CIS 3362 11/16/22

Quizzes Returned Fri (11/18) (11/18)
Com Serv Due Fri IN CLASS @ BEGINNING!

Next 3 LEC: Elliptic Curve Cryptography

before: RSA, El Gamal

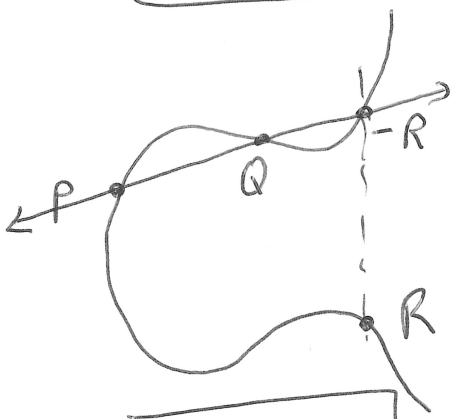
GOAL: faster Public Key Scheme?

TODAY: Define Elliptic Curves

gen $y^2 + axy + by = x^3 + cx^2 + dx + e$

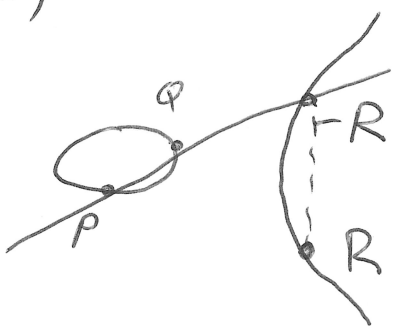
SIMPLIFY $\boxed{y^2 = x^3 + ax + b}$

real #s



$\boxed{P + Q = R}$

usually



People defined "adding points on elliptic curves" like so.

(1) Draw line through pts P, Q. Hit curve 3rd pts called $-R$.

(2) reflect $-R$ over x-axis to pt R on curve.
This is Pt Q,

For crypto, we will do

$$y^2 = (x^3 + ax + b) \bmod p$$

where $p \in$ Prime (x, y) are ~~values~~ integers in range $[0, p-1]$ and a and b are as well. (Note $-y \equiv p - y \pmod p$)

For curve to be valid $4a^3 + 27b^2 \not\equiv 0 \pmod p$

Addition Rules

Pts will form an Abelian group

1) Define a pt O, Origin, (no coordinates), but for all $P \in$ Curve $P + O = P$.

2) If $P = (x, y)$ then $-P = (x, -y)$ → $p - y$
$P + (-P) = O$

3) Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$
Define $P + Q = R$, $R = (x_R, y_R)$

(slope) $$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \bmod p \quad \text{if} \quad \begin{matrix} P \neq Q \\ Q \neq -P \end{matrix}$$

$$\lambda = \frac{3x_P^2 + a}{2y_P} \bmod p \quad \text{if} \quad P = Q$$

$$y^2 = x^3 + ax + b$$
$$2yy' = 3x^2 + a \quad \rightarrow \quad y' = \frac{3x^2 + a}{2y}$$

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$

$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

function $y^2 = x^3 + ax + b \bmod p$ $E_p(a,b)$

1st example $E_{23}(1,1)$ $y^2 = (x^3 + x + 1) \bmod 23$

$P = (3,10)$ $Q = (9,7)$

$$\lambda = \frac{7-10}{9-3} = \frac{-3}{6} = \frac{-1}{2} \bmod 23$$

$$= -(2^{-1}) \bmod 23$$

$$\equiv -12 \equiv 11 \bmod 23$$

$$x_R = (\lambda^2 - x_P - x_Q) = (11^2 - 3 - 9) = 109 \equiv 17 \bmod 23$$

-92

$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

$$= (11(3-17) - 10) \bmod 23$$

$$\equiv (11 \times 9 - 10) \equiv 89 \equiv 20 \bmod 23$$

$$(3,10) + (9,7) = (17,20)$$

$P = (3,10)$ Calculate $2P$

$$\lambda = \frac{3x_P^2 + a}{2y_P} = \frac{3(3)^2 + 1}{2(10)}$$

$$= \frac{28}{20} = \frac{7}{5} \equiv 7(5^{-1} \bmod 23)$$

$$\equiv 7(-9) \equiv -63 \equiv 6 \bmod 23$$

$23 = 4 \times 5 + 3$

$5 = 3 + 2$

$3 = 2 + 1$

$3 - 2 = 1$

$3 - (5-3) = 1$

$2 \times 3 - 5 = 1$

$2(23 - 4 \times 5) - 5 = 1$

$2 \times 23 - 9 \times 5 = 1$

$$x_R = (\lambda^2 - x_p - x_p) = (6^2 - 3 - 3)$$
$$= 30 \mod 23$$
$$\equiv \boxed{7}$$

$$y_R = (\lambda(x_p - x_R) - y_p) \mod p$$
$$= (6(3-7) - 10) \mod p$$
$$= -24 - 10 \mod 23$$
$$= -34 \mod 23$$
$$\equiv \boxed{12 \mod 23}$$

$$2 \times (3, 10) = (7, 12)$$