20. ĐỊNH LÝ THẶNG DƯ TRUNG HOA

20.1. GIỚI THIỆU

Chúng ta xét bài toán mở đầu sau. Giải hệ phương trình đồng dư

$$\begin{cases} x \equiv 3 (\mod 5) & (1) \\ x \equiv 7 (\mod 8) & (2) \\ x \equiv 5 (\mod 7) & (3). \end{cases}$$

Giải. Từ đồng dư (1) ta có

$$x = 5q_1 + 3. \quad (4)$$

Thay kết quả (4) trên vào đồng dư (2) ta được

$$5q_1 + 3 \equiv 7 (\mod 8) \Rightarrow 5q_1 \equiv 4 (\mod 8).$$

Do $5.5 = 25 \equiv 1 (\mod 8)$ và $(5,8) = 1$ nên

$$5.5q_1 \equiv 5.4 (\mod 8) \Rightarrow q_1 \equiv 4 (\mod 8) \Rightarrow q_1 = 8q_2 + 4.$$

Từ đó (4) cho ta $x = 5(8q_2 + 4) + 3 = 40q_2 + 23$ (5). Thay (5) vào (3) ta được

$$40q_2 + 23 \equiv 5 (\mod 7) \Rightarrow 40q_2 \equiv -18 (\mod 7) \Rightarrow 5q_2 \equiv 3 (\mod 7).$$

Vì $3.5 = 15 \equiv 1 (\mod 7)$ và $(3,7) = 1$ nên

$$3.5q_2 \equiv 3.3 (\mod 7) \Rightarrow 15q_2 \equiv 9 (\mod 7) \Rightarrow q_2 \equiv 2 (\mod 7) \Rightarrow q_2 = 7q_3 + 2.$$

Lại thay kết quả trên vào (5) ta được

$$x = 40(7q_3 + 2) + 23 = 280q_3 + 103 \Rightarrow x \equiv 103 (\mod 280).$$

Để ý $280 = 5 \times 8 \times 7$. Tức hệ phương trình trên có nghiệm

$$x \equiv 103 (\mod 5 \times 8 \times 7).$$

□

20.2. ĐỊNH LÝ

Định lý 20.2.1. *Cho k số nguyên dương đôi một nguyên tố cùng nhau $m_1, m_2, \ldots, m_k$, và $a_1, a_2, \ldots, a_k$ là k số nguyên tùy ý. Khi đó hệ đồng dư tuyến tính*

$$\begin{cases} x \equiv a_1 (\mod m_1) \\ x \equiv a_2 (\mod m_2) \\ \ldots\ldots\ldots \\ x \equiv a_k (\mod m_k) \end{cases}$$

có nghiệm duy nhất mod $m_1 m_2 \ldots m_k$.

Chứng minh. 1. *Chứng minh sự duy nhất*. Giả sử ta có hai nghiệm là x, y. Dẫn đến

$$x \equiv y(\equiv a_1(\bmod m_1)), \quad x \equiv y(\equiv a_2(\bmod m_2)), \ldots, x \equiv y(\equiv a_k(\bmod m_k)).$$

Vì $m_1, m_2, \ldots, m_n$ nguyên tố cùng nhau đôi một nên

$$x \equiv y(\bmod m_1 m_2 \ldots m_k).$$

Tức y và x cùng thuộc một lớp thặng dư theo mod $m_1 m_2 \ldots m_k$

2. *Chứng minh sự tồn tại*. Ta muốn viết các nghiệm như là một tổ hợp tuyến tính của các $a_1, a_2, \ldots, a_k$

$$x = A_1 a_1 + A_2 a_2 + \cdots + A_k a_k.$$

Với các A_i phải tìm thỏa mãn

$$A_j \equiv 0(\bmod m_i), \forall j \neq i \quad \text{và} \quad A_i \equiv 1(\bmod m_i).$$

Đặt

$$\begin{aligned} N_1 &= m_2 m_3 \ldots m_k \\ N_2 &= m_1 m_3 \ldots m_k \\ &\ldots\ldots\ldots \\ N_i &= m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k. \end{aligned}$$

Khi đó $(N_i, m_i) = 1$ vì $(m_i, m_1) = (m_i, m_2) = \ldots = (m_i, m_{i-1}) = (m_i, m_{i+1}) = \ldots = (m_i, m_k) = 1$ và $m_j | N_i, \forall j \neq i$. Vì $(N_i, m_i) = 1$ nên tồn tại N_i^{-1}, tức là

$$N_i . N_i^{-1} \equiv 1(\bmod m_i).$$

Đến đây đặt

$$A_i = N_i . N_i^{-1}$$

thì

$$A_i \equiv 1(\bmod m_i) \quad \text{và} \quad A_i \equiv 0(\bmod m_j), \forall j \neq i (\text{vì } N_i \equiv 0(\bmod m_j) \Rightarrow A_i \equiv 0(\bmod m_j)).$$

Khi đó

$$x = A_1 a_1 + A_2 a_2 + \cdots + A_k a_k = N_1 . N_1^{-1} a_1 + N_2 N_2^{-1} a_2 + \cdots + N_k N_k^{-1} a_k$$

sẽ thỏa mãn

$$x \equiv N_i N_i^{-1} a_i \equiv a_i(\bmod m_i)$$

(vì tất cả các thừa số còn lại đều đồng dư 0 do $m_i | N_j, \forall j \neq i$).

□

20.3. ÁP DỤNG CƠ BẢN

Ví dụ 20.3.1. *Giải hệ phương trình đồng dư*

$$\begin{cases} x \equiv 2(\bmod 3) \\ x \equiv 3(\bmod 5) \\ x \equiv 5(\bmod 7). \end{cases}$$

Giải. Ta có

$$N_1 = 5.7 = 35 \equiv 2(\bmod 3) \Rightarrow N_1^{-1} = 2,$$
$$N_2 = 3.7 = 21 \equiv 1(\bmod 5) \Rightarrow N_2^{-1} = 1,$$
$$N_3 = 3.5 = 15 \equiv 1(\bmod 7) \Rightarrow N_3^{-1} = 1.$$

Từ đó ta có

$$x = 2.35.2 + 1.21.3 + 1.15.5 = 278 \equiv 68(\bmod 105)$$

là nghiệm của hệ phương trình. □

Ví dụ 20.3.2. *Giải hệ phương trình*

$$\begin{cases} x \equiv 6(\bmod 11) \\ x \equiv 13(\bmod 16) \\ x \equiv 9(\bmod 21) \\ x \equiv 19(\bmod 25). \end{cases}$$

Chứng minh. Ta có

$$N_1 = 16.21.25 = 8400 \equiv 7(\bmod 11) \Rightarrow N_1^{-1} = 8,$$
$$N_2 = 11.21.25 = 5775 \equiv 15(\bmod 16) \Rightarrow N_2^{-1} = 15,$$
$$N_3 = 11.16.25 = 4400 \equiv 11(\bmod 21) \Rightarrow N_3^{-1} = 2,$$
$$N_4 = 11.16.21 = 3696 \equiv 21(\bmod 25) \Rightarrow N_4^{-1} = 6.$$

Khi đó nghiệm của hệ phương trình là

$$x = 6.8400.8 + 13.5775.15 + 9.4400.2 + 19.3696.6 = 2029869 \equiv 51669(\bmod 11.16.21.25 = 92400).$$

□

Ví dụ 20.3.3. *Tìm tất cả các nghiệm của phương trình* $x^2 \equiv 1(\bmod 144)$.

Chứng minh. Vì $144 = 16.9$, và $(16,9) = 1$. Do đó theo định lý thặng dư Trung Hoa thì nghiệm của bài toán chính là nghiệm của hệ phương trình

$$\begin{cases} x \equiv 1(\bmod 16) \\ x \equiv 1(\bmod 9). \end{cases}$$

Vì $x^2 \equiv 1(\mod 16)$ có 4 nghiệm $x \equiv \pm 1, \pm 7(\mod 16)$ và $x^2 \equiv 1(\mod 9)$ có hai nghiệm $x \equiv \pm 1(\mod 9)$. Do đó ta có tất cả 8 trường hợp xảy ra

$$x \equiv 1(\mod 16) \quad \text{và} \quad x \equiv 1(\mod 9) \quad (1),$$

$$x \equiv 1(\mod 16) \quad \text{và} \quad x \equiv -1(\mod 9) \quad (2),$$

$$x \equiv -1(\mod 16) \quad \text{và} \quad x \equiv 1(\mod 9) \quad (3),$$

$$x \equiv -1(\mod 16) \quad \text{và} \quad x \equiv -1(\mod 9) \quad (4),$$

$$x \equiv 7(\mod 16) \quad \text{và} \quad x \equiv 1(\mod 9) \quad (5),$$

$$x \equiv 7(\mod 16) \quad \text{và} \quad x \equiv -1(\mod 9) \quad (6),$$

$$x \equiv -7(\mod 16) \quad \text{và} \quad x \equiv 1(\mod 9) \quad (7),$$

$$x \equiv -7(\mod 16) \quad \text{và} \quad x \equiv -1(\mod 9) \quad (8).$$

Cả tám hệ phương trình trên đều ứng với $k = 2$ và

$$N_1 = 9 \equiv 9(\mod 16) \Rightarrow N_1^{-1} = 9 \Rightarrow N_1.N_1^{-1} = 81,$$

$$N_2 = 16 \equiv 7(\mod 9) \Rightarrow N_2^{-1} = 4 \Rightarrow N_2.N_2^{-1} = 64.$$

Do đó phương trình ban đầu có tất cả 8 nghiệm sau

$$\begin{aligned}
&(1): x \equiv 1.81 + 1.64 = 145 && \equiv 1(\mod 144),\\
&(2): x \equiv 1.81 + (-1).64 = 17 && \equiv 17(\mod 144),\\
&(3): x \equiv (-1).81 + 1.64 = -17 && \equiv -17(\mod 144),\\
&(4): x \equiv (-1).81 + (-1).64 = -145 && \equiv -1(\mod 144),\\
&(5): x \equiv 7.81 + 1.64 = 631 && \equiv 55(\mod 144),\\
&(6): x \equiv 7.81 + (-1).64 = 503 && \equiv 71(\mod 144),\\
&(7): x \equiv (-7).81 + 1.64 = -503 && \equiv -71(\mod 144),\\
&(8): x \equiv (-7).81 + (-1).64 = -603 && \equiv -55(\mod 144).
\end{aligned}$$

□

20.4. CHỨNG MINH SỰ TỒN TẠI MỘT MỆNH ĐỀ TOÁN HỌC

Bài 20.4.1. Cho a, b là hai số nguyên dương lớn hơn 1, $(a,b) = 1$. Chứng minh rằng tồn tại $k \in \mathbb{Z}$ sao cho

$$A = (ab-1)^n.k + 1$$

là hợp số với mọi n nguyên dương.

Phân tích và giải. 1. *Để chứng minh A là hợp số, thì cần chứng minh A chia hết cho một số nào đó. Tự nhiên nhất trong bài này là chứng minh luôn A chia hết cho a hoặc chia hết cho b.* Xét theo mod a thì

$$\begin{cases} A \equiv k+1(\mod a) & \text{với } n \text{ chẵn} \\ A \equiv -k+1(\mod a) & \text{với } n \text{ lẻ}. \end{cases}$$

2. *Khi đó cần $A\vdots a$ thì cần điều kiện gì của k?* Để $A\vdots a$ thì

$$\begin{cases} k \equiv -1 (\bmod a) & \text{với } n \text{ chẵn} \\ k \equiv 1 (\bmod a) & \text{với } n \text{ lẻ.} \end{cases}$$

3. *Hoàn toàn tương tự cho điều kiện của k để muốn $A\vdots b$??* Tương tự để $A\vdots b$ thì

$$\begin{cases} k \equiv -1 (\bmod b) & \text{với } n \text{ chẵn} \\ k \equiv 1 (\bmod b) & \text{với } n \text{ lẻ.} \end{cases}.$$

4. *Từ đây, để đảm bảo A luôn chia hết cho cả a hoặc b ứng với n chẵn hoặc n lẻ, thì phải chọn k như thế nào?* Theo định lý thặng dư Trung hoa thì hệ

$$\begin{cases} k \equiv 1 (\bmod a) \\ k \equiv -1 (\bmod b) \end{cases}$$

có nghiệm.

5. *Kiểm tra lại thông tin của A ứng với k chọn là nghiệm của hệ trên?* Khi đó

$$\begin{cases} A\vdots a & \text{với } n \text{ lẻ} \\ A\vdots b & \text{với } n \text{ chẵn} \end{cases}$$

Ta có điều phải chứng minh.

□

Bài 20.4.2. Chứng minh rằng với mọi số nguyên dương n tùy ý, luôn tồn tại n số nguyên dương liên tiếp gồm toàn hợp số.

Phân tích và giải. 1. *Để chứng minh n số nguyên dương liên tiếp gồm toàn hợp số, thì ta phải chứng minh mỗi số trong n số này phải có một ước nguyên tố. Từ đó cần phải bắt đầu từ đâu?* Gọi $p_1 < p_2 < \ldots < p_n$ là n số nguyên tố tùy ý.

2. *Ta muốn n số dạng: $m+1, m+2, \ldots, m+n$, mỗi số chia hết cho một thừa số nguyên tố trên? Hãy triển khai chi tiết này?* Ta chỉ ra tồn tại số m mà

$$\begin{cases} m+1 \equiv 0 (\bmod p_1) \\ m+2 \equiv 0 (\bmod p_2) \\ \ldots\ldots\ldots \\ m+n \equiv 0 (\bmod p_n) \end{cases} \Leftrightarrow \begin{cases} m \equiv -1 (\bmod p_1) \\ m \equiv -2 (\bmod p_2) \\ \ldots\ldots\ldots \\ m \equiv -n (\bmod p_n). \end{cases}$$

Theo định lý thặng dư Trung Hòa thì hệ trên có nghiệm m lớn tùy ý. Từ đó với mọi $i = 1, 2, \ldots, n$ thì

$$p_i | m+i.$$

(*tuy nhiên vì $p_i|m+i$ nên có thể $m+i=p_i$, lúc đó thì $m+i$ lại là số nguyên tố. Để đảm bảo $m+i$ là hợp số thì ta chọn m sao cho $m>p_n$ là được*). Ta chọn $m>p_n$ thì n số

$$m+1, m+2, \ldots, m+n$$

đều là hợp số (mỗi số $m+i$ chia hết cho một ước nguyên tố p_i).

□

Bài 20.4.3 (**IMO 1989**)**.** Chứng minh rằng với mọi số nguyên dương n tùy ý, luôn tồn tại n số nguyên dương liên tiếp mà mỗi số không là lũy thừa của một số nguyên dương nào khác.

Phân tích và giải. 1. *Nhìn bài toán này, ta nghĩ ngay đến một sự tương tự với bài 20.2. Tuy nhiên đối với bài 20.2 chứng minh mỗi số đó là hợp số. Còn trong bài toán này chứng minh mỗi số không là lũy thừa của một số nguyên dương. Mượn ý tưởng của bài trên, từ hợp số đến không là lũy thừa, ta lưu ý điều gì?* Một số nguyên a chia hết cho số nguyên tố p, nhưng không chia hết cho p^2 thì a không là lũy thừa của một số nguyên.

2. Gọi $p_1<p_2<\ldots<p_n$ là n số nguyên tố tùy ý. *Ta muốn n số dạng: $m+1, m+2, \ldots, m+n$, mỗi số $m+i$ chia hết cho một thừa số nguyên tố p_i, nhưng không được chia hết cho p_i^2. Từ đó xây dựng đồng dư như thế nào?* Ta chỉ ra tồn tại số m mà

$$\begin{cases} m+1\equiv p_1 (\bmod p_1^2) \\ m+2\equiv p_2 (\bmod p_2^2) \\ \ldots\ldots\ldots \\ m+n\equiv p_n (\bmod p_n^2) \end{cases} \Leftrightarrow \begin{cases} m\equiv p_1-1 (\bmod p_1^2) \\ m\equiv p_2-2 (\bmod p_2^2) \\ \ldots\ldots\ldots \\ m\equiv p_n-n (\bmod p_n^2). \end{cases}$$

Theo định lý thặng dư Trung Hòa thì hệ trên có nghiệm m lớn tùy ý, chọn $m>p_n$. Từ đó với mọi $i=1,2,\ldots,n$ thì

$$p_i|m+i \quad \text{nhưng} \quad p_i^2 \nmid m+i.$$

Chứng tỏ n số liên tiếp $m+1, m+2, \ldots, m+n$ đều không là lũy thừa của một số nguyên nào đó.

□

Cách 2. Với mỗi $m\in\mathbb{Z}^+$, xét $2n$ số nguyên tố phân biệt $p_1, p_2, \ldots, p_n, q_1, q_2, \ldots, q_n$ và hệ phương trình đồng dư

$$\begin{cases} x\equiv -1 (\bmod p_1q_1) \\ x\equiv -2 (\bmod p_2q_2) \\ \ldots\ldots\ldots \\ x\equiv -n (\bmod p_nq_n). \end{cases}$$

Theo định lý thặng dư Trung Hoa thì hệ trên có nghiệm. Tức là tồn tại $m\in\mathbb{Z}$ sao cho

$$m\equiv -i (\bmod p_iq_i), \forall i=1,2,\ldots,n.$$

Từ đó suy ra các số $m+1, m+2, \ldots, m+n$ là n số nguyên liên tiếp và không có số nào là lũy thừa của một số nguyên nào cả (vì trong phân tích của mỗi số đó có ít nhất hai thừa số nguyên tố). □

Bài 20.4.4. Chứng minh rằng với mỗi số tự nhiên n, tồn tại một cấp số cộng gồm n số hạng sao cho mọi số hạng của nó đều là lũy thừa của một số tự nhiên với số mũ lớn hơn 1.

Phân tích và giải. 1. *Việc chỉ ra một cấp số cộng nào là khó. Do đó việc đầu tiên là nghĩ đến chọn cấp số cộng nào cho dễ kiểm tra. Cấp số cộng đơn giản nhất là* $1,2,\ldots,n$. *Tuy nhiên dãy này không thỏa. Do đó ta nghĩ đến chọn cấp số cộng "tương tự như trên" là* $a,2a,3a,\ldots,na$.

2. *Vì mong muốn* $a,2a,\ldots,na$ *là lũy thừa của một số tự nhiên. Do đó số* a *cần sự xuất hiện của các hạng tử* $2,3,\ldots,n$ *trong biểu diễn, tức cần có dạng*

$$a = 2^{k_2}3^{k_3}4^{k_4}\ldots n^{k_n}.$$

(ở đây đánh chỉ số của k *theo số hạng trong cơ số)*

3. *Để* a *là lũy thừa của một số nguyên tố, thì các lũy thừa* $k_2,k_3,\ldots,k_n$ *phải có nhân tử chung, nhân tử chung này tự nhiên nhất là nhân tử nguyên tố chung* p_2, *tức là cần*

$$\begin{cases} k_2 \vdots p_2 \\ k_3 \vdots p_2 \\ \ldots\ldots \\ k_n \vdots p_2. \end{cases}$$

4. *Khi đó* $2a = 2^{k_2+1}3^{k_3}4^{k_4}\ldots n^{k_n}$, *để* $2a$ *là lũy thừa của một số nguyên tố, thì các lũy thừa* $k_2+1,k_2,\ldots,k_n$ *phải có nhân tử nguyên tố chung* p_3, *tức là cần*

$$\begin{cases} k_2+1 \vdots p_3 \\ k_3 \vdots p_3 \\ \ldots\ldots \\ k_n \vdots p_3. \end{cases}$$

5. *Cứ tiếp tục tìm điều kiện cho các số* $2a,3a,\ldots,na$ *là lũy thừa của một số nguyên, thì điều kiện cho các lũy thừa* $k_2,k_3,\ldots,k_n$ *là gì?* Như phân tích ở trên thì cần có

$$\begin{array}{rrrrrr} k_2 \vdots p_2, & k_3 \vdots p_2, & k_4 \vdots p_2, & k_5 \vdots p_2, & \ldots, & k_n \vdots p_2, \\ k_2+1 \vdots p_3, & k_3 \vdots p_3, & k_4 \vdots p_3, & k_5 \vdots p_3, & \ldots, & k_n \vdots p_3, \\ k_2 \vdots p_4, & k_3+1 \vdots p_4, & k_4 \vdots p_4, & k_5 \vdots p_4, & \ldots, & k_n \vdots p_4, \\ \ldots, & \ldots, & \ldots, & \ldots, & \ldots, & \ldots \end{array}$$

6. Từ đó các số $k_2,k_3,\ldots,k_n$ tồn tại theo định lý thặng dư Trung Hoa. Với mọi $i=3,\ldots,n$ tồn tại số nguyên dương k_i thỏa mãn

$$\begin{cases} k_{i-1} \equiv -1 (\bmod p_i) \\ k_i \equiv 0 (\bmod p_j), j \neq i, j \in \{3,\ldots,n\}. \end{cases}$$

và

$$k_i \vdots p_2, \forall i = 2,3,\ldots,n.$$

Khi đó thì

$$a = 2^{k_2}3^{k_3}\ldots n^{p_n} = \left(2^{\frac{k_2}{p_2}}.2^{\frac{k_3}{p_2}}\ldots n^{\frac{k_n}{p_2}}\right)^{p_2}$$
$$2a = 2^{k_2+1}3^{k_3}\ldots n^{p_n} = \left(2^{\frac{k_2+1}{p_3}}.2^{\frac{k_3}{p_3}}\ldots n^{\frac{k_n}{p_3}}\right)^{p_3}$$
$$\ldots\ldots\ldots\ldots$$
$$na = 2^{k_2}3^{k_3}\ldots n^{p_n+1} = \left(2^{\frac{k_2}{p_n}}.2^{\frac{k_3}{p_n}}\ldots n^{\frac{k_n+1}{p_n}}\right)^{p_n}.$$

Ta có điều phải chứng minh. □

Bài 20.4.5 (**Bankal 2000**). Cho A là một tập con khác rỗng của $\mathbb{Z}^+$. Chứng minh rằng tồn tại số nguyên dương n sao cho tập hợp

$$nA = \{nx | x \in A\}$$

chứa toàn lũy thừa của một số tự nhiên với số mũ lớn hơn 1.

Giải. Bài toán này tương tự như bài 20.4. Do đó lời giải tương tự. Đặt

$$A = \{a_1, a_2, \ldots, a_k\}$$

và

$$p_1, p_2, \ldots, p_k$$

là k số nguyên tố phân biệt. Theo định lý thặng dư Trung Hoa, với mọi $i = 1,2,\ldots,k$, tồn tại số nguyên dương m_i thỏa mãn

$$\begin{cases} m_i \equiv -1 (\bmod p_i) \\ m_i \equiv 0 (\bmod p_j) (j \neq i, j \in \{1,2,\ldots,k\}). \end{cases}$$

Khi đó

$$\begin{array}{llll} m_1+1 \vdots p_1, & m_2 \vdots p_1, & \ldots, & m_k \vdots p_1, \\ m_1 \vdots p_2, & m_2+1 \vdots p_2, & \ldots, & m_k \vdots p_2, \\ \ldots, & \ldots, & \ldots, & m_k \vdots p_1, \\ m_1 \vdots p_k, & m_2 \vdots p_k, & \ldots, & m_k+1 \vdots p_k. \end{array}$$

Đến đây đặt

$$n = a_1^{m_1}a_2^{m_2}\ldots a_k^{m_k}$$

ta có

$$na_1 = a_1^{m_1+1}a_2^{m_2}\dots a_k^{m_k} = \left(a_1^{\frac{m_1+1}{p_1}}a_2^{\frac{m_2}{p_1}}\dots a_k^{\frac{m_k}{p_1}}\right)^{p_1}$$
$$na_2 = a_1^{m_1}a_2^{m_2+1}\dots a_k^{m_k} = \left(a_1^{\frac{m_1}{p_2}}a_2^{\frac{m_2+1}{p_2}}\dots a_k^{\frac{m_k}{p_2}}\right)^{p_2}$$
$$\dots\dots\dots$$
$$na_k = a_1^{m_1}a_2^{m_2}\dots a_k^{m_k+1} = \left(a_1^{\frac{m_1}{p_k}}a_2^{\frac{m_2}{p_k}}\dots a_k^{\frac{m_k+1}{p_k}}\right)^{p_k}$$

□

Bài 20.4.6. Chứng minh rằng với mọi số nguyên n, tồn tại một tập số nguyên n phần tử để tổng các phần tử của các tập con không rỗng của nó là 1 lũy thừa.

Giải. Ta sét tập số nguyên $S = \{x_1, x_2, \dots, x_n\}$, tập S có $2^n - 1$ tập con không rỗng của S. Đặt

$$S_1, S_2, \dots, S_{2^n-1}$$

là tổng các phần tử của các tập này. Áp dụng bài 20.5, tồn tại số nguyên b thỏa mãn

$$\{bS_1, bS_2, \dots, bS_{2^n-1}\}$$

bao gồm toàn các lũy thừa. Từ đó ta chọn tập

$$F = \{bx_1, bx_2, \dots, bx_n\}$$

thì tập F thỏa mãn điều kiện bài toán. □

Bài 20.4.7. Chứng minh rằng với mọi số tự nhiên n, luôn tồn tại n số tự nhiên liên tiếp sao cho bất kỳ số nào cũng có ước dạng $2^k - 1, k \in \mathbb{N}$.

Phân tích giải.

1. Gọi n số nguyên liên tiếp là $x+1, x+2, \dots, x+n$. Yêu cầu bài toán giúp ta nghĩ đến hệ thặng dư
$$\begin{cases} x \equiv -1 (\bmod p_1) \\ x \equiv -2 (\bmod p_2) \\ \dots\dots \\ x \equiv -n (\bmod p_n) \end{cases}$$
Từ đây dẫn đến việc chọn $p_1, p_2, \dots, p_n$.
2. Nếu p_i là các số nguyên tố thì rất khó kiểm soát điều kiện $2^k - 1$, nên ta chọn luôn p_i là các số Mersen $p_i = 2^{k_i} - 1$ (p_i không cần nguyên tố).
3. Để đảm bảo $(p_i, p_j) = 1$ dẫn đến việc chọn k_i, k_j.

4. Mặt khác
$$\left(2^{k_i}-1,2^{k_j}-1\right)=1\Leftrightarrow(k_i,k_j)=1$$
(thật vậy, nếu gọi q là ước nguyên tố chung của $2^{k_i}-1,2^{k_j}-1$ thì
$$\begin{cases}2^{k_i}\equiv 1(\bmod q)\\ 2^{k_j}\equiv 1(\bmod q)\end{cases}\Rightarrow 2^{(k_i,k_j)}\equiv 1(\bmod q)\Rightarrow q=1\Leftrightarrow(k_i,k_j)=1.$$
)

5. Từ các nhận xét trên, ta dễ dàng chọn được $k_1,k_2,\ldots,k_n$ thỏa $(k_i,k_j)=1,\forall i,j=1,2,\ldots,n(i\neq j)$ (có thể chọn luôn k_i là số nguyên tố thứ i).

□

Bài 20.4.8. Cho n là số nguyên dương lẻ và $n>3$. Gọi k,t là các số nguyên dương nhỏ nhất sao cho $kn+1$ và tn đều là số chính phương. Chứng minh rằng điều kiện cần và đủ để n là số nguyên tố là
$$\min\{k,t\}>\frac{n}{4}.$$

1. Điều kiện cần: Giả sử n nguyên tố. Khi đó
$$n|tn \text{ và } tn \text{ chính phương nên } n^2|tn\Rightarrow n|t.$$
Từ đó
$$t\geq n>\frac{n}{4}.$$
Hơn nữa đặt $a^2=kn+1$ thì $a^2\equiv 1(\bmod n)$. Kết hợp n nguyên tố nên $a\equiv\pm 1(\bmod n)$. Nhưng vì $a>1$ nên $a\geq n-1$ (vì $n-1$ là số nhỏ nhất đồng -1 modulo n). Dẫn đến
$$kn+1\geq(n-1)^2\Rightarrow k\geq n-2\Rightarrow k>\frac{n}{4}\text{ vì } n>3 \text{ nên } n-2>\frac{n}{3}.$$

2. Điều kiện đủ

- n chỉ có một ước nguyên tố duy nhất, đặt $n=p^\alpha$, với $p\geq 3$ do n lẻ. Nếu α chẵn, ta lấy
$$t=1<\frac{n}{4}$$
thì
$$tn=p^\alpha$$
là số chính phương, mâu thuẫn với giả thiết. Nếu α lẻ, $\alpha\geq 3$, ta lấy
$$t=p<\frac{p^\alpha}{4}=\frac{n}{4}$$
thì
$$tn=p^{\alpha+1},\alpha+1 \text{ chẵn}$$
nên tn là số chính phương với $t<\frac{n}{4}$, mâu thuẫn. Vậy $\alpha=1$ hay n là số nguyên tố.

- Nếu n có ít nhất hai ước nguyên tố phân biệt. Khi đó ta có thể n dưới dạng $n = p^{\alpha}.m$, trong đó p là một số nguyên tố lẻ, m là số nguyên dương lẻ, $(m,p) = 1$. Theo định lý thặng dư Trung Hoa, tồn tại số nguyên s sao cho

$$\begin{cases} s \equiv 1 (\bmod p^{\alpha}) \\ s \equiv -1 (\bmod m). \end{cases}$$

Từ đó $n|s^2 - 1$. Hơn nữa ta có thể chọn s sao cho

$$|s| \leq \frac{n}{2}.$$

Vì $s \not\equiv 1 (\bmod m)$ nên $s \neq 1$ và $s \not\equiv -1 (\bmod p^{\alpha})$ nên $s \neq -1$. Dẫn đến $s^2 \neq 1$. Từ đây lấy

$$k = \frac{s^2 - 1}{n}$$

thì k là số nguyên dương, hơn nữa $kn + 1 = s^2$ là số chính phương và

$$k = \frac{s^2 - 1}{n} < \frac{s^2}{n} \leq \frac{\frac{n^2}{4}}{n} = \frac{n}{4}$$

mâu thuẫn với điều kiện

$$\min\{k,t\} > \frac{n}{4}.$$

Vậy trường hợp này không thể xảy ra.

Từ đó n phải là số nguyên tố.

20.5. ĐỊNH LÝ THẶNG DƯ TRUNG HOA VÀ SỐ FERMAT

Bài 20.5.1. Chứng minh rằng tồn tại số nguyên k sao cho $2^n.k + 1$ là hợp số với mọi số nguyên dương n.

Phân tích giải. 1. Xét n viết dưới dạng $n = 2^m.l$, l là số tự nhiên lẻ. Khi đó

$$2^n k + 1 = 2^{2^m.l} k + 1 \equiv -k + 1 (\bmod 2^{2^m} + 1).$$

Do đó ta sẽ tìm k để

$$-k + 1 \equiv 0 (\bmod 2^{2^m} + 1).$$

2. Trước hết ta có F_0, F_1, F_2, F_3, F_4 là các số nguyên tố và $F_5 = 641 \times 6700417$ và $(F_i, F_j) = 1, \forall i \neq j$. Đặt $p = 641, q = 6700417$.

3. Theo định lý thặng dư Trung Hoa, tồn tại số nguyên dương k thỏa mãn

$$\begin{cases} k \equiv 1 (\bmod F_0) \\ k \equiv 1 (\bmod F_1) \\ k \equiv 1 (\bmod F_2) \\ k \equiv 1 (\bmod F_3) \\ k \equiv 1 (\bmod F_4) \\ k \equiv 1 (\bmod p) \\ k \equiv -1 (\bmod q). \end{cases}$$

4. Nếu $m < 5$ thì

$$2^n = 2^{2^m l} \equiv -1 (\bmod F_m) \Rightarrow 2^n k \equiv -1 (\bmod F_m) \Rightarrow 2^n k + 1 \vdots F_m.$$

5. Nếu $m = 5$ thì

$$2^n = 2^{2^n l} \equiv -1 (\bmod F_5) \Rightarrow 2^n k \equiv -1 (\bmod p) \Rightarrow 2^n k + 1 \vdots p.$$

6. Nếu $m > 5$ thì

$$2^n = 2^{2^m l} = \left(2^{2^5}\right)^{2^{m-5} l} \equiv 1 (\bmod F_5) \Rightarrow 2^n k \equiv -1 (\bmod q) \Rightarrow 2^n k + 1 \vdots q.$$

□

Bài 20.5.2. Cho trước các số nguyên dương n, s. Chứng minh rằng tồn tại n số nguyên dương liên tiếp mà mỗi số đều có ước là lũy thừa bậc s của một số nguyên dương lớn hơn 1.

Phân tích giải. 1. Xét dãy số Fermat $F_n = 2^{2^n} + 1 (n = 1, 2, \ldots)$. Liên quan đến số này có tính chất đáng lưu ý là

$$(F_n, F_m) = 1, \forall n \neq m.$$

2. Áp dụng định lý thặng dư Trung Hoa cho n số nguyên tố cùng nhau $F_1^s, F_2^s, \ldots, F_n^s$ và n số $r_i = -i (i = 1, 2, \ldots, n)$ thì tồn tại số nguyên x_0 sao cho

$$x_0 + i \vdots F_i^s.$$

Vậy dãy $\{x_0 + 1, x_0 + 2, \ldots, x_0 + n\}$ gồm n số nguyên dương liên tiếp, số hạng thứ i chia hết cho F_i^s.

□

Bài 20.5.3 (IMO Shortlist 1998). Xác định tất cả số nguyên dương n sao cho với n này tồn tại $m \in \mathbb{Z}$ để

$$2^n - 1 | m^2 + 9.$$

Phân tích giải. 1. Viết n dưới dạng $n = 2^s.t (s, t \in \mathbb{N})$, t là số lẻ.

2. Nếu $t \geq 3$ thì $2^t - 1 | 2^n - 1$ nên $2^t - 1 | m^2 + 9$. Ta có

$$2^t - 1 \equiv -1 (\bmod 4).$$

Tức là số $2^t - 1$ có dạng $4k+3$, do đó nó có ước nguyên tố p mà $p \equiv -1 (\bmod 4)$. Dĩ nhiên $p \neq 3$ vì

$$3 \nmid 2^t - 1, \forall t \text{ lẻ}.$$

Từ đó suy ra

$$p | m^2 + 9 \Rightarrow m^2 \equiv -9 (\bmod p).$$

Chứng tỏ -9 là thặng dư bậc hai theo modulo p, tuy nhiên

$$1 = \left(\frac{-9}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{9}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right)^2 = (-1)^{\frac{p-1}{2}}$$

nên $\dfrac{p-1}{2}$ phải là số chẵn, tức là $p \equiv 1 (\bmod 4)$, vô lý.

3. Từ đây suy ra $t = 1$ hay $n = 2^s$. Ta chứng minh đây là tất cả các số cần tìm bằng cách chỉ ra số m để $2^n - 1 | m^2 + 9$. Ta có

$$2^n - 1 = 2^{2^s} - 1 = (2-1)(2+1)(2^2+1)\left(2^{2^2}+1\right)\cdots\left(2^{2^{s-1}}+1\right).$$

Từ đó để

$$2^n - 1 | m^2 + 9 \Rightarrow 2^{2^k} + 1 | m^2 + 9, \forall k = 0, 1, \ldots, s-1.$$

Mặt khác các số Fermat có tính chất

$$\left(2^{2^m}+1, 2^{2^n}+1\right) = 1, \forall m \neq n.$$

Theo định lý thặng dư Trung Hoa thì tồn tại nghiệm x_0 thỏa mãn hệ đồng dư

$$\begin{cases} x \equiv 2 (\bmod 2^2+1) \\ x \equiv 2^2 (\bmod 2^3+1) \\ x \equiv 2^3 (\bmod 2^4+1) \\ \ldots\ldots \\ x \equiv 2^{2^{s-2}} (\bmod 2^{2^{s-1}}+1). \end{cases}$$

Từ đó suy ra

$$x_0^2 + 1 \equiv 0 (\bmod 2^{2^{t+1}}+1), \forall t = 0, 1, 2, \ldots, s-2.$$

Từ đây suy ra

$$2^n - 1 | 9(x_0^2+1) = m^2 + 9$$

với $m = 3x_0$, đây chính là giá trị m cần tìm.

□

Bài 20.5.4 (HÀN QUỐC 1999). Tìm tất cả các số tự nhiên n thỏa mãn 2^n-1 chia hết cho 3 và tồn tại số nguyên m để

$$\frac{2^n-1}{3}|4m^2+1.$$

Phân tích giải. 1. Nếu $n \equiv 1(\bmod 2)$ thì $n = 2k+1 (k \in \mathbb{N})$, khi đó

$$2^n = 2^{2k+1} = 2.4^k \equiv 2(\bmod 3) \Rightarrow 2^n - 1 \equiv 1(\bmod 3)$$

không thỏa mãn $2^n - 1 \vdots 3$.

2. Nếu $n \equiv 0(\bmod 2)$, đặt $n = 2^k.u$ (u là số tự nhiên lẻ). Nếu $u \geq 3$ thì

$$2^u - 1 | 2^n - 1 \text{ vì } 2^n - 1 = 2^{2^k.u} - 1 = (2^u)^{2^k} - 1.$$

Do đó

$$2^u - 1 | 4m^2 + 1.$$

Mặt khác, vì $u \geq 3$ nên

$$2^u - 1 \equiv -1(\bmod 4).$$

Khi đó tồn tại p nguyên tố, $p \equiv -1(\bmod 4)$, là ước của $2^u - 1$. Khi đó

$$p | 4m^2 + 1.$$

Sử dụng tính chất "Nếu p là số nguyên tố dạng $4k+3$ và $a^2 + b^2 \vdots p$ thì cả a và b đều chia hết cho p". Áp dụng vào đẳng thức trên thì

$$2m \vdots p \text{ và } 1 \vdots p,$$

vô lý. Do đó $u = 1$, tức n có dạng $\boxed{n = 2^k}$. Ta chứng minh đây là tất cả các số cần tìm.

3. Khi $n = 2^k$ thì

$$\frac{2^n-1}{3} = \frac{2^{2^k}-1}{3} = F_1.F_2.\ldots.F_{k-1}$$

với F_i là số Fermat thứ i : $F_i = 2^{2^i} + 1$. Theo định lý thặng dư Trung Hoa thì hệ

$$\begin{cases} x \equiv 2(\bmod 2^2+1) \\ x \equiv 2^2(\bmod 2^3+1) \\ x \equiv 2^3(\bmod 2^4+1) \\ \ldots\ldots \\ x \equiv 2^{2^{k-2}}(\bmod 2^{2^{k-1}}+1). \\ x \equiv 0(\bmod 2). \end{cases}$$

có nghiệm, gọi nghiệm đó là x_0 thì x_0 chẵn, đặt $x_0 = 2m$ thì

$$4m^2 + 1 = x_0^2 + 1 \vdots 2^n - 1.$$

□

20.6. ỨNG DỤNG TRONG CÁC BÀI TOÁN SỐ TỔ HỢP

Bài 20.6.1 (ĐÀI LOAN TST 2002). Trong lưới điểm nguyên của mặt phẳng tọa độ Oxy, một điểm A với tọa độ $(x_0,y_0) \in \mathbb{Z}^2$ được gọi là nhìn thấy được từ O nếu đoạn thẳng OA không chứa điểm nguyên nào khác ngoài O và A. Chứng minh rằng với mọi n nguyên dương lớn tùy ý, tồn tại hình vuông $n \times n$ có các đỉnh có tọa độ nguyên, hơn nữa tất cả các điểm nguyên nằm bên trong và trên biên của hình vuông đều không nhìn thấy được từ O.

Phân tích giải. 1. *Trước tiên ta phải tìm điều kiện cần và đủ để $A(x_A,y_A)$ nhìn thấy được từ O?* Dễ thấy điều kiện cần và đủ để $A(x_A,y_A)$ nhìn thấy được từ O là $(x_A,y_A) = 1$.

(a) Thật vậy, nếu A nhìn thấy được, giả sử $(x_A,y_A) = d > 1$. Khi đó $x_A = dx_1, y_A = dy_1 (x_1,y_1) = 1$. Từ đây suy ra

$$\frac{x_A}{x_1} = \frac{y_A}{y_1} = d.$$

Chứng tỏ ba điểm $O, A(x_A,y_A)$ và $M(x_1,y_1)$ thẳng hàng, điểm $M(x_1,y_1)$ nguyên. Dẫn đến A không nhìn thấy được, vô lý. Vậy $(x_A,y_A) = 1$.

(b) Ngược lại, nếu $A(x_A,y_A)$ có $(x_A,y_A) = 1$ thì A nhìn thấy được từ O. Giả sử A không nhìn thấy được, tức tồn tại điểm nguyên $M(x_1,y_1)$ trên đoạn OA. Vì ba điểm O,M,A thẳng hàng nên

$$\frac{x_A}{x_1} = \frac{y_A}{y_1} \Rightarrow x_A.y_1 = y_A.x_1.$$

Vì $(x_A,y_A) = 1$ nên $x_A \vdots x_1$. Đặt $x_A = dx_1$ thay vào thì

$$dy_1 = y_A \Rightarrow y_A \vdots d.$$

Chứng tỏ $(x_A,y_A) \vdots d$ nên $(x_A,y_A) > 1$, vô lý. Do đó A nhìn thấy được từ O.

2. *Để giải quyết bài toán, ta xây dựng một hình vuông $n \times n$ với n nguyên dương tùy ý sao cho mọi điểm nguyên (x,y) nằm trong hoặc trên biên hình vuông đều không thể nhìn thấy được từ O. Tức là phải xây dựng một dãy tọa độ $(x_i,y_j) > 1$. Từ đây nghĩ đến sử dụng các thừa số nguyên tố, một mặt đồng dư theo dòng, một mặt đồng dư theo cột trong ma trận là sẽ thỏa mãn.* Thật vậy chọn p_{ij} là các số nguyên tố đôi một khác nhau $(0 \le i,j \le n)$ (gồm $(n+1)^2$ số nguyên tố). Sắp xếp các số nguyên tố này theo ma trận

$$M = \begin{pmatrix} p_{n0} & p_{n1} & p_{n2} & \cdots & p_{nn} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ p_{20} & p_{21} & p_{22} & \cdots & p_{2n} \\ p_{10} & p_{11} & p_{12} & \cdots & p_{1n} \\ p_{00} & p_{01} & p_{22} & \cdots & p_{0n} \end{pmatrix}$$

Khi đó xét hệ phương trình đồng dư theo tích các số trên dòng

$$\begin{cases} x \equiv 0(\bmod p_{00}.p_{01}.p_{02}\dots p_{0n}) \\ x+1 \equiv 0(\bmod p_{10}.p_{11}.p_{12}\dots p_{1n}) \\ x+2 \equiv 0(\bmod p_{20}.p_{21}.p_{22}\dots p_{2n}) \\ \dots\dots\dots\dots\dots \\ x+n \equiv 0(\bmod p_{n0}.p_{n1}.p_{n2}\dots p_{nn}) \end{cases}$$

và hệ phương trình đồng dư theo tích các số trên cột

$$\begin{cases} y \equiv 0(\bmod p_{00}.p_{10}.p_{20}\dots p_{n0}) \\ y+1 \equiv 0(\bmod p_{01}.p_{11}.p_{21}\dots p_{n1}) \\ y+2 \equiv 0(\bmod p_{02}.p_{12}.p_{22}\dots p_{n2}) \\ \dots\dots\dots\dots\dots \\ y+n \equiv 0(\bmod p_{0n}.p_{1n}.p_{2n}\dots p_{nn}) \end{cases}.$$

Theo định lý thặng dư Trung Hoa thì hai hệ trên có nghiệm, gọi x_0, y_0 là nghiệm tương ứng của hai hệ trên, ta thấy

$$(x_0+i, y_0+j) \vdots p_{ij} \Rightarrow (x_0+i, y_0+j) > 1, \forall 0 \le i, j \le n.$$

Điều đó chứng tỏ mọi điểm nằm trong hoặc trên biên hình vuông $n \times n$ xác định bởi điểm phía dưới bên trái là (x_0, y_0), điểm cao nhất bên phải là (x_0+n, y_0+n) đều không thể nhìn thấy được từ điểm O.

□

Bài toán này mặc dù xuất hiện khá lâu, nhưng tôi không để ý đến, và chỉ thực sự quan tâm và thấy được cái hay của nó khi học cùng em Lê Quang Bình trong đợt tập huấn thi TST 2013 với giáo sư Hà Huy Khoái, khi đó giả thiết phát biểu rất hay bởi ngôn ngữ đời thường là con cáo và ông thợ săn.

Bài 20.6.2 (**BULGARIA 2003**)**.** Ta gọi một tập hợp các số nguyên dương C là **tốt** nếu với mọi số nguyên dương k thì tồn tại a, b khác nhau trong C sao cho $(a+k, b+k) > 1$. Giả sử ta có một tập C tốt mà tổng các phần tử trong đó bằng 2003. Chứng minh rằng ta có thể loại đi một phần tử c trong C sao cho tập còn lại vẫn là tập tốt.

20.7. ỨNG DỤNG TRONG ĐA THỨC

Bài 20.7.1. Cho tập $S = \{p_1, p_2, \dots, p_k\}$ gồm k số nguyên tố phân biệt và $P(x)$ là đa thức với hệ số nguyên sao cho với mọi số nguyên dương n, đều tồn tại p_i trong S sao cho $p_i | P(n)$. Chứng minh rằng tồn tại p_{i_0} trong S sao cho

$$p_{i_0} | P(n), \forall n \in \mathbb{Z}^+.$$

Chứng minh. Giả sử không tồn tại một phần tử p_i nào trong S để

$$p_i | P(n), \forall n \in \mathbb{Z}^+.$$

Nghĩa là với mỗi $p_i \in S$ $(i = 1,2,\ldots,k)$, đều tồn tại $a_i \in \mathbb{Z}^+$ sao cho

$$p_i \nmid P(a_i).$$

Theo định lý thặng dư Trung Hoa thì tồn tại số nguyên dương x_0 sao cho

$$\begin{cases} x_0 \equiv a_1 (\bmod p_1) \\ x_0 \equiv a_2 (\bmod p_2) \\ \ldots\ldots \\ x_0 \equiv a_k (\bmod p_k). \end{cases}$$

Vì $P(x)$ là đa thức hệ số nguyên nên sử dụng tính chất "nếu $u \equiv v (\bmod m)$ thì $P(u) \equiv P(v) (\bmod m)$" ta được

$$\begin{cases} P(x_0) \equiv P(a_1) (\bmod p_1) \\ P(x_0) \equiv P(a_2) (\bmod p_2) \\ \ldots\ldots \\ P(x_0) \equiv P(a_k) (\bmod p_k). \end{cases}$$

Vì $P(a_i) \ \vdots\!\!\!/ \ p_i, \forall i = 1,2,\ldots,k$ nên từ hệ trên suy ra

$$P(x_0) \ \vdots\!\!\!/ \ p_i, \forall i = 1,2,\ldots,k$$

trái với giả thiết bài toán. Vậy giả thiết phản chứng là sai, ta có điều phải chứng minh. □

Không khó để nhận ra, tập số trong bài 20.9 có thể thay bằng $\{p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_k^{\alpha_k}\}$ mà không ảnh hưởng gì. Thậm chí có thể thay bằng tập $\{a_1, a_2, \ldots, a_k\}$ với các số a_i nguyên tố cùng nhau từng cặp một. Tuy nhiên kết quả của bài toán này còn có thể mở rộng hơn nữa, tức tập S có thể thay bằng tập số nguyên bởi ví dụ dưới đây.

Bài 20.7.2. Cho $S = \{a_1, a_2, \ldots, a_n\} \subset \mathbb{Z}^+$ và $P(x) \in \mathbb{Z}[x]$. Biết rằng với mọi số nguyên dương k, đều tồn tại chỉ số $i \in \{1,2,\ldots,n\}$ sao cho

$$a_i | P(k).$$

Chứng minh rằng tồn tại một chỉ số i_0 nào đó sao cho

$$a_{i_0} | P(k), \forall k \in \mathbb{Z}^+.$$

Phân tích giải. 1. *Tương tự như bài toán trên, ý tưởng ban đầu là phản chứng. Viết rõ ý phản chứng này?* Giả sử kết luận bài toán là sai. Tức là với mỗi $i \in \{1,2,\ldots,n\}$, tồn tại số nguyên x_i để

$$a_i \nmid P(x_i).$$

2. *Chuyển điều kiện $a_i \nmid P(x_i)$ về số nguyên tố. Điều kiện để $P(x_i)$ không chia hết cho a_i xét về mặt số nguyên tố như thế nào?* Khi đó tồn tại số $p_i^{k_i}$, với p_i nguyên tố thỏa mãn

$$p_i^{k_i} | a_i \quad \text{nhưng} \quad p_i^{k_i} \nmid P(x_i).$$

Cho i chạy từ 1 đến n ta được tập hợp các số sau $\{p_1^{k_1}, p_2^{k_2}, \ldots, p_n^{k_n}\}$.

3. *Tương tự như bài toán trên, đã chỉ ra mâu thuẫn khi áp dụng định lý thặng dư Trung Hoa được chưa? Rõ ràng chưa thể áp dụng được, vì các số p_i chưa phân biệt, tức trong chúng có một số số trùng nhau? Giả sử p_1, p_2 trùng nhau, $p_1^{k_1}|a_1, p_2^{k_2}|a_2$, khi đó ta chọn lũy thừa k_1, k_2 như thế nào để hai tính chất đó đều thỏa mãn? Rõ ràng phải chọn số nhỏ nhất trong hai số k_1, k_2. Từ đó định hướng cho những số nguyên tố trùng nhau.* Nếu trong tập $\{p_1^{k_1}, p_2^{k_2}, \ldots, p_n^{k_n}\}$ có những số có cơ số trùng nhau, với những cơ số đó, ta giữ lại cơ số có số mũ nhỏ nhất, và loại khỏi tập những lũy thừa còn lại. Khi đó ta được tập

$$\{p_1^{q_1}, p_2^{q_2}, \ldots, p_m^{q_m}\}, (m \leq n \text{ và } p_1, p_2, \ldots, p_m \text{ là những số nguyên tố phân biệt}).$$

Chú ý rằng $a_i (i = 1, 2, \ldots, n)$ sẽ chia hết cho một số số hạng trong tập này, chứ không nhất thiết chỉ chia hết cho 1 số.

4. *Đến đây hoàn thành nốt phần còn lại bằng cách áp dụng định lý thặng dư Trung Hoa?* Từ $p_1^{q_1}, p_2^{q_2}, \ldots, p_m^{q_m}$ là những số đôi một nguyên tố cùng nhau, ta xét hệ đồng dư sau

$$\begin{cases} x \equiv x_1 (\bmod p_1^{q_1}) \\ x \equiv x_2 (\bmod p_2^{q_2}) \\ \ldots\ldots \\ x \equiv x_m (\bmod p_m^{q_m}). \end{cases}$$

Theo định lý thặng dư Trung Hoa thì hệ trên có nghiệm x_0. Vì $P(x)$ là đa thức hệ số nguyên nên

$$\begin{cases} P(x_0) \equiv P(x_1) (\bmod p_1^{q_1}) \\ P(x_0) \equiv P(x_2) (\bmod p_2^{q_2}) \\ \ldots\ldots \\ P(x_0) \equiv P(x_m) (\bmod p_m^{q_m}). \end{cases}$$

Vì $P(x_i) \not\equiv 0 (\bmod p_i^{q_i}), i = 1, 2, \ldots, m$ nên

$$P(x_0) \not\equiv 0 (\bmod p_i^{q_i}), i = 1, 2, \ldots, m$$

chứng tỏ

$$P(x_0) \not\equiv 0 (\bmod a_i), i = 1, 2, \ldots, n$$

mâu thuẫn với giả thiết của bài toán. Ta có điều phải chứng minh.

□

Bài toán trên là điển hình cho cách sử dụng định lý Trung Hoa.

Bài 20.7.3. Chứng minh rằng tồn tại một đa thức $P(x) \in \mathbb{Z}[x]$, không có nghiệm nguyên sao cho với mọi số nguyên dương n, tồn tại số nguyên x sao cho

$$P(x) \vdots n.$$

Chứng minh. Phân tích giải

1. Xét đa thức $P(x)=(3x+1)(2x+1)$. Với mỗi số nguyên dương n, ta biểu diễn n dưới dạng $n=2^k(2m+1)$.

2. Vì $(2^k,3)=1$ nên tồn tại a sao cho
$$3a\equiv 1(\bmod 2^k).$$
Từ đó ta muốn có
$$3x\equiv -1(\bmod 2^k)$$
thì chỉ cần chọn x sao cho
$$x\equiv -a(\bmod 2^k).$$

3. Vì $(2,2m+1)=1$ nên tồn tại số nguyên b sao cho
$$2b\equiv 1(\bmod 2m+1).$$
Do đó ta muốn có
$$2x\equiv -1(\bmod 2m+1)$$
thì cần chọn x sao cho
$$x\equiv -b(\bmod 2m+1).$$

4. Nhưng do $(2^k,2m+1)=1$ nên theo định lý thặng dư Trung Hoa, tồn tại số nguyên x là nghiệm của hệ
$$\begin{cases} x\equiv -a(\bmod 2^k)\\ x\equiv -b(\bmod 2m+1).\end{cases}$$
Từ đó theo lý luận trên, với mọi số nguyên dương n đều tồn tại x để $P(x)\vdots n$. Rõ ràng $P(x)$ không có nghiệm nguyên.

□

Một câu hỏi thú vị không quá tầm thường. Đa thức $P(x)=(3x+1)(2x+1)$ có phải là đa thức duy nhất thỏa mãn điều kiện bài toán trên hay không? Hãy xây dựng đa thức trong trường hợp tổng quát xem sao??

Để hiểu hơn nội dung định lý dưới đây, ta xét ví dụ

Ví dụ 20.7.1. *Cho $n=12=2^2.3$ và đa thức $P(x)=x^2+5x$. Khi đó phương trình*
$$P(x)\equiv 0(\bmod 3)$$
có hai nghiệm là $x\equiv 0,1(\bmod 3)$ và phương trình
$$P(x)\equiv 0(\bmod 4)$$
có hai nghiệm $x\equiv 0,4(\bmod 4)$. Từ đó phương trình
$$P(x)\equiv 0(\bmod 12)$$
có bốn nghiệm là
$$x\equiv 0,3,4,7(\bmod 12).$$

Định lý 20.7.2. *Cho n có dạng biểu diễn chính tắc*

$$n = p_1^{\alpha_1} n_2^{\alpha_2} \dots n_k^{\alpha_k}$$

và $P(x)$ là đa thức hệ số nguyên. Khi đó phương trình đồng dư

$$P(x) \equiv 0 (\bmod n)$$

có nghiệm khi và chỉ khi tất cả các phương trình đồng dư

$$P(x) \equiv 0 (\bmod p_i^{\alpha_i}), i = 1, 2, \dots, k$$

có nghiệm. Hơn nữa nếu mỗi phương trình

$$P(x) \equiv 0 (\bmod p_i^{\alpha_i})$$

có r_i nghiệm modulo $p_i^{\alpha_i}$ ($i = 1, 2, \dots, k$) thì phương trình

$$P(x) \equiv 0 (\bmod n)$$

có $r = r_1.r_2 \dots r_k$ nghiệm modulo n.

Chứng minh. 1. Giả sử x là nghiệm của $P(x) \equiv 0 (\bmod n)$. Suy ra $P(x) \vdots n \Rightarrow P(x) \vdots p_i^{\alpha_i}$. Chứng tỏ x là nghiệm của phương trình

$$P(x) \equiv 0 (\bmod p_i^{\alpha_i}), i = 1, 2, \dots, k.$$

2. Ngược lại, nếu x_i là nghiệm của $P(x) \equiv 0 (\bmod p_i^{\alpha_i}), i = 1, 2, \dots, k$. Theo định lý thặng dư Trung Hoa, tồn tại duy nhất nghiệm x_0 (theo modulo n) của hệ

$$\begin{cases} x \equiv x_1 (\bmod p_1^{\alpha_1}) \\ x \equiv x_2 (\bmod p_2^{\alpha_2}) \\ \dots\dots \\ x \equiv x_k (\bmod p_k^{\alpha_k}). \end{cases} \qquad (I)$$

Theo tính chất của đa thức hệ số nguyên thì

$$x_0 \equiv x_i (\bmod p_i^{\alpha_i}) \Rightarrow P(x_0) \equiv P(x_i) \equiv 0 (\bmod p_i^{\alpha_i}).$$

Từ đó thì $P(x_0) \equiv 0 (\bmod n)$, chứng tỏ x_0 là nghiệm của phương trình $P(x) \equiv 0 (\bmod n)$.

3. Mỗi bộ nghiệm của $(I) : (x_1, x_2, \dots, x_k)$ cho ta một nghiệm x của phương trình

$$P(x) \equiv 0 (\bmod n).$$

Với hai bộ nghiệm của (I) khác nhau là $(x_1, x_2, \dots, x_k)$ và $(x_1', x_2', \dots, x_k')$, khi đó gọi x, x' là hai nghiệm của $P(x) \equiv 0 (\bmod n)$ sinh từ hai bộ này. Vì $(x_1, x_2, \dots, x_k) \neq (x_1', x_2', \dots, x_k')$ nên tồn tại chỉ số i để $x_i \neq x_i'$. Lại do

$$x \equiv x_i (\bmod p_i^{\alpha_i}), x' \equiv x_i' (\bmod p_i^{\alpha}) \Rightarrow x \neq\equiv x' (\bmod p_i^{\alpha_i})$$

chứng tỏ $x \neq x'$. Vậy mỗi bộ nghiệm $(x_1, x_2, \dots, x_k)$

□

Bài 20.7.4. Cho n có dạng biểu diễn chính tắc

$$n = p_1^{\alpha_1} n_2^{\alpha_2} \dots n_k^{\alpha_k}.$$

Tìm số nghiệm của phương trình $x^2 + x \equiv 0 (\bmod n)$.

Giải. Theo định lý trên thì

$$x^2 + x \equiv 0 (\bmod n) \Leftrightarrow x(x+1) \equiv 0 (\bmod p_i^{\alpha_i}), \forall i = 1, 2, \dots, k.$$

Vì $(x, x+1) = 1$ nên

$$x(x+1) \equiv 0 (\bmod p_i^{\alpha i})(i = 1, 2, \dots, k) \Leftrightarrow \begin{bmatrix} x \equiv 0 (\bmod p_i^{\alpha i}) \\ x \equiv -1 (\bmod p_i^{\alpha i}) \end{bmatrix}, \forall i = 1, 2, \dots, k.$$

□

Theo định lý thặng dư trung hoa thì mỗi hệ phương trình

$$\begin{cases} x \equiv a_1 (\bmod p_1^{\alpha_1}) \\ x \equiv a_2 (\bmod p_2^{\alpha_2}) \\ \dots\dots \\ x \equiv a_k (\bmod p_k^{\alpha_k}) \end{cases}, a_i \in \{0, -1\}, i = 1, 2, \dots, k$$

có duy nhất nghiệm modulo n. Vì có tất cả 2^k hệ như vậy (tương ứng với 2^k cách chọn bộ $(a_1, a_2, \dots, a_k)$, với mỗi $a_i \in \{0, -1\}, i = 1, 2, \dots, k$), do đó hệ có tất cả 2^k nghiệm modulo n.

Bài 20.7.5 (VMO 2008). Cho $m = 2007^{2008}$. Có bao nhiêu số tự nhiên $n < m$ sao cho $n(2n+1)(5n+1)$ chia hết cho m.

Phân tích giải.

1. Vì $(10, m) = 1$ nên

$$n(2n+1)(5n+1) \equiv 0 (\bmod m) \Leftrightarrow 10n(10n+5)(10n+2) \equiv 0 (\bmod m).$$

2. Ta có $m = 3^{4016} \times 223^{2008}$, để thuật tiên, ta đặt $10n = x, 3^{4016} = p, 223^{2008} = q$, $(p, q) = 0$ nên

$$x(x+5)(x+4) \equiv 0 (\bmod p.q) \Leftrightarrow \begin{cases} x(x+5)(x+4) \equiv 0 (\bmod p) \\ x(x+5)(x+4) \equiv 0 (\bmod q) \end{cases} \quad (I)$$

3. Vì $(x, x+5) = 5, (x, x+4) = 2$ hoặc $(x, x+4) = 4$, $(x+5, x+4) = 1$, tất cả các ước chung này đều khác 3 và 223. Lưu ý ta cần chọn giá trị $x \equiv 0 (\bmod 10)$. Một giá trị của x cho một giá trị n, hai giá trị x khác nhau sẽ cho hai giá trị n khác nhau. Do đó hệ (I), thêm điều kiện $x \equiv 0 (\bmod 10)$

tương đương với

$$\begin{cases} \left[\begin{array}{l} x\equiv 0(\bmod p)\\ x\equiv -4(\bmod p)\\ x\equiv -5(\bmod p)\end{array}\right.\\ \left[\begin{array}{l} x\equiv 0(\bmod q)\\ x\equiv -4(\bmod q)\\ x\equiv -5(\bmod q)\end{array}\right.\\ x\equiv 0(\bmod 10)\end{cases} \Leftrightarrow \left[\begin{array}{ll} \begin{cases} x\equiv 0(\bmod p)\\ x\equiv 0(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (1)\\ \begin{cases} x\equiv 0(\bmod p)\\ x\equiv -4(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (2)\\ \begin{cases} x\equiv 0(\bmod p)\\ x\equiv -5(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (3)\\ \begin{cases} x\equiv -4(\bmod p)\\ x\equiv 0(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (4)\\ \begin{cases} x\equiv -4(\bmod p)\\ x\equiv -4(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (5)\\ \begin{cases} x\equiv -4(\bmod p)\\ x\equiv -5(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (6)\\ \begin{cases} x\equiv -5(\bmod p)\\ x\equiv 0(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (7)\\ \begin{cases} x\equiv -5(\bmod p)\\ x\equiv -4(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (8)\\ \begin{cases} x\equiv -5(\bmod p)\\ x\equiv -5(\bmod q)\\ x\equiv 0(\bmod 10)\end{cases} & (9)\end{array}\right.$$

4. Theo định lý thặng dư Trung Hoa thì các hệ từ (1) đến (9), mỗi hệ đều có duy nhất một nghiệm x theo modulo $10m$. Do đó ta có tất cả 9 nghiệm x nhỏ hơn $10m$, dẫn đến có 9 giá trị n nhỏ hơn m thỏa đề bài.

□

Định lý 20.7.3. *Cho $P(x)=a_dx^d+\ldots+a_1x+1$ là đa thức hệ số nguyên bậc $d\geq 1$. Khi đó với mọi số nguyên dương n, tồn tại số nguyên x sao cho $P(x)$ có ít nhất n ước nguyên tố.*

Chứng minh. 1. Xét tập hợp $Q = \{p|\ p$ nguyên tố sao cho tồn tại số nguyên x mà $p|P(x)\}$. Khi đó tập Q này vô hạn. Thật vậy, giả sử chỉ có hữu hạn số nguyên tố $p_1, p_2, \ldots, p_k$ trong Q. Khi đó với mỗi số nguyên m thì $P(mp_1p_2\ldots p_k)$ là một số nguyên không có ước nguyên tố vì

$$P(mp_1p_2\ldots p_k) = (mp_1p_2\ldots p_k)^d + \cdots + (mp_1p_2\ldots p_k) + 1,$$

rõ ràng $p_i \nmid P(mp_1\ldots p_k)$, với mỗi $i = 1,2,\ldots,k$. $P(mp_1\ldots p_k)$ không có ước nguyên tố nên giá trị của nó chỉ có thể là 1 hoặc -1. Tuy nhiên do P là đa thức bậc $d \geq 1$ nên nó nhận giá trị 1 hay -1 không quá d lần, mâu thuẫn do $m \in \mathbb{Z}$.

2. Cho $p_1, \ldots, p_n, n \geq 1$ là các số nguyên tố trong Q. Khi đó tồn tại số nguyên x sao cho $P(x) \vdots p_1p_2\ldots p_k$. Thật vậy, với mỗi $i = 1,2,\ldots,n$, do $p_i \in Q$ nên tìm được một số nguyên c_i sao cho

$$P(c_i) \vdots p_i.$$

Khi đó nếu $x \equiv c_i (\bmod p_i)$ thì $P(x) \equiv P(c_i) \equiv 0 (\bmod p_i)$, từ đây dẫn đến việc chọn x. Theo định lý thặng dư Trung Hoa hệ đồng dư

$$\begin{cases} x \equiv c_1 (\bmod p_1) \\ x \equiv c_2 (\bmod p_2) \\ \ldots\ldots \\ x \equiv c_n (\bmod p_n) \end{cases}$$

có duy nhất nghiệm x_0 theo modulo n. Từ đó $P(x) \equiv P(c_i) \equiv 0 (\bmod p_i), i = 1,2,\ldots,n$ nên

$$P(x) \vdots p_1p_2\ldots p_n = n.$$

□

Bài 20.7.6 (USA 2008). Chứng minh rằng với mỗi số nguyên dương n, tồn tại n số nguyên dương nguyên tố với nhau từng cặp $k_1, k_2, \ldots, k_n (k_i > 1, \forall i = 1,2,\ldots,n)$, sao cho $k_0k_1\ldots k_n - 1$ là tích của hai số nguyên liên tiếp.

Giải. Giả sử $k_1k_2\ldots k_n - 1 = x(x+1) \Rightarrow k_1k_2\ldots k_n = x(x+1) + 1 = x^2 + x + 1$. Do đó bài toán có thể quy về: "Chứng minh rằng với mỗi số nguyên dương n, tồn tại số nguyên x sao cho đa thức $x^2 + x + 1$ có ít nhất n ước nguyên tố phân biệt". Đến đây thì bài toán này là một hệ quả của định lý trên. □

20.8. ỨNG DỤNG TRONG NGHIÊN CỨU THẶNG DƯ

Trong chuyên đề thặng dư bậc hai, chúng ta đã nghiên cứu một số điều kiện để số nguyên a là số chính phương modulo p. Tuy nhiên nhiều em lại không nhớ được các điều kiện đó để vận dụng trong các bài toán số học. Do đó trong phần này ta nêu những cái gì cần phải nhớ và cái gì có thể suy luận được dễ dàng.

Định lý 20.8.1 (Tiêu chuẩn Euler). *Cho p là số nguyên tố lẻ, a là số nguyên dương và $(a,p) = 1$. Khi đó*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\bmod p).$$

Cho $a=-11$ ta được

Hệ quả 20.8.2. *Cho p là số nguyên tố lẻ thì*

$$\left(\frac{-1}{p}\right)=1\Leftrightarrow p\equiv 1(\bmod 4).$$

Một đặc trưng nữa cần nhớ là

Hệ quả 20.8.3. *Cho p là số nguyên tố lẻ thì*

$$\left(\frac{2}{p}\right)=1\Leftrightarrow p\equiv \pm 1(\bmod 8).$$

Dùng tính chất nhân tính ta có ngay

$$\left(\frac{-2}{p}\right)=1\Leftrightarrow p\equiv 1,3(\bmod 8).$$

Một tiêu chuẩn nữa cần nhớ là

Định lý 20.8.4 (Luật tương hỗ Gauss). *Cho p và q là hai số nguyên tố lẻ phân biệt. Khi đó*

1. *Nếu ít nhất một trong hai số p,q có dạng $4k+1$ thì p là số chính phương modulo q khi và chỉ khi q là số chính phương modulo p.*
2. *Nếu cả hai số p,q có dạng $4k+3$ thì p là số chính phương modulo q khi và chỉ khi q không là số chính phương modulo p.*

Bài 20.8.1. Tìm tất cả các số nguyên tố lẻ $p(p\neq 3)$ sao cho 3 là số chính phương mod p.

Giải. Vì $3=4\times 0+3$ nên 3 có dạng $4k+3$.

1. Nếu p có dạng $4k+1$. Theo luật tương hỗ Gauss thì

$$\left(\frac{3}{p}\right)=1\Leftrightarrow\left(\frac{p}{3}\right)=1\Leftrightarrow p^{\frac{3-1}{2}}\equiv 1(\bmod 3)\Leftrightarrow p\equiv 1(\bmod 3).$$

Từ đó

$$\begin{cases}p\equiv 1(\bmod 4)\\ p\equiv 1(\bmod 3).\end{cases}$$

Theo định lý thặng dư Trung Hoa thì $p\equiv 1(\bmod 12)$.

2. Nếu $p=4k+3$ thì lại theo luật tương hỗ Gauss

$$\left(\frac{3}{p}\right)=1\Leftrightarrow -\left(\frac{p}{3}\right)=1\Leftrightarrow -p^{\frac{3-1}{2}}\equiv 1(\bmod 3)\Leftrightarrow p\equiv -1(\bmod 3).$$

Từ đó

$$\begin{cases}p\equiv -1(\bmod 3)\\ p\equiv 3(\bmod 4).\end{cases}$$

Theo định lý thặng dư Trung Hoa thì $p\equiv -1(\bmod 12)$.

Từ đó ta có

$$\left(\frac{3}{p}\right)=1 \Leftrightarrow p \equiv \pm 1 (\mathrm{mod}\, 12).$$

□

Bài 20.8.2. Tìm tất cả các số nguyên tố lẻ $p(p \neq 3)$ sao cho 5 là số chính phương mod p.

Giải. Vì $3 = 4 \times 0 + 3$ nên 3 có dạng $4k+3$.

1. Nếu p có dạng $4k+1$. Theo luật tương hỗ Gauss thì

$$\left(\frac{3}{p}\right)=1 \Leftrightarrow \left(\frac{p}{3}\right)=1 \Leftrightarrow p^{\frac{3-1}{2}} \equiv 1 (\mathrm{mod}\, 3) \Leftrightarrow p \equiv 1 (\mathrm{mod}\, 3).$$

   Từ đó

$$\begin{cases} p \equiv 1 (\mathrm{mod}\, 4) \\ p \equiv 1 (\mathrm{mod}\, 3). \end{cases}$$

   Theo định lý thặng dư Trung Hoa thì $p \equiv 1 (\mathrm{mod}\, 12)$.

2. Nếu $p = 4k+3$ thì lại theo luật tương hỗ Gauss

$$\left(\frac{3}{p}\right)=1 \Leftrightarrow -\left(\frac{p}{3}\right)=1 \Leftrightarrow -p^{\frac{3-1}{2}} \equiv 1 (\mathrm{mod}\, 3) \Leftrightarrow p \equiv -1 (\mathrm{mod}\, 3).$$

   Từ đó

$$\begin{cases} p \equiv -1 (\mathrm{mod}\, 3) \\ p \equiv 3 (\mathrm{mod}\, 4). \end{cases}$$

   Theo định lý thặng dư Trung Hoa thì $p \equiv -1 (\mathrm{mod}\, 12)$.

Từ đó ta có

$$\left(\frac{3}{p}\right)=1 \Leftrightarrow p \equiv \pm 1 (\mathrm{mod}\, 12).$$

□

Bài 20.8.3. Tìm tất cả các số nguyên tố lẻ $p(p \neq 5)$ sao cho 5 là thặng dư bình phương mod p.

Giải. Vì $5 = 4.1 + 1$ có dạng $4k+1$. Do đó nếu $p = 4k+1$ hoặc $p = 4k+3$ thì đều có

$$\left(\frac{5}{p}\right)=1 \Rightarrow \left(\frac{p}{5}\right)=1 \Rightarrow p^{\frac{5-1}{2}} \equiv 1 (\mathrm{mod}\, 5) \Rightarrow p^2 \equiv 1 (\mathrm{mod}\, 5) \Rightarrow \left[\begin{array}{r} p \equiv 1 (\mathrm{mod}\, 5) \\ p \equiv -1 (\mathrm{mod}\, 5). \end{array}\right.$$

Từ đó xét các trường hợp

1. $\begin{cases} p \equiv 1 (\mathrm{mod}\, 5) \\ p \equiv 1 (\mathrm{mod}\, 4) \end{cases} \Rightarrow p \equiv 1 (\mathrm{mod}\, 20),$

2. $\begin{cases} p \equiv 1 (\mathrm{mod}\, 5) \\ p \equiv 3 (\mathrm{mod}\, 4) \end{cases} \Rightarrow p \equiv -9 (\mathrm{mod}\, 20),$

3. $\begin{cases} p \equiv -1 (\bmod 5) \\ p \equiv 1 (\bmod 4) \end{cases} \Rightarrow p \equiv 9 (\bmod 20),$

4. $\begin{cases} p \equiv -1 (\bmod 5) \\ p \equiv 3 (\bmod 4) \end{cases} \Rightarrow p \equiv -1 (\bmod 20).$

Do đó p có dạng $p = 20k \pm 1, 20k \pm 9$. Xét hai trường hợp k chẵn, lẻ ta được $p \equiv \pm 1 (\bmod 10)$. Từ đây ta có

$$\left(\frac{5}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 (\bmod 10).$$

□

20.9. BÀI TẬP TỰ LUYỆN

Bài 20.9.1 (**IMO Shortlist 2000**)**.** Xác định tất cả các số nguyên dương $n \geq 2$ thỏa mãn điều kiện: Với mọi a và b nguyên tố cùng nhau với n

$$a \equiv b (\bmod n) \Leftrightarrow ab \equiv 1 (\bmod n).$$

Bài 20.9.2 (**AMC 2011**)**.** Tìm chữ số hàng trăm của số 2011^{2011}.

Bài 20.9.3 (**AIME 2014**)**.** Các số N và N^2 có bốn chữ số tận cùng trong cơ số 10 là $abcd$, với a khác 0. Tìm abc.

Bài 20.9.4 (**ROMANIAN TST 2004**)**.** Cho m là số nguyên dương lớn hơn 1. Giả sử n là số nguyên dương thỏa mãn

$$n | a^m - 1, \forall a \in \mathbb{Z}, (a, n) = 1.$$

Chứng minh rằng $n \leq 4m(2^m - 1)$. Đẳng thức xảy ra khi nào?

Bài 20.9.5. Tìm ba chữ số tận cùng của số $2008^{2007^{2006^{\cdot^{\cdot^{\cdot^{2^1}}}}}}$.

Bài 20.9.6 (**USA TST 2013**)**.** Cho hàm số $f : \mathbb{N} \to \mathbb{N}$ xác định bởi

$$f(1) = 1, f(n+1) = f(n) + 2^{f(n)}, \forall n \in \mathbb{N}.$$

Chứng minh rằng $f(1), f(2), \ldots, f(3^{2013})$ tạo thành hệ thặng dư đầy đủ modulo 3^{2013}.

Bài 20.9.7. Số nguyên dương n được gọi là có tính chất P nếu như với mọi số nguyên dương a, b mà

$$a^3 b + 1 \vdots n \Rightarrow a^3 + b \vdots n.$$

Chứng minh rằng số các số nguyên có tính chất P không vượt quá 24.

Bài 20.9.8. Cho số nguyên dương $a = p_1 p_2 \ldots p_k$, trong đó $p_1, p_2, \ldots, p_k$ là các số nguyên tố đôi một khác nhau và số nguyên dương n thỏa $k < n < a$. Chứng minh rằng trong dãy sau có n^k số chia hết cho a

$$u_1 = 1.2 \ldots n, u_2 = 2.3 \ldots (n+1), u_3 = 3.4 \ldots (n+2), \ldots, u_a = a(a+1) \ldots (a+n-1).$$

Bài 20.9.9. Tìm tất cả các số nguyên tố lẻ $p \neq 7$ sao cho 7 là thặng dư bậc hai modulo p.

Bài 20.9.10. Giả sử n là số nguyên dương và có khai triển ra thừa số nguyên tố $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, ở đây p_i là các số nguyên tố, $\alpha_i \geq 0$ là các số nguyên $(i = 1, 2, \dots, k)$. Cho a là số nguyên, nguyên tố cùng nhau với n. Chứng minh rằng

$$\left(\frac{a}{n}\right) = 1 \Leftrightarrow \left(\frac{a}{p_i^{\alpha_i}}\right) = 1, \forall i = 1, 2, \dots, k.$$

Bài 20.9.11 (VMO 2013). Tìm số các bộ sắp thứ tự (a, b, c, a', b', c') thỏa mãn

$$\begin{cases} ab + a'b' \equiv 1 (\bmod 15) \\ bc + b'c' \equiv 1 (\bmod 15) \\ ca + c'a' \equiv 1 (\bmod 15) \end{cases}$$

với $a, b, c, a', b', c' \in \{0, 1, 2, \dots, 14\}$.

Bài 20.9.12. Cho n là số nguyên dương không có ước chính phương. Chứng minh rằng tồn tại số tự nhiên $b, 1 < b < n, (b, n) = 1$ sao cho

$$\left(\frac{b}{n}\right) = -1.$$

Bài 20.9.13 (Modolva TST 2009).

1. Chứng minh rằng tập các số nguyên có thể phân hoạch thành các cấp số cộng với công sai khác nhau.
2. Chứng minh rằng tập hợp các sô nguyên không thể viết dưới dạng hợp của các cấp số cộng với công sai đôi một nguyên tố cùng nhau.

Bài 20.9.14 (Czech-Slovakia 1997). Chứng minh rằng tồn tại vô số dãy vô hạn tăng $\{a_n\}$ các số tự nhiên sao cho với mọi số tự nhiên k, dãy $\{k + a_n\}$ chỉ chứa hữu hạn số nguyên tố.

Bài 20.9.15. Tìm số nguyên dương n sao cho với mọi hệ thặng dư thu gọn modulo n: $\{a_1, a_2, \dots, a_{\varphi(n)}\}$, ta có

$$a_1.a_2 \dots a_{\varphi(n)} \equiv -1 (\bmod n).$$

Bài 20.9.16. Cho $f_1(x), f_2(x), \dots, f_n(x)$ là n đa thức với hệ số nguyên khác 0. Chứng minh rằng tồn tại đa thức $P(x)$ hệ nguyên sao cho với mọi $i = 1, 2, \dots, n$ ta luôn có

$$P(x) + f_i(x)$$

là đa thức bất khả quy trên $\mathbb{Z}$.

Bài 20.9.17 (Công thức Euler). Cho số nguyên dương n viết dạng chính tắc là $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, trong đó $p_1, p_2, \dots, p_n$ là các số nguyên tố phân biệt, $\alpha_i \geq 0$ là các số tự nhiên, $i = 1, 2, \dots, k$. Hàm $\varphi(n)$ là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n. Khi đó

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right).$$

Bài 20.9.18. Với mỗi số tự nhiên n, đặt

$$A_n = \{a \in \mathbb{N} | (a,n) = (a+1,n) = 1, 1 \leq a \leq n\}.$$

Tính $|A_n|$.

Bài 20.9.19 (**Nauy 1998**)**.** Tồn tại hay không dãy vô hạn $\{x_n\}_{n\in\mathbb{N}}$ là một hoán vị của $\mathbb{N}$ sao cho với mọi số tự nhiên k luôn có

$$x_1 + x_2 + \cdots + x_k \vdots k.$$

Bài 20.9.20 (**Công thức tổng quát định lý Euler**)**.** Cho m là số nguyên dương. Khi đó

$$a^m \equiv a^{m-\varphi(m)} (\bmod m).$$