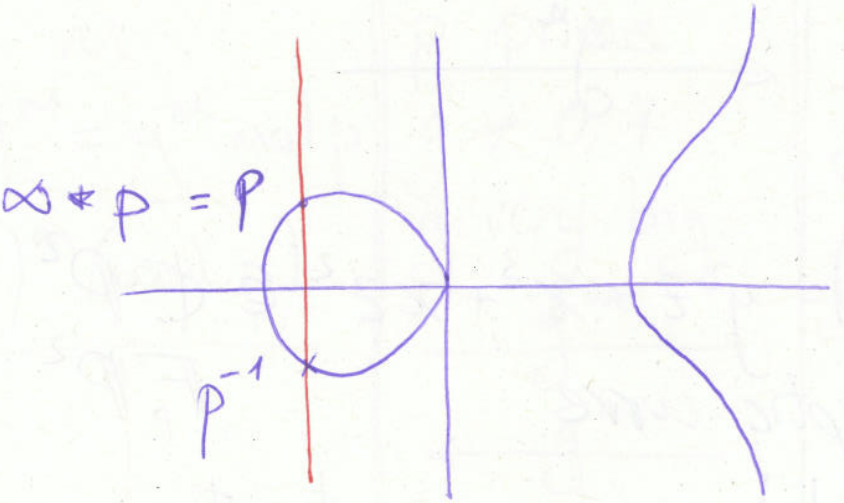
$P, Q \in C \rightsquigarrow P * Q \in C$

If $P = Q$ take the tangent

- Check that $(C, *)$ is a (commutative) group:

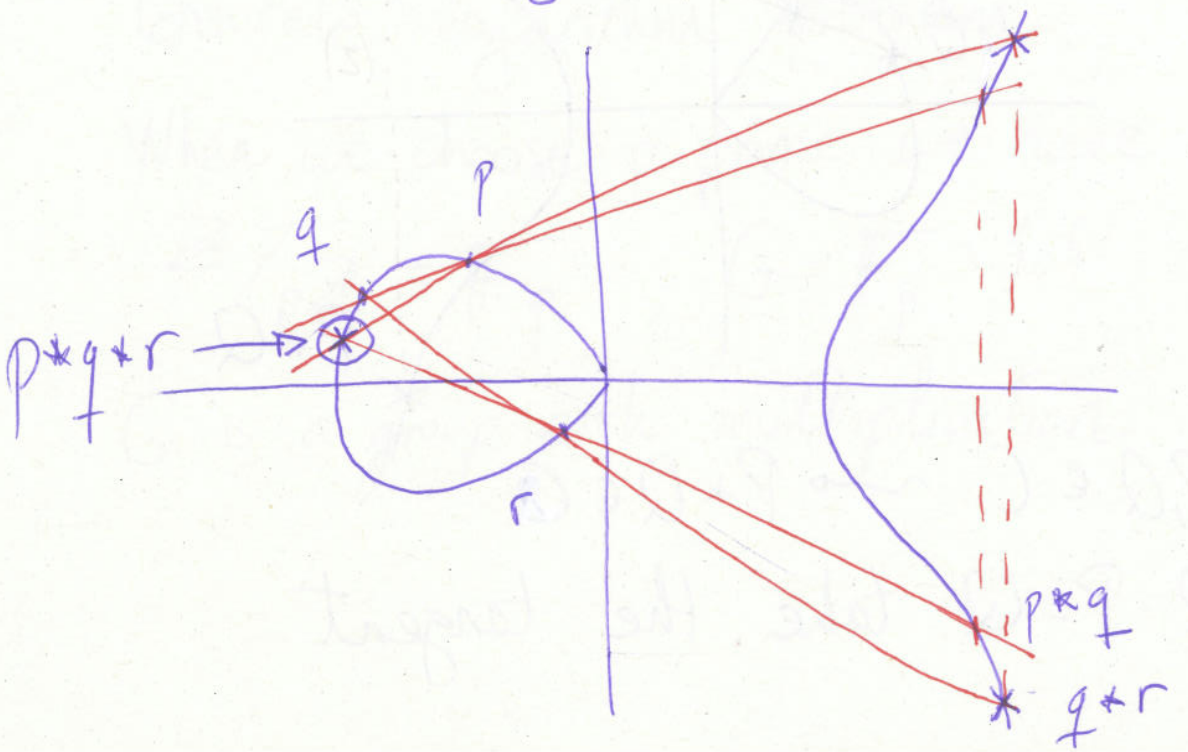
→ identity $1 * P = P$

$\underline{1 = \infty}$



→ inverse: P^{-1} = reflexion of P in the x-axis

→ associativity: $(P * Q) * R = P * (Q * R)$



References:

Fischer: plane algebraic curves

Vainsencher:

=

Fulton