Knapsack Cipher

0-1 knapsack problem (subset sum)

$S = \{3, 12, 17, 9, 37, 18\}$

target = 42

Is there a subset of items from S that adds upto the target (exactly)?

$S = \{2, 5, 13, 25, 47, 119\}$

target = 62

Super increasing

$S_k > \sum_{i=1}^{k-1} S_i$

Secret key will be a super-increasing set
Public key will NOT be.

$S = \{1, 5, 7, 19\}$

$S' = \{10, 9, 29, 26\}$ public key

Plain = 1 0 0 1

Cipher = 10 + 26 = 36

$p = 41 \rightarrow$ public

$a = 10 \rightarrow$ private

each value in S' is a value in S multiplied by a, modded by p

$$41 \overline{)190}\ 4 \qquad -164 \qquad 26$$

$$41 \overline{)370}\ 9 \qquad -369 \qquad 1$$

Bob takes 36 and multiplies by $10^{-1} \bmod 41 = 37$

$36 \times 37 \bmod 41$

$(-5) \times (-4) = 20 \bmod 41$

$S = \{ s_1, s_2, s_3, \ldots s_n \}$

p = prime
a = private mult

$S' = \{ as_1, as_2, as_3, \ldots as_n \}$

1 0 1 0 0 0

Ciphertext = $a[s_i + s_j + s \ldots] \bmod p$

Bob just multiplies ciphertext by $a^{-1} \bmod p$

$\longrightarrow \quad a^{-1} \times a[s_i + s_j + s \ldots] \bmod p$

$= [s_i + s_j + s \ldots] \bmod p$

Sum of items from set S

NOT set S'.

El Gamal

Public elements: q - prime #
α - primitive root/ generator of q.

$e(m_1) \rightarrow c_1$
$e(m_1) \rightarrow c_2$

$m_1 \rightarrow c_1$, $m_1 \rightarrow c_2$

only possible if $|M| < |C|$

$M \rightarrow (C_1, C_2)$

Alice makes her keys

1. Choose $X_A < q-1$, secret.
2. Calculates $Y_A = \alpha^{X_A} \bmod q$. PUBLIC
3. All public keys: q, α, Y_A.

Bob sends to Alice

1. Plaintext $= M < q$
2. Select random integer k $k < q$.
3. Calculate $K = (Y_A)^k \bmod q$.
4. Calculate $C_1 = \alpha^k \bmod q$
5. Calculate $C_2 = KM \bmod q$
6. Send (C_1, C_2)

$$C_2 = KM = (Y_A)^k \cdot M \bmod q$$
$$= (\alpha^{X_A})^k \cdot M \bmod q$$
$$= \boxed{\alpha^{X_A k} \cdot M \bmod q}$$

Alice to decrypt:

Alice calculates $K = C_1^{X_A} = (\alpha^k)^{X_A} \bmod q$

Alice then calculates $M = K^{-1} \times C_2 \bmod q$

$= K^{-1} \times K \times M = M \bmod q$

Fermat Factoring

$x^2 - y^2 = (x+y)(x-y)$

$x^2 - y^2 = N$

$y^2 = N - x^2$

$y^2 = x^2 - N$

$221 = 17 \times 13 = (15+2)(15-2)$

if $221 = x^2 - y^2$, then $x^2 > 221$, $x > \sqrt{221}$

idea start ② sqrt + plug in different values for x:

$\sqrt{15589} \sim 124$

$15589 = $ ~~$(125-y)(125+y)$~~

$y^2 = 125^2 - 15589$

$y^2 = 36 \rightarrow y = 6$

$15589 = (125+6)(125-6) = 131 \times 119$ ✓

40379

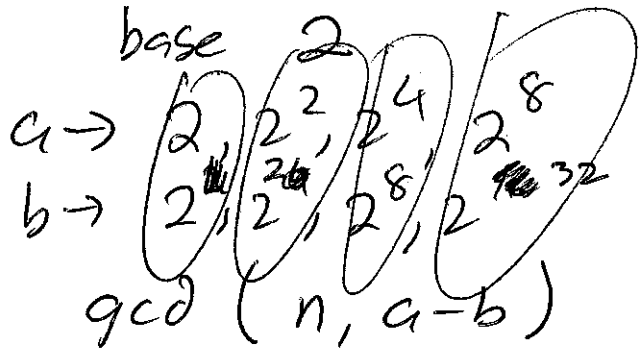
$\sqrt{40379} \sim 200$

x	$x^2 - N$
201	22 x
202	425 x
203	830 x
204	1237 x
205	1646 x
206	2057 x
207	2470 x
208	2885 x
209	3302 x
210	$3721 = 61^2$

$40379 = (210-61)(210+61)$

149×271

Pollard Rho



Elliptic Curve Arithmetic

Elliptic Curves are **Abelian** Groups:

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

(A2) Associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(A3) Identity element: $\exists e \in G \mid a \cdot e = e \cdot a = a$

(A4) Inverse element: $\forall a \in G \; \exists a' \in G$ s.t.

$a \cdot a' = e$

$a' \cdot a = e$.

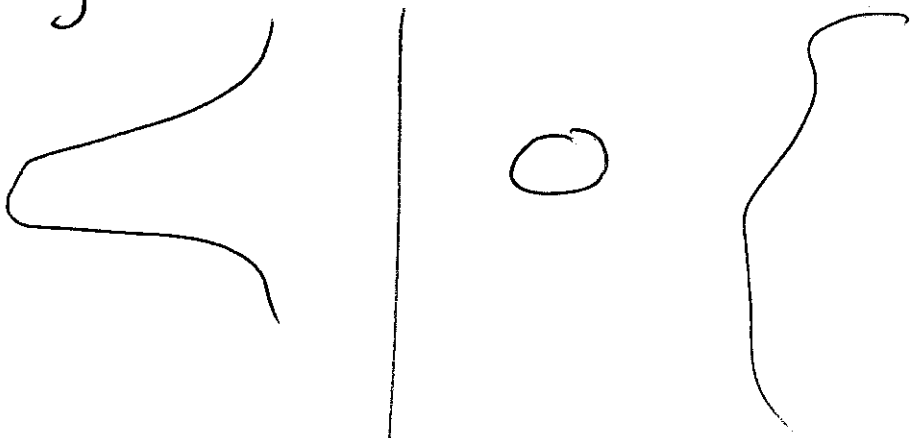
(A5) $a \cdot b = b \cdot a$

Commutative

Groups, Abelian Groups, Field (A1-A7)

An elliptic curve is a set of points (these are the elements of the group). (8,7)

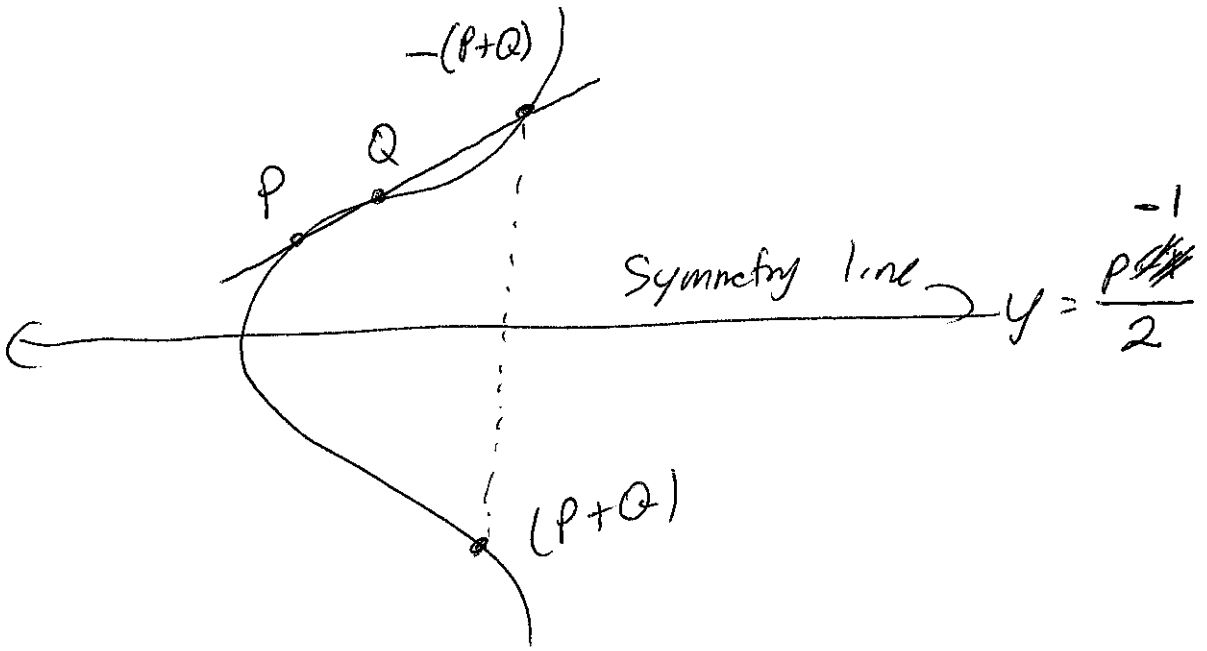
$y^2 = x^3 + ax + b$ (continuous math)



$y^2 = x^3 + ax + b \pmod p$

$p \in$ Prime Number

Operation: "Adding" points.



We define $\mathcal{O}$ as the additive identity.

for any P, $-P$ is $(x, \text{Prime} - 1 - y)$. $y^2 = x^3 + ax + b \pmod p$

(x,y)

Let's say we have 2 points (x_P, y_P) (x_Q, y_Q) and we want to add them to get (x_R, y_R).

1. $\Delta = \dfrac{y_Q - y_P}{x_Q - x_P}$

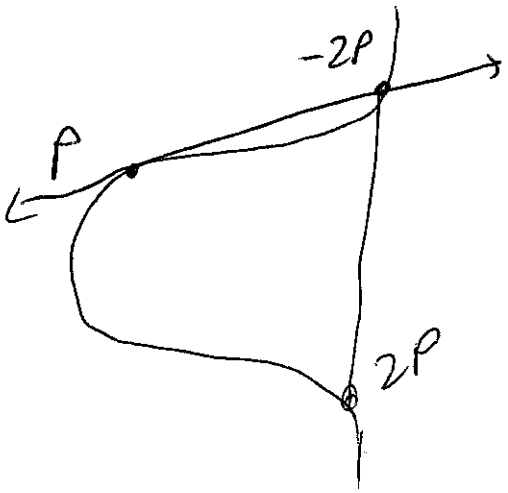
2. $x_R = \Delta^2 - x_P - x_Q$

3. $y_R = -y_P + \Delta(x_P - x_R)$

} work only if $x_P \neq x_Q$.

If we want to calculate 2P, I need a new set of formulas.

11/4/16 ③



$$X_R = \left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P$$

$$y_R = \left(\frac{3x_P^2+a}{2y_P}\right)(x_P - x_R) - y_P$$

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

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

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

$4a^3+27b^2 \neq 0 \bmod p$

Curve: $E_{23}(1,1)$ → prime = 23, $a=1$, $b=1$

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

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

$$\Delta = \frac{7-10}{9-3} = \frac{-3}{6} \bmod 23$$

$(-3)(6^{-1}) \bmod 23$

$(-3)(4) \bmod 23$

$-12 \bmod 23$

$11 \bmod 23$

$X_R = \Delta^2 - x_P - x_Q = 11^2 - 3 - 9$

$= 121 - 12$

$= 109 \bmod 23$

$= \underline{17}$

$$y_R = -y_P + \lambda(x_P - x_R)$$
$$= -10 + 11(3-17)$$
$$= -10 + 11(-14) \mod 23$$
$$\equiv -10 + 11(9) \mod 23$$
$$\equiv 99 - 10 \mod 23$$
$$\equiv 89 \mod 23$$
$$\equiv \boxed{20}$$

$(17, 20)$

$2P \qquad P(3,10) \qquad E_{23}(1,1) \qquad y^2 = x^3 + x + 1$ (a = 1)

$$x_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P$$
$$= \left(\frac{27+1}{20}\right)^2 - 2(3)$$
$$= \left(\frac{28}{20}\right)^2 - 6$$
$$= \left(\frac{7}{5}\right)^2 - 6$$
$$= (7 \times 5^{-1} \mod 23)^2 - 6$$
$$= (7 \times 14)^2 - 6$$
$$= (98)^2 - 6$$
$$\equiv 6^2 - 6 \mod 23$$
$$\equiv 30 \mod 23$$
$$\equiv \boxed{7}$$

$$y_R = \left(\frac{3x_P^2 + a}{2y_P}\right)(x_P - x_R) - y_P$$
$$= 6(3-7) - 10$$
$$= 6(-4) - 10$$
$$= -24 - 10$$
$$= -34$$
$$\equiv -34 + 46$$
$$\equiv \boxed{12}$$

$(7, 12)$