CIS 3362

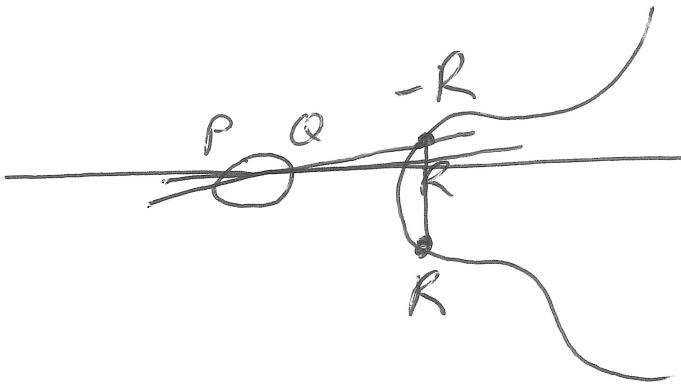
Elliptic Curves, 11/3/21

Number Theory - Group Theory (~~Abel~~) Galois
GALOIS

↳ real #s

$y^2 = x^3 + ax + b$ for constant a, b

↳ Can represent all cubics this way w/a variable substitution to remove the x^2 term.



Usually, a line through 2 pts of the curve hit a 3rd pt.

We define addition of 2 pts of the curve as follows:

(1) Draw line through pts. (P, Q)
(2) Get the 3rd intersection w/curve -R.
(3) Reflect the this point across the axis of symmetry to get the result, R.

Repeated Addition is Multiplication.
If I tell you kP, and you know P, it's hard to figure out k.

This property is similar to the Discrete Logarithm Problem - key difference is that for equivalent security, the computation of repeated addition is less intensive than fast mod expo.

For US $\Rightarrow$ we need integers under mod!

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

p = prime $\qquad 4a^3 + 27b^2 \neq 0 \mod p$

$$y^2 \equiv x^3 + x + 1 \mod 23 \qquad E_{23}(1,1)$$

Name of curve is $E_p(a,b)$.

There's a point called O (origin).

1. $P + O = P$ (additive identity)
2. $P = (x,y)$, $-P = (x,-y)$ and $P + (-P) = O$.
   under mod 23, if $P = (6,4)$, then $-P = (6,19)$
3. $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$ $\quad R = P + Q$

$$\lambda = \begin{cases} \dfrac{y_Q - y_P}{x_Q - x_P} \mod p, & \text{if } P \neq Q \\ \left(\dfrac{3x_P^2 + a}{2y_P}\right) \mod p, & \text{if } P = Q \end{cases}$$

(slope)

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

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