CIS 3362 10/30/23

Public Key Schemes So Far: RSA, El Gamal

Now: Elliptic Curve Cryptography

advantages - faster than RSA for comparable security
- not broken if factoring can be done quickly

disadvantage - more complicated + less clear how to map a plaintext to "points"

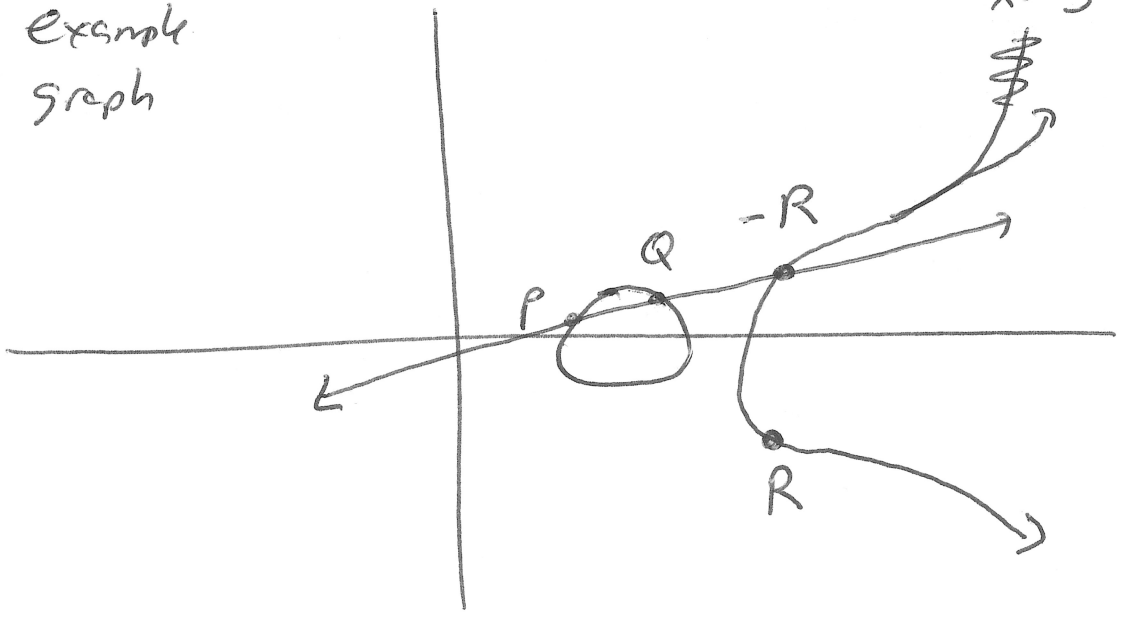
Elliptic curves defined for both real #s and int.

Real # form $y^2 = x^3 + ax + b$ (a, b are constants)

let $a = 1, b = 1 \rightarrow y^2 = x^3 + x + 1$ $x = 1 \rightarrow y = \pm\sqrt{3}$

$x = 3 \rightarrow y = \pm\sqrt{31}$

Example graph



Sym w/respect x-axis

Let's define adding points

Define P+Q as follows: (1) draw straight line btw pts.

(2) calc where it intersects curve call this pt -R

(3) define sum as R, to negate, flip y value.

In crypto we only define curve on int pts

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

a, b constants, p ∈ Prime.

Let $E_p(a,b)$ refer to this elliptic curve.

In order for this to be a "valid curve" the requirement is that $4a^3 + 27b^2 \not\equiv 0 \pmod p$

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

2 pts on curve are (3,10) (9,7)

$LHS = y^2 = 10^2 = 100 \equiv 8 \bmod 23$ ✓

$RHS = 3^3 + 3 + 1 = 31 \equiv 8 \bmod 23$ ✓

$LHS = y^2 = 7^2 = 49 \equiv 3 \bmod 23$ ✓

$RHS = 9^3 + 9 + 1 = 729 + 10 = 739 \equiv 3 \bmod 23$ ✓

739
-690
49

In addition to "regular" pts, we'll add a pt called the origin O, it doesn't have coordinate but it's the additive identity.

Rules for addition

1. For all pts P, $P + O = P$
2. For each pt $P = (x,y)$, $-P = (x,-y)$ under mod
   if $P = (x,y)$, then $-P = (x, p-y)$, where p is the prime for the curve.
   $p = 11$, 3, consider $-3 \equiv (11-3) \equiv 8 \bmod 11$
   line of symm $y = \frac{p}{2}$ $p-1$ — — — — — — — — — — $y = \frac{p}{2}$
   $P + (-P) = O$ 1 0

3. Let $P=(x_P, y_P)$ $Q=(x_Q, y_Q)$ Let $P \neq Q$

Define $R = P+Q$, calculate (x_R, y_R) as follows

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \bmod p \qquad (P \neq Q)$$

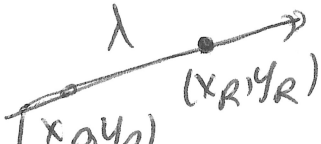
$$= (y_Q - y_P) \times (x_Q - x_P)^{-1} \bmod p$$

note if $\gcd(y_Q - y_P, x_Q - x_P) > 1$ you can divide through!

$$\frac{5}{20} = 5 \times 20^{-1}$$
$$\equiv (5 \times 1) \times (5^{-1} \times 4^{-1}) \bmod p$$
$$\equiv 1 \times 1 \times 4^{-1} \bmod p$$

Curve $P_{23}(1,1)$

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



Example $P = (3, \underline{10})$, $Q = (\underline{9}, \underline{7})$

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

$2 \times 12 \equiv 24 \equiv 1 \bmod 23$ so $2^{-1} \equiv 12 \bmod 23$

$$\lambda \equiv (-1)(12) \equiv -12 \equiv 11 \pmod{23}$$

$$x_R = 11^2 - 3 - 9 = 121 - 12 = 109 \equiv 17 \bmod 23$$

$$y_R = (11(3-17) - 10) \equiv (11 \times (-14) - 10)$$
$$\equiv 11 \times 9 - 10$$
$$\equiv 99 - 10$$
$$\equiv 89 \equiv 20 \bmod 23$$

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

Note: there isn't necessarily a pt for each x value because $y^2 \bmod p$ can't equal all possible mod values!

$p = 11$

0, 1, (4) 9, 16, 25, 36, 49, 64, (81) 100, 121

mod 11 → 0, 1, 4, 9, 5, 3, 3, 5, 9, 4, 1, 0

$-x \equiv p - x \bmod p$

$(-x)^2 \equiv (p-x)^2 \bmod p$

2^2

9^2 $(11-2)^2$

$(-2)^2$

$\equiv 2^2$

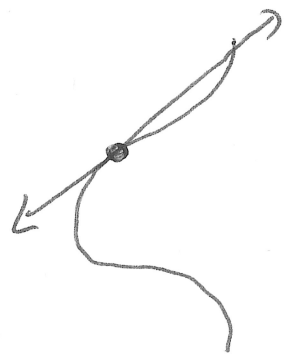
How about $P + P$ If adding same pt

$P = (3, 10)$ curve $E_{23}(1,1)$.

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

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

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



$y^2 = x^3 + ax + b$

$2yy' = 3x^2 + a$

$$\boxed{y' = \frac{3x^2 + a}{2y}}$$

$P = Q = (3, 10)$

$$\lambda = \frac{3(3)^2+1}{2 \cdot 10} \equiv \frac{28}{20} \equiv \frac{7}{5} \equiv 7 \, (5^{-1} \bmod 23)$$

$23 = 4 \times 5 + 3$
$5 = 1 \times 3 + 2$
$3 = 1 \times 2 + 1$

$3 - 1 \times 2 = 1$
$3 - (5 - 3) = 1$
$2 \times 3 - 1 \times 5 = 1$
$2(23 - 4 \times 5) - 1 \times 5 = 1$
$2 \times 23 - 9 \times 5 = 1$
$\equiv$
$5^{-1} \equiv -9 \equiv 14 \bmod 23$

$\lambda = 7 \times 14 = 98 \equiv 6 \pmod{23}$

$x_R = (6^2 - 3 - 3) = 30 \equiv 7 \pmod{23}$
$y_R = (6(3-7) - 10) = -24 - 10 = -34$
$\equiv 12 \pmod{23}$

$2 \times (3, 10) = (7, 12)$
on the curve $E_{23}(1, 1)$.