

## HƯỚNG DẪN GIẢI BÀI TẬP CHƯƠNG I

### §1. Chia hết và chia có dư

1. a)  $1997^{1999} - 1997^{1998} = 1997^{1998} (1997 - 1) : 4$ , vì  $1996 : 4$ .

b) Ta có:  $1998 = 4k + 2$ . Suy ra  $1998^2 = (4k + 2)^2 = 4(2k + 1)^2 : 4$ .

Bởi vậy  $1998^{1999} = 1998^{1997} \cdot 1998^2 : 4$ .

Mặt khác,  $1997 = 4k + 1$ , nên theo khai triển nhị thức Newton ta có:

$$(4k + 1)^n = C_n^0 (4k)^n + C_n^1 (4k)^{n-1} + \dots + C_n^{n-1} (4k) + 1 = 4q + 1.$$

Từ đó suy ra  $1997^{1998} - 1998^{1999} \not\equiv 4$ .

2. Hai số chẵn liên tiếp có dạng  $2k$  và  $2k + 2$ ,  $k \in \mathbb{Z}$ .

- Nếu  $k$  là số chẵn,  $k = 2t$ ,  $t \in \mathbb{Z}$  thì  $2k = 4t$  và  $2k + 2 = 4t + 2$ .

- Nếu  $k$  là số lẻ,  $k = 2t + 1$  thì  $2k = 4t + 2$  và  $2k + 2 = 4t + 4$ .

Như vậy trong cả hai trường hợp chỉ có đúng một số chia hết cho 4.

3. Ta có  $(mq + np) - (mp + nq) = m(q - p) - n(q - p) = (m - n)(q - p)$ .

Từ đó nếu  $mp + nq = (m - n)t$ ,  $t \in \mathbb{Z}$  thì  $mq + np = (m - n)(q - p) + (m - n)t = (m - n)(q - p + t)$  chia hết cho  $m - n$ .

4. Giả sử  $a = bq + r$ ,  $0 \leq r < b$ . Khi đó  $bq \leq a < b(q + 1)$ .

a)  $a = 133$  và  $q = 11 \Rightarrow 11b \leq 133 < 12b$ .

Bằng phép thử trực tiếp ta có  $b = 12$ , còn  $r = a - bq = 133 - 11 \cdot 12 = 1$ .

b)  $a = 350$  và  $q = 47 \Rightarrow 47b \leq 350 < 48b$ .

Bằng phép thử trực tiếp ta thấy  $47b \leq 350 \Rightarrow b \leq 7$ ,  $350 < 48b \Rightarrow b > 8$ .

Vậy các số  $b, q$  không tồn tại.

5. Các số  $a, b, c$  có thể viết dưới dạng:

$$a = 3p_1 + r_1$$

$$b = 3p_2 + r_2$$

$$c = 3p_3 + r_3$$

trong đó mỗi số  $r_i$  ( $i = 1, 2, 3$ ) nhận các giá trị thuộc tập hợp  $\{0; 1; -1\}$ . Dễ thấy rằng  $r_i^3 = r_i$ , do đó

$$a^3 = (3p_1 + r_1)^3 = 9k_1 + r_1,$$

$$b^3 = 9k_2 + r_2,$$

$$c^3 = 9k_3 + r_3,$$

với  $k_1, k_2, k_3$  thuộc  $\mathbb{Z}$ . Vậy  $a^3 + b^3 + c^3 = 9(k_1 + k_2 + k_3) + (r_1 + r_2 + r_3)$ . Ta có  $|r_1 + r_2 + r_3| \leq 3$

nên để  $(a^3 + b^3 + c^3) : 9$  thì phải có  $r_1 + r_2 + r_3 = 0$ .

Khi đó buộc phải có một trong  $r_i$  bằng 0. Điều này có nghĩa là một trong ba số  $a, b, c$  phải chia hết cho 3.

6. Xét tổng của  $n$  số nguyên liên tiếp ta có

$$(a + 1) + (a + 2) + \dots + (a + n) = na + \frac{n(n + 1)}{2}.$$

Tổng này chia hết cho  $n$  khi và chỉ khi  $n + 1$  là số chẵn, tức là  $n$  lẻ

7. Nếu  $x = 5k, k \in \mathbb{Z}$  thì  $x^2 + 2 = 25k^2 + 2$ .

Nếu  $x = 5k \pm 1$  thì  $x^2 + 2 = 5A + 3$ .

Nếu  $x = 5k \pm 2$  thì  $x^2 + 2 = 5A + 1$ .

Như vậy, trong mọi trường hợp  $x^2 + 2$  đều không chia hết cho 5, nghĩa là phương trình  $x^2 + 2 = 5y$  không có nghiệm nguyên.

8. Xét hệ 
$$\begin{cases} x - y + z = 2 & (1) \\ 2x^2 - xy + x - 2z = 1 & (2) \end{cases}.$$

Từ (1) có  $z = 2 + y - x$ .

Thế vào (2) ta được  $2x^2 - xy + x - 4 - 2y + 2x = 1$  hay  $2x^2 + 3x - 5 = y(x + 2)$ . Do  $x = -2$  không thỏa mãn phương trình nên

$$y = \frac{2x^2 + 3x - 5}{x + 2} = 2x - 1 - \frac{3}{x + 2}$$

$y$  nguyên khi và chỉ khi  $x + 2$  là ước của 3.

Suy ra  $x + 2 = \pm 1; \pm 3$ . Vậy  $x = -1; -3; 1; -5$ .

Từ đó ta có các nghiệm nguyên của hệ phương trình đã cho là:

$x = -1$	$x = -3$	$x = 1$	$x = -5$
$y = -6$	$y = -4$	$y = 0$	$y = -10$
$z = -3$	$z = 1$	$z = 1$	$z = -3$

## §2. Ước chung lớn nhất (ƯCLN)

9. Giả sử  $a, b, c \in \mathbb{Z}, a \leq b \leq c, b = aq_1 + r_1, c = aq_2 + r_2$ .

Khi đó  $\text{ƯCLN}(a, b) = \text{ƯCLN}(a, r_1)$  và  $\text{ƯCLN}(a, c) = \text{ƯCLN}(a, r_2)$ .

Suy ra

$$\begin{aligned} \text{ƯCLN}(a, b, c) &= \text{ƯCLN}(\text{ƯCLN}(a, b), c) \\ &= \text{ƯCLN}(\text{ƯCLN}(a, r_1), r_2) \\ &= \text{ƯCLN}(\text{ƯCLN}(a, c), r_1) \\ &= \text{ƯCLN}(\text{ƯCLN}(a, r_2), r_1) \\ &= \text{ƯCLN}(a, r_1, r_2). \end{aligned}$$

Áp dụng ta có:

$$1794 = 1.1248 + 546; 2730 = 2.1248 + 234$$

nên

$$\text{ƯCLN}(1248, 1794, 2730) = \text{ƯCLN}(1248, 546, 234).$$

Ta lại có:  $1248 = 5.234 + 78; 546 = 2.234 + 78$

nên

$$\text{ƯCLN}(1248, 546, 234) = \text{ƯCLN}(234, 78, 78) = (234, 78) = 78.$$

10. a) Chứng minh  $\text{ƯCLN}(a - b, ab) = 1$ .

Sử dụng tính chất  $(m = nq + r) \Rightarrow \text{ƯCLN}(m, n) = \text{ƯCLN}(n, r)$  (\*).

Ta có  $\text{ƯCLN}(a - b, a) = \text{ƯCLN}(a, b) = 1; \text{ƯCLN}(a - b, b) = \text{ƯCLN}(a, b) = 1$ .

Do  $\text{ƯCLN}(m, c) = \text{ƯCLN}(m, d) = 1$  thì  $\text{ƯCLN}(m, cd) = 1$  (\*\*) nên  $\text{ƯCLN}(a - b, ab) = 1$ .

b) Chứng minh  $\text{ƯCLN}(2a + b, a(a + b)) = 1$ .

Sử dụng tính chất (\*) ta có:

$$\begin{aligned} \text{ƯCLN}(2a + b, a) &= \text{ƯCLN}(a, b) = 1; \\ \text{ƯCLN}(2a + b, a + b) &= \text{ƯCLN}(a + b, a) \\ &= \text{ƯCLN}(a, b) = 1. \end{aligned}$$

Từ đó theo tính chất (\*\*) ta có:  $\text{ƯCLN}(2a + b, a(a + b)) = 1$ .

11. a) Giả sử  $a + b = 432$  và  $\text{ƯCLN}(a, b) = 36$ .

Khi đó  $a = 36a_1, b = 36b_1$  và  $\text{ƯCLN}(a_1, b_1) = 1$  (1).

Suy ra  $36(a_1 + b_1) = 432; a_1 + b_1 = 12$  (2).

Có thể giả thiết rằng  $a_1 \leq b_1$ .

Khi đó từ (1) và (2) suy ra  $a_1 = 1$  và  $b_1 = 11$  hoặc  $a_1 = 5$  và  $b_1 = 7$ .

Vậy  $a = 36$  và  $b = 396$  hoặc  $a = 180$  và  $b = 252$ .

b) Giả sử  $ab = 8400$  và  $\text{ƯCLN}(a, b) = 20, a \leq b$ .

Khi đó  $a = 20a_1, b = 20b_1$  và  $(a_1, b_1) = 1$ .

Suy ra  $ab = 400a_1b_1 = 8400 \Rightarrow a_1b_1 = 21$ .

Do  $a_1, b_1$  nguyên tố cùng nhau nên  $a_1 = 1$  và  $b_1 = 21$  hoặc  $a_1 = 3$  và  $b_1 = 7$ .

Vậy  $a = 20$  và  $b = 420$  hoặc  $a = 60$  và  $b = 140$ .

12. a)  $a = 21m + 4, b = 14m + 3$ .

Ta có:  $a = 21m + 4 = (14m + 3) + (7m + 1); 14m + 3 = 2(7m + 1) + 1$ .

Do đó  $\text{ƯCLN}(a, b) = \text{ƯCLN}(14m + 3, 7m + 1) = \text{ƯCLN}(7m + 1, 1) = 1$ .

b)  $a = m^3 + 2m, b = m^4 + 3m^2 + 1$ .

Ta có:

$m^4 + 3m^2 + 1 = m(m^3 + 2m) + (m^2 + 1)$ ;  $m^3 + 2m = m(m^2 + 1) + m$ ;  $m^2 + 1 = m \cdot m + 1$ ,  
do đó

$$UCLN(a, b) = UCLN(m^3 + 2m, m^2 + 1) = UCLN(m^2 + 1, m) = UCLN(m, 1) = 1.$$

c)  $a = m^2n + 2m$ ,  $b = mn + 1$ .

Ta có:  $a = m^2n + 2m = m(mn + 1) + m$ ,

do đó

$$UCLN(a, b) = UCLN(mn + 1, m) = UCLN(m, 1) = 1.$$

13. Từ đẳng thức  $(ac - bd) - (a - b)c = b(c - d)$  suy ra  $n$  là ước của  $b(c - d)$ .

Mặt khác,  $UCLN(a - b, b) = UCLN(a, b) = 1$ .

Do  $n$  là ước của  $a - b$  nên ta cũng có  $UCLN(n, b) = 1$ .

Từ đó ta kéo theo  $b(c - d) : n \Rightarrow (c - d) : n$ .

14. a) Xét tập hợp  $A = \{bx + 1 / 0 \leq x < a, x \in \mathbb{N}\}$ .

Trong tập  $A$  nếu  $x_1 \neq x_2$  thì  $bx_1 + 1, bx_2 + 1$  sẽ có các số dư khác nhau trong phép chia cho  $a$ . Thật vậy

$$(bx_1 + 1 - bx_2 + 1) : a \Leftrightarrow b(x_1 - x_2) : a \Leftrightarrow x_1 - x_2 : a \Leftrightarrow x_1 - x_2 = 0 \text{ (do } |x_1 - x_2| < a).$$

Từ nhận xét trên suy ra rằng trong  $A$  có đúng một số chia hết cho  $a$ , chẳng hạn đó là  $bn + 1$   
 $bn + 1 = am, m > 0$ .

Bây giờ ta chứng tỏ cặp  $(m, n)$  là duy nhất. Giả sử có cặp  $(m', n')$  sao cho  $am' - bn' = 1, 0 < m', 0 \leq n' < a$ . Khi đó  $am' - bn' = am - bn \Rightarrow a(m' - m) = b(n' - n)$ . Do  $(a, b) = 1$  nên  $a$  là ước của  $n' - n$ . Do  $|n' - n| < a$  nên  $n' - n = 0$ . Từ đó  $n' = n$  và  $m' = m$ .

b) Tương tự câu a).

15. a) Đặt  $UCLN(a + b, a^2 + b^2 - ab) = d$ , ta có  $d$  là ước của  $(a + b)^2$  và do đó  $d$  là ước của  $UCLN((a + b)^2, a^2 + b^2 - ab) = UCLN((a + b)^2, (a + b)^2 - 3ab) = UCLN((a + b)^2, 3ab)$ .

Từ đó suy ra  $d$  là ước của 3 hoặc  $d$  là ước của  $UCLN((a + b)^2, ab)$ .

Mặt khác, do  $UCLN(a, b) = 1$  và  $UCLN(a + b, a) = UCLN(a + b, b) = 1$  nên  $UCLN(a + b, ab) = 1$  suy ra  $UCLN((a + b)^2, ab) = 1$ .

Vậy  $d \mid 1$  hoặc  $d \mid 3$ , nghĩa là  $d = 1$  hoặc  $d = 3$ .

b) Đặt  $d = UCLN(11a + 2b, 18a + 5b)$ , ta có  $d$  là ước của  $UCLN(5(11a + 2b), 2(18a + 5b)) = UCLN(5(11a + 2b), 5(11a + 2b) - 19a) = UCLN(5(11a + 2b), 19a)$ .

Từ đó suy ra  $d$  là ước của  $19a$ , nghĩa là  $d = 1$  hoặc  $d = 19$  hoặc  $d \mid a$ .

Nếu  $d \mid a$  thì do  $d \mid (11a + 2b)$  và  $d \mid (18a + 5b)$  nên  $d \mid 2b$  và  $d \mid 5b$ , từ đó  $d \mid b$ .

Mà  $UCLN(a, b) = 1$  nên  $d = 1$ .

Vậy  $d = 1$  hoặc  $d = 19$ .

16. a) Trước hết, ta chứng minh bằng qui nạp theo  $n$  rằng:

$$UCLN(a^m - 1, a^n - 1) = a^{(m,n)} - 1, (*) \text{ với mọi } m, n \in \mathbb{N}, m \neq 0.$$

- Với  $n = 0$  thì  $a^n - 1 = 0$  và  $UCLN(m, n) = m$ , do đó:

$$UCLN(a^m - 1, a^n - 1) = a^m - 1 = a^{(m,n)} - 1.$$

Vậy (\*) đúng với  $n = 0$ .

- Giả sử đẳng thức (\*) đúng với mọi  $0 \leq k < n, n \neq 0$ .

Theo định lý về phép chia có dư ta có:

$$m = nq + r, q \in \mathbb{N} \text{ và } 0 \leq r < n.$$

Nếu  $q = 0$  thì  $a^{nq} - 1 = 0$ ; còn nếu  $q \geq 1$  thì  $a^{nq} - 1 = (a^n - 1)(a^{n(q-1)} + \dots + a^n + 1)$ .

Do  $a^{nq} - 1$  luôn chia hết cho  $a^n - 1$ . Ta có  $a^m - 1 = a^{nq+r} - 1 = a^r \cdot a^{nq} - 1 = a^r(a^{nq} - 1) + (a^r - 1)$ .

Bởi vậy  $UCLN(a^m - 1, a^n - 1) = UCLN(a^r - 1, a^n - 1)$ .

Do  $r < n$  nên theo giả thiết qui nạp

$$UCLN(a^r - 1, a^n - 1) = a^{(r,n)} - 1.$$

Mặt khác, từ  $m = nq + r$  suy ra

$$UCLN(m, n) = UCLN(r, n).$$

Vậy  $UCLN(a^m - 1, a^n - 1) = a^{(m,n)} - 1$ . Đẳng thức (\*) đúng với mọi  $n$ .

b) Bây giờ áp dụng đẳng thức (\*) và giả thiết  $(m, n) = 1$ , ta có:

$$(a^m - 1, a^n - 1) = a - 1.$$

Từ đó  $a^m - 1 = (a - 1).B$ ;  $a^n - 1 = (a - 1).C$ , với  $(B, C) = 1$ .

Ta cũng có  $a^{mn} - 1 = (a - 1).D$  và  $(a^{mn} - 1) : (a^m - 1)$

nên

$$(a - 1).D : (a - 1).B \Rightarrow D : B$$

Tương tự ta có  $D : C$ . Do  $(B, C) = 1$  nên  $D : BC$

$$\Rightarrow (a - 1)^2.D : (a - 1)^2.BC$$

$$\Rightarrow (a - 1)(a^{mn} - 1) : (a^m - 1)(a^n - 1).$$

**17. a) Điều kiện cần.** Giả sử  $2^p - 1$  và  $2^q - 1$  nguyên tố cùng nhau. Ta chứng minh  $p$  và  $q$  nguyên tố cùng nhau. Giả sử ngược lại  $p = ku$ ,  $q = kv$ ,  $k > 1$ . Khi đó

$$2^p - 1 = 2^{ku} - 1 = (2^k)^u - 1$$

do đó

$$2^p - 1 : 2^k - 1.$$

Tương tự ta cũng có

$$2^q - 1 : 2^k - 1.$$

Như vậy  $2^p - 1$  và  $2^q - 1$  có ước chung là  $2^k - 1 > 1$ , trái giả thiết. Vậy  $p$  và  $q$  nguyên tố cùng nhau.

**b) Điều kiện đủ.** Bây giờ giả sử  $p$  và  $q$  nguyên tố cùng nhau. Không mất tính tổng quát ta giả sử  $p > q$  và  $p = qk + r$ , trong đó  $0 < r < q$ ,  $k > 0$  và  $(q, r) = (p, q) = 1$ .

Khi đó

$$2^p - 1 = 2^r.2^{qk} - 2^r + 2^r - 1$$

$$= 2^r(2^{qk} - 1) + (2^r - 1)$$

$$= 2^r(2^q - 1).M + (2^r - 1), M \in \mathbb{N}.$$

- Nếu  $\text{ƯCLN}(2^p - 1, 2^q - 1) = d > 1$  thì ta cũng có

$$\text{ƯCLN}(2^q - 1, 2^r - 1) = d, q > r.$$

Bây giờ tương tự như trên ta lại có

$$q = rk_1 + r_1, 0 < r_1 < r \text{ và } \text{ƯCLN}(2^r - 1, 2^{r_1} - 1) = d.$$

Lập luận này không thể tiếp tục đến vô hạn vì  $q, r, r_1, \dots$  là dãy số tự nhiên giảm.

Vậy  $2^p - 1$  và  $2^q - 1$  phải là nguyên tố cùng nhau.

### §3. Bội chung nhỏ nhất (BCNN)

**18. a)** Tìm BCNN  $(2^n - 1, 2^n + 1), n \in \mathbb{N}$ .

Nếu  $n = 0$  thì  $2^n - 1 = 0$ .

Nếu  $n > 0$  thì  $2^n + 1 = (2^n - 1) + 2$ . Do đó  $\text{ƯCLN}(2^n + 1, 2^n - 1) = \text{ƯCLN}(2^n - 1, 2) = 1$ .

Suy ra

$$\text{BCNN}(2^n + 1, 2^n - 1) = (2^n + 1)(2^n - 1) = 4^n - 1.$$

**19.** Gọi ba số nguyên liên tiếp khác 0 là  $a, a + 1, a + 2$ . Trước hết ta nhận xét rằng

$$\text{ƯCLN}(a(a + 2), (a + 1)) = 1.$$

Thật vậy,  $a(a + 2) = a^2 + 2a = a(a + 1) + a$

nên

$$\begin{aligned} \text{ƯCLN}(a(a + 2), (a + 1)) &= \text{ƯCLN}(a + 1, a) \\ &= \text{ƯCLN}(a, 1) = 1. \end{aligned}$$

Nếu  $a$  lẻ thì

$$\begin{aligned} \text{BCNN}(a, a + 1, a + 2) &= \text{BCNN}(\text{BCNN}(a, a + 2), a + 1) \\ &= \text{BCNN}(|a(a + 2)|, a + 1) = |a(a + 1)(a + 2)|. \end{aligned}$$

Nếu  $a$  chẵn thì

$$\begin{aligned} \text{BCNN}(a, a+1, a+2) &= \text{BCNN}(\text{BCNN}(a, a+2), a+1) \\ &= \text{BCNN}\left(\frac{1}{2}|a(a+2)|, a+1\right) = \frac{1}{2}|a(a+1)(a+2)|. \end{aligned}$$

20. Giả sử  $\text{U'CLN}(a, b) = 15$ ,  $\text{BCNN}(a, b) = 2835$ ,  $0 < a \leq b$ .

Ta có  $a = 15a_1$ ,  $b = 15b_1$ , với  $\text{U'CLN}(a_1, b_1) = 1$ .

Khi đó

$$2835 = \text{BCNN}(15a_1, 15b_1) = 15 \cdot \text{BCNN}(a_1, b_1) = 15a_1b_1 \Rightarrow a_1b_1 = 189 = 3^3 \cdot 7.$$

Do  $\text{U'CLN}(a_1, b_1) = 1$  nên hoặc  $a_1 = 1$ ,  $b_1 = 189$  hoặc  $a_1 = 7$ ,  $b_1 = 27$ .

Khi đó  $a = 15$ ,  $b = 2835$  hoặc  $a = 105$ ,  $b = 495$ .

21. Giả sử  $a \leq b$ ,  $a = da_1$ ,  $b = db_1$ ,  $(a_1, b_1) = 1$ . Khi đó theo giả thiết ta có

$$\begin{cases} d^2(a_1^2 + b_1^2) = 468 \\ d + da_1b_1 = 42 \end{cases} \Rightarrow \frac{a_1^2 + b_1^2}{(1 + a_1b_1)^2} = \frac{468}{42^2} = \frac{13}{7} \Rightarrow \begin{cases} 1 + a_1b_1 = 7k \\ a_1^2 + b_1^2 = 13k^2 \end{cases}.$$

Vì  $d(1 + a_1b_1) = 42$  nên  $1 \leq k \leq 6$ .

$$\text{Với } k = 1 \text{ ta có } \begin{cases} 1 + a_1b_1 = 7 \\ a_1^2 + b_1^2 = 13 \end{cases} \Rightarrow \begin{cases} a_1b_1 = 6 \\ a_1 + b_1 = 5 \end{cases} \Rightarrow a_1 = 2, b_1 = 3 \Rightarrow a = 12, b = 18.$$

Thử với các giá trị còn lại của  $k$  ta không nhận thêm được cặp  $a, b$  nào thoả mãn bài toán.

22.

$$\begin{aligned} \text{a) } m^5 - m &= m(m^2 - 1)(m^2 + 1) = m(m^2 - 1)(m^2 - 4) + 5m(m^2 - 1) \\ &= (m - 2)(m - 1)m(m + 1)(m + 2) + 5(m - 1)m(m + 1). \end{aligned}$$

Mỗi số hạng của tổng đều chia hết cho  $5 \cdot 6 = 30$  nên tổng chia hết cho 30.

$$\text{b) } m^5 - 5m^3 + 4m = m(m^4 - 5m^2 + 4) = m(m^2 - 1)(m^2 - 4) = (m - 2)(m - 1)m(m + 1)(m + 2).$$

Trong 5 số nguyên liên tiếp phải có hai số chẵn liên tiếp, một trong hai số này chia hết cho 4, vì vậy tích của 5 số nguyên chia hết cho  $4 \cdot 2 = 8$ .

Mặt khác, tích của 5 số nguyên liên tiếp phải chia hết cho 3 và 5.

Bởi vậy tích này chia hết cho  $8 \cdot 3 \cdot 5 = 120$ .

23. a) Giả sử  $m = 2k + 1$ . Khi đó

$$\begin{aligned} m^3 + 3m^2 - m - 3 &= m^2(m + 3) - (m + 3) \\ &= (m + 3)(m^2 - 1) \\ &= (m - 1)(m + 1)(m + 3) \\ &= 2k(2k + 2)(2k + 4) \\ &= 8k(k + 1)(k + 2). \end{aligned}$$

Rõ ràng tích cuối cùng chia hết cho  $8 \cdot 6 = 48$ .

b) Với  $m = 2k + 1$ , ta có

$$\begin{aligned} m^{12} - m^8 - m^4 + 1 &= m^8(m^4 - 1) - (m^4 - 1) \\ &= (m^4 - 1)(m^8 - 1) \\ &= (m^4 - 1)^2(m^4 + 1) \\ &= (m - 1)^2(m + 1)^2(m^2 + 1)^2(m^4 + 1) \\ &= (2k)^2(2k + 2)^2(2p)^2(2q) \\ &= 4 \cdot 4[k(k + 1)]^2 \cdot 4p^2 \cdot 2q \\ &= 128[k(k + 1)]^2 \cdot p^2 \cdot q. \end{aligned}$$

$k(k + 1)$  chia hết cho 2 nên tích cuối cùng chia hết cho  $128 \cdot 2^2 = 512$ .

24. Chứng minh  $\text{U'CLN}(a + b, m) = \text{U'CLN}(a, b)$ , với  $m = \text{BCNN}(a, b)$ .

Gọi  $d = \text{U'CLN}(a, b)$  ta có  $a = da_1$ ,  $b = db_1$ ,  $\text{U'CLN}(a_1, b_1) = 1$ . Khi đó

$$\text{U'CLN}(a + b, m) = \text{U'CLN}(da_1 + db_1, da_1b_1) = d \cdot \text{U'CLN}(a_1 + b_1, a_1b_1).$$

Ta có

$$UCLN(a_1 + b_1, a_1) = UCLN(a_1, b_1) = 1;$$

$$UCLN(a_1 + b_1, b_1) = UCLN(a_1, b_1) = 1 \Rightarrow UCLN(a_1 + b_1, a_1 b_1) = 1.$$

Từ đó suy ra

$$UCLN(a + b, m) = d = UCLN(a, b).$$

25. Ta có D chia hết  $M_i$  và  $M_i$  chia hết M với  $i = 1, 2, \dots, n$ , do đó D chia hết M.

Đặt  $q = \frac{M}{D}$  ta có  $M_i = Dq_i \Rightarrow a_i Dq_i = a_i M_i = M \Rightarrow a_i q_i = q$ . Suy ra q chia hết cho  $a_i$

với mọi  $i = 1, 2, \dots, n$ .

Giả sử m là một bội chung của các  $a_i$ , ( $i = 1, 2, \dots, n$ ). Đặt  $m = a_i r_i$  ta có  $m M_i = r_i a_i M_i = r_i M$  do đó M chia hết  $m M_i$ . Suy ra  $M \mid (m M_1, m M_2, \dots, m M_n) \Rightarrow M \mid m(M_1, M_2, \dots, M_n) \Rightarrow M \mid mD$ .

Từ đó  $q = \frac{M}{D}$  chia hết m.

Như vậy,  $q = \frac{M}{D}$  là một bội chung của các  $a_i$  và mọi bội chung khác của các  $a_i$  đều là bội

của q. Điều đó chứng tỏ  $q = \frac{M}{D} = [a_1, a_2, \dots, a_n]$ .

26. a) Vai trò của n và k như nhau, ta chỉ cần chứng minh  $(n!)^k$  là ước của  $(nk)!$ .

Phép chứng minh được tiến hành quy nạp theo k

Với  $k = 1$  mệnh đề hiển nhiên đúng.

Giả sử  $(n!)^k$  là ước của  $(nk)!$ . Khi đó ta có

$$C_{n(k+1)}^n = \frac{(n(k+1))!}{n!(nk)!} \in \mathbb{Z} \Rightarrow (n(k+1))! : n!(nk)!$$

Theo giả thiết quy nạp  $(nk)! : (n!)^k$ . Do đó  $(n(k+1))! : n!(n!)^k = (n!)^{k+1}$ .

Vậy  $(nk)! : (n!)^k$  với mọi  $k \geq 1$ .

b) Vì  $(n!)^k \mid (nk)!$  và  $(k!)^n \mid (nk)!$  nên  $(nk)!$  là một bội chung của  $(n!)^k$  và  $(k!)^n$ . Từ đó  $(nk)!$  là một bội của  $[(n!)^k, (k!)^n]$ .

#### §4. Số nguyên tố

27.  $n^4 + 4 = (n^4 + 4n^2 + 4) - 4n^2 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2 + 2n)(n^2 + 2 - 2n)$ .

28.  $p^2 - 1 = (p - 1)(p + 1)$ .

Đây là tích của hai số chẵn liên tiếp nên có một số chia hết cho 4, một số chia hết cho 2.

Vậy tích chia hết cho 8.

Mặt khác,  $p^2 - 1 = (3k \pm 1)^2 - 1 = 9k^2 \pm 6k = 3Q$ , do đó  $p^2 - 1$  chia hết cho 3.

Hai số 3 và 8 nguyên tố cùng nhau nên  $p^2 - 1$  chia hết cho  $3 \cdot 8 = 24$ .

29. Ta lần lượt xét các trường hợp:

- Nếu  $p = 3$  thì  $p + 4 = 7$ ,  $p + 8 = 11$  đều là những số nguyên tố.

- nếu  $p = 3k + 1$  thì  $p + 8 = 3k + 9 = 3(k + 3)$  là hợp số.

- Nếu  $p = 3k - 1$  thì  $p + 4 = 3k + 3 = 3(k + 1)$  là hợp số.

Vậy  $p = 3$  là số nguyên tố duy nhất phải tìm.

30. Giả sử có  $p = 30q + r$ ,  $0 < r < 30$ .

Nếu r là hợp số thì r có các ước nguyên tố  $u < \sqrt{30}$ .

Vì vậy u chỉ có thể nhận một trong các giá trị 2, 3, 5.

Những giá trị này cũng là ước của 30 và do đó là ước của p, trái với tính nguyên tố của p.

31. Chứng minh tích hai số có dạng  $4n + 1$  là một số cũng có dạng đó.

Giả sử  $a = 4p + 1$ ,  $b = 4q + 1$ . Khi đó  $ab = (4p + 1)(4q + 1) = 4(4pq + p + q) + 1 = 4c + 1$ .

Chứng minh có vô số số nguyên tố có dạng  $4m + 3$ .

Giả sử có hữu hạn số nguyên tố có dạng  $4m + 3$ :  $p_1 = 3$ ,  $p_2 = 7$ , ...,  $p_n$ .

Xét số

$$a = 4p_1 p_2 \dots p_n - 1.$$

Nếu tất cả các ước số nguyên tố của  $a$  đều có dạng  $4k + 1$  thì theo phản chứng minh trên số  $a$  cũng có dạng đó, trái với giả thiết về  $a$  ( $a = 4u - 1$ ).

Bởi vậy  $a$  phải có một ước nguyên tố  $q$  dạng  $4k + 3$ . Số  $q$  này không trùng với các  $p_i$  ( $i = 1, 2, \dots, n$ ), vì nếu  $q$  trùng với một trong các  $p_i$  thì  $q$  sẽ là ước của  $1 = 4p_1p_2\dots p_n - a$ , vô lý.

Lập luận trên chứng tỏ tập các số nguyên tố  $4m + 3$  là vô hạn.

\* Để chứng minh có vô số số nguyên tố dạng  $6m + 5$  trước hết ta chứng minh tích hai số dạng  $6m + 1$  là một số dạng đó.

Sau đó lại lý luận như trường hợp các số nguyên tố dạng  $4m + 3$ .

**32.** Do  $m > 2$  nên  $m! - 1 > 4$ . Gọi  $p$  là một ước số nguyên tố của  $a = m! - 1$  ta có  $p \leq a \Rightarrow p < m!$ .

Bây giờ ta chứng tỏ  $p < m$ . Giả sử ngược lại  $p \leq m$ . Khi đó  $p$  là ước của  $m!$  và do đó  $p$  là ước của  $m! - (m! - 1) = 1$ , vô lý. Vậy  $p$  là số nguyên tố thỏa mãn  $m < p < m!$ .

Chứng minh có vô số số nguyên tố.

Giả sử ngược lại chỉ có hữu hạn số nguyên tố:  $p_1, p_2, \dots, p_n$ . Đặt  $m = p_1p_2\dots p_n$ , thế thì  $m > 2$  và theo phản chứng minh trên có số nguyên tố  $p$  sao cho  $m < p < m!$ .

Vì  $m = p_1p_2\dots p_n < p$  nên  $p$  khác với  $p_i$  ( $i = 1, 2, \dots, n$ ). Điều này mâu thuẫn với điều giả sử trên.

**33.** Ta có thể giả sử  $m > n$  và đặt  $m = n + r$ ,  $r \in \mathbb{N}^*$ . Khi đó  $b = 2^{2^m} + 1 = (2^{2^n})^{2^r} + 1$ . Đặt  $a = 2^{2^n} + 1$  ta có  $b = (a - 1)^{2^r} + 1 = ak + 2$  (sau khi khai triển nhị thức  $(a - 1)^{2^r}$  với  $k$  nào đó. Từ đó  $(a, b) = (a, 2) = 1$  (do  $a$  là số lẻ).

Bây giờ với mỗi số nguyên dương  $n$  ta gọi  $p_n$  là ước nguyên tố nhỏ nhất của  $2^{2^n} + 1$ . Theo chứng minh trên  $p_n \neq p_m$  với mọi  $m \neq n$ .

Vậy dãy số nguyên tố  $(p_n)$ ,  $n \in \mathbb{N}$  là đôi một khác nhau. Điều này chứng tỏ tập hợp các số nguyên tố là vô hạn.

**34.** Từ phương trình ta thấy hai số  $x^y$  và  $z$  không cùng tính chẵn lẻ.

Nếu  $z$  chẵn thì  $z = 2$  do nó là số nguyên tố. Khi đó  $x^y = 1 \Rightarrow x = y = 1$  hoặc  $x \neq 0, y = 0$  nhưng như vậy chúng không là số nguyên tố.

Nếu  $x^y$  chẵn thì  $x$  phải chẵn và do đó  $x = 2$ . Từ đó ta có  $2^y + 1 = z$ .

Nếu  $y$  lẻ thì  $2^y + 1$  là bội của  $2 + 1$  và như vậy  $z = 2^y + 1$  là một hợp số. Bởi vậy  $y$  phải là số chẵn,  $y = 2$ . Khi đó  $z = 5$ .

Vậy  $(x, y, z) = (2, 2, 5)$ .

**35.** Ta nhận xét rằng, nếu  $n$  là một số chính phương thì trong sự phân tích tiêu chuẩn của  $n$ , mỗi một nhân tử đều có dạng lũy thừa bậc chẵn.

Bây giờ giả sử có  $x^2 + y^2 + z^2 = u^2$ .

Nếu trong ba số  $x, y, z$  chỉ có một số chẵn, giả sử là  $z$  thì ta có thể đặt

$$x = 2m + 1, y = 2n + 1, z = 2z.$$

Khi đó

$$u^2 = (2m + 1)^2 + (2n + 1)^2 + (2z)^2 = 4(m^2 + n^2 + z^2 + m + n) + 2 = 2[2(m^2 + n^2 + z^2 + m + n) + 1].$$

Suy ra trong phân tích tiêu chuẩn của  $u^2$ ,  $2$  có lũy thừa bậc lẻ, điều này không thể xảy ra do nhận xét trên.

Nếu  $x, y, z$  đều là lẻ thì

$$x^2 + y^2 + z^2 = u^2$$

sẽ có dạng  $4q + 3$ .

Mặt khác, nếu  $u$  là lẻ thì  $u$  có dạng  $4k \pm 1$ , vì vậy  $u^2$  có dạng  $4t + 1$ . Do đó  $x, y, z$  không thể cùng lẻ.

Vậy trong 3 số  $x, y, z$  có ít nhất là hai số chẵn.

**36.** Trước hết ta có nhận xét rằng nếu  $n = 2s + 1$  với  $s \geq 1$  thì  $a^n + 1$  là hợp số. Thật vậy, khi đó ta có

$$a^{2s+1} + 1 = (a + 1).q \text{ với } q = a^{2s} - a^{2s-1} + \dots + a^2 - a + 1.$$

Do  $s \geq 1$  nên  $q > 1$  và bởi vậy  $a^n + 1$  là hợp số.

Như vậy để  $a^n + 1$  là số nguyên tố thì  $n$  là số chẵn.

Giả sử  $n = n_1.2k$  với  $n_1$  là số lẻ. Khi đó  $n_1 = 1$  vì nếu  $n_1 > 1$  thì  $n_1 = 2s + 1$  với  $s \geq 1$  và

$$a^n + 1 = (a^{2^k})^{2^{s+1}} + 1,$$

do đó theo nhận xét trên  $a^n + 1$  là hợp số. Vậy  $n = 2^k$ .

### §5. Phương trình Đi-ô-phăng $ax + by = c$ (\*)

37. a)  $83x - 79y = 105$ .  $y = \frac{83x - 105}{79} = x - 1 + \frac{2(2x - 13)}{79}$ .

Đặt  $2x - 13 = 79t$ ,  $t \in \mathbb{Z}$  ta có

$$x = \frac{79t + 13}{2} = 39t + 6 + \frac{t + 1}{2}.$$

Đặt  $t + 1 = 2u$ ,  $u \in \mathbb{Z}$  ta có  $t = 2u - 1$ .

Suy ra

$$\begin{cases} x = 79u - 33 \\ y = 83u - 36 \end{cases}$$

b)  $114x - 41y = 5$ .  $y = \frac{114x - 5}{41} = 3x - \frac{9x + 5}{41}$ .

Đặt  $9x + 5 = 41t$ ,  $t \in \mathbb{Z}$  ta có

$$x = \frac{41t - 5}{9} = 4t + \frac{5(t - 1)}{9}.$$

Đặt  $t - 1 = 9u$ ,  $u \in \mathbb{Z}$  ta có  $t = 9u + 1$ .

Suy ra

$$\begin{cases} x = 41u + 4 \\ y = 114u + 11 \end{cases}$$

38. a)  $2x + 3y - 5z = 15$ .  $x = \frac{15 - 3y + 5z}{2} = 7 - y + 2z + \frac{1 - y + z}{2}$ .

Đặt  $1 - y + z = 2t$ ,  $t \in \mathbb{Z}$  ta có

$$\begin{cases} x = z + 3t + 6 \\ y = z - 2t + 1, u \in \mathbb{Z}. \\ z = u \end{cases}$$

b)  $3x + 4y + 5z = 25$ .  $x = \frac{25 - 4y - 5z}{3} = 8 - y - 2z + \frac{1 - y + z}{3}$ .

Đặt  $1 - y + z = 3t$ ,  $t \in \mathbb{Z}$  ta có

$$\begin{cases} x = 4t - 3z + 7 \\ y = z - 3t + 1, u \in \mathbb{Z}. \\ z = u \end{cases}$$

39. a)  $6x - 11y = m + 2$ .  $x = \frac{11y + m + 2}{6} = 2y + \frac{m + 2 - y}{6}$ .

Đặt  $m + 2 - y = 6t$ ,  $t \in \mathbb{Z}$  ta có

$$\begin{cases} x = 2(m + 2) - 11t \\ y = m + 2 - 6t \end{cases}$$

b)  $3x + my = 3$ .

Nếu  $m = 3t$ ,  $t \in \mathbb{Z}$  thì  $x + ty = 1 \Rightarrow x = 1 - ty$ ,  $y$  tùy ý.

Nếu  $m \neq 3t$  thì  $x = \frac{3 - my}{3} = 1 - m \frac{y}{3}$ .

Đặt  $y = 3t$ ,  $t \in \mathbb{Z}$  ta có

$$\begin{cases} x = 1 - mt \\ y = 3t \end{cases}$$



*Nhận xét.* Trong trường hợp  $m \neq 3t$  thì  $m$  và  $3$  nguyên tố cùng nhau,  $d = (m, 3) = 1$ . Do  $(x_0; y_0) = (1; 0)$  là một nghiệm của phương trình nên có thể suy ra ngay dạng tổng quát của nghiệm là:

$$\begin{cases} x = 1 - mt \\ y = 3t \end{cases}, t \in \mathbb{Z}$$

$$c) 3x + (2m - 1)y = m + 1. \quad x = \frac{m+1-(2m-1)y}{3} = -my + \frac{(m+1)(y+1)}{3}.$$

Nếu  $m + 1 = 3t$ ,  $t \in \mathbb{Z}$  thì phương trình đã cho có dạng

$$3x + (6t - 3)y = 3t \text{ hay } x + (2t - 1)y = t.$$

Khi đó nghiệm của phương trình là:

$$\begin{cases} x = -(2t - 1)y + t \\ y \in \mathbb{Z} \end{cases}.$$

Nếu  $m + 1$  không là bội của  $3$  ta đặt  $y + 1 = 3t$ .

Khi đó

$$\begin{cases} x = m + (1 - 2m)t \\ y = -1 + 3t \end{cases} (*)$$

*Nhận xét.* Trong trường hợp  $m + 1$  không chia hết cho  $3$  thì  $(3, m + 1) = 1$ . Do  $(x_0; y_0) = (m; -1)$  là một nghiệm của phương trình nên ta có nghiệm tổng quát là nghiệm  $(*)$  nêu trên.

$$40. a) \begin{cases} x + 2y + 4z = 7 \\ 2x - 5y - 7z = -7 \end{cases}$$

Rút ẩn  $x$  từ phương trình thứ nhất rồi thế vào phương trình thứ hai ta được:  $3y + 5z = 7$ .

Từ đó

$$y = \frac{7 - 5z}{3} = 2 - 2z + \frac{1 + z}{3}.$$

Đặt  $1 + z = 3t$ ,  $t \in \mathbb{Z}$ , ta có

$$\begin{cases} x = -2t + 3 \\ y = -5t + 4 \\ z = 3t - 1 \end{cases}$$

$$b) \begin{cases} 2x + 3y - 5z = 2 \\ 3x - 5y + 2z = 3 \end{cases} \Rightarrow \begin{cases} 6x + 9y - 15z = 6 \\ 6x - 10y + 4z = 6 \end{cases} \text{ trừ từng vế hai phương trình của hệ cuối ta có:}$$

$$19y - 19z = 0 \Rightarrow y = z.$$

Thay vào phương trình thứ nhất của hệ xuất phát ta có

$$2x - 2y = 2 \Rightarrow x = y + 1.$$

Vậy hệ đã cho có nghiệm

$$\begin{cases} x = z + 1 \\ y = z = u \end{cases}, u \in \mathbb{Z}.$$

$$c) \begin{cases} 5x - 5y + 3z = 6 \\ 3x - 2y + 3z = 5 \end{cases} \text{ trừ từng vế hai phương trình của hệ ta được}$$

$$2x - 3y = 1 \Rightarrow x = \frac{1 + 3y}{2} = y + \frac{1 + y}{2}.$$

$$\text{Đặt } 1 + y = 2t, t \in \mathbb{Z}, \text{ ta được } \begin{cases} x = 3t - 1 \\ y = 2t - 1 \end{cases}.$$

Thay giá trị của  $x$  và  $y$  vào hệ xuất phát ta được  $5t + 3z = 6$ . Rõ ràng phải có  $t = 3u$ ,  $u \in \mathbb{Z}$ .

Khi đó  $5u + z = 2 \Rightarrow z = 2 - 5u$ .

Vậy hệ đã cho có nghiệm

$$\begin{cases} x = 9u - 1 \\ y = 6u - 1 \\ z = 2 - 5u \end{cases}$$

41. b) Trước hết ta tìm  $x$  nguyên để  $\frac{7x-1}{5}$  là số nguyên.

$$\text{Ta có } \frac{7x-1}{5} = x + \frac{2x-1}{5}.$$

$$\text{Đặt } 2x - 1 = 5m, m \in \mathbb{Z}, \text{ ta có } x = \frac{5m+1}{2} = 2m + \frac{m+1}{2}.$$

$$\text{Đặt } m + 1 = 2u, u \in \mathbb{Z}, \text{ ta có } m = 2u - 1 \text{ và do đó} \\ x = 5u - 2 \quad (1).$$

$$\text{Mặt khác, } \frac{5x-1}{7} \text{ là số nguyên nếu } 5x - 1 = 7t, t \in \mathbb{Z} \quad (2).$$

$$\text{Thay (1) vào (2) ta được } 25u - 11 = 7t \Rightarrow t = \frac{25u-11}{7} = 3u - 1 + \frac{4(u-1)}{7}.$$

$$\text{Đặt } u - 1 = 7k, k \in \mathbb{Z}, \text{ ta được } u = 1 + 7k. \text{ Từ đó } x = 35k + 3.$$

42. Số  $\overline{xy2}$  chia hết cho 28 có nghĩa là

$$100x + 10y + 2 = 28t, t \in \mathbb{Z} \text{ hay } 50x + 5y + 1 = 14t \Rightarrow y = \frac{14t - 50x - 1}{5} = 3t - 10x - \frac{t+1}{5}.$$

$$\text{Đặt } t + 1 = 5u, u \in \mathbb{Z} \text{ ta có } t = 5u - 1.$$

$$\text{Khi đó } y = 14u - 10x - 3.$$

$$\text{Do } 1 \leq y \leq 9 \text{ nên } 4 \leq 14u - 10x \leq 12 \text{ hay } 2 \leq 7u - 5x \leq 6.$$

Lần lượt thay  $x$  bởi các giá trị từ 1 đến 9 ta nhận được giá trị tương ứng của  $u$  (nếu có) và từ đó suy ra giá trị tương ứng. Cụ thể ta có

$x$	1	2	3	4	5	6	7	8	9
$u$	1	2	3		4	5		6	7
$y$	1	5	9		3	7		1	5

Vậy các số phải tìm là: 112, 252, 392, 532, 672, 812, 952.

Cách 2. Biểu diễn số phải tìm dưới dạng  $\overline{xy2} = 10a + 2, 10 \leq a \leq 99 \quad (1).$

$$\text{Ta có } 10a + 2 = 28t, t \in \mathbb{Z} \text{ hay } 5a + 1 = 14t \Rightarrow a = \frac{14t-1}{5} = 3t - \frac{t+1}{5}.$$

$$\text{Đặt } t + 1 = 5k, k \in \mathbb{Z}, \text{ ta có } t = 5k - 1 \text{ và do đó } a = 3(5k - 1) - k = 14k - 3.$$

Từ điều kiện (1) suy ra  $1 \leq k \leq 7$  và nhận được 7 số phải tìm như cách thứ nhất.

43. Gọi  $a$  là số nguyên phải tìm ta có  $a = 19x + 4 = 11y + 1, x, y \in \mathbb{Z}.$

Từ đó

$$y = \frac{19x+3}{11} = 2x - \frac{3(x-1)}{11}.$$

$$\text{Đặt } x - 1 = 11k, k \in \mathbb{Z}, \text{ ta có } x = 11k + 1 \text{ và do đó } a = 19x + 4 = 209k + 23.$$

44. Gọi số quả cam, quýt, thanh yên theo thứ tự là  $x, 5y, z (x, y, z \in \mathbb{Z})$  ta có

$$\begin{cases} x + 5y + z = 100 & (1) \\ 3x + y + 5z = 60 & (2) \end{cases}$$

Nhân hai vế của (1) với 3 rồi trừ cho (2) ta được  $14y - 2z = 240 \Rightarrow z = 7y - 120.$

Từ (2) suy ra  $0 < 5z < 56 \Leftrightarrow 0 < z \leq 11.$

$$\text{Do đó } 0 < 7y - 120 \leq 11 \Leftrightarrow y = 8.$$

$$\text{Từ đó suy ra } z = 6, x = 4.$$

Vậy số quả cam, quýt, thanh yên theo thứ tự là: 4, 40, 6.