CIS 3362 10/31/25

1) 11/7 - I'll will be away travelling w/Prog. Team
Recorded Lecture - Watch next R/F.
Link off main Webcourses Page.
Associated files w/notes.

2) Elliptic Curves

RSA is good, works, a bit slow.

Goal: Create alternative public key schemes that are faster but still equally secure.

El Gamel - SLOWER

current "improvement" is called Elliptic Curve Cryptography.

WHY FASTER

1) fewer key bits for same security
2) relies on a different computation that fastmodexpo. The latter is slower than what ECC uses.

Today: Elliptic Curve Arithmetic
Mon: How to "encrypt"/decrypt a POINT
Wed: How to store arbitrary bits in a POINT.

For Cryptography only allow integers and compute mod p, $p \in$ Prime.

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

$x, y \in [0, p-1]$.

Turns out that the curve is only valid iff

$$4a^3 + 27b^2 \not\equiv 0 \pmod p$$

We write a specific curve as $E_p(a,b)$

So $y^2 \equiv (x^3 + x + 1) \bmod p$ is the curve $E_{23}(1,1)$.

$E_{29}(4,5)$ is curve $y^2 \equiv (x^3 + 4x + 5) \bmod 29$

~~Rules for addition of pts~~

ON real curve → infinite # pts

ON integer curve → finite # pts usually $O(p)$ roughly.

↳ some x's have no solution for y
other x's have 2 solutions for y
graph (of dots/pts) is symmetric about $y = \frac{p-1}{2}$

$-y = p - y$ under mod

$p = 23$ $y = 7$, $-y = 16$

1
256
675
931

3✓
29 | 931
87
61

Elliptic Curves in Real Valued functions

$y^2 = x^3 + ax + b$ (cubic)

if (x,y) is on curve
$(x,-y)$ is also on curve

Incidentally, any cubic of form ax^3+bx^2+cx+d can be rewritten w/adjusted roots in form x^3+ax+b.

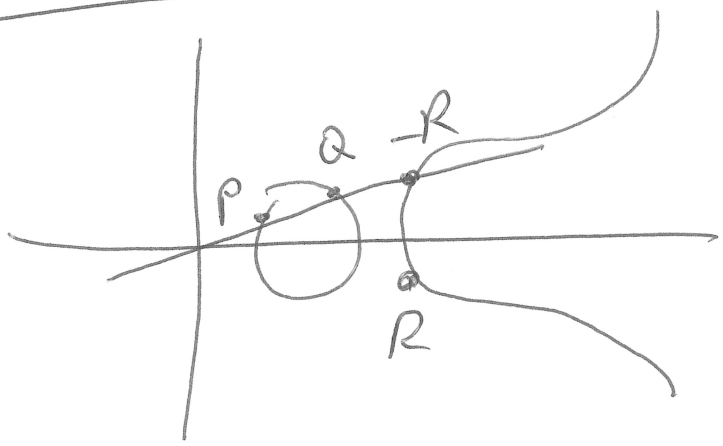
→ let $x = t - \frac{b}{3a}$

$$a\left(t-\frac{b}{3a}\right)^3 + b\left(t-\frac{b}{3a}\right)^2 + c\left(t-\frac{b}{3a}\right) + d$$

$$= \left(at^3 - 3\cdot a\frac{b}{3a}t^2 + \cdots\right) + \left(bt^2 - \cdots\right) + ct - \frac{bc}{3a} + d$$

$-bt^2$ $\quad$ $+bt^2$

Graph



example

$y=0$ symmetric

If P and Q are points on curve define addition as follows

$P+Q=R$, Draw the line through P and Q. Let this intersection point be $-R$. To negate a point reflect it over y-axis

Rules for addition

There's a special pt called the origin that is part of the curve but it doesn't have fixed x, y values. Call this point O. (Identity element for addition)

1. For each point, P, $P + O = P$.

2. For each pt $P(x, y)$, $-P = (x, -y) = (x, p-y)$
   $P + (-P) = O$

3. Let $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$
   Define $R = (x_R, y_R)$ Calculate R as follows

   1. $\lambda = \dfrac{y_Q - y_P}{x_Q - x_P} \bmod p$

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

   if $\gcd(y_Q - y_P, x_Q - x_P) > 1$, you can divide through by that gcd:

   $(ar) \times (as)^{-1}$ ← $\dfrac{20}{4} \bmod 29$

   $\equiv r \times s^{-1} \bmod p$ $\equiv 5 \times 1^{-1} \bmod 29$

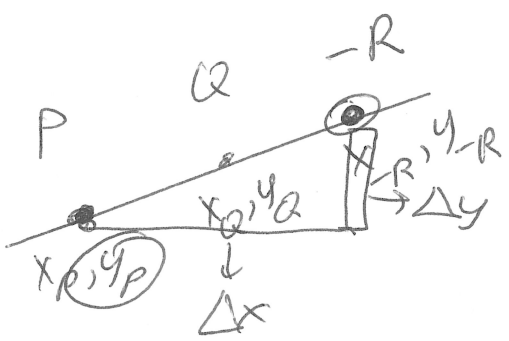
   $a \times r \times a^{-1} \times s^{-1}$

   $a \times a^{-1} \times r \times s^{-1}$

   $1 \times \boxed{r \times s^{-1}}$

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

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



λ = slope

$y = \lambda x + b$ → y int

$y_{-R} = \lambda(x_R - x_P) + y_P$

Δy

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

$E_{23}(1,1)$ $\quad p=23,\ a=1,\ b=1$

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

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

$= (7-10)(9-3)^{-1} \bmod p$

$= \frac{-3}{6} \bmod 23$

$= -1 \times 2^{-1} \bmod 23$, note $2 \times 12 = 24 \equiv 1 \bmod 23$

$= -1 \times 12 \bmod 23$

$\equiv 11 \bmod 23$

$$\begin{array}{r|l} & 4 \\ \hline 23 & 109 \\ & 92 \\ \hline & 17 \end{array}$$

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

$= (11^2 - 3 - 9) \bmod 23$

$= 121 - 12 = 109 \equiv \boxed{17} \bmod 23$

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

$-14 \equiv 9 \bmod 23$

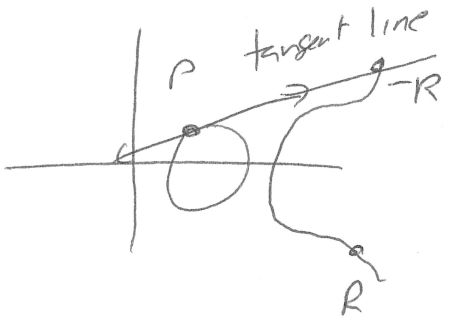
$= (11(3-17) - 10) \equiv (11 \times 9 - 10)$

$\equiv 89 \equiv \boxed{20} \bmod 23$

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

What about $P+P$?

$P=(3,10)$



$$\lambda = \frac{3x_P^2 + a}{2y_P}$$ ✓, $y^2 = x^3 + ax + b$

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

$y' = \frac{3x^2+a}{2y}$ ✓

$$\lambda = \frac{3\times 3^2 + 1}{2\times 10} \pmod{23}$$

$$= \frac{28}{20} = \frac{7}{5} = 7\times 5^{-1} \pmod{23},$$ since $-9\times 5 = -45 \equiv 1 \pmod{23}$

$5^{-1} \equiv -9$

$$= 7\times(-9)$$

$$= -63 \equiv 6 \pmod{23}$$

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

$$= 6^2 - 3 - 3$$

$$= 30 \equiv 7 \pmod{23}$$

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

$$= (6(3-7) - 10) \bmod p$$

$$= (-24-10)$$

$$= -34$$

$$\equiv 12 \pmod{23}$$

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