

HƯỚNG DẪN GIẢI BÀI TẬP CHƯƠNG II

§1. Đồng dư thức

45. $100a + 10b + c \equiv 0 \pmod{21} \Leftrightarrow 100a - 105a + 10b + c - 21c \equiv 0 \pmod{21}$

$$\Leftrightarrow -5a + 10b - 20c \equiv 0 \pmod{21}$$

$$\Leftrightarrow -5(a - 2b + 4c) \equiv 0 \pmod{21}$$

$$\Leftrightarrow a - 2b + 4c \equiv 0 \pmod{21} \text{ (do } (5, 21) = 1).$$

46. $10! \equiv 1.2.3.4.5.(-5).(-4).(-3).(-2).(-1) \equiv -(2.3.4.5)^2 \equiv -120^2 \equiv -(-1)^2 \equiv -1 \equiv 10 \pmod{11}$.

Vậy $r = 10$.

47. Theo môđun 13 ta có:

$$4^{2n+1} + 3^{n+2} \equiv 4.16^n + 9.3^n \equiv 4.16^n - 4.3^n \equiv 4(16^n - 3^n) \equiv 4(16 - 3)(16^{n-1} + \dots + 3^{n-1}) \equiv 0 \pmod{13}.$$

48. Với mọi $n \in \mathbb{N}$ ta đặt $x_n = 2^{2^n}$ và dễ dàng kiểm tra rằng $x_0 = 2$ và $x_{n+1} = x_n^2$.

Ta có

$$x_1 \equiv 4 \pmod{7}$$

$$x_2 \equiv 16 \equiv 2 \pmod{7}$$

$$x_3 \equiv 4 \pmod{7}.$$

Bằng qui nạp ta có thể thấy $x_n \equiv 2 \pmod{7}$ với n chẵn và $x_n \equiv 4 \pmod{7}$ với n lẻ.

Từ đó

$$4^{2^n} + 2^{2^n} + 1 \equiv 2^{2^{n+1}} + 2^{2^n} + 1$$

$$\equiv x_{n+1} + x_n + 1$$

$$\equiv 2 + 4 + 1$$

$$\equiv 0 \pmod{7}$$

49. a) Ta có: $51200 \equiv 32 \equiv -9 \pmod{41}$; $(-9)^2 = 81 \equiv -1 \pmod{41}$.

Suy ra $51200^4 \equiv (-9)^4 \equiv (-1)^2 \equiv 1 \pmod{41}$. Do $2^{100} = 4^k$ với k nguyên nào đó nên

$$51200^{2^{100}} = (51200^4)^k \equiv 1 \pmod{41}.$$

b) Ta có: $1035125 \equiv 12 \equiv -5 \pmod{17}$;

$$(-5)^2 = 25 \equiv 8 \pmod{17}; (-5)^4 \equiv 64 \equiv -4 \pmod{17};$$

$$(-5)^8 \equiv 16 \equiv -1 \pmod{17}; (-5)^{16} \equiv (-1)^2 \equiv 1 \pmod{17} \text{ và } 5642 = 16.352 + 8 + 2$$

nên

$$(1035125)^{5642} \equiv (-5)^{5642} \equiv (-5)^8 \cdot (-5)^2 \equiv (-1) \cdot 8 \equiv -8 \equiv 9 \pmod{17}.$$

50. Ta có $1001 = 7.143$, do đó $10^3 \equiv -1 \pmod{7}$ và vì vậy $10^6 \equiv 1 \pmod{7}$.

Bằng qui nạp ta có với mọi số nguyên dương k : $10^k \equiv 4 \pmod{7}$.

Từ đó

$$10^{10^k} \equiv 10^{6m+4} \equiv (10^6)^m \cdot 10^4 \equiv 1 \cdot 10^4 \equiv (-1) \cdot 10 \equiv 4 \pmod{7}.$$

Suy ra

$$\sum_{k=1}^{10} 10^{10^k} \equiv 10 \cdot 4 \equiv 5 \pmod{7}.$$

51. a) Ta có $10^3 = 9.111 + 1$ do đó $10^3 \equiv 1 \pmod{111}$.

Từ đó với số tự nhiên n ta có:

$$10^{6n} + 10^{3n} - 2 \equiv (10^3)^{2n} + (10^3)^n - 2 \equiv 1^{2n} + 1^n - 2 \equiv 0 \pmod{111}.$$

b) Với $\forall n \in \mathbb{N}^*$ ta có:

$$7^{2n+1} - 48n - 7 = 7(49^n - 1) - 48n = 48[7(49^{n-1} + \dots + 49 + 1) - n].$$

Vì $288 = 6.48$ nên điều phải chứng minh tương đương với:

$$7(49^{n-1} + \dots + 49 + 1) - n \equiv 0 \pmod{6} \Leftrightarrow 7(49^{n-1} + \dots + 49 + 1) \equiv n \pmod{6}.$$

Vì $7 \equiv 1 \pmod{6}$ nên ta có

$$7(49^{n-1} + \dots + 49 + 1) \equiv 1 \cdot (1 + \dots + 1 + 1) \equiv n \pmod{6}.$$

52. Giả sử $p = 1093$ không là số nguyên tố.

Gọi q là ước nguyên tố nhỏ nhất của p , vậy thì $1 \leq q^2 \leq p$. Vì $34^2 = 1156 > p$ nên $q \leq 34$.

Mặt khác, p là lẻ nên q là số nguyên tố lẻ.

Vậy q có thể nhận các giá trị: 3, 5, 7, 11, 19, 23, 29, 31.

Các số này không phải là ước của $p = 1093$. Vậy $p = 1093$ là số nguyên tố.

Ta có: $2^{1092} \equiv 2^{6 \cdot 182} \equiv (2^{182})^6 \pmod{p^2}$.

Ta sẽ chứng minh $2^{182} \equiv -1 \pmod{p^2}$.

Thật vậy, vì $182 = 2 \cdot 13 \cdot 7$ nên $2^{182} = ((2^{13})^2)^7$;

$$\begin{aligned} 2^{13} &= 8192 = 7p + 541 \Leftrightarrow 2^{26} = 49p^2 + 1082 \cdot 7p + 541^2 \\ &= 49p^2 + (p-11)7p + 267p + 850 = 49p^2 + 7p^2 + 190p + 850 \\ &= 56p^2 + 191p - 243 = 56p^2 + 191p - 3^5 \end{aligned}$$

Suy ra

$$2^{26} \equiv 191p - 3^5 \pmod{p^2}.$$

Lũy thừa 7 hai vế của đồng dư thức và chú ý là $p^k : p^2$ với mọi $k \geq 2$, ta có:

$$(2^{26})^7 \equiv 7 \cdot 191 \cdot p \cdot (3^5)^6 - (3^5)^7 \pmod{p^2} \Leftrightarrow 2^{182} \equiv 7 \cdot 191 \cdot p \cdot 3^{30} - 3^{35} \pmod{p^2}.$$

Vì $3^7 = 2187 = 1 + 2p$ nên $3^{30} \equiv (3^7)^4 \cdot 3^2 \equiv 3^2 \pmod{p}$.

Do đó

$$7 \cdot 191 \cdot 3^{30} \equiv 7 \cdot 191 \cdot 3^2 \equiv 10 \pmod{p}.$$

Suy ra

$$2^{182} \equiv 10p - (1 + 2p)^5 \equiv 10p - (1 + 5 \cdot 2p) \equiv -1 \pmod{p^2}.$$

Vậy $2^{1092} \equiv (-1)^6 \equiv 1 \pmod{p^2}$.

§2. Vành các lớp thặng dư

53. Do $238 = 12 \cdot 20 - 2$ nên $\overline{238} \pmod{12} \equiv -2 \pmod{12}$.

Mỗi số nguyên thuộc lớp này có dạng $x = -2 + 12t$, $t \in \mathbb{Z}$.

Bởi vậy thặng dư có giá trị tuyệt đối nhỏ nhất là -2.

Đối với lớp thặng dư $\overline{5^{1945}} \pmod{12}$ ta có $5^2 \equiv 1 \pmod{12}$ nên $5^{1945} = (5^2)^{972} \cdot 5 \equiv 5 \pmod{12}$.

Mỗi số nguyên thuộc lớp này có dạng $x = 5 + 12t$, $t \in \mathbb{Z}$.

Bởi vậy thặng dư phải tìm là 5.

54. Ta có $A = \overline{13} \pmod{15} = \{13 + 15t / t \in \mathbb{Z}\} = \{1 + 3(4 + 5t) / t \in \mathbb{Z}\} \subset \overline{1} \pmod{3}$.

Đối với môđun 4 ta có $13 + 15t = (1 - t) + 4(3 + 4t) \in \overline{1-t} \pmod{4}$.

Khi t thay đổi các lớp $\overline{1-t}$ nhận các giá trị khác nhau trong \mathbb{Z}_4 .

Bởi vậy A không là tập con của một lớp thặng dư nào trong \mathbb{Z}_4 .

55. Do 7 là số nguyên tố nên \mathbb{Z}_7 là trường và $\mathbb{Z}_7^* = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

Để thử lại rằng theo môđun 7 ta có

$$\overline{1} = \overline{3^0}; \overline{2} = \overline{3^2}; \overline{3} = \overline{3^1}; \overline{4} = \overline{3^4}; \overline{5} = \overline{3^5}; \overline{6} = \overline{3^3}.$$

Do đó $\mathbb{Z}_7^* = \{\overline{3^k} / k = 0, 1, 2, 3, 4, 5\}$.

56. Ta có:

$$2000 \equiv 5 \pmod{15} \text{ và } \text{UCLN}(5, 15) = 5 \neq 1;$$

$$5181 \equiv 6 \pmod{15} \text{ và } \text{UCLN}(6, 15) = 3 \neq 1;$$

$$291998 \equiv 8 \pmod{15} \text{ và } \text{UCLN}(8, 15) = 1.$$

Suy ra chỉ có lớp $\overline{291998}$ là khả nghịch trong vành \mathbb{Z}_{15} .

57. a) Giả sử $X = \overline{x}$ là nghiệm của $f(X) = \overline{4}X - \overline{2}$.

Khi đó $\overline{4x} = \overline{2}$ hay $4x \equiv 2 \pmod{6} \Leftrightarrow 2x \equiv 1 \pmod{3} \Leftrightarrow x \equiv 2 \pmod{3}$.

Vậy đa thức $f(X)$ có hai nghiệm: $\overline{x} = \overline{2}, \overline{x} = \overline{5} \pmod{6}$.

b) Giả sử $X = \overline{x}$ là nghiệm của $f(X) = \overline{1}X^2 - \overline{2}$ trong \mathbb{Z}_{19} .

Khi đó

$$a^2 + 2 \equiv 0 \pmod{19}.$$

Khi cho a chạy qua hệ thặng dư có giá trị tuyệt đối nhỏ nhất

$$\{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, \pm 6, \pm 7, \pm 8, \pm 9\}$$

ta được $a = \pm 6$. (Do $a^2 + 2 \geq 19$ nên $a^2 \geq 17 \Rightarrow |a| > 4$, vì vậy chỉ cần thử với $|a| \geq 5$).

Vậy $f(X)$ có hai nghiệm $x = \bar{6} \pmod{19}$, $x = \bar{-6} \pmod{19}$.

58. Nếu các số $ax_1 + b, ax_2 + b, \dots, ax_m + b$ lập thành một hệ thặng dư đầy đủ môđun m thì

$$ax_i + b \not\equiv ax_j + b \pmod{m} \text{ với } i \neq j, 1 \leq i, j \leq m.$$

Từ đó suy ra $ax_i \not\equiv ax_j \pmod{m} \Rightarrow x_i \not\equiv x_j \pmod{m}$.

Vậy các số x_1, x_2, \dots, x_m cũng lập thành một hệ thặng dư đầy đủ môđun m.

59. Ta có $1997 \equiv 2 \pmod{15}$.

Bởi vậy có thể chọn một hệ thặng dư thu gọn môđun 15 có chứa 1997 là:

$$\{\pm 1, 1997, -2, \pm 4, \pm 7\}.$$

60. Do a nguyên tố cùng nhau với m và b chia hết cho m nên \bar{a} là phần tử khả nghịch và $\bar{b} = \bar{0}$ trong \mathbb{Z}_m .

Nếu x chạy qua hệ TDTG thì x khả nghịch.

Khi đó $ax + b = \bar{a}x + \bar{b} = \bar{a}x$ cũng khả nghịch, nghĩa là $ax + b$ thuộc một hệ thặng dư thu gọn.

Bây giờ, nếu $((ax_1 + b) - (ax_2 + b)) : m$ thì $a(x_1 - x_2) : m \Rightarrow (x_1 - x_2) : m$.

Điều này chứng tỏ nếu $\bar{x}_1 \neq \bar{x}_2$ thì $\overline{ax_1 + b} \neq \overline{ax_2 + b}$, do đó $ax + b$ chạy qua một hệ thặng dư thu gọn.

61. Khi mỗi x_i chạy qua m_i giá trị của một hệ thặng dư đầy đủ môđun m_i ($i = 1, 2, \dots, k$) thì tổng

$$x = a_1x_1 + a_2x_2 + \dots + a_kx_k \quad (*)$$

chạy qua $m = m_1m_2\dots m_k$ giá trị.

Ta cần chứng tỏ rằng các tổng này thực sự thuộc m lớp khác nhau theo môđun m.

Giả sử $a_1x_1 + a_2x_2 + \dots + a_kx_k = a_1x'_1 + a_2x'_2 + \dots + a_kx'_k \pmod{m}$. Thế thì

$$a_1(x_1 - x'_1) + a_2(x_2 - x'_2) + \dots + a_k(x_k - x'_k) \equiv 0 \pmod{m}$$

$$\Rightarrow a_1(x_1 - x'_1) + a_2(x_2 - x'_2) + \dots + a_k(x_k - x'_k) \equiv 0 \pmod{m_i}$$

với $i = 1, 2, \dots, k$. Do $a_j : m_i, \forall j \neq i$ và $\text{UCLN}(a_i, m_i) = 1$ nên từ đồng dư thức trên ta suy ra

$$a_i(x_i - x'_i) \equiv 0 \pmod{m_i} \Rightarrow x_i - x'_i \equiv 0 \pmod{m_i}, i = 1, 2, \dots, k.$$

Điều này chứng tỏ khi x_i, x'_i thuộc hai lớp đồng dư khác nhau môđun m_i với mỗi i nào đó thì các tổng x, x' tương ứng (lấy theo $(*)$) là thuộc các lớp đồng dư khác nhau theo môđun m. Từ đó suy ra điều phải chứng minh.

62. Trước hết ta thấy với $n = 0$ thì $2^m = 2$ và do đó $(m; n) = (1; 0)$.

Với $n = 1$ thì $2^m = 4$ và do đó $(m; n) = (2; 1)$.

Bây giờ ta sẽ chứng minh không còn cặp số nguyên dương $(m; n)$ nào khác thoả mãn

$$2^m - 3^n = 1 \quad (*).$$

Thật vậy, giả sử $m > 2$ và $n > 1$ là hai số nguyên thoả mãn $(*)$. Khi đó

$$2^m = 9 \cdot 3^{n-2} + 1 \Rightarrow 2^m \equiv 1 \pmod{9}.$$

Cho m chạy qua hệ thặng dư đầy đủ $\{0, 1, 2, \dots, 8\}$ ta thấy chỉ có $2^6 \equiv 2^0 \equiv 1 \pmod{9}$.

Từ đó suy ra

$$2^m \equiv 1 \pmod{9} \Leftrightarrow m = 6k, k \in \mathbb{N}.$$

Do $m > 2$ nên $k \geq 1$. Khi đó $2^m - 1 = (2^6)^k - 1^k = (2^6 - 1) \cdot M$ với $M \in \mathbb{N}^*$.

Do $2^6 - 1 = 63 = 9 \cdot 7$ chia hết cho 7.

Điều này cho thấy $2^m - 1$ không thể là một lũy thừa của 3, mâu thuẫn với $2^m - 1 = 3^n$.

§3. Định lý Ô-le - Định lý Phéc-ma

63. a) Với $3^\alpha 5^\beta 7^\gamma$ và $\varphi(m) = 3600$ ta có

$$\varphi(m) = 3^\alpha \cdot 5^\beta \cdot 7^\gamma \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) = 3^{\alpha-1} \cdot 5^{\beta-1} \cdot 7^{\gamma-1} \cdot 2 \cdot 4 \cdot 6 = 3600$$

$$\Rightarrow 3^{\alpha-1} \cdot 5^{\beta-1} \cdot 7^{\gamma-1} = 75 = 3 \cdot 5^2 \Rightarrow \alpha = 2, \beta = 3, \gamma = 1.$$

b) Với $m = 2^\alpha p$ và $\varphi(m) = 8$ ta có $\varphi(m) = 2^\alpha \cdot p \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{p}\right) = 2^{\alpha-1} \cdot (p-1) = 2^3$.

Xây ra các trường hợp sau:

$\alpha = 1, p - 1 = 8$. Khi đó $p = 9$, loại.

$\alpha = 2, p - 1 = 4$. Khi đó $p = 5$.

$\alpha = 3, p - 1 = 2$. Khi đó $p = 3$.

Đáp số: $m = 2^2 \cdot 5; 2^3 \cdot 3$.

64. Ta đã biết nếu p là số nguyên tố thì $\varphi(p) = p - 1$.

Ngược lại, giả sử rằng $p > 1$ và p là hợp số.

Khi đó p có ước thật sự. Do đó số các số tự nhiên $a, 1 \leq a \leq p - 1$, mà nguyên tố cùng với p là nhỏ hơn $p - 1$ nghĩa là $\varphi(p) < p - 1$.

65. $\alpha \equiv \beta \pmod{\varphi(m)} \Rightarrow \alpha = \beta + t \cdot \varphi(m), t \in \mathbb{Z}$.

Theo định lý Ô-le $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Từ đó

$$a^\alpha = a^\beta \cdot (a^{\varphi(m)})^t \equiv a^\beta \pmod{m}.$$

66. Ta có $240 = 2^4 \cdot 3 \cdot 5$. $\text{UCLN}(a, 240) = 1$ nên $\text{UCLN}(a, 2) = \text{UCLN}(a, 3) = \text{UCLN}(a, 5) = 1$.

Do $\varphi(3) = 2, \varphi(5) = 4$ nên theo định lý Ô-le

$$a^2 \equiv 1 \pmod{3} \Rightarrow a^4 \equiv 1 \pmod{3}, \text{ và } a^4 \equiv 1 \pmod{5}.$$

Mặt khác a lẻ nên $a^4 - 1 = (a - 1)(a + 1)(a^2 + 1)$

là tích của ba số chẵn, trong đó có hai số chẵn liên tiếp, do đó $a^4 - 1$ chia hết cho 16, hay

$$a^4 \equiv 1 \pmod{2^4}.$$

Từ đó suy ra $a^4 \equiv 1 \pmod{2^4 \cdot 3 \cdot 5}$ hay $a^4 - 1$ chia hết cho 240.

67. Chứng minh $(20^{15} - 1) : 11 \cdot 31 \cdot 61$.

Trước hết, $\text{UCLN}(20, 11) = 1$ nên $20^{\varphi(11)} = 20^{10} \equiv 1 \pmod{11}$.

Từ đó $20^{15} \equiv 20^5 \equiv (-2)^5 \equiv 1 \pmod{11}$.

Mặt khác theo môđun 31 ta có

$$20^{15} \equiv (-11)^{15} \equiv 121^7 \cdot (-11) \equiv (-3)^7 \cdot (-11) \equiv 3^6 \cdot 2 \equiv 27^2 \cdot 2 \equiv (-4)^2 \cdot 2 \equiv 1 \pmod{31}.$$

Tương tự theo môđun 61 ta có

$$20 \equiv 81 \equiv 3^4 \pmod{61} \Rightarrow 20^{15} \equiv 3^{60} \equiv 1 \pmod{61} \text{ (theo định lý Ô-le)}.$$

Vậy $20^{15} \equiv 1 \pmod{11 \cdot 31 \cdot 61} \Leftrightarrow 20^{15} - 1 \equiv 0 \pmod{11 \cdot 31 \cdot 61}$ hay $(20^{15} - 1) : 11 \cdot 31 \cdot 61$.

68. a) Theo môđun 83 ta có $3^{40} = (3^4)^{10} \equiv (-2)^4 \equiv 128 \cdot 2^3 \equiv 45 \cdot 2 \cdot 4 \equiv 7 \cdot 4 \equiv 28 \pmod{83}$.

Vậy số dư trong phép chia 3^{40} cho 83 là 28.

b) Giả sử

$$35^{150} = 425q + r, 0 \leq r < 425. \text{ Do } 425 = 5^2 \cdot 17, 35^{150} = (5 \cdot 7)^{150},$$

nên

$$\text{UCLN}(425, 35^{150}) = 5^2.$$

Đặt $r = 5^2 \cdot r'$ ta có $(5 \cdot 49)^{75} = 17q + r', 0 \leq r' < 17$.

Theo môđun 17 ta có

$$(5 \cdot 49)^{75} \equiv 7^{75} \equiv (7^{16})^4 \cdot 7^{11} \equiv 7^{11} \equiv 49^5 \cdot 7 \equiv (-2)^4 \cdot (-14) \equiv 16 \cdot 3 \equiv (-1) \cdot 3 \equiv 14.$$

Vậy $r' = 14$ và do đó $r = 350$.

69. Trước hết ta chứng minh rằng với mọi số nguyên a thì $a^5 - a$ chia hết cho 30.

Thật vậy,

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

Mỗi số hạng của tổng trên chia hết cho 5 và chia hết cho 6 nên tổng chia hết cho 30.

Từ nhận xét trên ta suy ra

$$\sum_{i=1}^n a_i^5 - \sum_{i=1}^n a_i = \sum_{i=1}^n (a_i^5 - a_i)$$

chia hết cho 30. Từ đó suy ra điều phải chứng minh.

70. a) $2^{3^{4n+1}} = 2^{3 \cdot 3^{4n}} = 8^{81^n}$.

Do $\text{UCLN}(8, 11) = 1$ nên $8^{\varphi(11)} = 8^{10} \equiv 1 \pmod{11}$.

Theo môđun 10 ta có

$$81^n \equiv 1^n \equiv 1 \pmod{10} \Rightarrow 81^n = 10k + 1, k \in \mathbb{Z}.$$

Do đó theo môđun 11 ta có $8^{81^n} = 8^{10k+1} = 8^{10k} \cdot 8 \equiv 8 \pmod{11}$.

Từ đó suy ra điều phải chứng minh.

b) Do $\text{UCLN}(2, 23) = 1$ nên $2^{\varphi(23)} = 2^{22} \equiv 1 \pmod{23}$.

Giả sử $2^{10n+1} = 22q + r, 0 \leq r < 22 \Rightarrow 2^{10n} = 11q + r', r = 2r'$.

Do $\text{UCLN}(2, 11) = 1$ nên $2^{\varphi(11)} = 2^{10} \equiv 1 \pmod{11}$.

Vì vậy $2^{10n} \equiv 1 \pmod{11} \Rightarrow r' = 1$.

Từ đó

$$2^{10n+1} = 22q + 2.$$

Theo môđun 23 ta có $2^{2^{10n+1}} \equiv 2^{22q} \cdot 2^2 \equiv 4 \pmod{23}$.

Từ đó suy ra điều cần chứng minh.

c) Do $\text{UCLN}(2, 37) = 1$ nên $2^{\varphi(37)} = 2^{36} \equiv 1 \pmod{37}$. Ta có $2^{6n+2} = 4 \cdot 2^{6n}$.

Theo môđun 9 ta có

$$2^{6n} = (2^6)^n \equiv 1^n \equiv 1 \pmod{9} \Rightarrow 4 \cdot 2^{6n} \equiv 4 \pmod{36}.$$

Do đó $2^{6n+2} = 36k + 4, k \in \mathbb{Z}$ và $2^{2^{6n+2}} = 2^{36k} \cdot 2^4 \equiv 16 \pmod{37}$.

Từ đó suy ra điều phải chứng minh.

71. a) Do $\text{UCLN}(9, 100) = 1$ và $\varphi(100) = 40$ nên $9^{\varphi(100)} = 9^{40} \equiv 1 \pmod{100}$.

Theo môđun 40 ta có

$$9^2 \equiv 1 \pmod{40} \Rightarrow 9^9 = (9^2)^4 \cdot 9 \equiv 9 \pmod{40}.$$

Vậy $9^{9^9} = 9^{40k+9} \equiv 9^9 \pmod{100}$. Theo môđun 100 ta có

$$9^3 \equiv 29, 9^4 \equiv 61, 9^5 \equiv 49 \Rightarrow 9^9 \equiv 61 \cdot 49 \equiv 89 \pmod{100}.$$

b) Trước hết ta viết $14^{14^{14}} = 2^{14^{14}} \cdot 7^{14^{14}}$.

Ta lần lượt tìm số dư trong các phép chia $2^{14^{14}}, 7^{14^{14}}$ cho 100.

Tìm số dư của phép chia $7^{14^{14}}$ cho 100.

Do $\text{UCLN}(7, 100) = 1$ và $\varphi(100) = 40$ nên $7^{\varphi(100)} = 7^{40} \equiv 1 \pmod{100}$.

Theo môđun 40 ta có

$$2^7 = 2^6 \cdot 2 \equiv 24 \cdot 2 \equiv 8 \pmod{40} \Rightarrow 2^{14} \equiv 64 \equiv 24 \pmod{40}.$$

$$7^2 \equiv 9 \pmod{40} \Rightarrow 7^4 \equiv 1 \pmod{40} \Rightarrow 7^{14} = 7^2 \cdot 7^{4 \cdot 3} \equiv 9 \pmod{40}.$$

Suy ra $14^{14} \equiv 24 \cdot 9 \equiv 16 \pmod{40}$. Vậy $7^{14^{14}} = 7^{40k+16} \equiv 7^{16} \equiv 1 \pmod{100}$.

Tìm số dư của phép chia $2^{14^{14}}$ cho 100.

Do $\text{UCLN}(2, 25) = 1$ và $\varphi(25) = 20$ nên $2^{20} \equiv 1 \pmod{25}$.

Theo môđun 20 ta có $14^{14} \equiv 16 \pmod{20}$ (do ở trên ta có $14^{14} \equiv 16 \pmod{40}$).

Bởi vậy theo môđun 25 thì $2^{14^{14}} = 2^{20k+16} \equiv 2^{16} \pmod{25} \Rightarrow 2^{14^{14}} = 25t + 2^{16}, t \in \mathbb{Z}$.

Đẳng thức này chứng tỏ $t = 4t'$ và do đó $2^{14^{14}} \equiv 2^{16} \pmod{100}$.

Có thể tính ngay

$$2^{16} \equiv 36 \pmod{36}.$$

Từ kết quả của hai phần trên ta suy ra $14^{14^{14}} \equiv 36 \pmod{100}$.

72. Vì $42 = 2.3.7$ và 2, 3, 7 là các số đôi một nguyên tố cùng nhau nên điều phải chứng minh tương đương với

$$n^7 \equiv n \pmod{2} \wedge n^7 \equiv n \pmod{3} \wedge n^7 \equiv n \pmod{7}.$$

Vì 7 là nguyên tố nên theo định lý Phéc-ma ta có $n^7 \equiv n \pmod{7}$.

Vì $n \equiv 2 \pmod{2}$ hoặc $n \equiv 1 \pmod{2}$ nên $n^7 \equiv n \pmod{2}$.

Tương tự,

$n \equiv 0 \pmod{3}$ hoặc $n \equiv 1 \pmod{3}$ hoặc $n \equiv -1 \pmod{3}$ nên ta luôn có $n^7 \equiv n \pmod{3}$.

Vậy $n^7 \equiv n \pmod{42}$.

73. Ta thấy a và b không thể cùng chia hết cho 5 vì khi đó $1 = b^2 - 24a^2$ chia hết cho 5.

Giả sử a, b cùng không chia hết cho 5.

Khi đó theo định lý Phéc-ma, $a^4 - 1, b^4 - 1$ là bội của 5 và do đó $a^4 - b^4$ là bội của 5.

Vì $a^4 - b^4 = (a^2 + b^2)(a^2 - b^2)$ nên một trong hai số $(a^2 + b^2)$ và $(a^2 - b^2)$ là bội của 5.

Giả sử $(a^2 + b^2)$ là bội của 5.

Khi đó từ $24a^2 + 1 = b^2$ ta suy ra $25a^2 + 1 = a^2 + b^2$ và do đó $25a^2 + 1$ là bội của 5. Điều này không thể xảy ra.

Vậy $a^2 - b^2$ là bội của 5. Từ $24a^2 + 1 = b^2$ ta có $23a^2 + 1 = b^2 - a^2$, do đó $23a^2 + 1$ là bội của 5.

Vì a khi chia cho 5 có thể cho các số dư là ± 1 hoặc ± 2 nên a^2 chia cho 5 có thể có các số dư là 1 hoặc 4. Do đó $23a^2 + 1$ chia cho 5 dư 4 hoặc 3, nghĩa là $23a^2 + 1$ không thể là bội của 5.

Vậy có một và chỉ một trong các số a và b là bội của 5.

74. Ta có sự phân tích $16320 = 64.3.5.17$. Vì 3, 5, 17 là các số nguyên tố nên theo định lý Phéc-ma ta có:

$$p^2 \equiv 1 \pmod{3} \Rightarrow p^{16} \equiv 1 \pmod{3}; p^4 \equiv 1 \pmod{5} \Rightarrow p^{16} \equiv 1 \pmod{5}; p^{16} \equiv 1 \pmod{17}$$

Do 64, 3, 5, 17 đôi một nguyên tố nên ta chỉ cần chứng minh $p^{16} \equiv 1 \pmod{64}$.

Vì $p > 17$ nên p lẻ, đặt $p = 2k + 1$ ($k \in \mathbb{N}$).

Vậy thì $p^2 = 1 + 4k + 4k^2 = 1 + 4k(k + 1)$. Do $k(k + 1)$ chẵn nên p^2 có dạng $p^2 = 1 + 8h$, với h là một số nguyên nào đó. Khi đó $p^{16} = (1 + 8h)^8$.

Vì $64 = 8^2$ nên $(8h + 1)^8 \equiv 1 + 8.8h \pmod{64} \Rightarrow p^{16} \equiv 1 + 64h \equiv 1 \pmod{64}$.

Vậy $p^{16} - 1 \equiv 0 \pmod{16320}$.

75. Vì $42p = 2.3.7.p$ và $p > 7$ nên để chứng minh $A = (3^p - 2^p - 1) : 42p$ ta chứng minh A chia hết cho 2, 3, 7 và p.

$A = (3^p - 2^p - 1) : 2$ vì $3^p - 1$ là số chẵn. $A = (3^p - 2^p - 1) : 3$ vì $2^p + 1$ chia hết cho $2 + 1 = 3$.

Ngoài ra theo định lý Phéc-ma ta có

$$(3^p - 3) : p \text{ và } (2^p - 2) : p \text{ suy ra } A = (3^p - 3) - (2^p - 2) : p.$$

Ta chỉ còn chứng minh $A : 7$. Ta có

$$\begin{aligned} A &= 3.3^{p-1} - 2^p - 1 = 3.9^{\frac{p-1}{2}} - 2^p - 1 = 3.(2+7)^{\frac{p-1}{2}} - 2^p - 1 = 7k + 3.2^{\frac{p-1}{2}} - 2^p - 1 \\ &= 7k + (2+1)2^{\frac{p-1}{2}} - 2^p - 1 = 7k + 2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1. \end{aligned}$$

Vì $\text{UCLN}(p, 3) = 1$ nên một trong hai số $\frac{p-1}{2}$ và $\frac{p+1}{2}$ phải chia hết cho 3.

Giả sử $\frac{p+1}{2} : 3$. Khi đó $2^{\frac{p+1}{2}} - 1 = (2^3)^m - 1 = 8^m - 1 : 7$.

Ngoài ra $2^p - 2^{\frac{p+1}{2}} = 2^{\frac{p-1}{2}} \left(2^{\frac{p+1}{2}} - 1 \right) \vdots 7$. Do đó $A \vdots 7$.

Trường hợp $\frac{p-1}{2} \vdots 3$, cũng lập luận tương tự ta có $A \vdots 7$. Vậy $A \vdots 42p$.

76. a) Đặt $q = (a^2 - 1)(a^4 - 16) \left[a^2 - (2n+1)^2 \right]^2$.

Vì $23040 = 2^9 \cdot 3^2 \cdot 5$ nên $q \equiv 0 \pmod{23040}$ khi và chỉ khi

$$q \equiv 0 \pmod{2^9} \wedge q \equiv 0 \pmod{3^2} \wedge q \equiv 0 \pmod{5}.$$

Vì $\text{UCLN}(a, 5) = 1$ và 5 là nguyên tố nên theo định lý Phéc-ma ta có

$$a^4 \equiv 1 \pmod{5} \Rightarrow a^4 \equiv 16 \pmod{5} \Rightarrow (a^4 - 16) \equiv 0 \pmod{5} \Rightarrow q \equiv 0 \pmod{5}.$$

Vì $\text{UCLN}(a, 3) = 1$ nên $a = 3k \pm 1, k \in \mathbb{Z}$.

Thay k bởi $3s, 3s \pm 1$ ta được a đồng dư với $\pm 1, \pm 2$ hoặc ± 4 theo mod 9, do đó a^2 đồng dư với 1, 4 hoặc 7 theo mod 9. Ta có

$$(a^2 - 1)(a^4 - 16) = (a^2 - 1)(a^2 - 4)(a^2 + 4).$$

Nếu $a^2 \equiv 1 \pmod{9}$ hoặc $a^2 \equiv 4 \pmod{9}$ thì $(a^2 - 1)(a^4 - 16) \equiv 0 \pmod{9}$.

Nếu $a^2 \equiv 7 \pmod{9}$ thì $(a^2 - 1)(a^4 - 16) \equiv (7 - 1)(49 - 16) \equiv 6 \cdot 33 \equiv 0 \pmod{9}$.

Còn lại phải chứng minh $q \equiv 0 \pmod{2^9}$.

Trước hết với mọi số lẻ, $x = 2k + 1$ ($k \geq 0$) ta có

$$(2k+1)^2 = 4k(k+1) + 1 \equiv 1 \pmod{8} \text{ do } k(k+1) \text{ là số chẵn.}$$

Vì a là số lẻ nên từ nhận xét trên ta có

$$a^2 - (2n+1)^2 \equiv 0 \pmod{8} \Rightarrow (a^2 - 1) \left[a^2 - (2n+1)^2 \right]^2 \equiv 0 \pmod{8} \Rightarrow q \equiv 0 \pmod{2^9}.$$

Vậy $q \equiv 0 \pmod{23040}$.

b) Đặt $q = (a^2 - 1)(a^2 - 9)(a^2 - 49)$.

Cũng như trên ta tìm số dư của q khi chia cho $2^9, 3^2$ và 5.

Ta có

$$q \equiv (a^2 - 1)(a^2 + 1)(a^2 + 1) \pmod{5} \Rightarrow q \equiv (a^4 - 1)(a^2 + 1) \pmod{5}.$$

Theo định lý Phéc-ma ta có

$$a^4 - 1 \equiv 0 \pmod{5}, \text{ suy ra } q \equiv 0 \pmod{5}. \text{ Ta có } q \equiv (a^2 - 1)a^2(a^2 - 1) \pmod{9}.$$

Vì một số nguyên khi chia cho 9 có thể có các số dư là 0, $\pm 1, \pm 2, \pm 3, \pm 4$, nên bình phương của nó khi chia cho 9 có thể có số dư là 0, 1, 4 hoặc 7.

Nếu a^2 chia cho 9 dư 0, 1 hoặc 4 thì $q \equiv 0 \pmod{9}$.

Nếu $a^2 \equiv 7 \pmod{9}$ thì $q \equiv (7 - 1) \cdot 7 \cdot (7 - 4) \equiv 0 \pmod{9}$.

Vậy $q \equiv 0 \pmod{9}$.

Bây giờ, tương tự câu a) ta có $a^2 \equiv 1 \pmod{8}$. Đặt $a^2 = 8h + 1$, khi đó

$$q = 8h(8h - 8)(8h - 48) = 8^3 h(h - 1)(h - 6).$$

Vì $8^3 = 2^9$ nên $q \equiv 0 \pmod{2^9}$.

Vậy $q \equiv 0 \pmod{23040}$.