Mục lục

Chương 4

Tính chất của số nguyên: quy nạp toán học

4.1 Nguyên lý sắp tốt: quy nạp toán học

Nguyên lý sắp tốt: Mọi tập con *khác rỗng* của $\mathbb{Z}^+$ đều có phần tử nhỏ nhất. $\mathbb{Z}^+$ gọi là *được sắp tốt*.

Các tập $\mathbb{Q}^+$, $\mathbb{R}^+$ không có tính chất này. Chẳng hạn, $\mathbb{Q}^+$ không có số nhỏ nhất. Thật vậy, giả sử ngược lại, $\mathbb{Q}^+$ có số nhỏ nhất q. Khi đó $q \in \mathbb{Q}^+$, và $q \leq x$, $\forall x \in \mathbb{Q}^+$. Chọn $x = \dfrac{q}{2} \in \mathbb{Q}^+$, thì $q \leq x \Leftrightarrow q \leq \dfrac{q}{2} \Leftrightarrow q \leq 0$, mâu thuẫn với $q \in \mathbb{Q}^+$.

Định lý 4.1 (Nguyên lý quy nạp toán học). *Cho $S(n)$ là khẳng định mở, $n \in \mathbb{Z}^+$. Ta có suy luận:*

$$\begin{array}{lll} a) & S(1) & \textit{giả thiết ban đầu} \\ b) & \forall n \in \mathbb{Z}^+, S(n) \Rightarrow S(n+1) & \textit{bước quy nạp} \\ \hline \therefore & \forall n \in \mathbb{Z}^+, S(n) & \end{array}$$

Tổng quát, với $n_0, n_1 \in \mathbb{Z}$, $n_0 \leq n_1$

$$\begin{array}{ll} a) & S(n_0), S(n_0+1), \dots, S(n_1) \\ b) & \forall n \geq n_1,\ S(n_0) \wedge S(n_0+1) \wedge \cdots \wedge S(n) \Rightarrow S(n+1) \\ \hline \therefore & \forall n \geq n_0, S(n) \end{array}$$

Trong bước quy nạp (b), các mệnh đề $S(n_0)$, $S(n_0+1), \dots, S(n)$ bên trái dấu $\Rightarrow$ gọi là các giả thiết quy nạp.

Trong nguyên lý quy nạp tổng quát, với n bất kỳ, để chứng minh $S(n+1)$, giả sử chỉ cần sử dụng các giả thiết quy nạp $S(n-a_i)$ với $a_i \geq 0$, $i = \overline{1, k}$ là các hằng số. Khi đó $n_0 \leq n - a_i \leq n$, hay $n \geq n_0 + a_i$, $i = \overline{1, k}$. Do đó, trong giả thiết ban đầu, ta nên chọn $n_1 = n_0 + \max\limits_{1 \leq i \leq k} a_i$, tức là có $\max\limits_{1 \leq i \leq k} a_i + 1$ giả thiết ban đầu liên tiếp.

Chứng minh. Ta chứng minh lập luận thứ nhất. Lập luận thứ hai được chứng minh tương tự.

Giả sử ngược lại, $\neg \forall n \in \mathbb{Z}^+, S(n)$, hay $\exists n \in \mathbb{Z}^+$, $S(n)$ sai. Đặt $F = \{n \in \mathbb{Z}^+ \mid S(n) \text{ sai}\}$, thì $F \neq \varnothing$. Theo nguyên lý sắp tốt, F có số nhỏ nhất m. Vì $S(1)$ đúng, nên $1 \notin F$, suy ra $m \neq 1$, vì thế $m > 1$, cho nên $m - 1 \in \mathbb{Z}^+$.

Mặt khác, $m - 1 \notin F$, nên $S(m-1)$ đúng. Theo giả thiết (b), $S((m-1)+1) = S(m)$ đúng, mâu thuẫn với $m \in F$. Nguyên lý quy nạp được chứng minh. □

Ví dụ 4.1. Chứng minh tổng các số nguyên dương đầu tiên:

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2},\ \forall n \in \mathbb{Z}^+. \tag{4.1}$$

Giải. Xét khẳng định mở $S(n)$: $\displaystyle\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

1) $S(1)$: $1 = \dfrac{1(1+1)}{2}$ đúng.

2) Giả sử với $n \in \mathbb{Z}^{+}$ cho trước, $S(n)$ đúng. Ta chứng minh $S(n+1)$ đúng. Thật vậy

$$\begin{aligned}\sum_{i=1}^{n+1} i &= \sum_{i=1}^{n} i + (n+1)\\ &= \frac{n(n+1)}{2} + (n+1), \quad \text{vì } S(n) \text{ đúng} \qquad (*)\\ &= \frac{(n+1)(n+2)}{2}.\end{aligned}$$

Theo nguyên lý quy nạp, $S(n)$ đúng $\forall n \in \mathbb{Z}^{+}$. □

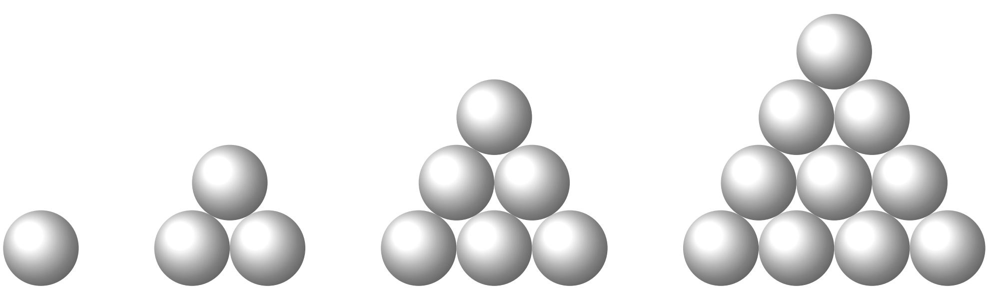
Với Python, ta có thể tính được $\sum_{i=1}^{n} i$ là $\frac{n(n+1)}{2}$. Tuy nhiên, chứng minh đẳng thức này cần thể hiện chặt chẽ như ví dụ trên.

```python
from sympy import *
n, i = symbols('n i')
Sum(i, (i, 1, n)).doit().simplify()   # dự đoán
```

$$\sum_{i=1}^{n} i \stackrel{?}{=} \frac{n(n+1)}{2}$$

```python
( n*(n+1)/2 + (n+1) ).factor()        # phân tích đa thức
    ở (*)
```

Các số $t_n = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, $n \in \mathbb{N}$, gọi là *số tam giác*.



$t_1 = 1$ $t_2 = 1 + 2$ $t_3 = 1 + 2 + 3$ $t_4 = 1 + 2 + 3 + 4$

Kết quả của ví dụ trên được vận dụng trong Ví dụ 4.2 và 4.3.

Ví dụ 4.2. Đánh số ngẫu nhiên từ 1 đến 36 trên một đường tròn. Chứng minh có ba số liên tiếp trên đường tròn có tổng ít nhất là 55.

Giải. Giả sử ngược lại, bất kỳ ba số liên tiếp trên đường tròn đều có tổng nhỏ hơn 55. Gọi $x_1, x_2, \dots, x_{36}$ là các số trên đường tròn. Khi đó $\{x_1, x_2, \dots, x_{36}\} = \{1, 2, \dots, 36\}$, và

$$x_1 + x_2 + x_3 < 55,\ x_2 + x_3 + x_4 < 55,\ \dots,\ x_{34} + x_{35} + x_{36} < 55,$$
$$x_{35} + x_{36} + x_1 < 55, x_{36} + x_1 + x_2 < 55.$$

Cộng từng vế các bất đẳng thức, lưu ý mỗi x_i, $i = \overline{1, 36}$ xuất hiện đúng ba lần

$$3\sum_{i=1}^{36} x_i < 36 \cdot 55 = 1980.$$

Mặt khác, $\{x_1, x_2, \dots, x_{36}\} = \{1, 2, \dots, 36\}$, suy ra $\sum_{i=1}^{36} x_i = \sum_{i=1}^{36} i = \frac{36 \cdot 37}{2} =$ 666, nên $3 \cdot 666 = 1998 < 1980$, mâu thuẫn!

Vậy có ba số liên tiếp trên đường tròn có tổng ít nhất là 55. □

Ví dụ 4.3. Số tự nhiên gọi là *đối xứng*, nếu đọc các chữ số từ trái sang phải hay từ phải sang trái đều như nhau, chẳng hạn 131, 222, 303, 717, 848, và 969.
Tính tổng các số đối xứng có ba chữ số.

Giải. Số đối xứng có ba chữ số có dạng $\overline{aba} = 100a + 10b + a = 101a + 10b$, với $1 \le a \le 9$ và $0 \le b \le 9$. Các số này có tổng bằng

$$\begin{aligned}
\sum_{a=1}^{9}\left(\sum_{b=0}^{9} aba\right) &= \sum_{a=1}^{9}\sum_{b=0}^{9}(101a + 10b) = \sum_{a=1}^{9}\left(10 \cdot 101a + 10\sum_{b=0}^{9} b\right)\\
&= \sum_{a=1}^{9}\left(1010a + 10\sum_{b=1}^{9} b\right) = \sum_{a=1}^{9}\left(1010a + 10\frac{9 \cdot 10}{2}\right)\\
&= \sum_{a=1}^{9}(1010a + 450) = 1010\sum_{a=1}^{9} a + 9 \cdot 450\\
&= 1010\frac{9 \cdot 10}{2} + 4050 = 49500.
\end{aligned}$$

□

Ví dụ 4.4. a) Bằng Python, với $n \in \mathbb{Z}^+$, dự đoán tổng n số chính phương đầu tiên:

$$\sum_{i=1}^{n} i^2 = 1^2 + 2^2 + 3^2 + \cdots + n^2.$$

b) Chứng minh kết quả ở ý (a).

Giải. a)

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} \tag{4.2}$$

```python
from sympy import *
n, i = symbols('n i')
Sum(i**2, (i, 1, n)).doit().factor()
```

b) Xét khẳng định mở $S(n)$: $\displaystyle\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$, $\forall n \in \mathbb{Z}^+$.

1) $S(1)$: $\quad 1^2 = \dfrac{1(1+1)(2\cdot 1+1)}{6}$ đúng.

2) Giả sử với $n \in \mathbb{Z}^+$ cho trước, $S(n)$ đúng. Ta sẽ chứng minh

$$S(n{+}1) : \quad \sum_{i=1}^{n+1} i^2 = \frac{(n+1)[(n+1)+1][2(n+1)+1]}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

đúng. Thật vậy

$$\begin{aligned}
\sum_{i=1}^{n+1} i^2 &= \sum_{i=1}^{n} i^2 + (n+1)^2 \\
&= \frac{n(n+1)(2n+1)}{6} + (n+1)^2, \quad \text{vì } S(n) \text{ đúng} && (*) \\
&= \frac{n+1}{6}[n(2n+1) + 6(n+1)] = \frac{(n+1)(2n^2+7n+6)}{6} \\
&= \frac{(n+1)(n+2)(2n+3)}{6}.
\end{aligned}$$

Theo nguyên lý quy nạp, $S(n)$ đúng $\forall n \in \mathbb{Z}^+$.

```python
(n*(n+1)*(2*n+1)/6 + (n+1)**2).factor()   # rút gọn
    (*)
```

□

Áp dụng kết quả của Ví dụ 4.1 và 4.4, ta có thể chứng minh trực tiếp kết quả sau

Ví dụ 4.5. Chứng minh tổng các số tam giác đầu tiên

$$\sum_{i=1}^{n} t_i = \frac{n(n+1)(n+2)}{6}, \quad \forall n \in \mathbb{Z}^+. \tag{4.3}$$

Giải.

$$\sum_{i=1}^{n} t_i = \sum_{i=1}^{n} \frac{i(i+1)}{2} = \frac{1}{2}\Big(\sum_{i=1}^{n} i^2 + \sum_{i=1}^{n} i\Big)$$
$$= \frac{1}{2}\Big[\frac{n(n+1)(2n+1)}{6} + \frac{n(n+1)}{2}\Big] = \frac{n(n+1)(n+2)}{6}$$

□

Ví dụ 4.6. a) Tính tổng của n số tự nhiên lẻ đầu tiên, với $n = \overline{1,5}$, và cho biết quy luật của các tổng này.

b) Dự đoán kết quả tổng quát và chứng minh dự đoán này.

Giải. a)

n	Tổng	Quy luật
1	$1 = 1$	1^2
2	$1 + 3 = 4$	2^2
3	$1 + 3 + 5 = 9$	3^2
4	$1 + 3 + 5 + 7 = 16$	4^2
5	$1 + 3 + 5 + 7 + 9 = 25$	5^2

```
for n in range(1, 6):
    a = [2*i - 1 for i in range(1, n+1)]   # dãy 1, 3,..., 2n − 1
    print(a, sum(a))
```

b) Dự đoán

$$\sum_{i=1}^{n} (2i-1) = n^2, \quad \forall n \in \mathbb{Z}^+. \tag{4.4}$$

Cách 1: Xét khẳng định mở $S(n)$: $\sum_{i=1}^{n} (2i-1) = n^2$.

1) $S(1)$: $1 = 1^2$ đúng.

2) Giả sử với $n \in \mathbb{Z}^+$ cho trước, $S(n)$ đúng. Ta sẽ chứng minh $S(n+1)$ đúng. Thật vậy

$$\begin{aligned}\sum_{i=1}^{n+1}(2i-1) &= \sum_{i=1}^{n}(2i-1) + [2(n+1)-1] \\ &= n^2 + (2n+1), \quad \text{vì } S(n) \text{ đúng} \\ &= (n+1)^2.\end{aligned}$$

Theo nguyên lý quy nạp, $S(n)$ đúng $\forall n \in \mathbb{Z}^+$.

Cách 2: $\displaystyle\sum_{i=1}^{n}(2i-1) = 2\sum_{i=1}^{n} i - \sum_{i=1}^{n} 1 = 2\frac{n(n+1)}{2} - n = n^2.$

□

Ví dụ 4.7. a) Tìm ba số nguyên dương n đầu tiên thỏa mãn $4n < n^2 - 7$.

b) Chứng minh $\forall n \in \mathbb{Z}^+$ $(n \geq 6)$, $4n < n^2 - 7$.

Giải. a)

n	$4n$	n^2-7	n	$4n$	n^2-7
1	4	-6	5	20	18
2	8	-3	6	24	29
3	12	2	7	28	42
4	16	9	8	32	57

```python
count = 0
n = 1
while count <= 3:
    print(n, 4*n, n**2 - 7)
    n += 1
    if 4*n < n**2 - 7:
        count += 1
```

b) Xét khẳng định mở $S(n)$: $\quad 4n < n^2 - 7$.

1) $S(6)$ đúng theo bảng ở ý (a).

2) Giả sử với $n \geq 6$ cho trước, $S(n)$ đúng. Ta chứng minh $S(n+1)$ đúng. Thật vậy

$$4(n+1) = 4n + 4 < (n^2 - 7) + 4.$$

Lúc này ta cần $(n^2-7)+4 \overset{?}{<} (n+1)^2 - 7$. Biến đổi tương đương bất đẳng thức, được

$$4 < 2n + 1,$$

và điều này đúng vì $n \geq 6$. Suy ra $4(n+1) < (n+1)^2 - 7$.

Theo nguyên lý quy nạp, $S(n)$ đúng $\forall n \geq 6$.

□

Ví dụ 4.8. [*]Cho số nguyên dương n. Chứng minh số tổng riêng của n là 2^{n-1}. [*Gợi ý:* xét số hạng đầu của mỗi tổng riêng là 1 hoặc khác 1.]

Giải. Xét khẳng định mở $S(n)$: số tổng riêng của n là 2^{n-1}.

1) $n = 1$ chỉ có một tổng riêng ($= 2^{1-1}$) là 1, tức là $S(1)$ đúng.

2) Giả sử với n cho trước, $S(n)$ đúng. Ta sẽ chứng minh $S(n+1)$ đúng.

   Với mỗi tổng riêng $x_1 + x_2 + \cdots + x_k$ của $n + 1$, xét hai khả năng

   i) $x_1 = 1$. Ta có tương ứng 1-1 giữa $(1, x_2, x_3, \ldots, x_k)$ với $(x_2, x_3, \ldots, x_k)$, trong đó $x_2 + x_3 + \cdots + x_k = n$, là một tổng riêng của n. Vì $S(n)$ đúng, số tổng riêng loại này là 2^{n-1}.

   ii) $x_1 > 1$. Ta lại có tương ứng 1-1 giữa $(x_1, x_2, \ldots, x_k)$ với $(x_1 - 1, x_2, x_3, \ldots, x_k)$, trong đó $(x_1 - 1) + x_2 + x_3 + \cdots + x_k = n$ là một tổng riêng của n. Số tổng riêng loại này là 2^{n-1}.

   Theo quy tắc cộng, số tổng riêng của $n + 1$ là $2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n$.

Theo nguyên lý quy nạp, $S(n)$ đúng $\forall n \in \mathbb{Z}^+$. □

Theo ví dụ trên, ta có thể xây dựng các tổng riêng của $n + 1$ đệ quy theo tổng riêng của n, được mô tả trong bảng sau, với $n = \overline{1, 4}$.

$n = 1$:		1	$n = 4$:	(1’)	1 + 1 + 1 + 1
				(1”)	1 + 1 + 2
$n = 2$:		1 + 1		(2’)	1 + 2 + 1
		2		(2”)	1 + 3
$n = 3$	(1)	1 + 1 + 1		(3’)	2 + 1 + 1
	(2)	1 + 2		(3”)	2 + 2
	(3)	2 + 1		(4’)	3 + 1
	(4)	3		(4”)	4

[*]Xem Ví dụ 1.30 trang 44 và 3.5 trang 103

```python
def summands(n):
    if n == 1:
        return [[1]]
    L = []
    for x in summands(n - 1):
        y = x.copy()
        x.append(1)
        L.append(x)
        y[-1] += 1
        L.append(y)
    return L
```

Ví dụ 4.9. *Với số tự nhiên n, chứng minh số tập con của tập cỡ n là 2^n.

Giải. Xét khẳng định mở $S(n)$: số tập con của tập cỡ n là 2^n.

1) Tập cỡ 0, tức là không có phần tử nào, là tập rỗng. Tập này chỉ có $1 = 2^0$ tập con. Ta có $S(0)$ đúng.

2) Giả sử với $n \geq 0$, $S(n)$ đúng. Xét tập A cỡ $n+1$. Khi đó $A = B \cup \{a\}$ trong đó B có cỡ n, và $a \notin B$. Mỗi tập con X của B ứng với hai tập con của A là X và $X \cup \{a\}$, và ngược lại. Vậy số tập con của A là $2 \cdot 2^n = 2^{n+1}$, tức là $S(n+1)$ đúng.

Theo nguyên lý quy nạp, $S(n)$ đúng, $\forall n \in \mathbb{N}$. □

Các ví dụ sau sử dụng nguyên lý quy nạp tổng quát.

Ví dụ 4.10. Chứng minh mọi số nguyên từ 14 trở đi đều phân tích được thành tổng của các số 3 và/hoặc 8.

Giải. Xét mệnh đề mở $S(n)$: n viết được thành tổng các số 3 và/hoặc 8.

1) $S(14)$ đúng, vì $14 = 3 + 3 + 8$

   $S(15)$ đúng, vì $15 = 3 + 3 + 3 + 3 + 3$

   $S(16)$ đúng, vì $16 = 8 + 8$.

*Định lý 3.3 trang 101

2) Giả sử với $n \geq 16$ cho trước, $S(14), S(15), \dots, S(n)$ đúng. Ta sẽ chứng minh $S(n+1)$ đúng. Trước hết, ta tách

$$n + 1 = 3 + (n - 2).$$

Vì $n \geq 16$, nên $14 \leq n - 2 \leq n$. Vì thế $S(n-2)$ đúng, tức là $n-2$ viết được thành tổng các số 3 và/hoặc 8. Do đó $n+1$ cũng vậy.

Theo giả thiết quy nạp, $S(n)$ đúng $\forall n \geq 14$. □

Ví dụ 4.11. Cho dãy (a_n) xác định bởi $a_0 = 1, a_1 = 2, a_2 = 3$ và $a_n = a_{n-1} + a_{n-2} + a_{n-3}, \forall n \in \mathbb{Z}^+, n \geq 3$. Chứng minh $\forall n \in \mathbb{N},\ a_n \leq 3^n$.

Giải. Xét khẳng định mở $S(n)$: $\quad a_n \leq 3^n$.

1) $S(0)$: $\quad 1 \leq 1^0$, đúng

$S(1)$: $\quad 2 \leq 3^1$, đúng

$S(2)$: $\quad 3 \leq 3^2$, đúng.

2) Giả sử với $n \geq 2$ cho trước, $S(0), S(1), \dots, S(n)$ đúng. Ta sẽ chứng minh $S(n+1)$ đúng. Vì $0 \leq n, n-1, n-2 \leq n$, nên $S(n), S(n-1), S(n-2)$ đúng. Suy ra

$$a_{n+1} = a_n + a_{n-1} + a_{n-2} \leq 3^n + 3^{n-1} + 3^{n-2} \leq 3^n + 3^n + 3^n = 3 \cdot 3^n = 3^{n+1}.$$

Theo nguyên lý quy nạp, $S(n)$ đúng $\forall n \in \mathbb{N}$. □

Bài tập 4.1

4.1. Chứng minh các khẳng định sau với mọi $n \geq 1$ bằng phương pháp quy nạp.

a) $1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \dfrac{n(2n-1)(2n+1)}{3}$

b) $1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + n(n+2) = \dfrac{n(n+1)(2n+7)}{6}$

c) $\displaystyle\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$

d) $\displaystyle\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4} = \left(\sum_{i=1}^{n} i\right)^2$

e) $\displaystyle\sum_{i=1}^{n} 2^{i-1} = \sum_{i=0}^{n-1} 2^i = 2^n - 1$

f) $\displaystyle\sum_{i=1}^{n} i \cdot 2^i = 2 + (n-1)2^{n+1}$

g) $\displaystyle\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$

Kiểm tra giả thiết ban đầu tại $n = 1$. Trong bước quy nạp, chỉ ra

a) $\dfrac{n(2n-1)(2n+1)}{3} + (2n+1)^2 = \dfrac{(n+1)(2n+1)(2n+3)}{3}$

b) $\dfrac{n(n+1)(2n+7)}{6} + (n+1)(n+3) = \dfrac{(n+1)(n+2)(2n+9)}{6}$

c) $\dfrac{n}{n+1} + \dfrac{1}{(n+1)(n+2)} = \dfrac{n+1}{n+2}$

d) $\dfrac{n^2(n+1)^2}{4} + (n+1)^3 = \dfrac{(n+1)^2(n+2)^2}{4}$

e) $(2^n - 1) + 2^n = 2^{n+1} - 1$

f) $[2 + (n-1)2^{n+1}] + (n+1)2^{n+1} = 2 + n \cdot 2^{n+2}$

g) $[(n+1)! - 1] + (n+1)(n+1)! = (n+2)! - 1$

4.2. a) Dùng phép biến đổi $\displaystyle\sum_{i=1}^{n} i^3 + (n+1)^3 = \sum_{i=0}^{n} (i+1)^3 = \sum_{i=0}^{n} (i^3 + 3i^2 + 3i + 1)$, và kết quả của Ví dụ 4.1 để tính $\displaystyle\sum_{i=1}^{n} i^2$ trong Ví dụ 4.2.

b) Dùng ý tưởng của ý (a), sử dụng kết quả của Ví dụ 4.1 và 4.2 để tính $\displaystyle\sum_{i=1}^{n} i^3$ trong Bài tập 4.1(d). Từ đó tiếp tục tính $\displaystyle\sum_{i=1}^{n} i^4$.

a) $\displaystyle\sum_{i=1}^{n} i^3 + (n+1)^3 = \sum_{i=0}^{n} (i^3 + 3i^2 + 3i + 1) = \sum_{i=1}^{n} i^3 + 3\sum_{i=1}^{n} i^2 + 3\sum_{i=1}^{n} i + \sum_{i=0}^{n} 1$. Suy ra $\displaystyle 3\sum_{i=1}^{n} i^2 = (n+1)^3 - 3\frac{n(n+1)}{2} - (n+1) = \frac{n(n+1)(2n+1)}{2}$.

b) $\displaystyle\sum_{i=1}^{n} i^4 + (n+1)^4 = \sum_{i=0}^{n} (i+1)^4 = \sum_{i=0}^{n} (i^4 + 4i^3 + 6i^2 + 4i + 1) = \sum_{i=1}^{n} i^4 + 4\sum_{i=1}^{n} i^3 + 6\sum_{i=1}^{n} i^2 + 4\sum_{i=1}^{n} i + \sum_{i=0}^{n} 1$. Suy ra $\displaystyle 4\sum_{i=1}^{n} i^3 = (n+1)^4 - 6\frac{n(n+1)(2n+1)}{6} - 4\frac{n(n+1)}{2} - (n+1)$.

Tương tự, từ $\displaystyle\sum_{i=1}^{n} i^5 + (n+1)^5 = \sum_{i=0}^{n} (i+1)^5 = \sum_{i=0}^{n} (i^5 + 5i^4 + 10i^3 + 10i^2 + 5i + 1)$, ta được $\displaystyle\sum_{i=1}^{n} i^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30}$.

4.3. Đặt ngẫu nhiên các số từ 1 tới 25 trên một vòng tròn. Chứng minh trên vòng tròn có ba số liên tiếp có tổng ít nhất là 39.

Xem Ví dụ 4.2

4.4. Cho đoạn chương trình (dạng giả mã)

```
1 for i := 1 to 123 do
2     for j := 1 to i do
3         print i*j
```

a) Lệnh `print` ở dòng 3 được thực hiện bao nhiêu lần?

b) Ở dòng 2, nếu thay i bởi i^2 thì câu trả lời ở ý (a) là bao nhiêu?

a) $\sum_{i=1}^{123} i = 7\,626$ (theo quy tắc cộng) b) $\sum_{i=1}^{123} i^2 = 627\,874$

4.5. a) Trong các số tự nhiên có bốn chữ số (từ 1000 tới 9999), có bao nhiêu số đối xứng? Tính tổng các số đó.

b) Viết một chương trình để tính tổng ở ý (a).

a) $9 \cdot 10$, $495\,000$ [Xem Ví dụ 4.3]

b) **Cách 1:**

```
s = 0
for a in range(1, 10):
    for b in range(10):
        s += 1001*a + 110*b

s
```

Cách 2:

```
from sympy import *
a, b = symbols('a b')
Sum(1001*a + 110*b, (a, 1, 9), (b, 0, 9)).doit()
```

4.6. Một đống gồm $4n + 110$ khúc gỗ xếp thành n lớp sao cho mỗi lớp nhiều hơn hai khúc so với lớp ngay trên nó. Nếu lớp trên cùng có 6 khúc gỗ, thì đống gỗ có bao nhiêu lớp?

$$4n + 110 = \sum_{i=0}^{n-1} (6 + 2i) = \sum_{i=0}^{n-1} 6 + 2\sum_{i=0}^{n-1} i = 6n + 2\frac{(n-1)n}{2} \Rightarrow n = 10.$$

4.7. Tìm số nguyên dương n để $\sum_{i=1}^{2n} i = \sum_{i=1}^{n} i^2$.

$$\frac{(2n)(2n+1)}{2} = \frac{n(n+1)(2n+1)}{6} \Rightarrow n = 5.$$

4.8. Tính

a) $\sum_{i=11}^{33} i$ b) $\sum_{i=11}^{33} i^2$

a) $\sum_{i=1}^{33} i - \sum_{i=1}^{10} i = \frac{33\cdot 34}{2} - \frac{10\cdot 11}{2} = 506$

b) $\sum_{i=1}^{33} i^2 - \sum_{i=1}^{10} i^2 = \frac{33\cdot 34(2\cdot 33+1)}{6} - \frac{10\cdot 11(2\cdot 10+1)}{6} = 12144$

4.9. Tính $\sum_{i=51}^{100} t_i$, trong đó t_i là số tam giác thứ i.

$$\sum_{i=1}^{100} t_i - \sum_{i=1}^{50} t_i = \frac{100\cdot 101\cdot 102}{6} - \frac{50\cdot 51\cdot 52}{6} = 149\,600$$

4.10. a) Chứng minh $(\cos\theta + i\sin\theta)^2 = \cos 2\theta + i\sin 2\theta$, trong đó $i \in \mathbb{C}$ và $i^2 = -1$.

b) Dùng phương pháp quy nạp, chứng minh công thức Moivre*: $\forall n \in \mathbb{Z}^+$, $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$.

c) Kiểm tra $1 + i = \sqrt{2}(\cos 45^\circ + i\sin 45^\circ)$, và tính $(1+i)^{100}$.

4.11. Chứng minh $\forall n \in \mathbb{Z}^+, n > 3 \Rightarrow 2^n < n!$

4.12. Chứng minh $\forall n \in \mathbb{Z}^+, n > 4 \Rightarrow n^2 < 2^n$.

4.13. Với $n \in \mathbb{Z}^+$, xét H_n là số điều hòa thứ n (xem Ví dụ 4.14). Chứng minh

a) $1 + \frac{n}{2} \leq H_{2^n}, \ \forall n \in \mathbb{N}$.

b) $\sum_{j=1}^{n} jH_j = \frac{n(n+1)}{2}(H_{n+1} - \frac{1}{2}), \ \forall n \in \mathbb{Z}^+$.

4.14. Xét bốn đẳng thức sau

1)	$1 = 1$
2)	$2+3+4 = 1+8$
3)	$5+6+7+8+9 = 8+27$
4)	$10+11+12+13+14+15+16 = 27+64$

Dự đoán công thức tổng quát và chứng minh công thức đó.

*Abraham de Moivre, 1667–1754, nhà toán học Pháp

4.15. a) Cho $n \in \mathbb{Z}^+ - \{1, 3\}$. Chứng minh n có thể biểu diễn thành tổng của 2 và/hoặc 5.

b) Chứng minh $\forall n \in \mathbb{Z}^+$, nếu $n \geq 24$ thì có thể viết n thành tổng của 5 và/hoặc 7.

4.16. Dãy số $a_1, a_2, a_3, \ldots$ xác định bởi $a_1 = 1$, $a_2 = 2$, và $a_n = a_{n-1} + a_{n-2},\ n \geq 3$.

a) Tìm a_3, a_4, a_5, a_6, và a_7.

b) Chứng minh $\forall n \geq 1, a_n < \left(\frac{7}{4}\right)^n$.

4.17. Cho $n \in \mathbb{Z}^+$. Xét biến ngẫu nhiên X có phân bố đều trên $\{1, 2, \ldots, n\}$, tức là $P(X = x) = \frac{1}{n}$, $x = 1, 2, \ldots, n$. Xác định EX và VX.

4.18. Lập trình liệt kê các tập con của tập cỡ n.

4.2 Định nghĩa đệ quy

Cho dãy số (a_n). Đẳng thức chỉ ra sự phụ thuộc của một phần tử của dãy vào các phần tử đứng trước nó gọi là hệ thức đệ quy.

Ví dụ 4.12.

$$a_0 = 1, a_1 = 2, a_2 = 3, \quad \text{và}$$
$$a_n = a_{n-1} + a_{n-2} + a_{n-3}, \quad n = 3, 4, \ldots$$

Ví dụ 4.13. Các dãy số như số nguyên chẵn, số giai thừa, số điều hòa có thể viết dưới dạng hệ thức đệ quy

a) 1) $e_0 = 0$, và
2) $e_{n+1} = e_n + 2$, với $n \geq 0$.

b) 1) $0! = 1$, và
2) $(n+1)! = (n+1)(n!)$, với $n \geq 0$.

c) 1) $H_1 = 1$, và
2) $H_{n+1} = H_n + \dfrac{1}{n+1}$, với $n \geq 1$.

Ví dụ 4.14. Ký hiệu $H_n = \sum_{i=1}^{n} \frac{1}{i} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$, với $n \in \mathbb{Z}^+$, gọi là *số điều* *hòa*. Chứng minh $\sum_{i=1}^{n} H_i = (n+1)H_n - n, \ \forall n \in \mathbb{Z}^+$.

Giải. Xét khẳng định mở $S(n)$: $\sum_{i=1}^{n} H_i = (n+1)H_n - n$.

1) $S(1)$: $1 = (1+1)\cdot 1 - 1$ đúng.

2) Giả sử với $n \in \mathbb{Z}^+$ cho trước, $S(n)$ đúng. Ta sẽ chứng minh $S(n+1)$ đúng. Thật vậy

$$\begin{aligned}
\sum_{i=1}^{n+1} H_i &= \sum_{i=1}^{n} H_i + H_{n+1} \\
&= [(n+1)H_n - n] + H_{n+1}, \quad \text{vì } S(n) \text{ đúng} \\
&= \left[(n+1)\left(H_{n+1} - \frac{1}{n+1}\right) - n\right] + H_{n+1} \\
&= (n+2)H_{n+1} - (n+1).
\end{aligned}$$

Theo nguyên lý quy nạp, $S(n)$ đúng $\forall n \in \mathbb{Z}^+$. □

Ví dụ 4.15. Dãy số Fibonacci* F_n định nghĩa đệ quy bởi

1) $F_0 = 0, F_1 = 1$, và

2) $F_n = F_{n-1} + F_{n-2}, \ n \geq 2$.

Hãy

a) Tìm F_n, với $2 \leq n \leq 10$.

b) Chứng minh $\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}, \ \forall n \in \mathbb{N}$.

Giải. a)

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

b) Ký hiệu khẳng định mở $S(n)$: $\sum_{i=0}^{n} F_i^2 = F_n F_{n+1}$.

*Fibonacci, 1170–1250, nhà toán học Ý

1) $S(0)$: $F_0^2 = F_0F_1$, hay $0^2 = 0 \cdot 1$, là khẳng định đúng.

2) Giả sử, với $n \in \mathbb{N}$ cố định, $S(n)$ đúng. Khi đó

$$\begin{aligned}\sum_{i=0}^{n+1} F_i^2 &= \sum_{i=0}^{n} F_i^2 + F_{n+1}^2 \\ &= F_nF_{n+1} + F_{n+1}^2, \quad \text{vì } S(n) \text{ đúng} \\ &= F_{n+1}(F_n + F_{n+1}) \\ &= F_{n+1}F_{n+2}\end{aligned}$$

nên $S(n+1)$ đúng.

Theo nguyên lý quy nạp, $S(n)$ đúng, $\forall n \in \mathbb{N}$.

□

Ví dụ 4.16. Số Lucas* L_n có định nghĩa đệ quy

1) $L_0 = 2, L_1 = 1$, và

2) $L_n = L_{n-1} + L_{n-2}$, $n \geq 2$.

Hãy

a) Tìm L_n với $2 \leq n \leq 7$.

b) Chứng minh $\forall n \in \mathbb{Z}^+$, $L_n = F_{n-1} + F_{n+1}$.

Giải. a)

n	0	1	2	3	4	5	6	7
L_n	2	1	3	4	7	11	18	29

b) Ký hiệu khẳng định mở $S(n)$: $L_n = F_{n-1} + F_{n+1}$.

1) $S(1)$: $L_1 = F_0 + F_2$, hay $1 = 0 + 1$, là khẳng định đúng.

$S(2)$: $L_2 = F_1 + F_3$, hay $3 = 1 + 2$, đúng.

2) Giả sử, với $n \geq 2$ cố định, $S(1), S(2), \ldots, S(n)$ đúng. Khi đó

$$\begin{aligned}L_{n+1} &= L_n + L_{n-1} \\ &= (F_{n-1} + F_{n+1}) + (F_{n-2} + F_n), \quad S(n), S(n-1) \text{ đúng vì } 1 \leq n, n-1 \leq n\end{aligned}$$

*François Édouard Anatole Lucas, 1842–1891, nhà toán học Pháp

$$= (F_{n-1} + F_{n-2}) + (F_n + F_{n+1})$$
$$= F_n + F_{n+2}$$

nên $S(n+1)$ đúng.

Theo nguyên lý quy nạp, $S(n)$ đúng, $\forall n \in \mathbb{Z}^+$.

□

Ví dụ 4.17. Số Euler* a_{mk}, với $m, k \in \mathbb{N}$, định nghĩa đệ quy bởi

1) $a_{mk} = (m-k)a_{m-1,k-1} + (k+1)a_{m-1,k}$, với $0 \leq k \leq m-1$, trong đó

2) $a_{00} = 1$, $a_{mk} = 0$ với $k \geq m$ (ngoại trừ $a_{00} = 1$) hoặc $k < 0$.

Hãy

a) Tìm các số a_{mk} với $0 \leq k < m \leq 5$.

b) Chứng minh $\sum\limits_{k=0}^{m-1} a_{mk} = m!$, $\forall m \in \mathbb{Z}^+$.

Giải. a)

m	$k = \overline{0, m-1}$				
1	1				
2	1	1			
3	1	4	1		
4	1	11	11	1	
5	1	26	66	26	1

b) Ký hiệu khẳng định mở $S(n)$: $\sum\limits_{k=0}^{m-1} a_{mk} = m!$.

1) $S(1)$: $a_{10} = 1 = 1!$, là khẳng định đúng.

2) Giả sử với $m \in \mathbb{Z}^+$ cố định, $S(m)$ đúng. Khi đó

$$\sum_{k=0}^{m} a_{m+1,k} = \sum_{k=0}^{m} [(m+1-k)a_{m,k-1} + (k+1)a_{mk}]$$

*Leonhard Euler, 1707–1783, nhà toán học, vật lý, thiên văn học, nhà lý luận và kỹ sư Thụy Sĩ

$$\begin{aligned}
&= \sum_{k=0}^{m} (m+1)a_{m,k-1} - \sum_{k=0}^{m} k a_{m,k-1} + \sum_{k=0}^{m} (k+1)a_{mk} \\
&= (m+1)\sum_{k=-1}^{m-1} a_{mk} - \sum_{k=-1}^{m} (k+1)a_{mk} + \sum_{k=0}^{m} (k+1)a_{mk} \\
&= (m+1)\sum_{k=0}^{m-1} a_{mk} - \sum_{k=0}^{m} (k+1)a_{mk} + \sum_{k=0}^{m} (k+1)a_{mk} \\
&= (m+1)\sum_{k=0}^{m-1} a_{mk} \\
&= (m+1)\cdot m! = (m+1)!
\end{aligned}$$

nên $S(n+1)$ đúng.

Theo nguyên lý quy nạp, $S(n)$ đúng, $\forall n \in \mathbb{Z}^+$.

$\square$

Ví dụ 4.18. Dùng hệ thức đệ quy

1) $\binom{n+1}{r} = \binom{n}{r} + \binom{n}{r-1}$ với $n \geq r \geq 0$, trong đó

2) $\binom{0}{0} = 1$, $\binom{n}{r} = 0$ với $r > n$ hoặc $r < 0$.

để chứng minh $\displaystyle\sum_{r=0}^{n} \binom{n}{r} = 2^n$, $\forall n \in \mathbb{N}$.

Giải. Ký hiệu khẳng định mở $S(n)$: $\displaystyle\sum_{r=0}^{n} \binom{n}{r} = 2^n$.

1) $S(0)$: $\binom{0}{0} = 2^0$, là khẳng định đúng.

2) Giả sử với $n \in \mathbb{N}$ cố định, $S(n)$ đúng. Khi đó

$$\begin{aligned}
\sum_{r=0}^{n+1} \binom{n+1}{r} &= \sum_{r=0}^{n+1} \left[\binom{n}{r} + \binom{n}{r-1}\right] \\
&= \sum_{r=0}^{n+1} \binom{n}{r} + \sum_{r=0}^{n+1} \binom{n}{r-1}
\end{aligned}$$

$$= \sum_{r=0}^{n+1} \binom{n}{r} + \sum_{r=-1}^{n} \binom{n}{r}$$
$$= \sum_{r=0}^{n} \binom{n}{r} + \sum_{r=0}^{n} \binom{n}{r}$$
$$= 2^n + 2^n = 2^{n+1}$$

nên $S(n+1)$ đúng.

Theo nguyên lý quy nạp, $S(n)$ đúng, $\forall n \in \mathbb{N}$. □

Một tập hợp được định nghĩa đệ quy bởi

1) các phần tử ban đầu, và

2) các quy tắc thành tìm phần tử mới theo phần tử đã có.

Tập A gọi là tập "nhỏ nhất" thỏa mãn định nghĩa đệ quy trên, nếu B là tập bất kỳ cũng thỏa mãn định nghĩa đệ quy, thì $A \subseteq B$.

Ví dụ 4.19. Cho A là tập nhỏ nhất thỏa mãn định nghĩa đệ quy

1) $1 \in A$.

2) $\forall a \in X,\ a + 2 \in A$.

Chứng minh A là tập các số tự nhiên lẻ.

Giải. Ký hiệu tập các số tự nhiên lẻ là $B = \{2n+1 \mid n \in \mathbb{N}\}$. Ta sẽ chứng minh $A = B$.

a) Để chứng minh $A \subseteq B$, ta chỉ ra B cũng thỏa mãn định nghĩa đệ quy. Thật vậy

   1) Với $n = 0 \in \mathbb{N}$, ta có $2 \cdot 0 + 1 = 1 \in B$.

   2) Giả sử $a \in B$, tức là $\exists n \in \mathbb{N},\ a = 2n+1$. Khi đó $a + 2 = (2n+1) + 2 = 2(n+1) + 1 \in B$, vì $n + 1 \in \mathbb{N}$.

b) Tiếp theo, ta chứng minh $B \subseteq A$, tức là $2n+1 \in A,\ \forall n \in \mathbb{N}$, bằng phương pháp quy nạp. Xét khẳng định mở

$$S(n): \quad 2n+1 \in A,$$

với $n \in \mathbb{N}$.

1) $S(0)$ đúng, vì $2 \cdot 0 + 1 = 1 \in A$.

2) Giả sử với $n \in \mathbb{N}$ nào đó, $S(n)$ đúng, hay $2n+1 \in A$. Khi đó $2(n+1)+1 = (2n+1)+2 \in A$, tức là $S(n+1)$ đúng.

Theo phương pháp quy nạp, ta có $B \subseteq A$.

Vì $A \subseteq B$, và $B \subseteq B$, nên $A = B$. □

Với các phép toán hai ngôi có tính chất kết hợp, ta có thể "định nghĩa tốt" phép toán đó cho nhiều ngôi bằng cách đệ quy theo phép toán với ít ngôi hơn. Chẳng hạn, phép $\vee, \wedge$ đối với mệnh đề, hay $\cup, \cap$ đối với tập hợp.

Ví dụ 4.20. Chứng minh với mọi $n \in \mathbb{Z}^+$, $n \geq 3$, với các mệnh đề $p_1, p_2, \dots, p_n$ ta có

$$(p_1 \wedge p_2 \wedge \cdots \wedge p_r) \wedge (p_{r+1} \wedge \cdots \wedge p_n) \Leftrightarrow p_1 \wedge p_2 \wedge \cdots \wedge p_n, \ \forall 1 \leq r < n.$$

Trường hợp đặc biệt, với $r = n - 1$

$$p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1} \wedge p_n \Leftrightarrow (p_1 \wedge p_2 \wedge \cdots \wedge p_{n-1}) \wedge p_n.$$

Tương tự, cho các tập $A_1, A_2, \dots, A_n$, $n \geq 3$, ta cũng có các định nghĩa đệ quy

$$\begin{aligned} A_1 \cup A_2 \cup \cdots \cup A_n &= (A_1 \cup A_2 \cup \cdots \cup A_r) \cup (A_{r+1} \cup \cdots \cup A_n), \ \forall 1 \leq r < n \\ &= (A_1 \cup A_2 \cup \cdots \cup A_{n-1}) \cup A_n. \end{aligned}$$

Bài tập 4.2

4.19. Dãy số nguyên $a_1, a_2, a_3, \dots$ có công thức hiện $a_n = 5n$ với $n \in \mathbb{Z}^+$, có thể định nghĩa đệ quy bởi

1) $a_1 = 5$, và

2) $a_{n+1} = a_n + 5$, với $n \geq 1$.

Còn dãy số nguyên $b_1, b_2, b_3, \dots$ trong đó $b_n = n(n+2)$ với $n \in \mathbb{Z}^+$, cũng có dạng đệ quy

1) $b_1 = 3$, và

2) $b_{n+1} = b_n + 2n + 3$, với $n \geq 1$.

Tìm một định nghĩa đệ quy cho dãy số nguyên $c_1, c_2, c_3, \dots$, trong đó với $n \in \mathbb{Z}^+$,

a) $c_n = 7n$

b) $c_n = 7^n$

c) $c_n = 3n + 7$

d) $c_n = 7$

e) $c_n = n^2$

f) $c_n = 2 - (-1)^n$

4.20. Cho $n \geq 2$ và các tập bất kỳ $A_2, A_2, \ldots, A_n \subseteq \mathcal{U}$. Chứng minh

$$\overline{A_1 \cup A_2 \cup \cdots \cup A_n} = \overline{A}_1 \cap \overline{A}_2 \cap \cdots \cap \overline{A}_n.$$

4.21. Chứng minh rằng nếu $n \in \mathbb{Z}^+$, $n \geq 2$, và $x_1, x_2, \ldots, x_n \in \mathbb{R}$, thì

$$|x_1 + x_2 + \cdots + x_n| \leq |x_1| + |x_2| + \cdots + |x_n|.$$

4.22. Cho định nghĩa đệ quy của dãy $a_0, a_1, a_2, \ldots$

1) $a_0 = 1, a_1 = 1, a_2 = 1$; và

2) Với $n \geq 3$, $a_n = a_{n-1} + a_{n-3}$.

Chứng minh $a_{n+2} \geq (\sqrt{2})^n$, $\forall n \geq 0$.

4.23. Với $n \geq 0$, ký hiệu F_n là số Fibonacci thứ n. Chứng minh

$$F_0 + F_1 + F_2 + \cdots + F_n = \sum_{i=0}^{n} F_i = F_{n+2} - 1.$$

4.24. Chứng minh $\forall n \in \mathbb{Z}^+$, $\displaystyle\sum_{i=1}^{n} \frac{F_{i-1}}{2^i} = 1 - \frac{F_{n+2}}{2^n}$.

4.25. Trong Ví dụ 4.16, ký hiệu $L_0, L_1, L_2, \ldots$ là các số Lucas, trong đó (1) $L_0 = 2, L_1 = 1$; và (2) $L_{n+2} = L_{n+1} + L_n$, với $n \geq 0$. Khi $n \geq 1$, chứng minh

$$L_1^2 + L_2^2 + L_3^2 + \cdots + L_n^2 = L_n L_{n+1} - 2.$$

4.26. Với $n \in \mathbb{N}$, chứng minh $5F_{n+2} = L_{n+4} - L_n$.

4.27. Cho một định nghĩa đệ quy cho tập

a) các số nguyên dương chẵn

b) các số nguyên không âm chẵn

4.3 Thuật toán chia: số nguyên tố

Định nghĩa 4.1. *Cho $a, b \in \mathbb{Z}$, $b \neq 0$. Ta nói b phân chia a, hay b là ước của a, ký hiệu $b \mid a$, nếu $\exists n \in \mathbb{Z},\ a = bn$. Ta cũng nói a chia hết cho b, hay a là bội của b.*

Định lý 4.2. *Với $a, b, c \in \mathbb{Z}$*

a) $1 \mid a$, và $a \mid 0$.

b) $a \mid b \wedge b \mid a \Rightarrow a = \pm b$.

c) $a \mid b \wedge b \mid c \Rightarrow a \mid c$.

d) $a \mid b \Rightarrow a \mid bc$.

e) *Nếu $x = y + z$, với $x, y, z \in \mathbb{Z}$, và a là ước của hai trong ba số x, y, z, thì a là ước của số còn lại.*

f) $a \mid b \wedge a \mid c \Rightarrow a \mid (bx + cy),\ \forall x, y \in \mathbb{Z}$. *(Biểu thức $bx + cy$ gọi là tổ hợp tuyến tính của b và c.)*

g) *Cho $n \in \mathbb{Z}^+$, $c_i \in \mathbb{Z}$, $i = \overline{1, n}$. Nếu $a \mid c_i$, $\forall i = \overline{1, n}$ thì $a \mid (c_1x_1 + c_2x_2 + \cdots + c_nx_n),\ \forall x_1, x_2, \ldots, x_n \in \mathbb{Z}$.*

Ví dụ 4.21. Có tồn tại các số nguyên x, y, z để $6x + 9y + 15z = 107$?

Giải. Giả sử $\exists x, y, z \in \mathbb{Z},\ 6x + 9y + 15z = 107$. Vì 3 là ước của 6, 9 và 15, nên $3 \mid (6x + 9y + 15z)$, tức là $3 \mid 107$, mâu thuẫn! Vậy $\nexists x, y, z \in \mathbb{Z},\ 6x + 9y + 15z = 107$. □

Ví dụ 4.22. Cho $a, b \in \mathbb{Z}$ sao cho $17 \mid (2a + 3b)$. Chứng minh $17 \mid (9a + 5b)$.

Giải. Ta có $4(2a+3b) + (9a+5b) = 17(a+b)$. Vì $17 \mid (2a+3b)$ nên $17 \mid 4(2a+3b)$. Mặt khác, $17 \mid 17(a+n)$, nên $17 \mid (9a+5b)$. □

Định nghĩa 4.2. *Cho số nguyên $n > 1$. n gọi là số nguyên tố nếu nó chỉ có hai ước là 1 và chính nó. Ngược lại, n gọi là hợp số.*

Bổ đề 4.1. *Mọi số nguyên lớn hơn 1 đều có ước nguyên tố.*

Định lý 4.3 (Euclid)**.** [*] *Có vô hạn số nguyên tố.*

Định lý 4.4 (Thuật toán chia)**.** *Nếu $a, b \in \mathbb{Z}$ với $b > 0$, thì tồn tại duy nhất $q, r \in \mathbb{Z}$, $0 \leq r < b$ sao cho $a = qb + r$.*

Trong biểu thức chia $a = qb + r$, a gọi là số bị chia, b là số chia, và q là thương, r là phần dư của phép chia a cho b, ký hiệu

$$q = a \text{ div } b, \quad r = a \bmod b.$$

Ví dụ 4.23. a) $170 = 15 \cdot 11 + 5$, trong đó $0 \leq 5 < 11$, nên $170 \text{ div } 11 = 15$, $170 \bmod 11 = 5$.

b) $98 = 14 \cdot 7$, hay $98 = 14 \cdot 7 + 0$, nên $98 \text{ div } 7 = 14$, $98 \bmod 7 = 0$. Ở đây $7 \mid 98$.

c) $-45 = (-6)8 + 3$, trong đó $0 \leq 3 < 8$, nên $-45 \text{ div } 8 = -6$, $-45 \bmod 8 = 3$.

d) Với $a, b \in \mathbb{Z}^+$,

1) Nếu $a = qb$, với $q \in \mathbb{Z}^+$, thì $-a = (-q)b$. Khi đó

$$-a \text{ div } b = -q, -a \bmod b = 0.$$

2) Nếu $a = qb + r$, với $q \in \mathbb{Z}$ và $0 < r < b$, thì $-a = (-q)b - r = (-q)b - b + b - r = (-q - 1) + (b - r)$, trong đó $0 < b - r < b$. Khi đó

$$-a \text{ div } b = -q - 1, -a \bmod b = b - r.$$

Ví dụ 4.24. Nếu $n \in \mathbb{Z}^+$ là hợp số, thì có số nguyên tố $p \leq \sqrt{n}$ sao cho $p \mid n$.

Giải. Vì n là hợp số, ta có thể viết $n = n_1 n_2$, trong đó $n_1, n_2 > 1$ là các số nguyên.

Trước hết, ta chứng minh $n_1 \leq \sqrt{n}$ hoặc $n_2 \leq \sqrt{n}$. Thật vậy, nếu ngược lại, tức là $n_1, n_2 > \sqrt{n}$, thì $n_1 n_2 > \sqrt{n}\sqrt{n}$, suy ra $n > n$, mâu thuẫn!

[*] Euclid, khoảng 330–275 trước công nguyên, nhà toán học Hy Lạp

Không mất tổng quát, giả sử $n_1 \le \sqrt{n}$. Vì $n_1 > 1$, theo Bổ đề 4.1, có số nguyên tố p là ước của n_1. Vì $n_1 \mid n$ nên $p \mid n$. Mặt khác, $p \le n_1 \le \sqrt{n}$, nên p là số nguyên tố thỏa mãn bài toán. □

Bài tập 4.3

4.28. Cho $a, b, c, d \in \mathbb{Z}^+$. Chứng minh

a) $a \mid b \wedge c \mid d \Rightarrow ac \mid bd$

b) $a \mid b \Rightarrow ac \mid bc$, và

c) $ac \mid bc \Rightarrow a \mid b$.

4.29. Nếu p, q nguyên tố, thì $p \mid q$ khi và chỉ khi $p = q$.

4.30. Nếu $a, b, c \in \mathbb{Z}^+$ và $a \mid bc$, thì có suy ra được $a \mid b$ hoặc $a \mid c$ không?

4.31. Với $a, b, c \in \mathbb{Z}$, chứng minh nếu $a \nmid bc$, thì $a \nmid b$ và $a \nmid c$.

4.32. Cho $n \in \mathbb{Z}^+$, $n \geq 2$. Chứng minh nếu $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{Z}^+$ và $a_i \mid b_i$, $\forall i = \overline{1, n}$, thì $(a_1 a_2 \cdots a_n) \mid (b_1 b_2 \cdots b_n)$.

4.33. a) Tìm một giá trị của các số nguyên dương a, b, c sao cho $31 \mid (5a + 7b + 11c)$.

b) Cho $a, b, c \in \mathbb{Z}$ và $31 \mid (5a + 7b + 11c)$, chứng minh $31 \mid (21a + 17b + 9c)$.

4.34. Cho $a, b \in \mathbb{Z}^+$. Nếu $b \mid a$ và $b \mid (a + 2)$, chứng minh $b = 1$ hoặc $b = 2$.

4.35. Nếu $n \in \mathbb{Z}^+$, và n lẻ, chứng minh $8 \mid (n^2 - 1)$.

4.36. Nếu $a, b \in \mathbb{Z}^+$, và cùng lẻ, chứng minh $2 \mid (a^2 + b^2)$ nhưng $4 \nmid (a^2 + b^2)$.

4.37. Tìm thương q và phần dư r của phép chia a cho b:

a) $a = 23, b = 7$

b) $a = -115, b = 12$

c) $a = 0, b = 42$

d) $a = 434, b = 31$

4.38. Chứng minh $3 \mid (7^n - 4^n)$, $\forall n \in \mathbb{N}$.

4.39. Viết các số nguyên sau (cơ số 10) theo cơ số 2, 4, và 8.

a) 137 b) 6243 c) 12 345

4.40. Viết các số nguyên (cơ số 10) theo cơ số 2 và 16.

a) 22 b) 527 c) 1234 d) 6923

4.41. Chuyển các số trong hệ thập lục phân sau sang cơ số 2 và 10.

a) A7 b) 4C2 c) 1C2B d) A2DFE

4.42. Chuyển các số nhị phân sau sang cơ số 10 và 16.

a) 11 001 110 b) 00 110 001 c) 11 110 000 d) 01 010 111

4.43. Trong cơ số nào ta có đẳng thức $251 + 445 = 1026$?

4.44. Tìm tất cả $n \in \mathbb{Z}^+$ để n chia đều $5n + 18$.

4.45. Thuật toán chia có thể tổng quát hóa như sau: Với $a, b \in \mathbb{Z}$, $b \neq 0$, tồn tại duy nhất $q, r \in \mathbb{Z}$ sao cho $a = qb + r$, $0 \leq r < |b|$. Dùng Định lý 4.4, kiểm tra dạng tổng quát này của thuật toán với $b < 0$.

4.46. Cho $n \in \mathbb{Z}^+$, viết chương trình máy tính (hoặc phát triển một thuật toán) liệt kê các ước dương của n.

4.47. Tập $X \subseteq \mathbb{Z}^+$ là tập nhỏ nhất xác định bởi

1) $3 \in X$, và
2) Nếu $a, b \in X$, thì $a + b \in X$.

Chứng minh $X = \{3k \mid k \in \mathbb{Z}^+\}$, là tập các số nguyên dương chia hết cho 3.

4.48. Cho $n \in \mathbb{Z}^+$ với $n = r_k \cdot 10^k + \cdots + r_2 \cdot 10^2 + r_1 \cdot 10 + r_0$ (biểu diễn cơ số 10 của n). Chứng minh

a) $2 \mid n \Leftrightarrow 2 \mid r_0$
b) $4 \mid n \Leftrightarrow 4 \mid (r_1 \cdot 10 + r_0)$
c) $8 \mid n \Leftrightarrow 8 \mid (r_2 \cdot 10^2 + r_1 \cdot 10 + r_0)$

Phát biểu kết luận tổng quát từ các khẳng định trên.

4.4 Ước chung lớn nhất: thuật toán Euclid

Định nghĩa 4.3. *Cho a, b* $\in \mathbb{Z}$*. Số nguyên dương c gọi là ước chung của a và b nếu c* $\mid$ *a và c* $\mid$ *b.*

Định nghĩa 4.4. *Cho a, b* $\in \mathbb{Z}$*, trong đó a* $\neq 0$ *hoặc b* $\neq 0$*. Khi đó c* $\in \mathbb{Z}^+$ *gọi là ước chung lớn nhất của a, b nếu*

1) *c là ước chung của a, b, và*

2) *nếu d cũng là ước chung của a và b, thì d* $\mid$ *c.*

Định lý 4.5. *Cho hai số nguyên a, b không đồng thời bằng 0. Khi đó, có duy nhất một ước chung lớn nhất của a và b, ký hiệu* $\gcd(a, b)$*.*

Giải. Đặt $C = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\} \subseteq \mathbb{Z}^+$. Vì $C \neq \varnothing$, theo nguyên lý sắp tốt, tồn tại $c = \min C$. Ta sẽ chứng minh c là một ước chung lớn nhất của a và b.

Vì $c \in C$, nên $\exists x, y \in \mathbb{Z}, c = ax + by$.

a) Trước hết, ta chứng minh $c \mid a$. Giả sử ngược lại, $c \nmid a$. Theo thuật toán chia, $a = qc + r$, với $q, r \in \mathbb{Z}$ và $0 < r < c$. Khi đó

$$r = a - qc = a - q(ax + by) = a(1 - qx) + b(-qy),$$

nên $r \in C$. Mặt khác, $c = \min C$ nên $c \leq r$, mâu thuẫn! Do đó $c \mid a$. Lập luận tương tự, ta có $c \mid b$. Vậy c là một ước chung của a và b.

b) Giả $d \in \mathbb{Z}^+$ sao cho $d \mid a$ và $d \mid b$. Theo Định lý 4.2(f), $d \mid (ax + by)$, hay $d \mid c$.

Do đó c là một ước chung lớn nhất của a và b.

Cuối cùng, giả sử c' cũng là một ước chung lớn nhất của a và b. Vì c' là một ước chung của a và b, nên $c' \mid c$. Hoàn toàn tương tự, $c \mid c'$. Theo Định lý 4.2(b), và lưu ý $c, c' \in \mathbb{Z}^+$, suy ra $c = c'$.

Vậy hai số nguyên dương a, b có duy nhất một ước chung lớn nhất. □

$\gcd(a, 0) = |a|$, và $\gcd(a, b) = \gcd(b, a) = \gcd(|a|, |b|)$. Ở đây, ta không định nghĩa

$\gcd(0, 0)$. Ngoài ra, $\gcd(a, b)$ là một tổ hợp tuyến tính của a, b, tức là

$$\exists x, y \in \mathbb{Z},\ \gcd(a, b) = ax + by.$$

Định nghĩa 4.5. *Cho $a, b \in \mathbb{Z}$ với $a \neq 0$ hoặc $b \neq 0$. a, b gọi là nguyên tố cùng nhau nếu $\gcd(a, b) = 1$.*

Cho $a, b \in \mathbb{Z}^+$. Xét thuật toán chia a cho b: $a = qb + r$, với $0 \leq r < b$. Khi đó

$$\gcd(a, b) = \gcd(b, r) = \gcd(b, a \bmod b).$$

Định lý 4.6 (Thuật toán Euclid)**.** *Cho $a, b \in \mathbb{Z}^+$. Đặt $r_0 = a$, $r_1 = b$, và áp dụng thuật toán chia như sau*

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2, && 0 < r_2 < r_1\\
r_1 &= q_2 r_2 + r_3, && 0 < r_3 < r_2\\
r_2 &= q_3 r_3 + r_4, && 0 < r_4 < r_3\\
&\dots\\
r_{i-1} &= q_i r_i + r_{i+1}, && 0 < r_{i+1} < r_i\\
&\dots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n, && 0 < r_n < r_{n-1}\\
r_{n-1} &= q_n r_n.
\end{aligned}$$

Khi đó $\gcd(a, b) = r_n$, là phần dư khác không cuối cùng trong dãy phép chia.

Ví dụ 4.25. Tìm $\gcd(91, 287)$.

Giải.

$$\begin{aligned}
91 &= 0 \cdot 287 + 91\\
287 &= 3 \cdot 91 + 14\\
91 &= 6 \cdot 14 + 7\\
14 &= 2 \cdot 7 + 0
\end{aligned}$$

nên $\gcd(91, 287) = 7$.

Cách 1: Dùng hàm `gcd` của thư viện `math` hoặc `igcd` của `sympy`

```
import math
math.gcd(91, 287)
```

hoặc

```
from sympy import *
igcd(91, 287)
```

Cách 2: Đệ quy

```
def gcd(a, b):
    if b == 0:
        return a
    return gcd(b, a % b)
```

Cách 3: Phương pháp quy hoạch động cho hệ thức đệ quy

$$r_{i+1} = r_{i-1} \bmod r_i, \ \ i = 1, 2, \dots, \quad \text{với } r_0 = a, r_1 = b,$$

đến khi $r_{n+1} = 0$.

```
def gcd(a, b):
    while b != 0:
        r = a % b
        a = b
        b = r
    return a
```

hoặc

```
def gcd(a, b):
    while b != 0:
        a, b = b, a % b
    return a
```

□

Ví dụ 4.26. Với $n \in \mathbb{Z}^+$, chứng minh $8n + 3$ và $5n + 2$ nguyên tố cùng nhau.

Giải.

$$\begin{aligned}
8n + 3 &= 1 \cdot (5n + 2) + (3n + 1) \\
5n + 2 &= 1 \cdot (3n + 1) + (2n + 1) \\
3n + 1 &= 1 \cdot (2n + 1) + n \\
2n + 1 &= 2 \cdot n + 1
\end{aligned}$$

$$n = n \cdot 1$$

nên $\gcd(8n + 3, 5n + 2) = 1$.

```python
from sympy import *
n = symbols('n')
gcd(8*n + 3, 5*n + 2)
```

□

Gọi x_i, y_i là các hệ số của biểu diễn tuyến tính r_i theo a và b, tức là $r_i = ax_i + by_i$. Thay biểu diễn này vào phép chia ở trên:

$$ax_{i-1} + by_{i-1} = q_i(ax_i + by_i) + (ax_{i+1} + by_{i+1}),$$

rồi cân bằng hệ số của a và b, được $x_{i-1} = q_i x_i + x_{i+1}$ và $y_{i-1} = q_i y_i + y_{i+1}$. Ta có hệ thức đệ quy

$$\begin{aligned} x_{i+1} &= x_{i-1} - q_i x_i, \quad \text{và} \\ y_{i+1} &= y_{i-1} - q_i y_i, \end{aligned}$$

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

Khi thuật toán Euclid dừng, $r_n = ax_n + by_n$. Đặt $x_n = x, y_n = y$, ta có biểu diễn

$$\gcd(a, b) = ax + by,$$

gọi là thuật toán Euclid mở rộng.

Ví dụ 4.27. Tìm khai triển Euclid mở rộng của 91 và 287.

Giải. $\gcd(91, 297) = 7$, và biểu diễn tuyến tính $7 = 19 \cdot 91 + (-6)287$. Quá trình tính được thể hiện trong bảng sau

i	a	b	q_i	x_i	y_i
0	91	287		1	0
1	287	91	0	0	1
2	91	14	3	1	0
3	14	**7**	6	−3	1
4	7	0		**19**	**−6**

Cách 1: dùng gói lệnh

```
from sympy import *
gcdex(91, 287)
```

kết quả $(19, -6, 7)$ cho ta hệ thức $19 \cdot 91 + (-6)287 = 7$

Cách 2: lập trình

```
def gcdex(a, b):
    x0, y0 = 1, 0
    x1, y1 = 0, 1
    while b != 0:
        q = a // b
        a, b = b, a % b
        x = x0 - x1 * q
        y = y0 - y1 * q
        x0, y0 = x1, y1
        x1, y1 = x, y
    return x0, y0, a
```

□

Định lý 4.7. *Với $a, b, c \in \mathbb{Z}$, $a \neq 0$ hoặc $b \neq 0$, phương trình Diophant*[*] *$ax + by = c$ có nghiệm nguyên khi và chỉ khi* $\gcd(a, b) \mid c$.

Đặc biệt, với $c = 1$

$$\gcd(a, b) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z},\ ax + by = 1.$$

Hai số nguyên liên tiếp $a, a+1$ nguyên tố cùng nhau, vì $a(-1) + (a+1) \cdot 1 = 1$.

Định nghĩa 4.6. *Cho $a, b \in \mathbb{Z}^+$. Số $c \in \mathbb{Z}^+$ gọi là một bội chung của a, b nếu c là bội của cả a và b. Số nhỏ nhất trong các bội chung của a, b gọi là bội chung nhỏ nhất của a, b, ký hiệu* $\operatorname{lcm}(a, b)$.

Ví dụ 4.28. Tìm $\operatorname{lcm}(6, 15)$.

[*] Diophantus, thế kỷ 3, nhà toán học Hy Lạp

Giải.

$$
\begin{aligned}
A &= \{a \in \mathbb{Z}^+ : 6 \mid a\} = \{6, 12, 18, 24, 30, 36, ...\} \\
B &= \{a \in \mathbb{Z}^+ : 15 \mid a\} = \{15, 30, 45, 60, 75, ...\} \\
\Rightarrow A \cap B &= \{a \in Z^+ : 6 \mid a \wedge 15 \mid a\} = \{30, 60, ...\} \\
\Rightarrow \operatorname{lcm}(6, 15) &= \min A \cap B = 30.
\end{aligned}
$$

□

Định lý 4.8. *Cho* $a, b \in \mathbb{Z}^+$ *và* $c = \operatorname{lcm}(a, b)$*. Nếu d là một ước chung của a và b, thì* $c \mid d$*.*

Định lý 4.9. $\forall a, b \in \mathbb{Z}^+,\ ab = \operatorname{lcm}(a, b) \cdot \gcd(a, b)$*.*

Ví dụ 4.29. a) Cho $a, b \in \mathbb{Z}^+$.

i) Nếu a, b nguyên tố cùng nhau, thì $\operatorname{lcm}(a, b) = ab$.

ii) Nếu $a \mid b$ thì $\gcd(a, b) = a$, $\operatorname{lcm}(a, b) = b$.

b) $\gcd(456, 148) = 24 \Rightarrow \operatorname{lcm}(456, 168) = \dfrac{456 \cdot 168}{24} = 3\,192.$

```python
from sympy import *
ilcm(456, 168)
```

Hai ví dụ sau góp phần đánh giá tốc độ của thuật toán Euclid

Ví dụ 4.30. Chứng minh $F_n > \varphi^{n-2}$, $\forall n \geq 3$ trong đó[*] $\varphi = \dfrac{1 + \sqrt{5}}{2} \approx 1.61803$.

Giải. Trước hết nhận xét φ là nghiệm của phương trình $x^2 - x - 1 = 0$, suy ra $\varphi^2 = \varphi + 1$.

Ký hiệu $S(n) : F_n > \varphi^{n-2}$.

- $S(3)$: $F_3 > \varphi$, hay $2 > \varphi$, đúng; và

  $S(4)$: $F_4 > \varphi^2$, hay $3 > \varphi + 1$, đúng.

[*] φ gọi là tỷ lệ vàng

- Giả sử với $n \geq 4$, $S(k)$ đúng $\forall k = 3, \ldots, n$, tức là $F_k > \varphi^{k-2}$. Khi đó

$$\begin{aligned} F_{n+1} &= F_n + F_{n-1} > \varphi^{n-2} + \varphi^{n-3} = && \text{áp dụng } S(n), S(n-1) \text{ vì } 3 \leq n, n-1 \leq n \\ &= \varphi^{n-3}\left(\varphi + 1\right) = \varphi^{n-3} \cdot \varphi^2 = \varphi^{n-1} \end{aligned}$$

tức là $S(n+1)$ đúng.

Vậy $S(n)$, $\forall n \geq 3$. □

Ví dụ 4.31 (Định lý Lamé)**.** [*]Cho $a, b \in \mathbb{Z}^+$, $a, b \geq 2$. Số phép chia dùng trong thuật toán Euclid để tìm ước chung lớn nhất của a và b không quá 5 lần số chữ số của b.

Giải. Đặt $r_0 = a$ và $r_1 = b$, ta có

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, && 0 < r_2 < r_1 \\ r_1 &= r_2 q_2 + r_3, && 0 < r_3 < r_2 \\ r_2 &= r_3 q_3 + r_4, && 0 < r_4 < r_3 \\ &\cdots\cdots\cdots\cdots\cdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_n. \end{aligned}$$

Khi đó, $\gcd(a, b) = r_n$, là phần dư khác không cuối cùng, và thuật toán thực hiện n phép chia.

Ta thấy, $q_i \geq 1$, $\forall i = \overline{1, n}$. Riêng $q_n \geq 2$, vì $r_{n-1} = r_n q_n$ mà $0 < r_n < r_{n-1}$. Như vậy

$$\begin{aligned} r_n > 0 \Rightarrow r_n &\geq 1 = F_2 \\ r_{n-1} = r_n q_n &\geq 1 \cdot 2 = 2 = F_3 \\ r_{n-2} = r_{n-1} q_{n-1} + r_n &\geq F_3 \cdot 1 + F_2 = F_4 \\ r_{n-3} = r_{n-2} q_{n-2} + r_{n-1} &\geq F_4 \cdot 1 + F_3 = F_5 \\ &\cdots\cdots\cdots\cdots\cdots \\ r_2 = r_3 q_3 + r_4 &\geq F_{n-1} \cdot 1 + F_{n-2} = F_n \\ b = r_1 = r_2 q_2 + r_3 &\geq F_n \cdot 1 + F_{n-1} = F_{n+1} \end{aligned}$$

[*]Gabriel Lamé, 1795–1870, nhà toán học Pháp

Dẫn đến

$$\begin{aligned} &b \geq F_{n+1} > \alpha^{(n+1)-2} = \alpha^{n-1} \\ \Rightarrow\ &n - 1 < \log_\alpha b = \log_\alpha 10 \cdot \log_{10} b = 4.784971 \log_{10} b < 5\log_{10} b. \end{aligned}$$

Nếu b có k chữ số, thì $10^{k-1} \leq b < 10^k$, nên $\log_{10} b < k$. Do đó $n - 1 < 5k$, hay $n \leq 5k$, tức là số phép chia trong thuật toán Euclid không quá 5 lần số chữ số của b. □

Bài tập 4.4

4.49. Với $a, b \in \mathbb{Z}^+$, tìm $\gcd(a, b)$ và biểu diễn nó bởi tổ hợp tuyến tính của a, b.

a) 231, 1820 b) 1369, 2597 c) 2689, 4001

4.50. Với $a, b \in \mathbb{Z}^+$ và $x, y \in \mathbb{Z}$, có thể nói gì về $\gcd(a, b)$ nếu

a) $ax + by = 2$ b) $ax + by = 3$ c) $ax + by = 4$ d) $ax + by = 6$

4.51. Với $a, b \in \mathbb{Z}^+$ và $d = \gcd(a, b)$, chứng minh $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

4.52. Với $a, b, n \in \mathbb{Z}^+$, chứng minh $\gcd(na, nb) = n \cdot \gcd(a, b)$.

4.53. Cho $a, b, c \in \mathbb{Z}^+$ với $c = \gcd(a, b)$. Chứng minh $c^2 \mid ab$.

4.54. Cho $n \in \mathbb{Z}^+$.

a) Chứng minh $\gcd(n, n + 1) = 1$ hoặc 2.

b) $\gcd(n, n + 3)$ có thể bằng bao nhiêu? Và $\gcd(n, n + 4)$?

c) Nếu $k \in \mathbb{Z}^+$, có thể nói gì về $\gcd(n, n + k)$?

4.55. Với $a, b, c, d \in \mathbb{Z}^+$, chứng minh nếu $d = a + bc$, thì $\gcd(b, d) = \gcd(a, b)$.

4.56. Cho $a, b, c \in \mathbb{Z}^+$ với $\gcd(a, b) = 1$. Nếu $a \mid c$ và $b \mid c$, chứng minh $ab \mid c$. Khẳng định còn đúng không nếu $\gcd(a, b) \neq 1$?

4.57. Cho $a, b \in \mathbb{Z}$ trong đó ít nhất một số khác 0.

a) Dùng lượng từ, phát biểu lại định nghĩa $c = \gcd(a, b)$.

b) Với $c \in \mathbb{Z}^+$, dùng kết quả ở ý (a) để chỉ ra khi nào $c \neq \gcd(a, b)$.

4.58. Nếu a, b nguyên tố cùng nhau và $a > b$, chứng minh $\gcd(a - b, a + b) = 1$ hoặc 2.

4.59. Cho $a, b, c \in \mathbb{Z}^+$ với $\gcd(a, b) = 1$. Nếu $a \mid bc$, chứng minh $a \mid c$.

4.60. Cho $a, b \in \mathbb{Z}^+$ với $a \geq b$. Chứng minh $\gcd(a, b) = \gcd(a - b, b)$.

4.61. Chứng minh $\gcd(5n + 3, 7n + 4) = 1,\ \forall n \in \mathbb{Z}^+$.

4.62. Cho $a, b \in \mathbb{Z}^+$. Chứng minh tồn tại $c, d \in \mathbb{Z}^+$ sao cho $cd = a$ và $\gcd(c, d) = b$ khi và chỉ khi $b^2 \mid a$.

4.63. Tìm các giá trị của $c \in \mathbb{Z}^+$, $10 < c < 20$, để phương trình Diophant $84x + 990y = c$ vô nghiệm. Tìm nghiệm của phương trình với các giá trị còn lại của c.

4.64. Cho $a, b \in \mathbb{Z}^+$ với $a = 630$, $\gcd(a, b) = 105$ và $\operatorname{lcm}(a, b) = 242\,550$. Tìm b.

4.65. Với các cặp a, b trong 4.49, tìm $\operatorname{lcm}(a, b)$.

4.66. Với $n \in \mathbb{Z}^+$, tìm $\gcd(n, n + 1)$ và $\operatorname{lcm}(n, n + 1)$.

4.67. Chứng minh $\operatorname{lcm}(na, nb) = n \cdot \operatorname{lcm}(a, b),\ \forall n, a, b \in \mathbb{Z}^+$.

4.5 Định lý cơ bản của số học

Bổ đề 4.2. *Cho $a, b \in \mathbb{Z}$ và số nguyên tố p. Nếu $p \mid (ab)$ thì $p \mid a$ hoặc $p \mid b$.*
Tổng quát, với $n \in \mathbb{Z}^+$, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, nếu $p \mid (a_1 a_2 \cdots a_n)$ thì $\exists i \in \{1, 2, \ldots, n\},\ p \mid a_i$.

Ví dụ 4.32. Chứng minh $\sqrt{2}$ là số vô tỷ.*

*Aristotle, 384–322 trước công nguyên, nhà triết học Hy Lạp

Giải. Giả sử ngược lại, $\sqrt{2} = \dfrac{a}{b}$, với $a, b \in \mathbb{Z}^+$ và $\gcd(a, b) = 1$. Khi đó $2 = \dfrac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow 2 \mid a^2 \Rightarrow 2 \mid (a \cdot a) \Rightarrow 2 \mid a$. Vì thế, $\exists c \in \mathbb{Z}$, $a = 2c$, nên $2b^2 = a^2 = (2c)^2 = 4c^2 \Rightarrow b^2 = 2c^2 \Rightarrow 2 \mid b^2 \Rightarrow 2 \mid b$. Như vậy, 2 là một ước chung của a, b, mà $\gcd(a, b) = 1$, nên $2 \leq 1$, mâu thuẫn! Vậy $\sqrt{2}$ là số vô tỷ.

□

Định lý 4.10 (Định lý cơ bản của số học)**.** *Mọi số nguyên $n > 1$ đều phân tích được thành tích các số nguyên tố, một cách duy nhất theo nghĩa chỉ sai khác thứ tự các thừa số nguyên tố. (Ở đây, một số nguyên tố có phân tích chỉ gồm một thừa số.)*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

trong đó $k \in \mathbb{Z}^+$, $p_1 < p_2 < \ldots < p_k$ là các số nguyên tố, và $e_1, e_2, \ldots, e_k \in \mathbb{Z}^+$.

Ví dụ 4.33. Tìm phân tích nguyên tố của 980 220.

Giải.

$$\begin{aligned} 980\,220 &= 2^1 \cdot 490\,110 = 2^2 \cdot 245\,055 = 2^2 \cdot 3^1 \cdot 81\,685 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 16\,337 \\ &= 2^2 \cdot 3^1 \cdot 5^1 \cdot 17^1 \cdot 961 = 2^2 \cdot 3^1 \cdot 5^1 \cdot 17^1 \cdot 31^2. \end{aligned}$$

Cách 1:

```
from sympy import *
factorint(980220)   # {2: 2, 3: 1, 5: 1, 17: 1, 31: 2}
```

Cách 2:

```
def factorint(n):
    i = 2
    f = {}
    while n > 1:
        while n % i != 0:
            i += 1
        e = 0
        while n % i == 0:
            n //= i
            e += 1
```

```
            f[i] = e
    return f
```

□

Ví dụ 4.34. a) Nếu n có phân tích nguyên tố $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, thì nó có bao nhiêu ước dương?

b) Số $n = 29\,338\,848\,000 = 2^8 3^5 5^3 7^3 11$ có bao nhiêu

i) ước dương là bội của 360? ii) ước là số chính phương?

Giải. a) Mỗi ước dương của n có dạng $m = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, trong đó $0 \le f_i \le e_i$, $\forall i = \overline{1, k}$. Theo quy tắc nhân, số ước dương của n là $(e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$.

b) Mỗi ước dương của $n = 2^8 3^5 5^3 7^3 11$ có dạng $m = 2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4} 11^{e_5}$, trong đó $0 \le e_1 \le 8$, $0 \le e_2 \le 5$, $0 \le e_3 \le 3$, $0 \le e_4 \le 3$ và $0 \le e_5 \le 1$.

i) Để m là bội của $360 = 2^3 3^2 5$, ta cần thêm điều kiện $e_1 \ge 3$, $e_2 \ge 2$ và $e_3 \ge 1$. Số ước dương của n là bội của 360 là

$$[(8 - 3) + 1]\,[(5 - 2) + 1]\,[(3 - 1) + 1]\,[(3 - 0) + 1]\,[(1 - 0) + 1] = 576.$$

ii) Để m là số chính phương, $\forall i = \overline{1, 5}$, e_i chẵn. Ta có

e_i	Cách chọn	Số cách chọn
e_1	0, 2, 4, 6, 8	5
e_2	0, 2, 4	3
Mỗi e_3, e_4	0, 2	2
e_5	0	1

Theo quy tắc nhân, số ước chính phương của n là $5 \cdot 3 \cdot 2 \cdot 2 \cdot 1 = 60$.

□

Cho $m, n \in \mathbb{Z}^+$ các phân tích nguyên tố $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ và $n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, với $k \in \mathbb{Z}^+$, $p_1 < p_2 < \ldots < p_k$ là các số nguyên tố, và $e_i, f_i \in \mathbb{N}$, $i = \overline{1, k}$. Đặt

$$a_i = \min\{e_i, f_i\},\ b_i = \max\{e_i, f_i\},\ i = \overline{1, k},$$

thì
$$\gcd(m,n) = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \quad \text{và} \quad \operatorname{lcm}(m,n) = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}.$$

Ví dụ 4.35. Cho $m = 491\,891\,400 = 2^3 3^3 5^2 7^2 11^1 13^2$ và $n = 1\,138\,845\,708 = 2^2 3^2 7^1 11^2 13^3 17^1$. Tìm ước chung lớn nhất và bội chung nhỏ nhất của m và n.

Giải. Viết lại $m = 2^3 3^3 5^2 7^2 11^1 13^2 \underline{17^0}$ và $n = 2^2 3^2 \underline{5^0} 7^1 11^2 13^3 17^1$. Khi đó
$$\gcd(m,n) = 2^2 3^2 5^0 7^1 11^1 13^2 17^0 = 468\,468$$
$$\operatorname{lcm}(m,n) = 2^3 3^3 5^2 7^2 11^2 13^3 17^1 = 1\,195\,787\,993\,400.$$
□

Ví dụ 4.36. Chứng minh tích của ba số nguyên dương liên tiếp không là số chính phương.

Giải. Giả sử ngược lại, $\exists m, n \in \mathbb{Z}^+,\ m(m+1)(m+2) = n^2$. Xét ước nguyên tố bất kỳ p của $m+1$. Vì $gcd(m, m+1) = 1 = \gcd(m+1, m+2)$, nên $p \not| m$ và $p \not| (m+2)$. Do đó, trong phân tích nguyên tố của $m(m+1)(m+2) = n^2$ và $m+1$, lũy thừa của p bằng nhau. Nhưng n^2 là số chính phương, nên theo định lý cơ bản của số học, lũy thừa đó của p là số chẵn. Vậy $m+1$ là số chính phương, vì thế $m(m+2)$ là số chính phương. Nhưng $m^2 < m(m+2) = m^2 + 2m < (m+1)^2$, nên $m(m+2)$ không là số chính phương, mâu thuẫn! Do đó tích của ba số nguyên dương liên tiếp không là số chính phương. □

Bài tập 4.5

4.68. Viết các số nguyên sau thành tích các số nguyên tố $p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, trong đó $n_i > 0 \forall i = \overline{1,k}$ và $p_1 < p_2 < \ldots < p_k$.

a) 148 500 b) 7 114 800 c) 7 882 875

4.69. Tìm ước chung lớn nhất và bội chung nhỏ nhất của các cặp số nguyên trong 4.68.

4.70. Cho $k \in \mathbb{Z}^+$ và $p_1, p_2, \ldots, p_k$ là các số nguyên tố phân biệt. Nếu $n \in \mathbb{Z}^+$ có phân tích nguyên tố $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, hãy tìm phân tích nguyên tố của (a) n^2, và (b) n^3.

4.71. Chứng minh $\sqrt{p}$ là số vô tỷ với số nguyên tố p bất kỳ.

4.72. Tìm số ước dương của mỗi số nguyên trong 4.68.

4.73. a) Có bao nhiêu ước dương của $n = 2^{14}3^{9}5^{8}7^{10}11^{3}13^{5}37^{10}$?

b) Trong các ước dương ở ý (a), có bao nhiêu số

i) chia hết cho $2^{3}3^{4}5^{7}11^{2}37^{2}$?

ii) chia hết cho 1 166 400 000?

iii) chính phương?

iv) chính phương và chia hết cho $2^{2}3^{4}5^{2}11^{2}$?

v) lập phương?

vi) lập phương là bội của $2^{10}3^{9}5^{2}7^{5}11^{2}13^{2}37^{2}$?

vii) vừa chính phương vừa lập phương?

4.74. Cho $m, n \in \mathbb{Z}^{+}$ với $mn = 2^{4}3^{4}5^{3}7^{1}11^{3}13^{1}$ và $\mathrm{lcm}(m, n) = 2^{2}3^{3}5^{2}7^{1}11^{2}13^{1}$. Tìm $\gcd(m, n)$.

4.75. Có bao nhiêu số nguyên dương n là ước của $100\,137n + 248\,396\,544$?

4.76. Cho $a \in \mathbb{Z}^{+}$. Tìm a nhỏ nhất sao cho $2a$ là số chính phương và $3a$ là số lập phương?

4.77. a) Cho $a \in \mathbb{Z}^{+}$. Chứng minh hoặc bác bỏ

i) Nếu $10 \mid a^2$ thì $10 \mid a$.

ii) Nếu $4 \mid a^2$ thì $4 \mid a$.

b) Tổng quát hóa các kết quả ở ý (a).

4.78. Cho $a, b, c \in \{0, 1, 2, \dots, 9\}$ trong đó có ít nhất một số khác 0. Chứng minh số có sáu chữ số $abcabc$ chia hết cho ít nhất ba số nguyên tố phân biệt.

4.79. Tìm số chính phương nhỏ nhất chia hết cho 7!

4.80. Với $n \in \mathbb{Z}^{+}$, chứng minh n là số chính phương khi và chỉ khi n có một số lẻ các ước dương.

4.81. Tìm số nguyên dương nhỏ nhất n sao cho $1260n$ là số lập phương.

4.82. a) Cho $n = 88\,200$. Có bao nhiêu cách phân tích n thành ab trong đó $1 < a \le b < n$ và $\gcd(a, b) = 1$.

b) Trả lời ý (a) với $n = 970\,200$.

c) Tổng quát hóa kết quả ở ý (a) và (b).

4.83. Khi nào số nguyên dương n có đúng

a) hai ước dương?

b) ba ước dương?

c) bốn ước dương?

d) năm ước dương?

4.84. Cho $n \in \mathbb{Z}^+$. Ta nói n là số *hoàn hảo* nếu $2n$ bằng tổng các ước dương của n. Ví dụ, 6 là số hoàn hảo vì $2 \cdot 6 = 1 + 2 + 3 + 6$.

a) Chỉ ra 28 và 496 là các số hoàn hảo.

b) Nếu $m \in \mathbb{Z}^+$ và $2^m - 1$ nguyên tố, chứng minh $2^{m-1}(2^m - 1)$ là số hoàn hảo. [dùng ý (e) trong 4.1]

4.6 Biểu diễn số nguyên và thuật toán

4.6.1 Biểu diễn số nguyên

Định lý 4.11 (Biểu diễn số nguyên)**.** *Cho $b \in \mathbb{Z}^+$, $b > 1$. Khi đó mọi số $n \in \mathbb{Z}^+$ biểu diễn duy nhất dưới dạng:*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \tag{4.5}$$

trong đó $0 \le a_i < b\ \forall i = \overline{0, k},\ a_k \neq 0$.

Ký hiệu $n = (a_k a_{k-1} \dots a_1 a_0)_b$ gọi là khai triển n theo cơ số b. Khai triển theo cơ số 2 gọi là khai triển nhị phân, hay xâu bit. Hệ cơ số 16, hay thập lục phân, gồm các chữ số 0, 1, 2,. . . , 9 và các chữ A, B, C, D, E, F tương ứng với giá trị 10, 11, 12, 13, 14, 15.

Với $b = 10$, hệ thập phân không cần ghi cơ số, chẳng hạn

$$965_{10} = 9 \cdot 10^2 + 6 \cdot 10 + 5 = 965.$$

Ví dụ 4.37.

$$\begin{aligned}
245_8 &= 2 \cdot 8^2 + 4 \cdot 8 + 5 = 165 \\
1\,0101\,1111_2 &= 2^8 + 2^6 + 2^4 + 2^3 + 2^2 + 2 + 1 = 351 \\
2AE0B_{16} &= 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 11 = 175\,627
\end{aligned}$$

Tìm giá trị n của biểu diễn $(\mathbf{a_k a_{k-1} \dots a_1 a_0})_\mathbf{b}$

Biến đổi

$$\begin{aligned} n = n_0 &= b(a_k b^{k-1} + a_{k-1} b^{k-2} + \cdots + a_2 b + a_1) + a_0 = bn_1 + a_0 \\ n_1 &= b(a_k b^{k-2} + a_{k-1} b^{k-3} + \cdots + a_3 b + a_2) + a_1 = bn_2 + a_1 \\ n_2 &= b(a_k b^{k-3} + a_{k-1} b^{k-4} + \cdots + a_4 b + a_3) + a_2 = bn_3 + a_2, \dots \end{aligned}$$

trong đó $n_i = a_k b^{k-i} + a_{k-1} b^{k-i-1} + \cdots + a_{i+1} b + a_i$ với $i = \overline{0, k}$. Khi đó, ta có công thức Horner*

$$\begin{aligned} n_k &= a_k, \text{ và} \\ n_i &= bn_{i+1} + a_i, \ \forall i = \overline{k-1 \downarrow 0}. \end{aligned} \tag{4.6}$$

Ở đây $n = n_0$.

Ví dụ 4.38. Tính $30\,071_8$.

Giải.

$$\begin{aligned} n_4 &= 3 \\ n_3 &= 8 \cdot 3 + 0 = 24 \\ n_2 &= 8 \cdot 24 + 0 = 192 \\ n_1 &= 8 \cdot 192 + 7 = 1\,543 \\ n = n_0 &= 8 \cdot 1\,543 + 1 = 12\,345 \end{aligned}$$

nên $30\,071_8 = 12\,345$.

```python
a = [1, 7, 0, 0, 3]
b = 8

n = 0
k = len(a)   # hơn k lý
    thuyết 1 đơn vị
for i in range(k-1, -1,
   -1):
    n = n * b + a[i]

n
```

□

Tìm biểu diễn $(\mathbf{a_k r_{a-1} \dots a_1 a_0})_\mathbf{b}$ của n

$$a_i = n_i \bmod b, \ n_{i+1} = n_i \operatorname{div} b. \tag{4.7}$$

*William George Horner, 1786–1837, nhà toán học Anh trong đó $n_0 = n$, và quá trình thực hiện đến khi $n_{k+1} = 0$. Khi đó biểu diễn của n trong cơ số b là $n = (a_k r_{a-1} \dots a_1 a_0)_b$.

Ví dụ 4.39. Tìm khai triển của 6 137 theo cơ số 8.

Giải. Thực hiện liên tiếp các phép chia cho 8 đến khi thương bằng 0

$$\begin{array}{rcrcccc} 6\,137 & = & 767 & \cdot & 8 & + & \mathbf{1} \\ 767 & = & 95 & \cdot & 8 & + & \mathbf{7} \\ 95 & = & 11 & \cdot & 8 & + & \mathbf{7} \\ 11 & = & 1 & \cdot & 8 & + & \mathbf{3} \\ 1 & = & \boxed{0} & \cdot & 8 & + & \mathbf{1} \end{array}$$

```python
n, b = 6137, 8

a = []
while n != 0:
    a.append(n % b)
    n //= b

a  # → [1, 7, 7, 3, 1]
```

Ta được $6\,137 = 13\,771_8$. □

4.6.2 Phép cộng số nguyên cùng cơ số

Giả sử $n = \left(a_k a_{k-1} \dots a_1 a_0\right)_b$, $m = \left(b_k b_{k-1} \dots b_1 b_0\right)_b$. Khi cộng hàng thứ i, ta phải cộng cả phần nhớ r_{i-1} ở hàng $i - 1$, rồi ghi ra giá trị s_i cộng được ở hàng này kèm theo phần nhớ r_i:

$$\begin{aligned} s_i &= \left(a_i + b_i + r_{i-1}\right) \bmod b \\ r_i &= \left\lfloor \frac{a_i + b_i + r_{i-1}}{b} \right\rfloor \\ i &= \overline{0, k} \end{aligned} \tag{4.8}$$

trong đó $r_{-1} = 0$. Đặt $s_{k+1} = r_k$, ta có

$$n + m = (s_{k+1} s_k \dots s_1 s_0)_b.$$

Ví dụ 4.40. Tính $7\,246_8 + 4\,735_8$.

Giải.

$$\begin{array}{ccccc} & 7 & 2 & 4 & 6 \\ & 4 & 7 & 3 & 5 \\ \hline 1 & 4_1 & 2_1 & 0_1 & 3_1 \end{array}$$

Ta được $7\,246_8 + 4\,735_8 = 12\,103_8$.

```
a = [6, 4, 2, 7]
b = [5, 3, 7, 4]
base = 8

k = len(a)   # = len(b), hơn k lý thuyết 1 đơn vị
r = 0
s = [0] * (k+1)
for i in range(k):
    t = a[i] + b[i] + r
    s[i] = t % base
    r = t // base
s[k] = r

s  # → [3, 0, 2, 4, 1]
```

□

4.6.3 Phép nhân số nguyên cùng cơ số

Bổ đề 4.3. *Trong cơ số b, biểu diễn của nb^i thu được bằng cách thêm i chữ số 0 vào bên phải biểu diễn của b.*

Chứng minh. Giả sử $n = \left(a_k a_{k-1} \dots a_1 a_0\right)_b$. Ta có

$$\begin{aligned} n &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \\ \Rightarrow nb^i &= a_k b^{k+i} + a_{k-1} b^{k+i-1} + \cdots + a_1 b^{i+1} + a_0 b^i \\ &= a_k b^{k+i} + a_{k-1} b^{k+i-1} + \cdots + a_1 b^{i+1} + a_0 b^i + 0b^{i-1} + \cdots + 0b + 0 \\ &= \Big(a_k a_{k-1} \dots a_1 a_0 \underbrace{00 \dots 0}_{i}\Big)_b \end{aligned}$$

□

Xét $n = (a_k \dots a_1 a_0)_b$ và $m = (b_l \dots b_1 b_0)_b = \sum_{i=0}^{l} b_i b^i$. Ta có

$$nm = n \sum_{i=0}^{k} b_i b^i = \sum_{i=0}^{k} (nb_i)\, b^i$$

trong đó nb_i có dạng $\left(p^i_{k+1} p^i_k \dots p^i_0\right)_b$. Để tính hàng $j = \overline{0, k}$, ta nhân hàng j của n với b_i, thêm phần nhớ r^i_{j-1} ở hàng $j-1$; sau đó xác định giá trị p^i_j ở hàng này và lưu phần nhớ r_j^i:

$$
\begin{aligned}
p_j^i &= \left(a_j b_i + r_{j-1}^i\right) \bmod b \\
r_j^i &= \left(a_j b_i + r_{j-1}^i\right) \operatorname{div} b
\end{aligned}
$$

và $p_{k+1}^i = r_k^i$ (lưu ý $r_{-1}^i = 0$).

Gọi $\left(s_{k+i+1}^i s_{k+i}^i \dots s_0^i\right)_b$ là tổng thu được sau bước ứng với b_i. Khi đó

$$\left(s_{k+i+1}^i s_{k+i}^i \dots s_0^i\right)_b = \left(s_{k+i}^{i-1} s_{k+i-1}^{i-1} \dots s_0^{i-1}\right)_b + \left(p_{k+1}^i p_k^i \dots p_0^i \underbrace{00\dots0}_{i}\right)_b$$

Ta có i chữ số đầu giữ nguyên: $\forall j = \overline{0, i-1}$

$$s_j^i = s_j^{i-1}$$

Với $k+1$ chữ số tiếp theo: $\forall j = \overline{i, k+i}$

$$
\begin{aligned}
s_j^i &= \left(s_j^{i-1} + p_{j-i}^{i-1} + R_{j-1}^i\right) \bmod b \\
R_j^i &= \left(s_j^{i-1} + p_{j-i}^{i-1} + R_{j-1}^i\right) \operatorname{div} b
\end{aligned}
$$

và đặt $s_{k+i+1}^i = p_{k+1}^i + R_{k+i}^i = r_k^i + R_{k+i}^i$.

Ví dụ 4.41. Tính $342_5 \times 4\,213_5$.

Giải.

$$
\begin{array}{ccccccc}
 & & & & 3 & 4 & 2 \\
 & & & 4 & 1 & 2 & 3 \\ \cline{4-7}
 & & & 2 & 1_2 & 3_2 & \mathbf{1}_1 \\
 & & 1 & 2_1 & 3_1 & 4_0 & \\ \cline{3-6}
 & & 2 & 0_1 & 0_1 & \mathbf{2}_1 & \\
 & 0 & 3_0 & 4_0 & 2_0 & & \\ \cline{2-5}
 & 1 & 0_1 & 4_0 & \mathbf{2}_0 & & \\
3 & 0_3 & 2_3 & 3_1 & & & \\ \cline{1-4}
\mathbf{3} & \mathbf{1}_0 & \mathbf{3}_0 & \mathbf{2}_1 & & &
\end{array}
$$

Ta được $342_5 \times 4\,213_5 = 3\,132\,221_5$.

```
a = [2, 4, 3]
b = [3, 2, 1, 4]
base = 5
```

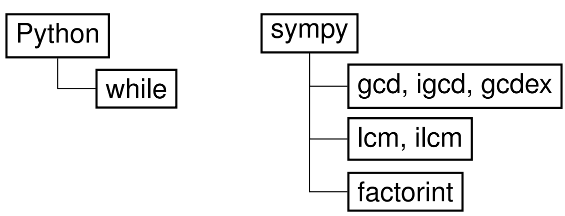
```
k = len(a)   # hơn k lý thuyết 1 đơn vị
l = len(b)   # ... l ..................

s = [0] * (k+l)
for i in range(l):
    r = R = 0
    for j in range(k):
        t = a[j] * b[i] + r
        p = t % base
        r = t // base
        t = s[i+j] + p + R
        s[i+j] = t % base
        R = t // base
    s[k+i] = r + R

s  # → [1, 2, 2, 2, 3, 1, 3]
```

□

4.7 Tóm tắt Python



Bài tập bổ sung

4.85. Cho $a, d \in \mathbb{Z}$, $n \in \mathbb{Z}^+$. Nêu công thức hiện của tổng $a+(a+d)+(a+2d)+\cdots+(a+(n-1)d)$. Chứng minh công thức bằng phương pháp quy nạp.

4.86. Xét năm đẳng thức

$$
\begin{aligned}
&\textbf{1)} & 1 &= 1 \\
&\textbf{2)} & 1-4 &= -(1+2) \\
&\textbf{3)} & 1-4+9 &= 1+2+3
\end{aligned}
$$

$$\begin{aligned} \textbf{4)} \quad 1 - 4 + 9 - 16 &= -(1 + 2 + 3 + 4) \\ \textbf{5)} \quad 1 - 4 + 9 - 16 + 25 &= 1 + 2 + 3 + 4 + 5 \end{aligned}$$

Hãy dự đoán và chứng minh công thức tổng quát.

4.87. Với $n \in \mathbb{Z}^+$, chứng minh

a) $5 \mid (n^5 - n)$

b) $6 \mid (n^3 + 5n)$

4.88. Với $n \in \mathbb{Z}^+$, đặt $S(n)$ là khẳng định mở: $n^2 + n + 41$ nguyên tố.

a) Chỉ ra $S(n)$ đúng $\forall n = \overline{1, n}$.

b) Với mọi $n \in \mathbb{Z}^+$, $S(n)$ kéo theo $S(n + 1)$ có đúng không?

4.89. Với $n \in \mathbb{Z}^+$, định nghĩa tổng s_n bởi công thức

$$s_n = \frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n-1}{n!} + \frac{n}{(n+1)!}$$

a) Tính s_n, $n = \overline{1, 6}$.

b) Dự đoán công thức hiện của s_n và chứng minh công thức đó bằng quy nạp.

4.90. Với $n \in \mathbb{N}$, chứng minh

a) $2^{2n+1} + 1$ chia hết cho 3.

b) $n^3 + (n + 1)^3 + (n + 2)^3$ chia hết cho 9.

4.91. Cho $n \in \mathbb{Z}^+$ lẻ và không chia hết cho 5. Chứng minh có lũy thừa của n có chữ số đơn vị là 1.

4.92. Tìm các chữ số x, y, z để $(xyz)_9 = (zyx)_6$.

4.93. Nếu $n \in \mathbb{Z}^+$, có bao nhiêu giá trị có thể của $\gcd(n, n + 3000)$?

4.94. Nếu $n \in \mathbb{Z}^+$ và $n \geq 2$, chứng minh $2^n < \binom{2n}{n} < 4^n$.

4.95. Nếu $n \in \mathbb{Z}^+$, chứng minh 57 là ước của $7^{n+2} + 8^{2n+1}$.

4.96. Với mọi $n \in \mathbb{Z}^+$, chứng minh nếu $n \geq 64$, thì n có thể viết thành tổng của 5 và/hoặc 17.

4.97. Tìm tất cả $a, b \in \mathbb{Z}$ sao cho $\frac{a}{7} + \frac{b}{12} = \frac{1}{84}$.

4.98. Với $r \in \mathbb{Z}^+$, ta viết $r = r_0 + r_1 \cdot 10 + r_2 \cdot 10^2 + \cdots + r_n \cdot 10^n$, trong đó $0 \leq r_i \leq 9$ với $i = \overline{0, n}$ và $r_n \neq 0$.

a) Chứng minh $9 \mid r \Leftrightarrow 9 \mid (r_n + r_{n-1} + \cdots r_2 + r_1 + r_0)$.

b) Chứng minh $3 \mid r \Leftrightarrow 3 \mid (r_n + r_{n-1} + \cdots r_2 + r_1 + r_0)$.

c) Nếu $t = 137486x225$, trong đó x là một chữ số, tìm các giá trị của x sao cho $3 \mid t$. Trong đó, các giá trị nào của x làm t chia hết cho 9?

4.99. a) Có bao nhiêu số nguyên dương là tích của chín số nguyên tố trong các số 2, 3, 5, 7, 11 (có thể lặp và thứ tự không quan trọng).

b) Có bao nhiêu số nguyên dương trong ý (a) chứa tất cả thừa số 2, 3, 4, 5, 11.

4.100. Tìm tích của các ước dương của (a) 1000; (b) 5000; (c) 7000; (d) 9000; (e) $p^m q^n$; và (f) $p^m q^n r^k$, trong đó p, q, r là các số nguyên tố phân biệt và $m, n, k \in \mathbb{Z}^+$.

4.101. Cho $A = \{a_1, a_2, a_3, a_4, a_5\} \subseteq Z^+$. Chứng minh A chứa tập con $S \neq \varnothing$ có tổng các phần tử là bội của 5. (Ở đây tổng có thể có đúng một số hạng.)

4.102. Tìm các số nguyên n sao cho $\frac{5n-4}{6}$ và $\frac{7n+1}{4}$ đều là số nguyên.

4.103. Cho $a, b \in \mathbb{Z}^+$.

a) Chứng minh nếu $a^2 \mid b^2$ thì $a \mid b$.

b) Khẳng định nếu $a^2 \mid b^3$ thì $a \mid b$ có đúng không?

4.104. Cho n là số nguyên dương thỏa mãn tính chất: $\forall a, b \in \mathbb{Z}^+,\ n \mid ab \Rightarrow n \mid a \vee n \mid b$. Chứng minh $n = 1$ hoặc n nguyên tố.

4.105. Giả sử $a, b, k \in \mathbb{Z}^+$ và k không phải lũy thừa của 2.

a) Chứng minh nếu $a^k + b^k \neq 2$, thì $a^k + b^k$ là hợp số.

b) Nếu $n \in \mathbb{Z}^+$ và n không là lũy thừa của 2, chứng minh nếu $2^n + 1$ nguyên tố, thì n nguyên tố.

4.106. Nhắc lại H_n, F_n và L_n tương ứng là số điều hòa, Fibonacci, và Lucas thứ n. Chứng minh $\forall n \in \mathbb{N}$,

a) $H_{2^n} \leq 1 + n$

b) $F_n < \left(\frac{5}{3}\right)^n$

c) $L_0 + L_1 + L_2 + \cdots + L_n = \sum_{i=0}^{n} L_i = L_{n+2} - 1$

4.107. Cho $n \in \mathbb{Z}^+$, u là chữ số đơn vị của n. Chứng minh $7 \mid n \Leftrightarrow 7 \mid \left(\frac{n-u}{10} - 2u\right)$.

4.108. Cho $m, n \in \mathbb{Z}^+$ với $19m + 90 + 8n = 1998$. Tìm m, n sao cho

a) n nhỏ nhất

b) m nhỏ nhất

4.109. Chọn tùy ý ba số nguyên từ {0, 1, 2,. . . , 9} và lập sáu số gồm ba chữ số này (cho phép chữ số 0 ở đầu). Chẳng hạn, nếu chọn 1, 3 và 7, ta lập được các số 137, 173, 317, 371, 713 và 731. Chứng minh sáu số lập được không đồng thời là số nguyên tố.

4.110. Bỏ đi một số nguyên trong các số $1, 2, 3, \ldots, n$, thì trung bình của các số còn lại là hỗn số $35\frac{7}{17}$. Tìm n và số đã bỏ đi đó.

4.111. Chọn ngẫu nhiên một số nguyên từ 1 đến 100. Tính xác suất để số đó chia hết cho

a) 2 hoặc 3

b) 2, 3, hoặc 5

4.112. Cho $m = p_1^{e_1} p_2^{e_2} p_3^{e_3} p_4^{e_4}$ và $n = p_1^{f_1} p_2^{f_2} p_3^{f_3} p_5^{f_5}$, trong đó p_1, p_2, p_3, p_4, p_5 là các số nguyên tố phân biệt, và $e_1, e_2, e_3, e_4, f_1, f_2, f_3, f_5 \in \mathbb{Z}^+$. Có bao nhiêu ước chung của m và 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.