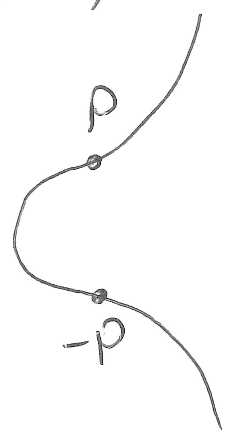
Elliptic Curves

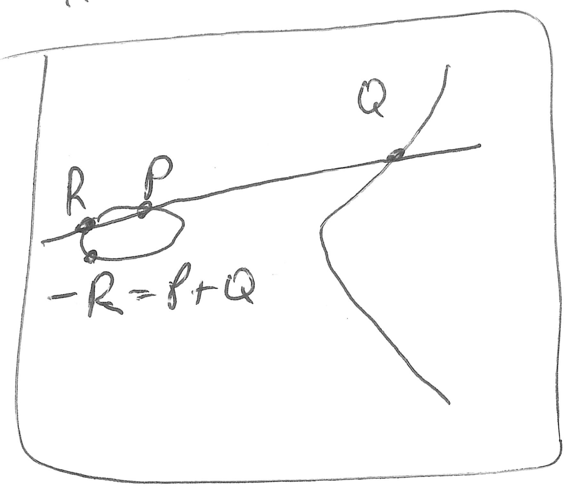
11/13/19 ①

Real-Valued

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

Simplify : $y^2 = x^3 + ax + b$ $\quad 4a^3 + 27b^2 \neq 0.$





Define addition over pts on curve

1. Point O call additive identity.
   for all point P, $P + O = P$. $O = -O$.
2. $-P$ is going to have the same x-coordinate as P
3. $P+Q$ = draw line btw P and Q and call the point of intersection R (with curve), then $P+Q = -R$.
4. $P+P$ use tangent line.
5. Multiplication is repeated addition.
   $$kP = \underbrace{P + P + P + \cdots + P}_{k \text{ times}},$$

Change Discrete $\Rightarrow$ $y^2 = x^3 + ax + b \mod p$

Valid pts have $x, y \in [0, p-1]$ $x, y \in \mathbb{Z}$

11/13/19

These curves addition of form an Abelian Group. (Abel)

(A1) Closure if $a, b \in G$ $a \cdot b \in G$

(A2) Associate $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

Identity (A3) $\exists\ I \in G$ s.t. $a \cdot I = a$ for all a.

(A4) Inverse For each $a \in G$ there exists a' such that $a \cdot a' = I$

(A5) Commutative $a \cdot b = b \cdot a$

$P = (x_P, y_P)$

$Q = (x_Q, y_Q)$

Lets use the curve $E_{23}(1,1)$

$y^2 = x^3 + x + 1 \mod 23$

$E_{29}(2,4)$ $y^2 = x^3 + 2x + 4 \mod 29$

How to do $P+Q$

Calculate λ:

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

$\to (y_Q - y_P)(x_Q - x_P)^{-1} \mod p$

$\to (3x_P^2 + a)(2y_P)^{-1} \mod p$

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

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

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

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

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

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

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} = \frac{7 - 10}{9 - 3} = \frac{-3}{6}$$

$6^{-1} \bmod 23 = 4$

$\frac{-3}{6} = -3(4) \equiv -12 \equiv 11 \bmod 23$

$$\begin{aligned} x_R = (\lambda^2 - x_P - x_Q) &= 11^2 - 3 - 9 \\ &= 121 - 12 \\ &= 109 \bmod 23 \\ &= 17 \checkmark \end{aligned}$$

$$\begin{aligned} y_R &= (\lambda(x_P - x_R) - y_P) \\ &= 11(3 - 17) - 10 \\ &= -154 - 10 \\ &= -164 \\ &= 20 \bmod 23 \checkmark \end{aligned}$$

$\begin{array}{r} 23 \\ \hline 154 \end{array} \checkmark$