1. ĐỊNH LÍ PHẦN DƯ TRUNG HOA

Định lí: Cho n số nguyên dương $m_1, m_2, ..., m_n$ số nguyên dương đôi một nguyên tố cùng nhau. Khi đó hệ đồng dư tuyến tính

$$\begin{cases} x \equiv a_i (\mathrm{mod}\, m_i) \\ i = \overline{1,n} \end{cases}$$

có nghiệm duy nhất modun $M = m_1 m_2 ... m_n$.

Chứng minh:

Đặt $M_i = \dfrac{M}{m_i} \Rightarrow (M_i, m_i) = 1, i = \overline{1,n}$ và $M_i \vdots m_j, \forall i \neq j.$

Suy ra $\forall i = \overline{1,n}$, tồn tại số nguyên y_i thoả mãn $M_i y_i \equiv a_i (\mathrm{mod}\, m_i)$.

Xét $\bar{x} = \sum_{i=1}^{n} M_i y_i$ ta có: $\begin{cases} \bar{x} \equiv a_i (\mathrm{mod}\, m_i) \\ i = \overline{1,n} \end{cases}$.

Do đó: $\begin{cases} x \equiv a_i (\mathrm{mod}\, m_i) \\ i = \overline{1,n} \end{cases} \Leftrightarrow \begin{cases} x \equiv \bar{x} (\mathrm{mod}\, m_i) \\ i = \overline{1,n} \end{cases} \Leftrightarrow x \equiv \bar{x} (\mathrm{mod}\, M)$

Vậy định lí được chứng minh.

Nhận xét: *Định lí phần dư Trung Hoa khẳng định về sự tồn tại duy nhất của một lớp thặng dư các số nguyên thoả mãn đồng thời nhiều đồng dư tuyến tính. Do đó có thể sử dụng định lí để giải quyết những bài toán về sự tồn tại và đếm số các số nguyên thoả mãn một hệ các điều kiện quan hệ đồng dư, chia hết..., hay đếm số nghiệm của phương trình đồng dư. Việc sử dụng hợp lí các bộ* $m_1, m_2, ..., m_n$ *và bộ* $a_1, a_2, ..., a_n$ *(trong định lí) cho ta nhiều kết quả rất thú vị và từ đó có thể đưa ra nhiều bài tập hay và khó. Sau đây là một số ứng dụng của định lí phần dư Trung Hoa giải các bài toán số học.*

2. MỘT SỐ ỨNG DỤNG

Bài toán 1. Cho hai số nguyên dương p, q nguyên tố cùng nhau. Chứng minh rằng tồn tại số nguyên k sao cho $(pq-1)^n k+1$ là hợp số với mọi số nguyên dương n.

Lời giải:

Vì (p,q)=1 nên theo định lí phần dư Trung Hoa, tồn tại số nguyên k thoả mãn:

$$\begin{cases} k \equiv 1(\text{mod } p) \\ k \equiv -1(\text{mod } q) \end{cases}$$

Khi đó:

+ Nếu n chẵn thì $(pq-1)^n \equiv 1(\text{mod } q) \Rightarrow (pq-1)^n k \equiv -1(\text{mod } q) \Rightarrow (pq-1)^n k+1 \vdots q$

+ Nếu n lẻ thì $(pq-1)^n \equiv -1(\text{mod } p) \Rightarrow (pq-1)^n k \equiv -1(\text{mod } p) \Rightarrow (pq-1)^n k+1 \vdots p$

Vậy $(pq-1)^n k+1$ là hợp số với mọi số nguyên dương n.

Nhận xét: Chứng minh trên thật gọn gàng nhờ vào việc sử dụng định lí đồng dư Trung Hoa. Mấu chốt của vấn đề ở đây là chúng ta phải thấy rằng để $(pq-1)^n k+1$ là hợp số ta cần chỉ ra $(pq-1)^n k+1$ chia hết cho p hoặc q, khi phân tích tính chẵn lẻ của n ta dễ dàng thấy được sự xuất hiện của hệ $\begin{cases} k \equiv 1(\text{mod } p) \\ k \equiv -1(\text{mod } q) \end{cases}$.

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

Lời giải:

Nhận xét: Bài tập này gần giống với bài tập số một nhưng nó phức tạp hơn bài toán 1 nhiều vì trong bài toán này ta không thể nhìn thấy ngay để $2^n k+1$ là hợp số ta cần chỉ ra nó chia hết cho số nào.

Để ý thấy trằng trong bài toán 1 ta xét hai trường hợp n chẵn và n lẻ hay tổng quát là xét n ở dạng sau $2^m l$ với m, l là các số tự nhiên, l lẻ.

Khi đó $2^n k+1 = 2^{2^m l} k+1$ và ta có $2^{2^m l} \equiv -1 \text{mod}(2^{2^m}+1)$, do đó để $2^n k+1$ là hợp số ta chỉ ra $2^n k+1$ chia hết cho $F_m = 2^{2^m}+1$(Dãy Fermat).

Ta trình bày lời giải bài toán này như sau:

Trước hết ta có F_0, F_1, F_2, F_3, F_4 là các số nguyên tố, $F_5 = 641.6700417$ và $(F_i, F_j) = 1, \forall i \neq j.$

Theo định lí phần dư Trung Hoa, tồn tại số nguyên dương k thoả mãn:

$$\begin{cases} k \equiv 1 (\text{mod } F_m) \\ m = 0,1,2,3,4 \\ k \equiv 1 (\text{mod } p) \\ k \equiv -1 (\text{mod } q) \end{cases} \text{ (p = 641, q = 6700417, (p,q)=1).}$$

Ta có $n = 2^m l$, với m, l là các số tự nhiên, l lẻ.

+ Nếu m < 5 thì $2^n = 2^{2^m l} \equiv -1 (\text{mod } F_m) \Rightarrow 2^n k \equiv -1 (\text{mod } F_m) \Rightarrow 2^n k + 1 \vdots F_m$

+ Nếu m = 5 thì $2^n = 2^{2^m l} \equiv -1 (\text{mod } F_5) \Rightarrow 2^n k \equiv -1 (\text{mod } p) \Rightarrow 2^n k + 1 \vdots p$

+ Nếu m > 5 thì $2^n = (2^{2^5})^{2^{m-5} l} \equiv 1 (\text{mod } F_5) \Rightarrow 2^n k \equiv -1 (\text{mod } q) \Rightarrow 2^n k + 1 \vdots q$

Do đó $2^n k + 1$ là hợp số với mọi số nguyên dương n.

Bài toán 3. Cho là tập $S = \{p_1, p_2, ... p_k\}$ gồm k số nguyên tố phân biệt, và $f(x)$ là đa thức với hệ số nguyên sao cho với mọi số nguyên dương n đều tồn tại p_i trong S sao cho $p_i \mid f(n)$. Chứng minh rằng tồn tại i sao cho $p_i \mid f(n), \forall n \in N^*$.

Lời giải:

Giả sử không tồn tại i sao cho $p_i \mid f(n), \forall n \in N^*$, suy ra với mọi $i=\overline{1;k}$ luôn tồn tại a_i sao cho $p_i \nmid f(a_i)$. Mặt khác theo định lí Phần dư Trung Hoa tồn tại số tự nhiên x thỏa mãn $\begin{cases} x \equiv a_i (\text{mod } p_i) \\ i = \overline{1,k} \end{cases}$, do đó $\begin{cases} f(x) \equiv f(a_i) (\text{mod } p_i) \\ i = \overline{1,k} \end{cases}$ hay $p_i \nmid f(x), \forall i = \overline{1;k}$

(Mâu thuẫn)

Bài toán 4. Cho $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ và $f(x)$ là một đa thức với hệ số nguyên. Khi đó phương trình đồng dư $f(x) \equiv 0 (\text{mod } n)$ có nghiệm khi và chỉ khi tất cả các phương trình đồng dư $f(x) \equiv 0 (\text{mod } p_i^{\alpha_i}),\ i = \overline{1;\ k}$ có nghiệm. Nếu gọi là số nghiệm của phương trình $f(x) \equiv 0 (\text{mod } p_i^{\alpha_i})$ là $n_i, i = \overline{1;k}$ thì phương trình $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ có đúng $n_1.n_2...n_k$ nghiệm (môđun n)

Lời giải:

- Giả sử $\overline{x}$ là một nghiệm của $f(x)\equiv 0(\text{mod}\, n)$, hiển nhiên $\overline{x}$ là một nghiệm của hệ $\begin{cases} f(x)\equiv 0(\text{mod}\, p_i^{\alpha_i}) \\ i=\overline{1;k} \end{cases}$.

- Giả sử $\overline{x_i}$ là một nghiệm của $f(x)\equiv 0(\text{mod}\, p_i^{\alpha_i}), i=\overline{1;k}$. Theo định lí Phần dư Trung Hoa tồn tại duy nhất $\overline{x}$ là nghiệm của hệ $\begin{cases} x\equiv \overline{x_i}(\text{mod}\, p_i^{\alpha_i}) \\ i=\overline{1;k} \end{cases}$ (mod n). Mà $\overline{x}\equiv \overline{x_i}(\text{mod}\, p_i^{a_i}) \Rightarrow f(\overline{x})\equiv f(\overline{x_i})(\text{mod}\, p_i^{a_i})$ (vì $(f(\overline{x})-f(\overline{x_i}))\vdots(\overline{x}-\overline{x_i})$), suy ra $\overline{x}$ là một nghiệm của $f(x)\equiv 0(\text{mod}\, n)$.

Mỗi bộ $(\overline{x_1},\overline{x_2},...,\overline{x_k})$ với $\overline{x_i}$ là một nghiệm của $f(x)\equiv 0(\text{mod}\, p_i^{\alpha_i}), i=\overline{1;k}$ cho ta một nghiệm của $f(x)\equiv 0(\text{mod}\, n)$ và hiển nhiên các nghiệm này là phân biệt (vì trong hai bộ khác nhau phải tồn tại ít nhất một cặp $\overline{x_{i_1}},\overline{x_{i_2}}$ là hai nghiệm khác nhau của $f(x)\equiv 0(\text{mod}\, p_i^{\alpha_i})$, do đó hai nghiệm tương ứng với hai bộ đó không đồng dư theo $\text{mod}\, p_i^{\alpha_i}$). Do đó số nghiệm của $f(x)\equiv 0$ đúng bằng $n_1.n_2\ldots n_k$.

Như vậy dựa vào định lí Phần dư Trung Hoa ta có thể đếm được số nghiệm của một phương trình đồng dư. Bài toán 5, bài toán 6 sau đây là các ví dụ cụ thể cho bài toán 4.

Bài toán 5. Cho số nguyên dương $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$, trong đó $p_1,p_2,...,p_k$ là các số nguyên tố đôi một khác nhau. Tìm số nghiệm của phương trình đồng dư $x^2+x\equiv 0(\text{mod}\, n)$.

Lời giải:

$$x^2+x\equiv 0(\text{mod}\, n)\Leftrightarrow \begin{cases} x(x+1)\equiv 0(\text{mod}\, p_i^{\alpha_i}) \\ i=\overline{1,k} \end{cases}\Leftrightarrow \begin{cases} \left[\begin{array}{l} x\equiv 0(\text{mod}\, p_i^{\alpha_i}) \\ x\equiv -1(\text{mod}\, p_i^{\alpha_i}) \end{array}\right. \\ i=\overline{1,k} \end{cases}$$

Theo định lí phần dư Trung Hoa mỗi hệ phương trình $\begin{cases} x\equiv a_i(\text{mod}\, p_i^{\alpha_i}) \\ a_i\in\{-1;0\} \\ i=\overline{1,k} \end{cases}$ có duy nhất một nghiệm (thặng dư modn) và ta có 2^k hệ (bằng số bộ

$(a_1, a_2, ..., a_k), a_i \in \{-1; 0\}$), nghiệm của các hệ khác nhau. Suy ra phương trình $x^2 + x \equiv 0 (\mathrm{mod}\, n)$ có đúng 2^k nghiệm.

Bài toán 6. Cho số nguyên dương $a = p_1 p_1 ... p_k$, trong đó $p_1, p_2, ..., p_k$ là các số nguyên tố đôi một khác nhau và số nguyên dương n thoả mãn k < n < $p_1, p_2, ..., p_k$. Chứng minh rằng trong dãy sau có n^k số chia hết cho a.

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

Lời giải:

Nhận xét: Bài tập này tư tưởng giống như bài 4.

$u_j \vdots a \Leftrightarrow \begin{cases} i \equiv a_i (\mathrm{mod}\, p_i) \\ a_i \in \{0, -1, -2, ..., -(n-1)\}, \quad j = \overline{1, a.} \\ i = \overline{1, k} \end{cases}$ Do đó ta có n^k số chia hết cho a.

**** Cùng với tư tưởng như bài 4, ta có thể chứng minh công thức của Phi hàm Ơl bằng cách đưa về đếm số nghiệm của một hệ đồng dư.***

Bài toán 7. Cho số nguyên dương n, $\varphi(n)$ là số các số nguyên dương không vượt quá n và nguyên tố cùng nhau với n. Chứng minh rằng với $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, trong đó $p_1, p_2, ..., p_k$ là các số nguyên tố đôi một khác nhau, ta có :

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

(Phi hàm Ơle)

Lời giải

Nhận xét: Công thức trên đã được chứng minh bằng cách sử dụng tính chất $\varphi(n)$ là hàm nhân tính. Và để chứng minh tính chất trên ta phải sử dụng đến các tính chất của hệ thặng dư. Cách này khá phức tạp.

Bài toán này có thể giải đẹp hơn bằng định lí đồng dư Trung Hoa

$A_n = \{a \in N \mid 1 \le a \le n, (a, n) = 1\}$

Khi $n = p^\alpha \Rightarrow \varphi(n) = p^\alpha - p^{\alpha-1}$

Khi $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, trong đó $p_1, p_2, ..., p_k$ là các số nguyên tố đôi một khác nhau. Với số nguyên dương a thoả mãn $1 \le a \le n$ ta có:

$$a \in A_n \Leftrightarrow (a, p_i^{\alpha_i}) = 1, i = \overline{1,k} \Leftrightarrow \begin{cases} a \equiv a_i (\text{mod } p_i^{\alpha_i}) \\ a_i \in A_{p^{\alpha_i}} \\ i = \overline{1,k} \end{cases}$$

Mà theo định lí phần dư Trung Hoa, tồn tại duy nhất số nguyên dương a, $1 \le a \le n$ thoả mãn $\Leftrightarrow \begin{cases} a \equiv a_i (\text{mod } p_i^{\alpha_i}) \\ a_i \in A_{p^{\alpha_i}} \\ i = \overline{1,k} \end{cases}$ và ta có $\prod_{i=1}^{k} | A_{p_i^{\alpha_i}} | = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$ hệ dạng trên, nghiệm của các hệ khác nhau.

Do đó $| A_n | = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})...(1 - \frac{1}{p_k})$.

Bài toán 8. Cho $A_n = \{a \in N \mid 1 \le a \le n, (a,n) = (a+1,n) = 1\}$. Tìm $| A_n |$.

Lời giải:

Nhận xét: Bài toán này có thể giải tương tự như cách chứng minh công thức phi hàm Ơle $\varphi(n)$. Giả sử $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, trong đó $p_1, p_2, ..., p_k$ là các số nguyên tố đôi một khác nhau, ta có $| A_n | = n(1 - \frac{2}{p_1})(1 - \frac{2}{p_2})...(1 - \frac{2}{p_k})$.

**** Sử dụng định lí đồng dư Trung Hoa chứng minh công thức của Phi hàm Ơle, cho ta một lời giải đẹp, nhưng cũng với tư tưởng trên và tính chất của hệ thặng dư ta còn có thể giải bài toán mở rộng của định lí Wilson.***

Bài toán 9. Tìm số nguyên dương n lẻ sao cho với mọi hệ thặng dư thu gọn mođun n $\{a_1, a_2, ..., a_{\varphi(n)}\}$ ta có $a_1 a_2 ... a_{\varphi(n)} \equiv -1 (\text{mod } n)$.

Lời giải:

- Theo định lí Wilson ta suy ra n nguyên tố thoả mãn.
- Với $n = p^m$ với p là số nguyên tố lẻ.

Ta có $\{a_1, a_2, ..., a_{\varphi(n)}\}$ là một hệ thặng dư thu gọn mođun n, suy ra với mỗi $a \in \{a_1, a_2, ..., a_{\varphi(n)}\}$ đều tồn tại duy nhất $\overline{a} \in \{a_1, a_2, ..., a_{\varphi(n)}\}$ thoả mãn $a\overline{a} \equiv 1 (\text{mod } n)$ và $a \ne b \Rightarrow \overline{a} \ne \overline{b}$.

$$a=\overline{a}\Leftrightarrow a^2-1\vdots n\Leftrightarrow (a-1)(a+1)\vdots n\Leftrightarrow \left[\begin{array}{l} a\equiv 1(\mathrm{mod}\, n)\\ a\equiv -1(\mathrm{mod}\, n)\end{array}\right.\Leftrightarrow \left[\begin{array}{l} a=1\\ a=n-1\end{array}\right. \text{(vì (a-1,a+1)<3).}$$

Suy ra $\{a_1,a_2,...,a_{\varphi(n)}\}\setminus\{1,\ n-1\}$ chia thành $\frac{\varphi(n)-1}{2}$ cặp nghịch đảo mođun n.

Do đó $a_1a_2...a_{\varphi(n)}\equiv -1(\mathrm{mod}\, n)$.

- Với $n=p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$ trong đó $p_1,p_2,...,p_k$ là k (k>1) số nguyên tố lẻ, phân biệt.

Tương tự như trên: Với mỗi $a\in\{a_1,a_2,...,a_{\varphi(n)}\}$ đều tồn tại duy nhất $\overline{a}\in\{a_1,a_2,...,a_{\varphi(n)}\}$ thoả mãn $a\overline{a}\equiv 1(\mathrm{mod}\, n)$ và $a\neq b\Rightarrow \overline{a}\neq\overline{b}$.

$$a=\overline{a}\Leftrightarrow a^2-1\vdots n\Leftrightarrow (a-1)(a+1)\vdots n\Leftrightarrow \begin{cases}\left[\begin{array}{l} a\equiv 1(\mathrm{mod}\, p_i^{\alpha_i})\\ a\equiv -1(\mathrm{mod}\, p_i^{\alpha_i})\end{array}\right. \text{(Vì (a-1,a+1)<3)}\\ i=\overline{1,k}\end{cases}$$

Theo định lí phần dư Trung Hoa mỗi hệ phương trình $\begin{cases} a\equiv a_i(\mathrm{mod}\, p_i^{\alpha_i})\\ a_i\in\{-1;1\}\\ i=\overline{1,k}\end{cases}$ có duy nhất một nghiệm (thặng dư modn) và ta có 2^k hệ (bằng số bộ $(a_1,a_2,...,a_k)$, $a_i\in\{-1;0\}$), nghiệm của các hệ khác nhau.

Suy ra có đúng 2^k số $a\in\{a_1,a_2,...,a_{\varphi(n)}\}$ mà $a=\overline{a}$, Kí hiệu A_n là tập hợp $a\in\{a_1,a_2,...,a_{\varphi(n)}\}$ mà $a=\overline{a}$.

Dễ thấy $\prod_{a\in A_n} a\equiv(-1)^{2^{k-1}}\equiv 1(\mathrm{mod}\, p_i^{\alpha_i}), i=\overline{1,k}\Rightarrow \prod_{a\in A_n} a\equiv 1(\mathrm{mod}\, n)$

Mặt khác tập $\{a_1,a_2,...,a_{\varphi(n)}\}\setminus A_n$ chia thành $\frac{\varphi(n)-2^k}{2}$ cặp nghịch đảo mođun n

Suy ra: $a_1a_2...a_{\varphi(n)}\equiv 1(\mathrm{mod}\, n)$.

Kết luận: $n=p^m$.

Sau đây là một số bài toán chứng minh sự tồn tại của một dãy số thỏa mãn một số tính chất cho trước bằng các kỹ thuật lựa chọn bộ $a_1,a_2,...,a_n$ ***(trong định lí phần dư Trung Hoa).***

Bài toán 10. Chứng minh rằng với mọi số tự nhiên n, luôn tồn tại n số tự nhiên liên tiếp sao cho bất kì số nào trong các số đó cũng đều là hợp số.

Lời giải:

Nhận xét: n số tự nhiên liên tiếp có dạng a+1, a+2,…,a+n. Các số này là hợp số nếu tồn tại các số nguyên dương $p_1, p_2, ..., p_n$ khác 1 sao cho $(a+i) \vdots p_i^2$. Suy ra a là nghiệm của hệ phương trình $\begin{cases} x \equiv -i (\text{mod } p_i^2) \\ i = \overline{1,n} \end{cases}$.

Theo định lí đồng dư Trung Hoa hệ $\begin{cases} x \equiv -i (\text{mod } p_i^2) \\ i = \overline{1,n} \end{cases}$ có nghiệm khi $p_1, p_2, ..., p_n$ đôi một nguyên tố cùng nhau.

Do đó ta chỉ cần chọn $p_1, p_2, ..., p_n$ là n số nguyên tố phân biệt.

Bài toán 11. Chứng minh rằng với mọi số tự nhiên n, luôn tồn tại n số tự nhiên liên tiếp sao cho bất kì số nào trong các số đó cũng đều không phải là luỹ thừa (với số mũ nguyên lớn hơn 1) của một số nguyên tố.

(Đề thi toán quốc tế 1989)

Lời giải:

Nhận xét: Khi giải bài toán này chúng ta đặt ra câu hỏi bài toán này có tư tưởng có giống bài 5 không?. Nếu để ý đến bổ đề sau đây chúng ta sẽ thấy bài toán này có liên quan đến bài toán trên.

Bổ đề: Nếu a chia hết cho p và không chia hết cho p^2 với p là một số nguyên tố thì a không là luỹ thừa (với số mũ nguyên lớn hơn 1) của một số nguyên tố.

Trở lại bài toán:

Gọi $p_1, p_2, ..., p_n$ là n số nguyên tố phân biệt, theo định lí phần dư Trung Hoa, tồn tại số nguyên dương a sao cho $\begin{cases} a \equiv -i + p_i (\text{mod } p_i^2) \\ i = \overline{1,n} \end{cases}$.

Khi đó $a + i \vdots p_i$, và không chia hết cho $p_i^2, i = \overline{1,n}$. Suy ra điều phải chứng minh.

Bài toán 12. Tồn tại hay không dãy vô hạn $\{x_n\}$ là một hoán vị của tập N sao cho với mọi số tự nhiên k luôn có $x_1 + x_2 + ... + x_k \vdots k$.

(Nordic 1998)

Lời giải:

Nhận xét: trong bài toán này ta cần chú ý đến giả thiết dãy $\{x_n\}$ là một hoán vị của tập N, nếu không có giả thiết này bài toán trở nên qua dễ, ta quy nạp như sau, mỗi bộ $x_1, x_2, ..., x_{n-1}$ ta luôn chọn được x_n sao cho $x_1 + x_2 + ... + x_n \vdots n$. Do vậy yêu cầu của bài toán là ta phải xây dựng dãy $\{x_n\}$ sao cho quét hết tập N, đây là câu hỏi chính cần trả lời.

Trở lại bài toán ta chứng minh sự tồn tại dãy số bằng quy nạp như sau:

Chọn $x_1 = 0, x_2 = 2, x_3 = 1$.

Giả sử tồn tại $x_1, x_2, ..., x_n$ thoả mãn $x_1 + x_2 + ... + x_k \vdots k, \forall k = \overline{1,n}$.

Đặt $S_n = x_1 + x_2 + ... + x_n$.

Chọn $x_{n+2} = \min(N \setminus \{x_1, x_2, ..., x_n\})$ và x_{n+1} là nghiệm nguyên dương lớn hơn $x_1, x_2, ..., x_n$ của hệ

$$\begin{cases} x \equiv -S_n (\text{mod}(n+1)) \\ x \equiv -S_n - x_{n+2} (\text{mod}(n+2)) \end{cases}.$$

Do (n+1,n+2)=1 nên hệ trên có nghiệm (Định lí đồng dư Trung Hoa).

Vì chọn $x_{n+2} = \min(N \setminus \{x_1, x_2, ..., x_n\})$ nên $\{x_n\}$ quét hết tập N.

Bài toán 13. 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 luỹ thừa của một số tự nhiên với số mũ lớn hơn 1.

Lời giải:

Nhận xét: Trong các cấp số cộng thì cấp số cộng dạng a, 2a, 3a,…,na là thích hợp nhất trong bài toán này vì trong mỗi số hạng không có phép cộng dễ sử lí để phù hợp hơn yêu cầu mọi số hạng của nó đều là luỹ thừa của một số tự nhiên với số mũ lớn hơn 1. Do đó a có dạng $2^{m_2}3^{m_3}...n^{m_n}$ và $(m_2, m_3, ..., m_n), (m_2 + 1, m_3, ..., m_n)$, $(m_2, m_3 + 1, ..., m_n), ..., (m_2, m_3, ..., m_n + 1) > 1$.

Lời giải bài toán trình bày như sau:

Giả sử $p_1, p_2, ..., p_n$ là n số nguyên tố phân biệt.

Theo định lí phần dư Trung Hoa, với mọi $i=\overline{2,n}$ tồn tại số nguyên dương m_i thoả mãn

$$\begin{cases} m_i \equiv -1 (\text{mod } p_i) \\ m_i \equiv 0 (\text{mod } p_j) \\ j=\overline{1,n}, j \neq i \end{cases}.$$

Khi đó $(m_2, m_3, ..., m_n) \vdots p_1$, $(m_2+1, m_3, ..., m_n) \vdots p_2, \ldots,$ $(m_2, m_3, ..., m_n+1) \vdots p_n$.

$$\Rightarrow a = 2^{m_2} 3^{m_3} ... n^{m_n} = \left(2^{\frac{m_2}{p_1}} 3^{\frac{m_3}{p_1}} ... n^{\frac{m_n}{p_1}} \right)^{p_1}, \; 2a = 2^{m_2+1} 3^{m_3} ... n^{m_n} = \left(2^{\frac{m_2+1}{p_2}} 3^{\frac{m_3}{p_2}} ... n^{\frac{m_n}{p_2}} \right)^{p_2}, \ldots,$$

$$na = 2^{m_2} 3^{m_3} ... n^{m_n+1} = \left(2^{\frac{m_2}{p_n}} 3^{\frac{m_3}{p_n}} ... n^{\frac{m_n+1}{p_n}} \right)^{p_n}.$$ Điều phải chứng minh.

Bài toán 14. Cho A là tập con khác rỗng của N. Chứng minh rằng tồn tại số nguyên dương n sao cho $nA = \{nx \mid x \in A\}$ là tập hợp là luỹ thừa của một số tự nhiên với số mũ lớn hơn 1.

(Balkan 2000)

Lời giải:

Nhận xét: Bài toán này tư tưởng giống bài toán trên.

Giả sử $A = \{a_1, a_2, ..., a_k\}$, $p_1, p_2, ..., p_k$ là k số nguyên tố phân biệt.

Theo định lí đồng dư Trung Hoa, với mọi $i=\overline{1,k}$ tồn tại số nguyên dương m_i thoả mãn

$$\begin{cases} m_i \equiv -1 (\text{mod } p_i) \\ m_i \equiv 0 (\text{mod } p_j) \\ j=\overline{1,k}, j \neq i \end{cases}.$$

Khi đó $(m_1+1, m_2, ..., m_k) \vdots p_1$, $(m_1, m_2+1, m_3, ..., m_n) \vdots p_2, \ldots,$ $(m_1, m_2, ..., m_n+1) \vdots p_n$.

Đặt $n = a_1^{m_1} a_2^{m_2} ... a_k^{m_k}$, ta có:

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

$$,\ldots,\ na_k = a_1^{m_1}a_2^{m_2}...a_k^{m_k+1} = \left(a_1^{\frac{m_1}{p_k}}a_2^{\frac{m_2}{p_k}}...a_k^{\frac{m_k+1}{p_k}}\right)^{p_k}$$. Điều phải chứng minh.

***

3. MỞ RỘNG ĐỊNH LÍ PHẦN DƯ TRUNG HOA

Trong định lí phần dư Trung Hoa, có điều kiện $m_1, m_2, ..., m_n$ là các số nguyên dương đôi một nguyên tố cùng nhau. Câu hỏi đặt ra là nếu $m_1, m_2, ..., m_n$ không thoả mãn điều kiện đôi một nguyên tố cùng nhau thì kết quả định lí này sẽ như thế nào?

Định lí (Phần dư Trung Hoa mở rộng)

Cho n số nguyên dương $m_1, m_2, ..., m_n$ và $a_1, a_2, ..., a_n$ là các số nguyên dương bất kì. Khi đó hệ đồng dư tuyến tính

$$\begin{cases} x \equiv a_i (\text{mod}\, m_i) \\ i = \overline{1,n} \end{cases}$$

có nghiệm khi và chỉ khi $a_i \equiv a_j (\text{mod}(m_i, m_j))$ với mọi i, j thoả mãn $1 \le i < j \le n$.

Khi đó hệ có nghiệm duy nhất modun $M = [m_1, m_2, ..., m_n]$.

Chứng minh:

- Giả sử hệ có nghiệm x_0, đặt $(m_i, m_j) = d_{ij} \Rightarrow a_i \equiv x_0 \equiv a_j (\text{mod}\, d_{ij})$ với mọi i, j thoả mãn $1 \le i < j \le n$.
- Ngược lại nếu $a_i \equiv a_j (\text{mod}(m_i, m_j))$ với mọi i, j thoả mãn $1 \le i < j \le n$ thì ta chứng minh hệ trên có nghiệm duy nhất modun $M = [m_1, m_2, ..., m_n]$ bằng quy nạp như sau:

Với n = 2, đặt $(m_1, m_2) = d, m_1 = dd_1, m_2 = dd_2, (d_1, d_2) = 1 \Rightarrow a_1 \equiv a_2 \equiv a (\text{mod}\, d)$

Đặt $a_1 = a + k_1 d, a_2 = a + k_2 d$, ta có:

$$\begin{cases} x \equiv a_1 (\text{mod}\, m_1) \\ x \equiv a_2 (\text{mod}\, m_2) \end{cases} \Leftrightarrow \begin{cases} \dfrac{x-a}{d} \equiv k_1 (\text{mod}\, d_1) \\ \dfrac{x-a}{d} \equiv k_2 (\text{mod}\, d_2) \end{cases}$$

Vì $(d_1, d_2) = 1$ nên theo định lí phần dư Trung Hoa, tồn tại số nguyên dương $\bar{x}$ thoả mãn $\begin{cases} \bar{x} \equiv k_1 (\text{mod}\, d_1) \\ \bar{x} \equiv k_1 (\text{mod}\, d_1) \end{cases}$. Do đó $\begin{cases} x \equiv a_1 (\text{mod}\, m_1) \\ x \equiv a_2 (\text{mod}\, m_2) \end{cases} \Leftrightarrow \dfrac{x-a}{d} \equiv \bar{x} (\text{mod}(d_1 d_2))$

$\Leftrightarrow x \equiv \overline{x}d + a(\text{mod}(dd_1d_2))$ hay $x \equiv \overline{x}d + a(\text{mod}[m_1, m_2])$.

Suy ra hệ $\begin{cases} x \equiv a_1(\text{mod}\, m_1) \\ x \equiv a_2(\text{mod}\, m_2) \end{cases}$ có nghiệm duy nhất modun $[m_1, m_2]$.

Giả sử định lí đúng đến n – 1. Ta chứng minh định định lí đúng đến n.

Đặt $\overline{m_1} = [m_1, m_2, ..., m_{n-1}], \overline{m_2} = m_n$

Theo giả thiết quy nạp, hệ phương trình $\begin{cases} x \equiv a_i(\text{mod}\, m_i) \\ i = \overline{1, n-1} \end{cases}$ có nghiệm duy nhất $x \equiv \overline{a_1}(\text{mod}\, \overline{m_1})$. Do đó ta có $\begin{cases} x \equiv a_i(\text{mod}\, m_i) \\ i = \overline{1, n} \end{cases} \Leftrightarrow \begin{cases} x \equiv \overline{a_1}(\text{mod}\, \overline{m_1}) \\ x \equiv \overline{a_2}(\text{mod}\, \overline{m_2}) \end{cases}$ (đặt $\overline{a_2} = a_n$).

Vì $a_i \equiv a_j(\text{mod}(m_i, m_j))$ với mọi i, j thoả mãn $1 \le i < j \le n$ nên $\overline{a_1} \equiv \overline{a_2}(\text{mod}(\overline{m_1}, \overline{m_2}))$.

Từ đó theo trường hợp n = 2, hệ phương trình $\begin{cases} x \equiv \overline{a_1}(\text{mod}\, \overline{m_1}) \\ x \equiv \overline{a_2}(\text{mod}\, \overline{m_2}) \end{cases}$ có nghiệm duy nhất modun $[\overline{m_1}, \overline{m_2}] = [m_1, m_2, ..., m_n]$.

Theo nguyên lí quy nạp định lí được chứng minh.

***

Một số bài tập áp dụng:

Bài 1. Chứng minh rằng với mọi số tự nhiên n, luôn tồn tại n số tự nhiên liên tiếp sao cho bất kì số nào trong các số đó cũng có ước nguyên dương dạng $2^k - 1$.

Bài 2. 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.

Czech-Slovakia 1997

Bài 3. Tìm tất cả các số nguyên dương n sao cho $2^n - 1 \vdots 3$ và $\frac{2^n - 1}{3}$ là ước của một số nguyên có dạng $4m^2 + 1$.

Korea 1999

Bài 4. Ta định nghĩa hình vuông tốt là một hình vuông có 4 đỉnh là các điểm nguyên , đồng thời đoạn thẳng nối tâm O với tất cả các điểm nguyên trên biên và trong hình vuông đó chứa ít nhất một điêm nguyên khác hai đầu mút . Chứng minh rằng với mọi số nguyên dương n đều tồn tại một hình vuông tốt dạng n×n.

Bài 5. Tìm số nguyên dương n sao cho với mọi hệ thặng dư thu gọn mođun n $\{a_1, a_2, ..., a_{\varphi(n)}\}$ ta có $a_1 a_2 ... a_{\varphi(n)} \equiv -1 (\mathrm{mod}\, n)$.

Bài 6. Cho $f_1(x), f_2(x), ..., f_n(x)$ 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 $\forall i = \overline{1;n}$ ta luôn có $P(x) + f_i(x)$ là đa thức bất khả quy trên Z.

Bài 7. Cho $m = 2007^{2008}$, hỏi có tất cả bao nhiêu số tự nhiên $n < m$ sao cho $m \mid n(2n+1)(5n+2)$.

Bài 8. 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 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 .

Bulgaria TST 2003

Bài 9. Chứng minh rằng tồn tại dãy (a_n) tăng thực sự sao cho với mọi n thì $a_1a_2...a_n - 1$ là tích của hai số nguyên liên tiếp.

USA -TST 2009

Bài 10. a) Chứng minh rằng tập các số nguyên có thể phân hoạch thành các cấp số cộng với công sai khác nhau.

b) 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.

Moldova TST 2009

Tài liệu tham khảo

- Đặng Hùng Thắng – Đồng dư và phương trình đồng dư
- Nguyễn Vũ Lương – Các bài giảng về số học
- Tuyển chọn các chuyên đề toán học tuổi trẻ – Tập 3
- Diễn đàn – http://mathvn.org