

## CHƯƠNG 3. KỸ THUẬT MÃ HOÁ – CƠ SỞ TOÁN HỌC

### I. THUẬT TOÁN:

- **Thuật toán** là một chuỗi hữu hạn các chỉ dẫn nghiêm ngặt được sử dụng để tìm lời giải cho một loại bài toán cụ thể.
- Các thuật toán được **sử dụng làm thông số kỹ thuật** để thực hiện tính toán và xử lý dữ liệu.
- Các thuật toán có thể **được thể hiện bằng nhiều loại ký hiệu**, bao gồm mã giả, lưu đồ, biểu đồ drakon, ngôn ngữ lập trình hay bảng điều khiển
- Một thuật toán tốt phải thỏa mãn các đặc tính sau:
  - **Tính hữu hạn:** Thuật toán phải kết thúc sau một số hữu hạn bước thực hiện.
  - **Tính xác định:**
    - Mỗi bước trong thuật toán phải rõ ràng, có ý nghĩa cụ thể.
    - Nếu thuật toán thực hiện nhiều lần với cùng một bộ dữ liệu đầu vào thì kết quả đầu ra phải giống nhau.
- **Độ phức tạp của thuật toán** dựa trên **số các phép tính phải làm** khi thực hiện thuật toán.
- Khi tiến hành cùng một thuật toán, số các phép tính phải thực hiện còn phụ thuộc vào độ lớn của dữ liệu đầu vào. Vì thế, **độ phức tạp của thuật toán sẽ là một hàm số của độ lớn đầu vào**.
- Độ phức tạp của một thuật toán còn được đo bằng số các phép tính bit. Phép tính bit là một phép tính logic hay số học thực hiện trên các bit 0 và 1. Việc đo bằng số phép tính bit giúp đánh giá **chi tiết hơn về chi phí thực sự mà máy tính phải thực hiện**.

### II. HÀM XOR TRONG MẬT MÃ

- Độ dài (kích thước số bit) của khóa  $K$  rõ ràng có tác động rất lớn đến khả năng bảo mật của mã đối xứng.
- Nếu bạn dùng khóa có độ dài  $n$  bit, thì số khóa có thể tạo ra là  $2^n$ . Ví dụ:
  - Khóa dài **56 bit**  $\Rightarrow 2^{56} \approx 7.2 \times 10^{16}$  khóa khác nhau.
  - Khóa dài **128 bit**  $\Rightarrow 2^{128} \approx 3.4 \times 10^{38}$  khóa — cực kỳ khó bị tấn công bằng brute-force.  
 $\Rightarrow$  **Độ dài khóa càng lớn  $\rightarrow$  bảo mật càng cao**, vì số khả năng cần thử trong tấn công brute-force tăng theo cấp số mũ.
- **Phép XOR thực hiện rất nhanh ở mức phần cứng** (bitwise), chỉ cần **1 phép toán logic đơn giản** trên từng bit (chỉ so sánh và trả về giá trị 0 hoặc 1 dựa trên hai bit đầu vào). Do đó, **tốc độ mã hóa/giải mã cao** — rất phù hợp cho các ứng dụng yêu cầu **hiệu suất thời gian** cao như truyền thông, IoT, hoặc mã hóa theo luồng (stream cipher).
- Hơn nữa, XOR có **tính chất thuận nghịch**: Nếu  $C = P \oplus K$ , thì  $P = C \oplus K$ . Tính chất này cho phép sử dụng cùng một phép toán cho cả mã hóa và giải mã, giúp đơn giản hóa thiết kế thuật toán.
- Và vì các phép OR và AND **không** có tính thuận nghịch, do đó, OR và AND không phù hợp cho mã hóa vì không thể giải mã một cách đáng tin cậy.

- XOR là khả nghịch:

Nếu  $C = A \oplus K$ , thì ta có thể khôi phục lại  $A = C \oplus K$ .

=> Cùng một hàm (XOR), vừa mã hóa vừa giải mã được.

- AND và OR thì không khả nghịch:

- Nếu  $A \text{ AND } K = C$ , thì từ  $C$  không thể biết chắc được  $A$  là gì, vì thông tin đã bị **mất** (bit nào là 0 thì không thể phục hồi).
- Ví dụ:  $A = 1010, K = 1100 \rightarrow C = A \text{ AND } K = 1000$ .  
→ Không thể đảo ngược để tìm lại  $A$ .

### III. GIẢI THUẬT EUCLIDE

#### 1. Ước số và số nguyên tố:

- Với  $a, b \in \mathbb{Z}$  ta nói rằng  $b$  chia hết cho  $a$ , nếu như  **$b$  có thể viết thành tích của  $a$  với một số nguyên khác** ( $b = m \cdot a, m \in \mathbb{Z}$ ), lúc đó ta có thể nói rằng  $b$  chia hết cho  $a$ , hay  $a$  là một ước số của  $b$ , ký hiệu  $a|b$ .
- **1 số tính chất:**
  - Nếu  $a, b, c \in \mathbb{Z}$  và  $a|b$  thì  $a|bc$ ;
  - Nếu  $a|b$  và  $b|c$  thì  $a|c$ ;
  - Nếu  $a|b$  và  $a|c$  thì  $a|b \pm c$ ;
  - Nếu  $a|b$  và  $a|c$  thì  $a|b \pm c$ ;
- Số tự nhiên **lớn hơn 1** mà không chia hết cho số tự nhiên nào khác, **trừ chính nó và 1** thì được gọi là số nguyên tố. Ngược lại, số đó được gọi là **hợp số**.
- **Hệ quả:**
  - Nếu  $p$  là một số nguyên tố và  $p|ab$  thì **ít nhất một trong 2 số  $a, b$  phải chia hết cho  $p$** .
  - Ước chung lớn nhất của 2 số tự nhiên  $a, b$  là số lớn nhất trong tập các ước chung của 2 số đó, được ký hiệu là  $\gcd(a, b)$  (*Greatest common divisor*).
  - Khi **2 số tự nhiên** có ước chung lớn nhất  $\gcd(a, b) = 1$  thì chúng được gọi là **nguyên tố cùng nhau**.

#### 2. Giải thuật Euclide & Euclide mở rộng:

**Thuật toán Euclide ban đầu** được phát biểu như sau: *UCLN của hai số nguyên  $a$  và  $b$  (với  $b \neq 0$ ) không thay đổi khi thay số lớn hơn bằng hiệu của nó với số nhỏ hơn. Quá trình thay thế này được lặp đi lặp lại cho tới khi hai số bằng nhau, khi đó UCLN chính là một trong hai số.*

Tuy nhiên, thuật toán này không hiệu quả khi khoảng cách hai số là rất lớn. Ví dụ, tìm  $\text{UCLN}(1000000000, 1)$  thì thuật toán cần lặp 999999999 lần.

Vì thế, người ta cải tiến thuật toán Euclide như sau: *UCLN của hai số nguyên  $a$  và  $b$  (với  $b \neq 0$ ) không thay đổi nếu ta thay số lớn hơn bằng số dư của phép chia số lớn cho số nhỏ.* Nói cách khác, ta có:  $\text{UCLN}(a, b) = \text{UCLN}(b, a \% b)$ . Thuật toán thực hiện việc thay thế này nhiều lần cho đến khi số dư bằng 0. Khi đó, số khác 0 còn lại chính là UCLN của hai số ban đầu.

**Giải thuật Euclid mở rộng** sử dụng để giải phương trình vô định nguyên (phương trình Diophantos):

$$a \cdot x + b \cdot y = d \quad (1)$$

Với  $a, b, c$  là các hệ số nguyên;  $x, y$  là các biến nhận giá trị nguyên.

Để phương trình (1) có nghiệm (nguyên) cần thỏa:  $d = \text{UCLN}(a, b)$ .

Quá trình thực hiện như sau:

a) Cho hai số tự nhiên  $a, b$  với  $a > b$ . Thực hiện tìm  $d = UCLN(a, b)$  theo **thuật toán Euclide** như sau:

- Cho 2 số nguyên  $a, b$  ( $b \neq 0$ ), ta tìm  $UCLN(a, b) = d$  như sau:
- Nếu  $b$  là ước của  $a$ , thì  $d = b$ .
- Ngược lại, đặt  $r_0 = a, r_1 = b$ . Ta có  $r_0$  chia cho  $r_1$  được số dư  $r_2$

$$r_0 = q_1 r_1 + r_2, \quad 0 \leq r_2 < r_1$$

$$r_1 = q_2 r_2 + r_3, \quad 0 \leq r_3 < r_2$$

$$r_2 = q_3 r_3 + r_4, \quad 0 \leq r_4 < r_3$$

- Do  $r_1 > r_2 > \dots \geq 0$  nên phép chia như trên sẽ dừng sau một số hữu hạn bước. Gọi  $r_{m+2}$  là số dư đầu tiên bằng 0. Ta có

$$r_{m-1} = q_m r_m + r_{m+1}, \quad 0 \leq r_{m+1} < r_m$$

$$r_m = q_{m+1} r_{m+1} + 0$$

- Khi đó  $d = r_{m+1}$ . Dễ thấy thuật toán Euclide thông qua  $m$  bước để tìm được  $UCLN(a, b)$ .

b) Bài toán đặt ra là tìm hai biến  $x, y$  sao cho  $a \cdot x + b \cdot y = d (= r_{m+1})$ .

Xây dựng công thức truy hồi: Tìm  $x_i, y_i$  sao cho:  $a \cdot x_i + b \cdot y_i = r_i$  (2), với  $i = 0, 1, \dots$

Vì ta đã đặt  $r_0 = a, r_1 = b$  nên ta có:  $\begin{cases} a \cdot 1 + b \cdot 0 = a = r_0 \\ a \cdot 0 + b \cdot 1 = b = r_1 \end{cases}$ , nghĩa là  $\begin{cases} x_0 = 1, y_0 = 0 \\ x_1 = 0, y_1 = 1 \end{cases}$  (\*). Đây chính là các

giá trị khởi tạo.

Ta cũng có:  $a \cdot x_{i+1} + b \cdot y_{i+1} = r_{i+1}$  (3) và

$$r_i = q_{i+1} \cdot r_{i+1} + r_{i+2} \Rightarrow r_{i+2} = r_i - q_{i+1} \cdot r_{i+1} \quad (4)$$

Thay (2), (3) vào (4), ta được:

$$\begin{aligned} r_{i+2} &= (a \cdot x_i + b \cdot y_i) - q_{i+1} (a \cdot x_{i+1} + b \cdot y_{i+1}) \\ \Leftrightarrow r_{i+2} &= a(x_i - q_{i+1} \cdot x_{i+1}) + b(y_i - q_{i+1} \cdot y_{i+1}) \\ \Rightarrow \begin{cases} x_{i+2} = x_i - q_{i+1} \cdot x_{i+1} & (**) \\ y_{i+2} = y_i - q_{i+1} \cdot y_{i+1} & (***) \end{cases} \end{aligned}$$

Khi  $i = m - 1$ , ta có được  $x_{m+1}$  &  $y_{m+1}$ , chính là các biến  $x, y$  cần tìm.

Các công thức (\*), (\*\*), (\*\*\*) là các công thức truy hồi để tính  $x, y$ .

**Ví dụ:** Giả sử cho  $a = 29, b = 8$ , giải thuật trải qua các bước như sau:

Bước $i$	$r_i$	$r_{i+1}$	$r_{i+2}$	$q_{i+1}$	$x_i$	$x_{i+1}$	$x_{i+2}$	$y_i$	$y_{i+1}$	$y_{i+2}$
0	29 $= r_0 = a$	8 $= r_1 = b$	5 $= r_2$	3 $= q_1$	1 $= x_0$	0 $= x_1$	1 $= x_2$	0 $= y_0$	1 $= y_1$	-3 $= y_2$
1	8	5	3	1	0	1	-1	1	-3	4
2	5	3	2	1	1	-1	2	-3	4	-7
3	3	2	1	1	-1	2	-3	4	-7	11
4	2	1	0	2	-	-	-	-	-	-
<b>Thuật toán Euclide</b>					<b>Thuật toán Euclide mở rộng</b>					

Giải thích **Bước 0:** Khởi tạo  $r_0 = 29 = a$ ,  $r_1 = 8 = b$ ,  $\begin{cases} x_0 = 1, y_0 = 0 \\ x_1 = 0, y_1 = 1 \end{cases}$

$$\text{Tính } q_1 = \left[ \frac{r_0}{r_1} \right] = \left[ \frac{29}{8} \right] = 3, \quad \begin{cases} r_2 = r_0 - q_1 \cdot r_1 = 29 - 3 \cdot 8 = 5. \\ x_2 = x_0 - q_1 \cdot x_1 = 1 - 3 \cdot 0 = 1. \\ y_2 = y_0 - q_1 \cdot y_1 = 0 - 3 \cdot 1 = -3. \end{cases}$$

**Các bước còn lại thực hiện tương tự, đến khi số dư bằng 0 thì dừng.**

Kết quả thuật toán:  $d = \gcd(29, 8) = 1$  và  $x = -3$ ,  $y = 11$ . Dễ dàng kiểm tra hệ thức  $29 \cdot (-3) + 8 \cdot 11 = 1$ .

### 3. Áp dụng giải thuật Euclid mở rộng tìm số nghịch đảo trong vành $\mathbb{Z}_m$

Trong lý thuyết số, vành  $\mathbb{Z}_m$  được định nghĩa là **vành thương của  $\mathbb{Z}$  (vành các số nguyên) với quan hệ đồng dư theo modulo  $m$** , mà các phần tử của nó là các lớp đồng dư theo modulo  $m$  ( **$m$  là một số nguyên  $> 1$** ).

Có thể hiểu đơn giản, **vành** như một tập hợp số có thể thực hiện phép **cộng, nhân** mà phải tuân theo nguyên tắc nào đó.

Khi đó:  $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ .

**Phép cộng và phép nhân** trong  $\mathbb{Z}_m$  được định nghĩa như sau:  $\begin{cases} a + b = (a + b) \bmod m \\ a \cdot b = (a \cdot b) \bmod m \end{cases}$ . Nghĩa là KQ sau

khi thực hiện phép cộng/nhân phải nằm trong  $\mathbb{Z}_m$  bằng cách thực hiện chia lấy dư với  $m$ .

Một phần tử  $a \in \mathbb{Z}_m$  được gọi là **khả đảo** (có nghịch đảo) (theo modulo  $m$ ) nếu tồn tại phần tử  $a' \in \mathbb{Z}_m$  sao cho  $a \cdot a' \equiv 1 \pmod{m}$ . Khi đó  $a'$  được gọi là nghịch đảo modulo  $m$  theo  $a$ .

Ngoài ra  $a$  khả đảo khi và chỉ khi  $\text{UCLN}(a, m) = 1$ , hay  $a$  và  $m$  nguyên tố cùng nhau.

Khi đó tồn tại các số nguyên  $x, y$  sao cho  $m \cdot x + a \cdot y = 1$  (5). Đẳng thức này lại chỉ ra  $y$  là **nghịch đảo của  $a$  theo modulo  $m$** .

Điều này có thể giải thích như sau:

- Vì  $a \cdot a' \equiv 1 \pmod{m}$  nên ta có thể viết thành  $a \cdot a' = q \cdot m + 1 \Rightarrow a \cdot a' - q \cdot m = 1$  (6). Nếu ta đặt

$\begin{cases} x = a' \\ y = -q \end{cases}$  thì (6) trở thành  $ax + my = 1$ . Đẳng thức này chỉ ra rằng  $x$  là nghịch đảo của  $a$  theo modulo  $m$ .

- Tuy nhiên trong đẳng thức (5), người ta lại quy ước rằng  $\begin{cases} x = -q \\ y = a' \end{cases}$  để ra được đẳng thức này, và

điều này không ảnh hưởng đến tính đúng đắn của thuật toán.

Do đó có thể tìm được phần tử nghịch đảo của  $a$  theo modulo  $m$  nhờ **thuật toán Euclid mở rộng** khi chia  $m$  cho  $a$ .

**Ví dụ:** Tìm số nghịch đảo (nếu có) của 30 theo modulo 101. Nghĩa là  $30.a' \equiv 1 \pmod{101}$ .

Vậy ta cũng lập bảng như thuật toán Euclid mở rộng, tuy nhiên chỉ cần thực hiện tính  $y$ .

Bước $i$	$m$	$a$	$r$	$b$	$y_0$	$y_1$	$y(y_2)$
0	101	30	11	3	0	1	-3
1	30	11	8	2	1	-3	7
2	11	8	3	1	-3	7	-10
3	8	3	2	2	7	-10	27
4	3	2	1	1	-10	27	<b>-37</b>
5	2	1	0	.	.	.	.

Kết quả tính toán trong bảng cho ta  $y = -37$ . Tuy nhiên  $-37 \notin \mathbb{Z}_{101}$ , nên ta tiến hành lấy số đối của 37 theo modulo 101, bằng cách lấy  $-37 + 101 = 64$ . Vậy  $30^{-1} \pmod{101} = 64$ .

## **IV. HÀM MODULO, ĐỒNG DƯ THỨC, ĐỊNH LÝ FERMAT & ĐỊNH LÝ SỐ DƯ TRUNG HOA**

### **1. Modulo và đồng dư thức:**

Hàm modulo có thể hiểu một cách đơn giản chính là **số dư trong phép chia các số nguyên**. Muốn tính  $X$  modulo  $Y$  (ký hiệu là  $X \bmod Y$ ) ta chỉ cần làm phép chia  $X$  cho  $Y$  và tìm số dư trong phép chia đó.

$X \bmod Y$  chỉ có thể lấy các giá trị từ 0, 1, ... cho đến  $Y - 1$ .

Trong số học, hai số nguyên  $a$  và  $b$  được gọi là “**đồng dư** theo modulo  $n$ ” nếu **chúng có cùng số dư** trong phép chia cho  $n$ . Ta ký hiệu:  $a \equiv b \pmod{n}$  và đọc là “ $a$  đồng dư với  $b$  theo modulo  $n$ ”. Biểu thức đó gọi là một **đồng dư thức**.

*Một số tính chất của phép tính đồng dư:*

- $a \equiv a \pmod{n}$ ;
- Nếu  $a \equiv b \pmod{n}$  thì  $b \equiv a \pmod{n}$ ;
- Nếu  $a \equiv b \pmod{n}$  và  $b \equiv c \pmod{n}$  thì  $a \equiv c \pmod{n}$ ;
- Nếu  $a \equiv b \pmod{n}$ ,  $c \equiv d \pmod{n}$  thì  $a \pm c \equiv b \pm d \pmod{n}$ ,  $ac \equiv bd \pmod{n}$ ;
- Nếu  $a \equiv b \pmod{n}$  và  $d = \text{UC}(a, m)$  thì  $d$  là ước của  $b$ .

Như vậy ta có thể tự do thực hiện các phép tính số học thông thường trên tập  $\mathbb{Z}/n\mathbb{Z}$ .

Nếu  $x \in \mathbb{Z}/n\mathbb{Z}$  (hay  $\mathbb{Z}_n$ ) và  $\text{UCLN}(x, n) = 1$ , thì tồn tại các số  $u, v$  sao cho  $u.x + v.n = 1$ , tức là  $u.x \equiv 1 \pmod{n}$ , nên người ta nói  $x$  có nghịch đảo (trong  $\mathbb{Z}/n\mathbb{Z}$ ) là  $u$ , ký hiệu  $x^{-1}$  hay  $1/x$ .

**Ví dụ:** Xét vành  $\mathbb{Z}/9\mathbb{Z} = \{0, 1, 2, \dots, 8\}$ . Để tìm phần tử nghịch đảo của 5 (tức là  $5^{-1}$ ) ta dùng thuật toán Euclid mở rộng, tức là phân tích:

$$9 = 1.5 + 4 \Rightarrow 4 = 9 - 1.5$$

$$5 = 1.4 + 1 \Rightarrow 1 = 5 - 1.4 = 5 - 1.(9 - 1.5) = \mathbf{2.5} - 1.9$$

$$4 = 1.4 + 0$$

$$\text{Suy ra: } 2.5 \equiv 1 \pmod{9} \text{ hay } 5^{-1} = 2 \pmod{9}$$

Tập các phần tử trong  $\mathbb{Z}/n\mathbb{Z}$  **mà có nghịch đảo** thường được ký hiệu là  $\mathbb{Z}/n\mathbb{Z}^*$ .

Trên tập  $\mathbb{Z}/n\mathbb{Z}$ , ta có thể đưa vào phép tính **cộng, trừ, nhân, chia**.

Nếu  $a \equiv b \pmod{n}$ ,  $c \equiv d \pmod{n}$  với  $\text{gcd}(c, n) = 1$ , thì:  **$ac^{-1} \equiv bd^{-1} \pmod{n}$**  (Nghĩa là ta chia 2 vế của phép  $a \equiv b \pmod{n}$  cho  $c$  hoặc  $d$ , tức là ta nhân 2 vế với nghịch đảo của  $c$  hoặc  $d$ ).

**Ví dụ:** Xét  $\mathbb{Z}/9\mathbb{Z}$ , ta có  $\mathbb{Z}/9\mathbb{Z}^* = \{1, 2, 4, 5, 7, 8\}$ , ta có  $5^{-1} = 2 \pmod{9}$  và phép chia của 2 cho 5 (trong  $\mathbb{Z}/9\mathbb{Z}^*$ ) được thực hiện như sau:  $\frac{2}{5} = 2.5^{-1} = 2.2 \equiv 4 \pmod{9}$ . Từ đó,  $2 = 5.4 \pmod{9}$  vì  $5.4 = 20 = 2.9 + 2$ .

## 2. Phương trình đồng dư tuyến tính:

Có dạng  $a.x \equiv b \pmod{m}$ , với  $a, b, m \in \mathbb{Z}$ ,  $m > 0$ . Gọi  $g = \text{UCLN}(a, m)$ . Có 2 trường hợp xảy ra:

\* **Trường hợp 1:**  $g = 1 \Rightarrow x \equiv a^{-1}.b \pmod{m}$

\* **Trường hợp 2:**  $g \neq 1$

+ Nếu  $b \nmid g$ , phương trình có nghiệm  $x_0 \equiv \left(\frac{a}{g}\right)^{-1} \cdot \frac{b}{g} \pmod{\frac{m}{g}}$ , trong đó  $\frac{a}{g}$  nguyên tố cùng nhau

với  $\frac{m}{g}$ , và phương trình này có  $g$  nghiệm. Khi đó tập nghiệm của phương trình sẽ là:

$$x = x_0 + k \cdot \frac{m}{g}, k = \overline{0, (g-1)}.$$

+ Nếu  $b \nmid g$ , phương trình vô nghiệm.

**Ví dụ:**  $6x \equiv 9 \pmod{15}$ .

Ta có  $g = \text{gcd}(a, m) = \text{gcd}(6, 15) = 3 \neq 1$ .

Kiểm tra  $b$  có chia hết cho  $g$  không? Dễ thấy 9 chia hết cho 3, tức là  $b$  chia hết cho  $g$ . Vậy phương

trình có nghiệm  $\Rightarrow x_0 \equiv \left(\frac{a}{g}\right)^{-1} \cdot \frac{b}{g} \pmod{\frac{m}{g}} = 2^{-1}.3 \pmod{5} = 3.3 \pmod{5} = 4 \pmod{5}$ .

Tập nghiệm của phương trình là:  $x = x_0 + k \cdot \frac{m}{g} = 4 + 5k, k = 0, 1, 2$ .

## 3. Định lý Fermat nhỏ:

Dùng để đơn giản hóa việc tính toán các lũy thừa lớn.

- Nếu  $p$  là số nguyên tố,  $a$  là một số nguyên thì  $a^p \equiv a \pmod{p}$ .

- **Hệ quả:** Nếu  $\text{gcd}(p, a) = 1$  thì  $a^{p-1} \equiv 1 \pmod{p}$ .

Ta có thể viết lại biểu thức trên như sau:  $a^{p-1} = k.p + 1 \Rightarrow a^{p-1} - 1 = k.p \Rightarrow a^{p-1} - 1 \equiv 0 \pmod{p}$ .

$$\text{Ngoài ra: } \left. \begin{array}{l} a^{p-1} \equiv 1 \pmod{p} \\ a^{p-1} = a.a^{p-2} \end{array} \right\} \Rightarrow \left. \begin{array}{l} a.a^{p-2} \equiv 1 \pmod{p} \\ a.a^{-1} \equiv 1 \pmod{p} \end{array} \right\} \Rightarrow \boxed{a^{-1} \equiv a^{p-2} \pmod{p}} \quad (7).$$

**Ví dụ:**  $a = 2, b = 5$ .

Theo định lý Fermat:  $2^{5-1} = 2^4 \equiv 1 \pmod{5}$ .

$$(7) \Rightarrow 2^{-1} \equiv 2^{5-2} \pmod{5} \Rightarrow 2^{-1} \equiv 2^3 \pmod{5} \Rightarrow 2^{-1} \equiv 3 \pmod{5}.$$

**Nhận xét:** Ta có thể áp dụng hệ quả định lý Fermat để tìm nghịch đảo của 1 phần tử nằm trong  $\mathbb{Z}/n\mathbb{Z}$ .

- **Mở rộng:** Nếu  $\text{UCLN}(a, p) = 1$  thì  $a^{\phi(p)} \equiv 1 \pmod{p}$ , với  $\phi(p)$  là hàm Euler.

Trong trường hợp  $p$  là số nguyên tố, ta có  $\phi(p) = p - 1$ , và lúc đó ta cũng thu được định lý Fermat nhỏ.

Hàm Euler  $\phi(p)$  đếm số lượng số nguyên dương nhỏ hơn  $p$  và nguyên tố cùng nhau với  $p$ , được tính bởi công thức tổng quát:

$$\phi(p) = p \cdot \prod_{i=1}^m \left(1 - \frac{1}{p_i}\right), \text{ với } p = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_m^{k_m} \text{ (phân tích } p \text{ thành tích các thừa số nguyên tố).}$$

Tuy nhiên, ta có thể tính nhanh  $\phi(p)$  bằng cách:  $\phi(p) = \prod_{i=1}^m \phi(p_i)$ .

**Ta kiểm tra công thức tổng quát bằng phương pháp liệt kê.**

Giả sử cần tính  $\phi(15) = 15 \cdot \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 8$ , nghĩa là có 8 số nguyên dương nhỏ hơn 15 và nguyên tố cùng nhau với 15.

Xét trong  $\mathbb{Z}_{15} \setminus \{0\} = \{k_i\} = \{1, \dots, 14\}$ , vì dễ thấy  $\text{UCLN}(a, 0) = |a|$ , với mọi  $a \neq 0$ , vì mọi số khác 0 bất kỳ là ước của 0, và ước lớn nhất của  $a$  là  $|a|$ . Đây là trường hợp cơ sở trong thuật toán Euclid.

$$k_1 = 1: \gcd(1, 15) = 1$$

$$k_8 = 8: \gcd(8, 15) = 1$$

$$k_2 = 2: \gcd(2, 15) = 1$$

$$k_9 = 9: \gcd(9, 15) = 3$$

$$k_3 = 3: \gcd(3, 15) = 3$$

$$k_{10} = 10: \gcd(10, 15) = 5$$

$$k_4 = 4: \gcd(4, 15) = 1$$

$$k_{11} = 11: \gcd(11, 15) = 1$$

$$k_5 = 5: \gcd(5, 15) = 5$$

$$k_{12} = 12: \gcd(12, 15) = 3$$

$$k_6 = 6: \gcd(6, 15) = 3$$

$$k_{13} = 13: \gcd(13, 15) = 1$$

$$k_7 = 7: \gcd(7, 15) = 1$$

$$k_{14} = 14: \gcd(14, 15) = 1$$

Vậy có 8 giá trị nguyên dương nhỏ hơn 15 và nguyên tố cùng nhau với 15.

**Ta cũng có thể chứng minh:** Nếu  $p$  là số nguyên tố thì  $\phi(p) = p - 1$ .

+ Nếu  $p$  là số nguyên tố, thì  $\forall k \in \mathbb{Z}_p \setminus \{0\}$  đều nguyên tố cùng nhau với  $p$ .

+ Giả sử  $\exists k_i: \gcd(k_i, p) \neq 1, k_i < p$ . Vậy dễ thấy rằng  $p$  không thể là số nguyên tố (!).

+ Suy ra số lượng số nguyên dương nhỏ hơn  $p$  và nguyên tố cùng nhau với  $p$  chính bằng số lượng phần tử nguyên thuộc đoạn  $[1, p - 1]$ . Vì thế ta có thể nói rằng  $\phi(p) = p - 1$  khi  $p$  là số nguyên tố (đpcm).

**Ví dụ:** Với  $p = 15$  ta có  $\phi(15) = \phi(3) \cdot \phi(5) = 2 \cdot 4 = 8$  và do đó với mỗi số nguyên  $a$  sao cho  $\gcd(p, a) = 1$ , ta có  $7^8 \equiv 1 \pmod{15}$ ,  $11^8 \equiv 1 \pmod{15}$ , ...

- **Vậy định lý Fermat lớn là gì?**  $x^n + y^n = z^n$ , với  $n > 2$  thì không tồn tại nghiệm nguyên khác 0 nào. Đây cũng chính là nền tảng để xây dựng nên định lý Pytago trong tam giác vuông quen thuộc.

- **Hệ quả 1:** Nếu  $\text{UCLN}(c, n) = 1$ ,  $a \equiv b \pmod{\phi(n)}$  với  $a, b$  là các số tự nhiên, thì  $c^a \equiv c^b \pmod{n}$  &

ta có:  $c^a \bmod n = c^{b \bmod \phi(n)} \bmod n$

**Nhận xét:** Hệ quả này giúp ta giảm nhẹ sự phức tạp trong việc tính toán đồng dư của lũy thừa bậc cao một cách rất đáng kể.



**Ví dụ:** Tính  $5^{1005} \bmod 14$

Ta có  $\phi(14) = \phi(7) \cdot \phi(2) = 6$ .  $1 = 6$  và  $1005 \equiv 3 \pmod{6}$ , suy ra:

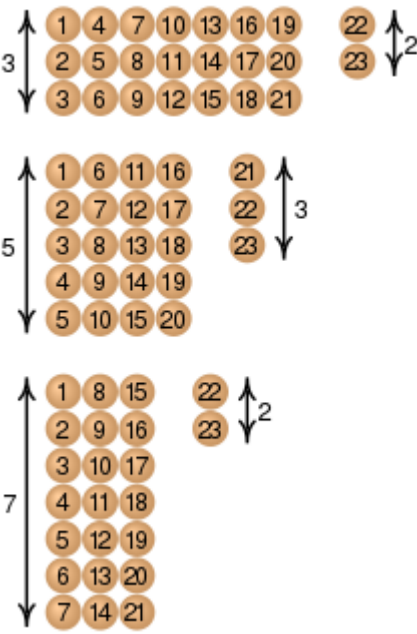
$$5^{1005} \bmod 14 = 5^3 \bmod 14 = 125 \bmod 14 = 13.$$

- **Hệ quả 2:** Nếu  $e, d$  là các số nguyên thỏa mãn  $e.d \equiv 1 \pmod{\phi(n)}$  thì với mọi số  $c$  nguyên tố cùng nhau với  $m$ , ta có  $(c^e)^d \equiv c \pmod{n}$ . Rõ ràng, với  $a = e.d$  và  $b = 1$ , từ Hệ quả 1 ta có ngay hệ quả 2.

#### 4. Định lý số dư Trung Hoa

Định lý số dư Trung Quốc (Chinese Theorem of Remainders) là tên người phương Tây đặt cho định lý này. Người Trung Quốc gọi nó là bài toán Hàn Tín điểm binh.

Tương truyền rằng khi Hàn Tín điểm quân, ông cho quân lính xếp hàng 3, hàng 5, hàng 7 rồi **báo cáo số dư**. Từ đó ông tính chính xác quân số đến từng người.

	<p>Từ hình bên ta thấy:</p> <ul style="list-style-type: none"> <li>✓ Khi xếp hàng 3 thì dư 2 người, suy ra số lượng binh sẽ có dạng <math>3k + 2</math>, nghĩa là số chia cho 3 dư 2, và sẽ bao gồm các số: 2, 5, 8, 11, 14, 17, 20, <b>23</b>, 26, ...</li> <li>✓ Khi xếp hàng 5 thì dư 3 người, suy ra số lượng binh sẽ có dạng <math>5k + 3</math>, nghĩa là số chia cho 5 dư 3, và sẽ bao gồm các số: 3, 8, 13, 18, <b>23</b>, 28, 35, ...</li> <li>✓ Khi xếp hàng 7 thì dư 2 người, suy ra số lượng binh sẽ có dạng <math>7k + 2</math>, nghĩa là số chia cho 7 dư 2, và sẽ bao gồm các số 2, 9, 16, <b>23</b>, 30, 37, 43, ...</li> </ul> <p>Vậy ta có thể quy về bài toán tìm nghiệm <math>x = \begin{cases} 3k + 2 \\ 5k + 3 \\ 7k + 2 \end{cases} \quad (k \in \mathbb{Z})</math>.</p> <p>Hay ta có thể viết rằng: <math>x \equiv \begin{cases} 2 \pmod{3} \\ 3 \pmod{5} \\ 2 \pmod{7} \end{cases}</math>. Đây được gọi là <b>hệ phương trình đồng dư</b>.</p> <p>Từ đó ta có thể suy ra được <math>x = \underbrace{23}_{\substack{\text{số chung} \\ \text{xuất hiện} \\ \text{đầu tiên}}} + \underbrace{105}_{\text{BCNN}(3, 5, 7)} \cdot k \quad (k \in \mathbb{Z})</math>.</p>
--	---

**Ta có định lý:**

Cho  $n$  số nguyên dương  $m_1, m_2, \dots, m_n$  đôi một nguyên tố cùng nhau. Khi đó hệ đồng dư tuyến tính:



$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \end{cases}.$$

Hệ phương trình đồng dư nói trên có nghiệm duy nhất theo modulo  $M = m_1 m_2 \dots m_n$ :

$$x \equiv a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \dots + a_n \cdot M_n \cdot y_n \pmod{M}$$

Với  $M_1 = \frac{M}{m_1}, M_2 = \frac{M}{m_2}, \dots, M_n = \frac{M}{m_n}$  ( $M_k$  bằng tích của các  $m_i$  ngoại trừ  $m_k$ ) và  $\begin{cases} y_1 = M_1^{-1} \pmod{m_1} \\ y_2 = M_2^{-1} \pmod{m_2} \\ \dots \\ y_n = M_n^{-1} \pmod{m_n} \end{cases}$ .

**Ví dụ:** Ta giải bài toán điểm binh trên như sau:  $x \equiv \begin{cases} 2 \pmod{3} \\ 3 \pmod{5} \\ 2 \pmod{7} \end{cases}$

$$\begin{cases} M_1 = \frac{M}{m_1} = m_2 \cdot m_3 = 5 \cdot 7 = 35 \\ M_2 = \frac{M}{m_2} = m_1 \cdot m_3 = 3 \cdot 7 = 21 \\ M_3 = \frac{M}{m_3} = m_1 \cdot m_2 = 3 \cdot 5 = 15 \end{cases} \quad \begin{cases} y_1 = M_1^{-1} \pmod{m_1} = 35^{-1} \pmod{3} = 2 \\ y_2 = M_2^{-1} \pmod{m_2} = 21^{-1} \pmod{5} = 1 \\ y_3 = M_3^{-1} \pmod{m_3} = 15^{-1} \pmod{7} = 1 \end{cases}$$

$$M = m_1 \cdot m_2 \cdot m_3 = 3 \cdot 5 \cdot 7 = 105$$

$$\Rightarrow x \equiv a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + a_3 \cdot M_3 \cdot y_3 \pmod{M}$$

$$\Leftrightarrow x \equiv 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \pmod{105}$$

$$\Leftrightarrow x \equiv 233 \pmod{105}, \text{ mà } 233 \pmod{105} = 23 \Rightarrow 233 \equiv 23 \pmod{105} \Rightarrow x \equiv 23 \pmod{105}$$

Như vậy, tập nghiệm  $x$  có dạng:  $x = 23 + 105 \cdot k$  ( $k \in \mathbb{Z}$ ).

\* Trong trường hợp các số nguyên dương  $m_1, m_2, \dots, m_n$  **không đôi một nguyên tố cùng nhau**, gọi  $d_{ij}$  là UCLN ( $m_i, m_j$ ), điều kiện để hệ phương trình đồng dư trên có nghiệm là  $d_{ij}$  chia chẵn cho  $|a_i - a_j|$ .

\* **Giải nghĩa:**  $a$  chia chẵn cho  $b$  khi  $a:b$  hoặc  $b:a$ .

Định lý số dư Trung Quốc khẳng định về **sự tồn tại duy nhất của một lớp thặng dư các số nguyên thỏa mãn đồng thời nhiều đồng dư thức tuyến tính**. Do đó có thể sử dụng định lý để giải quyết những bài toán về **sự tồn tại và đếm các số nguyên thỏa mãn một hệ các điều kiện quan hệ đồng dư, chia hết...**, hay **đếm số nghiệm của phương trình đồng dư**. Bản chất của bài toán Hàn Tín điểm binh là việc giải hệ phương trình đồng dư bậc nhất.

## V. TRƯỜNG HỮU HẠN

### 1. Trường $G_p$

Khi  $p \in \mathbb{Z}$ ,  $p > 1$ , ta có thể thực hiện các phép cộng (+), trừ (-), nhân ( $\times$ ) trên tập  $\mathbb{Z} / p\mathbb{Z}$ .

Khi  $p$  là số nguyên tố, với mỗi phần tử  $\alpha \in \mathbb{Z} / p\mathbb{Z}$  khác 0, ta luôn tìm được phần tử nghịch đảo  $\alpha^{-1} \in \mathbb{Z} / p\mathbb{Z}$ . Do đó trong trường hợp này ta vẫn thực hiện được phép chia trên tập  $\mathbb{Z} / p\mathbb{Z}$ .

**Chỉ khi  $p$  là số nguyên tố,  $\mathbb{Z} / p\mathbb{Z}$  mới thỏa cấu trúc của một trường.** Ta kí hiệu trường này là  $G_p$ . Vì trường này có hữu hạn số phần tử, nên được gọi là trường hữu hạn (Galois field). Ký hiệu của trường này ta có thể viết đầy đủ là  $GF(p)$ .

\* **Hiểu đơn giản:** Trường là một tập hợp được trang bị hai phép toán cộng và nhân, thỏa mãn một số tính chất (giao hoán, phân phối, phần tử nghịch đảo, v.v.). Ví dụ: tập số thực  $\mathbb{R}$ , tập số hữu tỉ  $\mathbb{Q}$ ... là các trường.

\* Trường có vô hạn phần tử gọi là trường vô hạn, ví dụ  $\mathbb{R}$ ,  $\mathbb{Q}$  là các trường vô hạn. Ngược lại, trường có hữu hạn các phần tử gọi là trường hữu hạn. Chẳng hạn  $G_p$  là một trường hữu hạn.

**\* Bậc của một trường hữu hạn sẽ bằng số lượng phần tử trong trường đó.**

Tập các phần tử khác 0 của trường  $G_p$  thỏa tính chất của một nhóm nhân, ký hiệu là  $G_p^*$ . Vì thế  $G_p^* = \{1, 2, \dots, p-1\}$ , với  $p$  là số nguyên tố.

\* Để một tập hợp  $G$  với phép nhân tạo thành một nhóm (group) (nhóm nhân), thì cần thỏa mãn 4 tính chất sau:

- **Đóng (Closure):**  $\forall a, b \in G$ , thì  $a * b \in G$ . Tức là nhân hai phần tử bất kỳ trong tập thì kết quả vẫn nằm trong tập.
- **Kết hợp (Associativity):**  $\forall a, b, c \in G$ , ta có:  $(a * b) * c = a * (b * c)$
- **Phần tử đơn vị (Identity element):**  $\exists e \in G$  sao cho:  $a * e = e * a = a, \forall a \in G$ . Nghĩa là  $e$  là phần tử không làm thay đổi giá trị của một phần tử khi nhân  $e$  với phần tử đó.
- **Phần tử nghịch đảo (Inverse element):** Với mỗi phần tử  $a \in G$ , tồn tại  $a^{-1} \in G$  sao cho:  $a * a^{-1} = a^{-1} * a = e$ .
- Nếu phép nhân còn có tính chất giao hoán (commutative):  $a * b = b * a$  thì nhóm đó được gọi là nhóm Abel hoặc nhóm giao hoán.

Một phần tử  $g \in G_p^*$  được coi là phần tử sinh (hoặc căn nguyên thủy) nếu tập các lũy thừa của  $g$  sinh ra được nhóm  $G_p^*$ . Nghĩa là:  $\{g, g^2, \dots, g^{p-1}\} = \{1, 2, \dots, p-1\}$ .

\* Nếu  $G^*$  tồn tại căn nguyên thủy thì được coi là nhóm cyclic (nhóm vòng).

\* Lưu ý: Một nhóm nhân có thể không phải là một trường hữu hạn.

**Ví dụ:** Xét nhóm nhân  $\mathbb{Z}_p^*$ ,  $k = 1, \dots, p-1$ .

$p = 11, \{1, 2, \dots, 10\}$ <b>m:</b> <b><math>m^k \pmod{11}</math></b> 1:        1 <b>2:</b> <b>2, 4, 8, 5, 10, 9, 7, 3, 6, 1</b> 3:        3, 9, 5, 4, 1 4:        4, 5, 9, 3, 1, 5:        5, 3, 4, 9, 1, <b>6:</b> <b>6, 3, 7, 9, 10, 5, 8, 4, 2, 1</b> <b>7:</b> <b>7, 5, 2, 3, 10, 4, 6, 9, 8, 1</b> <b>8:</b> <b>8, 9, 6, 4, 10, 3, 2, 5, 7, 1</b> 9:        9, 4, 3, 5, 1 10:       10, 1  2, 6, 7, 8 căn nguyên thủy modulo 11.	$p = 14, \{1, 3, 5, 9, 11, 13\}$ <b>m</b> : <b><math>m^k \pmod{14}</math></b> 1:        1 <b>3:</b> <b>3, 9, 13, 11, 5, 1</b> <b>5:</b> <b>5, 11, 13, 9, 3, 1</b> 9:        9, 11, 1 11:       11, 9, 1 13:       13, 1  3 và 5 là căn nguyên thủy của modulo 14.
---	--

**Số các phần tử sinh của nhóm  $G_p^*$**  chính bằng số các số nguyên tố cùng nhau với  $(p-1)$ , nghĩa là bằng  $\varphi(p-1)$ .

Nếu  $g$  là phần tử sinh của nhóm  $G_p^*$ , và có một số  $b$  nguyên tố cùng nhau với  $p-1$ , thì  $g^b$  cũng là một phần tử sinh của nhóm  $G_p^*$ .

**Ví dụ:** trên  $G_{11}^*$ , ta tính được số phần tử sinh của nhóm này là:

$$\varphi(11-1) = \varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = (2-1)(5-1) = 4.$$

2 là phần tử sinh của  $G_{11}^*$ . Thấy rằng 7 là số nguyên tố cùng nhau với 10 ( $= 11 - 1$ ) cho nên  $2^7 \pmod{11} = 7$  cũng là một phần tử sinh của  $G_{11}^*$ .

Trong  $G_p^*$ , có đúng  $\frac{p-1}{2}$  phần tử là số chính phương, nói cách khác, **một nửa số phần tử trong  $G_p^*$  là số chính phương.**

Bên cạnh đó, mọi phần tử  $h \in G_p^*$  có thể biểu diễn dưới dạng  $h = g^x \pmod{p}$ . Tuy nhiên việc tìm  $x$  để có được biểu diễn này là khó khăn, và đó cũng là **bài toán logarit rời rạc**. Bài toán này làm cơ sở cho các hệ mật mã hiện đại.

## 2. Trường $G_2^n$

Đây cũng là một trường hữu hạn, nhưng có sự khác biệt đối với trường  $G_p$ .

Ta lấy  $G_2(x)$  là **tập các đa thức có bậc bất kỳ**, với **hệ số nằm trong trường nhị phân  $G_2 = \{0, 1\}$** . Tập hợp này là một vành đa thức trên  $G_2$ .

Với mỗi  $n \in \mathbb{N}$ , có  $2^{n+1}$  đa thức có bậc không vượt quá  $n$ . **Mỗi đa thức được biểu diễn dưới dạng tổng quát như sau:**

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, \text{ với } a_i \in G_2.$$

Ta thực hiện cộng hoặc nhân đa thức theo quy tắc thông thường, nhưng lưu ý rằng các hệ số phải thuộc trường  $G_2$ . **Ví dụ:**  $(x^4 + x^2 + x)(x^2 + x) = x^6 + x^5 + x^4 + \underbrace{x^3 + x^3}_0 + x^2 = x^6 + x^5 + x^4 + x^2$

Đa thức được gọi là **bất khả quy** (trên một trường bất kỳ) nếu nó không thể phân tích được thành **tích của các đa thức có bậc nhỏ hơn**. Ở ví dụ trên,  $x^6 + x^5 + x^4 + x^2$  không phải là đa thức bất khả quy vì nó vẫn còn phân tích được thành tích của các đa thức có bậc nhỏ hơn. Thật vậy:  $x^6 + x^5 + x^4 + x^2 = x^2(x^4 + x^3 + x^2 + 1)$ .

**Xét ví dụ khác:** Xét 2 đa thức  $x^2 - 3$  và  $x^2 + 3$ . Ta biết rằng nếu phương trình bậc 2  $ax^2 + bx + c = 0$  có 2 nghiệm  $x_1, x_2$  thì  $ax^2 + bx + c = a(x - x_1)(x - x_2)$ . Vì thế ta có thể kiểm tra tính bất khả quy của 2 đa thức ở ví dụ này bằng cách đi tìm nghiệm của chúng trong các trường tương ứng.

- Xét trên trường  $\mathbb{Q}$  (số hữu tỷ):  $\begin{cases} x^2 + 3 = 0 \Leftrightarrow \nexists x \in \mathbb{Q} \\ x^2 - 3 = 0 \Leftrightarrow x = \pm\sqrt{3} \notin \mathbb{Q} \end{cases} \rightarrow 2 \text{ đa thức này bất khả quy trên } \mathbb{Q}.$
- Xét trên trường  $\mathbb{R}$ :
  - $x^2 + 3 = 0 \Leftrightarrow \nexists x \in \mathbb{R} \rightarrow x^2 + 3$  bất khả quy trên  $\mathbb{R}$ .
  - $x^2 - 3 = 0 \Leftrightarrow x = \pm\sqrt{3} \in \mathbb{R} \rightarrow x^2 - 3$  khả quy trên  $\mathbb{R}$ . Thật vậy,  $x^2 - 3 = (x - \sqrt{3})(x + \sqrt{3})$ .

Tập  $G_2(x)$  cũng có phép đồng dư theo modulo một đa thức. Khi đó  $G_2(x)$  sẽ được phân thành các **lớp** với các **đại diện là các đa thức có bậc thấp hơn bậc của đa thức mà ta lấy làm modulo**. **Ví dụ:** Nếu cho đa thức  $x^3 + x + 1$  (bất khả quy) làm modulo thì tập  $G_2(x)/(x^3 + x + 1)$  gồm các đa thức bậc nhỏ hơn 3, gồm  $\{0, 1, x, x + 1, x^2 + 1, x^2 + x + 1\}$ , trong đó phần tử 0 chính là đại diện của đa thức chọn làm modulo, nghĩa là  $x^3 + x + 1 = 0$ .

**Tổng quát,** người ta chứng minh được rằng, với mỗi đa thức bất khả quy thuộc  $GF_d(x)$  có bậc  $d$ , tập hợp  $G_2(x)/GF_d(x)$  là một trường, chứa  $2^d$  phần tử. Trường này được ký hiệu là  $G_{2^d}$ . Mỗi phần tử trong trường này được đại diện bởi **một đa thức có bậc không quá  $d - 1$** .

Người ta cũng chứng minh được rằng, **tập các phần tử khác 0 của trường  $G_{2^d}$  cũng lập thành một nhóm nhân**, ký hiệu là  $G_{2^d}^*$ . Phần tử sinh của nó phải có các lũy thừa có bậc là ước của  $(2^d - 1)$ , khác 1; số lượng phần tử sinh trong nhóm này là  $\varphi(2^d - 1)$ . **Ví dụ:** Ta dễ dàng thấy rằng  $x$  là phần tử sinh của  $G_{2^3}^*$  khi thực hiện phép đồng dư theo modulo đa thức  $(x^3 + x + 1)$ . Với  $g = x$ , ta có:

- $g = x$
- $g^2 = x^2$
- $g^3 = x^3 = x + 1$
- $g^4 = x^4 = x \cdot x^3 = x(x + 1) = x^2 + x$
- $g^5 = x^5 = x \cdot x^4 = x(x^2 + x) = x^3 + x^2 = (x + 1) + x^2 = x^2 + x + 1$

$$\blacksquare g^6 = x^6 = x \cdot x^5 = x(x^2 + x + 1) = x^3 + x^2 + x = (x + 1) + x^2 + x = x^2 + 1$$

$$\blacksquare g^7 = x^7 = x \cdot x^6 = x(x^2 + 1) = x^3 + x = (x + 1) + x = 1$$

Một phần tử của nhóm  $G_{2^d}^*$  được gọi là **chính phương** khi nó là bình phương của một phần tử khác trong nhóm. **Ví dụ:**  $x^2$  là chính phương trong  $G_{2^3}^*$  vì nó là bình phương của phần tử  $x$ .

Mỗi phần tử của trường  $G_{2^d}$  (hoặc nhóm  $G_{2^d}^*$ ) có thể biểu diễn dễ dàng trên máy tính bởi **một chuỗi nhị phân lập từ các hệ số của đa thức** tương ứng. Vì thế, trường  $G_{2^d}$  thường được sử dụng nhiều hơn là trường  $G_p$ , nhất là khi  $p$  khá lớn. **Ví dụ:**  $x^4 + x^2 + 1 = 1.x^4 + 0.x^3 + 1.x^2 + 0.x + 1$  sẽ được biểu diễn bởi chuỗi nhị phân **10101**.

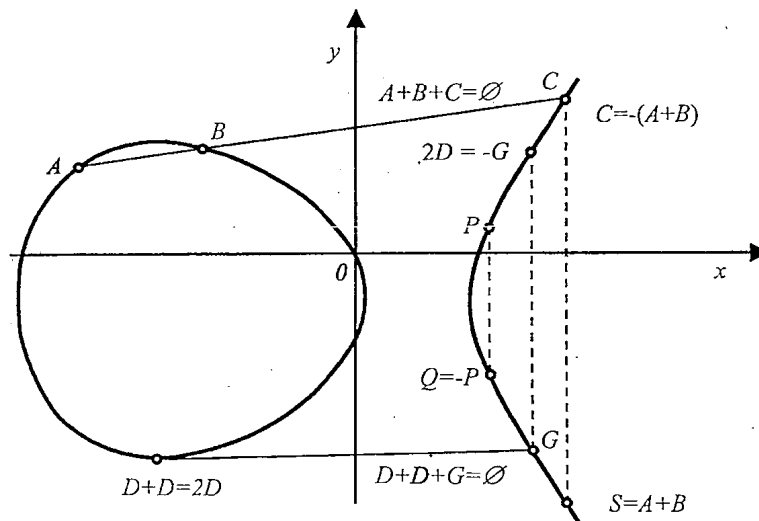
Ta có thể xây dựng được trường hữu hạn dạng  $G_{p^d}^*$ , với  $p$  là số nguyên tố bất kỳ. Khi  $p > 2$ , có thể chỉ ra rằng một phần tử là chính phương khi và chỉ khi lũy thừa của nó với bậc  $\frac{(p^d - 1)}{2}$  đúng bằng 1.

## VI. ĐƯỜNG CONG ELLIPTIC

### 1. Khái niệm

Đường cong Elliptic là tập các điểm thỏa phương trình có dạng:  $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$  và được bổ sung thêm **1 điểm tại vô cùng**, được kí hiệu là  $\emptyset$ .

Trên tập điểm của đường cong ta thiết lập các quy tắc sau:



\* **Quy tắc cộng:** tổng của  $A, B, C$  thẳng hàng (cùng thuộc 1 đường cong) sẽ bằng điểm vô cùng (tại điểm vô cùng được quy ước là 0):  $A + B + C = \emptyset$ .

\* **Quy tắc điểm nghịch đảo:** Xét 2 điểm  $P, Q$  thuộc đường cong.

+ Khi hai điểm  $P, Q$  cùng nằm trên một **đường thẳng đứng** thì nó thẳng hàng với điểm vô cùng:  $P + Q + \emptyset = \emptyset$  hay  $P = -Q$ .

+ Khi hai điểm  $A, B$  **không** nằm trên một **đường thẳng đứng** thì tồn tại điểm  $C$  thẳng hàng với hai điểm này, và theo quy tắc cộng ta có:  $A + B + C = \emptyset$  hay  $A + B = -C$ , bên cạnh đó **điểm đối xứng của  $C$  qua trục hoành, tức là điểm  $S$** , là kết quả của phép cộng 2 điểm này:  $A + B = S$ .

\* **Quy tắc cộng một điểm với chính nó:** Xét điểm  $D$  thuộc đường cong:  $D + D = 2D$ . Về một đường tiếp tuyến tại  $D$ , đường này sẽ cắt đường cong tại một điểm khác, đặt là  $G$ .

Theo quy tắc lấy điểm nghịch đảo ta có:  $2D + G = \emptyset$  hay  $2D = -G$ .

Xét 2 điểm khác hoành độ  $P_1 = (x_1, y_1)$ ,  $P_2 = (x_2, y_2)$ ,  $x_1 \neq x_2$ , phép cộng 2 điểm này biểu diễn bởi:  $P_1 + P_2 = P_3 = (x_3, y_3)$ . Ta tính  $x_3, y_3$  dựa vào hai trường hợp:

\* Trường hợp 1:  $x_1 \neq x_2$  thì 
$$\begin{cases} x_3 = \alpha^2 + a_1 \alpha - (x_1 + x_2 + a_2) \\ y_3 = \alpha(x_1 - x_3) - a_1 x_3 - a_3 - y_1 \end{cases}$$

với  $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ : **độ dốc** của đường thẳng đi qua  $P_1, P_2$  so với trục  $Ox$ .

\* Trường hợp 2:  $P_1 = P_2$  thì công thức tính  $\alpha$  phức tạp hơn nhiều (tính tiếp tuyến thông qua đạo hàm):

$$\alpha = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

Vì thế, để đơn giản hơn, ta sử dụng phương trình đường cong elliptic có dạng **Weierstrass**:

$$y^2 = x^3 + ax + b \quad (\text{với } a_1 = a_2 = a_3 = 0, a_4 = a, a_6 = b), \text{ điều kiện là } 4a^3 + 27b^2 \neq 0.$$

Ta tính  $x_3, y_3$  dựa vào hai trường hợp:

\* Trường hợp 1:  $x_1 \neq x_2$  thì 
$$\begin{cases} x_3 = \alpha^2 - (x_1 + x_2) \\ y_3 = -y_1 + \alpha(x_1 - x_3) \end{cases} \quad \text{với } \alpha = \frac{y_2 - y_1}{x_2 - x_1}.$$

\* Trường hợp 2:  $P_1 = P_2$  thì 
$$\begin{cases} x_3 = \alpha'^2 - 2x_1 \\ y_3 = -y_1 + \alpha'(x_1 - x_3) \end{cases} \quad \text{với } \alpha' = \frac{3x_1^2 + a}{2y_1}.$$

## 2. Đường cong elliptic trên trường hữu hạn

Xét đường cong  $(E)$  trên trường  $G_p$ , với  $p > 2$  là số nguyên tố, tập hợp các điểm của đường cong  $(E)$  sẽ được ký hiệu là  $E(G_p)$ . Đây là một **tập hợp điểm rời rạc**, không phải là một “đường cong” theo nghĩa thông thường, và do đó không có hình ảnh minh họa như trường số thực.

Nếu  $g$  là **phần tử sinh** nhóm  $G_p^*$  thì các lũy thừa bậc **chẵn** của nó là **số chính phương**.

Khi đặc số của trường không phải là 2 hay 3, bằng phép đổi biến tuyến tính, người ta luôn có thể đưa phương trình đường cong elliptic về dạng Weierstrass:  $y^2 = x^3 + ax + b$  (Dạng chuẩn tắc của đường cong *Elliptic*), khi đó công thức cộng các điểm có dạng đã nêu ở phần trước.

\* **Đặc số** của một trường là **số lần ta cộng số 1 với chính nó** cho ra kết quả **bằng 0**.

+ Nếu cộng mãi mà không bao giờ ra 0  $\rightarrow$  **đặc số là 0**.

+ Nếu sau  $p$  lần cộng mà được 0  $\rightarrow$  **đặc số là  $p$** .

**Cách tìm các điểm  $(x, y)$  thuộc  $(E)$ :**

\* **Bước 1:** Với mỗi giá trị  $x_i \in G_p$ , ta thế vào vế phải của phương trình đường cong  $y^2 = x^3 + ax + b$ , giả sử ta được kết quả là  $a_i'$ .

$$a_i' \equiv x_i^3 + ax_i + b \pmod{p}$$

\* *Bước 2:* Bài toán trở thành tìm  $y \in G_p$  sao cho  $y^2 \equiv a_i' \pmod{p}$ .

+ Nếu  $a_i'$  là số chính phương trong  $G_p^*$  thì phương trình có 2 nghiệm.

+ Ngược lại thì phương trình vô nghiệm.

Một điểm  $D \in E(G_p)$  được coi là phần tử sinh trong  $E(G_p)$  nếu tập các bội của điểm này sinh được tập các điểm của  $E(G_p)$ .

**Ví dụ:** Với đường cong  $E$  có phương trình  $y^2 = x^3 + 1$ , tập điểm của trường  $G_5$  nằm trên đường cong này, tức là tập  $E(G_5)$  (*thực hiện phép đồng dư modulo 5*), được xác định như sau:

Trên trường  $G_5 = \{0, 1, 2, 3, 4\}$  chỉ có 3 phần tử “chính phương” là 0, 1, 4 ( $0 = 0^2$ ,  $1 = 1^2 = 4^2$ ,  $4 = 2^2 = 3^2$ ), do đó với  $x = 1$  hay 3 ta thấy ngay  $x^3 + 1$  không phải là chính phương.

Như vậy hoành độ của các điểm trên đường cong chỉ có thể là 1 trong các số còn lại của trường  $G_5$ : 0, 2, 4. Thế lần lượt  $x = 0, 2, 4$  vào phương trình. Ta nhận được các điểm sau

$$x = 0 \Rightarrow y^2 = 0^3 + 1 = 1 \Leftrightarrow y = \pm 1 \Rightarrow \begin{cases} y = 1 \\ y = 4 \end{cases} \text{ (do thực hiện với phép đồng dư modulo 5)} \Rightarrow \begin{cases} A = (0, 1) \\ B = (0, 4) \end{cases}$$

$$x = 2 \Rightarrow y^2 = 2^3 + 1 = 9 \equiv 4 \pmod{5} \Leftrightarrow y = \pm 2 \Rightarrow \begin{cases} y = 2 \\ y = 3 \end{cases} \Rightarrow \begin{cases} C = (2, 2) \\ D = (2, 3) \end{cases}$$

$$x = 4 \Rightarrow y^2 = 4^3 + 1 = 65 \equiv 0 \pmod{5} \Leftrightarrow y = 0 \Rightarrow G(4, 0) \text{ và điểm } \emptyset.$$

Như vậy  $E(G_5)$  có 6 điểm rời rạc.

Lấy điểm  $D = (2, 3)$  trên “đường cong”, ta tính được các bội của điểm này như sau:

$$\begin{aligned} \bullet \text{ Tính } 2D = (x_3, y_3): & \begin{cases} x_3 = \left( \frac{3 \cdot 2^2 + 0}{2 \cdot 3} \right)^2 - 2 \cdot 2 = 0 \\ y_3 = -3 + \left( \frac{3 \cdot 2^2 + 0}{2 \cdot 3} \right) (2 - 0) = 1 \end{cases} \Rightarrow 2D = (0, 1) = A; \\ \bullet \text{ Tính } 3D = 2D + D = (x_4, y_4): & \begin{cases} x_4 = \left( \frac{2 - 0}{3 - 1} \right)^2 - (2 + 0) = -1 \equiv 4 \pmod{5} \\ y_4 = -1 + \left( \frac{2 - 0}{3 - 1} \right) (0 - 4) = -5 \equiv 0 \pmod{5} \end{cases} \Rightarrow 3D = (4, 0) = G; \\ \bullet \text{ Tính } 4D = 2 \cdot 2D = (x_5, y_5): & \begin{cases} x_5 = \left( \frac{3 \cdot 0^2 + 0}{2 \cdot 1} \right)^2 - 2 \cdot 0 = 0 \\ y_5 = -1 + \left( \frac{3 \cdot 0^2 + 0}{2 \cdot 1} \right) \cdot (0 - 0) = -1 \equiv 4 \pmod{5} \end{cases} \Rightarrow 4D = (0, 4) = B; \end{aligned}$$



$$\bullet \quad \text{Tính } 5D = 4D + D = (x_6, y_6) : \begin{cases} \alpha = \frac{3-4}{2-0} = \frac{-1}{2} = -2^{-1} \equiv -3 \equiv 2 \pmod{5} \\ x_6 = 2^2 - 2 = 2 \\ y_6 = -3 + 2(2-2) = -3 \equiv 2 \pmod{5} \end{cases} \Rightarrow 5D = (2, 2) = C;$$

- $6D = 2D + 4D = \emptyset$  (vì  $2D$  và  $4D$  có cùng hoành độ, nên là nghịch đảo của nhau).

Tóm lại, các bội của điểm  $D$  lại cho ta tất cả các điểm trên đường cong hay nói cách khác, **điểm  $D$  có thể được xem là phần tử sinh** của tập  $E(G_5)$ .