Mục lục

Phần IV

Đại số hiện đại ứng dụng

Chương 13

Vành và số học đồng dư

13.1 Cấu trúc vành: định nghĩa và ví dụ

Định nghĩa 13.1. *Cho cặp $(G, \circ)$ gồm tập $G \neq \varnothing$ và phép toán (hai ngôi) $\circ$ đóng trên G.*

a) $\circ$ *có tính kết hợp, nếu* $(a \circ b) \circ c = a \circ (b \circ c)$, $\forall a, b, c \in G$.

b) $\circ$ *có tính giao hoán, nếu* $a \circ b = b \circ a$, $\forall a, b \in G$.

c) $\circ$ *có đơn vị, nếu* $\exists \iota \in G$, $a \circ \iota = \iota \circ a = a$, $\forall a \in R$. *Khi đó* ι *gọi là một đơn vị của* $\circ$.

d) Phần tử $a \in G$ *gọi là khả nghịch (hay, có nghịch đảo), nếu* $\exists b \in G$, $a \circ b = b \circ a = \iota$. *Khi đó* b *gọi là một nghịch đảo của* a.

$(G, \circ)$ gọi là một nhóm, nếu $\circ$ có tính kết hợp, có đơn vị, và mọi phần tử đều khả nghịch. Nếu $\circ$ có tính giao hoán, thì nhóm $(G, \circ)$ gọi là nhóm giao hoán, hay nhóm Abel[*].

.

Nếu không có nhầm lẫn về phép toán, ta ký hiệu $(G, \circ)$ bởi G.

Do tính kết hợp, ta có thể viết $a \circ b \circ c$ thay cho $(a \circ b) \circ c$ và $a \circ (b \circ c)$. Theo nguyên lý quy nạp, nếu $\forall n, r \in \mathbb{Z}^+$ với $n \geq 3$ và $1 \leq r < n$, thì

$$a_1 \circ a_2 \circ \cdots \circ a_r \circ a_{r+1} \circ \cdots \circ a_n \overset{đn}{=\!=} (a_1 \circ a_2 \circ \cdots \circ a_r) \circ (a_{r+1} \circ \cdots \circ a_n).$$

Một định nghĩa đệ quy về lũy thừa của a: $a^n = \underbrace{a \circ a \circ \cdots \circ a}_{n \text{ lần}}$ xác định bởi

1) $a^0 = \iota$, và

2) $a^n = a \circ a^{n-1}$, hoặc $a^n = a^{n-1} \circ a$, $n = 1, 2, \ldots$

Định lý sau chỉ ra tính duy nhất của đơn vị và phần tử nghịch đảo.

Định lý 13.1. *Cho tập $G \neq \varnothing$ với phép toán $\circ$. Khi đó*

a) Đơn vị của $\circ$, nếu có, là duy nhất.

b) Nếu $\circ$ có tính kết hợp, thì $\forall a \in G$, nghịch đảo của a, nếu có, là duy nhất, và ký hiệu a^{-1}.

Với $n \in \mathbb{Z}^+$, định nghĩa $a^{-n} = (a^n)^{-1}$. Ta cũng chứng minh được $a^{-n} = (a^{-1})^n$.

Trong một số trường hợp cụ thể, phép toán $\circ$ viết theo lối nhân, ký hiệu $\cdot$ hoặc $\times$, thay vì $a \cdot b$, ta viết ab, và đơn vị thường ký hiệu là 1. Nhóm giao hoán thường viết theo lối cộng, đơn vị gọi là phần tử trung hòa, ký hiệu 0, và nghịch đảo của a gọi là đối của a, ký hiệu $-a$. Ngoài ra, $a - b \overset{đn}{=\!=} a + (-b)$, và

$$na = \begin{cases} 0 & \text{nếu } n = 0 \\ \underbrace{a + a + \cdots + a}_{n \text{ lần}} & \text{nếu } n > 0 \\ (-n)(-a) = -[(-n)a] & \text{nếu } n < 0. \end{cases}$$

[*]Niels Henrik Abel (1802–1829), nhà toán học Nauy

Ví dụ 13.1. Bảng sau kiểm tra các thuộc tính trên cho các phép toán trên tập số quen thuộc.

$(G, \circ)$	Kết hợp	Giao hoán	ι	a^{-1}	Nhóm
$(\mathbb{N}, +)$	có	có	0	$0^{-1} = 0.\ \forall a \in \mathbb{N} - \{0\},\ \nexists a^{-1}$	
$(\mathbb{Z}^+, +)$	có	có			
$(\mathbb{Z}, +)$	có	có	0	$-a$	có
$(\mathbb{Z}, -)$	không	không			
$(\mathbb{Z}, \cdot)$	có	có	1	$1^{-1} = 1, (-1)^{-1} = -1.\ \forall a \in \mathbb{Z} - \{1, -1\},\ \nexists a^{-1}$	
$(\mathbb{Q}^*, \cdot)$	có	có	1	$\frac{1}{a}$	có

Ví dụ 13.2. Tập $M_n(\mathbb{Z})$ các ma trận nguyên cấp n, với phép cộng ma trận, là một nhóm giao hoán, có phần tử trung hòa là ma trận không $\theta = (0)_n$, và ma trận đối của ma trận $A = (a_{ij})_n \in M_n(\mathbb{Z})$ là $-A = (-a_{ij})_n$.

Ví dụ 13.3. Với $n \in \mathbb{Z}^+, n \geq 2$, tập $GL_n(\mathbb{R})$[*] các ma trận thực cấp n có định thức khác không, với phép nhân ma trận, là một nhóm không giao hoán, có đơn vị ma trận đơn vị I.

Định nghĩa 13.2. *Cho tập $R \neq \varnothing$, trên đó có hai phép toán (hai ngôi) đóng, ký hiệu $+$ và $\cdot$ (có thể hoàn toàn khác với phép cộng và phép nhân thông thường mà ta vốn quen thuộc), và phép $\cdot$ được ưu tiên trước phép $+$. Khi đó $(R, +, \cdot)$ là một vành nếu*

a–d) $(R, +)$ *là nhóm Abel.*

e) *Phép $\cdot$ có tính kết hợp, tức là,* $\forall a, b, c \in R,\ (ab)c = a(bc)$.

f) *Phép $\cdot$ có tính phân phối đối với phép $+$, tức là*

$$\forall a, b, c \in R,\ a(b + c) = ab + ac,\ \text{và}\ (b + c)a = ba + ca.$$

[*] $GL_n(\mathbb{R})$ gọi là nhóm tuyến tính tổng quát.

Định nghĩa 13.3. *Cho vành $(R, +, \cdot)$, có phần tử trung hòa của phép $+$ là 0.*

a) *R gọi là vành giao hoán, nếu phép $\cdot$ có tính giao hoán, tức là $ab = ba$, $\forall a, b \in R$.*

b) *R gọi là vành có đơn vị, nếu phép nhân có phần tử đơn vị khác 0, [và là duy nhất], ký hiệu 1, tức là $1 \in R$ thỏa mãn $1 \neq 0$ và $a1 = 1a = a$, $\forall a \in R$.*

c) *R gọi là không có ước của không, nếu $\forall a, b \in R$, $ab = 0 \Rightarrow a = 0$ hoặc $b = 0$.*

Định nghĩa 13.4. *Cho vành có đơn vị R. Phần tử $a \in R$ gọi là khả nghịch (theo phép nhân) nếu $\exists b \in R$, $ab = ba = 1$. Khi đó phần tử b [là duy nhất] gọi là nghịch đảo của a, ký hiệu a^{-1}.*

Định nghĩa 13.5. *Cho vành R giao hoán, có đơn vị.*

a) *R gọi là miền nguyên nếu R không có ước của không.*

b) *R gọi là trường nếu mọi phần tử khác 0 của R đều khả nghịch.*

Ví dụ 13.4. Các tập $\mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ với hai phép toán cộng và nhân thông thường là các vành. Đối với phép cộng, phần tử trung hòa là 0, phần tử đối của a là $-a$, và đối với phép nhân, phần tử đơn vị là 1. Đây cũng đều là các miền nguyên.
Trên vành $\mathbb{Z}$, $1^{-1} = 1$ và $(-1)^{-1} = -1$, các số còn lại không khả nghịch, nên $\mathbb{Z}$ không là một trường. Các vành $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ đều là trường.

Ví dụ 13.5. Với $n \in \mathbb{Z}^+$, $n \geq 2$, tập $M_n(\mathbb{Z})$ với phép cộng và nhân ma trận là vành không giao hoán, không là miền nguyên.

Để kiểm tra tính không giao hoán của phép nhân ma trận, ta có thể lấy ngẫu nhiên hai ma trận vuông A, B bất kỳ, thì khả năng cao $AB \neq BA$.

Còn để chỉ ra $M_n(\mathbb{Z})$ không là miền nguyên, chẳng hạn với $n = 2$, ta chọn $A = B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \theta$, nhưng $AB = \theta$.

Ví dụ 13.6. Xét tập $\mathbb{Z}$ với hai phép toán $\oplus$ và $\odot$ xác định bởi

$$a \oplus b = a + b - 1, \text{ và } a \odot b = a + b - ab.$$

Kiểm tra các thuộc tính của các phép toán và đưa ra kết luận về $(\mathbb{Z}, \oplus, \odot)$.

Giải. a) Phép toán $\oplus$ có tính kết hợp vì $\forall a, b, c \in \mathbb{Z}$,

$$\begin{aligned}(a \oplus b) \oplus c &= a + b + c - 2\\ &= a \oplus (b \oplus c).\end{aligned}$$

b) Với $a, b \in \mathbb{Z}$, dễ thấy $a \oplus b = b \oplus a$, nên $\oplus$ có tính giao hoán.

c) Ta thử tìm $\theta \in \mathbb{Z}$ sao cho $a \oplus \theta = \theta \oplus a = a, \ \forall a \in \mathbb{Z}$. Do tính giao hoán của $\oplus$, ta chỉ cần xét $a \oplus \theta = a, \ \forall a \in \mathbb{Z} \Leftrightarrow a + \theta - 1 = a, \ \forall a \in \mathbb{Z} \Leftrightarrow \theta = 1 \in \mathbb{Z}$. Do đó, phép toán $\oplus$ có phần tử trung hòa $\theta = 1$.

d) Với $a \in \mathbb{Z}$ tùy ý, ta thử tìm $b \in \mathbb{Z}$ thỏa mãn $a \oplus b = b \oplus a = \theta$. Vẫn do tính giao hoán của $\oplus$, ta chỉ cần xét $a \oplus b = \theta \Leftrightarrow a + b - 1 = 1 \Leftrightarrow b = 2 - a \in \mathbb{Z}$. Phần tử đối của a theo phép toán $\oplus$ là $\ominus a = 2 - a$.

Vậy $(\mathbb{Z}, \oplus)$ là nhóm giao hoán. Ta xét tiếp tính chất của phép toán $\odot$.

e) $\odot$ có tính kết hợp, vì $\forall a, b, c \in \mathbb{Z}$,

$$\begin{aligned}(a \odot b) \odot c &= abc - ab - ac + a - bc + b + c\\ &= a \odot (b \odot c).\end{aligned}$$

f) Với $a, b \in \mathbb{Z}$, dễ thấy $a \odot b = b \odot a$, nên $\odot$ có tính giao hoán.

g) $\forall a, b, c \in \mathbb{Z}$,

$$\begin{aligned}a \odot (b \oplus c) &= -ab - ac + 2a + b + c - 1\\ &= a \odot b \ \oplus \ a \odot c.\end{aligned}$$

Mặt khác, do tính giao hoán của $\odot$, ta cũng có

$$(b \oplus c) \odot a = a \odot (b \oplus c) = a \odot b \ \oplus \ a \odot c = b \odot a \ \oplus \ c \odot a,$$

nên phép nhân $\odot$ có tính phân phối đối với phép cộng $\oplus$.

h) Ta thử tìm $\iota \in \mathbb{Z}$, sao cho $a \odot \iota = \iota \odot a = a,\ \forall a \in \mathbb{Z}$. Do tính giao hoán của $\odot$, ta chỉ cần xét $a \odot \iota = a,\ \forall a \in \mathbb{Z} \Leftrightarrow a + \iota - a\iota = a,\ \forall a \in \mathbb{Z} \Leftrightarrow \iota = 0$. Do đó phần tử đơn vị của phép toán $\odot$ là $\iota = 0$.

i) Ta thử tìm $a, b \in \mathbb{Z}$ sao cho $a \odot b = \theta \Leftrightarrow a + b - ab = 1 \Leftrightarrow a = 1$ hoặc $b = 1 \Leftrightarrow a = \theta$ hoặc $b = \theta$, tức là phép toán $\odot$ không có ước của không.

j) Với $a \in \mathbb{Z} - \{\theta = 1\}$ bất kỳ, ta thử tìm $b \in \mathbb{Z}$ sao cho $a \odot b = b \odot a = \iota$. Do tính giao hoán của $\odot$, ta chỉ cần xét $a \odot b = \iota \Leftrightarrow a + b - ab = 0 \Leftrightarrow b = \dfrac{a}{a-1} \notin \mathbb{Z}$ với hầu hết $a \in \mathbb{Z} - \{1\}$, chẳng hạn, với $a = 3$ thì $b = \dfrac{3}{2} \notin \mathbb{Z}$, tức là $a = 3$ không khả nghịch theo phép toán $\odot$.

Vậy $(\mathbb{Z}, \oplus, \odot)$ là vành giao hoán, có đơn vị, không có ước của không, tức là miền nguyên, và không phải là trường. □

Ví dụ 13.7. Cho tập $\mathcal{U} \neq \varnothing$, xét tập $R = \mathcal{P}(\mathcal{U})$, với hai phép toán Δ và $\cap$.

$$A \Delta B = \{x \mid x \in A \text{ hoặc } x \in B, \text{ nhưng không thuộc cả hai}\}$$
$$= (A \cup B) - (A \cap B) = (A - B) \cup (B - A) = A \cap \overline{B} \ \cup \ \overline{A} \cap B.$$

Chẳng hạn

1) $A \Delta \varnothing = A$,
2) $A \Delta \mathcal{U} = \overline{A}$,
3) $A \Delta A = \varnothing$, và
4) $A \Delta \overline{A} = \mathcal{U}$.

Kiểm tra các thuộc tính của các phép toán và đưa ra kết luận về $(\mathcal{P}(\mathcal{U}), \Delta, \cap)$.

Giải. a) Với $A, B, C \in \mathcal{P}(\mathcal{U})$, hay $A, B, C \subseteq \mathcal{U}$, ta có $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.

b) $\forall A, B \in \mathcal{P}(\mathcal{U}),\ A \Delta B = B \Delta A$.

c) Theo (1), phần tử trung hòa của phép toán Δ là tập $\varnothing$.

d) Theo (3), phần tử đối của $A \in \mathcal{P}(\mathcal{U})$ theo phép toán Δ là chính nó.
Như vậy, $(\mathcal{P}(\mathcal{U}), \Delta)$ là nhóm giao hoán. Ta xét tiếp phép toán $\cap$.

e) $\cap$ có tính kết hợp, vì $\forall A, B, C \in \mathcal{P}(\mathcal{U}),\ (A \cap B) \cap C = A \cap (B \cap C)$.

f) $\cap$ có tính giao toán, vì $\forall A, B \in \mathcal{P}(\mathcal{U}),\ A \cap B = B \cap A$.

g) $\cap$ có tính phân phối đối với Δ, tức là $\forall A, B, C \in \mathcal{P}(\mathcal{U})$,

$$A \cap (B \,\Delta\, C) = (A \cap B) \,\Delta\, (A \cap C).$$

h) $\mathcal{U}$ là phần tử đơn vị của phép toán $\cap$, vì $\forall A \in \mathcal{P}(\mathcal{U})$, $A \cap \mathcal{U} = A$.

Do đó, $(\mathcal{P}(\mathcal{U}), \Delta, \cap)$ là vành giao hoán có đơn vị.

i) Ta thử tìm $A, B \in \mathcal{P}(\mathcal{U}) - \{\varnothing\}$ sao cho $A \cap B = \varnothing \Leftrightarrow B \subseteq \overline{A}$. Điều này có thể đạt được khi và chỉ khi $|\mathcal{U}| \geq 2$. Chẳng hạn, với $\mathcal{U} = \{a, b\}$, ta chọn $A = \{a\}$, $B = \{b\}$. $(\mathcal{P}(\mathcal{U}), \Delta, \cap)$ là miền nguyên khi và chỉ khi $|\mathcal{U}| = 1$.

j) Với $A \in \mathcal{P}(\mathcal{U}) - \{\varnothing\}$, ta thử tìm $B \in \mathcal{P}(\mathcal{U})$ sao cho $A \cap B = \mathcal{U}$. Vì $A, B \subseteq \mathcal{U}$, nên $A \cap B = \mathcal{U} \Leftrightarrow A = B = \mathcal{U}$. Do đó, nếu $|\mathcal{U}| = 1$, thì mọi tập của $\mathcal{P}(\mathcal{U}) - \{\varnothing\}$ đều khả nghịch; và nếu $|\mathcal{U}| > 1$, thì có tập của $\mathcal{P}(\mathcal{U}) - \{\varnothing\}$ không khả nghịch, chẳng hạn $\mathcal{U} = \{a, b\}$, $A = \{a\}$. Nếu $|\mathcal{U}| > 1$, thì $(\mathcal{P}(\mathcal{U}), \Delta, \cap)$ không là trường.

□

13.2 Tính chất vành và vành con

Định lý 13.2 (Luật rút gọn)**.** *Cho tập G, với phép toán $\circ$ kết hợp, có đơn vị. Giả sử phần tử $a \in G$ khả nghịch. Khi đó $\forall b, c \in G$, ta có*

a) $a \circ b = a \circ c \Rightarrow b = c$, *và* *b)* $b \circ a = c \circ a \Rightarrow b = c$.

Định lý 13.3. *Cho vành R. Khi đó $\forall a, b \in R$,*

a) $a0 = 0a = 0$,

b) $-(-a) = a$,

c) $a(-b) = b(-a) = -(ab)$, *và*

d) $(-a)(-b) = ab$.

Định lý 13.4. *Cho vành R giao hoán, có đơn vị. Khi đó R là miền nguyên khi và chỉ khi $\forall a, b, c \in R$, $a \neq 0$, $ab = ac \Rightarrow b = c$. (Vì thế, một vành giao hoán có đơn vị thỏa mãn luật rút gọn theo phép nhân là một miền nguyên.)*

Định lý 13.5. *Nếu vành $(F, +, \cdot)$ là một trường, thì nó là miền nguyên.*

Định lý 13.6. *Miền nguyên hữu hạn $(D, +, \cdot)$ là một trường.*

Định nghĩa 13.6. *Cho vành $(R, +, \cdot)$. Tập con $S \neq \varnothing$ của R gọi là một vành con của R nếu $(S, +, \cdot)$ –tức là, S với phép cộng và phép nhân, hạn chế trên S– là một vành.*

Ví dụ 13.8. Với mọi vành R, các tập con $\{0\}$ và R đều là vành con của R.

Ví dụ 13.9. a) Tập số nguyên chẵn là vành con của $(\mathbb{Z}, +, \cdot)$. Tổng quát, với $n \in \mathbb{Z}^+$, $n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\}$ là vành con của $\mathbb{Z}$.

b) $\mathbb{Z}$ là vành con của $\mathbb{Q}$, $\mathbb{Q}$ là vành con của $\mathbb{R}$, $\mathbb{R}$ là vành con của $\mathbb{C}$.

Định lý 13.7. *Cho vành $(R, +, \cdot)$. Tập con $S \neq \varnothing$ của R là vành con của R khi và chỉ khi $\forall a, b \in S,\ -a, a+b, ab \in S$ (tức là, S đóng dưới tất cả phép toán –một ngôi hay hai ngôi– trên R).*

Ví dụ 13.10. Xét vành $(\mathbb{Z}, \oplus, \odot)$, và tập con gồm các số nguyên lẻ $S = \{..., -5, -3, -1, 1, 3, 5, ...\}$. Với $a, b \in S$, $\ominus a = 2 - a \in S$, $a \oplus b = a + b - 1 \in S$, và $a \odot b = a + b - ab \in S$, nên S là vành con của $(\mathbb{Z}, \oplus, \odot)$.

Tập S trong ví dụ trên không là vành con của $(\mathbb{Z}, +, \cdot)$, vì, chẳng hạn, chọn $a, b \in S$ tùy ý, ta có $a + b \notin S$. Tập $\mathbb{Z}^+$ không là vành con của $(\mathbb{Z}, +, \cdot)$, vì nếu chọn $a \in \mathbb{Z}^+$ tùy ý, thì $-a \notin \mathbb{Z}^+$.

Định lý 13.8. *Cho vành $(R, +, \cdot)$, và $\varnothing \neq S \subseteq R$. Khi đó*

a) S là vành con của $R \Leftrightarrow \forall a, b \in S,\ a - b, ab \in S$.

b) nếu S hữu hạn, thì S là vành con của $R \Leftrightarrow \forall a, b \in S,\ a + b, ab \in S$.

Ví dụ 13.11. Xét vành $R = M_2(\mathbb{Z})$ và tập con $S = \left\{ \begin{bmatrix} a & a+b \\ a+b & a \end{bmatrix} \mid a, b \in \mathbb{Z} \right\}$ của R. Chứng minh S là vành con của R.

Giải. Khi $a = b = 0$, ta có $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \in S$, nên $S \neq \varnothing$.

Với $\begin{bmatrix} a & a+b \\ a+b & a \end{bmatrix}, \begin{bmatrix} c & c+d \\ c+d & c \end{bmatrix} \in S$, trong đó $a, b, c, d \in \mathbb{Z}$, ta có

$$\begin{bmatrix} a & a+b \\ a+b & a \end{bmatrix} - \begin{bmatrix} c & c+d \\ c+d & c \end{bmatrix} = \begin{bmatrix} a-c & (a+b)-(c+d) \\ (a+b)-(c+d) & a-c \end{bmatrix}$$
$$= \begin{bmatrix} a-c & (a-c)+(b-d) \\ (a-c)+(b-d) & a-c \end{bmatrix} \in S, \text{ và}$$
$$\begin{bmatrix} a & a+b \\ a+b & a \end{bmatrix} \cdot \begin{bmatrix} c & c+d \\ c+d & c \end{bmatrix} = \begin{bmatrix} ac & (a+b)(c+d) \\ (a+b)(c+d) & ac \end{bmatrix}$$
$$= \begin{bmatrix} ac & ac+(ad+bc+bd) \\ ac+(ad+bc+bd) & ac \end{bmatrix} \in S.$$

Do đó, S đóng dưới phép trừ và phép nhân, tức là, S là vành con của R. □

Định nghĩa 13.7. *Tập con khác rỗng I của vành R gọi là một ideal của R nếu $\forall a, b \in I,\ \forall r \in R,\ a - b \in I$ và $ar, ra \in I$.*

Ví dụ 13.12. a) Với $n \in \mathbb{Z}^+$, $n\mathbb{Z}$ là ideal của $(\mathbb{Z}, +, \cdot)$. Thật vậy, với $a, b \in n\mathbb{Z}$, $r \in \mathbb{Z}$, hay $a = nk, b = nl$, với $k, l \in \mathbb{Z}$, ta có $a - b = n(k - l) \in n\mathbb{Z}$, và $ar = ra = n(kr) \in n\mathbb{Z}$.

b) Trong Ví dụ 13.6, S là ideal của $(\mathbb{Z}, \oplus, \odot)$. Thật vậy, với $a, b \in S$, $r \in \mathbb{Z}$,

$a \ominus b = a \oplus (\ominus b) = a \oplus (2 - b) = a + (2 - b) - 1 = a - b + 1 \in \mathbb{S}$, và

$a \odot r = r \odot a = a + r - ar = a + r(1 - a) \in S$.

Mỗi ideal là một vành con, nhưng ngược lại không đúng. $(\mathbb{Z}, +, \cdot)$ là vành con của $(\mathbb{Q}, +, \cdot)$, nhưng không là ideal của $\mathbb{Q}$ vì, chẳng hạn, $\frac{1}{2} \cdot 9 \notin \mathbb{Z}$ với $\frac{1}{2} \in \mathbb{Q}, 9 \in \mathbb{Z}$.

13.3 Vành các số nguyên modulo n

Trong phần này, ta xây dựng một loại vành, trường đặc biệt, và ứng dụng của nó.

Định nghĩa 13.8. *Cho $n \in \mathbb{Z}^+, n > 1$. Với $a, b \in \mathbb{Z}$, ta nói a đồng dư với b modulo n, và viết $a \equiv b \pmod{n}$, nếu $n \mid (a - b)$, hay, tương đương, $a = b + kn$ với $k \in \mathbb{Z}$.*

Ví dụ 13.13. 1) $17 \equiv 2 \pmod{5}$, vì $17 - 2 = 15 = 3 \cdot 5$, hay $17 = 2 + 3 \cdot 5$.

2) $-7 \equiv -49 \pmod{6}$, vì $-7 - (-49) = 42 = 7 \cdot 6$, hay $-7 = -49 + 7 \cdot 6$.

3) $11 \equiv -5 \pmod{8}$, vì $11 - (-5) = 16 = 2 \cdot 8$, hay $11 = -5 + 2 \cdot 8$.

Với $a, b, n \in \mathbb{Z}$, với $n > 1$,

1) Dễ thấy, $a = b \Rightarrow a \equiv b \pmod{n}$, nhưng ngược lại không đúng. Tuy nhiên, nếu $a \equiv b \pmod{n}$ và $a, b \in \{0, 1, 2, \dots, n - 1\}$, thì $a = b$.

2) Theo thuật toán chia, ta có thể viết $a = q_1 n + r_1$ và $b = q_2 n + r_2$, với $0 \leq r_1 < n$, $0 \leq r_2 < n$. Khi đó $a - b = (q_1 - q_2)n + (r_1 - r_2)$. Do đó, $a \equiv b \pmod{n}$ hay $n \mid (a - b) \Leftrightarrow n \mid (r_1 - r_2)$. Nhưng $0 \leq |r_1 - r_2| < n$, nên $n \mid (r_1 - r_2) \Leftrightarrow r_1 = r_2$, hay $a \bmod n = b \bmod n$.

   Vậy, $a \equiv b \pmod{n}$ khi và chỉ khi a, b có cùng phần dư khi chia n.

Định lý 13.9. *Đồng dư modulo n là một quan hệ tương đương trên $\mathbb{Z}$.*

Vì một quan hệ tương đương trên một tập cho ta một phân hoạch tập đó, nên với $n \geq 2$, quan hệ đồng dư modulo n phân hoạch $\mathbb{Z}$ thành n lớp tương đương

$$
\begin{aligned}
[0] &= \{\dots, -2n, -n, 0, n, 2n, \dots\} = \{0 + kn \mid k \in \mathbb{Z}\} \\
[1] &= \{\dots, -2n + 1, -n + 1, 1, n + 1, 2n + 1, \dots\} = \{1 + kn \mid k \in \mathbb{Z}\} \\
[2] &= \{\dots, -2n + 2, -n + 2, 2, n + 2, 2n + 2, \dots\} = \{2 + kn \mid k \in \mathbb{Z}\} \\
&\dots \\
[n - 1] &= \{\dots, -n + 1, -1, n - 1, 2n - 1, 3n - 1, \dots\} = \{(n - 1) + kn \mid k \in \mathbb{Z}\}.
\end{aligned}
$$

Với mỗi $t \in \mathbb{Z}$, theo thuật toán chia ta có thể viết $t = qn+r$, trong đó $0 \leq r < n$, nên $t \in [r]$, hay $[t] = [r]$. Ký hiệu tập các lớp tương đương*

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\} \tag{13.1}$$

Ta sẽ định nghĩa các phép toán hai ngôi đóng trên $\mathbb{Z}_n$, để thu được một vành. Với $[a], [b] \in \mathbb{Z}_n$, định nghĩa phép toán cộng + và nhân · modulo bởi

$$[a] + [b] = [a + b], \quad \text{và} \quad [a] \cdot [b] = [a][b] = [ab]. \tag{13.2}$$

Chẳng hạn, nếu $n = 7$, thì $[2] + [6] = [8] = [1]$, và $[2][6] = [12] = [5]$.

Ta cần chỉ ra hai phép toán trên được định nghĩa tốt, theo nghĩa nếu $[a] = [c], [b] = [d]$, thì $[a] + [b] = [c] + [d]$ và $[a][b] = [c][d]$, hay $[a + b] = [c + d]$ và $[ab] = [cd]$, tức là vế phải của các phép toán không phụ thuộc vào phần tử đại diện của các lớp tương đương. Ta thấy $[a] = [c] \Rightarrow a = c + kn$, với $k \in \mathbb{Z}$ nào đó, và $[b] = [d] \Rightarrow b = d + ln$, với $l \in \mathbb{Z}$. Khi đó

$$a + b = (c + kn) + (d + ln) = (c + d) + (k + l)n \Rightarrow [a + b] = [c + d], \text{ và}$$

$$ab = (c + kn)(d + ln) = cd + (cl + dk + kln)n \Rightarrow [ab] = [cd].$$

Định lý 13.10. *Với $n \in \mathbb{Z}^+$, $n > 1$, $\mathbb{Z}_n$ với phép toán cộng và nhân modulo là vành giao hoán có đơn vị là $[1]$ (và theo phép cộng, phần tử trung hòa là $[0]$, phần tử đối của $[a]$ là $-[a] = [-a]$, và hiệu $[a] - [b] = [a - b]$).*

Cụ thể, xét hai vành $\mathbb{Z}_5$ và $\mathbb{Z}_6$. Trong bảng tính ở dưới, ta thay $[a]$ bởi a.

$\mathbb{Z}_5$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

*Khi không có gì gây nhầm lẫn, ta thay $[a]$ bởi a và viết $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$.

Trong $\mathbb{Z}_5$, mọi phần tử khác không đều khả nghịch, nên $\mathbb{Z}_5$ là một trường. Tuy nhiên, với $\mathbb{Z}_6$, chỉ có 1 và 5 khả nghịch, còn 2, 3, 4 là các ước thực sự của không. Cũng như vậy, trong $\mathbb{Z}_9$, $3 \cdot 3 = 3 \cdot 6 = 0$, nên 3 và 6 là các ước thực sự của không. Vậy khi nào thì $\mathbb{Z}_n$, với $n \geq 2$, là một trường?

Định lý 13.11. *$\mathbb{Z}_n$ là trường khi và chỉ khi n là số nguyên tố.*

Trong $\mathbb{Z}_6$, [5] khả nghịch và [3] là ước của không. Tổng quát, khi n là hợp số, dấu hiệu để $[a]$ khả nghịch trong $\mathbb{Z}_n$ là

Định lý 13.12. *Trong $\mathbb{Z}_n$, $[a]$ khả nghịch khi và chỉ khi* $\gcd(a, n) = 1$.

Ký hiệu $\mathbb{Z}_n^* = \{a \in \mathbb{Z} \mid 1 \leq a < n, \gcd(a, n) = 1\}$. Ta đã biết $|\mathbb{Z}_n^*| = \Phi(n)$. Suy ra, số ước thực sự của không là $n - 1 - \Phi(n)$.

Trong Phần 4.4, ta biết rằng nếu $\gcd(a, n) = 1$ thì $\exists x, y \in \mathbb{Z},\ ax + ny = 1$. Khi đó, $ax \equiv 1 \pmod{n}$, hay $[a][x] = [1]$, tức là $[a]$ khả nghịch, và $[a]^{-1} = [x]$.

Ví dụ 13.14. Trong $\mathbb{Z}_{72}$, [25] khả nghịch và $[25]^{-1} = [49]$.

Lệnh

```
pow(25, -1, 72)
```

cho kết quả là 49. Trong tình huống lệnh báo lỗi, ta nói rằng phần tử đã cho không khả nghịch theo modulo tương ứng.

Nhắc lại thuật toán Euclid tìm ước chung lớn nhất của hai số tự nhiên a, b không đồng thời bằng 0. Đặt $r_0 = a, r_1 = b$, và với $k = 1, 2, ...$, nếu $r_k \neq 0$, thì chia r_{k-1} cho r_k:

$$r_{k-1} = q_k r_k + r_{k+1},$$

tới khi $r_{n+1} = 0$. Khi đó, $\gcd(a, b) = r_n$, là phần dư khác 0 cuối cùng của dãy phép chia.

Gọi x_k, y_k là các hệ số khi biểu diễn r_k theo a và b, tức là $r_k = x_k a + y_k b$. Thay biểu diễn này vào phép chia ở trên:

$$x_{k-1}a + y_{k-1}b = (x_k a + y_k b)q_k + (x_{k+1}a + y_{k+1}b),$$

rồi cân bằng hệ số của a và b, được $x_{k-1} = x_k q_k + x_{k+1}$ và $y_{k-1} = y_k q_k + y_{k+1}$. Ta có

hệ thức đệ quy

$$x_{k+1} = x_{k-1} - x_k q_k, \text{ và}$$
$$y_{k+1} = y_{k-1} - y_k q_k,$$

trong đó $r_0 = a = 1a + 0b$, cho ta $x_0 = 1, y_0 = 0$, và $r_1 = b = 0a + 1b$, hay $x_1 = 0, y_1 = 1$.

Công thức trên giúp ta xây dựng chương trình Python để xác định nghịch đảo đồng dư, nếu có, của $[a]$ trong $\mathbb{Z}_n$.

```
def InvMod(a, n):
    b = n
    x0, x1 = 1, 0
    while b != 0:
        q, r = a // b, a % b
        a, b = b, r
        x = x0 - x1 * q
        x0, x1 = x1, x
    if a == 1:
        return x0 % n
    else:
        print('không khả nghịch')

InvMod(25, 72)  # kết quả là 49
```

Xác định được $[a]^{-1}$ trong $\mathbb{Z}_n$, ta có thể giải phương trình đồng dư tuyến tính theo biến nguyên x. Với $b, c \in \mathbb{Z}$,

1) $ax \equiv b \pmod{n} \Leftrightarrow [ax] = [a][x] = [b] \Leftrightarrow [x] = [a]^{-1}[b]$, và

2) $ax + b \equiv c \pmod{n} \Leftrightarrow [ax + b] = [ax] + [b] = [a][x] + [b] = [c] \Leftrightarrow [a][x] = [c] - [b] = [c - b] \Leftrightarrow [x] = [a]^{-1}[c - b]$.

Một ứng dụng đơn giản của nhận xét trên là *mật mã affine*. Trước hết, quy ước chuyển chữ cái thành số, chẳng hạn

Chữ cái	A	B	C	D	E	F	G	H	I	J	K	L	M
Chữ số x	0	1	2	3	4	5	6	7	8	9	10	11	12
Chữ cái	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Chữ số x	13	14	15	16	17	18	19	20	21	22	23	24	25

```
num2chr = lambda x: chr(x + 65) # chuyển số thành chữ cái, 'A' có mã 65
[(x, num2chr(x)) for x in range(26)]
```

và hàm mã hóa $E : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$ xác định bởi $E(x) = (ax + b) \bmod 26$, trong đó $a, b \in \mathbb{Z}$ và $\gcd(a, 26) = 1$.

Trong tin nhắn ban đầu, thay chữ cái ứng với x bởi chữ cái ứng với $E(x)$, ta được tin nhắn mã hóa.

Muốn giải mã tin nhắn, ta cần biết hàm E. Trong $\mathbb{Z}_{26}$, $E(x)$ cũng có thể viết dưới dạng $E(x) = [ax + b] = [a][x] + [b]$. Vì $\gcd(a, 26) = 1$, tức là a khả nghịch, nên $\forall y \in \mathbb{Z}_{26}$, phương trình $[a][x] + [b] = [y]$ có nghiệm duy nhất $[x] = [a]^{-1}[y - b]$. Do đó, hàm E là song ánh, có hàm ngược

$$D(y) = [a]^{-1}[y - b].$$

Vậy để giải mã, ta thay chữ cái ứng với y bởi chữ cái ứng với ứng với $D(y)$.

Ví dụ 13.15. Cho hàm mã hóa $E(x) = (11x + 7) \bmod 26$.

a) Mã hóa tin nhắn "Send more money".

b) Giải mã tin nhắn mã hóa ở ý (a).

Giải. a) Quá trình mã được trình bày trong bảng (không bao gồm cột cuối)

Tin nhắn M	S	E	N	D	M	O	R	E	M	O	N	E	Y	M
x	18	4	3	13	12	14	17	4	12	14	13	4	24	$D(y)$
$E(x)$	23	25	20	14	9	5	12	25	9	5	20	25	11	y
Mã hóa N	X	Z	U	O	J	F	M	Z	J	F	U	Z	L	N

```
chr2num = lambda c: ord(c) - 65  # chuyển chữ cái thành số, 'A' có mã 65

E = lambda x: (11*x + 7) % 26  # D = lambda y: 19 * (y - 7) % 26
M = 'SEND MORE MONEY'          # N = 'XZUO JFMZ JFUZL'

N = ''                         # M
```

```
for c in M:                          # N
  if c == ' ':
    N += c                           # M
  else:
    x = chr2num(c)                   # y
    y = E(x)                         # x = D(y)
    N += num2chr(y)                  # M, x
```

b) Trong $\mathbb{Z}_{26}$, $[11]^{-1} = [19]$. Ta có hàm giải mã $D(y) = [19][y - 7] = 19(y - 7) \bmod 26$. Quá trình giải mã được thể hiện như như bảng trên, nhưng thay cột tiêu đề đầu bằng cột cuối, và theo trình tự từ dưới lên. Vì vậy, mã Python từ dòng 2 cũng được thay thế `E` bởi `D`, `M` bởi `N`, `x` bởi `y`, và ngược lại, như phần ghi chú.

```
pow(11, -1, 26)
```

□

Ví dụ 13.16. Cho $a, k, n \in \mathbb{Z}^+$. Bằng phương pháp quy nạp, ta chứng minh được $a^k \bmod n = [a]^k$ trong $\mathbb{Z}_n$. Lập chương trình tính $a^k \bmod n$ theo phương pháp chia đôi, và kiểm thử $5^{143} \bmod 222 = 89$.

Giải. **Cách 1:** lập trình, xem Ví dụ 5.70 và **??**

```
def PowMod(a, k, n):
    if k == 0:
        return 1
    if k % 2 == 0:
        return PowMod(a * a % n, k // 2, n)
    else:
        return PowMod(a * a % n, k // 2, n) * a %
    n

PowMod(5, 143, 222)  # kết quả là 89
```

Cách 2: dùng lệnh `pow(5, 143, 222)`

□

Ví dụ 13.17. Cho $n, r \in \mathbb{Z}^+$ trong đó $\gcd(r, n) = 1$. Có bao nhiêu cách chọn r số, có lặp, trong tập n số $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ để có tổng bằng $s \pmod n$?

Giải. Đặt A là tập các cách chọn r số, có lặp, trong $\mathbb{Z}_n$. Theo Phần 1.6, $|A| = \binom{n+r-1}{r}$. Trên A, xét quan hệ hai ngôi $\mathcal{R}$ xác định bởi: với hai cách chọn $x = \{x_1, x_2, \dots, x_r\}$, $y = \{y_1, y_2, \dots, y_r\} \in A$, $x \mathcal{R} y$ nếu tổng các phần tử trong x đồng dư với tổng các phần tử trong y theo modulo n:

$$(x_1 + x_2 + \dots + x_r) \bmod p = (y_1 + y_2 + \dots + y_r) \bmod n$$
$$\Leftrightarrow [x_1] + [x_2] + \dots + [x_r] = [y_1] + [y_2] + \dots + [y_r] \text{ (trong } \mathbb{Z}_n).$$

Khi đó $\mathcal{R}$ là quan hệ tương đương, nên A được phân hoạch thành n lớp tương đương $A_0, A_1, \dots, A_{n-1}$, với $A_s, 0 \le s \le n-1$ là các cách chọn có tổng là s (mod n). Vì $\gcd(r, n) = 1$, nên $\exists k,\ s = rk \bmod n = [r][k] = [rk]$. Xét hàm $f : A_0 \to A_s$ xác định bởi: với $x = \{x_1, x_2, \dots, x_r\} \in A_0$, $f(x) = \{[x_1 + k], [x_2 + k], \dots, [x_r + k]\}$. Hàm f xác định vì

$[x_i + k] \in \mathbb{Z}_n,\ \forall 1 \le i \le r,$ và

$[x_1 + k] + [x_2 + k] + \dots + [x_r + k] = [x_1 + x_2 + \dots x_r + rk] = [x_1 + x_2 + \dots + x_r] + [rk] = [s].$

Mặt khác, xét hàm $g : A_s \to A_0$ xác định bởi $g(\{y_1, y_2, \dots, y_r\}) = \{[y_1 - k], [y_2 - k], \dots, [y_r - k]\}$, thì $g = f^{-1}$. Do đó $|A_0| = |A_1| = \dots = |A_{n-1}| = \frac{1}{n}|A| = \frac{1}{n}\binom{n+r-1}{r}$. □

13.4 Đồng cấu và đẳng cấu nhóm, vành

Định nghĩa 13.9. *Cho các vành $(R, +, \cdot)$ và $(S, \oplus, \odot)$. Hàm $f : R \to S$ gọi là đồng cấu vành nếu $\forall a, b \in R$,*

a) $f(a + b) = f(a) \oplus f(b)$, và

b) $f(a \cdot b) = f(a) \odot f(b)$.

Nếu f là đơn ánh, thì f gọi là đơn cấu vành; nếu f là toàn ánh, thì f gọi là toàn cấu vành; nếu f là song ánh, thì f gọi là đẳng cấu vành, và khi đó R và S gọi là các vành đẳng cấu.

Ví dụ 13.18. Xét hai vành $(\mathbb{Z}, +, \cdot)$ và $(\mathbb{Z}_n, +, \cdot)$. Hàm $f : \mathbb{Z} \to \mathbb{Z}_n$ xác định bởi $f(a) = [a]$, là toàn cấu vành.

Định nghĩa 13.10. *Cho đồng cấu vành* $f : (R, +, \cdot) \to (S, \oplus, \odot)$. *Khi đó*

a) $f(0_R) = 0_S$, *trong đó* $0_R, 0_S$ *tương ứng là phần tử không của* R, S;

b) $f(-a) = \ominus f(a),\ \forall a \in R$;

c) $f(na) = nf(a),\ \forall a \in R, n \in \mathbb{Z}$;

d) $f(a^n) = [f(a)]^n,\ \forall a \in R, n \in \mathbb{Z}$;

e) nếu A *là vành con của* R, *thì* $f(A)$ *là vành con của* S.

Định lý 13.13. *Cho toàn cấu vành* $f : (R, +, \cdot) \to (S, \oplus, \odot)$, *với* $|S| > 1$. *Khi đó*

a) nếu R *có đơn vị* 1_R, *thì* $f(1_R)$ *là đơn vị của* S;

b) nếu a *khả nghịch trong* R, *thì* $f(a)$ *khả nghịch trong* S *và* $f(a^{-1}) = [f(a)]^{-1}$;

c) nếu R *giao hoán, thì* S *giao hoán;*

d) nếu I *là một ideal của* R, *thì* $f(I)$ *là một ideal của* S.

13.5 Định lý phần dư Trung Quốc

Định lý 13.14 (Định lý phần dư Trung Quốc)**.** *Cho* $n_1, n_2, \ldots, n_k \in \mathbb{Z}^+ - \{1\}$ *với* $k \geq 2$, *và* $\gcd(n_i, n_j) = 1,\ \forall 1 \leq i < j \leq k$. *Khi đó hệ* k *phương trình đồng dư*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\ldots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

có một nghiệm là

$$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \ldots + a_k N_k x_k.$$

trong đó $N_i = \dfrac{N}{n_i}$, *với* $N = n_1 n_2 \cdots n_k$, *và* $[x_i]_{n_i} = [N_i]_{n_i}^{-1}$ *là nghịch đảo của* N_i *trong* $\mathbb{Z}_{n_i}$.
Hơn nữa, hai nghiệm bất kỳ của hệ đồng dư theo mudulo $n_1 n_2 \ldots n_k$.

Trường hợp đặc biệt, giả sử $n, m \in \mathbb{Z}^+ - \{1\}$ với $\gcd(n, m) = 1$. Dùng thuật toán Euclid, ta tìm được $n', m' \in \mathbb{Z}$ sao cho $nn' + mm' = 1$. Khi đó, hệ hai phương trình đồng dư

$$x \equiv a \pmod{n}$$
$$x \equiv b \pmod{m}$$

có nghiệm $x = amm' + bnn' + kmn$, với $k \in \mathbb{Z}$.

Ví dụ 13.19. Giải hệ $x \equiv 4 \pmod{11}$ và $x \equiv 1 \pmod{7}$.

Giải. Với $\gcd(11, 7) = 1$, ta xác định hệ thức $11 \cdot 2 + 7(-3) = 1$. Suy ra

$$x_0 = [4 \times 7(-3) + 1 \times 11 \cdot 2] \bmod (11 \cdot 7) = 15$$

Hệ có nghiệm $x = 15 + 77k,\ k \in \mathbb{Z}$. □

```
from sympy import *
n, m = 11, 7
a, b = 4, 1

ans = gcdex(n, m)   # (2, -3, 1)

( a * m * ans[1] + b * n * ans[0] ) % (n * m)
```

Ví dụ 13.20. Giải hệ $x \equiv 14 \pmod{31}$, $x \equiv 16 \pmod{32}$, $x \equiv 18 \pmod{33}$.

Giải. Ta có $N = 31 \cdot 32 \cdot 33 = 32\,736$; $N_1 = \dfrac{32\,736}{31} = 1056$, $N_2 = 1023$, $N_3 = 992$. Suy ra $[x_1]_{31} = [1056]_{31}^{-1} = [16]$, $[x_2] = [31]$, $[x_3] = [17]$. Do đó

$$\begin{aligned} x &\equiv 14 \cdot 1056 \cdot 16 + 16 \cdot 1023 \cdot 31 + 18 \cdot 992 \cdot 17 \pmod{32\,736} \\ &\equiv 1\,047\,504 \pmod{32\,736} \\ &\equiv 32\,688 \pmod{32\,736}. \end{aligned}$$

□

```
a = [14, 16, 18]
n = [31, 32, 33]

P = 1  # P thay cho N
for ni in n:
    P *= ni

N = [P // ni for ni in n]
x = [pow(N[i], -1, n[i]) for i in range(3)]

[a[i] * N[i] * x[i] for i in range(3)]
sum(_)
x0 = _ % P
```

Một ứng dụng hay của định lý phần dư Trung Quốc, chứng minh tính chất nhân tính của hàm Euler phi.

Với hai số nguyên dương m, n,

$$\Phi(mn) = \Phi(m) \cdot \Phi(n).$$

Giải. Xét hàm $f : \mathbb{Z}_{mn}^* \to \mathbb{Z}_m^* \times \mathbb{Z}_n^*$, xác định bởi $f([a]_{mn}) = ([a]_m, [a]_n)$. Hàm f định nghĩa tốt vì nếu $[a]_{mn} = [a']_{mn}$, tức là $(mn) \mid (a - a')$, thì nói riêng $m \mid (a - a')$ và $n \mid (a - a')$, hay $[a]_m = [a']_m$ và $[b]_n = [b']_n$.

1) Giả sử $f([a]_{mn}) = f([b]_{mn})$, tức là $[a]_m = [b]_m$ và $[a]_n = [b]_n$, hay $m \mid (a - b)$ và $n \mid (a - b)$. Vì $\gcd(m, n) = 1$, nên $(mn) \mid (a - b)$, tức là $[a]_{mn} = [b]_{mn}$. Do đó f là đơn ánh.

2) Với $[a]_m, [b]_n$, liệu có $[x]_{mn}$ sao cho $f([x]_{mn}) = ([a]_m, [b]_n)$, hay $[x]_m = [a]_m$ và $[x]_n = [b]_n$. Điều này tương đương với hệ phương trình đồng dư

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

Theo định lý phần dư trung quốc, hệ này luôn có nghiệm. Do đó f là toàn ánh.

Vậy f là song ánh. Suy ra

$$\Phi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*| \times |\mathbb{Z}_n^*| = \Phi(m) \cdot \Phi(n).$$

□

Trong Phần 7.1, ta tính $\Phi(n)$ bằng nguyên lý bù trừ. Sử dụng kết quả trên, ta có một cách nữa. Trước hết

Cho p nguyên tố, và $e \in \mathbb{Z}^+$. Khi đó

$$\Phi(p^e) = p^{e-1}(p-1).$$

Chứng minh. Từ 1 tới p^e, số các bội của p là $\lfloor \frac{p^e}{p} \rfloor = p^{e-1}$. Mặt khác, số nguyên dương n nguyên tố cùng nhau với p^e, nếu p không là ước của n, hay n không là bội của p, nên

$$\Phi(p^e) = p^e - p^{e-1} = p^{e-1}(p-1).$$

□

Giả sử số nguyên $n \geq 2$ có phân tích $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, với p_i nguyên tố, và $e_i \in \mathbb{Z}^+$. Khi đó

$$\Phi(n) = \prod_{i=1}^{k} \Phi(p_i^{e_i}) = \prod_{i=1}^{k} p_i^{e_i-1}(p_i-1) = \prod_{i=1}^{k} p_i^{e_i}(1-\frac{1}{p_i})$$
$$= \prod_{i=1}^{k} p_i^{e_i} \times \prod_{i=1}^{k} (1-\frac{1}{p_i}) = n\prod_{i=1}^{k} (1-\frac{1}{p_i})$$

Bài tập 13.5

1. * Chứng minh với hai số nguyên dương m, n, ta có $\Phi(mn) = \Phi(m)\Phi(n)\frac{d}{\Phi(d)}$, trong đó $d = \gcd(m, n)$.

2. * Cho số nguyên dương n. Chứng minh $\sum_{d|n} \Phi(d) = n$.

13.6 Mã hóa khóa công khai: Giới thiệu

Trong Ví dụ 13.15 về mã hóa affine, quá trình giải mã được quyết định bởi việc tìm hàm ngược của hàm mã hóa E, một việc khá dễ dàng. Việc để lộ E sẽ làm mất

hoàn toàn tính bảo mật của tin nhắn mã hóa. Vậy có cách nào giúp ta tạo hàm mã hóa E thì dễ, nhưng lại rất khó tìm hàm ngược D của nó.

Alice muốn nói với Bob một bí mật. Vấn đề là mọi thứ họ nói với nhau đều bị tên trộm Eve nghe được. Alice có thể nói cho Bob bí mật đó không? Họ có thể giữ tính riêng tư cho cuộc trò chuyện không? Có lẽ họ cần tạo một mã bí mật và chỉ trò chuyện trong mã này. Vấn đề là Eve có thể nghe thấy mọi điều họ nói với nhau - bao gồm tất cả chi tiết về mã bí mật của họ! Một lựa chọn là Alice và Bob tạo mã riêng của họ (nơi mà Eve có thể nghe thấy). Lựa chọn này có thể không thực tế, chậm và tốn kém (ví dụ: nếu Alice và Bob sống cách xa nhau). Có vẻ như Alice và Bob không thể có một cuộc trò chuyện riêng tư trong khi Eve đang lắng nghe mọi điều họ nói. Những nỗ lực truyền thông điệp riêng tư của họ bị cản trở bởi vì Eve biết hệ thống mã hóa đó.

Mã hóa khóa công khai là một kỹ thuật xây dựng giao tiếp riêng tư trong một diễn đàn công cộng. Bí quyết là phát triển một mã bí mật với thuộc tính sau: Tiết lộ quy trình mã hóa không làm suy yếu tính bảo mật của quy trình giải mã. Ý tưởng là tìm ra một thủ tục tương đối dễ thực hiện, nhưng rất khó để hoàn tác. Ví dụ, nhân hai số nguyên tố cỡ lớn không khó (ít nhất là đối với máy tính). Tuy nhiên, phân tích tích đó thành thừa số nguyên tố (nếu không biết ước nguyên tố) là cực kỳ khó.

Phân tích số nguyên tố

Giả sử p, q là hai số nguyên tố cỡ lớn, khoảng 500 chữ số. Nhân các số này không khó. Kết quả $n = pq$ là số khoảng 1000 chữ số. Trên máy tính, phép tính này mất chưa đến một giây. Nếu quả thật buộc phải nhân hai số 500 chữ số chỉ bằng bút và giấy (rất nhiều giấy!), có thể mất vài giờ hoặc vài ngày.

Giả sử thay vì cho hai số nguyên tố p, q, ta có tích $n = pq$ và phải tìm lại thừa số nguyên tố p, q. Ta không biết p, q, chỉ biết n. Nếu dùng phép chia thử để phân tích n, ta cần khoảng 10^{500} phép chia, và sẽ mất một thời gian không tưởng ngay cả trên máy tính cực nhanh (xem Bài tập 5.39).

Có các thuật toán phân tích tinh vi, nhanh hơn phép chia thử nhiều. Ta không thảo luận về các phương pháp phức tạp hơn, nhưng nhanh hơn trong cuốn sách này. Mà cho dù các kỹ thuật này nhanh hơn nhiều phép phân thử, nhưng chúng không nhanh đến mức chúng có thể phân tích một số 1000 chữ số trong một khoảng thời gian hợp lý (ví dụ, dưới một thế kỷ).

Hơn nữa, việc chạy các kỹ thuật này trên các máy tính nhanh hơn không giúp việc phân tích dễ dàng hơn. Thay vì sử dụng các số nguyên tố 500 chữ số, ta có

thể sử dụng các số nguyên tố 1000 chữ số (vì vậy $n = pq$ tăng từ 1000 lên 2000 chữ số). Thời gian nhân p và q tăng vừa phải (khoảng 4 lần). Tuy nhiên, thời gian để phân tích $n = pq$ tăng vô cùng nhiều. Số n dài không quá hai lần so với trước nhưng thời gian tăng gấp 10^{1000} lần.

Như vậy, phân tích một số nguyên tố lớn là cực khó. Đến nay chưa có thuật toán phân tích nào hiệu quả. Dựa vào phán đoán này, ta có hai kỹ thuật để gửi tin nhắn riêng tư ở nơi công cộng: phương pháp Rabin và thuật toán RSA. Tính bảo mật của hệ thống mã hóa là do người khác không biết mã khóa, không phải do hạn chế về kiến thức.

Đổi chữ thành số

Alice cần nhắn cho Bob

Dear Bob, Do you want to go to the movies tonight?

Trước hết, Alice chuyển tin nhắn này thành số, một cách tiêu chuẩn là dùng mã ASCII. Mã này không có gì bí mật, biểu thị các chữ cái A-Z (chữ thường và chữ hoa), chữ số, dấu chấm câu,... tương ứng các số trong tập $\{0, 1, \ldots, 255\}$. Ví dụ: chữ D trong mã ASCII là số 68. Chữ e là 101. Ký tự trắng là 32. Tin nhắn của Alice, được hiển thị dưới dạng số, là

D	e	a	r	␣	B	o	b	,	...
068	101	097	114	032	066	111	098	044	

Tiếp theo, Alice nối các số có ba chữ số này thành một số nguyên lớn

$$M = 068\,101\,097\,114\,032\,066\,111\,098\,044\ \ldots\ 116\,063$$

Vì tin nhắn gốc dài khoảng 50 ký tự, tin nhắn này dài khoảng 150 chữ số.

```
T = 'Dear Bob, Do you want to go to the movies
   tonight?'
M = 0
for c in T:
  M = M * 1000 + ord(c)
```

Đây là cách Alice gửi tin nhắn cho Bob:

1) (Bí mật) Bob tạo ra một cặp hàm, D và E, là hàm ngược của nhau, tức là

$$D[E(M)] = M$$

2) Bob cho Alice hàm E. Lúc này, Eve có thể biết E. Hàm này khá dễ tính toán, nhưng rất khó để Eve tìm ra D mà chỉ biết E

3) (Bí mật) Alice lập tin nhắn M và tính $N = E(M)$.

4) Alice gửi số nguyên N cho Bob. Eve cũng thấy số này.

5) (Bí mật) Bob dùng hàm giải mã riêng của mình D để tính $D(N)$. Kết quả là

$$D(N) = D[E(M)] = M$$

Vậy là Bob đã đọc được tin nhắn M. Vì Eve không biết D nên không thể tìm ra M.

Khó khăn ở đây là tạo ra các hàm D và E hoạt động cho giao thức này. Dưới đây trình bày hai phương pháp để thực hiện điều này.

13.7 Mã hóa khóa công khai: Phương pháp Rabin

13.7.1 Khai căn đồng dư

Định nghĩa 13.11. *Cho $n \in \mathbb{N}^*$, $a \in \mathbb{Z}_n$. Nếu $\exists b \in \mathbb{Z}_n$, $[a] = [b^2] = [b]^2$ thì a gọi là thặng dư bậc hai* mod$n$*, và ký hiệu $b \in \sqrt{a}$ là một căn bậc hai của a, ở đây ta xem $\sqrt{a}$ là một tập.*
Ngược lại, $\sqrt{a} = \varnothing$, a không thặng dư bậc hai.

Ví dụ 13.21. Trong $\mathbb{Z}_{19} = \{0, 1, 2, \ldots, 18\}$, tìm $\sqrt{17}$ và $\sqrt{2}$.

Giải.

b	0	1	2	3	4	5	6	7	8	9
$[b^2]$	0	1	4	9	16	6	**17**	11	7	5
	10	11	12	13	14	15	16	17	18	
	5	7	11	**17**	6	16	9	4	1	

Ta có $\sqrt{17} = \{6, 13\}$, $\sqrt{2} = \varnothing$. □

Định lý 13.15. *Cho số nguyên tố p và $a \in \mathbb{Z}_p$. Khi đó a có không quá hai căn trong $\mathbb{Z}_p$.*

Định lý 13.16. *Cho số nguyên tố $p \equiv 3 \pmod 4$ và $a \in \mathbb{Z}_p$ thặng dư bậc hai. Khi đó các căn của a trong $\mathbb{Z}_p$ là*

$$\left[\pm a^{(p+1)/4}\right]. \tag{13.3}$$

Ví dụ 13.22. Số nguyên tố $59 \equiv 3 \pmod 4$. Trong $\mathbb{Z}_{59}$,

$$\left[17^{(p+1)/4}\right] = [17^{15}] = [28],$$

và $[-28] = [31]$. Do đó, $\sqrt{17} = \{28, 31\}$.

Xét $n = pq$, với p, q là hai số nguyên tố khác nhau và $p, q \equiv 3 \pmod 4$. Giả sử $x \in \sqrt{a}$ trong $\mathbb{Z}_n$:

$$a = x^2 \bmod n = x^2 \bmod (pq) \Rightarrow x^2 = a + kpq,\ k \in \mathbb{Z}.$$

Do đó $x^2 \equiv a \pmod p$, hay $[x^2]_p = [a]_p$. Theo Định lý 13.16, $[x]_p = \left[\pm a_p^{(p+1)/4}\right]_p$ trong $\mathbb{Z}_p$. Sau tính toán, ta được $[x]_p = [a_1]_p$ hoặc $[x]_p = [a_2]_p$, tức là

$$\begin{bmatrix} x \equiv a_1 & (\text{mod } p), \\ x \equiv a_2 & (\text{mod } p). \end{bmatrix}$$

Tương tự $x \equiv b_1$ hoặc $b_2 \pmod q$.

Kết hợp chúng lại, ta có bốn hệ phương trình $x \equiv a_i \pmod p$, $x \equiv b_j \pmod q$, $i, j = 1, 2$. Vì p, q là hai số nguyên tố khác nhau nên $\gcd(p, q) = 1$. Theo định lý phần dư Trung Quốc, mỗi hệ có nghiệm $x_{ij} \in \mathbb{Z}_{pq}$, là các căn của a trong $\mathbb{Z}_n$.

Ví dụ 13.23. Trong $\mathbb{Z}_{1121}$, tìm $\sqrt{17}$.

Giải. 1) Phân tích $n = 1121 = 19 \cdot 59$, ở đây $19, 59 \equiv 3 \pmod 4$.

2) Trong $\mathbb{Z}_{19}$, $\sqrt{17} = \{6, 13\}$ và trong $\mathbb{Z}_{59}$, $\sqrt{17} = \{28, 31\}$.

3) Từ thuật toán Euclid, ta có hệ thức $19 \cdot 28 + 59(-9) = 1$.

4) $\sqrt{17}$ trong $\mathbb{Z}_{1121}$ gồm $\left[\sqrt{[17]}_{19} \times 59(-9) + \sqrt{[17]}_{59} \times 19 \cdot 28\right]$ theo nghĩa:

$$\begin{bmatrix} 6 \\ 6 \\ 13 \\ 13 \end{bmatrix} \times 59(-9) + \begin{bmatrix} 28 \\ 31 \\ 28 \\ 31 \end{bmatrix} \times 19 \cdot 28 = \begin{bmatrix} 500 \\ 975 \\ 146 \\ 621 \end{bmatrix}.$$

□

Định lý 13.17. *Giả sử n là tích hai số nguyên tố nào đó. Nếu $x \in \mathbb{Z}_n$ có 4 căn phân biệt và xác định thì phân tích được n.*

Ví dụ 13.24. Cho $n = 38\,989$. Trong $\mathbb{Z}_n$, biết $\sqrt{25}$ gồm $a = 5, b = -5 = 38\,984, c = 2154, d = -2154 = 36\,835$. Ta có

$$\gcd(a - c, n) = \gcd(-2\,149, 38\,989) = 307,$$
$$\gcd(a + c, n) = \gcd(2\,159, 38\,989) = 127,$$

và $307 \cdot 127 = 38\,989$.

13.7.2 Thủ tục mã hóa và giải mã

1) (Bí mật) Người Bob tìm hai số nguyên tố lớn p, q (khoảng 100 chữ số) p, q mà $p \equiv q \equiv 3 \pmod 4$, tính $n = pq$.

2) Bob cho Alice biết số n. Ai cũng có thể biết số này.

3) (Bí mật) Alice lập tin nhắn M và dùng hàm mã hóa Rabin*:

$$N = E(M) = M^2 \bmod n.$$

4) Alice gửi số N cho Bob. Ai cũng thấy số này.

5) (Bí mật) Bob tính bốn căn của N (trong $\mathbb{Z}_n$). Vì Bob biết các thừa số của n (là p và q) nên tính được các căn đó, và chỉ một trong đó là tin nhắn M của Alice dạng ASCII; ba căn kia thường vô nghĩa.

Ví dụ 13.25. 3) Nếu Alice nhận được số $n = 137\,941\,061$ từ Bob, tìm mã hóa của Alice theo phương pháp Rabin cho tin nhắn "CS".

5) Bob biết được phân tích nguyên tố $n = pq$, với $p = 7\,919$ và $q = 17\,419$. Tìm bốn kết quả giải mã của Bob đối với tin nhắn mã hóa trên của Alice.

*Michael Oser Rabin (1931–), nhà toán học và khoa học máy tính Israel

Giải. 3) Số ứng với từ "CS" sau khi ghép mã ASCII ba chữ số là $M = 067\,083$. Tin nhắn mã hóa Alice gửi cho Bob là

$$N = M^2 \bmod n = 86\,014\,937.$$

```
T = 'CS'
M = 0
for c in T:
  M = M * 1000 + ord(c)

n = 137941061
N = M ** 2 % n
```

5) Bob thực hiện các bước sau

i) khai căn N trong $\mathbb{Z}_p$ và $\mathbb{Z}_p$, được

$$\text{Trong } \mathbb{Z}_p,\ \sqrt{N} = \{a_1, a_2\} = \{4188, 3731\}, \quad \text{và}$$
$$\text{Trong } \mathbb{Z}_q,\ \sqrt{N} = \{b_1, b_2\} = \{14826, 2593\}.$$

ii) Tìm khai triển Euclide mở rộng của p và q, được hệ số $x = 1245$, $y = -566$ sao cho $px + qy = 1$.

```
from sympy import gcdex
x, y, _ = gcdex(p, q)
```

iii) Mỗi căn của N trong $\mathbb{Z}_n$ là một nghiệm của hệ phương trình $x \equiv a_i \pmod p$ và $y \equiv b_j \pmod q$, với $i = 1, 2$ và $j = 1, 2$, có công thức tính nhanh dạng

$$a_i \times qy + b_j \times px$$

Ta được bốn căn của N trong $\mathbb{Z}_n$ là

$$46\,488\,718,\ 137\,873\,978,\ 67\,083, \text{ và } 91\,452\,343.$$

Trong bốn số, chỉ có số thứ ba là nghiệm, tức là đưa được về dạng chữ bằng mã ASCII, và chữ đó có nghĩa.

```
(a1 * q*y + b1 * p*x) % n
(a1 * q*y + b2 * p*x) % n
M = (a2 * q*y + b2 * p*x) % n  # đây là nghiệm
    cần tìm
(a2 * q*y + b2 * p*x) % n
```

iv) Tin nhắn giải mã được là “CS”.

```
T = ''
while M != 0:
  r = M % 1000
  T = chr(r) + T
  M = M // 1000
```

□

Bài tập 13.7

3. Tìm nghiệm của hệ đồng dư $x \equiv 5 \pmod 8$ và $x \equiv 73 \pmod{81}$.

4. Một chiếc rương chứa các đồng tiền vàng giống hệt nhau. Nếu chia đều thành 17 phần thì vẫn còn ba đồng, chia đều thành 16 phần thì vẫn dư 10 đồng, và chia đều thành 15 phần thì không còn xu nào. Số đồng xu nhỏ nhất có thể có trong rương là bao nhiêu?

5. Tìm nghiệm của hệ đồng dư $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$ và $x \equiv 5 \pmod 7$.

6. Giả sử máy tính mất 1 giây để nhân hai số có 500 chữ số. Muốn nhân hai số có 1000 chữ số thì mất bao lâu?

7. Tìm bốn căn bậc hai của 500 trong $\mathbb{Z}_{589}$.

8. Tìm tất cả giá trị của $\sqrt{17985}$ trong $\mathbb{Z}_{34751}$.

9. Bước đầu tiên trong mã hóa khóa công khai là chuyển tin nhắn sang dạng số M. Điều này thường được thực hiện bằng mã ASCII. Trong bài toán này, ta sử dụng phương pháp đơn giản hơn.
Xét các tin nhắn chỉ chứa 26 ký tự viết hoa, ta dùng bảng tương ứng

Chữ cái	A	B	C	...	Z
Số	01	02	03	...	26

chẳng hạn, từ LOVE ứng với số 12 152 205.
Giả sử khóa công khai của Bob là $n = 3\,2841\,9349$. Alice mã hóa tin nhắn theo phương pháp Rabin $M^2 \bmod n$. Ví dụ, tin nhắn LOVE được mã hóa thành

$$1215\,2205^2 \bmod 3\,2841\,9349 = 2714\,8732,$$

và vì vậy Alice truyền tín hiệu 2714 8732 cho Bob.

Alice gửi bốn tin nhắn mã hóa nữa cho Bob, nội dung như sau

a) 2 4950 0293 b) 2988 3150 c) 2 3273 2214 d) 9841 1064

Giải mã bốn từ này.

10. Giả sử khóa công khai của Bob là một hợp số n có 1000 chữ số, và Alice mã hóa tin nhắn M bởi $E(M) = M^2 \bmod n$. Khi Alice muốn gửi tin nhắn có c ký tự, sẽ tạo ra một số nguyên có $3c$ chữ số (dùng mã ASCII). Alice nên làm gì nếu

a) $3c > 1000$ b) $3c < 500$

11. Giả sử $n = 171121$ là tích của hai số nguyên tố. Bốn căn bậc hai của 56 248 trong $\mathbb{Z}_n$ là 68 918, 75 406, 95 715, và 102 203.
Không dùng phép chia thử, hãy phân tích n.

12. Giả sử $n = 5\,947\,529\,662\,023\,524\,748\,841$ là tích của hai số nguyên tố. Bốn căn bậc hai của $5\,746\,634\,461\,808\,278\,371\,316$ trong $\mathbb{Z}_n$ là

602 161 451 924 4 038 208 561 704 737 244 676 và

1 909 321 100 318 787 504 165 5 947 529 661 421 363 296 917

Hãy phân tích n.

13. Chứng minh mọi phần tử của $\mathbb{Z}_{17}$ đều là lập phương (modulo 17), và có số nguyên e sao cho $\forall a \in \mathbb{Z}_{17}$, a^e là một căn bậc ba của a.

14. Chứng minh kết quả tổng quát của Bài tập 13: Cho số nguyên tố $p \equiv 2 \pmod 3$. Khi đó có số nguyên dương e sao cho $\forall a \in \mathbb{Z}_p$, a^e là căn bậc ba của a.

13.8 Mã hóa khóa công khai: RSA

13.8.1 Định lý nhỏ Fermat

Định lý 13.18 (Fermat)**.** *Cho số nguyên tố p và số nguyên a. Khi đó $a^p \equiv a \pmod p$.*

Ví dụ 13.26. Với $p = 23$, các lũy thừa của 5 lấy theo modulo 23 là

$$\begin{array}{lllll} 5^1 \equiv 5 & 5^2 \equiv 2 & 5^3 \equiv 10 & 5^4 \equiv 4 & 5^5 \equiv 20 \\ 5^6 \equiv 8 & 5^7 \equiv 17 & 5^8 \equiv 16 & 5^9 \equiv 11 & 5^{10} \equiv 9 \\ 5^{11} \equiv 22 & 5^{12} \equiv 18 & 5^{13} \equiv 21 & 5^{14} \equiv 13 & 5^{15} \equiv 19 \\ 5^{16} \equiv 3 & 5^{17} \equiv 15 & 5^{18} \equiv 6 & 5^{19} \equiv 7 & 5^{20} \equiv 12 \\ 5^{21} \equiv 14 & 5^{22} \equiv 1 & \boxed{5^{23} \equiv 5} & 5^{24} \equiv 2 & 5^{25} \equiv 10. \end{array}$$

Ví dụ 13.27. Khẳng định $a^n \equiv a \pmod{n}$ không còn đúng với số n không nguyên tố. Với $n = 9$ thì

$$\begin{array}{lll} 1^9 \equiv 1 & 2^9 \equiv 8 \not\equiv 2 & 3^9 \equiv 0 \not\equiv 3 \\ 4^9 \equiv 1 \not\equiv 4 & 5^9 \equiv 8 \not\equiv 5 & 6^9 \equiv 0 \not\equiv 6 \\ 7^9 \equiv 1 \not\equiv 7 & 8^9 \equiv 8 & 9^9 \equiv 0 \equiv 9. \end{array}$$

Với $8^9 \equiv 8 \pmod 9$, điều ngược lại của Định lý nhỏ Fermat không đúng, tức là, nếu $a^n \equiv a \bmod n$, chưa chắc n nguyên tố.

Định lý 13.19 (Euler)**.** *Cho số nguyên dương n và số nguyên a nguyên tố cùng nhau với n. Khi đó* $a^{\Phi(n)} \equiv 1 \pmod{n}$.

Ví dụ 13.28. $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$ và $\Phi(9) = 6$:

$$\begin{array}{lll} 1^6 \equiv 1 & 2^6 \equiv 1 & 3^6 \equiv 0 \\ 4^6 \equiv 1 & 5^6 \equiv 1 & 6^6 \equiv 0 \\ 7^6 \equiv 1 & 8^6 \equiv 1 & 9^6 \equiv 0. \end{array}$$

Định lý 13.20. *Cho số nguyên dương a, n. Nếu* $a^n \not\equiv a \pmod{n}$*, thì n không nguyên tố.*

Ví dụ 13.29. $2^{3007} \bmod 3007 = 66 \neq 2$. Vậy 3007 không nguyên tố.

Như vậy ta chỉ ra 3007 không nguyên tố mà không cần phân tích thừa số. Có vẻ đây là cách khá phức tạp để kiểm tra một số không là nguyên tố. Phân tích 3007 đơn giản là 31×97. Việc phân tích 3007 liệu có đơn giản và nhanh hơn việc tính $2^{3007} \bmod 3007$?

Để phân tích, phương pháp đơn giản nhất là phép chia thử: chia 3007 cho số nguyên từ 2 đến $\sqrt{3007} = 54.8$. Phương pháp này mất khoảng 54 phép chia.

Mặt khác, việc tính 2^{3007} dường như cần hàng ngàn phép nhân. Tuy nhiên, theo phương pháp chia đôi liên tiếp, tính $2^{3007} \bmod 3007$ cần khoảng $6\left(1 + \log_2 3007\right) \approx 75$ phép toán. Khối lượng tính toán của hai phương pháp dường như gần giống nhau, thậm chí có vẻ phương pháp phân tích có ít phép tính hơn.

Tuy nhiên, giả sử ta dùng phép chia thử để kiểm tra tính nguyên tố của số 1000 chữ số. Vì $n \approx 10^{1000}$, ta có $\sqrt{n} \approx 10^{500}$. Ta cần thực hiện 10^{500} phép chia. Nếu dùng siêu máy tính mạnh nhất, Summit, mỗi giây chỉ thực hiện được cỡ 10^{18} phép tính, thì cũng mất thời gian rất dài!

Mặt khác, tính $a^n \bmod n$ chỉ cần không quá $6\left(1 + \log_2 10^{1000}\right) = 6\left(1 + 1000\log_2 10\right) \approx 20\,000$ phép tính, có thể thực hiện chưa đến một phút trên máy tính.

Định nghĩa 13.12. *Số nguyên dương n gọi là số Carmichael nếu*

a) n là hợp số; và

b) $\forall a\ (1 < a < n),\ a^n \equiv a \pmod{n}$.

Năm số Carmichael đầu tiên là 561, 1105, 1729, 2465, 2821.

13.8.2 Thủ tục mã hóa và giải mã

Hàm mã hóa và giải mã RSA*:

$$E(M) = M^e \bmod n, \quad \text{và} \quad D(N) = N^d \bmod n.$$

Công khai E tức là ai cũng có thể biết n và e. Nhưng phải giữ bí mật D, tức là, không tiết lộ d.

Ta cần chọn d, e sao cho

$$D[E(M)] = M.$$

Tính trong $\mathbb{Z}_n$:

$$D[E(M)] = D([M]^e) = ([M]^e)^d = [M]^{ed} \stackrel{?}{=} [M].$$

Theo định lý Euler, nếu $\gcd(M, n) = 1$ thì $M^{\Phi(n)} \equiv 1 \pmod{n}$, tức là trong $\mathbb{Z}_n$:

$$[M]^{\Phi(n)} = [1] \Rightarrow ([M]^{\Phi(n)})^k = [1]^k \Rightarrow [M]^{k\Phi(n)} = [1] \Rightarrow [M]^{k\Phi(n)+1} = [M],\ (k \in \mathbb{Z}^+).$$

*1970, bởi Ronald **R**ivest (1948–), Adi **S**hamir (1952–), và Leonard **A**dleman (1945–)

Ta cần $ed = k\Phi(n) + 1$, hay

$$ed \equiv 1 \pmod{\varphi(n)},$$

tức là trong $\mathbb{Z}^*_{\Phi(n)}$:

$$[ed] = [1] \Leftrightarrow [d] = [e]^{-1},$$

trong đó $e \in \mathbb{Z}^*_{\Phi(n)}$ tùy ý. Lưu ý rằng nếu biết các ước nguyên tố p của n thì tính được $\Phi(n)$. Theo định lý cơ bản của số học, giả sử

$$n = p_1^{k_1} \dots p_r^{k_r}$$

thì

$$\Phi(n) = (p_1 - 1)p_1^{k_1-1} \cdots (p_r - 1)p_r^{k_r-1} = n\prod_{p|n}\Big(1 - \frac{1}{p}\Big).$$

Trường hợp $n = pq$, là tích của hai số nguyên tố khác nhau, thì $\Phi(n) = (p-1)(q-1)$. Các bước như sau:

(1) (Bí mật) Bob tìm hai số nguyên tố rất lớn p, q (khoảng 500 chữ số). Tính $n = pq$ và $\Phi(n) = (p-1)(q-1)$.

Trong $\mathbb{Z}^*_{\Phi(n)}$, chọn ngẫu nhiên e và tính $[d] = [e]^{-1}$ bằng thuật toán Euclide.

(2) Bob cho Alice biết n và e (nhưng giữ bí mật số d). Ai cũng có thể biết hai số này.

(3) (Bí mật) Alice lập tin nhắn M và tính $N = E(M) = M^e \bmod n$.

(4) Alice gửi số N cho Bob. Ai cũng thấy số này.

(5) (Bí mật) Bob tính $D(N) = N^d \bmod n = M$ và đọc được tin nhắn của Alice.

Ví dụ 13.30. a) Alice nhận được số mã không khai $n = 35\,143$ và $e = 28\,407$ từ Bob. Tìm mã hóa cho tin nhắn $M = 12\,345$.

b) Bob gửi mã công khai n và e cho Alice, và giữ lại khóa bí mật là $p = 113$ và $q = 311$. Tìm nốt những khóa bí mật $\Phi(n)$ và d. Từ đó giải mã tin nhắn N của Alice.

Giải. a) $N = E(M) = M^e \bmod n = 27374$.

```
n, e = 35143, 28407
M = 12345
N = pow(M, e, n)
```

b) $\Phi(n) = (p-1)(q-1) = 34\,720$.

Trong $\mathbb{Z}^*_{\Phi(n)}$, nghịch đảo của $e = 28\,407$ là $d = 23\,143$.

Tin nhắn gốc mà Alice gửi cho Bob là $M = D(N) = N^d \bmod n = 12\,345$.

```
p, q = 113, 311
Phi = (p-1) * (q-1)

e = 28407
d = pow(e, -1, Phi)
M = pow(N, d, n)
```

□

Việc giải mã cần giả thiết $\gcd(M, n) = 1$ (nếu không thì không dùng được định lý Euler). Khi $n = pq$, thủ tục trên vẫn đúng nếu $\gcd(M, n) \neq 1$.

Định lý 13.21. *Giả sử biết n và $\Phi(n)$. Nếu n có dạng tích hai số nguyên tố khác nhau nào đó thì có thể phân tích được n.*

Ví dụ 13.31. Tìm p và q biết $n = pq = 414\,847$ và $\Phi(n) = (p-1)(q-1) = 413\,280$.

Giải. Ta có $q = \dfrac{414\,847}{p}$ và

$$(p-1)\Big(\frac{414\,847}{p} - 1\Big) = 413\,280 \Rightarrow (p-1)(p-414\,847) + 413\,280p = 0$$

$$\Rightarrow p^2 - 1\,568p + 414\,847 = 0 \Rightarrow \begin{bmatrix} p = 337 & \Rightarrow q = 1\,231 \\ p = 1\,231 & \Rightarrow p = 337. \end{bmatrix}$$

□

Định lý 13.22. *Cho n, và biết n có dạng tích hai số nguyên tố khác nhau nào đó. Nếu trong $\mathbb{Z}^*_{\Phi(n)}$ luôn tìm được nghịch đảo của mọi phần tử thì có thể phân tích được n.*

Bài tập 13.8

15. Cho $n = 589 = 19 \times 31$, và $e = 53$. Nếu hàm mã hóa là $E(M) = M^e \bmod n$, tìm hàm giải mã.

16. Cho $n = 589 = 19 \times 31$, và $d = 53$. Nếu hàm giải mã là $D(N) = N^d \bmod n$, tìm hàm mã hóa.

17. Giả sử hàm mã hóa là $E(M) = M^{53} \bmod 589$. Alice mã hóa tin nhắn M, tính được $E(M) = 289$, và gửi giá trị 289 cho Bob. Tin nhắn M là gì?

18. Số nguyên $n = 331\,2997$ là tích của hai số nguyên tố. Biết $\Phi(n) = 330\,9280$, tìm các ước nguyên tố của n.

19. Bước đầu tiên trong mã hóa khóa công khai là chuyển tin nhắn sang dạng số M. Điều này thường được thực hiện bằng mã ASCII. Trong bài toán này, ta sử dụng phương pháp đơn giản hơn.
Xét các tin nhắn chỉ chứa 26 ký tự viết hoa, ta dùng bảng tương ứng

Chữ cái	A	B	C	...	Z
Số	01	02	03	...	26

chẳng hạn, từ LOVE ứng với số 12 152 205. (như Bài tập 9)
Khóa công khai RSA là $n = 3\,2841\,9349$ và $e = 2\,2003\,7467$. Để mã hóa từ LOVE, Alice tính

$$1215\,2205^{2\,2003\,7467} \bmod 3\,2841\,9349 = 7601\,0536$$

và gửi 7601 0536 cho Bob.
Alice mã hóa thêm bốn từ nữa gửi cho Bob, được

a) 3 2277 6966
b) 4380 8278
c) 1 6631 8297 và
d) 1803 5306

Giải mã bốn từ này.

Bài tập bổ sung

20. Không dùng công cụ hỗ trợ tính toán, tính $2^{90} \bmod 89$.

21. Cho $n = 3816\,8467$. Biết $2^n \equiv 617\,8104 \pmod{n}$, chỉ ra n là số nguyên tố hay hợp số.

22. Cho $n = 3816\,8467$ và $\Phi(n) = 3815\,5320$. Không dùng công cụ hỗ trợ tính toán, tính

$$2^{3815\,5321} \bmod 3816\,8467.$$

23. Chỉ dùng máy tính cầm tay cơ bản, tính $874^{256} \bmod 9432$.

24. Tìm các giá trị của $\sqrt{17}$ trong $\mathbb{Z}_{883}$.

25. Tìm các giá trị của $\sqrt{1}$ trong $\mathbb{Z}_{44\,0617}$, biết 44 0617 có phân tích nguyên tố 499×883.

26. Cho $n = 546\,0947$ là tích của hai số nguyên tố. Trong $\mathbb{Z}_n$ ta có

$$123\,5907^2 = 184\,2412^2 = 361\,8535^2 = 422\,5040^2 = 101\,0120.$$

Hãy phân tích nguyên tố cho n.

27. Alice và Bob liên lạc bằng mã hóa Rabin. Mã công khai của Bob là $n = 71\,3809$.
Alice gửi tin nhắn cho Bob. Đầu tiên, Alice chuyển tin nhắn của mình (một từ có ba chữ cái) thành số bằng cách lấy tương ứng A là 01, B là 02,... Sau đó chuyển tin nhắn mã hóa là 49 6410 cho Bob.
Biết $71\,3809 = 787 \times 907$, giải mã tin nhắn của Alice.

28. Alice và Bob liên lạc bằng mã hóa RSA. Mã công khai của Bob là $n = 45\,3899$ và $e = 449$. Bob biết $45\,3899 = 541 \times 839$. Tìm số mũ d để giải mã bí mật của Bob.

29. Trong bài trên, Alice gửi Bob tin nhắn bằng cách dùng mã công khai RSA của Bob. Thay A bởi 01, B bởi 02,..., Alice chuyển tin nhắn (từ có ba ký tự) thành số nguyên M, và mã hóa bằng hàm mã hóa của Bob, được $E(M) = 10\,5015$.
Tin nhắn của Alice là gì?

30. Cho $n = 4011\,9451$ là tích của hai số nguyên tố phân biệt, và $\Phi(n) = 4010\,6592$. Phân tích nguyên tố cho n.

Tài liệu tham khảo

[1] NumPy community. *NumPy User Guide*. phiên bản 1.22.4. 535 trang. URL: https://numpy.org/doc/stable.

[2] Judi J. McDonald David C. Lay Steven R. Lay. *Linear Algebra and Its Applications*. In lần thứ 6. Pearson, 2022. 755 trang.

[3] Ralph P. Grimaldi. *Discrete and Combinatorial Mathematics: An Applied Introduction*. In lần thứ 5. Pearson Addison-Wesley, 2004. 992 trang.

[4] Ralph P. Grimaldi. *Discrete and Combinatorial Mathematics: Instructor's Solutions Manual*. In lần thứ 5. Pearson Addison-Wesley, 2004. 465 trang.

[5] Thomas Koshy. *Catalan Numbers with Applications*. Oxford University Pres, 2009. 439 trang.

[6] Kenneth H. Rosen. *Discrete Mathematics and Its Applications*. In lần thứ 8. McGraw-Hill Education, 2019. 1118 trang.

[7] Edward R. Scheinerman. *Mathematics: A Discrete Introduction*. In lần thứ 3. Brooks/Cole, Cengage Learning, 2013. 506 trang.

[8] Watson S. Stewart J. Clegg D. *Calculus: Early Transcendentals*. In lần thứ 9. Cengage Learning, 2011. 1421 trang.

[9] SymPy Development Team. *SymPy Documentation*. phiên bản 1.8. 2750 trang. URL: https://github.com/sympy/sympy/releases.