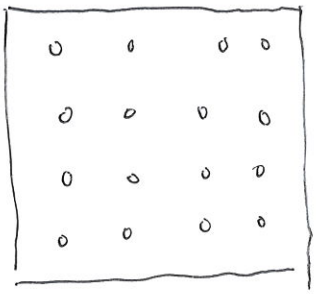
Classic Problem The Artillerymens Dilemma



~~Cannonball~~ cannon ball packed in a square box

pyramid of cannon ball

box of size 1×1 → pyramid with height 1

box of size 2×2 (4 balls) → not a pyramid.

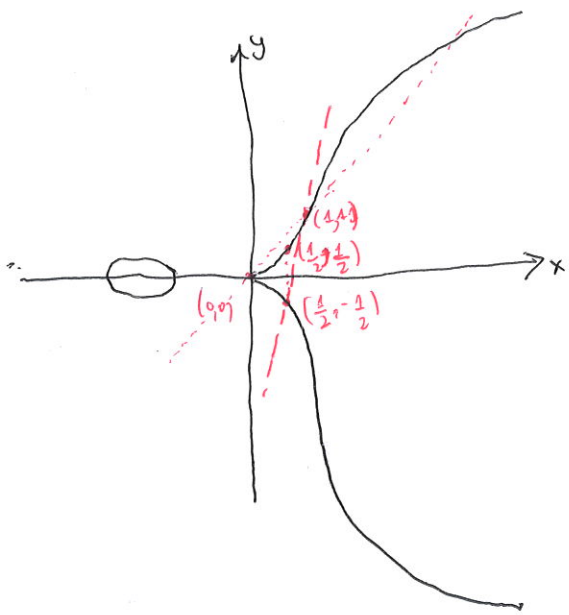
box of size 3×3 (9 balls) → not a pyramid.

o
o
o

box of size $y\times y$ (y^2 balls) → pyramid with height x

$$1^2+2^2+3^2+\cdots+x^2 = \frac{x(x+1)(2x+1)}{6} = \frac{x^3}{3}+\frac{x^2}{2}+\frac{x}{6}$$

Task Find non trivial $x,y\in\mathbb{Z}_{>0}$ such that $y^2 = \frac{x^3}{3}+\frac{x^2}{2}+\frac{x}{6}$



- Draw a line between $(0,0)$ and $(0,1)$
- Find where the line cuts the curve again.

The line is $x=y$. $\Leftrightarrow y^2 = \frac{x^3}{3}+\frac{x^2}{2}+\frac{x}{6}$

$$x^2 = \frac{x^3}{3}+\frac{x^2}{2}+\frac{x}{6}$$

$$0 = \frac{x^3}{3}-\frac{x^2}{2}+\frac{x}{6} \qquad 0 = x^3-\frac{3}{2}x^2+\frac{x}{2}$$

Coefficient of $-x^2$ is the sum of all x solution.

$$x_1+x_2+x_3 = \frac{3}{2}$$

$$0+1+x_3 = \frac{3}{2}$$

$$x_3 = 1/2$$

$$y^2 = \frac{1}{3\cdot8}+\frac{1}{2\cdot4}+\frac{1}{12} = \frac{1}{24}+\frac{1}{8}+\frac{1}{12} = \frac{1}{4}$$

$$y = 1/2$$

The cut point is $\left(\frac{1}{2},\frac{1}{2}\right)$

Specialty

If we draw a line that pass 2 ~~lines~~ points in the curve, it will pass 3 points.
(that line must not parallel to y-axis.)

$$(0,0)+(1,1) = \left(\frac{1}{2},-\frac{1}{2}\right)$$

- Draw a line between $(1,1)$ and $(\frac{1}{2}, -\frac{1}{2})$ $\quad y = mx + c \rightarrow m = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1 - (\frac{1}{2})}{\frac{3}{4} - \frac{1}{2}} = 3$

$y = 3x - 2$

$y = 3x + c \rightarrow c = -2$

$\uparrow \quad \uparrow$

$1 \quad 1$

$\updownarrow$

$y^2 = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6} \longrightarrow (3x-2)^2 = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6}$

$9x^2 - 12x + 4 = \frac{x^3}{3} + \frac{x^2}{2} + \frac{x}{6}$

$27x^2 - 36x + 12 = x^3 + \frac{3}{2}x^2 + \frac{x}{2}$

$0 = x^3 - \frac{51}{2}x^2 + (36 + \frac{1}{2})x - 12$

$x_1 + x_2 + x_3 = \frac{51}{2}$

$1 + \frac{1}{2} + x_3 = \frac{51}{2}$

$x_3 = 24$

$y_3 = mx_3 + c$

$= 3 \cdot 24 - 2 = 70$

$(1,1) \oplus (\frac{1}{2}, -\frac{1}{2}) = (24, -70)$ We have got the non-trivial solution

x = height of pyramid = 24

y = width of box = 70

Conclusion.

Point addition.

1. Draw a line which cut the 2 operands.
2. Check where the line cut the curve again.
3. Addition result will be at another side of x-axis.

Weierstrass Equation : $y^2 = x^3 + Ax + B$ when $4A^3 + 27B^2 \neq 0$

(most well-known elliptic curve)

(1) Draw a line $y = mx + c$ where

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

$$c = y_1 - mx_1$$

(2) Find another cut point

$(mx + c)^2 = x^3 + Ax + B$

coefficient of x^2 is m^2

$m^2 = x_1 + x_2 + x_3$

$x_3 = m^2 - x_1 - x_2$

$y_3 = mx_3 + c$

(3) Another side of x-axis $\quad (x_1, y_1) \oplus (x_2, y_2) = (x_3, -y_3)$

Special Case $(x_1, y_1) + (x_1, y_2) = \infty$ ← point at infinity.

the line will not cut the curve again

$(x, y) + \infty = (x, y)$, $\infty + \infty = \infty$

$(x, y) + (x, y) = ?$

① Draw a line that touch the curve at (x, y)

$$2y\,dy = (3x^2 + A)\,dx$$

$$m = \frac{dy}{dx} = \frac{3x^2 + A}{2y}$$

∴ The other steps would not be different.

Weierstrass Equation on Prime Field

$$E(\mathbb{F}_p) = \{ (x, y) \in \mathbb{F}_p^2 : y \otimes y = [x \otimes x \otimes x] \oplus [A \otimes x] \oplus B \}$$

$\{0, \dots, p-1\}$

operation on prime field $y \otimes y = (y^2) \bmod p$.

Ex $A = 1$, $B = 1$, $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$

x	$(x \otimes x \otimes x) \oplus x \oplus 1$
0	$(0^3 + 0 + 1) \bmod 5 = 1$
1	$(1^3 + 1 + 1) \bmod 5 = 3$
2	$(2^3 + 2 + 1) \bmod 5 = 1$
3	$(3^3 + 3 + 1) \bmod 5 = 1$
4	$(4^3 + 4 + 1) \bmod 5 = 4$

y	$(y \otimes y)$
0	$0 \bmod 5 = 0$
1	$1 \bmod 5 = 1$
2	$4 \bmod 5 = 4$
3	$9 \bmod 5 = 4$
4	$16 \bmod 5 = 1$

$E(\mathbb{F}_5) = \{(0,0), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3), \infty\}$ $\quad |E(\mathbb{F}_5)| = 8$

Hasse's Theorem (Weil's) $\quad (p-1) - 2\sqrt{p} \le |E(\mathbb{F}_p)| \le (p+1) + 2\sqrt{p}$ $\quad [\,|E(\mathbb{F}_p)| \approx p\,]$

$(x_1, y_1) \oplus (x_2, y_2)$

$m = [y_2 \oplus (-y_1)] \otimes [1 / (x_2 \oplus (-x_1))]$ → $O(\log^3 q)$ computation time

$c = y_1 \oplus [m \otimes x_1]$

$x_3 = [m \otimes m] \oplus [-x_1] \oplus (-x_2)$

$y_3 = (-[m \otimes x_3]) \oplus [-c]$

Ex $(4, 2) \oplus (0, 1)$

$m = [2 \oplus 4] \otimes [1 / (0 \oplus (-4))]$

$= 1 \otimes [1/1] = 1$

$c = 2 \oplus [-(1 \otimes 4)]$

$= 2 \oplus [-4] = 2 \oplus 1$

$m = [1 \oplus (-2)] \otimes [1 / (0 \oplus (-4))]$

$= [1 \otimes 3] \otimes [1/1] = 3 \otimes 4$

$c = 2 \oplus [-(4 \otimes 4)] = 2 \oplus [-1] = 2 \oplus 4 = 1$

$x_3 = (m \otimes m) \oplus -x_1 \oplus -x_2 = (4 \otimes 4) \oplus -4 \oplus -0 = 1 \oplus 1 \oplus 0 = 2$

$y_3 = -[(m \otimes x_3) \oplus c_2] = -[(4 \otimes 2) \oplus 1] = -[3 \oplus 1] = -4 = 1$

$\therefore (4,2) \oplus (0,1) = (2,1)$

Bonus Question Calculate $(3,1) + (4,2)$

Theorem $(E(\mathbb{F}_p), \text{point addition})$ is an abelian group.

1. Closure The addition result is always in $E(\mathbb{F}_p)$
2. Associativity $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$ for all $P, Q, R \in E(\mathbb{F}_p)$
3. Identity $P + \infty = P = \infty + P$
4. Inverse $(x, y) * (x, -y) = \infty$ $(x, -y)$ is an inverse of (x, y)
5. Commutativity $P \oplus Q = Q \oplus P$

Faster Scalar Multiplication

$n \cdot P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{n \text{ times}}$ [n-1 additions]

Suppose that we want to calculate $16P$

$2P = P + P$
$4P = 2P + 2P$
$8P = 4P + 4P$
$16P = 8P + 8P$

4 points addition instead of 15 additions
$O(\lg n)$ $O(n)$

Use for calculating $2^m P$ for some m.

How about other n?

$57 = 32 + 16 + 8 + 1$
$= 2^5 + 2^4 + 2^3 + 2^0$

$57P = 2^5 P + 2^4 P + 2^3 P + 2^0 P$

15 additions instead of 56 additions

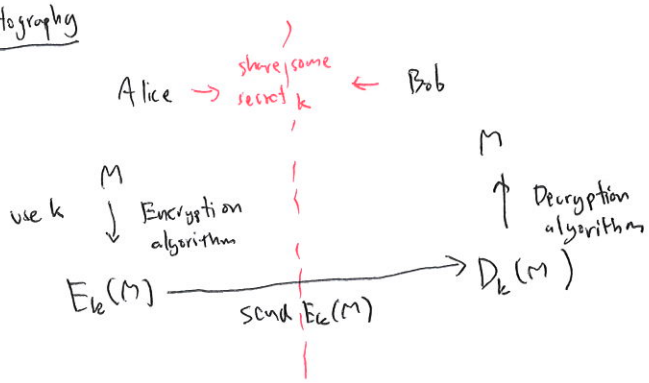
5 additions 4 additions 3 additions.

$n \cdot P = 2^{i_0} \cdot P + 2^{i_1} P + \cdots + 2^{i_n} P$ $O(\lg^2 n)$ addition

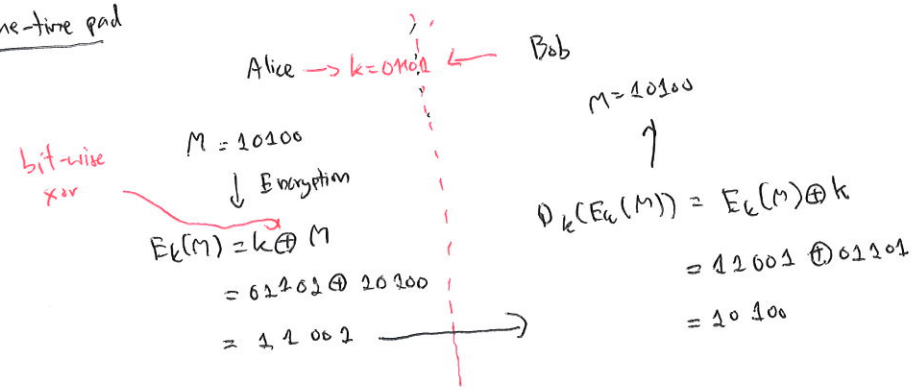
$\lg n$ $\lg n$ $\lg n$.

As $n \leq p$ and it takes $O(\lg^3 n)$ for one addition, it takes $O(\lg^5 n)$ for one scalar multiplication.

Private Key Cryptography



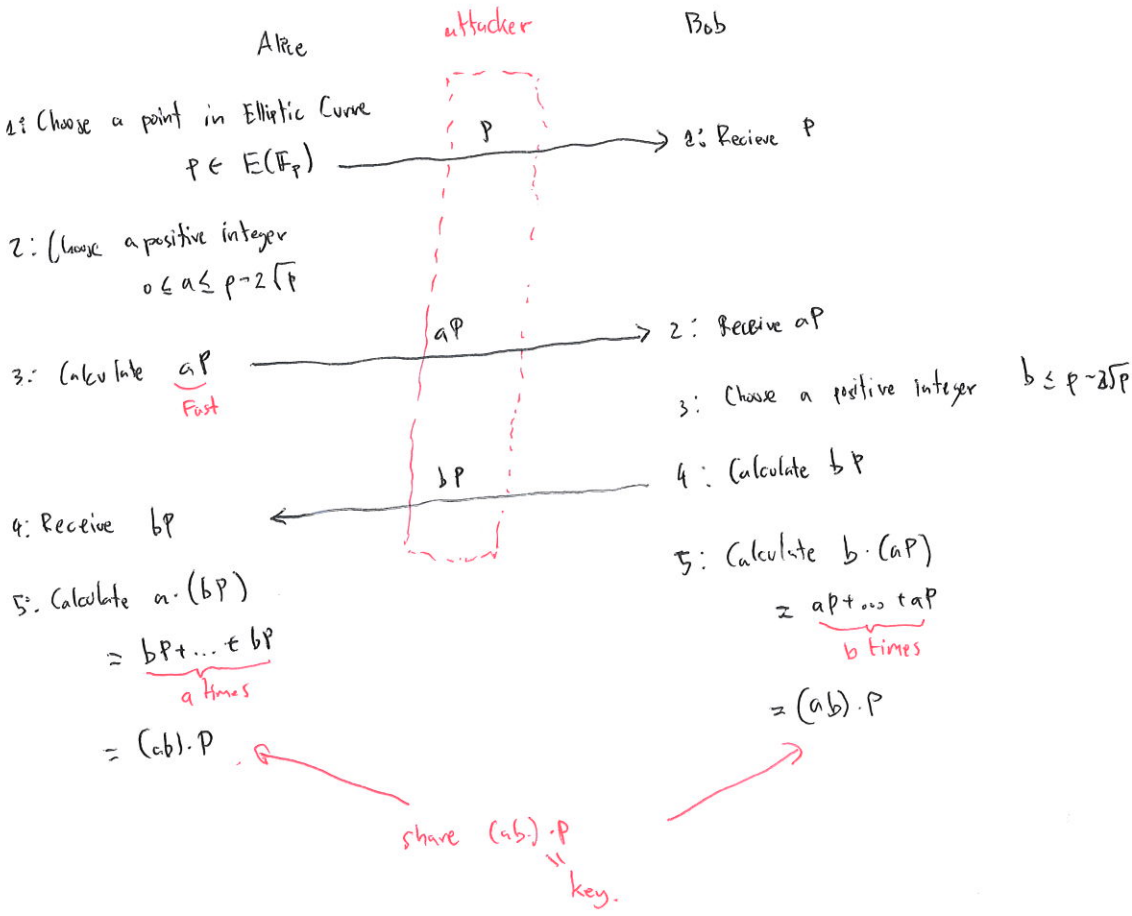
One-time pad



- One-time pad is known to be costly and weak.
- Advanced Encryption System (AES) is the most commonly used cryptosystem.

Problem How can Alice and Bob share their key to each other? → Key exchange Protocol.

Diffie-Hellman Key Exchange Protocol



Attacker knows P, aP, bP

Diffie-Hellman Problem

Input: P, aP, bP

Output: $(ab)P$

$\Longleftrightarrow$

Discrete Logarithm Problem

Input: P, aP

Output: a

very hard problem!!

No algorithm is faster than $O(\sqrt{p})$

Impossible to be solved when $p \approx 2^{256}$