Chuyên đề

SỐ HỌC

Diễn đàn Toán học

Chuyên đề

SỐ HỌC

Chế bản

Trần Quốc Nhật Hân [perfectstrong]
Trần Trung Kiên [Ispectorgadget]
Phạm Quang Toàn [Phạm Quang Toàn]
Lê Hữu Điền Khuê [Nesbit]
Đinh Ngọc Thạch [T*genie*]

Lời giới thiệu

Bạn đọc thân mến,

Số học là một phân môn quan trọng trong toán học đã gắn bó với chúng ta xuyên suốt quá trình học Toán từ bậc tiểu học đến trung học phổ thông. Chúng ta được tiếp xúc với Số học bắt đầu bằng những khái niệm đơn giản như tính chia hết, ước chung lớn nhất, bội chung nhỏ nhất... giúp làm quen dễ dàng hơn với sự kì diệu của những con số cho đến những vấn đề đòi hỏi nhiều tư duy hơn như đồng dư, số nguyên tố, các phương trình Diophantine mà nổi tiếng nhất là định lý lớn Fermat..., đâu đâu từ tầm vi mô đến vĩ mô, từ cậu bé lớp một bi bô 4 chia hết cho 2 đến Giáo sư thiên tài Andrew Wiles (người giải quyết bài toán Fermat), chúng ta đều có thể thấy được hơi thở của Số học trong đó.

Số học quan trọng như vậy nhưng lạ thay số chuyên đề viết về nó lại không nhiều nếu đem so với kho tàng đồ sộ các bài viết về bất đẳng thức trên các diễn đàn mạng. Xuất phát từ sự thiếu hụt đó cũng như để kỉ niệm tròn một năm Diễn đàn Toán học khai trương trang chủ mới (16/01/2012 - 16/01/2013), nhóm biên tập chúng tôi cùng với nhiều thành viên tích cực của diễn đàn đã chung tay biên soạn một chuyên đề gửi đến bạn đọc.

Chuyên đề là tập hợp các bài viết riêng lẻ của các tác giả *Nguyễn Mạnh Trùng Dương* (duongld) , *Nguyễn Trần Huy* (yeutoan11), Nguyễn Trung Hiếu (nguyentrunghieua), *Phạm Quang Toàn* (Phạm Quang Toàn), *Trần Nguyễn Thiết Quân* (L Lawliet), *Trần Trung Kiên* (Ispectorgadget), *Nguyễn Đình Tùng* (tungc3sp)... cùng sự góp sức

gián tiếp của nhiều thành viên tích cực trên Diễn đàn Toán học như Nguyen Lam Thinh, nguyenta98, Karl Heinrich Marx, The Gunner, perfectstrong...

Kiến thức đề cập trong chuyên đề tuy không mới nhưng có thể giúp các bạn phần nào hiểu sâu hơn một số khái niệm cơ bản trong Số học cũng như trao đổi cùng các bạn nhiều dạng bài tập hay và khó từ cấp độ dễ đến các bài toán trong các kì thi Học sinh giỏi quốc gia, quốc tế.

Chuyên đề gồm 7 chương. Chương 1 đề cập đến các khái niệm về **Ước và Bội**. **Số nguyên tố** và một số bài toán về nó được giới thiệu trong chương 2. Chương 3 nói sâu hơn về **Các bài toán chia hết**. **Phương trình nghiệm nguyên**, **Phương trình đồng dư** được phác họa trong các chương 4 và 5. **Hệ thặng dư và định lý Thặng dư Trung Hoa** sẽ được gửi đến chúng ta qua chương 6 trước khi kết thúc chuyên đề bằng **Một số bài toán số học hay trên VMF** ở chương 7.

Do thời gian chuẩn bị gấp rút nội dung chuyên đề chưa được đầu tư thật sự tỉ mỉ cũng như có thể còn nhiều sai sót trong các bài viết, chúng tôi mong bạn đọc thông cảm. Mọi sự ủng hộ, đóng góp, phê bình của độc giả sẽ là nguồn động viên tinh thần to lớn cho ban biên tập cũng như cho các tác giả để những phiên bản cập nhật sau của chuyên đề được tốt hơn, đóng góp nhiều hơn nữa cho kho tàng học thuật của cộng đồng toán mạng. Chúng tôi hi vọng qua chuyên đề này sẽ giúp các bạn tìm thêm được cảm hứng trong số học và thêm yêu vẻ đẹp của những con số. Mọi trao đổi góy ý xin gửi về địa chỉ email : contact@diendantoanhoc.net.

Trân trọng,
Nhóm biên tập Chuyên đề Số học.

Mục lục

Chương

1 Ước và Bội

Nguyễn Mạnh Trùng Dương (DUONGLD)
Nguyễn Trần Huy (YEUTOAN11)

Ước và bội là 2 khái niệm quan trọng trong chương trình số học THCS. Chuyên đề này sẽ giới thiệu những khái niệm và tính chất cơ bản về ước, ước số chung, ước chung lớn nhất, bội, bội số chung, bội chung nhỏ nhất. Một số bài tập đề nghị về các vấn đề này cũng sẽ được đề cập đến ở cuối bài viết.

1.1 Ước số, ước số chung, ước số chung lớn nhất

Trong phần này, chúng tôi sẽ trình bày một số khái niệm về ước số, ước số chung và ước số chung lớn nhất kèm theo một vài tính chất của chúng. Một số bài tập ví dụ cho bạn đọc tham khảo cũng sẽ được đưa ra.

1.1.1 Định nghĩa

Định nghĩa 1.1 *Số tự nhiên $d \neq 0$ được gọi là một ước số của số tự nhiên a khi và chỉ khi a chia hết cho d. Ta nói d chia hết a, kí hiệu $d|a$. Tập hợp các ước của a là: $U(a) = \{d \in \mathbb{N} : d|a\}$.* △

Tính chất 1.1– *Nếu $U(a) = \{1; a\}$ thì a là số nguyên tố.* □

Định nghĩa 1.2 *Nếu $U(a)$ và $U(b)$ có những phần tử chung thì những phần tử đó gọi là ước số chung của a và b. Ta kí hiệu:*

$$\begin{aligned} USC(a;b) &= \{d \in \mathbb{N} : (d|a) \wedge (d|b)\} \\ &= \{d \in \mathbb{N} : (d \in U(a)) \wedge (d \in U(b))\}. \end{aligned}$$

Tính chất 1.2– *Nếu $USC(a;b) = \{1\}$ thì a và b nguyên tố cùng nhau.* □

Định nghĩa 1.3 *Số $d \in \mathbb{N}$ được gọi là ước số chung lớn nhất của a và b $(a; b \in \mathbb{Z})$ khi d là phần tử lớn nhất trong tập $USC(a;b)$. Ký hiệu ước chung lớn nhất của a và b là $UCLN(a;b)$, $(a;b)$ hay $gcd(a;b)$.* △

1.1.2 Tính chất

Sau đây là một số tính chất của ước chung lớn nhất:

- Nếu $(a_1; a_2; \ldots; a_n) = 1$ thì ta nói các số $a_1; a_2; \ldots; a_n$ nguyên tố cùng nhau.
- Nếu $(a_m; a_k) = 1, \forall m \neq k, \{m; k\} \in \{1; 2; \ldots; n\}$ thì ta nói các $a_1; a_2; \ldots; a_n$ đôi một nguyên tố cùng nhau.
- $c \in USC(a;b)$ thì $\left(\frac{a}{c}; \frac{b}{c}\right) = \frac{(a;b)}{c}$.
- $d = (a;b) \Leftrightarrow \left(\frac{a}{d}; \frac{b}{d}\right) = 1$.
- $(ca; cb) = c(a;b)$.
- $(a;b) = 1$ và $b|ac$ thì $b|c$.
- $(a;b) = 1$ và $(a;c) = 1$ thì $(a;bc) = 1$.
- $(a;b;c) = ((a;b);c)$.
- Cho $a > b > 0$
  - Nếu $a = b.q$ thì $(a;b) = b$.
  - Nếu $a = bq + r (r \neq 0)$ thì $(a;b) = (b;r)$.

1.1.3 Cách tìm ước chung lớn nhất bằng thuật toán Euclide

Để tìm $(a;b)$ khi a không chia hết cho b ta dùng thuật toán Euclide sau:

- $a = b.q + r_1$ thì $(a;b) = (b;r_1)$.
- $b = r_1.q_1 + r_2$ thì $(b;r_1) = (r_1;r_2)$.
- $\dots$
- $r_{n-2} = r_{n-1}.q_{n-1} + rn$ thì $(r_{n-2};r_{n-1}) = (r_{n-1};r_n)$.
- $r_{n-1} = r_n.q_n$ thì $(r_{n-1};r_n) = r_n$.
- $(a;b) = r_n$.
- $(a;b)$ là số dư cuối cùng khác 0 trong thuật toán Euclide.

1.1.4 Bài tập ví dụ

Ví dụ 1.1. *Tìm* $(2k-1;9k+4), k \in \mathbb{N}^*$. △

Lời giải. Ta đặt $d = (2k-1;9k+4)$. Theo tính chất về ước số chung ta có $d|2k-1$ và $d|9k+4$. Tiếp tục áp dụng tính chất về chia hết ta lại có $d|9(2k-1)$ và $d|2(9k+4)$. Suy ra $d|2(9k+4)-9(2k-1)$ hay $d|17$. Vậy $(2k-1;9k+4) = 1$. ■

Ví dụ 1.2. *Tìm* $(123456789;987654321)$. △

Lời giải. Đặt $b = 123456789; a = 987654321$. Ta nhận thấy a và b đều chia hết cho 9.
Ta lại có :

$$\begin{aligned} a+b &= 1111111110 \\ &= \frac{10^{10}-10}{9}. \\ \Leftrightarrow 9a+9b &= 10^{10}-10 \end{aligned} \tag{1.1}$$

Mặt khác :

$$\begin{aligned} 10b+a &= 9999999999 \\ &= 10^{10}-1. \end{aligned} \tag{1.2}$$

Trừ (1.2) và (1.1) vế theo vế ta được $b-8a=9$. Do đó nếu đặt $d=(a;b)$ thì $9\vdots d$.
Mà a và b đều chia hết cho 9, suy ra $d=9$. ■

Dựa vào thuật toán Euclide, ta có lời giải khác cho Ví dụ 1.2 như sau :
Lời giải. ↱ $987654321 = 123456789.8+9$ thì $(987654321; 123456789) = (123456789; 9)$.

↱ $123456789 = 9.1371421$.

↱ $(123456789; 987654321) = 9$. ■

Ví dụ 1.3. *Chứng minh rằng dãy số* $A_n = \frac{1}{2}n(n+1), n \in \mathbb{N}^*$ *chứa những dãy số vô hạn những số đôi một nguyên tố cùng nhau.* △

Lời giải. Giả sử trong dãy đang xét có k số đôi một nguyên tố cùng nhau là $t_1 = 1; t_2 = 3; \ldots; t_k = m (m \in \mathbb{N}^*)$. Đặt $a = t_1 t_2 \ldots t_k$. Xét số hạng t_{2a+1} trong dãy A_n:

$$\begin{aligned} t_{2a+1} &= \frac{1}{2}(2a+1)(2a+2) \\ &= (a+1)(2a+1) \\ &\geq t_k \end{aligned}$$

Mặt khác ta có $(a+1; a) = 1$ và $(2a+1; a) = 1$ nên $(t_{2a+1}; a) = 1$.
Do đó t_{2a+1} nguyên tố cùng nhau với tất cả k số $\{t_1; t_2; \ldots t_k\}$. Suy ra dãy số A_n chứa vô hạn những số đôi một nguyên tố cùng nhau. ■

1.2 Bội số, bội số chung, bội số chung nhỏ nhất

Tương tự như cấu trúc đã trình bày ở phần trước, trong phần này chúng tôi cũng sẽ đưa ra những định nghĩa, tính chất cơ bản của bội số, bội số chung, bội số chung nhỏ nhất và một số bài tập ví dụ minh họa.

1.2.1 Định nghĩa

Định nghĩa 1.4 *Số tự nhiên m được gọi là một bội số của $a \neq 0$ khi và chỉ khi m chia hết cho a hay a là một ước số của m.* △

Nhận xét. Tập hợp các bội số của $a \neq 0$ là: $B(a) = \{0; a; 2a; \ldots; ka\}, k \in \mathbb{Z}$.

Định nghĩa 1.5 *Số tự nhiên m được gọi là một bội số của $a \neq 0$ khi và chỉ khi m chia hết cho a hay a là một ước số của m* △

Định nghĩa 1.6 *Nếu 2 tập $B(a)$ và $B(b)$ có phần tử chung thì các phần tử chung đó gọi là bội số chung của a và b. Ta ký hiệu bội số chung của a và b: $BSC(a; b)$.*

Định nghĩa 1.7 *Số $m \neq 0$ được gọi là bội chung nhỏ nhất của a và b khi m là phần tử dương nhỏ nhất trong tập $BSC(a; b)$. Ký hiệu : $BCNN(a; b)$, $[a; b]$ hay $lcm(a; b)$.* △

1.2.2 Tính chất

Một số tính chất của bội chung lớn nhất:

- Nếu $[a; b] = M$ thì $\left(\frac{M}{a}; \frac{M}{b}\right) = 1$.
- $[a; b; c] = [[a; b]; c]$.
- $[a; b].(a; b) = a.b$.

1.2.3 Bài tập ví dụ

Ví dụ 1.4. *Tìm $[n; n+1; n+2]$.* △

Lời giải. Đặt $A = [n; n+1]$ và $B = [A; n+2]$. Áp dụng tính chất $[a; b; c] = [[a; b]; c]$, ta có: $B = [n; n+1; n+2]$.
Dễ thấy $(n; n+1) = 1$, suy ra $[n; n+1] = n(n+1)$.

Lại áp dụng tính chất $[a;b]=\dfrac{a.b}{(a;b)}$ thế thì

$$[n;n+1;n+2]=\frac{n(n+1)(n+2)}{(n(n+1);n+2)}$$

.
Gọi $d=(n(n+1);n+2)$. Do $(n+1;n+2)=1$ nên

$$\begin{aligned} d &= (n;n+2)\\ &= (n;2). \end{aligned}$$

Xét hai trường hợp:

- Nếu n chẵn thì $d=2$, suy ra $[n;n+1;n+2]=\dfrac{n(n+1)(n+2)}{2}$.
- Nếu n lẻ thì $d=1$, suy ra $[n;n+1;n+2]=n(n+1)(n+2)$. ■

Ví dụ 1.5. *Chứng minh rằng* $[1;2;\dots 2n]=[n+1;n+2;\dots;2n]$. △

Lời giải. Ta thấy được trong k số nguyên liên tiếp có một và chỉ một số chia hết cho k. Do đó bất trong các số $\{1;2;\dots;2n\}$ đều là ước của một số nào đó trong các số $\{n+1;n+2;\dots;2n\}$. Do đó $[1;2;\dots n;2n]=[n+1;n+2;\dots;2n]$. ■

1.3 Bài tập đề nghị

Thay cho lời kết, chúng tôi xin gửi đến bạn đọc một số bài tập đề nghị để luyện tập nhằm giúp các bạn quen hơn với các khái niệm và các tính chất trình bày trong chuyên đề.

Bài 1. a. Cho $A=5a+3b;B=13a+8b(a;b\in\mathbb{N}^*)$ chứng minh $(A;B)=(a;b)$.

b. Tổng quát $A=ma+nb;B=pa+qb$ thỏa mãn $|mq-np|=1$ với $a,b,m,n,p,q\in\mathbb{N}^*$. Chứng minh $(A;B)=(a;b)$.

Bài 2. Tìm $(6k+5;8k+3)(k\in\mathbb{N})$.

Bài 3. Từ các chữ số $1;2;3;4;5;6$ thành lập tất cả số có sáu chữ số (mỗi số chỉ viết một lần). Tìm $UCLN$ của tất cả các số đó.

Bài 4. Cho $A = 2n+1; B = \dfrac{n(n+1)}{2} (n \in \mathbb{N}^*)$. Tìm $(A;B)$.

Bài 5.
a. Chứng minh rằng trong 5 số tự nguyên liên tiếp bao giờ cũng chọn được một số nguyên tố cùng nhau với các số còn lại.

b. Chứng minh rằng trong 16 số nguyên liên tiếp bao giờ cũng chọn được một số nguyên tố cùng nhau với các số còn lại.

Bài 6. Cho $1 \leq m \leq n (m;n \in \mathbb{N})$.

a. Chứng minh rằng $(2^{2^n}-1; 2^{2^n}+1) = 1$.

b. Tìm $(2^m-1; 2^n-1)$.

Bài 7. Cho $m,n \in \mathbb{N}$ với $(m,n) = 1$. Tìm $(m^2+n^2; m+n)$.

Bài 8. Cho $A = 2^n+3; B = 2^{n+1}+3^{n+1} (n \in \mathbb{N}^*); C = 2^{n+2}+3^{n+2} (n \in \mathbb{N}^*)$. Tìm $(A;B)$ và $(A;C)$.

Bài 9. Cho sáu số nguyên dương $a;b;a';b';d;d'$ sao cho $(a;b) = d; (a';b') = d'$. Chứng minh rằng $(aa';bb';ab';a'b) = dd'$.

Bài 10. Chứng minh rằng dãy số $B_n = \dfrac{1}{6} n(n+1)(n+2) (n \in \mathbb{N}^*)$ chứa vô hạn những số nguyên tố cùng nhau.

Bài 11. Chứng minh rằng dãy số $2^n - 3$ với mọi $n \in N$ và $n \geq 2$ chứa dãy số vô hạn những số nguyên tố cùng nhau.

Bài 12. Chứng minh dãy Mersen $M_n = 2^n - 1 (n \in \mathbb{N}^*)$ chứa dãy số vô hạn những số nguyên tố cùng nhau.

Bài 13. Chứng minh rằng dãy Fermat $F_n = 2^{2^n} + 1 (n \in \mathbb{N})$ là dãy số nguyên tố cùng nhau.

Bài 14. Cho $n \in \mathbb{N}; n > 1$ và $2^n - 2$ chia hết cho n. Tìm $(2^{2^n}; 2^n - 1)$.

Bài 15. Chứng minh rằng với mọi $n \in \mathbb{N}$, phân số $\dfrac{21n+1}{14n+3}$ tối giản.

Bài 16. Cho ba số tự nhiên $a; b; c$ đôi một nguyên tố cùng nhau. Chứng minh rằng $(ab+bc+ca; abc) = 1$.

Bài 17. Cho $a; b \in \mathbb{N}^*$. Chứng minh rằng tồn tại vô số $n \in \mathbb{N}$ sao cho $(a+n; b+n) = 1$.

Bài 18. Giả sử $m; n \in \mathbb{N}(m \geq n)$ thỏa mãn $(199k-1; m) = (1993-1; n)$. Chứng minh rằng tồn tại $t(t \in \mathbb{N})$ sao cho $m = 1993^t.n$.

Bài 19. Chứng minh rằng nếu $a; m \in \mathbb{N}; a > 1$ thì $\left(\dfrac{a^m-1}{a-1}; a-1\right) = (m; a-1)$.

Bài 20. Tìm số nguyên dương n nhỏ nhất để các phân số sau tối giản:

a. $\dfrac{1}{n^{1996}+1995n+2}$,

b. $\dfrac{2}{n^{1996}+1995n+3}$,

c. $\dfrac{1994}{n^{1996}+1995n+1995}$,

d. $\dfrac{1995}{n^{1996}+1995n+1996}$.

Bài 21. Cho 20 số tự nhiên khác 0 là $a_1; a_2; \ldots a_n$ có tổng bằng S và $UCLN$ bằng d. Chứng minh rằng $UCLN$ của $S-a_1; S-a_2; \ldots; S-a_n$ bằng tích của d với một ước nào đó của $n-1$.

Chương

2 Số Nguyên Tố

Nguyễn Trung Hiếu (NGUYENTRUNGHIEUA)
Phạm Quang Toàn (PHẠM QUANG TOÀN)

2.1 Một số kiến thức cơ bản về số nguyên tố

2.1.1 Định nghĩa, định lý cơ bản

Định nghĩa 2.1 *Số nguyên tố là những số tự nhiên lớn hơn 1, chỉ có 2 ước số là 1 và chính nó.* △

Định nghĩa 2.2 *Hợp số là số tự nhiên lớn hơn 1 và có nhiều hơn 2 ước.* △

Nhận xét. Các số 0 và 1 không phải là số nguyên tố cũng không phải là hợp số. Bất kỳ số tự nhiên lớn hơn 1 nào cũng có ít nhất một ước số nguyên tố.

ĐỊNH LÝ 2.1– *Dãy số nguyên tố là dãy số vô hạn.* □

Chứng minh. Giả sử chỉ có hữu hạn số nguyên tố là $p_1; p_2; p_3; ...; p_n$; trong đó p_n là số lớn nhất trong các nguyên tố.
Xét số $N = p_1p_2...p_n + 1$ thì N chia cho mỗi số nguyên tố $p_i (i = \overline{1,n})$ đều dư 1 (*)
Mặt khác N là một hợp số (vì nó lớn hơn số nguyên tố lớn nhất là p_n) do đó N phải có một ước nguyên tố nào đó, tức là N chia hết cho một trong các số p_i (**).
Ta thấy (**) mâu thuẫn (*). Vậy không thể có hữu hạn số nguyên tố.■

Định lý 2.2– *Mọi số tự nhiên lớn hơn 1 đều phân tích được ra thừa số nguyên tố một cách duy nhất (không kể thứ tự các thừa số).* □

Chứng minh. * Mọi số tự nhiên lớn hơn 1 đều phân tích được ra thừa số nguyên tố:
Thật vậy: giả sử điều khẳng định trên là đúng với mọi số m thoả mãn: $1 < m < n$ ta chứng minh điều đó đúng đến n.
Nếu n là nguyên tố, ta có điều phải chứng minh.
Nếu n là hợp số, theo định nghĩa hợp số, ta có: $n = a.b$ (với $a, b < n$)
Theo giả thiết quy nạp: a và b là tích các thừa số nhỏ hơn n nên n là tích cuả các thừa số nguyên tố.
* Sự phân tích là duy nhất:
Giả sử mọi số $m < n$ đều phân tích được ra thừa số nguyên tố một cách duy nhất, ta chứng minh điều đó đúng đến n:
Nếu n là số nguyên tố thì ta được điều phải chứng minh. Nếu n là hợp số: Giả sử có 2 cách phân tích n ra thừa số nguyên tố khác nhau:

$$n = p.q.r....$$
$$n = p'.q'.r'....$$

Trong đó $p, q, r.....$ và $p', q', r'....$ là các số nguyên tố và không có số nguyên tố nào cũng có mặt trong cả hai phân tích đó (vì nếu có số thoả mãn điều kiện như trên, ta có thể chia n cho số đó lúc đó thường sẽ nhỏ hơn n, thương này có hai cách phân tích ra thừa số nguyên tố khác nhau, trái với giả thiết của quy nạp).
Không mất tính tổng quát, ta có thể giả thiết p và p' lần lượt là các số nguyên tố nhỏ nhất trong phân tích thứ nhất và thứ hai.
Vì n là hợp số nên $n > p^2$ và $n > p'^2$. Do $p \neq p \Rightarrow n > p.p'$

Xét $m = n - pp' < n$ được phân tích ra thừa số nguyên tố một cách duy nhất ta thấy:

$$p|n \Rightarrow p|n - pp' \text{ hay } p|m$$

Khi phân tích ra thừa số nguyên tố ta có: $m = n - pp' = p'p.P.Q...$ với $P, Q \in \mathbb{P}$ ($\mathbb{P}$ là tập các số nguyên tố).
$\Rightarrow pp'|n \Rightarrow pp'|p.q.r... \Rightarrow p|q.r... \Rightarrow p$ là ước nguyên tố của $q.r...$
Mà p không trùng với một thừa số nào trong $q, r...$ (điều này trái với gỉa thiết quy nạp là mọi số nhỏ hơn n đều phân tích được ra thừa số nguyên tố một cách duy nhất).
Vậy, điều giả sử không đúng. Định lý được chứng minh. ■

2.1.2 Cách nhận biết một số nguyên tố

Cách 1

Chia số đó lần lượt cho các nguyên tố từ nhỏ đến lớn: $2; 3; 5; 7...$

Nếu có một phép chia hết thì số đó không nguyên tố.

Nếu thực hiện phép chia cho đến lúc thương số nhỏ hơn số chia mà các phép chia vẫn có số dư thì số đó là nguyên tố.

Cách 2

Một số có hai ước số lớn hơn 1 thì số đó không phải là số nguyên tố.

Cho học sinh lớp 6 học cách nhận biết 1 số nguyên tố bằng phương pháp thứ nhất (nêu ở trên), là dựa vào định lý cơ bản:

Ước số nguyên tố nhỏ nhất của một hợp số A là một số không vượt quá $\sqrt{A}$.

Với quy tắc trên trong một khoản thời gian ngắn, với các dấu hiệu chia hết thì ta nhanh chóng trả lời được một số có hai chữ số nào đó là

nguyên tố hay không.

Hệ quả 2.1– *Nếu có số $A > 1$ không có một ước số nguyên tố nào từ 2 đến $\sqrt{A}$ thì A là một nguyên tố.* □

2.1.3 Số các ước số và tổng các ước số của 1 số

Giả sử: $A = p_1^{x_1}.p_2^{x_2}.....p_n x_n$; trong đó: $p_i \in \mathbb{P}; x_i \in \mathbb{N}; i = \overline{1,n}$

Tính chất 2.1– *Số các ước số của A tính bằng công thức:*

$$T(A) = (x_1 + 1)(x_2 + 1).....(x_n + 1)$$

Ví dụ 2.1. $30 = 2.3.5$ *thì* $T(A) = (1+1)(1+1)(1+1) = 8$. *Kiểm tra:* $(30) = \{1; 2; 3; 5; 6; 10; 15; 30\}$ *nên* (30) *có 8 phân tử.* △

Tính chất 2.2– *Tổng các ước một số của A tính bằng công thức:*

$$\sigma(A) = \prod_{i=1}^{n} \frac{p_i^{x_i+1} - 1}{p_i - 1}$$

2.1.4 Hai số nguyên tố cùng nhau

Định nghĩa 2.3 *Hai số tự nhiên được gọi là nguyên tố cùng nhau khi và chỉ khi chúng có ước chung lớn nhất (ƯCLN) bằng 1.* △

Tính chất 2.3– *Hai số tự nhiên liên tiếp luôn nguyên tố cùng nhau.* □

Tính chất 2.4– *Hai số nguyên tố khác nhau luôn nguyên tố cùng nhau.* □

Tính chất 2.5– *Các số a, b, c nguyên tố cùng nhau khi và chỉ khi $(a, b, c) = 1$.* □

Định nghĩa 2.4 *Nhiều số tự nhiên được gọi là nguyên tố sánh đôi khi chúng đôi một nguyên tố cùng nhau.* △

2.1.5 Một số định lý đặc biệt

Định lý 2.3 (Dirichlet)– *Tồn tại vô số số nguyên tố p có dạng: $p = ax + b$ ($x, a, b \in \mathbb{N}$, a, b là 2 số nguyên tố cùng nhau).* □

Việc chứng minh định lý này khá phức tạp, trừ một số trường hợp đặc biệt, chẳng hạn có vô số số nguyên tố dạng: $2x - 1; 3x - 1; 4x + 3; 6x + 5; \ldots$

Định lý 2.4 (Tchebycheff-Betrand)– *Trong khoảng từ số tự nhiên n đến số tự nhiên $2n$ có ít nhất một số nguyên tố ($n > 2$).* □

Định lý 2.5 (Vinogradow)– *Mọi số lẻ lớn hơn 3^3 là tổng của 3 số nguyên tố.* □

2.2 Một số bài toán cơ bản về số nguyên tố

2.2.1 Có bao nhiêu số nguyên tố dạng $ax + b$

Ví dụ 2.2. *Chứng minh rằng: có vô số số nguyên tố có dạng $3x - 1$.*△

Lời giải. Mọi số tự nhiên không nhỏ hơn 2 có 1 trong 3 dạng: $3x; 3x+1$ hoặc $3x - 1$

- Những số có dạng $3x$ (với $x > 1$) là hợp số
- Xét 2 số có dạng $3x + 1$: đó là số $3m + 1$ và số $3n + 1$.

  Xét tích $(3m + 1)(3n + 1) = 9mn + 3m + 3n + 1$. Tích này có dạng: $3x + 1$
- Lấy một số nguyên tố p bất có dạng $3x - 1$, ta lập tích của p với tất cả các số nguyên tố nhỏ hơn p rồi trừ đi 1 ta có: $M = 2.3.5.7....p - 1 = 3(2.5.7....p) - 1$ thì M có dạng $3x - 1$.

  Có 2 khả năng xảy ra:

  1. Khả năng 1: M là số nguyên tố, đó là số nguyên tố có dạng $3x - 1 > p$, bài toán được chứng minh.

2. Khả năng 2: M là hợp số: Ta chia M cho $2, 3, 5, ..., p$ đều tồn tại một số dư khác 0 nên các ước nguyên tố của M đều lớn hơn p, trong các ước này không có số nào có dạng $3x+1$ (đã chứng minh trên). Do đó ít nhất một trong các ước nguyên tố của M phải có dạng $3x$ (hợp số) hoặc $3x+1$

Vì nếu tất cả có dạng $3x+1$ thì M phải có dạng $3x+1$ (đã chứng minh trên). Do đó, ít nhất một trong các ước nguyên tố của M phải có dạng $3x-1$, ước này luôn lớn hơn p.

Vậy: Có vô số số nguyên tố dạng $3x-1$. ■

Ví dụ 2.3. *Chứng minh rằng: Có vô số số nguyên tố có dạng* $4x+3$.△

Lời giải. *Nhận xét.* Các số nguyên tố lẻ không thể có dạng $4x$ hoặc $4x+2$. Vậy chúng chỉ có thể tồn tại dưới 1 trong 2 dạng $4x+1$ hoặc $4x+3$.
Ta sẽ chứng minh có vô số số nguyên tố có dạng $4x+3$.

- Xét tích 2 số có dạng $4x+1$ là: $4m+1$ và $4n+1$.

  Ta có: $(4m+1)(4n+1) = 16mn+4m+4n+1 = 4(4mn+m+n)+1$.

  Vậy tích của 2 số có dạng $4x+1$ là một số cũng có dạng $4x+1$.

- Lấy một số nguyên tố p bất kỳ có dạng $4x+3$, ta lập tích của $4p$ với tất cả các số nguyên tố nhỏ hơn p rồi trừ đi 1 khi đó ta có: $N = 4(2.3.5.7.....p) - 1$. Có 2 khả năng xảy ra

  1. N là số nguyên tố $\Rightarrow N = 4(2.3.5.7....p) - 1$ có dạng $4x-1$. Những số nguyên tố có dạng $4x-1$ cũng chính là những số có dạng $4x+3$ và bài toán được chứng minh.
  2. N là hợp số. Chia N cho $2, 3, 5, ..., p$ đều được các số dư khác 0. Suy ra các ước nguyên tố của N đều lớn hơn p.

  Các ước này không thể có dạng $4x$ hoặc $4x+2$ (vì đó là hợp số). Cũng không thể toàn các ước có dạng $4x+1$ vì như thế N phải có dạng $4x+1$. Như vậy trong các ước nguyên tố của N có ít nhất 1 ước có dạng $4x-1$ mà ước này hiển nhiên lớn hơn p.

Vậy: Có vô số số nguyên tố có dạng $4x-1$ (hay có dạng $4x+3$). ■

Trên đây là một số bài toán chứng minh đơn giản của định lý Dirichlet: Có vô số số nguyên tố dạng $ax+b$ trong đó $a,b,x \in \mathbb{N}, (a,b)=1$.

2.2.2 Chứng minh số nguyên tố

Ví dụ 2.4. *Chứng minh rằng: $(p-1)!$ chia hết cho p nếu p là hợp số, không chia hết cho p nếu p là số nguyên tố.* △

Lời giải.
- Xét trường hợp p là hợp số: Nếu p là hợp số thì p là tích của các thừa số nguyên tố nhỏ hơn p và số mũ các luỹ thừa này không thể lớn hơn số mũ của chính các luỹ thừa ấy chứa trong $(p-1)!$. Vậy: $(p-1)!\vdots p$ (đpcm).
- Xét trường hợp p là số nguyên tố: Vì $p \in \mathbb{P} \Rightarrow p$ nguyên tố cùng nhau với mọi thừa số của $(p-1)!$ (đpcm). ■

Ví dụ 2.5. *Cho 2^m-1 là số nguyên tố. Chứng minh rằng m cũng là số nguyên tố.* △

Lời giải. Giả sử m là hợp số $\Rightarrow m = p.q$ $(p,q \in \mathbb{N}; p,q>1)$
Khi đó: $2^m-1 = 2^{pq}-1 = (2^p)^q-1 = (2^p-1)((2^p)^{q-1}+(2^p)^{q-2}+.....+1)$
vì $p>1 \Rightarrow 2^p-1>1$ và $(2^p)^{q-1}+(2^p)^{q-2}+.....+1>1$
Dẫn đến 2^m-1 là hợp số :trái với giả thiết $2^m\breve{}1$ là số nguyên tố.
Vậy m phải là số nguyên tố (đpcm) ■

Ví dụ 2.6. *Chứng minh rằng: mọi ước nguyên tố của $1994!-1$ đều lớn hơn 1994.* △

Lời giải. Gọi p là ước số nguyên tố của $1994!-1$

Giả sử $p \le 1994 \Rightarrow 1994.1993.....3.2.1\vdots p \Rightarrow 1994!\vdots p$.

Mà $1994!-1\vdots p \Rightarrow 1\vdots p$ (vô lý)
Vậy: $p>1994$ (đpcm). ■

Ví dụ 2.7. *Chứng minh rằng: $n>2$ thì giữa n và $n!$ có ít nhất 1 số nguyên tố (từ đó suy ra có vô số số nguyên tố).* △

Lời giải. Vì $n > 2$ nên $k = n! - 1 > 1$, do đó k có ít nhất một ước số nguyên tố p. Tương tự bài tập 3, ta chứng minh được mọi ước nguyên tố p của k đều lớn hơn k.
Vậy: $p > n \Rightarrow n < p < n! - 1 < n!$ (đpcm) ■

2.2.3 Tìm số nguyên tố thỏa mãn điều kiện cho trước

Ví dụ 2.8. *Tìm tất cả các giá trị của số nguyên tố p để: $p + 10$ và $p + 14$ cũng là số nguyên tố.* △

Lời giải. Nếu $p = 3$ thì $p + 10 = 3 + 10 = 13$ và $p + 14 = 3 + 14 = 17$ đều là các số nguyên tố nên $p = 3$ là giá trị cần tìm.
Nếu $p > 3 \Rightarrow p$ có dạng $3k + 1$ hoặc dạng $3k - 1$

- Nếu $p = 3k + 1$ thì $p + 14 = 3k + 15 = 3(k + 5) \vdots 3$
- Nếu $p = 3k - 1$ thì $p + 10 = 3k + 9 = 3(k + 3) \vdots 3$

Vậy nếu $p > 3$ thì hoặc $p + 10$ hoặc $p + 14$ là hợp số : không thỏa mãn bài. Vậy $p = 3$. ■

Ví dụ 2.9. *Tìm $k \in \mathbb{N}$ để trong 10 số tự nhiên liên tiếp:*

$$k + 1; k + 2; k + 3; ....k + 10$$

có nhiều số nguyên tố nhất. △

Lời giải. Nếu $k = 0$: từ 1 đến 10 có 4 số nguyên tố: $2; 3; 5; 7$.
Nếu $k = 1$: từ 2 đến 11 có 5 số nguyên tố: $2; 3; 5; 7; 11$.
Nếu $k > 1$: từ 3 trở đi không có số chẵn nào là số nguyên tố. Trong 5 số lẻ liên tiếp, ít nhất có 1 số là bội số của 3 do đó, dãy sẽ có ít hơn 5 số nguyên tố.
Vậy với $k = 1$, dãy tương ứng: $k + 1; k + 2, ...k + 10$ có chứa nhiều số nguyên tố nhất (5 số nguyên tố). ■

Ví dụ 2.10. *Tìm tất cả các số nguyên tố p để: $2^p + p^2$ cũng là số nguyên tố.* △

Lời giải. Xét 3 trường hợp:

- $p = 2 \Rightarrow 2^p + p^2 = 2^2 + 2^2 = 8 \notin \mathbb{P}$
- $p = 3 \Rightarrow 2^p + p^2 = 2^3 + 3^2 = 17 \in \mathbb{P}$
- $p > 3 \Rightarrow p \not\vdots 3$. Ta có $2^p + p^2 = (p^2 - 1) + (2^p + 1)$.
  Vì p lẻ $\Rightarrow 2^p + 1 \vdots 3$ và $p^2 - 1 = (p+1)(p-1) \vdots 3 \Rightarrow 2^p + p^2 \notin \mathbb{P}$

Vậy có duy nhất 1 giá trị $p = 3$ thoả mãn. ■

Ví dụ 2.11. *Tìm tất cả các số nguyên tố p sao cho: $p|2^p + 1$.* △

Lời giải. Vì $p \in \mathbb{P} : p|2^p + 1 \Rightarrow p > 2 \Rightarrow (2; p) = 1$
Theo định lý Fermat, ta có: $p|2^{p-1} - 1$. Mà

$$p|2^p + 1 \Rightarrow p|2(2^{p-1} - 1) + 3 \Rightarrow p|3 \Rightarrow p = 3$$

Vậy: $p = 3$. ■

2.2.4 Nhận biết số nguyên tố

Ví dụ 2.12. *Nếu p là số nguyên tố và 1 trong 2 số $8p + 1$ và $8p - 1$ là số nguyên tố thì số còn lại là số nguyên tố hay hợp số?* △

Lời giải.
- Nếu $p = 2 \Rightarrow 8p + 1 = 17 \in \mathbb{P}; 8p - 1 = 15 \notin \mathbb{P}$
- Nếu $p = 3 \Rightarrow 8p - 1 = 23 \in \mathbb{P}; 8p - 1 = 25 \notin \mathbb{P}$
- Nếu $p > 3$, xét 3 số tự nhiên liên tiếp: $8p - 1; 8p$ và $8p + 1$. Trong 3 số này ắt có 1 số chia hết cho 3. Nên một trong hai số $8p + 1$ và $8p - 1$ chia hết cho 3.

Kết luận: Nếu $p \in \mathbb{P}$ và 1 trong 2 số $8p + 1$ và $8p - 1$ là số nguyên tố thì số còn lại phải là hợp số. ■

Ví dụ 2.13. *Nếu $p \geq 5$ và $2p + 1$ là các số nguyên tố thì $4p + 1$ là nguyên tố hay hợp số?* △

Lời giải. Xét 3 số tự nhiên liên tiếp: $4p; 4p + 1; 4p + 2$. Trong 3 số ắt có một số là bội của 3.
Mà $p \geq 5; p \in \mathbb{P}$ nên p có dạng $3k + 1$ hoặc $3k + 2$

- Nếu $p = 3k + 1$ thì $2p + 1 = 6k + 3 \vdots 3$: (trái với giả thiết)

- Nếu $p = 3k+2$. Khi đó $4p+1 = 4(3k+2)+1 = 12k+9 \vdots 3 \Rightarrow 4p+1$ là hợp số ■

Ví dụ 2.14. *Trong dãy số tự nhiên có thể tìm được 1997 số liên tiếp nhau mà không có số nguyên tố nào hay không ?* △

Lời giải. Chọn dãy số: $(a_i) : a_i = 1998! + i + 1$ $(i = \overline{1, 1997}) \Rightarrow a_i \vdots i + 1$ $\forall i = \overline{1, 1997}$
Như vậy: Dãy số $a_1; a_2; a_3; .....a_{1997}$ gồm có 1997 số tự nhiên liên tiếp không có số nào là số nguyên tố. ■

Ví dụ 2.15 (Tổng quát bài tập 2.14). *Chứng minh rằng có thể tìm được 1 dãy số gồm n số tự nhiên liên tiếp $(n > 1)$ không có số nào là số nguyên tố ?* △

Lời giải. Ta chọn dãy số sau: $(a_i) : a_i = (n+1)! + i + 1 \Rightarrow a_i \vdots i + 1$ $\forall i = \overline{1, n}$.
Bạn đọc hãy tự chứng minh dãy (a_i) ở trên sẽ gồm có n số tự nhiên liên tiếp trong đó không có số nào là số nguyên tố cả. ■

2.2.5 Các dạng khác

Ví dụ 2.16. *Tìm 3 số nguyên tố sao cho tích của chúng gấp 5 lần tổng của chúng.* △

Lời giải. Gọi 3 số nguyên tố phải tìm là a, b, c. Ta có: $abc = 5(a + b + c) \Rightarrow abc \vdots 5$
Vì a, b, c có vai trò bình đẳng nên không mất tính tổng quát, giả sử: $a \vdots 5 \Rightarrow a = 5$
Khi đó: $5bc = 5(5 + b + c) \Leftrightarrow 5 + b + c = bc \Leftrightarrow (c - 1)(b - 1) = 6$
Do vậy: $\left[\begin{array}{l} \left\{ \begin{array}{l} b-1=1 \\ c-1=6 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} b=2 \\ c=7 \end{array} \right. \text{ chọn} \\ \left\{ \begin{array}{l} b-1=2 \\ c-1=3 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} b=3 \\ c=4 \end{array} \right. \text{ loại} \end{array} \right.$
Vậy bộ số $(a; b; c)$ cần tìm là hoán vị của $(2; 5; 7)$. ■

Ví dụ 2.17. *Tìm $p, q \in \mathbb{P}$ sao cho $p^2 = 8q + 1$.* △

Lời giải. Ta có:

$$p^2 = 8q + 1 \Rightarrow 8q = p^2 - 1 = (p+1)(p-1) \tag{2.1}$$

Do $p^2 = 8q + 1$: lẻ $\Rightarrow p^2$: lẻ $\Rightarrow p$: lẻ. Đặt $p = 2k + 1$.
Thay vào (2.1) ta có:

$$8q = 2k(2k+2) \Rightarrow 2q = k(k+1) \tag{2.2}$$

Nếu $q = 2 \Rightarrow 4 = k(k+1) \Rightarrow$ không tìm được $k \in \mathbb{N}$
Vậy $q > 2$. Vì $q \in \mathbb{P} \Rightarrow (2, q) = 1$.
Từ (2.2) ta có:

a) $k = 2$ và $q = k + 1 \Rightarrow k = 2; q = 3$. Thay kết quả trên vào (2.2) ta có: $p = 2.2 + 1 = 5$

b) $q = k$ và $2 = k + 1 \Rightarrow q = 1$:loại.

Vậy $(q; p) = (5; 3)$. ■

2.3 Bài tập

2.3.1 Bài tập có hướng dẫn

Bài 1. Ta biết rằng có 25 số nguyên tố nhỏ hơn 100. Tổng của 25 số nguyên tố nhỏ hơn 100 là số chẵn hay số lẻ?

HD :Trong 25 số nguyên tố nhỏ hơn 100 có chứa một số nguyên tố chẵn duy nhất là 2, còn 24 số nguyên tố còn lại là số lẻ. Do đó tổng của 25 số nguyên tố là số chẵn.

Bài 2. Tổng của 3 số nguyên tố bằng 1012. Tìm số nguyên tố nhỏ nhất trong ba số nguyên tố đó.

HD: Vì tổng của 3 số nguyên tố bằng 1012, nên trong 3 số nguyên tố đó tồn tại ít nhất một số nguyên tố chẵn. Mà số nguyên tố chẵn duy nhất là 2 và là số nguyên tố nhỏ nhất. Vậy số nguyên tố nhỏ nhất trong 3 số nguyên tố đó là 2.

Bài 3. Tổng của 2 số nguyên tố có thể bằng 2003 hay không? Vì sao?

HD: Vì tổng của 2 số nguyên tố bằng 2003, nên trong 2 số nguyên tố đó tồn tại 1 số nguyên tố chẵn. Mà số nguyên tố chẵn duy nhất là 2. Do đó số nguyên tố còn lại là 2001. Do 2001 chia hết cho 3 và 2001 > 3. Suy ra 2001 không phải là số nguyên tố.

Bài 4. Tìm số nguyên tố p, sao cho $p+2; p+4$ cũng là các số nguyên tố.

Bài 5. Cho p và $p+4$ là các số nguyên tố ($p > 3$). Chứng minh rằng $p+8$ là hợp số.

HD: Vì p là số nguyên tố và $p > 3$, nên số nguyên tố p có 1 trong 2 dạng:

- *Nếu $p = 3k+2$ thì $p+4 = 3k+6 = 3(k+2) \Rightarrow p+4 \vdots 3$ và $p+4 > 3$. Do đó $p+4$ là hợp số: trái đề bài.*
- *Nếu $p = 3k+1$ thì $p+8 = 3k+9 = 3(k+3) \Rightarrow p+8 \vdots 3$ và $p+8 > 3$. Do đó $p+8$ là hợp số.*

Bài 6. Chứng minh rằng mọi số nguyên tố lớn hơn 2 đều có dạng $4n+1$ hoặc $4n-1$.

Bài 7. Tìm số nguyên tố, biết rằng số đó bằng tổng của hai số nguyên tố và bằng hiệu của hai số nguyên tố.

HD: Giả sử a, b, c, d, e là các số nguyên tố và $d > e$. Theo đề bài:

$$a = b + c = d - e \quad (*)$$

Từ (*) $\Rightarrow a > 2$ nên a là số nguyên tố lẻ $\Rightarrow b+c; d-e$ là số lẻ. Do b, d là các số nguyên tố $\Rightarrow b, d$ là số lẻ $\Rightarrow c, e$ là số chẵn.
$\Rightarrow c = e = 2$ (do c, elà số nguyên tố) $\Rightarrow a = b+2 = d-2 \Rightarrow d = b+4$.
Vậy ta cần tìm số nguyên tố b sao cho $b+2$ và $b+4$ cũng là các số nguyên tố.

Bài 8. Tìm tất cả các số nguyên tố x, y sao cho: $x^2 - 6y^2 = 1$.

Bài 9. Cho p và $p+2$ là các số nguyên tố ($p > 3$). Chứng minh rằng $p + 1 \vdots 6$.

2.3.2 Bài tập không có hướng dẫn

Bài 1. Tìm số nguyên tố p sao cho các số sau cũng là số nguyên tố:

a) $p+2$ và $p+10$.
b) $p+10$ và $p+20$.
c) $p+10$ và $p+14$.
d) $p+14$ và $p+20$.
e) $p+2$ và $p+8$.
f) $p+2$ và $p+14$.
g) $p+4$ và $p+10$.
h) $p+8$ và $p+10$.

Bài 2. Tìm số nguyên tố p sao cho các số sau cũng là số nguyên tố:

a) $p+2, p+8, p+12, p+14$
b) $p+2, p+6, p+8, p+14$
c) $p+6, p+8, p+12, p+14$
d) $p+2, p+6, p+8, p+12, p+14$
e) $p+6, p+12, p+18, p+24$
f) $p+18, p+24, p+26, p+32$
g) $p+4, p+6, p+10, p+12, p+16$

Bài 3. Cho trước số nguyên tố $p > 3$ thỏa

a) $p+4 \in \mathbb{P}$. Chứng minh rằng: $p+8$ là hợp số.
b) $2p+1 \in \mathbb{P}$. Chứng minh rằng: $4p+1$ là hợp số.
c) $10p+1 \in \mathbb{P}$. Chứng minh rằng: $5p+1$ là hợp số.

d) $p+8 \in \mathbb{P}$. Chứng minh rằng: $p+4$ là hợp số.

e) $4p+1 \in \mathbb{P}$. Chứng minh rằng: $2p+1$ là hợp số.

f) $5p+1 \in \mathbb{P}$. Chứng minh rằng: $10p+1$ là hợp số.

g) $8p+1 \in \mathbb{P}$. Chứng minh rằng: $8p-1$ là hợp số.

h) $8p-1 \in \mathbb{P}$. Chứng minh rằng: $8p+1$ là hợp số.

i) $8p^2-1 \in \mathbb{P}$. Chứng minh rằng: $8p^2+1$ là hợp số.

j) $8p^2+1 \in \mathbb{P}$. Chứng minh rằng: $8p^2-1$ là hợp số.

Bài 4. Chứng minh rằng:

a) Nếu p và q là hai số nguyên tố lớn hơn 3 thì $p^2-q^2 \vdots 24$.

b) Nếu $a, a+k, a+2k (a,k \in \mathbb{N}^*)$ là các số nguyên tố lớn hơn 3 thì $k \vdots 6$.

Bài 5. a) Một số nguyên tố chia cho 42 có số dư r là hợp số. Tìm số dư r.

b) Một số nguyên tố chia cho 30 có số dư r. Tìm số dư r biết rằng r không là số nguyên tố.

Bài 6. Tìm số nguyên tố có ba chữ số, biết rằng nếu viết số đó theo thứ tự ngược lại thì ta được một số là lập phương của một số tự nhiên.

Bài 7. Tìm số tự nhiên có 4 chữ số, chữ số hàng nghìn bằng chữ số hàng đơn vị, chữ số hàng trăm bằng chữ số hàng chục và số đó viết được dưới dạng tích của 3 số nguyên tố liên tiếp.

Bài 8. Tìm 3 số nguyên tố là các số lẻ liên tiếp.

Bài 9. Tìm 3 số nguyên tố liên tiếp p, q, r sao cho $p^2+q^2+r^2 \in \mathbb{P}$.

Bài 10. Tìm tất cả các bộ ba số nguyên tố a, b, c sao cho $abc < ab+bc+ca$.

Bài 11. Tìm 3 số nguyên tố p, q, r sao cho $p^q+q^p=r$.

Bài 12. Tìm các số nguyên tố x, y, z thoả mãn $x^y + 1 = z$.

Bài 13. Tìm số nguyên tố $\overline{abcd}$ thỏa $\overline{ab}, \overline{ac}$ là các số nguyên tố và $b^2 = \overline{cd} + b - c$.

Bài 14. Cho các số $p = b^c + a, q = a^b + c, r = c^a + b (a, b, c \in \mathbb{N}^*)$ là các số nguyên tố. Chứng minh rằng 3 số p, q, r có ít nhất hai số bằng nhau.

Bài 15. Tìm tất cả các số nguyên tố x, y sao cho:

a) $x^2 - 12y^2 = 1$

b) $3x^2 + 1 = 19y^2$

c) $5x^2 - 11y^2 = 1$

d) $7x^2 - 3y^2 = 1$

e) $13x^2 - y^2 = 3$

f) $x^2 = 8y + 1$

Bài 16. Chứng minh rằng điều kiện cần và đủ để p và $8p^2 + 1$ là các số nguyên tố là $p = 3$.

Bài 17. Chứng minh rằng: Nếu $a^2 - b^2$ là một số nguyên tố thì $a^2 - b^2 = a + b$.

Bài 18. Chứng minh rằng mọi số nguyên tố lớn hơn 3 đều có dạng $6n+1$ hoặc $6n - 1$.

Bài 19. Chứng minh rằng tổng bình phương của 3 số nguyên tố lớn hơn 3 không thể là một số nguyên tố.

Bài 20. Cho số tự nhiên $n \geq 2$. Gọi $p_1, p_2, ..., p_n$ là những số nguyên tố sao cho $p_n \leq n+1$. Đặt $A = p_1.p_2...p_n$. Chứng minh rằng trong dãy số các số tự nhiên liên tiếp: $A + 2, A + 3, ..., A + (n + 1)$, không chứa một số nguyên tố nào.

Bài 21. Chứng minh rằng: Nếu p là số nguyên tố thì $2.3.4...(p - 3)(p - 2) - 1 \vdots p$.

Bài 22. Chứng minh rằng: Nếu p là số nguyên tố thì $2.3.4...(p-2)(p-1)+1 \vdots p$.

2.4 Phụ lục: Bạn nên biết

Mười số nguyên tố có 93 chữ số lập thành cấp số cộng

Sau đây là một số nguyên tố gồm 93 chữ số:

$$100996972469714247637786655587969840329509324689190041$$
$$80360341775890434170334888215906722971 9$$

Kỷ lục này do 70 nhà toán học lập được năm 1998 thật khó mà đánh bại được. Họ mất nhiều tháng tính toán mới tìm được mười số nguyên tố tạo thành một cấp số cộng.

Từ mục trò chơi trong 1 tạp chí khoa học, hai nhà nghiên cứu ở trường Đại học Lyonl (Pháp) đã đào sâu ý tưởng: Tìm 6 số nguyên tố sao cho hiệu 2 số liên tiếp luôn luôn như nhau. Điều đó là dễ đối với các chuyên gia nhưng họ muốn đi xa hơn. Cũng không có vấn đề gì khó khăn đối với một dãy 7 số. Họ cần sự hỗ trợ một chút để đạt được 8 số, một sự hỗ trợ hơn nữa để đạt tới 9 số. Cuối cùng tháng 3 năm 1998 có 70 nhà toán học từ khắp trên thế giới cùng với 200 máy điện toán hoạt động liên tục đã tìm ra 10 số, mỗi số có 93 chữ số, mà hiệu số của 2 số liên tiếp luôn luôn là 210. Từ số nguyên tố ở trên chỉ cần thêm vào 210 là được số nguyên tố thứ 2....

Kỷ lục có lẽ dừng ở đó: Theo ước tính của các nhà khoa học muốn tìm được 1 dãy 11 số nguyên tố thì phải mất hơn 10 tỉ năm.

"Sinh ba" rất ít, phải chăng "sinh đôi" lại rất nhiều

Ta biết rằng các số nguyên tố "có thể xa nhau tuỳ ý" điều này thể hiện ở bài tập:

Bài toán 2.1. *Cho trước số nguyên dương n tuỳ ý. Chứng minh rằng tồn tại n số tự nhiên liên tiếp mà mỗi số trong chúng đều là hợp số.* △

Vậy nhưng, các số nguyên tố cũng "có thể rất gần nhau". Cặp số $(2, 3)$ là cặp số tự nhiên liên tiếp duy nhất mà cả hai bên đều là số nguyên tố. Cặp số đ(p, q)ược gọi là cặp số "sinh đôi", nếu cả 2 đều là số nguyên tố và $q = p + 2$. Bộ 3 số (p, q, r) gọi là bộ số nguyên tố "sinh ba" nếu cả 3 số p,q,r đều là các số nguyên tố và $q = p + 2; r = q + 2$.

Bài toán 2.2. *Tìm tất cả các bộ số nguyên tố "sinh ba"?* △

Đây là một bài toán dễ, dùng phương pháp chứng minh duy nhất ta tìm ra bộ $(3, 5, 7)$ là bộ ba số nguyên tố sinh ba duy nhất, các bộ 3 số lẻ lớn hơn 3 luôn có 1 số là hợp số vì nó chia hết cho 3.
Từ bài toán 2.2 thì bài toán sau trở thành một giả thuyết lớn đang chờ câu trả lời.

Dự đoán 2.1– *Tồn tại vô hạn cặp số sinh đôi.* □

Số hoàn hảo (hoàn toàn) của những người Hy Lạp cổ đại

Người Hy Lạp cổ đại có quan niệm thần bí về các số. Họ rất thú vị phát hiện ra các số hoàn hảo, nghĩa là các số tự nhiên mà tổng các ước số tự nhiên thực sự của nó (các ước số nhỏ hơn số đó) bằng chính nó.

Chẳng hạn:

$$6 = 1 + 2 + 3 \qquad 28 = 1 + 2 + 4 + 7 + 14$$

Người Hy Lạp cổ đại đã biết tìm tất cả các số hoàn hảo chẵn nghĩa là họ đã làm được bài toán sau đây:

Bài toán 2.3. *Một số tự nhiên chẵn $n \neq 0$ là số hoàn hảo nếu và chỉ nếu: $n = 2^{m+1}(2^m - 1)$. Trong đó m là số tự nhiên khác 0 sao cho $2^m - 1$ là số nguyên tố.* △

Từ đó ta có giả thuyết

Dự đoán 2.2– *Không tồn tại số hoàn hảo lẻ.* □

Ở bài toán 2.3 trên, số nguyên tố dạng $2^m - 1$ gọi là số nguyên tố Merseme. Các số nguyên tố Merseme có vai trò rất quan trọng. Cho đến nay người ta vẫn chưa biết có hữu hạn hay vô hạn số nguyên tố Merseme.

Dự đoán 2.3– *Tồn tại vô hạn số nguyên tố Merseme.* □

Năm 1985 số nguyên tố lớn nhất mà người ta biết là số $2^{132049} - 1$ gồm 39751 chữ số ghi trong hệ thập phân. Gần đây 2 sinh viên Mỹ đã tìm ra một số nguyên tố lớn hơn nữa đó là số $2^{216091} - 1$ gồm 65050 chữ số.

Ta biết rằng với học sinh lớp 6 để thử xem số A có ít hơn 20 chữ số có là số nguyên tố không bằng cách thử xem A có chia hết cho số nào nhỏ hơn A hay không, thì để tìm hết các số nguyên tố với chiếc máy siêu điện toán cần hàng thế kỷ !!!

David SlowinSky đã soạn một phần mềm, làm việc trên máy siêu điện toán Gray-2 , sau 19 giờ ông đã tìm ra số nguyên tố $2^{756839} - 1$. Số này viết trong hệ thập phân sẽ có 227832 chữ số- viết hết số này cần 110 trang văn bản bình thường. Hoặc nếu viết hàng ngang những số trên phông chữ .VnTime Size 14 thì ta cần khoảng 570 m.

Lời Kết

Thông qua đề tài này, chúng ta có thể khẳng định rằng: Toán học có mặt trong mọi công việc, mọi lĩnh vực của cuộc sống quanh ta, nó không thể tách rời và lãng quên được, nên chúng ta phải hiểu biết và nắm bắt được nó một cách tự giác và hiệu quả.

Mục đích của đề tài này là trang bị những kiến thức cơ bản có đào sâu có nâng cao và rèn luyện tư duy toán học cho học sinh, tạo ra nền tảng tin cậy để các em có vốn kiến thức nhất định làm hành trang cho

những năm học tiếp theo.

Với điều kiện có nhiều hạn chế về thời gian, về năng lực trình độ nên trong khuôn khổ đề tài này phân chia dạng toán, loại toán chỉ có tính tương đối. Đồng thời cũng mới chỉ đưa ra lời giải chứ chưa có phương pháp, thuật làm rõ ràng. Tuy đã có cố gắng nhiều nhưng chnsg tôi tự thấy trong đề tài này còn nhiều hạn chế. Chúng tôi rất mong nhận được những ý kiến đóng góp của các thầy cô giáo cùng bạn đọc để toán học thật sự có ý nghĩa cao đẹp như câu ngạn ngữ Pháp đã viết:

"Toán học là Vua của các khoa học"
"Số học là Nữ hoàng"

Chương

3 Bài toán chia hết

Phạm Quang Toàn (Phạm Quang Toàn)

Chia hết là một đề tài quan trọng trong chương trình Số học của bậc THCS. Đi kèm theo đó là các bài toán khó và hay. Bài viết này xin giới thiệu với bạn đọc những phương pháp giải các bài toán chia hết: phương pháp xét số dư, phương pháp quy nạp, phương pháp đồng dư, v.v...

3.1 Lý thuyết cơ bản

3.1.1 Định nghĩa về chia hết

Định nghĩa 3.1 *Cho hai số nguyên a và b trong đó $b \neq 0$, ta luôn tìm được hai số nguyên q và r duy nhất sao cho*

$$a = bq + r$$

với $0 \leq r < b$.
Trong đó, ta nói a là số bị chia, b là số chia, q là thương, r là số dư.△

Như vậy, khi a chia cho b thì có thể đưa ra các số dư $r \in \{0; 1; 2; \cdots ; |b|\}$.

Đặc biệt, với $r = 0$ thì $a = bq$, khi đó ta nói a chia hết cho b (hoặc a là bội của b, hoặc b là ước của a). Ta kí hiệu $b \mid a$. Còn khi a không chia

hết cho b, ta kí hiệu $b \nmid a$.

Sau đây là một số tính chất thường dùng, chứng minh được suy ra trực tiếp từ định nghĩa.

3.1.2 Tính chất

Sau đây xin giới thiệu một số tính chất về chia hết, việc chứng minh khá là dễ dàng nên sẽ dành cho bạn đọc. Ta có với a, b, c, d là các số nguyên thì:

Tính chất 3.1– *Nếu* $a \neq 0$ *thì* $a \mid a$, $0 \mid a$. □

Tính chất 3.2– *Nếu* $b \mid a$ *thì* $b \mid ac$. □

Tính chất 3.3– *Nếu* $b \mid a$ *và* $c \mid b$ *thì* $c \mid a$. □

Tính chất 3.4– *Nếu* $c \mid a$ *và* $c \mid b$ *thì* $c \mid (ax \pm by)$ *với* x, y *nguyên.*

Tính chất 3.5– *Nếu* $b \mid a$ *và* $a \mid b$ *thì* $a = b$ *hoặc* $a = -b$.

Tính chất 3.6– *Nếu* $c \mid a$ *và* $d \mid b$ *thì* $cd \mid ab$.

Tính chất 3.7– *Nếu* $b \mid a, c \mid a$ *thì* $BCNN(b; c) \mid a$.

Tính chất 3.8– *Nếu* $c \mid ab$ *và* $UCLN(b, c) = 1$ *thì* $c \mid a$.

Tính chất 3.9– *Nếu* $p \mid ab$, p *là số nguyên tố thì* $p \mid a$ *hoặc* $p \mid b$. □

Từ tính chất trên ta suy ra hệ quả

Hệ quả 3.1– *Nếu* $p \mid a^n$ *với* p *là số nguyên tố,* n *nguyên dương thì* $p^n \mid a^n$. □

3.1.3 Một số dấu hiệu chia hết

Ta đặt $N = \overline{a_n a_{n-1} \dots a_1 a_0}$
Dấu hiệu chia hết cho $2; 5; 4; 25; 8; 125$

$$\begin{aligned} 2 \mid N &\Leftrightarrow 2 \mid a_0 \Leftrightarrow a_0 \in \{0; 2; 4; 6; 8\} \\ 5 \mid N &\Leftrightarrow 5 \mid a_0 \Leftrightarrow a_0 \in \{0; 5\} \\ 4; 25 \mid N &\Leftrightarrow 4; 25 \mid \overline{a_1 a_0} \\ 8; 125 \mid N &\Leftrightarrow 8; 125 \mid \overline{a_2 a_1 a_0} \end{aligned}$$

Dấu hiệu chia hết cho 3 *và* 9

$$3; 9 \mid N \Leftrightarrow 3; 9 \mid (a_0 + a_1 + \cdots + a_{n-1} + a_n)$$

Một số dấu hiệu chia hết khác

$$\begin{aligned} 11 \mid N &\Leftrightarrow 11 \mid [(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)] \\ 101 \mid N &\Leftrightarrow 101 \mid [(\overline{a_1 a_0} + \overline{a_5 a_4} + \cdots) - (\overline{a_3 a_2} + \overline{a_7 a_6} + \cdots)] \\ 7; 13 \mid N &\Leftrightarrow 7; 37 \mid [(\overline{a_2 a_1 a_0} + \overline{a_8 a_7 a_6} + \cdots) - (\overline{a_5 a_4 a_3} + \overline{a_{11} a_{10} a_9} + \cdots)] \\ 37 \mid N &\Leftrightarrow 37 \mid (\overline{a_2 a_1 a_0} + \overline{a_5 a_4 a_3} + \cdots + \overline{a_n a_{n-1} a_{n-2}}) \\ 19 \mid N &\Leftrightarrow 19 \mid \left(a_n + 2a_{n-1} + 2^2 a_{n-2} + \cdots + 2^n a_0\right) \end{aligned}$$

3.2 Phương pháp giải các bài toán chia hết

3.2.1 Áp dụng định lý Fermat nhỏ và các tính chất của chia hết

Định lý Fermat nhỏ

Định lý 3.1 (Định lý Fermat nhỏ)– *Với mọi số nguyên a và số nguyên tố p thì $a^p \equiv p \pmod p$.* □

Chứng minh. 1. Nếu $p \mid a$ thì $p \mid (a^5 - a)$.

2. Nếu $p \nmid a$ thì $2a, 3a, 4a, \cdots, (p-1)a$ cũng không chia hết cho p. Gọi $r_1, r_2, \cdots, r_{p-1}$ lần lượt là số dư khi chia $a, 2a, 3a, \cdots, (p-1)a$ cho p. thì chúng sẽ thuộc tập $\{1; 2; 3; \cdots; p-1\}$ và đôi một khác nhau (vì chẳng hạn nếu $r_1 = r_3$ thì $p \mid (3a - a)$ hay $p \mid 2a$,

chỉ có thể là $p = 2$, mà $p = 2$ thì bài toán không đúng). Do đó $r_1 r_2 \cdot r_{p-1} = 1 \cdot 2 \cdot 3 \cdots (p-1)$. Ta có

$$\begin{aligned} a &\equiv r_1 \pmod p \\ 2a &\equiv r_2 \pmod p \\ &\cdots \\ (p-1)a &\equiv r_{p-1} \pmod p \end{aligned}$$

Nhân vế theo vế ta suy ra

$$1\cdot 2\cdot 3\cdots (p-1)\cdot a^{p-1} \equiv r_1 r_2 \cdots r_{p-1} \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p$$

Vì $UCLN(a,p) = 1$ nên $a^p \equiv a \pmod p$.

Như vậy với mọi số nguyên a và số nguyên tố p thì $a^p \equiv a \pmod p$. ■

Nhận xét. Ta có thể chứng minh định lý bằng quy nạp. Ngoài ra, định lý còn được phát biểu dưới dạng sau:

Định lý 3.2– *Với mọi số nguyên a, p là số nguyên tố, $UCLN(a,p) = 1$ thì $a^{p-1} \equiv 1 \pmod p$.* □

Phương pháp sử dụng tính chất chia hết và áp dụng định lý Fermat nhỏ

Cơ sở: Sử dụng các tính chất chia hết và định lý Fermat nhỏ để giải toán.

Ví dụ 3.1. *Cho a và b là hai số tự nhiên. Chứng minh rằng $5a^2+15ab-b^2$ chia hết cho 49 khi và chỉ khi $3a+b$ chia hết cho 7.* △

Lời giải. $\Rightarrow$) Giả sử $49 \mid 5a^2 + 15ab - b^2 \Rightarrow 7 \mid 5a^2 + 15ab - b^2 \Rightarrow 7 \mid (14a^2 + 21ab) - (5a^2 + 15ab - b^2) \Rightarrow 7 \mid (9a^2 + 6ab + b^2) \Rightarrow 7 \mid (3a+b)^2 \Rightarrow 7 \mid 3a+b$.

$\Leftarrow$) Giả sử $7 \mid 3a+b$. Đặt $3a+b = 7c$ ($c \in \mathbb{Z}$. Khi đó $b = 7c - 3a$. Như vậy

$$\begin{aligned} \Rightarrow 5a^2 + 15ab - b^2 &= 5a^2 + 15a(7c-3a) - (7c-3a)^2 \\ &= 49(c^2 + 3ac - a^2) \end{aligned}$$

chia hết cho 49.
Vậy $5a^2 + 15ab - b^2$ chia hết cho 49 khi và chỉ khi $3a + b$ chia hết cho 7. ■

Ví dụ 3.2. *Cho* $11 \mid (16a + 17b)(17a + 16b)$ *với* a, b *là hai số nguyên. Chứng minh rằng* $121 \mid (16a + 17b)(17a + 16b)$. △

Lời giải. Ta có theo đầu bài, vì 11 nguyên tố nên ít nhất một trong hai số $16a + 17b$ và $17a + 16b$ chia hết cho 11. Ta lại có $(16a + 17b) + (17a + 16b) = 33(a + b)$ chia hết cho 11. Do đó nếu một trong hai số $16a + 17b$ và $17a + 16b$ chia hết cho 11 thì số còn lại cũng chia hết cho 11. Cho nên $121 \mid (16a + 17b)(17a + 16b)$. ■

Ví dụ 3.3. *Chứng minh rằng* $A = 1^{30} + 2^{30} + \cdot + 11^{30}$ *không chia hết cho* 11. △

Lời giải. Với mọi $a = 1, 2, \cdots, 10$ thì $(a, 10) = 1$. Do đó theo định lý Fermat bé thì $a^{10} \equiv 1 \pmod{11} \Rightarrow a^{30} \equiv 1 \pmod{11}$ với mọi $a = 1, 2, \cdots, 10$ và $11^{30} \equiv 0 \pmod{11}$. Như vậy

$$\begin{aligned} A &\equiv \underbrace{1 + 1 + \cdots + 1}_{10 \text{ số } 1} + 0 \pmod{11} \\ &\equiv 10 \pmod{11} \Rightarrow 11 \nmid A \end{aligned}$$

Ví dụ 3.4. *Cho* p *và* q *là hai số nguyên tố phân biệt. Chứng minh rằng* $p^{q-1} + q^{p-1} - 1$ *chia hết cho* pq. △

Lời giải. Vì q nguyên tố nên theo định lý Fermat nhỏ thì

$$p^{q-1} \equiv 1 \pmod{q}$$

Do đó

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$$

Vì q và p có vai trò bình đẳng nên ta cũng dễ dàng suy ra

$$q^{p-1} + p^{q-1} \equiv 1 \pmod{p}.$$

Cuối cùng vì $UCLN(q, p) = 1$ nên $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ hay $p^{q-1} + q^{p-1} - 1$ chia hết cho pq. ■

Bài tập đề nghị

Bài 1. Chứng minh rằng $11a+2b$ chia hết cho 19 khi và chỉ khi $18a+5b$ chia hết cho 19 với a, b là các số nguyên.

Bài 2. Chứng minh rằng $2a + 7$ chia hết cho 7 khi và chỉ khi $3a^2 + 10ab - 8b^2$.

Bài 3. Cho p là số nguyên tố lớn hơn 5. Chứng minh rằng nếu n là số tự nhiên có $p-1$ chữ số và các chữ số đó đều bằng 1 thì n chia hết cho p.

Bài 4. Giả sử $n \in \mathbb{N}, n \geq 2$. Xét các số tự nhiên $a_n = \overline{11\cdot 1}$ được viết bởi n chữ số 1. Chứng minh rằng nếu a_n là một số nguyên tố thì n là ước của $a_n - 1$.

Bài 5. Giả sử a và b là các số nguyên dương sao cho $2a-1, 2b-1$ và $a+b$ đều là số nguyên tố. Chứng minh rằng $a^b + b^a$ và $a^a + b^b$ đều không chia hết cho $a+b$.

Bài 6. Chứng minh rằng với mọi số nguyên tố p thì tồn tại số nguyên n sao cho $2^n + 3^n + 6^n - 1$ chia hết cho p.

3.2.2 Xét số dư

Cơ sở: Để chứng minh $A(n)$ chia hết cho p, ta xét các số n dạng $n = kp + r$ với $r \in \{0; 1; 2; \cdots; p-1\}$.
Chẳng hạn, với $p = 5$ thì số nguyên n có thể viết lại thành $5k; 5k+1; 5k+2; 5k+3; 5k+4$. Ta thế mỗi dạng này vào các vị trí của n rồi lý luận ra đáp số. Sau đây là một số ví dụ

Ví dụ 3.5. *Tìm $k \in \mathbb{N}$ để tồn tại $n \in \mathbb{N}$ sao cho*

$$4 \mid n^2 - k$$

với $k \in \{0; 1; 2; 3\}$. △

Lời giải. Giả sử tồn tại $k \in \mathbb{N}$ để tồn tại $n \in \mathbb{N}$ thỏa mãn $4 \mid n^2 - k$.
Ta xét các Trường hợp: $(m \in \mathbb{N}^*)$

1. Nếu $n = 4m$ thì $n^2 - k = 16m^2 - k$ chia hết cho 4 khi và chỉ khi $4 \mid k$ nên $k = 0$.

2. Nếu $n = 4m \pm 1$ thì $n^2 - k = 16m^2 \pm 8m + 1 - k$ chia hết cho 4 khi và chỉ khi $4 \mid 1 - k$ nên $k = 1$.

3. Nếu $n = 4m \pm 2$ thì $n^2 - k = 16m^2 \pm 16m + 4 - k$ chia hết cho 4 khi và chỉ khi $4 \mid k$ nên $k = 0$.

Vậy $k = 0$ hoặc $k = 1$. ■

Ví dụ 3.6. *Chứng minh rằng với mọi $n \in \mathbb{N}$ thì $6 \mid n(2n+7)(7n+1)$.* △

Lời giải. Ta thấy một trong hai số n và $7n + 1$ là số chẵn $\forall n \in \mathbb{N}$. Do đó $2 \mid n(2n+7)(7n+1)$. Ta sẽ chứng minh $3 \mid n(2n+7)(7n+1)$. Thật vậy, xét

1. Với $n = 3k$ thì $3 \mid n(2n + 7)(7n + 1)$.

2. Với $n = 3k + 1$ thì $2n + 7 = 6k + 9$ chia hết cho 3 nên $3 \mid n(2n + 7)(7n + 1)$.

3. Với $n = 3k + 2$ thì $7n + 1 = 21k + 15$ chia hết cho 3 nên $3 \mid n(2n + 7)(7n + 1)$.

Do đó $3 \mid n(2n+7)(7n+1)$ mà $(2, 3) = 1$ nên $6 \mid n(2n+7)(7n+1)$ $\forall n \in \mathbb{N}$. ■

Ví dụ 3.7. *(HSG 9, Tp Hồ Chí Minh, vòng 2, 1995) Cho x, y, z là các số nguyên thỏa mãn*

$$(x - y)(y - z)(z - x) = x + y + z \tag{3.1}$$

Chứng minh rằng $27 \mid (x + y + z)$. △

Lời giải. Xét hai trường hợp sau

1. Nếu ba số x, y, z chia hết cho 3 có các số dư khác nhau thì các hiệu $x-y, y-z, z-x$ cùng không chia hết cho 3. Mà $3 \mid (x+y+z)$ nên từ (3.1) suy ra vô lí .

2. Nếu ba số x, y, z chỉ có hai số chia cho 3 có cùng số dư thì trong ba hiệu $x-y, y-z, z-x$ có một hiệu chia hết cho 3. Mà $3 \nmid (x+y+z)$ nên từ (3.1) suy ra vô lí.

Vậy x, y, z chia cho 3 có cùng số dư, khi đó $x-y, y-z, z-x$ đều chia hết cho 3. Từ (3.1) ta suy ra $27 \mid (x+y+z)$, ta có đpcm. ■

Bài tập đề nghị

Bài 1. i) Tìm số tự nhiên n để $7 \mid (2^n - 1)$.
ii) Chứng minh rằng $7 \nmid (2^n + 1) \ \ \forall n \in \mathbb{N}$.

Bài 2. Chứng minh rằng với mọi số nguyên a thì $a(a^6 - 1)$ chia hết cho 7.

Bài 3. Tìm n để $13 \mid 3^{2n} + 3^n + 1$.

Bài 4. Chứng minh rằng với mọi $a, b \in \mathbb{N}$ thì $ab(a^2 - b^2)(4a^2 - b^2)$ luôn luôn chia hết cho 5.

Bài 5. Chứng minh rằng $24 \mid (p-1)(p+1)$ với p là số nguyên tố lớn hơn 3.

Bài 6. Chứng minh rằng không tồn tại số nguyên a để $a^2 + 1$ chia hết cho 12.

Bài 7. Chứng minh rằng với mọi số nguyên x, y, z nếu $6 \mid x+y+z$ thì $6 \mid x^3 + y^3 + z^3$.

Bài 8. Cho $ab = 2011^{2012}$, với $a, b \in \mathbb{N}$. Hỏi tổng $a + b$ có chia hết cho 2012 hay không ?

Bài 9. Số $3^n + 2003$ trong đó n là số nguyên dương có chia hết cho 184 không ?

Bài 10. Cho các số nguyên dương x, y, z thỏa mãn $x^2+y^2=z^2$. Chứng minh rằng xyz chia hết cho 60.

Bài 11. Cho các số nguyên dương x, y, z thỏa mãn $x^2+y^2=2z^2$. Chứng minh rằng x^2-y^2 chia hết cho 84.

Bài 12. Cho $n>3$, $(n\in\mathbb{N})$. Chứng minh rằng nếu $2^n=10a+b$, $(0<b<9)$ thì $6\mid ab$.

3.2.3 Phân tích

Phân tích thành tích

Cơ sở: Để chứng minh $A(n)$ chia hết cho p, ta phân tích $A(n)=D(n)p$, còn nếu trong ta không thể đưa ra cách phân tích như vậy, ta có thể viết $p=kq$.

- Nếu $(k,q)=1$ thì ta chứng minh $A(n)$ cùng chia hết cho k và q.
- Nếu $(k,q)\neq 1$ thì ta viết $A(n)=B(n)C(n)$ và chứng minh $B(n)$ chia hết cho k, $C(n)$ chia hết cho q.

Ví dụ 3.8. *Cho n là một số nguyên dương. Chứng minh rằng*

$$2^n \mid (n+1)(n+2)\cdots(2n).$$

Lời giải. Ta có

$$\begin{aligned}(n+1)(n+2)\cdots(2n) &= \frac{(2n)!}{n!} = \frac{(1.3.5...(2n-1))(2.4.6...2n)}{n!}\\ &= 1.3.5...(2n-1).2^n.\frac{n!}{n!}\\ &= 1.3.5...(2n-1).2^n.\end{aligned}$$

Do đó $2^n \mid (n+1)(n+2)\cdots(2n)$. ■

Ví dụ 3.9. *Chứng minh rằng với mọi số nguyên n thì $6 \mid n^3 - n$.* △

Lời giải. Phân tích

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

Biểu thức là tích ba số nguyên liên tiếp nên tồn tại ít nhất một trong ba số một số chia hết cho 2 và một số chia hết cho 3. Mà $(2,3) = 1$ nên $6 \mid n^3 - n$. ■

Ví dụ 3.10. *Chứng minh rằng $n^6 - n^4 - n^2 + 1$ chia hết cho 128 với n lẻ.* △

Lời giải. Ta có

$$n^6 - n^4 - n^2 + 1 = (n^2-1)^2(n+1) = (n-1)^2(n+1)^2$$

Vì n lẻ nên đặt $n = 2k,\ k \in \mathbb{N}$, suy ra

$$(n^2-1)^2 = \left[(2k+1)^2 - 1\right] = (4k^2+4k)^2 = [4k(k+1)]^2$$

Vậy $64 \mid (n^2-1)^2$. Vì n lẻ nên $2 \mid n+1$, suy ra đpcm. ■

Ví dụ 3.11. *Cho ba số nguyên dương khác nhau x, y, z. Chứng minh rằng $(x-y)^5 + (y-z)^5 + (x-z)^5$ chia hết cho $5(x-y)(y-z)(x-z)$.* △

Lời giải. Ta có

$$\begin{aligned}
& (x-y)^5 + (y-z)^5 + (x-z)^5 \\
= \ & (x-z+z-y)^5 + (y-z)^5 + (z-x)^5 \\
= \ & (x-z)^5 + 5(x-z)^4(z-y) + 10(x-z)^3(z-y)^2 \\
& +10(x-z)^4(z-y) + 10(x-z)^3(z-y)^2 \\
& +10(x-z)^2(z-y)^3 + 5(x-z)(z-y)^4 \\
= \ & 5(x-z)(z-y)\times \\
& \times \left[(x-z)^3 + 2(x-z)^2(z-y) + 2(x-z)(z-y)^2 + (z-y)^3\right].
\end{aligned}$$

Nhưng ta cũng có:

$$\begin{aligned}
& (x-z)^3+2(x-z)^2(z-y)+2(x-z)(z-y)^2+(z-y)^3\\
= \; & (x-y+y-z)^3+2(x-y+y-z)^2(z-y)\\
& +2(x-y+y-z)(z-y)^2+(z-y)^3\\
= \; & (x-y)^3+2(x-y)^2(y-z)+3(x-y)(y-z)^2\\
& +(y-z)^3+2(x-y)^2(z-y)\\
& +4(x-y)(y-z)(z-y)+2(y-z)^2(z-y)\\
& +2(x-y)(z-y)^2+2(y-z)(z-y)^2+(z-y)^3\\
= \; & (x-y)^3+3(x-y)^2(y-z)+3(x-y)(y-z)^2\\
& +2(x-y)^2(z-y)+4(x-y)(y-z)(z-y)+2(x-y)(z-y)^2,
\end{aligned}$$

Biểu thức cuối cùng có nhân tử chung $(x-y)$. Ta suy ra điều phải chứng minh. ■

Bài tập đề nghị

Bài 1. Chứng minh rằng nếu a, k là các số nguyên, a lẻ thì $2^{k+1} \mid (a^{2^k}-1)$.

Bài 2. Chứng minh rằng n^5-n chia hết cho 30 với mọi $n \in \mathbb{Z}$.

Bài 3. Chứng minh rằng $3n^4-14n^3+21n^2-10n$ chia hết cho 24 với mọi $n \in \mathbb{Z}$.

Bài 4. Chứng minh rằng n^5-5n^3+4n chia hết cho 120 với mọi $n \in \mathbb{Z}$.

Bài 5. Chứng minh rằng n^3-3n^2-n+3 chia hết cho 48 với mọi n lẻ, $n \in \mathbb{Z}$.

Bài 6. Chứng minh rằng $n^8-n^6-n^4+n^2$ chia hết cho 1152 với mọi số nguyên n lẻ.

Bài 7. Chứng minh rằng $n^4-4n^3-4n^2+16n$ chia hết cho 348 với mọi n là số nguyên chẵn.

Bài 8. Chứng minh rằng $n^4-14n^3+71n^2-154n+120$ chia hết cho 24 với mọi số tự nhiên n.

Bài 9. Cho x, y, z là các số nguyên khác 0. Chứng minh rằng nếu $x^2 - yz = a, y^2 - zx = b, z^2 - xy = c$ thì tổng $(ax + by + cz)$ chia hết cho tổng $(a + b + c)$.

Bài 10. Cho m, n là hai số chính phương lẻ liên tiếp. Chứng minh rằng $mn - m - n + 1$ chia hết cho 192.

Bài 11. *(HSG 9 TQ 1970)* Chứng minh rằng $n^{12} - n^8 - n^4 + 1$ chia hết cho 512 với mọi số tự nhiên n lẻ.

Bài 12. *(HSG 9 TQ 1975)* Chứng minh rằng $n^4 + 6n^3 + 11n^2 + 6n$ chia hết cho 24 với mọi số nguyên dương n.

Tách tổng

Cơ sở: Để chứng minh $A(n)$ chia hết cho p, ta biến đổi $A(n)$ thành tổng nhiều hạng tử rồi chứng minh mỗi hạng tử đều chia hết cho p.

Ta có thể sử dụng một số hằng đẳng thức áp dụng vào chia hết, ví dụ như:

> Cho a, b là các số thực và n là số nguyên dương. Khi đó ta có
>
> $$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1})$$

Ta sẽ có hệ quả là:

Hệ quả 3.2– *Nếu $a - b \neq 0$ thì $a^n - b^n$ chia hết cho $a - b$.* □

Hệ quả 3.3– *Nếu $a + b \neq 0$ và n lẻ thì $a^n + b^n$ chia hết cho $a + b$.* □

Hệ quả 3.4– *Nếu $a + b \neq 0$ và n chẵn thì $a^n - b^n$ chia hết cho $a + b$* □

Ví dụ 3.12. *Chứng minh rằng $ax^2 + bx + c \in \mathbb{Z}$, $\forall x \in \mathbb{Z}$ khi và chỉ khi $2a, a + b, c \in \mathbb{Z}$* △

Lời giải. Phân tích

$$\begin{aligned} ax^2+bx+c &= ax^2-ax+(a+b)x+c \\ &= 2a.\frac{x(x-1)}{2}+(a+b)x+c \in \mathbb{Z}, \quad \forall x \in \mathbb{Z}. \end{aligned}$$

Ví dụ 3.13. *Chứng minh rằng* $6 \mid (a^3+5a)$ $\forall a \in \mathbb{N}$. △

Lời giải. Phân tích $a^3+5a = (a^3-a)+6a$. Hiển nhiên đúng vì $6 \mid n^3-n$ (chứng minh ở ví dụ Equation 4.27). ■

Nhận xét. Từ ví dụ Equation 4.27 ta cũng có thể đưa ra các bài toán sau, chứng minh cũng bằng cách vận dụng phương pháp tách tổng:

Bài toán 3.1. *Cho* $m, n \in \mathbb{Z}$. *Chứng minh rằng* $6 \mid m^2n^2(m-n)$. △

Bài toán 3.2. *Cho* $a, b, c \in \mathbb{Z}$. *Chứng minh rằng* $6 \mid (a^3+b^3+c^3)$ *khi và chỉ khi* $6 \mid (a+b+c)$ △

Bài toán 3.3. *Cho* $a \in \mathbb{Z}$. *Chứng minh rằng* $\dfrac{a}{3}+\dfrac{a^2}{2}+\dfrac{a^3}{6} \in \mathbb{Z}$ △

Bài toán 3.4. *Viết số* 2011^{2012} *thành tổng các số nguyên dương. Dem tổng lập phương tất cả các số hạng đó chia cho* 3 *thì được dư là bao nhiêu ?* △

Ví dụ 3.14. *Cho* m, n *là các số nguyên thỏa mãn:*

$$\frac{m}{n} = 1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{1334}+\frac{1}{1335}$$

Chứng minh rằng $2003 \mid m$. △

Lời giải. Để ý rằng 2003 là số nguyên tố. Ta có

$$\begin{aligned}
\frac{m}{n} &= 1-\frac{1}{2}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{1334}+\frac{1}{1335}\\
&= \left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{1335}\right)-2\left(\frac{1}{2}+\frac{1}{4}+\frac{1}{6}+\cdots+\frac{1}{1334}\right)\\
&= \left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{1335}\right)-\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{667}\right)\\
&= \frac{1}{668}+\frac{1}{669}+\cdots+\frac{1}{1335}\\
&= \left(\frac{1}{668}+\frac{1}{1335}\right)+\left(\frac{1}{669}+\frac{1}{1334}\right)+\cdots+\left(\frac{1}{1001}+\frac{1}{1002}\right)\\
&= 2003\left(\frac{1}{668.1335}+\frac{1}{669.1334}+\cdots+\frac{1}{1001.1002}\right)\\
&= 2003.\frac{p}{q}
\end{aligned}$$

Ở đây p là số nguyên còn $q = 668\cdot 669\cdots 1335$. Vì 2003 nguyên tố nên $(q, 2003) = 1$.
Do đó từ $(*)$ suy ra $2003pn = mq$.
Vì p, n nguyên nên suy ra $2003|mq$ mà $(q, 2003) = 1$ nên $2003|m$. ■

Ví dụ 3.15. *Chứng minh rằng với mọi số tự nhiên n thì $A = 2005^n + 60^n - 1897^n - 168^n$ chia hết cho 2004.* △

Lời giải. Ta có $2004 = 12\times 167$. Vì $(12, 167) = 1$ nên để chứng minh A chia hết cho 2004 ta chứng minh A chia hết cho 12 và 167.
Áp dụng tính chất $a^n - b^n$ chia hết cho $a - b$ với mọi n tự nhiên và $a-b\neq 0$ suy ra $2005^n - 1897^n$ chia hết cho $2005 - 1897 = 108 = 12\times 9$, hay $2005^n - 1897^n$ chia hết cho 12. Tương tự thì $168^n - 60^n$ chia hết cho 12. Vậy A chia hết cho 12.
Tiếp tục phân tích

$$A = (2005^n - 168^n) - (1897^n - 60^n).$$

Lập luận tương tự như trên thì $2005^n - 168^n$ và $1897^n - 60^n$ chia hết cho 167, tức A chia hết cho 167. Vậy ta có điều phải chứng minh. ■

Ví dụ 3.16. *(Đề thi tuyển sinh ĐHKHTN-ĐHQG Hà Nội, vòng 1, năm 2007-2008) Cho a, b là hai số nguyên dương và $a+1, b+2007$ đều chia hết cho 6. Chứng minh rằng $4^a + a + b$ chia hết cho 6.* △

Lời giải. Phân tích

$$4^a + a + b = (4^a + 2) + (a + 1) + (b + 2007) - 2010$$
$$4^a + 2 = 4^a - 1 + 3 = (4 - 1)(4^{a-1} + \cdots 1) + 3$$

Như vậy $3 \mid 4^a + 2$. Do đó $4^a + a + b$ là tổng của các số nguyên dương chia hết cho 6 nên $4^a + a + b$ chia hết cho 6. ■

Bài tập đề nghị

Bài 1. Đưa ra các mở rộng từ bài tập đề nghị của phương pháp phân tích thành tích thành các bài toán vận dụng phương pháp tách tổng (giống như cách mở rộng của ví dụ 1.9).

Bài 2. *(Hungary MO 1947)* Chứng minh rằng $46^n + 296.13^n$ chia hết cho 1947 với mọi số tự nhiên n lẻ.

Bài 3. Chứng minh rằng $20^n + 16^n - 3^n - 1$ chia hết cho 323 với mọi số tự nhiên n chẵn.

Bài 4. Chứng minh rằng $2903^n - 803^n - 464^n + 261^n$ chia hết cho 1897 với mọi số tự nhiên n.

Bài 5. Chứng minh rằng với mọi số nguyên $n > 1$ ta có $n^n + 5n^2 - 11n + 5$ chia hết cho $(n-1)^2$.

Bài 6. *(HSG 9 Tp Hà Nội, vòng 2, 1998)* Chứng minh rằng $1997 \mid m$ với $m, n \in \mathbb{N}$ thỏa mãn

$$\frac{m}{n} = 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{1}{1329} - \frac{1}{1330} + \frac{1}{1331}.$$

Bài 7. Chứng minh rằng $3^{2n+1} + 2^{n+2}$ chia hết cho 7 với mọi $n \in \mathbb{N}$.

Bài 8. Chứng minh rằng $2003^{2005} + 2017^{2015}$ chia hết cho 12.

Bài 9. Cho p là số tự nhiên lẻ và các số nguyên a, b, c, d, e thỏa mãn $a+b+c+d+e$ và $a^2+b^2+c^2+d^2+e^2$ đều chia hết cho p. Chứng minh rằng số $a^5+b^5+c^5+d^5+e^5-5abcde$ cũng chia hết cho p.

Bài 10. *(Canada Training for IMO 1987)*
Kí hiệu:
$$1\cdot 3\cdot 5\cdots(2n-1) = (2n-1)!!$$
$$2\cdot 4\cdot 6\cdots(2n) = (2n)!!.$$
Chứng minh rằng $(1985)!! + (1986)!!$ chia hết cho 1987.

Bài 11. Chứng minh rằng số $2222^{5555} + 5555^{2222}$ chia hết cho 7.

Bài 12. Cho k là số nguyên dương sao cho số $p = 3k+1$ là số nguyên tố và
$$\frac{1}{1\cdot 2} + \frac{1}{3\cdot 4} + \cdots + \frac{1}{(2k-1)2k} = \frac{m}{n}$$
với hai số nguyên dương nguyên tố cùng nhau m và n.Chứng minh m chia hết cho p.
(Tạp chí Mathematics Reflections, đăng bởi T.Andreescu)

3.2.4 Xét đồng dư

Định nghĩa và một số tính chất

Định nghĩa 3.2 *Cho a, b là các số nguyên và n là số nguyên dương. Ta nói, a đồng dư với b theo modun n và kí hiệu $a \equiv b \pmod n$ nếu a và b có cùng số dư khi chia cho n.* △

Như vậy $a \equiv n \pmod n \iff n \mid (a-b)$. Ví dụ: $2012 \equiv 2 \pmod 5$.

Tính chất (bạn đọc tự chứng minh)
Cho a, b, c, d, n là các số nguyên.

Tính chất 3.10–
$$a \equiv a \pmod n,$$
$$a \equiv b \pmod n \Leftrightarrow b \equiv a \pmod n,$$
$$a \equiv b \pmod n,\ b \equiv c \pmod n \Rightarrow a \equiv c \pmod n.$$
□

Tính chất 3.11– $\begin{cases} a \equiv b \pmod n \\ c \equiv d \pmod n \end{cases} \Rightarrow \begin{cases} a \pm c \equiv b \pm d \pmod n \\ ac \equiv bd \pmod n \end{cases}$ □

Tính chất 3.12– $a \equiv b \pmod n \Rightarrow a^k \equiv b^k \pmod n, \ \forall k \geq 1.$ □

Tính chất 3.13– $a \equiv b \pmod n \Rightarrow ac \equiv bc \pmod{mc}, \ c > 0$ □

Tính chất 3.14– $(a+b)^n \equiv b^n \pmod a, \ (a > 0).$ □

Tính chất 3.15– *Nếu* d *là ước chung dương của* a, b *và* m *thì* $a \equiv b \pmod m$ *thì* $\dfrac{a}{d} \equiv \dfrac{b}{d} \pmod{\dfrac{m}{d}}$.

Tính chất 3.16– $a \equiv b \pmod m$, c *là ước chung của* a *và* b, $(c, m) = 1$ *thì* $\dfrac{a}{c} \equiv \dfrac{b}{c} \pmod m$.

Phương pháp đồng dư thức để giải các bài toán chia hết

Cơ sở: Sử dụng các tính chất và định nghĩa trên để giải các bài toán chia hết.

Ví dụ 3.17. *Chứng minh rằng với mọi số tự nhiên* n *thì* $7 \mid 8^n + 6$. △

Lời giải. Ta có $8^n \equiv 1 \pmod 7 \implies 8^n + 6 \equiv 7 \equiv 0 \pmod 7$. ■

Ví dụ 3.18. *Chứng minh rằng* $19 \mid 7 \cdot 5^{2n} + 12 \cdot 6^n$. *với mọi số nguyên dương* n. △

Lời giải. Ta có $5^2 = 25 \equiv 6 \pmod{19} \implies (5^2)^n \equiv 6^n \pmod{19} \implies 7 \cdot 5^{2n} \equiv 7 \cdot 6^n \pmod{19} \implies 7 \cdot 5^{2n} + 12 \cdot 6^n \equiv 19 \cdot 6^n \equiv 0 \pmod{19}$. ■

Ví dụ 3.19. *Viết liên tiếp các số* $111, 112, \cdots, 888$ *để được số* $A = 111112 \cdots 888$. *Chứng minh rằng* $1998 \mid A$. △

Lời giải. Ta thấy A chẵn nên $2 \mid A$. Mặt khác

$$A = 111 \cdot 1000^{777} + 112 \cdot 1000^{776} + \cdots + 888.$$

Do $1000^k \equiv 1 \pmod{999}$, $\forall k \in \mathbb{N}$ nên

$$A \equiv 111 + 112 + \cdots + 888 \equiv 0 \pmod{999}.$$

Suy ra $999 \mid A$, và $(999, 2) = 1$ nên $1998 \mid A$. ■

Ví dụ 3.20. *Chứng minh rằng* $7 \mid 5555^{2222} + 2222^{5555}$. △

Lời giải. Ta có

$$\begin{aligned} &2222 \equiv -4 \pmod 7 \implies 2222^{5555} \equiv (-4)^{5555} \pmod 7 \\ &5555 \equiv 4 \pmod 7 \implies 5555^{2222} \equiv 4 \pmod 7 \end{aligned}$$

$$\implies 5555^{2222} + 2222^{5555} \equiv -4^{5555} + 4^{2222} \pmod 7$$

Lại có

$$\begin{aligned} -4^{5555} + 4^{2222} &= -4^{2222}\left(4^{3333} - 1\right) \\ &= -4^{2222}\left(64^{1111} - 1\right) \end{aligned}$$

Và $64 \equiv 1 \pmod 7 \implies 64^{1111} - 1 \equiv 0 \pmod 7$.
Do đó $7 \mid 5555^{2222} + 2222^{5555}$ ■

Bài tập đề nghị

Bài 1. Một số bài tập ở phương pháp phân tích có thể giải bằng phương pháp đồng dư thức.

Bài 2. Chứng minh rằng $333^{555^{777}} + 777^{555^{333}}$ chia hết cho 10.

Bài 3. Chứng minh rằng số $11^{10^{1967}} - 1$ chia hết cho 10^{1968}.

Bài 4. Cho $9 \mid a^3 + b^3 + c^3$, $\forall a, b, c \in \mathbb{Z}$. Chứng minh rằng $3 \mid a \cdot b \cdot c$.

Bài 5. Chứng minh rằng $222^{333} + 333^{222}$ chia hết cho 13.

Bài 6. Chứng minh rằng $9^n + 1$ không chia hết cho 100, $\forall n \in \mathbb{N}$.

Bài 7. Chứng minh rằng với mọi số nguyên không âm n thì $2^{5n+3} + 5^n \cdot 3^{n+1}$ chia hết cho 17.

Bài 8. Tìm $n \in \mathbb{N}$ sao cho $2n^3 + 3n = 19851986$.

Bài 9. Viết liên tiếp 2000 số 1999 ta được số $X = 19991999\cdots1999$. Tìm số dư trong phép chia X cho 10001.

Bài 10. Chứng minh rằng $100 \mid 7^{7^{7^7}} - 7^{7^7}$.

Bài 11. Cho $b^2 - 4ac$ và $b^2 + 4ac$ là hai số chính phương với $a, b, c \in \mathbb{N}$. Chứng minh rằng $30 \mid abc$.

3.2.5 Quy nạp

Cơ sở : Để chứng minh mệnh đề đúng với mọi số tự nhiên $n \geq p$, ta làm như sau:

- Kiểm tra mệnh đề đúng với $n = p$.
- Giả sử mệnh đề đúng với $n = k$. Ta đi chứng minh mệnh đề cũng đúng với $n = k + 1$.

Ví dụ 3.21. *Chứng minh rằng $A = 4^n + 15 - 1$ chia hết cho 9 với mọi $n \in \mathbb{N}^*$.* △

Lời giải. Với $n = 1 \implies A = 18$ chia hết cho 9.
Giả sử bài toán đúng với $n = k$. Khi đó $9 \mid 4^k + 15^k - 1$, hay $4^k + 15^k - 1 = 9q$ với $q \in \mathbb{N}^*$. Suy ra $4^k = 9q - 15k + 1$.
Ta đi chứng minh bài toán đúng với $n = k+1$, tức $9 \mid 4^{k+1} + 15(k+1) - 1$.
Thật vậy:

$$\begin{aligned} 4^{k+1} + 15(k+1) - 1 &= 4 \cdot 4^k + 15k + 14 \\ &= 4(9q - 15k + 1) + 15k + 14 \\ &= 36q - 45k + 18 \end{aligned}$$

chia hết cho 9. Ta có đpcm. ■

Ví dụ 3.22. *(HSG 9 TQ 1978)Chứng minh rằng số được tạo bởi 3^n chữ số giống nhau thì chia hết cho 3^n với $1 \leq n,\ n \in \mathbb{N}$.* △

Lời giải. Với $n = 1$, bài toán hiển nhiên đúng.
Giả sử bài toán đúng với $n = k$, tức $3^k \mid \underbrace{\overline{aa\cdots a}}_{3^n \text{ số } a}$.
Với $n = k+1$ ta có:

$$\begin{aligned}\underbrace{\overline{aa\cdots a}}_{3^{k+1}} &= \underbrace{\overline{aa\cdots a}}_{3^k}\underbrace{\overline{aa\cdots a}}_{3^k}\underbrace{\overline{aa\cdots a}}_{3^k} \\ &= \underbrace{\overline{aa\cdots a}}_{3^k} \times 1\underbrace{00\cdots 0}_{3^k-1}\underbrace{00\cdots 0}_{3^k-1}1\end{aligned}$$

chia hết cho 3^{k+1}. Ta có đpcm. ■

Ví dụ 3.23. *Chứng minh rằng với mọi $n \in \mathbb{N}^*, k$ là số tự nhiên lẻ thì*

$$2^{n+2} \mid k^{2^n} - 1$$

Lời giải. Với $n = 1$ thì $k^{2^n} - 1 = k^2 - 1 = (k+1)(k-1)$. Do k lẻ,nên đặt $k = 2m+1$ với $m \in \mathbb{N}^*$, thì khi đó $(k+1)(k-1) = 4k(k+1)$ chia hết cho $2^3 = 8$.
Giả sử bài toán đúng với $n = p$, tức $2^{p+2} \mid k^{2^p} - 1$ hay $k^{2^p} = q \cdot 2^{p+2} + 1$ với $q \in \mathbb{N}^*$.
Ta chứng minh bài toán đúng với $n = p+1$. Thật vậy

$$\begin{aligned}A &= k^{2^{p+1}} - 1 = k^{2\cdot 2^p} - 1 = \left(k^{2^p}\right)^2 - 1 \\ &= \left(k^{2^p} - 1\right)\left(k^{2^p} + 1\right) \\ &= q \cdot 2^{p+2} \cdot \left(2 + q \cdot 2^{p+2}\right) \\ &= q \cdot 2^{p+3} \cdot \left(1 + q \cdot 2^{p+1}\right)\end{aligned}$$

chia hết cho 2^{p+3}. Ta có đpcm. ■

Bài tập đề nghị

Bài 1. Một số bài toán ở các phương pháp nêu trên có thể giải bằng phương pháp quy nạp.

Bài 2. Chứng minh rằng $255 \mid 16^n - 15n - 1$ với $n \in \mathbb{N}$.

Bài 3. Chứng minh rằng $64 \mid 3^{2n+3} + 40n - 27$ với $n \in \mathbb{N}$.

Bài 4. Chứng minh rằng $16 \mid 3^{2n+2} + 8n - 9$ với $n \in \mathbb{N}$.

Bài 5. Chứng minh rằng $676 \mid 3^{3n+3} - 16n - 27$ với $n \in \mathbb{N},\ n \geq 1$.

Bài 6. Chứng minh rằng $700 \mid 29^{2n} - 140n - 1$ với $n \in \mathbb{N}$.

Bài 7. Chứng minh rằng $270 \mid 2002^n - 138n - 1$ với $n \in \mathbb{N}$.

Bài 8. Chứng minh rằng $22 \mid 3^{2^{4n+1}} + 2^{3^{4n+1}} + 5$ với $n \in \mathbb{N}$.

Bài 9. Chứng minh rằng số $2^{3^n} + 1$ chia hết cho 3^n nhưng không chia hết cho 3^{n+1} với $n \in \mathbb{N}$.

Bài 10. Chứng minh rằng số $2001^{2^n} - 1$ chia hết cho 2^{n+4} nhưng không chia hết cho 2^{n+5} với $n \in \mathbb{N}$.

Bài 11. Chứng minh rằng với mọi số tự nhiên $n \geq 2$, tồn tại một số tự nhiên m sao cho $3^n \mid (m^3 + 17)$, nhưng $3^{n+1} \nmid (m^3 + 17)$.

Bài 12. Có tồn tại hay không một số nguyên dương là bội của 2007 và có bốn chữ số tận cùng là 2008.

Bài 13. Chứng minh rằng tồn tại một số có 2011 chữ số gồm toàn chữ số 1 và 2 sao cho số đó chia hết cho 2^{2011}.

Bài 14. Tìm phần dư khi chia 3^{2^n} cho 2^{n+3}, trong đó n là số nguyên dương.

Bài 15. Cho $n \in \mathbb{N},\ n \geq 2$. Đặt $A = 7^{7^{\cdot^{\cdot^{\cdot}}}}$ (lũy thừa n lần). Chứng minh rằng $A_n + 17$ chia hết cho 20.

3.2.6 Sử dụng nguyên lí Dirichlet

Nội dung: Nhốt 5 con thỏ vào 3 chuồng thì tồn tại chuồng chứa ít nhất 2 con.

Định lý 3.3– *Nhốt $m = nk + 1$ con thỏ vào k chuồng $(k < n)$ thì tồn tại chuồng chứa ít nhất $n + 1$ con thỏ.* □

Chứng minh. Giả sử không có chuồng nào chứa ít nhất $n + 1$ con thỏ, khi đó mỗi chuồng chứa nhiều nhất n con thỏ, nên k chuồng chứa nhiều nhất kn con thỏ, mâu thuẫn với số thỏ là $nk + 1$. ■

Định lý 3.4 (Áp dụng vào số học)– *Trong $m = nk + 1$ số có ít nhất $n + 1$ số chia cho k có cùng số dư.* □

Tuy nguyên lý được phát biểu khá đơn giản nhưng lại có những ứng dụng hết sức bất ngờ, thú vị. Bài viết này chỉ xin nêu một số ứng dụng của nguyên lí trong việc giải các bài toán về chia hết.

Ví dụ 3.24. *Chứng minh rằng luôn tồn tại số có dạng*

$$20112011\cdots201100\cdots0$$

chia hết cho 2012. △

Lời giải. Lấy 2013 số có dạng

$$2011;\ 20112011,\ \cdots,\ \underbrace{20112011\cdots2011}_{2012\text{ số }2011}.$$

Lấy 2013 số này chia cho 2012. Theo nguyên lí Dirichlet thì tồn tại hai số có cùng số dư khi chia cho 2012.
Giả sử hai số đó là $\underbrace{20112011\cdots2011}_{m\text{ số }2011}$ và $\underbrace{20112011\cdots2011}_{n\text{ số }2011}$ $(m > n > 0)$.

$$\Longrightarrow 2012 \mid \underbrace{20112011\cdots2011}_{m\text{ số }2011} - \underbrace{20112011\cdots2011}_{n\text{ số }2011}$$

$$\Longrightarrow 2012 \mid \underbrace{20112011\cdots2011}_{m-n \text{ số } 2011}\underbrace{00\cdots00}_{n \text{ số } 2011}$$

Vậy tồn tại số thỏa mãn đề bài. ■

Ví dụ 3.25. *Chứng minh rằng trong* 101 *số nguyên bất kì có thể tìm được hai số có* 2 *chữ số tận cùng giống nhau.* △

Lời giải. Lấy 101 số nguyên đã cho chia cho 100 thì theo nguyên lí Dirichlet tồn tại hai số có cùng số dư khi chia cho 100. Suy ra trong 101 số nguyên đã cho tồn tại hai số có chữ số tận cùng giống nhau. ■

Ví dụ 3.26 (Tuyển sinh 10 chuyên ĐHSPHN, 1993). *Cho* 5 *số nguyên phân biệt tùy ý* a_1, a_2, a_3, a_4, a_5. *Chứng minh rằng tích*

$$P = (a_1 - a_2)(a_1 - a_3)(a_1 - a_4)(a_1 - a_5)(a_2 - a_3)\times \\ \times (a_2 - a_4)(a_2 - a_5)(a_3 - a_4)(a_3 - a_5)(a_4 - a_5)$$

chia hết cho 288. △

Lời giải. Phân tích $288 = 2^5 \cdot 3^2$.

1. Chứng minh $9 \mid P$: Theo nguyên lí Dirichlet thì trong 4 số a_1, a_2, a_3 có hai số có hiệu chia hết cho 3. Không mất tính tổng quát, giả sử: $3 \mid a_1 - a_2$. Xét 4 số a_2, a_3, a_4, a_5 cũng có hai số có hiệu chia hết cho 3. Như vậy P có ít nhất hai hiệu khác nhau chia hết cho 3, tức $9 \mid p$.

2. Chứng minh $32 \mid P$: Theo nguyên lí Dirichlet thì tổng 5 số đã cho tồn tại ít nhất 3 số có cùng tính chẵn lẻ. Chỉ có thể có hai khả năng sau xảy ra:

   - Nếu có ít nhất 4 số có cùng tính chẵn lẻ, thì từ bốn số có thể lập thành sáu hiệu khác nhau chia hết cho 2. Do đó $32 \mid P$.

- Nếu có 3 số có cùng tính chẵn lẻ. Không mất tính tổng quát, giả sử ba số đó là a_1, a_2, a_3. Khi đó a_4, a_5 cũng cùng tính chẵn lẻ nhưng lại khác tính chẵn lẻ của a_1, a_2, a_3. Khi đó các hiệu sau chia hết cho 2: $a_1 - a_2, a_1 - a_3, a_2 - a_3, a_4 - a_5$. Mặt khác, trong 5 số đã cho có ít nhất hai hiệu chia hết cho 4, cho nên trong 4 hiệu $a_1 - a_2, a_1 - a_3, a_2 - a_3, a_4 - a_5$ có ít nhất một hiệu chia hết cho 4. Vậy $32 \mid P$.

Ta có đpcm. ■

Ví dụ 3.27. *Cho* 2012 *số tự nhiên bất kì* $a_1, a_2, \cdots, a_{2012}$. *Chứng minh rằng tồn tại một số chia hết cho* 2012 *hoặc tổng một số số chia hết cho* 2012. △

Lời giải. Xét 2012 số

$$\begin{aligned} S_1 &= a_2 \\ S_2 &= a_1 + a_2 \\ &\cdots \\ S_{2012} &= a_1 + a_2 + \cdots + a_{2012} \end{aligned}$$

Trường hợp 1: Nếu tồn tại số S_i $(i = 1, 2, \cdots, 2012)$ chia hết cho 2012 thì bài toán chứng minh xong.

Trường hợp 2: Nếu $2012 \nmid S_i$ với mọi $i = 1, 2, \cdots, 2012$. Đem 2012 số này chia cho 2012 nhận được 2012 số dư. Các số dư nhận giá trị thuộc tập $\{1; 2; \cdots; 2011\}$. Vì có 2012 số dư mà chỉ có 2011 giá trị nên theo nguyên lí Dirichlet chắc chắn có hai số dư bằng nhau. Gỉa sử gọi hai số đó là S_m và S_n có cùng số dư khi chia cho 2012 $(m, n \in \mathbb{N},\ 1 \leq n < m \leq 2012)$ thì hiệu

$$S_m - S_n = a_{n+1} + a_{n+2} + \cdots + a_m$$

chia hết cho 2012. ■

Nhận xét. Ta có thể rút ra bài toán tổng quát và bài toán mở rộng sau:

Bài toán 3.5 (Bài toán tổng quát). *Cho n số $a_1, a_2, \cdots, a_n$. Chứng minh rằng trong n số trên tồn tại một số chia hết cho n hoặc tổng một số số chia hết cho n.* △

Bài toán 3.6 (Bài toán mở rộng). *(Tạp chí Toán Tuổi Thơ số 115) Cho n là một số chuyên dương và n số nguyên dương $a_1, a_2, \cdots, a_n$ có tổng bằng $2n-1$. Chứng minh rằng tồn tại một số số trong n số đã cho có tổng bằng n.* △

Bài tập đề nghị

Bài 1. Chứng minh rằng có vô số số chia hết cho $2013^{11^{356}}$ mà trong biểu diễn thập phân của các số đó không có các chữ số $0, 1, 2, 3$.

Bài 2. *(HSG 9 Hà Nội, 2006)* Chứng minh rằng tồn tại số tự nhiên $n \neq 0$ thỏa mãn $3^{13579} \mid (13579^n - 1)$.

Bài 3. Chứng minh rằng trong 52 số nguyên dương bất kì luôn luôn tìm được hai số có tổng hoặc hiệu chia hết cho 100.

Bài 4. Cho 10 số nguyên dương $a_1, a_2, \cdots, a_{10}$. Chứng minh rằng tồn tại các số $c_i \in \{0, -1, 1\}$, $(i = 1, \cdots 10)$ không đồng thời bằng 0 sao cho

$$A = c_1a_1 + c_2a_2 + \cdots + c_{10}a_{10}$$

chia hết cho 1032.

Bài 5. Chứng minh rằng tồn tại số tự nhiên k sao cho $2002^k - 1$ chia hết cho 2003^{10}.

Bài 6. Biết rằng ba số $a, a+k, a+2k$ đều là các số nguyên tố lớn hơn 3. Chứng minh rằng khi đó k chia hết cho 6.

3.2.7 Phản chứng

Cơ sở: Để chứng minh $p \nmid A(n)$, ta làm như sau:

- Giả sử ngược lại $p \mid A(n)$.
- Chứng minh điều ngược lại sai.

Ví dụ 3.28. *Chứng minh rằng với mọi số nguyên n thì n^2+n+1 không chia hết cho 9.* △

Lời giải. Giả sử $9 \mid (n^2+n+1)$. Khi đó $n^2+n+1 = (n+2)(n-1)+3$ chia hết cho 3. Suy ra $3 \mid n+2$ và $3 \mid n-1$. Như vậy $(n+2)(n-1)$ chia hết cho 9, tức n^2+n+1 chia 9 dư 3, mâu thuẫn. Ta có đpcm. ■

Nhận xét. Bài toán này vẫn có thể giải theo phương pháp xét số dư.

Ví dụ 3.29. *Giả sử $p = k.2^t + 1$ là số nguyên tố lẻ, t là số nguyên dương và k là số tự nhiên lẻ. Giả thiết x và y là các số tự nhiên mà $p \mid \left(x^{2^t} + y^{2^t}\right)$. Chứng minh rằng khi đó x và y đồng thời chia hết cho p.* △

Lời giải. Giả sử trái lại $p \nmid x$, suy ra $p \nmid y$.
Do p là số nguyên tố nên theo định lý Fermat nhỏ ta có

$$\begin{cases} x^{p-1} \equiv 1 \pmod p \\ y^{p-1} \equiv 1 \pmod p \end{cases}$$

Theo giả thiết thì $p-1 = k.2^t$, do đó

$$\begin{cases} x^{k.2^t} \equiv 1 \pmod p \\ y^{k.2^t} \equiv 1 \pmod p \end{cases}$$

Từ đó ta có

$$x^{k.2^t} + y^{k.2^t} \equiv 2 \pmod p. \qquad (i)$$

Theo giả thiết thì

$$x^{2^t} + y^{2^t} \equiv 0 \pmod p.$$

Do k lẻ nên

$$\begin{aligned} x^{k.2^t}+y^{k.2^t} &= \left(x^{2^t}\right)^k+\left(y^{2^t}\right)^k \vdots \left(x^{2^t}+y^{2^t}\right) \\ \Rightarrow \left(x^{k.2^t}+y^{k.2^t}\right) &\equiv 0 \pmod p \qquad (ii) \end{aligned}$$

Từ (i) và (ii) suy ra điều mâu thuẫn. Vậy giả thiết phản chứng sai. Do đó x, y đồng thời chia hết cho p. ■

Bài tập đề nghị

Bài 1. Chứng minh n^2+n+2 không chia hết cho 15 với mọi $n \in \mathbb{Z}$.

Bài 2. Chứng minh n^2+3n+5 không chia hết cho 121 với mọi $n \in \mathbb{N}$.

Bài 3. Chứng minh $9n^3+9n^2+3n-16$ không chia hết cho 343 với mọi $n \in \mathbb{N}$.

Bài 4. Chứng minh $4n^3-6n^2+3n+37$ không chia hết cho 125 với mọi $n \in \mathbb{N}$.

Bài 5. Chứng minh $n^3+3n-38$ không chia hết cho 49 với mọi $n \in \mathbb{N}$.

Chương

4 Phương trình nghiệm nguyên

Trần Nguyễn Thiết Quân (L Lawliet)
Phạm Quang Toàn (Phạm Quang Toàn)

Trong chương trình THCS và THPT thì phương trình nghiệm nguyên vẫn luôn là một đề tài hay và khó đối với học sinh. Các bài toán nghiệm nguyên thường xuyên xuất hiện tại các kì thi lớn, nhỏ, trong và ngoài nước. Trong bài viết này tôi chỉ muốn đề cập đến các vấn đề cơ bản của nghiệm nguyên (các dạng, các phương pháp giải) chứ không đi nghiên cứu sâu sắc về nó. Tôi cũng không đề cập tới phương trình Pell, phương trình Pythagore, phương trình Fermat vì nó có nhiều trong các sách, các chuyên đề khác.

4.1 Xét tính chia hết

4.1.1 Phát hiện tính chia hết của 1 ẩn

Ví dụ 4.1. *Giải phương trình nghiệm nguyên*

$$13x + 5y = 175 \tag{4.1}$$

Lời giải. Giả sử x, y là các số nguyên thỏa mãn phương trình (4.1). Ta thấy 175 và $5y$ đều chia hết cho 5 nên $13x \vdots 5 \Rightarrow x \vdots 5$ (do $\text{GCD}(13;5) = 1$). Đặt $x = 5t$ $(t \in \mathbb{Z})$. Thay vào phương trình (4.1), ta được

$$13.5t + 5y = 175 \Leftrightarrow 13t + y = 35 \Leftrightarrow y = 35 - 13t$$

Do đó, phương trình (4.1) có vô số nghiệm nguyên biểu diễn dưới dạng

$$(x; y) = (5t; 35 - 13t), (t \in \mathbb{Z})$$

Bài tập đề nghị

Bài 1. Giải phương trình nghiệm nguyên $12x - 19y = 285$

Bài 2. Giải phương trình nghiệm nguyên $7x + 13y = 65$

Bài 3. Giải phương trình nghiệm nguyên $5x + 7y = 112$

4.1.2 Đưa về phương trình ước số

Ví dụ 4.2. *Tìm nghiệm nguyên của phương trình*

$$3xy + 6x + y - 52 = 0 \tag{4.2}$$

Lời giải. *Nhận xét.* Đối với phương trình này, ta không thể áp dụng phương pháp trên là phát hiện tính chia hết, vậy ta phải giải như thế nào?
Ta giải như sau:

$$\begin{aligned} (4.2) \Leftrightarrow 3xy + y + 6x + 2 - 54 &= 0 \\ \Leftrightarrow y(3x+1) + 2(3x+1) - 54 &= 0 \\ \Leftrightarrow (3x+1)(y+2) &= 54 \end{aligned}$$

Như vậy, đến đây ta có x và y nguyên nên $3x + 1$ và $y + 2$ phải là ước của 54. Nhưng nếu như vậy thì ta phải xét đến hơn 10 trường hợp sao? Vì:

$$\begin{aligned} &4 = 1.54 = 2.27 = 3.18 = 6.9 \\ &= (-1).(-54) = (-2).(-27) = (-3).(-18) = (-6).(-9) \end{aligned}$$

Có cách nào khác không? Câu trả lời là có! Nếu ta để ý một chút đến thừa số $3x+1$, biểu thức này chia cho 3 luôn dư 1 với mọi x nguyên. Với lập luận trên, ta được:

$$\left[\begin{array}{l} \begin{cases} 3x+1=1 \\ y+2=54 \end{cases} \Leftrightarrow \begin{cases} x=0 \\ y=52 \end{cases} \\ \begin{cases} 3x+1=-2 \\ y+2=-54 \end{cases} \Leftrightarrow \begin{cases} x=-1 \\ y=-56 \end{cases} \end{array}\right.$$

Ví dụ 4.3. *Giải phương trình nghiệm nguyên sau:*

$$2x+5y+3xy=8 \tag{4.3}$$

Lời giải. Ta có

$$\begin{aligned} (4.3) &\Leftrightarrow x(2+3y)+5y=8 \\ &\Leftrightarrow 3x(2+3y)+15y=24 \\ &\Leftrightarrow 3x(2+3y)+5(2+3y)=34 \\ &\Leftrightarrow (3x+5)(3y+3)=34 \end{aligned}$$

Đến đây phân tích $34=1\cdot 34=2\cdot 17$ rồi xét các trường hợp. Chú ý rằng $3x+5, 3y+2$ là hai số nguyên chia 3 dư 2, vận dụng điều này ta có thể giảm bớt số trường hợp cần xét. ■

Ví dụ 4.4. *Giải phương trình nghiệm nguyên*

$$x^2-y^2=2011 \tag{4.4}$$

Lời giải. $(4.4) \Leftrightarrow (x-y)(x+y)=2011$. Vì 2011 là số nguyên tố nên ước nguyên của 2011 chỉ có thể là $\pm 1, \pm 2011$. Từ đó suy ra nghiệm $(x;y)$ là $(1006;1005); (1006;-1005); (-1006;-1005); (-1006;1005)$. ■

Ví dụ 4.5. *Tìm các số nguyên x, y thoả mãn điều kiện*

$$x^2+y^2=(x-y)(xy+2)+9 \tag{4.5}$$

Lời giải. Đặt $a = x - y, b = xy$. Khi đó (4.5) trở thành

$$a^2 + 2b = a(b+2) + 9 \Leftrightarrow (a-2)(a-b) = 9 \tag{4.6}$$

Vì $x, y \in \mathbb{Z}$ nên $a, , a-2, a-b$ đều là các số nguyên. Từ (4.6) ta có các trường hợp sau:

- $\begin{cases} a-2=9 \\ a-b=1 \end{cases} \Leftrightarrow \begin{cases} a=11 \\ b=10 \end{cases} \Leftrightarrow \begin{cases} x-y=11 \\ xy=10 \end{cases}$ (4.7)
- $\begin{cases} a-2=3 \\ a-b=3 \end{cases} \Leftrightarrow \begin{cases} a=5 \\ b=2 \end{cases} \Leftrightarrow \begin{cases} x-y=5 \\ xy=2 \end{cases}$ (4.8)
- $\begin{cases} a-2=1 \\ a-b=9 \end{cases} \Leftrightarrow \begin{cases} a=3 \\ b=-6 \end{cases} \Leftrightarrow \begin{cases} x-y=3 \\ xy=-6 \end{cases}$ (4.9)
- $\begin{cases} a-2=-1 \\ a-b=-9 \end{cases} \Leftrightarrow \begin{cases} a=1 \\ b=10 \end{cases} \Leftrightarrow \begin{cases} x-y=1 \\ xy=10 \end{cases}$ (4.10)
- $\begin{cases} a-2=-3 \\ a-b=-3 \end{cases} \Leftrightarrow \begin{cases} a=-1 \\ b=2 \end{cases} \Leftrightarrow \begin{cases} x-y=-1 \\ xy=2 \end{cases}$ (4.11)
- $\begin{cases} a-2=-3 \\ a-b=-3 \end{cases} \Leftrightarrow \begin{cases} a=-1 \\ b=2 \end{cases} \Leftrightarrow \begin{cases} x-y=-1 \\ xy=2 \end{cases}$ (4.12)

Dễ thấy các hệ (4.7),(4.8),(4.10) không có nghiệm nguyên, hệ (4.9) vô nghiệm, hệ (4.11) có hai nghiệm nguyên $(1;2)$ và $(-2;-1)$, hệ (4.12) có hai nghiệm nguyên $(-1;6)$ và $(-6;1)$.
Tóm lại phương trình (4.5) có các cặp nghiệm nguyên $(x;y)$ là $(1;2)$; $(-2;-1)$; $(-1;6)$; $(-6;1)$. ■

Ví dụ 4.6. *Tìm nghiệm nguyên của phương trình:*

$$\left(x^2+1\right)\left(y^2+1\right) + 2\left(x-y\right)\left(1-xy\right) = 4\left(1+xy\right) \tag{4.13}$$

Lời giải. Phương trình (4.13) tương đương với:

$$\begin{aligned} & x^2y^2+x^2+y^2+1+2x-2x^2y-2y+2xy^2=4+4xy \\ \Leftrightarrow\ & (x^2+2x+1)y^2-2(x^2+2x+1)y+(x^2+2x+1)=4 \\ \Leftrightarrow\ & (x+1)^2(y-1)^2=4 \\ \Leftrightarrow\ & \left[\begin{array}{l}(x+1)(y-1)=2\\(x+1)(y-1)=-2\end{array}\right. \end{aligned}$$

Với $(x+1)(y-1)=2$ mà $x,y\in\mathbb{Z}$ nên ta có các trường hợp sau:

- $\left\{\begin{array}{l}x+1=1\\y-1=2\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=0\\y=3\end{array}\right.$
- $\left\{\begin{array}{l}x+1=2\\y-1=1\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=1\\y=2\end{array}\right.$
- $\left\{\begin{array}{l}x+1=-2\\y-1=-1\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=-3\\y=0\end{array}\right.$
- $\left\{\begin{array}{l}x+1=-1\\y-1=-2\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=-2\\y=-1\end{array}\right.$

Với $(x+1)(y-1)=-2$, tương tự ta cũng suy ra được:

- $\left\{\begin{array}{l}x+1=-1\\y-1=2\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=-2\\y=3\end{array}\right.$
- $\left\{\begin{array}{l}x+1=1\\y-1=-2\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=0\\y=-1\end{array}\right.$
- $\left\{\begin{array}{l}x+1=2\\y-1=-1\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=1\\y=0\end{array}\right.$
- $\left\{\begin{array}{l}x+1=-2\\y-1=1\end{array}\right. \Leftrightarrow \left\{\begin{array}{l}x=-3\\y=2\end{array}\right.$

Vậy phương trình đã cho có các cặp nghiệm nguyên:

$$(x;y)=\{(0;3);(1;2);(-3;0);(-2;-1);(-2;3);(0;-1);(1;0);(-3;2)\}$$

Ví dụ 4.7. *Tìm nghiệm nguyên của phương trình*

$$x^6+3x^3+1=y^4 \tag{4.14}$$

Lời giải. Nhân hai vế của phương trình (4.14) cho 4, ta được:

$$\begin{aligned} & 4x^6+12x^3+4=4y^4 \\ \Leftrightarrow\ & (4x^6+12x^3+9)-4y^4=5 \\ \Leftrightarrow\ & (2x^3+3)^2-4y^4=5 \\ \Leftrightarrow\ & (2x^3-2y^2+3)(2x^3+2y^2+3)=5. \end{aligned}$$

Với lưu ý rằng $5=1.5=5.1=(-1).(-5)=(-5).(-1)$ và $x,y\in\mathbb{Z}$ nên ta suy ra được các trường hợp sau:

- $\left\{\begin{array}{l} 2x^3-2y^2+3=1 \\ 2x^3+2y^2+3=5 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3-y^2=-1 \\ x^3+y^2=1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3=0 \\ y^2=1 \end{array}\right.$

  $\Leftrightarrow \left\{\begin{array}{l} \left[\begin{array}{l} x=0 \\ y=1 \end{array}\right. \\ \left[\begin{array}{l} x=0 \\ y=-1 \end{array}\right. \end{array}\right.$

- $\left\{\begin{array}{l} 2x^3-2y^2+3=-1 \\ 2x^3+2y^2+3=-5 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3-y^2=-2 \\ x^3+y^2=-4 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3=-3 \\ y^2=-1 \end{array}\right.$ (loại)

- $\left\{\begin{array}{l} 2x^3-2y^2+3=5 \\ 2x^3+2y^2+3=1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3-y^2=1 \\ x^3+y^2=-1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3=0 \\ y^2=-1 \end{array}\right.$ (loại)

- $\left\{\begin{array}{l} 2x^3-2y^2+3=-5 \\ 2x^3+2y^2+3=-1 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3-y^2=-4 \\ x^3+y^2=-2 \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} x^3=-3 \\ y^2=1 \end{array}\right.$ (loại)

Vậy phương trình đã cho có các cặp nghiệm nguyên:

$$\boxed{(x;y)=\{(0;1);(0;-1)\}}$$

Nhận xét. Bài toán này cũng có thể giải bằng phương pháp kẹp.

Ví dụ 4.8. *Giải phương trình nghiệm nguyên dương:*

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{p} \tag{4.15}$$

trong đó p là số nguyên tố. △

Lời giải.

$$(4.15) \Leftrightarrow xy = px + py \Rightarrow (x - y)(y - p) = p^2.$$

Vì p là số nguyên tố nên ước số nguyên của p^2 chỉ có thể là $\pm 1, \pm p, \pm p^2$. Thử lần lượt với các ước trên ta dễ tìm được kết quả. Phần trình bày xin dành cho bạn đọc. ■

Nhận xét. Phương pháp này cần hai bước chính: Phân tích thành ước số và xét trường hợp để tìm kết quả. Hai bước này có thể nói là không quá khó đối với bạn đọc, nhưng xin nói một số lưu ý thêm về bước xét trường hợp. Trong một số bài toán, hằng số nguyên ở vế phải sau khi phân tích là một số có nhiều ước, như vậy đòi hỏi xét trường hợp và tính toán rất nhiều. Một câu hỏi đặt ra là: Làm thế nào để giảm số trường hợp bị xét đây? Và để trả lời được câu hỏi đó, ta sẽ tham khảo ví dụ dưới đây.

Ví dụ 4.9. *Tìm nghiệm nguyên của phương trình:*

$$x^2 + 12x = y^2. \tag{4.16}$$

Lời giải. (thông thường) Phương trình (4.16) đã cho tương đương với:

$$(x + 6)^2 - y^2 = 36 \Leftrightarrow (x + 6 + y)(x + 6 - y) = 36$$

Suy ra $x + y + 6, x + 6 - y$ là ước của 36. Mà số 36 có tất cả 18 ước nên ta phải xét 18 trường hợp tương ứng với

$$x + 6 + y \in \{\pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 9; \pm 12; \pm 18; \pm 36\}$$

. Kết quả là ta tìm được các cặp nghiệm nguyên $(x; y)$ là

$$(0; 0); (-12; 0); (-16; 8); (-16; -8); (4; 8); (4; -8)$$

.

Nhận xét. Đúng như vấn đề mà ta đã nêu ra ở trên, số ước quá nhiều để xét. Cho nên ta sẽ có các nhận xét sau đề thực hiện thao tác "siêu phàm" chuyển từ con số 18 xuống chỉ còn 2!

Vì y có số mũ chẵn trong phương trình nên có thể giả sử $y \geq 0$. Khi đó $x+6-y \leq x+6+y$, do vậy ta loại được tám trường hợp và còn lại các trường hợp sau:

$$\begin{cases} x+6+y=9 \\ x+6-y=4 \end{cases}, \begin{cases} x+6+y=-9 \\ x+6-y=-4 \end{cases}, \begin{cases} x+y+6=-1 \\ x+y-6=-36 \end{cases},$$
$$\begin{cases} x+y+6=36 \\ x-y+6=1 \end{cases}, \begin{cases} x+y+6=-2 \\ x-y+6=-18 \end{cases}, \begin{cases} x+y+6=18 \\ x-y+6=2 \end{cases},$$
$$\begin{cases} x+y+6=-3 \\ x-y+6=-12 \end{cases}, \begin{cases} x+y+6=12 \\ x-y+6=3 \end{cases}, \begin{cases} x+y+6=-6 \\ x-y+6=-6 \end{cases},$$
$$\begin{cases} x+y+6=6 \\ x+y-6=6 \end{cases}.$$

Bây giờ ta đã có 10 trường hợp, ta sẽ tiếp tục lược bỏ. Nhận thấy $(x+y+6)-(x+6-y)=2y$ nên $x+6-y$ và $x+6+y$ có cùng tính chẵn lẻ, do đó ta loại thêm 6 trường hợp, chỉ còn

$$\begin{cases} x+y+6=18 \\ x+y-6=2 \end{cases}, \begin{cases} x+y+6=-2 \\ x+y-6=-18 \end{cases},$$
$$\begin{cases} x+y+6=-6 \\ x-y+6=-6 \end{cases}, \begin{cases} x+y+6=6 \\ x+y-6=6 \end{cases}.$$

Tiếp tục xét hai phương trình $\begin{cases} x+y+6=-6 \\ x-y+6=-6 \end{cases}$ và $\begin{cases} x+y+6=6 \\ x+y-6=6 \end{cases}$, hai phương trình này đều tìm được $y=0$. Vậy sao không để đơn giản hơn, ta xét $y=0$ ngay từ đầu. Phương trình có dạng $x(x+12)=y^2$, xét hai khả năng:

- Nếu $y=0$ thì $x=0$ hoặc $x=-12$.
- Nếu $y \neq 0$ thì $x+6+y > x+6-y$, áp dụng hai nhận xét trên ta chỉ có hai trường hợp: $\begin{cases} x+y+6=-2 \\ x-y+6=-18 \end{cases}$ và $\begin{cases} x+y+6=18 \\ x-y+6=2 \end{cases}$.

■

Phương trình đã cho có 6 nghiệm nguyên

$$(x;y) = (-16;8), (0;0), (-12;0), (-16;8), (4;8), (4;-8)$$

Nhận xét. Như vậy bài toán ngắn gọn, chính xác nhờ linh hoạt trong việc xét tính chẵn lẻ, giới hạn hai số để giảm số trường hợp cần xét. Ngoài các cách đánh giá trên ta còn có thể áp dụng xét số dư từng vế để đánh giá (đây cũng là một phương pháp giải phương trình nghiệm nguyên).

Bài tập đề nghị

Bài 1. Thử biến đổi các bài toán giải phương trình nghiệm nguyên ở phương pháp Biểu thị một ẩn theo ẩn còn lại bằng phương pháp đưa về ước số.

Bài 2. Tìm độ dài cạnh một tam giác vuông sao cho tích hai cạnh huyền gấp ba lần chu vi tam giác đó.

Bài 3. Giải phương trình nghiệm nguyên $x - y + 2xy = 6$

Bài 4. Giải phương trình nghiệm nguyên $2x + 5y + 2xy = 8$

Bài 5. (Thi HSG lớp 9 tỉnh Quảng Ngãi năm 2011-2012) Giải phương trình nghiệm nguyên $6x + 5y + 18 = 2xy$

Bài 6. Tìm nghiệm nguyên $(xy - 7)^2 = x^2 + y^2$

Bài 7. Tìm $x, y \in \mathbb{Z}$ thỏa mãn $2x^2 - 2xy = 5x - y - 19$.

Bài 8. Tìm nghiệm nguyên của phương trình $x^2+6xy+8y^2+3x+6y = 2$.

Bài 9. Tìm nghiệm nguyên dương của phương trình $x^3 - y^3 = xy + 61$

Bài 10. Tìm nghiệm nguyên của phương trình $4x^2y^2 = 22 + x(1 + x) + y(1 + y)$

Bài 11. Giải phương trình nghiệm nguyên $x(x + 1)(x + 7)(x + 8) = y^2$.

Bài 12. Tìm nghiệm nguyên dương của phương trình $6x^3 - xy(11x + 3y) + 2y^3 = 6$ (Tạp chí TTT2 số 106).

Bài 13. Tìm nghiệm nguyên dương của phương trình $x(x+2y)^3 - y(y+2x)^3 = 27$ (tạp chí THTT số 398).

Bài 14. Tìm nghiệm nguyên của phương trình $\sqrt{9x^2 + 16x + 96} = 3x - 16y - 24$.

Bài 15. Tìm nghiệm nguyên dương của phương trình

$$2 + \sqrt{x + \frac{1}{2} + \sqrt{x + \frac{1}{4}}} = y$$

.

Bài 16. Tìm số nguyên x để $x^2 - 4x - 52$ là số chính phương.

Bài 17. Giải phương trình nghiệm nguyên $x^2 + 2y^2 + 3xy - 2x - y = 6$.

Bài 18. Giải phương trình nghiệm nguyên $x^2 + 3xy - y^2 + 2x - 3y = 5$.

Bài 19. Giải phương trình nghiệm nguyên $2x^2 + 3y^2 + xy - 3x - 3 = y$.

Bài 20. (Tuyển sinh vào lớp 10 THPT chuyên trường KHTN Hà Nội năm học 2012-2013) Tìm tất cả các cặp số nguyên x, y thỏa mãn đẳng thức $(x + y + 1)(xy + x + y) = 5 + 2(x + y)$.

Bài 21. Giải phương trình nghiệm nguyên $x^4 - 2y^4 - x^2y^2 - 4x^2 - 7y^2 - 5 = 0$.

(Thi HSG lớp 9 tỉnh Hưng Yên năm 2011-2012)

Bài 22. *(Romanian 1999)* Chứng minh rằng phương trình sau không có nghiệm nguyên

$$x^5 - x^4y - 13x^3y^2 + 13x^2y^3 + 36xy^4 - 36y^5 = 1937$$

4.1.3 Biểu thị một ẩn theo ẩn còn lại rồi sử dụng tính chia hết

Ví dụ 4.10. *Tìm nghiệm nguyên của phương trình*

$$2x - xy + 3 = 0 \tag{4.17}$$

Lời giải. *Nhận xét.* Ở phương trình này ta không thể áp dụng các cách đã biết, vậy ta phải làm sao? Chú ý hơn một xíu nữa ta thấy có thể biểu diễn y theo x được rồi vận dụng kiến thức tìm giá trị nguyên ở lớp 8 tìm nghiệm nguyên của phương trình, thử làm theo ý tưởng đó xem sao.

$$(4.17) \Leftrightarrow xy = 2x + 3$$

Nếu $x = 0$ thì phương trình (4.17) đã cho vô nghiệm nguyên y.
Nếu $x \neq 0$ thì

$$(4.17) \Leftrightarrow y = \frac{2x+3}{x} = 2 + \frac{3}{x}$$

Như vậy muốn y nguyên thì ta cần $\dfrac{3}{x}$ nguyên hay nói cách khác x là ước của 3. Với mỗi giá trị nguyên x ta tìm được một giá trị y nguyên. Từ đó, ta có bộ nghiệm của (4.17) là

$$(x; y) = (-3; 1); (-1; -1); (1; 5); (3; 3)$$

Ví dụ 4.11 (Thi HSG lớp 9 Quảng Ngãi năm 2011-2012). *Tìm các số nguyên dương x, y sao cho*

$$6x + 5y + 18 = 2xy \tag{4.18}$$

Nhận xét. Hướng phân tích và định hướng lời giải. Đã xác định được phương pháp của dạng này thì bây giờ ta sẽ biểu diễn ẩn x theo y. Không khó để viết thành $x = \dfrac{-5y - 18}{6 - 2y}$. Ta dường như nhân thấy biểu thức này rất khó phân tích như biểu thức ở ví dụ đầu. Tuy nhiên, nếu để ý kĩ sẽ thấy bên mẫu là $2y$ và tử là $5y$, do đó ta mạnh dạn nhân 2 vào tử để xuất hiện $2y$ giống như ở mẫu.

Lời giải. Ta có

$$\begin{aligned}(4.18) &\Leftrightarrow x = \frac{-5y-18}{6-2y}\\ &\Leftrightarrow 2x = \frac{-10y-36}{6-2y}\\ &\Leftrightarrow 2x = \frac{-66+5(6-2y)}{6-2y} = \frac{-66}{6-2y}+5\\ &\Leftrightarrow 2x = \frac{-33}{3-y}+5\end{aligned}$$

Như vậy muốn x là số nguyên dương thì $3-y$ là phải là ước của -33. Hay $3-y \in \{\pm 1; \pm 3; \pm 11, \pm 33\}$. Lại để ý rằng vì $y \geq 1$ nên $3-y \leq 2$. Do đó chỉ có thể $3-y \in \{\pm 1; -3; -11; -33\}$. Ta có bảng sau:

$3-y$	1	-1	-3	-11	-33
y	2	4	6	14	36
x	-14	19	8	4	3

Thử lại thấy các cặp $(x;y)$ nguyên dương thỏa mãn (4.18) là $(x;y) = (19;4), (8;6), (4;14), (3;36)$. ■

Nhận xét. Bài này ta cũng có thể sử dụng phương pháp đưa về phương trình ước số. Cũng xin chú ý với bạn rằng ở lời giải trên thì ta đã nhân 2 ở x để biến đổi, do đó phải có một bước thử lại coi giá trị x, y tìm được có thỏa mãn (4.18) hay không rồi mới có thể kết luận.

Bài tập đề nghị

Bài 1. Giải phương trình nghiệm nguyên $x^2 - xy = 6x - 5y - 8$.

Bài 2. Giải phương trình nghiệm nguyên $x^2 + x + 1 = 2xy + y$.

Bài 3. Giải phương trình nghiệm nguyên $x^3 - x^2y + 3x - 2y - 5 = 0$.

Bài 4. *(Vào 10 chuyên THPT ĐHKHTN Hà Nội năm 2001-2002)* Tìm giá trị x, y nguyên thỏa mãn đẳng thức $(y-2)x^2 + 1 = y^2$.

Bài 5. *(Vào 10 chuyên THPT DHKHTN Hà Nội năm 2000-2001)* Tìm cặp số nguyên (x, y) thỏa mãn đẳng thức $y(x-1) = x^2 + 2$.

Bài 6. Tìm số nhỏ nhất trong các số nguyên dương là bội của 2007 và có 4 chữ số cuối cùng là 2008.

Bài 7. Tìm nghiệm nguyên của phương trình $5x - 3y = 2xy - 11$.

4.1.4 Xét số dư từng vế

Cơ sở phương pháp. Đọc ngay tiêu đề phương pháp thì chắc bạn sẽ hiểu ngay phương pháp này nói đến việc xét số dư ở từng vế cho cùng một số. Vậy, tại sao lại phải xét và xét như vậy có lợi ích gì trong "công cuộc" giải toán? Hãy cùng tìm hiểu qua ví dụ đầu sau:

Ví dụ 4.12. *Tìm nghiệm nguyên của phương trình*

$$x^2 + y^2 = 2011 \tag{4.19}$$

Lời giải. Ta có $x^2; y^2$ chia 4 có thể dư 0 hoặc 1 nên tổng chúng chia 4 chỉ có thể dư $0; 1$ hoặc 2. Mặt khác 2011 chia 4 dưa 3 nên phương trình (4.19) vô nghiệm nguyên. ■

Nhận xét. Qua ví dụ đầu này thì ta đã thấy rõ số dư khi chia cho 4 của hai số khác nhau thì phương trình vô nghiệm. Do đó ta lại càng hiểu thêm mục đích của phương pháp này. Bật mí thêm tí nữa thì phương pháp này chủ yếu dùng cho các phương trình không có nghiệm nguyên. Cho nên, nếu bạn bắt gặp một phương trình bất kì mà bạn không thể tìm ra được nghiệm cho phương trình đó, thì hãy nghĩ đến phương pháp này đầu tiên. Còn bây giờ ta tiếp tục đến với ví dụ sau:

Ví dụ 4.13 (Balkan MO 1998). *Tìm nghiệm nguyên của phương trình*

$$x^2 = y^5 - 4 \tag{4.20}$$

Lời giải. Ta có: $x^2 \equiv 0; 1; 3; 4; 5; 9 \pmod{11}$. Trong khi đó $y^5 - 4 \equiv 6; 7; 8 \pmod{11}$: vô lý. Vậy phương trình (4.20) vô nghiệm nguyên. ■

Nhận xét. Một câu hỏi nữa lại lóe lên trong đầu ta: Làm thế nào lại có thể tìm được con số 11 để mà xét đồng dư được nhỉ? Đáp án của câu hỏi này cũng chính là cái cốt lõi để bạn vận dụng phương pháp này, và đó cũng là những kinh nghiệm sau:

1. Đối với phương trình nghiệm nguyên có sự tham gia của các bình phương thì ta thường xét đồng dư với $3, 4, 5, 8$. Cụ thể là:
$$\begin{aligned} a^2 &\equiv 0, 1 \pmod 3 \\ a^2 &\equiv 0, 1 \pmod 4 \\ a^2 &\equiv 0, 1, 4 \pmod 5 \\ a^2 &\equiv 0, 1, 4 \pmod 8 \end{aligned}$$

2. Đối với các phương trình nghiệm nguyên có sự tham gia của các số lập phương thì ta thường xét đồng dư với 9, vì $x^3 \equiv 0; 1; 8 \pmod 9$ và đồng dư với 7, vì $x^3 \equiv 0, 1, 6 \pmod 7$.

3. Đối với phương trình nghiệm nguyên có sự tham gia của các lũy thừa bậc 4 thì ta thường xét đồng dư với 8, như: $z^4 \equiv 0, 1 \pmod 8$.

4. Một vấn đề cuối cùng là định lí Fermat: Đối với phương trình nghiệm nguyên có sự tham gia của các lũy thừa có số mũ là một số nguyên tố hay là một số mà khi cộng 1 vào số đó ta được một số nguyên tố thì ta thường sử dụng định lí nhỏ Fermat để xét đồng dư.

Trên đây là một số kinh nghiệm bản thân, còn nếu các bạn muốn vận dụng được phương pháp xét số dư này, yêu cầu hãy ghi nhớ kinh nghiệm trên và tìm cách chứng minh nó. Ngoài ra, nếu bạn muốn mở rộng tầm hiểu biết hơn nữa, bạn có thể tìm các đồng dư với lũy thừa khác nhau (chẳng hạn qua ví dụ 2 ta đã rút ra được modun 11 cho lũy thừa bậc hai, bậc năm). Còn bây giờ, hãy thử xem kinh nghiệm trên có hiệu quả không nhé!

Ví dụ 4.14 (Bài toán trong tuần - diendantoanhoc.net). *Chứng minh rằng phương trình sau không có nghiệm nguyên*
$$x^{10} + y^{10} = z^{10} + 199$$

Nhận xét. Thường thường các bài toán khi đặt câu hỏi phương trình có nghiệm hay không thì thường có câu trả lời là **không**. Do đó để chứng minh phương trình trên không có nghiệm, thì ta sẽ tìm một con số sao cho khi chia VT và VP cho con số này thì được hai số dư khác nhau.

Như vậy, công việc bây giờ của ta là tìm con số đó. Để ý đến số mũ 10 thì sẽ khiến ta liên tưởng con số 11 là số nguyên tố. Như vậy lời giải của ta sẽ áp dụng định lý Fermat nhỏ cho số 11 để chứng minh hai vế phương trình chia cho 11 không cùng số dư.

Lời giải. Áp dụng định lý Fermat nhỏ thì $\begin{cases} x^{10} \equiv 0,1 \pmod{11} \\ y^{10} \equiv 0,1 \pmod{11} \\ z^{10} \equiv 0,1 \pmod{11} \end{cases}$.
Do đó $x^{10} + y^{10} - z^{10} \equiv 0, 1, 2, 10 \pmod{11}$ mà $199 \equiv 8 \pmod{11}$ nên phương trình vô nghiệm nguyên. ■

Ví dụ 4.15 (Đề thi chọn HSG toán quốc gia năm 2003 - Bảng B). *Hệ phương trình sau có tồn tại nghiệm nguyên hay không:*

$$x^2 + y^2 = (x+1)^2 + u^2 = (x+2)^2 + v^2 = (x+3)^2 + t^2 \tag{4.21}$$

Nhận xét. Ta dự đoán phương trình trên cũng sẽ vô nghiệm. Do đó cần tìm một số và khi chia cả 5 vế được các số dư khác nhau. Để ý bài toán này có bình phương nên ta nghĩ tới việc sử dụng các tính chất như: $a^2 \equiv 0, 1 \pmod{3}$, $a^2 \equiv 0, 1 \pmod{4}$, $a^2 \equiv 0, 1, 4 \pmod{5}$, $a^2 \equiv 0, 1, 4 \pmod{8}$. Ở bài toán này, ta sẽ chọn 8. Bây giờ chỉ cần xét tính dư khi chia cho 8.

Lời giải. Giả sử phương trình (4.21) có nghiệm nguyên $(x_0, y_0, u_0, v_0, t_0)$, tức là:

$$x_0^2 + y_0^2 = (x_0+1)^2 + u_0^2 = (x_0+2)^2 + v_0^2 = (x_0+3)^2 + t_0^2 \tag{4.22}$$

Với $a \in \mathbb{Z}$ thì $a^2 \equiv 0, 1, 4 \pmod{8}$. Ta xét các khả năng sau:

1. Nếu $x_0 \equiv 0 \pmod 4$ thì $x_0^2 + y_0^2 \equiv 0, 1, 4 \pmod 8$. Và

$$\begin{aligned} x_0 + 1 \equiv 1 \pmod 8 &\Rightarrow (x_0+1)^2 \equiv 1 \pmod 8 \\ &\Rightarrow (x_0+1)^2 + u_0^2 \equiv 1, 2, 5 \pmod 8 \\ x_0 + 2 \equiv 2 \pmod 4 &\Rightarrow (x_0+2)^2 \equiv 4 \pmod 8 \\ &\Rightarrow (x_0+2)^2 + v_0^2 \equiv 0, 4, 5 \pmod 8 \\ x_0 + 3 \equiv 3 \pmod 4 &\Rightarrow (x_0+3)^2 \equiv 1 \pmod 8 \\ &\Rightarrow (x_0+3)^2 + t_0^2 \equiv 1, 2, 5 \pmod 8 \end{aligned}$$

   Nhận thấy $\{0, 1, 4\} \cap \{1, 2, 5\} \cap \{0, 4, 5\} \cap \{1, 2, 5\} = 0$ nên do đó phương trình không có nghiệm nguyên với $x \equiv 0 \pmod 4$.

2. Tương tự với $x_0 \equiv 1 \pmod 4, x_0 \equiv 2 \pmod 4$ và $x_0 \equiv 3 \pmod 4$ ta cũng thực hiện tương tự và cũng cho kết quả phương trình không có nghiệm nguyên.

Vậy phương trình (4.21) đã cho không có nghiệm nguyên. ■

Nhận xét. Ví dụ 4 ta có thể tổng quát lên:

Ví dụ 4.16. *Tìm số nguyên dương n lớn nhất sao cho hệ phương trình*

$$(x+1)^2 + y_1^2 = (x+2)^2 + y_2^2 = \ldots = (x+n)^2 + y_n^2$$

có nghiệm nguyên. △

Đây cũng chính là đề thi chọn đội tuyển HSG quốc gia toán năm 2003 - Bảng A. Lời giải xin giành cho bạn đọc. Cũng xin nói thêm một thừa nhận rằng, ở phương pháp xét số dư từng vế này, chúng ta cứ tưởng chừng như đơn giản, nhưng thực chất không phải thế. Dẫn chứng là các ví dụ ở trên, đều là các bài toán hay và khó lấy từ khác cuộc thi trong nước và ngoài nước.

Bài tập đề nghị

Bài 1. Cho đa thức $f(x)$ có các hệ số nguyên. Biết rằng $f(1).f(2)$ là số lẻ. Chứng minh rằng phương trình $f(0) = 0$ không có nghiệm nghiệm nguyên.

Bài 2. Tồn tại hay không nghiệm nguyên của phương trình $x^{12}+y^{12}+z^{12}=2\left(37^{2012}+2014^{1995}\right)$.

Bài 3. Giải phương trình nghiệm nguyên $31^{2x}+12^{2x}+1997^{2x}=y^2$.

Bài 4. Giải phương trình nghiệm nguyên dương $7^z=2^x\cdot 3^y-1$

Bài 5. Giải phương trình nghiệm nguyên dương $2^x\cdot 3^y=1+5^z$

Bài 6. Giải phương trình nghiệm tự nhiên $19^x+5^y+1890=1975^{4^{30}}+1993$.

Bài 7. Giải phương trình nghiệm nguyên $x^3+y^3+z^3=1012$

Bài 8. (Tuyển sinh vào lớp 10 chuyên Trần Phú, Hải Phòng năm học 2012-2013) $x^4+y^4+z^4=2012$

Bài 9. $|x-y|+|y-z|+|z-x|=\dfrac{10^n-1}{9}$ với mọi $n\in\mathbb{N}$

Bài 10. Tìm nghiệm nguyên của phương trình $(2^x+1)(2^x+2)(2^x+3)(2^x+4)-5^y=11879$

Bài 11. Tìm nghiệm nguyên của phương trình $x^2+(x+1)^2+(x+2)^2=y^2$.

Bài 12. *(Tuyển sinh vào THPT chuyên ĐHKHTN Hà Nội năm 2011-2012)* Chứng minh rằng không tồn tại bộ ba số nguyên $(x;y;z)$ thỏa mãn $x^4+y^4=7z^4+5$.

Bài 13. Giải phương trình nghiệm nguyên $x_1^4+x_2^4+\cdots=x_{13}^4+20122015$.

Bài 14. Cho p là số nguyên tố lẻ. Chứng minh rằng phương trình $x^p+y^p=p\left[(p-1)!\right]^p$ không có nghiệm nguyên

Bài 15. Tìm nghiệm nguyên của phương trình $x^{2012}-y^{2010}=7$.

Bài 16. Chứng minh rằng không tồn tại số nguyên x,y thỏa mãn $x^5+y^5+1=(x+2)^5+(y-3)^5$.

4.2 Sử dụng bất đẳng thức

4.2.1 Sắp thứ tự các ẩn

Ví dụ 4.17. *Giải phương trình nghiệm nguyên dương sau*

$$\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1 \tag{4.23}$$

Lời giải. Không mất tính tổng quát, ta có thể giả sử

$$1\le x\le y\le z\Rightarrow \frac{1}{x}+\frac{1}{y}+\frac{1}{z}=1\le \frac{3}{x}\Rightarrow x\le 3$$

- Với $x=1$ thì (4.23) không có nghiệm nguyên dương.
- Với $x=2$ thì $\frac{1}{2}+\frac{1}{y}+\frac{1}{z}=1\Leftrightarrow \frac{1}{y}+\frac{1}{z}=\frac{1}{2}\le\frac{2}{y}\Rightarrow y\le 4$ Mặt khác, $y\ge x=2\Rightarrow y\in\{2;3;4\}$. Ta thử lần lượt các giá trị của y
  - Với $y=2$ thì (4.23) vô nghiệm nguyên.
  - Với $y=3$ thì $z=6$.
  - Với $y=4$ thì $z=4$.
- Với $x=3$, ta có $\frac{1}{3}+\frac{1}{y}+\frac{1}{z}=1\Leftrightarrow \frac{1}{y}+\frac{1}{z}=\frac{2}{3}\le\frac{2}{y}\Rightarrow y\le 3$ Mặt khác, do $y\ge x=3\Rightarrow y=3\Rightarrow z=3$

Vậy nghiệm nguyên $(x;y;z)$ của (4.23) là hoán vị của các bộ $(2;3;6)$; $(2;4;4)$; $(3;3;3)$. ■

Nhận xét. Phương pháp này được sử dụng ở chỗ sắp thứ tự các ẩn $1\le x\le y\le z$ rồi giới hạn nghiệm để giải.
Ta chỉ sử dụng phương pháp sắp thứ tự các ẩn khi vai trò các ẩn là bình đẳng với nhau. Dó đó khi vận dụng phương pháp này các bạn cần chú ý để tránh nhầm lẫn. Cụ thể, ta sẽ đến với ví dụ sau:

Ví dụ 4.18. *Giải phương trình nghiệm nguyên dương*

$$x+y+1=xyz \tag{4.24}$$

Lời giải (Lời giải sai). Không mất tính tổng quát, giả sử $1 \le x \le y \le z$. Khi đó $x+y+1 \le 3z$ hay $xyz \le 3z$, suy ra $xy \le 3$. Mà $z \ge y \ge x \ge 1$ nên $x = y = z = 1$.

Nhận xét. Cái lỗi sai ở lời giải này là do x, y, z không bình đẳng, nên không thể sắp thứ tự các ẩn như trên. Sau đây là lời giải đúng:

Lời giải. Không mất tính tổng quát, giả sử $1 \le x \le y$. Ta xét trường hợp:

- Nếu $x = y$ thì

$$\begin{aligned}(4.24) &\Leftrightarrow 2y + 1 = y^2 z \\ &\Leftrightarrow y(z-2) = 1 \\ &\Leftrightarrow \begin{cases} y = 1 \\ yz - 2 = 1 \end{cases} \\ &\Leftrightarrow \begin{cases} y = 1 \\ z = 3 \end{cases}\end{aligned}$$

- Nếu $x < y$ thì từ (4.24) suy ra $2y + 1 > xyz$. $\Rightarrow 2y \ge xyz \Rightarrow xz \le 2 \Rightarrow xz \in \{1; 2\}$.
  - Với $xz = 1 \Rightarrow x = z = 1$, thay vào (4.24) suy ra $y + 2 = y$ (vô nghiệm).
  - Với $xz = 2 \Rightarrow \begin{cases} x = 1 \\ z = 2 \end{cases}$ hoặc $\begin{cases} x = 2 \\ z = 1 \end{cases}$. Từ đây ta tìm được nghiệm $x = 1, y = 2, z = 2$ hoặc $x = 1, y = 3, z = 1$.

Vậy phương trình có nghiệm nguyên dương là $(1; 1; 3)$, $(1; 2; 2)$, $(2; 1; 2)$, $(2; 3; 1)$, $(3; 2; 1)$. ■

Nhận xét. Bây giờ bạn đã hiểu vì cách sắp xếp các ẩn như thế nào. Nhưng tại sao ở bài này lại xét $x = y$ và $x < y$ mà lại không đi vào phân

tích luôn như bài trước. Nếu bạn để ý rằng nếu không phân chia thành hai trường hợp nhưu trên thì phương trình (4.24) sẽ thành $2y+1 \geq y^2 z$, rất khó để tiếp tục phân tích ra nghiệm. Do đó việc xét nhưu trên là hợp lí.

Bài tập đề nghị

Bài 1. Giải phương trình nghiệm nguyên dương $2(x+y+z)+9 = 3xyz$.

Bài 2. Giải phương trình nghiệm nguyên dương $xyz = 3(x+y+z)$.

Bài 3. Giải phương trình nghiệm nguyên dương $5(x+y+z+t)+10 = 2xyzt$

Bài 4. Giải phương trình nghiệm nguyên dương $x! + y! = (x+y)!$
(Kí hiệu $x!$ là tích các số tự nhiên liên tiếp từ 1 đến x).

Bài 5. Tìm nghiệm nguyên dương của phương trình $x^3 + 7y = y^3 + 7x$.

Bài 6. Tìm nghiệm nguyên dương của phương trình $x_1 + x_2 + \cdots + x_{12} = x_1 x_2 \cdots x_{12}$.

Bài 7. Tìm tất cả các nghiệm nguyên dương của phương trình $\dfrac{x}{y^2 z^2} + \dfrac{y}{z^2 x^2} + \dfrac{z}{x^2 y^2} = t$.

Bài 8. Tìm nghiệm nguyên dương của phương trình $x! + y! + z! = u!$.

4.2.2 Sử dụng bất đẳng thức

Nhận xét. Để giải phương trình này, ta thường sử dụng các bất đẳng thức quen thuộc để đánh giá một vế của phương trình không nhỏ hơn (hoặc không lớn hơn) vế còn lại. Muốn cho hai vế bằng nhau thì bất đẳng thức phải trở thành đẳng thức.
Cụ thể, ta có một số bất đẳng thức cơ bản thường dùng:

1. *Bất đẳng thức Cauchy (hay còn gọi là bất đẳng thức AM-GM):* Nếu $a_1, a_2, \cdots, a_n$ là các số thực không âm thì

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 a_2 \cdots a_n}$$

Dấu đẳng thức xảy ra khi và chỉ khi $a_1 = a_2 = \cdots = a_n$.

2. *Bất đẳng thức Bunhiacopxki (hay còn được gọi là bất đẳng thức Cauchy - Bunyakovsky - Schwarz):* Với hai bộ số thực bất kì $(a_1, a_2, \cdots, a_n)$ và $(b_1, b_2, \cdots, b_n)$, ta có

$$\left(a_1^2 + a_2^2 + \cdots + a_n^2\right)\left(b_1^2 + b_2^2 + \cdots + b_n^2\right) \geq \geq \left(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n\right)^2.$$

Đẳng thức xảy ra khi và chỉ khi tồn tại số thực k sao cho $a_i = kb_i$ với mọi $i = 1, 2, \cdots, n$.

3. *Bất đẳng thức Trebusep (hay còn viết là bất đẳng thức Chebyshev):* Cho dãy hữu hạn các số thực được sắp theo thứ tự $a_1 \leq a_2 \leq \cdots \leq a_n$ và $b_1 \leq b_2 \leq \cdots \leq b_n$. Khi đó ta có:

$$n(a_1b_1 + a_2b_2 + \cdots + a_nb_n) \geq (a_1 + a_2 + \cdots + a_n)(b_1 + b_2 + \cdots + b_n)$$

Dấu đẳng thức xảy ra khi và chỉ khi $\left[\begin{array}{l} a_1 = a_2 = \cdots = a_n \\ b_1 = b_2 = \cdots = b_n \end{array}\right.$.

Bây giờ ta sẽ cùng xem xét một số ví dụ sau:

Ví dụ 4.19. *Giải phương trình nghiệm nguyên dương sau:*

$$x^6 + z^3 - 15x^2z = 3x^2y^2z - (y^2 + 5)^3 \tag{4.25}$$

Lời giải. *Nhận xét.* Ở phương trình này khi mới nhìn vào hẳn đa số các bạn sẽ có phần rối, không xác định được phương pháp làm, không vận dụng được các phương pháp đã học. Tuy nhiên nếu để ý kĩ một xí thì ta thấy $x^6 = (x^2)^3$ điều này có gì đặc biệt? Ta thấy $(x^2)^3, z^3$ và $(y^2 + 5)^3$ đều có cùng bậc ba và đề bài đã cho nguyên dương nên ta nghĩ ngay đến một Bất đẳng thức kinh điển: Bất đẳng thức Cauchy hay còn gọi là bất đẳng thức AM-GM.
Ta giải như sau

$$(4.25) \Leftrightarrow (x^2)^3 + (y^2 + 5)^3 + z^3 = 3x^2z(y^2 + 5)$$

Áp dụng Bất đẳng thức AM-GM cho bộ ba số dương $(x^2)^3, z^3$ và $(y^2+5)^3$ ta được:

$$(x^2)^3+(y^2+5)^3+z^3 \geq 3\sqrt[3]{(x^2)^3.(y^2+5)^3.z^3} = 3x^2z(y^2+5) = VP(4.25)$$

Dấu bằng chỉ xảy ra khi $x^2 = y^2 + 5 = 5$.
Mặt khác ta có:

$$x^2 = y^2 + 5 \Leftrightarrow (x-y)(x+y) = 5$$

Đây là một dạng phương trình nghiệm nguyên quen thuộc ta đã học, tôi tin chắc các bạn đều có thể dễ dàng giải phương trình trên, và từ $x; y$ trên ta có thể tìm được z một cách dễ dàng.
Đáp số: Nghiệm nguyên của phương trình (4.25) là $(x; y; z) = (3; 2; 9)$.■

Ví dụ 4.20. *Tìm nghiệm nguyên của phương trình*

$$(x+y+z)^2 = 3(x^2+y^2+1)$$

Lời giải. Áp dụng bất đẳng thức Bunyakovsky cho hai bộ số $(x, y, 1)$ và $(1, 1, 1)$ ta có

$$(x+y+1)^2 \leq (1^2+1^2+1^2)(x^2+y^2+1) = 3(x^2+y^2+1)$$

Đẳng thức xảy ra khi và chỉ khi $x = y = 1$.
Vậy phương trình có nghiệm nguyên là $(x, y) = (1, 1)$. ■

Nhận xét. Các bài Toán về phương trình nghiệm nguyên mà giải bằng cách sử dụng Bất đẳng thức rất ít dung vì rất dễ bị lộ dụng ý nếu người ra đề không khéo léo. Tuy nhiên, ta vẫn phải thành thạo phương pháp này không được xem thường nó để tránh những sai lầm đáng tiếc không thể sửa được.

Bài tập đề nghị

Bài 1. Tìm nghiệm nguyên dương x, y thỏa mãn phương trình $(x^2+1)(x^2+y^2) = 4x^2y$

Bài 2. Tìm nghiệm nguyên của phương trình $\frac{xy}{z} + \frac{yz}{x} + \frac{zx}{y} = 3$.

Bài 3. (Đề thi tuyển sinh vào đại học Vinh) Tìm nghiệm nguyên của phương trình

$$(x^2+1)(y^2+4)(z^2+9)=48xyz$$

Bài 4. Giải phương trình nghiệm nguyên

$$\frac{4}{\sqrt{x-2}}+\frac{1}{\sqrt{y-1}}+\frac{25}{\sqrt{z-5}}=16-\sqrt{x-2}-\sqrt{y-1}-\sqrt{z-5}$$

Bài 5. Tìm nghiệm nguyên của hệ phương trình $\begin{cases} x^2+z^2=9 \\ y^2+t^2=16 \\ xt+yz=12 \end{cases}$

Bài 6. Tìm nghiệm nguyên dương của phương trình $x^3+y^3-6xy+8=0$.

Bài 7. Tìm nghiệm nguyên của hệ phương trình $\begin{cases} xy+yz+zx=12 \\ x^4+y^4+z^4=48 \end{cases}$.

Bài 8. Cho phương trình $x^3+y^3+z^3=nxyz$.

a, Chứng minh rằng khi $m=1$ và $m=2$ thì phương trình không có nghiệm nguyên dương.

b, Giải phương trình nghiệm nguyên dương khi $m=3$.

Bài 9. Giải phương trình nghiệm nguyên dương $(x^3+y^3)+4(x^2+y^2)+4(x+y)=16xy$.

Bài 10. Giải phương trình nghiệm nguyên dương

$$3(x^4+y^4+x^2+y^2+2)=2(x^2-x+1)(y^2-y+1)$$

Bài 11. Giải phương trình nghiệm nguyên dương với x,y,z là các số đôi một khác nhau

$$x^3+y^3+z^3=(x+y+z)^2$$

4.2.3 Chỉ ra nghiệm

Nhận xét. Phương pháp này dành cho những bài toán giải phương trình nghiệm nguyên khi mà ta đã tìm được chính xác nghiệm nguyên và muốn chứng minh phương trình chỉ có duy nhất các nghiệm nguyên đó mà thôi.

Ví dụ 4.21. *Tìm nghiệm nguyên dương của phương trình*

$$2^x + 3^x = 5^x \tag{4.26}$$

Lời giải. Chia 2 vế của phương trình (4.26) cho số dương 5^x, ta được:

$$(4.26) \Leftrightarrow \left(\frac{2}{5}\right)^x + \left(\frac{3}{5}\right)^x = 1$$

Với $x = 1$ thì ta được $\frac{2}{5} + \frac{3}{5} = 1$:đúng nên $x = 1$ là 1 nghiệm của (4.26).
Với $x > 1$ thì

$$\left(\frac{2}{5}\right)^x + \left(\frac{3}{5}\right)^x > \frac{2}{5} + \frac{3}{5} = 1$$

Do đó mọi giá trị $x > 1$ đều không là nghiệm của (4.26). Vậy nghiệm nguyên dương của (4.26) là $x = 1$. ■

Nhận xét. Ở ví dụ trên, ta dễ nhận thấy $x = 1$ là nghiệm duy nhất của phương trình nên chỉ cần chứng minh với $x > 1$ thì phương trình vô nghiệm. Ngoài ra, từ bài toán trên ta có thể mở rộng thành hai bài toán mới:

Bài toán 4.1. *Tìm nghiệm nguyên dương của phương trình*

$$(\sqrt{3})^x + (\sqrt{4})^x = (\sqrt{5})^x$$

Bằng cách giải tương tự ta cũng tìm được nghiệm duy nhất của phương trình trên là $x = 4$.

Bài toán 4.2. *Tìm nghiệm nguyên dương của phương trình*

$$3^x + 4^y = 5^z$$

Bài toán 4.2 rõ ràng đã được nâng cao lên rõ rệt, nhưng lời giải của bài toán này là sử dụng phương pháp xét số dư đã học. Sau đây là lời giải rất đẹp của khanh3570883 hiện là Điều hành viên THPT của VMF:
Lời giải. Xét theo module 3 ta có:

$$5^z \equiv (-1)^z \pmod 3 \Rightarrow 4^y \equiv (-1)^z \pmod 3 \Rightarrow z = 2h\,(h \in \mathbb{N})$$
$$\Rightarrow (5^h - 2^y)(5^h + 2^y) = 3^x$$

Do $5^h - 2^y$ và $5^h + 2^y$ không đồng thời chia hết cho 3 nên $5^h + 2^y = 3^x$ và $5^h - 2^y = 1$.
Ta có $5^h + 2^y \equiv (-1)^h + (-1)^y = 0 \pmod 3$ và $5^h - 2^y \equiv (-1)^h - (-1)^y = 1 \pmod 3 \Rightarrow h$ lẻ và y chẵn.
Nếu $y > 2$ thì $5^h + 2^y \equiv 1 \pmod 4 \Rightarrow 3^x \equiv 1 \pmod 4 \Rightarrow 3^x \equiv 1 \pmod 8$.
Mặt khác $5 \equiv 5^h + 2^y \pmod 8 \Rightarrow 5 \equiv 3^x \pmod 8 \Rightarrow 5 \equiv 1 \pmod 8$: vô lý.
Do đó $y = 2$. Suy ra $x = y = z = 2$. ■

Phương pháp này thường hay sử dụng cho các phương trình có ẩn ở số mũ và các phương trình có nghiệm nhỏ.

4.2.4 Sử dụng Δ của phương trình bậc 2

Nhận xét. Viết phương trình dưới dạng phương trình bậc hai đối với một ẩn, dùng điều kiện. $\Delta \geq 0$ hoặc Δ là số chính phương. Ta sẽ tùy trường hợp để chọn một trong hai cách xét Δ vào việc giải toán.

Ví dụ 4.22. *Giải phương trình nghiệm nguyên*

$$3x^2 + (3y - 1)x + 3y^2 - 8y = 0 \tag{4.27}$$

Lời giải. Coi (4.27) là phương trình bậc 2 ẩn x. Xét $\Delta_x = -27y^2 + 9y + 1$.
Đề (4.27) có nghiệm x thì

$$\Delta_x \geq 0 \Leftrightarrow -27y^2 + 9y + 1 \geq 0 \Leftrightarrow -0,01 \leq y \leq 3,3 \Rightarrow y \in \{0; 1; 2; 3\}$$

Nếu $y = 0 \Rightarrow 3x^2 - x = 0 \Rightarrow x = 0$ vì $x \in \mathbb{Z}$.
Nếu $y = 1 \Rightarrow 3x^2 + 2x - 5 = 0 \Rightarrow x = 1$ vì $x \in \mathbb{Z}$.
Nếu $y = 2$ hoặc $y = 3$ thì không tìm được x nguyên nên loại.
Vậy (4.27) có nghiệm nguyên $(x; y) = (0; 0); (1; 1)$. ■

Ví dụ 4.23. *Giải phương trình nghiệm nguyên*

$$3x^2 - y^2 - 2xy - 2x - 2y + 8 = 0 \tag{4.28}$$

Lời giải. Ta có

$$(4.28) \Leftrightarrow y^2 + 2(x+1)y - (3x^2 - 2x + 8) = 0$$
$$\Delta'_y = (x+1)^2 + 3x^2 - 2x + 8 = 4x^2 + 9$$

Để (4.28) có nghiệm thì $\Delta'_y = 4x^2 + 9$ là số chính phương. Đặt $4x^2 + 9 = k^2$ với $k \in \mathbb{N}$, ta đưa về phương trình ước số và tìm được $x \in \{2; 0; -2\}$.

- Với $x = 2$ ta được $y^2 + 6y - 16 = 0$ nên $y \in \{-8; 2\}$.
- Với $x = 0$ thì $y^2 + 2y - 8 = 0$ nên $y \in \{-4; 2\}$.
- Với $x = -2$ thì $y^2 - 2y - 24 = 0$ nên $y \in \{-6; 4\}$.

Kết luận. Vậy phương trình (4.28) có nghiệm $(x; y)$ là $(2; -8)$, $(2; 2)$, $(0; -4)$, $(0; 2)$, $(-2; 6)$, $(-2; -4)$. ■

Nhận xét. Hai bài toán trên đều có thể sử dụng phương pháp đưa về phương trình ước số để giải.

Bài tập đề nghị

Bài 1. Tìm ở các phương pháp trước (nhất là ở phương pháp đưa về phương trình ước số) các bài toán để giải bằng phương pháp này.

Bài 2. Tìm nghiệm nguyên của phương trình $x + xy + y = x^2 + y^2$.

Bài 3. Giải phương trình nghiệm nguyên $10x^2 + 5y^2 + 38 - 12xy + 16y - 36x = 0$.

Bài 4. Tìm nghiệm nguyên phương trình $9x^2 + x^2 + 4y^2 + 34 - 12xy + 20y - 36x = 0$.

Bài 5. Tìm nghiệm nguyên dương của $x + 2y^2 + 3xy + 3x + 5y = 14$.

Bài 6. Tìm nghiệm nguyên phương trình $x^2 - xy - 6y^2 + 2x - 6y - 10 = 0$.

Bài 7. Tìm nghiệm nguyên của phương trình $x^2 + 2y62 + 3xy + 3x + 5y = 15$.

Bài 8. Tìm nghiệm nguyên của phương trình $2x^2 + 6y^2 + 7xy - x - y = 25$.

Bài 9. Tìm nghiệm nguyên của phương trình $9x^2 - 10y^2 - 9xy + 3x - 5y = 9$.

Bài 10. Tìm nghiệm nguyên của phương trình $12x^2 + 6xy + 3y^2 = 28(x + y)$.

(Thi vào lớp 10 chuyên, DHKHTN-DHQGHN năm 1994)

Bài 11. Tìm nghiệm nguyên của phương trình $3(x^2 + xy + y^2) = x + 8y$.

Bài 12. Tìm nghiệm nguyên của phương trình $7(x^2 + xy + y^2) = 39(x + y)$.

Bài 13. Tìm nghiệm nguyên của phương trình $2x^2 + y^2 + 3xy + 3x + 2y + 2 = 0$.

Bài 14. Tìm nghiệm nguyên của phương trình $x^2 + 2y^2 + 3xy - x - y + 3 = 0$.

Bài 15. Tìm nghiệm nguyên của phương trình $3x^2 + 4y^2 + 12x + 3y + 5 = 0$.

4.2.5 Phương pháp kẹp

Nhận xét. Sử dụng tính chất lũy thừa cùng bậc của số nguyên liên tiếp hoặc tích các số nguyên liên tiếp ... để đưa phương trình nghiệm nguyên cần giải về dạng phương trình khác ít ẩn hơn và quen thuộc hơn. Phương pháp này còn có cách gọi khác là phương pháp khử ẩn. Ta thường vận dụng các nhận xét sau:

1. $X^n \le Y^n \le (X+a)^n \quad (a \in \mathbb{N}^*)$ thì $Y^n = (X+a-i)^n$ với $i = 0; 1; 2; \cdots; a$.
   Ví dụ với $n = 2$ thì:
   - Không tồn tại $x \in \mathbb{Z}$ để $a^2 < x^2 < (a+1)^2$ với $a \in \mathbb{Z}$.
   - Nếu $a^2 < x^2 < (a+2)^2$ thì $x^2 = (a+1)^2$
2. $X(X+1)\cdots(X+n) \le Y(Y+1)\cdots(Y+n) \le (X+a)(X+a+1)\cdots(X+a+n)$ thì $Y(Y+1)\cdots(Y+n) = (X+i)(X+1+i)\cdots(X+a+i)$ với $i = 0; 1; 2; \cdots; a$.
   Ví dụ:
   - Không tồn tại $b \in \mathbb{Z}$ để $a(a+1) < b(b+1) < (a+1)(a+2)$ với $a \in \mathbb{Z}$.
   - Với $a(a+1) < b(b+1) < (b+2)(b+3)$ thì $b(b+1) = (b+2)(b+3)$.

Ví dụ 4.24. *Tìm các số nguyên dương x để biểu thức sau là số chính phương*

$$A = x^4 + 2x^3 + 2x^2 + x + 3 \tag{4.29}$$

Lời giải. Vì A là số chính phương nên ta có thể đặt

$$A = x^4 + 2x^3 + 2x^2 + x + 3 = y^2 (y \in \mathbb{N})$$

Ta thấy

$$\begin{aligned} y^2 &= (x^4 + 2x^3 + x^2) + x^2 + x + 3 \\ &= (x^2+x)^2 + \left(x + \frac{1}{2}\right)^2 + \frac{11}{4} \\ &> (x^2+x)^2 \\ \Rightarrow y^2 &> (x^2+x)^2, (i) \end{aligned}$$

Nếu $x = 1 \Rightarrow A = 9$: là số chính phương nên thỏa đề.
Nếu $x > 1$ thì xét hiệu

$$(x^2+x+1)^2-y^2 = x^2+x-2 = (x+2)(x-1) > 0 \Rightarrow y^2 < (x^2+x+1)^2, (ii)$$

Từ (i) và (ii), ta có

$$(x^2+x)^2 < y^2 < (x^2+x+1)^2$$

Suy ra, không tồn tại $y \in \mathbb{N}$ để $y^2 = A$ khi $x > 1$.
Vậy $x = 1$ là giá trị cần tìm. ■

Ví dụ 4.25. *Giải phương trình nghiệm nguyên*

$$x^4 + x^2 + 4 = y^2 - y \tag{4.30}$$

Lời giải. Ta có đánh giá sau

$$x^2(x^2+1) < x^4 + x^2 + 4 < (x^2+2)(x^2+3) \tag{4.31}$$

Từ (4.30) và (4.31) suy ra

$$x^2(x^2+1) < y(y-1) < (x^2+2)(x^2+3). \tag{4.32}$$

Vì x, y, z nguyên nên từ (4.32) suy ra

$$y(y-1) = (x^2+1)(x^2+2) \tag{4.33}$$

Từ (4.30) và (4.33) thì

$$x^4 + x^2 + 4 = (x^2+1)(x^2+2) \Leftrightarrow x^2 = 1 \Leftrightarrow x = \pm 1$$

Từ đây dễ tìm được $y = -1$ hoặc $y = 3$.
Vậy pt đã cho có bốn cặp nghiệm

$$(x, y) = \{(1, -2), (1, 3), (-1, -2), (-1, 3)\}$$

Bài tập đề nghị
Tìm nghiệm nguyên của các phương trình sau:

Bài 1. $x^4 + x^2 + 1 = y^2$

Bài 2. $3(x^4 + y^4 + x^2 + y^2 + 2) = 2(x^2 - x + 1)(y^2 - y + 1)$

Bài 3. $2x^4 + 3x^2 + 1 - y^2 = 0$

Bài 4. $x^2 + (x + y)^2 = (x + 9)^2$

Bài 5. $y^3 - x^3 = 2x + 1$

Bài 6. $x^4 - y^4 + z^4 + 2x^2z^2 + 3x^2 + 4z^2 + 1 = 0$

Bài 7. $x^3 - y^3 - 2y^2 - 3y - 1 = 0$

Bài 8. $x^4 + (x + 1)^4 = y^2 + (y + 1)^2$

Bài 9. $9^x - 3^x = y^4 + 2y^3 + y^2 + 2y$

Bài 10. $x^4 + x^2 - y^2 + y + 10 = 0$

Bài 11. $x^6 - 4y^3 - 4y^4 = 2 + 3y + 6y^2$

Bài 12. $(x - 2)^4 - x^4 = y^3$

Bài 13. $x^3 + 8x^2 - 6x + 8 = y^3$

4.3 Nguyên tắc cực hạn, lùi vô hạn

4.3.1 Lùi vô hạn

Ví dụ 4.26 (Korea 1996). *Giải phương trình nghiệm nguyên sau:*

$$x^2 + y^2 + z^2 = 2xyz \tag{4.34}$$

Lời giải. Giả sử $(x_0; y_0; z_0)$ là bộ nghiệm nguyên của (4.34) thì ta có

$$x_0^2 + y_0^2 + z_0^2 = 2x_0y_0z_0$$

Rõ ràng VT (4.34) chẵn do VP (4.34) chẵn nên có 2 trường hợp xảy ra:

• *Trường hợp 1.* Trong $x_0; y_0; z_0$, có 2 số lẻ, 1 số chẵn. Không mất tính tổng quát, giả sử $x_0; y_0$ lẻ còn z_0 chẵn. Xét theo module 4 thì

$$VT(4.34) \equiv 2 \pmod 4,\ VP(4.34) \equiv 0 \pmod 4 : \text{vô lý!}$$

Vậy trường hợp này không xảy ra.
• *Trường hợp 2.* $x_0;\ y_0;\ z_0$ đều chẵn. Đặt $x_0 = 2x_1;\ y_0 = 2y_1;\ z_0 = 2z_1$ với $x_1; y_1; z_1 \in \mathbb{Z}$. Thay vào (4.34) và rút gọn, ta thu được

$$x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1$$

Lập luận như trên, ta lại được $x_1;\ y_1;\ z_1$ đều chẵn.

Quá trình đó diễn ra tiếp tục nên $x_0;\ y_0;\ z_0 \vdots 2^k$ với k tự nhiên tùy ý. Điều đó chỉ xảy ra khi và chỉ khi $x_0 = y_0 = z_0 = 0$. ■

4.3.2 Nguyên tắc cực hạn

Định nghĩa 4.1 *Nguyên tắc cực hạn hay còn gọi là nguyên lí khởi đầu cực trị. Về mặt hình thức thì phương pháp này khác với phương pháp lùi vô hạn nhưng cách sử dụng đều như nhau đều chứng minh phương trình chỉ có nghiệm tầm thường (nghiệm tầm thường là nghiệm bằng 0). Phương pháp giải như sau:*
Giả sử $(x_0; y_0; z_0; ...)$ là nghiệm của $f(x; y; z; ...)$ với một điều kiện nào đó ràng buộc bộ $(x_0; y_0; z_0; ...)$. Chẳng hạn x_0 nhỏ nhất hoặc $x_0 + y_0 + z_0 + ...$ nhỏ nhất và sau đó bằng các phép biến đổi số học ta lại tìm được 1 bộ nghiệm $(x_1; y_1; z_1; ...)$ trái với những điều kiện ràng buộc trên. Ví dụ ta chọn bộ $(x_0; y_0; z_0; ...)$ với điều kiện x_0 nhỏ nhất sau đó ta lại tìm được 1 bộ $(x_1; y_1; z_1; ...)$ với $x_1 < x_0$ dẫn đến phương trình có nghiệm tầm thường. △

Ví dụ 4.27. *Giải phương trình nghiệm nguyên sau*

$$8x^4 + 4y^4 + 2z^4 = t^4 \tag{4.35}$$

Lời giải. Giả sử $(x_0; y_0; z_0; t_0)$ là nghiệm nguyên không tầm thường của (4.35) với x_0 nhỏ nhất.

Từ (4.35) suy ra t_0 chẵn. Đặt $t = 2t_1 (t_1 \in \mathbb{Z})$ thế vào (4.35) và rút gọn, ta được

$$4x_o^4 + 2y_o^4 + z_o^4 = 8t_1^4$$

Do vậy z_0 chẵn. Đặt $z_0 = 2z_1 (z_1 \in \mathbb{Z})$, thế vào và rút gọn ta được

$$2x_o^4 + y_o^4 + 8z_1^4 = 4t_1^4$$

Do vậy y_0 chẵn. Đặt $y_0 = 2y_1 (y_1 \in \mathbb{Z})$, thế vào và rút gọn ta được

$$x_o^4 + 8y_1^4 + 4z_1^4 = 2t_1^4$$

Do vậy x_0 chẵn. Đặt $x_0 = 2x_1 (x_1 \in \mathbb{Z})$, thế vào phương trình ta được

$$8x_1^4 + 4y_1^4 + 2z_1^4 = t_1^4$$

Suy ra $(x_1; y_1; z_1; t_1)$ cũng là nghiệm của (4.35) . Dễ thấy $x_1 < x_0$ (vô lí với điều giả sử). Do đó phương trình có nghiệm nguyên duy nhất là $(x; y; z; t) = (0; 0; 0; 0)$. ■

Bài tập đề nghị

Bài 1. Giải các phương trình nghiệm nguyên $x^2 + y^2 = 3z^2$

Bài 2. Giải các phương trình nghiệm nguyên $x^3 + 2y^3 = 4z^3$

Bài 3. Giải các phương trình nghiệm nguyên $3x^2 + 6y^2 + 12z^2 = t^2$

Bài 4. Giải các phương trình nghiệm nguyên $x^2 + 6y^2 + 2z^2 = 4t^2$

Bài 5. Giải phương trình nghiệm nguyên $x^2 + y^2 + z^2 + t^2 = x^2y^2z^2$.

Bài 6. Giải phương trình nghiệm nguyên $5x^3 + 11y^3 + 13z^3 = 0$.

Chương

5 Phương trình đồng dư

Trần Trung Kiên (ISPECTORGADGET)
Nguyễn Đình Tùng (TUNGC3SP)

5.1 Phương trình đồng dư tuyến tính

Định nghĩa 5.1 *Phương trình đồng dư dạng* $ax \equiv b \pmod{m}$ *được gọi là phương trình đồng dư tuyến tính với* a, b, m *là các số đã biết.*
x_0 *là một nghiệm của phương trình khi và chỉ khi* $ax_0 \equiv b \pmod{m}$.
Nếu x_0 *là một nghiệm của phương trình thì các phần tử thuộc lớp* $\overline{x_0}$ *cũng là nghiệm.* △

Ví dụ 5.1. *Giải phương trình đồng dư sau:* $12x \equiv 7 \pmod{23}$
Lời giải. *Do* $(12; 23) = 1$ *nên phương trình luôn có nghiệm duy nhất. Ta tìm một số nguyên sao cho* $7 + 23k$ *chia hết cho 12. Chọn* $k = 7$ *suy ra* $12x \equiv 7.24 \pmod{23} \Rightarrow x \equiv 14 \pmod{23}$ ■

Ví dụ 5.2. *Giải phương trình* $5x \equiv 2 \pmod 7$ △

Lời giải. Vì $(5;2) = 1$ nên tồn tại số $k = 4$ sao cho $2 + 7k$ chia hết cho 5. Khi ấy $5x \equiv 2 + 6.7 \pmod 7$ ta được nghiệm $x \equiv \dfrac{30}{5} \equiv 6 \pmod 7$ hay $x = 6 + 7k$ ■

Ví dụ 5.3. *Giải phương trình:* $5x \equiv 4 \pmod{11}$ △

Lời giải. Ta có:

$$\begin{cases} 5x \equiv 4 \pmod{11} \\ 4 \equiv 4 \pmod{11} \end{cases}$$

Áp dụng tính chất bắc cầu ta có: $5x \equiv 4 \pmod{11} \Rightarrow 5x = 11t + 4$
Ta có thể lấy $t = 1; x = 3$. Từ đó phương trình có nghiệm duy nhất là $x \equiv 3 \pmod{11}$ ■

Nhận xét. Cách xác định nghiệm này là đơn giản nhưng chỉ dùng được trong trường hợp a là một số nhỏ hoặc dễ thấy ngay số k.

5.2 Phương trình đồng dư bậc cao

Ví dụ 5.4. *Giải phương trình* $2x^3 + 4 \equiv 0 \pmod 5$ △

Lời giải. Ta thấy $x = 2$ suy ra $2x^3 \equiv -4 \pmod 5$.
Nên $x = 2$ là nghiệm duy nhất của phương trình đã cho. ■

5.3 Hệ phương trình đồng dư bậc nhất một ẩn

Định nghĩa 5.2 *Hệ phương trình có dạng sau được gọi là hệ phương trình đồng dư bậc nhất một ẩn*

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ .... \\ x \equiv b_k \pmod{m_k} \end{cases}$$

Với $m_1; m_2; ...m_k$ *là những số nguyên lớn hơn 1 và* $b_1; b_2; ...; b_k$ *là những số nguyên tùy ý.* △

Nhận xét. • Trong trường hợp tổng quát, chúng ta có thể chứng minh được rằng: Điều kiện cần và đủ để hệ phương trình (5.2) có nghiệm là $UCLN(m_i; m_j)$ chia hết $b_i - b_j$ với $i \neq j (1 \leq i, j \leq k)$.

- Giả sử $m = p_1^{\alpha 1} p_2^{\alpha a_2} ... p_k^{\alpha k}$ là phân tích tiêu chuẩn của m. Khi ấy phương trình đồng dư $f(x) \equiv 0 \pmod{m}$ tương đương với hệ phương trình đồng dư $f(x) \equiv 0 \pmod{p_i^{\alpha 1}}, i = 1, 2, ..., k$. Từ đó suy ra rằng nếu $x \equiv b_1 \pmod{p_1^{\alpha 1}}$ là một nghiệm của phương trình $f(x) \equiv 0 \pmod{p_i}, i = 1, 2, ..., k$ thì nghiệm của hệ phương trình của hệ phương trình đồng dư

$$\begin{cases} x \equiv b_1 \left(\mathrm{mod} p_1^{\alpha_1}\right) \\ x \equiv b_2 \left(\mathrm{mod} p_2^{\alpha_2}\right) \\ \quad ... \\ x \equiv b_k \left(\mathrm{mod} p_k^{\alpha_k}\right) \end{cases}$$

cho ta nghiệm của phương trình $f(x) \equiv 0 (mod m)$.

Vậy trong • *Trường hợp tổng quát giải một phương trình đồng dư dẫn đến giải hệ trên. Với các module $m_1, m_2, ..., m_k$ đôi một nguyên tố cùng nhau.*

Phương pháp chung để giải:

- Trường hợp 1: hệ 2 phương trình

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \end{cases}$$

Với giả thiết $d = (m_1, m_2)$ chia hết cho $b_1 - b_2$. Trước tiên ta nhận xét rằng, mọi số $x = b_1 + m_1 t, t \in \mathbb{Z}$ là nghiệm của phương trình thứ nhất. Sau đó ta tìm cách xác định t sao cho x nghiệm đúng phương trình thứ hai, nghĩa là hệ hai phương trình trên tương đương với hệ phương trình

$$\begin{cases} x = b_1 + m_1 t \\ b_1 + m_1 t \equiv b_2 \pmod{m_2} \end{cases}$$

Vì giả thiết $d = (m_1, m_2)$ là ước $b_1 - b_2$ nên phương trình: $b_1 + m_1 t \equiv b_2 \pmod{m_2}$ tương đương với phương trình:

$$\frac{m_1}{d} t \equiv \frac{b_2 - b_1}{d} \pmod{\frac{m_2}{d}}$$

Nhưng $(\frac{m_1}{d}, \frac{m_2}{d}) = 1$ nên phương trình đồng dư này cho ta nghiệm $t \equiv t_0 \pmod{\frac{m_2}{d}}$, là tập hợp tất cả các số nguyên

$$t = t_0 + \frac{m_2}{d} u, u \in \mathbb{Z}$$

Thay biểu thức của t vào biểu thức tính x ta được tập hợp các giá trị của x nghiệm đúng cả hai phương trình đồng dư đang xét là:
$x = b_1 + m_1(t_0 + \frac{m_2}{d} u) = b_1 + m_1 t_0 + \frac{m_1 m_2}{d} u$, hay $x = x_0 + m_u$ với $x_0 = b_1 + m_1 t_0, m = BCNN(m_1, m_2)$.

Vậy $x \equiv x_0 \pmod{m}$ là nghiệm của hệ hai phương trình đồng dư đang xét.

- Trường hợp 2: Hệ gồm n phương trình. Đầu tiên giải hệ hai phương trình nào đó của hệ đã cho, rồi thay trong hệ hai phương trình đã giải bằng nghiệm tìm thấy, ta sẽ được một hệ gồm $n-1$ phương trình tương đương với với hệ đã cho. Tiếp tục như vậy sau $n-1$ bước ta sẽ được nghiệm cần tìm.

Ví dụ 5.5. *Giải hệ phương trình:* $\begin{cases} x \equiv 26 \pmod{36} \\ x \equiv 62 \pmod{60} \\ x \equiv 92 \pmod{150} \\ x \equiv 11 \pmod{231} \end{cases}$ △

Lời giải. Hệ hai phương trình:

$$\begin{cases} x \equiv 26 \pmod{36} \\ x \equiv 62 \pmod{60} \end{cases} \Leftrightarrow \begin{cases} x = 26 + 36t \\ 26 + 36t \equiv 62 \end{cases}, t \in \mathbb{Z}.$$

$$\begin{aligned} 26 + 36t &\equiv 62 \pmod{60} \\ \Leftrightarrow 36t &\equiv 36 \pmod{60} \\ \Leftrightarrow t &\equiv 1 \pmod{5} \end{aligned}$$

Vậy nghiệm của hệ là: $x \equiv 26 + 36.1 \pmod{180}$ hay $x \equiv 62 \pmod{180}$
Do đó hệ phương trình đã cho tương đương với hệ:

$$\begin{cases} x \equiv 62 \pmod{180} \\ x \equiv 92 \pmod{150} \\ x \equiv 11 \pmod{231} \end{cases}$$

Ví dụ 5.6. *Giải hệ phương trình*

$$\begin{cases} x \equiv 62 \pmod{180} \\ x \equiv 92 \pmod{150} \end{cases} \Leftrightarrow \begin{cases} x = 62 + 180t \\ 62 + 180t \equiv 92 \pmod{150} \end{cases}, t \in \mathbb{Z}.$$

Lời giải. Ta có:

$$\begin{aligned} & 62 + 180t \equiv 92 \pmod{1)50} \\ \Leftrightarrow & 180t \equiv 30 \pmod{150} \\ \Leftrightarrow & 6t \equiv 1 \pmod{5} \Leftrightarrow \qquad\qquad t \equiv 1 \pmod{5} \end{aligned}$$

Vậy nghiệm của hệ là:

$$x \equiv 62 + 180.(1+) \pmod{900} \Leftrightarrow x \equiv 242 \pmod{900}$$

Hệ đã cho tương đương với:

$$\begin{cases} x \equiv 242 \,(\mathrm{mod} 900) \\ x \equiv 11 \,(\mathrm{mod} 231) \end{cases}$$

Hệ này có nghiệm $x \equiv 242 \pmod{69300}$, và đây cũng là nghiệm của hệ đã cho cần tìm. ■

Ví dụ 5.7. *Tìm số nguyên dương nhỏ nhất thỏa tính chất: chia* 7 *dư* 5*, chia* 11 *dư* 7 *và chia* 13 *dư* 3*.* △

Lời giải. Ta có: $n_1 = 7; N_1 = 11.13 = 143; n_2 = 11; N_2 = 7.13 = 91; n_3 = 13; N_3 = 7.11 = 77$.
Ta có $N_1 b_1 \equiv 3b_1 \equiv 1 \pmod{7} \to b_1 = -2$. Tương tự $b_2 = 4; b_3 = -1$
Vậy $a = 143(-2)5 + (91)(4)(7) + (77)(-1)(3) = -1430 + 2548 - 231 = 887$ vậy các số cần tìm có dạng $b = 877 + 1001k$.
Vậy 877 là số cần tìm. ■

Ví dụ 5.8 (Chọn đội tuyển KHTN). *Xét hệ đồng dư gồm 3 phương trình:*

$$xy \equiv -1 \pmod{z} \quad (5.1)$$
$$yz \equiv 1 \pmod{x} \quad (5.2)$$
$$xz \equiv 1 \pmod{y} \quad (5.3)$$

Hãy tìm số bộ (x, y, z) nguyên dương phân biệt với 1 trong 3 số là 19. △

Lời giải. Từ ba phương trình, theo tính chất đồng dư ta lần lượt có $xy + 1 \vdots z$ và $yz - 1 \vdots x$ và $zx - 1 \vdots y$
Suy ra

$$\begin{aligned}&(xy+1)(yz-1)(zx-1) \vdots xyz\\ \Rightarrow &x^2y^2z^2 - x^2yz - xy^2z + xyz^2 + xy - yz - zx + 1 \vdots xyz\\ \Rightarrow &xy - yz - zx + 1 \vdots xyz\end{aligned}$$

Nhận thấy do x, y, z nguyên dương cho nên $xyz \geq 1$. Suy ra $xy - yz - zx + 1 \leq 2xyz$
Mặt khác $yz + zx - xy - 1 \leq 2xyz \Rightarrow -(yz + zx - xy - 1) \geq -2xyz$
Do đó ta có bất phương trình kép $-2xyz \leq xy - yz - zx + 1 \leq 2xyz$

Mà $xy-yz-zx+1 \vdots xyz \Rightarrow xy-yz-zx+1 = 2xyz, 1xyz, 0, -1xyz, -2xyz$
• Trường hợp 1: $xy - yz - zx + 1 = 2xyz \Rightarrow xy \equiv -1 \pmod{z}, yz \equiv 1 \pmod{x}, zx \equiv 1 \pmod{y}$
Cho nên ta chỉ cần tìm nghiệm của $xy - yz - zx + 1 = 2xyz$ là xong.
Vì x, y, z có một số bằng 19 nên ta thay lần lượt vào.
Nếu $x = 19 \Rightarrow 19y - yz - 19z + 1 = 38yz \Rightarrow 39yz - 19y + 19z = 1$
$\Rightarrow (39y + 19)(39z - 19) = -322$ Với $y = 19$ hoặc $z = 19$ thì tương tự.
• Trường hợp 2,3,4,5: $xy-yz-zx+1 = 1xyz, 0, -1xyz, -2xyz$ làm hoàn toàn tương tự, ta đẩy được về phương trình có dạng $au+bv = ab+uv+x$ với x là hằng số.
Đưa về $(a - v)(b - u) = x$ và giải kiểu phương trình ước số. Bài toán hoàn tất. ■

Nhận xét. Bài toán này mà không cho điều kiện một số bằng 19 thì không đưa được dạng $au + bv = ab + uv + x \leftrightarrow (a - v)(b - u) = x$ lúc đó suy ra vô hạn nghiệm.

5.4 Bậc của phương trình đồng dư

Định nghĩa 5.3 *Xét phương trình đồng dư* $f(x) = 0 \pmod m$ *với* $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n, a_i \in \mathbb{N}, i = 0, 1, ..., n$
Nếu a_0 *không đồng dư* $0 \pmod m$ *thì ta nói* n *là bậc của phương trình đồng dư.* △

Ví dụ 5.9. *Xác định bậc của phương trình* $15x^6 - 8x^4 + x^2 + 6x + 8 \equiv 0 \pmod 3$ △

Lời giải. Ta thấy $15 \equiv 0 \pmod 3$ nên bậc của phương trình không phải là bậc 6. Phương trình trên tương đương với $-8x^4 + x^2 + 2 \equiv 0 \pmod 3$
Vì $-8 \not\equiv 0 \pmod 3$ nên bậc phương trình là $n = 4$. ■

5.5 Bài tập

Bài 1. Giải các phương trình sau: a) $7x \equiv 6 \pmod{13}$ b) $(a + b)x \equiv a^2 + b^2 \pmod{ab}$ với $(a, b) = 1$ c) $17x \equiv 13 \pmod{11}$ d) $x^2 + x - 2 \equiv 1 \pmod 3$

Bài 2. Giải các hệ phương trình: a) $\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 4 \\ x \equiv 2 \pmod 7 \\ x \equiv 9 \pmod{11} \end{cases}$

b) $\begin{cases} 5x \equiv 1 \pmod{12} \\ 5x \equiv 2 \pmod 8 \\ 7x \equiv 3 \pmod{11} \end{cases}$

Bài 3. Tìm a nguyên để hệ phương trình sau có nghiệm

a) $\begin{cases} x \equiv 3 \pmod 3 \\ x \equiv 1 \pmod 4 \\ x \equiv 11 \pmod 7 \\ x \equiv a \pmod{11} \end{cases}$

b) $\begin{cases} 2x \equiv a \pmod 3 \\ 3x \equiv 4 \pmod{10} \end{cases}$

Bài 4. Một lớp gồm 40 học sinh đứng thành vòng tròn và quay mặt và trong vòng tròn để chơi bóng. Mỗi học sinh nhận được bóng phải ném qua mặt 6 bạn ở bên tay trái mình. Chứng minh rằng tất cả học sinh trong lớp đều nhận được bóng ném tới mình sau 40 lần ném bóng liên tiếp.

5.6 Ứng dụng định lý Euler để giải phương trình đồng dư

Qua bài viết này tôi xin giới thiệu một phương pháp để giải phương trình đồng dư bằng cách khai thác định lý Euler

Trước hết, xin nhắc lại vài kiến thức quen thuộc.

Định nghĩa 5.4 *Hàm Euler $\varphi(m)$ với số nguyên dương m là các số tự nhiên nhỏ hơn m là các số nguyên tố với m.* △

5.6.1 Định lý Euler.

Định lý 5.1 (Euler)– *Cho m là số nguyên dương và $(a, m) = 1$ thì* $a^{\varphi(m)} \equiv 1 \pmod m$

Hàm φ có tính chất sau:

- $\varphi(mn) = \varphi(m)\varphi(n)$ với $(m; n) = 1$
- Nếu p nguyên tố $\varphi(p) = p - 1; \varphi(p^n) = p^n - p^{n-1} (n > 1)$

- Nếu $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha^k}, p_i$ là các số nguyên tố thì

$$\phi(m) = m\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right)$$

Bây giờ ta xét $m = a.b$ trong đó $(a; b) = 1$ thì có các kết quả sau

Định lý 5.2–

$$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab} \tag{5.4}$$

Chứng minh. Theo định lý Euler ta có: $a^{\varphi(b)} \equiv 1 \pmod{b}$ mà $b^{\varphi(a)} \equiv 0 \pmod{b}$
Nên $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{b}$.
Tương tự ta có:$a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{a}$
Theo tính chất đồng dư thì : $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ ■

Định lý 5.3– *Giả sử có $k(k \geq 2)$ số nguyên dương $m_1; m_2; \ldots m_k$ và chúng nguyên tố với nhau từng đôi một. Đặt $M = m_1.m_2 \ldots m_k = m_i t_i$ với $i = 1, 2, 3 \ldots, k$ ta có*

$$t_1^{\varphi(m_1)} + t_2^{\varphi(m_2)} + ... + t_k^{\varphi(m_k)} \equiv 1 \pmod{M} \tag{5.5}$$

Chứng minh. Từ giả thiết ta có $(m_i, t_i) = 1$ với mỗi $i = 1, 2, \ldots, k$ nên theo định lý Euler thì

$$t_1^{\varphi(m_1)} \equiv 1 \pmod{m_i} \tag{5.6}$$

Mặt khác với $i; j$ thuộc tập 1;2;...;k và $i \neq j$ thì t_j chia hết cho m_j nên $(t_j; m_i) = m_i$ hay

$$t_j^{\varphi(m_i)} \equiv 0 \pmod{m_i} \tag{5.7}$$

Đặt $S = t_1^{\varphi(m_1)} + t_2^{\varphi(m_2)} + ... + t_k^{\varphi(m_k)}$
Từ (5.6) và (5.7) có $S \equiv t_i^{\varphi m_i} \equiv 1 \pmod{m_i}$
Vì $m_1; m_2; \ldots m_k$ nguyên tố với nhau từng đôi một, nên theo tính chất đồng dư thức có
$S - 1 \equiv 0 \pmod{m_1.m_2...m_k} \Leftrightarrow S \equiv 1 \pmod{M}$, tức là có (5.5). ■

Khi mở rộng (5.4) theo hướng nâng lên lũy thừa các số hạng ta có kết quả sau.

ĐỊNH LÝ 5.4– *Với $(a,b)=1$ và n,v là hai số nguyên dương nào đó thì*

$$a^{n\varphi(b)}+b^{v\varphi(a)}\equiv 1 \pmod{ab} \tag{5.8}$$

Chứng minh. Để tiện lập luận đặt $x=a^{\varphi(b)}$.
Theo định lý Euler thì $x=a^{\varphi(b)}\equiv 1 \pmod b \Leftrightarrow x-1\equiv 0 \pmod b$
Đồng thời $x=a^{\varphi(b)}\equiv 0 \pmod a$.
Từ đó có $x(x-1)\equiv 0 \pmod a$ và $x(x-1)\equiv 0 \pmod b$ nên $x(x-1)\equiv 0 \pmod{ab}$
Từ đó $x^3\equiv x^2.x\equiv x.x\equiv x^2\equiv x \pmod{ab}$ và cứ lập luận như thế có $x^n\equiv x \pmod{ab}$ hay $a^{n\varphi(b)}\equiv a^{\varphi(b)} \pmod{ab}$
Tương tự ta có: $b^{v\varphi(a)}\equiv b^{\varphi(a)} \pmod{ab}$ nên theo (5.4) có $a^{n\varphi(b)}+b^{v\varphi(a)}\equiv b^{\varphi(a)}+a^{\varphi(b)}\equiv 1 \pmod{ab}$.
(5.8) được chứng minh. ■

HỆ QUẢ 5.1– *Với $(a;b)=1$ thì $a^{n\varphi(b)}+b^{n\varphi(a)}\equiv 1 \pmod{ab}$* □

Hệ quả này có thể chứng minh trực tiếp khi nâng hai vế của hệ thức (5.4) lên lũy thừa bậc n (sử dụng khi triển nhị thức Newton) và chú ý rằng $ab\equiv 0 \pmod{ab}$. Nên lưu ý rằng trong đồng dư thức thì $a\not\equiv 0 \pmod{ab}$!

Với kí hiệu như ở định lý 5.3 ta có $t_i.t_j\equiv 0 \pmod M$ với i khác j và mọi $i;j$ thuộc tập 1,2,...,k (nhưng $t\not\equiv 0 \pmod M$ với mọi $i=1,2,3,...k$)

Từ đó khi nâng hai vế của (5.5) lên lũy thừa bậc n ta có kết quả sau.

ĐỊNH LÝ 5.5– *Với các giả thiết như định lý 5.3 ta có:*

$$t_1^{n\varphi(m_1)}+t_2^{n\varphi(m_2)}+...+t_k^{n\varphi(m_k)}\equiv 1 \pmod M \tag{5.9}$$

Với các kí hiệu như trên ta đặt $a=m_i$ và $b=t_i$ thì theo (5.4) có

$$m_i^{n\varphi(t_i)}+t_i^{n\varphi(m_i)}\equiv 1 \pmod M \tag{5.10}$$

Cộng từng vế của k đồng thức dạng (5.10) và sử dụng (5.5) ta được kết quả sau:

Định lý 5.6– *Với các giả thiết ở định lý 5.3 ta có:*

$$m_1^{\varphi(t_1)} + m_2^{\varphi(t_2)} + ... + m_k^{n\varphi(t_k)} \equiv k - 1 \pmod{M} \tag{5.11}$$

Khi nhân 2 vế của (??) với m_i ta được

$$m_1^{1+\varphi(t_i)} + m_i.t_i^{\varphi(m_i)} + \equiv m_i \pmod{M} \tag{5.12}$$

Do $m_i.t_i^{\varphi(m_i)} = m_i.t_i.t_i^{\varphi(m_i)-1} = M.t_i^{(m_i)-1}$ nên

$$m_i^{1+\varphi(t_1)} \equiv m_i \pmod{M}, i = \overline{1,k} \tag{5.13}$$

Cộng từng vế k đồng thức dạng (5.13) ta được kết quả sau:

Định lý 5.7– *Với các giả thiết như định lý 5.3 ta có:*

$$m_1^{1+\varphi(t_1)} + m_2^{2+\varphi(t_2)} + ... + m_k^{1+\varphi(t_k)} \equiv m_1 + m_2 + ... + m_k \pmod{M} \tag{5.14}$$

Khi nhân 2 vế của (5.10) với t_i ta được

$$m_1^{1+\varphi(t_1)} + m_2^{2+\varphi(t_2)} + ... + m_k^{1+\varphi(t_k)} \equiv m_1 + m_2 + ... + m_k \pmod{M} \tag{5.15}$$

$$\Rightarrow t_i^{1+\varphi(m_i)} \equiv t_i \pmod{M}, i = \overline{1,k} \tag{5.16}$$

Cộng từng vế của k đồng dư dạng (5.16) ta được kết quả sau

Định lý 5.8– *Với các giả thiết như định lý 5.3 ta có:*

$$t_1^{1+\varphi(m_1)} + t_2^{1+\varphi(m_2)} + ... + t_k^{1+\varphi(m_k)} \equiv t_1 + t_2 + ... + t_k \pmod{M} \tag{5.17}$$

Chú ý rằng $t_i.t_j \equiv 0 \pmod{M}$ nên khi nâng lên lũy thừa bậc n của tổng $t_1 + t_2 + ... + t_k$ ta có kết quả sau.

Định lý 5.9– *Với các giả thiết như định lý 5.3 ta có:*

$$t_1^n + t_2^n + ... + t_k^n \equiv (t_1 + t_2 + ... + t_k)^n \pmod{M} \tag{5.18}$$

Khả năng tìm ra các hệ thức đồng dư mới chưa phải đã hết mời bạn đọc nghiên cứu thêm. Để nắm rõ được những phần trên ta tìm hiểu qua một số ví dụ sau đây.

Ví dụ 5.10. *Tìm ít nhất bốn nghiệm của phương trình đồng dư:*

$$x^3 + y^7 \equiv 1 \pmod{30} \tag{5.19}$$

Lời giải. Do $30 = 5.6$ và $(6;5) = 1$ nên theo (5.4) có $5^{\varphi(6)} + 6^{\varphi(5)} \equiv 1 \pmod{30}$
vì $\varphi(6) = \varphi(2).\varphi(3) = 2$ và $\varphi(5) = 4; 6^2 \equiv 6 \pmod{30}$.
Tương tự ta có: $25^7 \equiv 25 \pmod{30}$ và $6^3 \equiv 6 \pmod{30}$ nên $6^3 + 25^7 \equiv 26 + 6 \equiv 1 \pmod{30}$
Nếu phân tích $30 = 3.10$ với $(3;10) = 1$ thì theo (5.4) có $3^{\varphi(10)} + 10^{\varphi(3)} \equiv 1 \pmod{30}$. Tính toán tương tự như trên ta có $3^4 + 10^2 \equiv 1 \pmod{30}$.
Vì $3^4 = 81 \equiv 21 \pmod{30}$ và $10^2 \equiv 10 \pmod{30}$ nên theo (5.8) có $(3^4)^3 + (10^2)^7 \equiv 1 \pmod{30}$ và $(3^4)^7 + (10^2)^3 \equiv 1 \pmod{30}$
Suy ra phương trình trên có ít nhất bốn nghiệm $(x;y)$ là $(25;6)$; $(6;25)$; $(21;10)$; $(10;21)$. ■

Ví dụ 5.11. *Chứng minh rằng phương trình đồng dư sau có nghiệm $(x;y;z;t)$ khác $(0;0;0;0)$:*

$$x^4 + y^4 + z^4 + t^4 \equiv t^3 \pmod{60}.$$

Lời giải. $60 = 3.4.5$ và $(5;3) = 1; (5;4) = 1; (3;4) = 1$ nên đặt $m_1 = 3; m_2 = 4; m_3 = 5; t_1 = 15; t_2 = 1; t_3 = 20$ theo (5.18)

$$15^4 + 12^4 + 20^4 \equiv (15 + 20 + 12)^4 \equiv 1 \pmod{60}$$

Ví dụ 5.12. *Tìm ít nhất một nghiệm của phương trình đồng dư $x^{17} + y^{19} \equiv 1 \pmod{35}$* △

Lời giải. Ta có: $35 = 5.7$ mà $(5;7) = 1$ nên theo (5.4): $5^{\varphi^7} + 7^{\varphi^5} \equiv 1 \pmod{35}$)
Vì $\varphi(5) = 4; \varphi(7) = 6$ nên $5^4 + 7^6 \equiv 1 \pmod{35}$
Theo (5.8): $14^{17} + 30^{19} \equiv 14 + 30 \equiv 1 \pmod{35}$
Vậy phương trình đồng dư có ít nhất một nghiệm $(x;y) = (14;30)$ ■

5.7 Bài tập

Bài 1. Chứng minh rằng phương trình đồng dư sau có nghiệm $(x; y; z; t)$ khác $(0; 0; 0; 0)$:

a) $x^3 + y^3 + z^3 \equiv t^3 \pmod{210}$

b) $x^5 + y^5 + z^5 \equiv t^5 \pmod{1155}$

Bài 2. Tìm ít nhất một nghiệm của phương trình đồng dư sau:

$$x^{11} + y^{13} \equiv 1 \pmod{45}$$

Bài 3. Chứng tỏ rằng mỗi phương trình sau có nghiệm nguyên dương.

a) $2^x + 3^y + 5^z + 7^t \equiv 3 \pmod{210}$

b) $3^x + 5^y + 7^z \equiv 2 \pmod{105}$

Chương

6 Hệ thặng dư và định lý Thặng dư Trung Hoa

Nguyễn Đình Tùng (TUNGC3SP)

Bài viết này trình bày về Hệ thặng dư và định lý Thặng dư Trung Hoa. Một số kí hiệu sử dụng được phác họa trong Phần 6.1. Phần 6.2 giới thiệu đến bạn đọc một số kiến thức cơ bản về Hệ thặng dư đầy đủ và Hệ thặng dư thu gọn kèm theo bài tập ứng dụng. Định lý Thặng dư Trung Hoa kèm ứng dụng của nó giúp giải quyết một số dạng toán được trình bày trong Phần 6.3. Phần 6.4 kết thúc bài viết bao gồm một số bài tập đề nghị kèm gợi ý hoặc đáp số.

6.1 Một số kí hiệu sử dụng trong bài viết

- $[x,y]$: bội chung nhỏ nhất của hai số nguyên dương x,y (nếu không nói gì thêm).
- (x,y) : ước chung lớn nhất của hai số nguyên x,y.
- $x \triangleq y \pmod p$: x không đồng dư với y theo module p.
- HĐĐ: hệ thặng dư đầy đủ.

- HTG: hệ thặng dư thu gọn.
- $\mathbb{P}$: tập các số nguyên tố.
- $\Phi(n)$: hàm Ơle của n.
- $|A|$: số phần tử của tập A.
- $\{x\}$: phần lẻ của số thực x, được xác định như sau: $\{x\} = x - [x]$, trong đó $[x]$ là phần nguyên của số thực x (là số nguyên lớn nhất không vượt quá x).
- $\prod_{i=1}^{n} p_i = p_1 p_2 ... p_n$

6.2 Hệ thặng dư

6.2.1 Kiến thức cơ bản

Hệ thặng dư đầy đủ

Định nghĩa 6.1 *Cho tập $A = \{a_1; a_2; ...; a_n\}$. Giả sử r_i, $0 \leq r_i \leq n-1$ là số dư khi chia $a_i$cho n. Nếu tập số dư $\{r_1; r_2; ...; r_n\}$ trùng với tập $\{0; 1; 2; ...; n-1\}$ thì ta nói A là một hệ thặng dư đầy đủ (gọi tắt là HĐD)* mod n.

Nhận xét. Từ định nghĩa, dễ thấy:

- ▷ Nếu $A = \{a_1; a_2; ...; a_n\}$ lập thành HĐD $\pmod n$ nếu và chỉ nếu: $i \neq j \Rightarrow a_i \neq a_j \pmod n$.
- ▷ Nếu $A = \{a_1; a_2; ...; a_n\}$ là HĐD $\pmod n$ thì từ định nghĩa dễ dàng suy ra:
  - Với mọi $m \in \mathbb{Z}$, tồn tại duy nhất $a_i \in A$ sao cho $a_i \equiv m \pmod n$.
  - Với mọi $a \in \mathbb{Z}$, tập $a + A = \{a + a_1; a + a_2; ...; a + a_n\}$ là một HĐD $\pmod n$.

– Với mọi $c \in \mathbb{Z}$ và $(c;n) = 1$; tập $cA = \{ca_1; ca_2; ...; ca_n\}$ là một HĐD $\pmod n$.

Chú ý: tập $A^* = \{0; 1; 2; 3; ...; n-1\}$ là một HĐD $\pmod n$ không âm nhỏ nhất. Số phần tử của tập A là $|A| = n$.

Ví dụ 6.1. *Cho hai HĐD* $\pmod n$*:* $A = \{a_1; a_2; ...; a_n\}$ *và* $B = \{b_1; b_2; ...; b_n\}$.

a. Chứng minh rằng: Nếu n chẵn thì tập $A + B = \{a_1 + b_1; a_2 + b_2; ...; a_n + b_n\}$ *không hợp thành HĐD* $\pmod n$

b. Kết luận ở câu a. sẽ thế nào nếu n là số lẻ △

Lời giải. *a.* Ta có một điều kiện cần sau đây đối với HĐD $\pmod n$, khi n chẵn. Giả sử $C = \{c_1; c_2; ...; c_n\}$ là một HĐD $\pmod n$. Khi đó theo định nghĩa ta có:

$$c_1 + c_2 + ... + c_n \equiv (1 + 2 + ... + (n-1)) \equiv \frac{n(n+1)}{2} \pmod n$$

Do n chẵn nên $n = 2k$, suy ra:

$$\frac{n(n+1)}{2} = k(2k+1) \not\vdots n \Rightarrow k(2k+1) \triangleq 0 \pmod n$$

$$\Rightarrow c_1 + c_2 + ... + c_n \triangleq 0 \pmod n \tag{6.1}$$

Ta có:

$$\begin{aligned} A + B &= \{a_1 + b_1; a_2 + b_2; ...; a_n + b_n\} \\ &\equiv \{(a_1 + a_2 + ... + a_n) + (b_1 + b_2 + ... + b_n)\} \pmod n \\ &\equiv \left\{\frac{n(n+1)}{2} + \frac{n(n+1)}{2}\right\} \pmod n \\ &\equiv [n(n+1)] \pmod n \end{aligned}$$

$$\Rightarrow A + B \equiv 0 \pmod n \tag{6.2}$$

(Ở đây ta cũng sử dụng giả thiết A và B là hai HĐD mod n).

Từ (6.1) và (6.2) ta suy ra đpcm.

b. Xét khi n lẻ: Lúc này chưa thể kết luận gì về tính chất của hệ $A+B$.

Thật vậy, ta xét $n=3$; $A=\{1;2;3\}$; $B=\{4;5;6\}$.

Khi đó $A+B=\{5;7;9\}$ là một HĐĐ mod 3.

Nhưng, xét hệ $\overline{A}=\{1;2;3\}, \overline{B}=\{5;4;6\}$.

Khi đó $\overline{A}+\overline{B}=\{6;6;9\}$ không phải là một HĐĐ mod 3. ■

Hệ thặng dư thu gọn

Định nghĩa 6.2 *Cho tập $B=\{b_1;b_2;...;b_k\}$ là một tập hợp gồm k số nguyên và $(b_i;n)=1$ với mọi $i=1;2;...;k$.*
Giả sử: $b_i=q_in+r_i$ với $1\le r_i<n$. Khi đó dễ thấy $(r_i;n)=1$.
Nếu tập $\{r_1;r_2;...;r_n\}$ bằng tập K gồm tất cả các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n thì B được gọi là hệ thặng dư thu gọn mod n, gọi tắt là HTG $\pmod n$. △

Nhận xét. Ta có thể rút ra hai nhận xét:

▷ Dễ thấy tập $B=\{b_1;b_2;...;b_k\}$ gồm k số nguyên lập thành một HTG khi và chỉ khi

i. $(b_i;n)=1$

ii. $b_i\not\equiv b_j \pmod n$ với $1\le i\ne j\le k$

iii. $|B|=\Phi(n)$

Điều kiện (iii) tương đương với (iii'): với mọi $x\in\mathbb{Z};(x;n)=1$ tồn tại duy nhất $b_i\in B$ sao cho $x\equiv b_i \pmod n$.

▷ Từ định nghĩa ta suy ra: cho tập $B=\{b_1;b_2;...;b_k\}$ là HTG mod n và $c\in\mathbb{Z};(c;n)=1$ thì tập $cB=\{cb_1;cb_2;...;cb_n\}$ cũng là HTG mod n.

Ví dụ 6.2. *Cho hai số nguyên dương m, n với $(m;n)=1$. Giả sử $A=\{a_1,a_2,...,a_h\}; B=\{b_1,b_2,...,b_k\}$ tương ứng là các hệ thu gọn mod m và mod n. Xét tập hợp $C=\{a_in+b_jm\}; 1\le i\le h; 1\le j\le k$.. Chứng minh rằng C là một hệ thu gọn HTG mod mn.* △

Lời giải. + Ta chứng minh $(a_in+b_jm, mn)=1\ \forall i=\overline{1,h};\ j=\overline{1,k}$ (điều kiện (i)).

Giả sử tồn tại i,j và số nguyên tố p là ước chung của a_in+b_jm và mn.

Ta có $a_in+b_jm\vdots p$ và $mn\vdots p$.

Do $mn\vdots p$ mà $(m,n)=1$ nên có thể giả sử $n\vdots p$, suy ra

$$a_in\vdots p\Rightarrow b_jm\vdots p\Rightarrow b_j\vdots p$$

Vậy p là ước nguyên tố chung của n và b_j. Điều này mâu thuẫn với giả thiết. Nên điều giả sử là sai. Vậy $(a_in+b_jm, mn)=1\ \forall i=\overline{1,h};\ j=\overline{1,k}$.

+ Chứng minh điều kiện (ii).

Giả sử tồn tại $a\in A;\ b\in B$ sao cho $an+bm\equiv a'n+b'm \pmod{mn}$

$$\Rightarrow an\equiv a'n \pmod m\Rightarrow a\equiv a' \pmod m \text{ (do } (m,n)=1)$$

(điều này mâu thuẫn).

Vậy $an+bm\triangleq a'n+b'm \pmod{mn}$.

+ Chứng minh điều kiện (iii').

Giả sử $(x,mn)=1\Rightarrow (x,m)=1; (x,n)=1$.

Vì $(m,n)=1$ nên tập $B=\{mb_1,mb_2,...,mb_k\}$ là một HTG mod n.

Vậy tồn tại duy nhất $b\in B$ để $x\equiv mb \pmod n$.

Tương tự, tồn tại duy nhất $a \in A$ để $x \equiv na \pmod{m}$.

Từ đó suy ra $x \equiv na + mb \pmod{n}$ và $x \equiv na + mb \pmod{m}$. Từ đó kết hợp với $(m, n) = 1$ suy ra $x \equiv na + mb \pmod{mn}$. ■

Nhận xét. Từ đây, ta có thể suy ra công thức tính hàm Ơle $\Phi(n)$.

6.2.2 Ứng dụng

Trong các bài toán về đa thức, dãy số

Ví dụ 6.3. *[THTT, số 340] Cho p là số nguyên tố lẻ và đa thức $Q(x) = (p-1)x^p - x - 1$. Chứng minh rằng tồn tại vô hạn số nguyên dương a sao cho $Q(a)$ chia hết cho p^p.* △

Lời giải. Thay cho việc chứng minh tồn tại vô hạn số nguyên dương a sao cho $Q(a)$ chia hết cho p^p, ta sẽ chứng minh tập

$$H = \{Q(1); Q(2); ...; Q(p^p)\}$$

là một HĐĐ mod p^p.
Ta có nhận xét sau: trong tập số $\{1; 2; ...; p^p\}$ gồm p^p số, giả sử có hai số u, v khác nhau thì $Q(u) \triangleq Q(v) \pmod{p^p}$.
Ta chứng minh điều này bằng phản chứng. Giả sử có $Q(u) \equiv Q(v) \pmod{p^p}$

$$\Leftrightarrow (p-1)u^p - u - 1 \equiv (p-1)v^p - v - 1 \pmod{p^p}$$

$$\Leftrightarrow (p-1)(u^p - v^p) - (u - v) \equiv 0 \pmod{p} \tag{6.3}$$

Theo định lí Ferma nhỏ thì $u^p \equiv u \pmod{p}$ và $v^p \equiv vp \pmod{p}$ với p là số nguyên tố nên $u^p - v^p \equiv u - v \pmod{p}$.
Từ (6.3) suy ra

$$(p-2)(u-v) \equiv 0 \pmod{p} \Rightarrow u \equiv v \pmod{p} \tag{6.4}$$

Cũng từ (6.3) ta có:

$$(u-v)((p-1)(u^{p-1} + u^{p-2}v + ... + uv^{p-2} + v^{p-1}) - 1) \equiv 0 \pmod{p^p}$$

Kết hợp với (6.4) suy ra

$$(u-v)((p-1).p.u^{p-1}-1) \equiv 0 \pmod{p^p} \Rightarrow u-v \equiv 0 \pmod{p^p}$$

Điều này mâu thuẫn với giả sử $u \triangleq v \pmod{p^p}$. Vậy nhận xét được chứng minh.

- Từ nhận xét trên suy ra $H = \{Q(1); Q(2); ...; Q(p^p)\}$ là một HĐĐ mod p^p. Từ đó suy ra trong tập số $\{1; 2; ...; p^p\}$ gồm p^p số thì tồn tại duy nhất một số a sao cho $Q(a) \equiv 0 \pmod{p^p}$ hay $Q(a) \vdots p^p$.
- Ta xét dãy số hạng $a_k = a + k.p^p$ với $k = 0, 1, 2...$, dễ thấy rằng:

$$Q(a^p) \equiv Q(a) \equiv 0 \pmod{p^p}.$$

Nghĩa là tồn tại vô hạn số a_k $(k = 0, 1, 2, ...)$ thỏa mãn $Q(a_k) \vdots p^p$. ■

Ví dụ 6.4. *Cho đa thức $P(x) = x^3 - 11x^2 - 87x + m$. Chứng minh rằng với mọi số nguyên m, tồn tại số nguyên n sao cho $P(n)$ chia hết cho 191.* △

Lời giải. Ý tưởng cũng tương tự Ví dụ 6.3, ta sẽ sử dụng HĐĐ. Trước hết ta đưa ra bổ đề sau:

Bổ đề 6.1– *Cho p là số nguyên tố, $p \equiv 2 \pmod 3$. Khi đó,với mọi số nguyên x, y mà $x^3 \equiv y^3 \pmod p \Rightarrow x \equiv y \pmod p$* □

Chứng minh. Thật vậy:

- Nếu $x \equiv 0 \pmod p \Rightarrow y^3 \equiv 0 \pmod p \Rightarrow y \equiv 0 \pmod p \Leftrightarrow x \equiv y (\mathrm{mod} p)$
- Nếu x, y cùng không chia hết cho p, do $p \equiv 2(\mathrm{mod} 3) \Rightarrow p = 3k + 2 (k \in \mathbb{Z})$.

Theo định lí Ferma:

$$x^{p-1} = x^{3k+1} \equiv 1 \pmod{p}$$
$$y^{p-1} = y^{3k+1} \equiv 1 \pmod{p}$$
$$\Rightarrow x^{3k+1} \equiv y^{3k+1} \pmod{p} \quad (6.5)$$

Mà theo giả thiết, $x^3 \equiv y^3 \bmod p \Rightarrow x^{3k} \equiv y^{3k} \pmod{p}$.

Từ đó suy ra $x \equiv y \pmod{p}$. Vậy bổ đề được chứng minh. ■

Trở lại bài toán, ta sẽ chứng minh $P(n_1) \equiv P(n_2) \pmod{191}$ với $n_1; n_2 \in \mathbb{Z}$ thì $n_1 \equiv n_2 \pmod{191}$.
Thật vậy, vì

$$27P(n_1) = (3n_1 - 11)^3 - 11.191.n_1 + 11^3 + 27m$$
$$27P(n_2) = (3n_2 - 11)^3 - 11.191.n_2 + 11^3 + 27m$$

nên

$$\begin{aligned}
& P(n_1) \equiv P(n_2) && \pmod{191} \\
\Leftrightarrow & 27P(n_1) \equiv 27P(n_2) && \pmod{191} \\
\Leftrightarrow & (3n_1 - 11)^3 \equiv (3n_2 - 11)^3 && \pmod{191} \\
\Leftrightarrow & 3n_1 - 11 \equiv 3n_2 - 11 && \pmod{191} \text{(suy ra từ bổ đề)} \\
\Leftrightarrow & n_1 \equiv n_2 && \pmod{191}
\end{aligned}$$

Với mọi $n_1, n_2 \in A = \{1; 2; 3; ...; 1991\}$ (A là một HĐĐ mod 191), $n_1 \neq n_2$ ta có $P(n_1) \triangleq P(n_2) \pmod{191}$
$\Rightarrow A^* = \{P(1); P(2); ...; P(191)\}$ là một HĐĐ mod 191.
Từ đó suy ra $\exists n \in A = \{1; 2; 3; ...; 191\}$ sao cho

$$P(n) \equiv 191 \pmod{191} \Leftrightarrow P(n) \vdots 191$$

. ■

Ví dụ 6.5. *Cho p là một số nguyên tố. Chứng minh rằng với mọi số m nguyên không âm bất kì, luôn tồn tại một đa thức $Q(x)$ có hệ số nguyên sao cho p^m là ước chung lớn nhất của các số $a_n = (p+1)^n + Q(n);\ n = 1, 2, 3...$* △

Lời giải. Ta có bổ đề sau:

Bổ đề 6.2– $\forall k \in \mathbb{N}, k < m$ *thì tồn tại* $b_k \in \mathbb{Z}$ *sao cho* $b_k p^m + p^k \vdots k!$ □

Chứng minh. Giả sử $k! = p^{\alpha_k} M_k$ với $(M_k; p) = 1$.
Khi e chạy trong tập $\{0; 1; ...; M_k - 1\}$ thì các số $\left\{ep^{m-k}\right\}$ lập thành một HĐĐ modM_k, thành thử tồn tại $b_k \in \mathbb{Z}$ sao cho $b_k p^{m-k} \equiv -1 \pmod{M_k}$

$$\begin{aligned} &\Leftrightarrow \quad (b_k p^{m-k} + 1) \vdots M_k \\ &\Leftrightarrow \quad (b_k p^m + p^k) \vdots p^k . M_k \end{aligned}$$

Mặt khác

$$\alpha_k \sum_{i=1}^{\infty} \left[\frac{k}{p^i}\right] < \sum_{i=1}^{\infty} \frac{k}{p^i} < k$$

Vậy $(b_k p^m + p^k) \vdots p^{\alpha_k} . M_k = k!$. Bổ đề được chứng minh. ■

Trở về bài toán.
Đặt $f_i(x) = \dfrac{x(x-1)...(x-i+1)}{i!}$ thì $f_i(n) = \begin{cases} C_n^i \text{ (nếu } n \geq i) \\ 0 \text{ (nếu } n < i) \end{cases}$.
Đặt $R(x) = -\sum\limits_{i=0}^{m-1} f_i(x)(b_i p^m + p^i)$ thì theo Bổ đề 6.2, $R(x)$ là đa thức có hệ số nguyên.
Ta có:

$$u_n = (p+1)^n + R(n) = \sum_{i=0}^{n} C_n^i p^i - \sum_{i=1}^{m-1} f_i(n) p^i - p^m \sum_{i=0}^{m-1} f_i(n) b_i$$

$$\begin{aligned} &\equiv \quad \sum_{i=0}^{\infty} f_i(n) p^i - \sum_{i=1}^{m-1} f_i(n) p^i \pmod{p^m} \\ &\equiv \quad \sum_{i=0}^{\infty} f_i(n) p^i \equiv 0 \pmod{p^m} \ \forall n = 1, 2, 3... \end{aligned}$$

Đặc biệt $u_1 = (p+1) + R(1) = ep^m$

Ta chứng minh đa thức $Q(x) = R(x)+p^m(1-e)$ là đa thức cần tìm.Thật vậy,

$$a_n = (p+1)^n + Q(n) = (p+1)^n + R(n) + p^m(1-e)$$
$$= u_n + p^m(1-e) \vdots p^m,\ \forall n = 1,2,3... \quad (6.6)$$

Mặt khác

$$a_1 = (p+1) + Q(1) = p+1+R(1)+p^m(1-e) = ep^m + p^m(1-e) \vdots p^m$$

Do đó p^m là ƯCLN của a_n với mọi $n = 1,2,3...$ ■

Ví dụ 6.6. *Cho $p \geq 3$ là một số nguyên tố và $a_1, a_2, ..., a_{p-2}$ là một dãy các số nguyên dương sao cho p không là ước số của a_k và ${a_k}^k - 1$ với mọi $k = 1,2,3,...,p-2$. Chứng minh rằng tồn tại một số phần tử trong dãy $a_1, a_2, ..., a_{p-2}$ có tích đồng dư với 2 module p.* △

Lời giải. Ta có bổ đề sau:

Bổ đề 6.3– *Với mỗi số nguyên $k = 1,2,...,p-1$ tồn tại một tập các số nguyên $\{b_{k,1}, b_{k,2}, ..., b_{k,k}\}$ thỏa mãn hai điều kiện sau:*

1. *Mỗi $b_{k,j}$ hoặc bằng 1, hoặc bằng tích của một số phần tử trong dãy $a_1, a_2, ..., a_{p-2}$,*
2. *$b_{k,i} \triangleq b_{k,j} \pmod p$ với $1 \leq i \neq j \leq k$.* □

Chứng minh. Với k=2 chọn $b_{21} = 1; b_{22} = a_1 \triangleq 1 \pmod p$ (do $a_1^1 - 1$ không chia hết cho p).
Giả sử với $2 \leq k \leq p-2$ ta đã chọn được tập $\{b_{k,1}, b_{k,2}, ..., b_{k,k}\}$ thỏa mãn hai tính chất trên.
Vì $a_k \not\vdots p$ nên hai phần tử khác nhau bất kì trong tập

$$\{a_k b_{k,1}, a_k b_{k,2}, ..., a_k b_{k,k}\}$$

là phân biệt theo mod p.

$$a_k^k \triangleq 1 (\mathrm{mod} p) \Rightarrow (a_k b_{k,1})(a_k b_{k,2})...(a_k b_{k,k}) \triangleq b_{k,1} b_{k,2} ... b_{k,k} \pmod p$$

Từ hai điều trên suy ra tồn tại chỉ số $j(1 \leq j \leq k)$ sao cho $a_k b_{k,j} \notin \{b_{k,1}, b_{k,2}, ..., b_{k,k}\}$.
Xét tập $\{b_{k,1}, b_{k,2}, ..., b_{k,k}, a_k b_{k,j}\}$.
Sau khi đánh số lại các phần tử ta thu được tập

$$\{b_{k+1,1}, b_{k+1,2}, ..., b_{k+1,k}, b_{k+1,k+1}\}$$

. Ta thấy tập này có $k+1$ phần tử thỏa mãn hai tính chất trên nên theo nguyên lí quy nạp, bổ đề được chứng minh. ■

Quay lại bài toán, áp dụng bổ đề 6.3, xét tập $\{b_{p-1,1}, b_{p-1,2}, ..., b_{p-1,p-1}\}$, ta thấy tập này là một HTG mod p nên nó chứa đúng một phần tử đồng dư với 2 mod p. Vì phần tử này khác 1 nên nó phải đồng dư với tích của một số a_k. Suy ra đpcm. ■

Trong tập con tập số nguyên dương, bài toán số học chia hết

Ví dụ 6.7. *Cho $p > 3$ là số nguyên tố có dạng $3k+2$.*

a. Chứng minh rằng tập $A = \{2^3 - 1; 3^3 - 1; 4^3 - 1; ...; p^3 - 1\}$ là HTG mod p.

b. Chứng minh rằng $\prod_{i=1}^{p} (i^2 + i + 3) \equiv 3 (\text{mod} p)$. △

Lời giải. *a.* Ta sẽ chứng minh tập A thỏa mãn 3 điều kiện đã nêu ở Định nghĩa 6.2.

- Hiển nhiên mỗi phần tử của A đều không chia hết cho p (thỏa mãn điều kiện (i)).
- Giả sử tồn tại $1 \leq i < j \leq p-1$ sao cho

$$\begin{aligned} & i^3 - 1 \equiv j^3 - 1 \pmod{p} \\ \Rightarrow\ & i^3 \equiv j^3 \pmod{p} \\ \Rightarrow\ & i^{3k} \equiv j^{3k} \pmod{p} \end{aligned}$$

Mặt khác, theo định lí Ferma, ta có: $i^{3k+1} \equiv j^{3k+1} \pmod{p}$
Từ đó suy ra $i \equiv j \pmod{p} \Rightarrow i = j$ (mâu thuẫn). Vậy A thỏa mãn điều kiện (ii).

- Vì $\Phi(p) = p - 1 = |A|$ nên điều kiện (iii) thỏa mãn. ■

Vậy A là một HTG mod p.

b. Vì $B = \{1; 2; 3; ...; p-1\}$ là một HTG mod p. Mà A cũng là một HTG mod p (theo phần a.) nên ta có:

$$\begin{aligned} & \prod_{i=2}^{p} (i^3 - 1) \equiv (p-1)! \pmod{p} \\ \Leftrightarrow \quad & \prod_{i=2}^{p} (i^2 + i + 1) \equiv 1 \pmod{p} \\ \Leftrightarrow \quad & \prod_{i=1}^{p} (i^2 + i + 1) \equiv 3 \pmod{p} \end{aligned}$$

Nhận xét. Ta có thể mở rộng Ví dụ 6.7 như sau:

Ví dụ 6.8. *Cho p là số nguyên tố lẻ có dạng $mk + 2$ (m, k là các số nguyên dương, $m > 2$). Tìm số dư của phép chia*

$$T = \prod_{t=1}^{p} (t^{m-1} + t^{m-2} + ... + t + 1)$$

cho p. △

Ví dụ 6.9. *Chứng minh rằng với mọi số nguyên dương n, tồn tại số tự nhiên n gồm n chữ số đều lẻ và nó chia hết cho $5n$.* △

Lời giải. Xét số $x_n = \overline{a_1 a_2 ... a_n} = 5^n.a$ thỏa mãn (với $a_i \in \mathbb{Z}^+$ lẻ với mọi $i = 1, 2, ..., n$ và $a \in \mathbb{Z}^+$)

Ta sẽ chứng minh bài toán bằng phương pháp quy nạp toán học.

Với $n = 1 \Rightarrow \exists a_1 = 5 \vdots 5^1$. Vậy mệnh đề đúng với $n = 1$.

Giả sử mệnh đề đúng với n $\Leftrightarrow x_n = \overline{a_1 a_2 ... a_n} = 5^n.a$, cần chứng minh mệnh đề đúng với $n + 1$.

Xét 5 số sau đây:

$$\begin{aligned} a_1 &= \overline{1 a_1 a_2 ... a_n} = 5^n (1.2^n + a) \\ a_2 &= \overline{3 a_1 a_2 ... a_n} = 5^n (3.2^n + a) \\ a_3 &= \overline{5 a_1 a_2 ... a_n} = 5^n (5.2^n + a) \\ a_4 &= \overline{7 a_1 a_2 ... a_n} = 5^n (7.2^n + a) \\ a_5 &= \overline{9 a_1 a_2 ... a_n} = 5^n (9.2^n + a) \end{aligned}$$

Do $B = \{1, 3, 5, 7, 9\}$ là một HDĐ mod 5 cho nên

$$B^* = \{1.2^n + 1; 3.2^n + a; 5.2^n + a; 7.2^n + a; 9.2^n + a\}$$

cũng là HDĐ mod 5 nên tồn tại duy nhất một số trong $B*$ chia hết cho 5.
$\Rightarrow$ Trong 5 số $a_1; a_2; a_3; a_4; a_5$ có duy nhất một số chia hết cho $5(n+1)$ mà số này gồm $n+1$ chữ số lẻ. Vậy mệnh đề đúng với $n+1$.
Theo nguyên lí quy nạp, mệnh đề đúng với mọi n nguyên dương. Vậy với mọi số nguyên dương n, luôn tồn tại một số tự nhiên gồm n chữ số đều lẻ và chia hết cho $5n$. ■

Trong một số dạng toán Số học khác

Ngoài các ứng dụng nêu trên, hệ thặng dư còn được dùng trong nhiều dạng toán số học khác, đơn biểu như trong các bài toán liên quan tới tính tổng, giải phương trình nghiệm nguyên (phương trình Diophant bậc nhất). Sau đây xin nêu ra một số ví dụ.

Ví dụ 6.10. *Với mỗi cặp số nguyên tố cùng nhau (p,q), đặt*

$$S = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + ... + \left[\frac{(p-1)q}{p}\right]$$

a. Chứng minh rằng: $S = \dfrac{(p-1)(q-1)}{2}$

b. Xác định giá trị của p, q *để* S *là số nguyên tố* △

Lời giải. *a.* Ta có $\left\{\dfrac{kq}{p}\right\} = \dfrac{r_k}{q}$, ở đây r_k là số dư trong phép chia q cho p $(0 \le r_k \le p-1)$.

Ta có:

$$S = \frac{q}{p} + \frac{2q}{p} + ... + \frac{(p-1)q}{p} - \left(\frac{r_1}{p} + \frac{r_2}{p} + ... + \frac{r_{p-1}}{p}\right)$$

Vì $(p,q) = 1 \Rightarrow r_k \neq 0 \ \forall \ k = 1, 2, ..., p-1$, từ đó ta thấy tập $A = \{r_1; r_2; ...; r_{p-1}\}$ chính là một hoán vị của tập $A = \{1; 2; ...; p-1\}$.

Thật vậy, ngược lại, giả sử $\exists\ i,j \in \{1;2;...;p-1\}, i<j$ mà $r_i = r_j$

$$\Rightarrow \begin{cases} 1 \le j-i \le p-2 \\ (j-i)q \vdots p \end{cases} \Leftrightarrow \begin{cases} \le j-i \le p-2 \\ j-i \vdots p \end{cases} \text{ (vô lý)}$$

Ta có:

$$\frac{r_1}{p}+\frac{r_2}{p}+...+\frac{r_{p-1}}{p} = \frac{1+2+...+p-1}{p} = \frac{p-1}{2}$$

$$\Rightarrow S = \frac{(p-1)(q-1)}{2} \quad (6.7)$$

b. Từ (6.7) suy ra để S là số nguyên tố cần có $p,q>1$ và ít nhất một trong hai số p,q lẻ.

- Trường hợp 1: p,q cùng lẻ $\Rightarrow p,q \ge 3, p \ne q$ (do (p,q)=1), kết hợp với (6.7) $\Rightarrow S$ là số chẵn lớn hơn 2 $\Rightarrow S$ không phải là số nguyên tố.
- Trường hợp 2: p là số chẵn, q là số lẻ

$$S \in \mathbb{P} \Leftrightarrow \left[\begin{array}{l} \begin{cases} (p,q)=1 \\ p-1=1 \\ \dfrac{q-1}{2} \in \mathbb{P} \end{cases} \\ \begin{cases} (p,q)=1 \\ p-1 \in P \\ \dfrac{q-1}{2}=1 \end{cases} \end{array}\right.$$

$$\Leftrightarrow \left[\begin{array}{l} \begin{cases} p=2 \\ q=2h+1\ (h \in \mathbb{P}) \end{cases} \\ \begin{cases} q=3 \\ p=t+1\ (t \in P,\ t \triangleq 2 \pmod 3) \end{cases} \end{array}\right. \quad (6.8)$$

- Trường hợp 3: q là số chẵn, p là số lẻ. Tương tự trường hợp 2, ta có:

$$\left[\begin{array}{l} \begin{cases} p = 2m+1 (m \in \mathbb{P}) \\ q = 2 \end{cases} \\ \begin{cases} p = 3 \\ q = n+1 (n \in \mathbb{P}, n \triangleq 2 \pmod 3) \end{cases} \end{array}\right. \tag{6.9}$$

Từ (6.8) và (6.9) ta có các cặp số p, q cần tìm. ■

Ví dụ 6.11. *Cho a, b, c là các số nguyên dương thỏa mãn $a \le b \le c$ và $(a, b, c) = 1$. Chứng minh rằng nếu $n > ac + b$ thì phương trình $n = ax + by + cz$ có nghiệm nguyên dương.* △

Lời giải. Gọi $(a, c) = d \Rightarrow (b, d) = 1 \Rightarrow A = \{bi\}_{i=1}^{d}$ là HĐĐ mod d

$\Rightarrow \exists\, y \in \{1, 2, ..., d\}$ sao cho $by \equiv n \pmod d \Leftrightarrow (n - by) \vdots d$.
Do $(a, c) = d \Rightarrow a = a_1 d$; $c = c_1 d$ $(a_1, c_1 \in Z^+;\ (a_1, c_2) = 1) \Rightarrow B = \{a_1 j\}_{j=1}^{c_1}$ là HĐĐ mod c_1.

$\Rightarrow \exists x \in \{1, 2, ..., c_1\}$ sao cho $a_1 x \equiv \dfrac{n - by}{d} \pmod{c_1} \Rightarrow \exists z \in \mathbb{Z}$ sao cho $\dfrac{n - by}{d} = a_1 x + c_1 z$.
Mặt khác, ta có:

$$\frac{n - by}{d} > \frac{ac + b - by}{d} = (d-1)\frac{ca_1 - b}{d} + a_1 c_1 \ge a_1 c_1 \ge a_1 x \Rightarrow z \in \mathbb{Z}^+$$

Từ đây suy ra $n - by = ax + cz \Leftrightarrow n = ax + by + cz$.
Vậy nếu $n > ac + b$ thì phương trình $n = ax + by + cz$ có nghiệm nguyên dương. ■

6.3 Định lí thặng dư Trung Hoa

6.3.1 Kiến thức cơ bản

Định lý 6.1– *Cho k số nguyên dương $n_1, n_2, ..., n_k$ đôi một nguên tố cùng nhau và k số nguyên bất kì $a_1, a_2, ..., a_k$. Khi đó tồn tại số nguyên a thỏa mãn $a \equiv a_i \pmod{n_i}, \forall i = \overline{1, k}$.*

Số nguyên b thỏa mãn $b \equiv a_i \pmod{n_i}, \forall i = \overline{1,k}$ khi và chỉ khi $b \equiv a \pmod{n}$ với $n = n_1 n_2 ... n_k$. □

Lời giải. • Đặt $n = n_1 n_2 ... n_k$ và đặt $N_i = \dfrac{n}{n_i}$.

Do $(n_i, n_j) = 1, \forall i \neq j$ nên suy ra $(N_i, n_i) = 1 \ \forall i = \overline{1;k}$.

Do $(N_i, n_i) = 1, \forall i = \overline{1;k}$ nên với mỗi $i (1 \leq i \leq k)$ tồn tại b_i sao cho

$$N_i b_i \equiv 1 \pmod{n_i} \tag{6.10}$$

Như vậy ta có bộ $b_1, b_2, ..., b_k$. Do $N_j \equiv 0 \pmod{n_i}$ khi $i \neq j$, từ đó dĩ nhiên suy ra

$$N_j b_j \equiv 0 \pmod{n_i} \tag{6.11}$$

Đặt $a = \sum_{j=1}^{k} N_j b_j a_j$.

Với mỗi $i \ (1 \leq i \leq k)$ ta có

$$a = N_i b_i a_i + \sum_{j=1; j \neq i}^{k} N_j b_j a_j \tag{6.12}$$

Từ (6.10),(6.11),(6.12) suy ra $a \equiv a_i \pmod{n_i}, \forall i = \overline{1,k}$.

• Dễ thấy, vì $n_1, n_2, ..., n_k$ đôi một nguyên tố cùng nhau nên ta có kết luận sau: Số nguyên b thỏa mãn $b \equiv a_i \pmod{n_i}, \forall i = \overline{1,k}$ khi và chỉ khi $b \equiv a \pmod{n}$ với $n = n_1 n_2 ... n_k$. ■

Nhận xét. 1. Ngoài cách chứng minh trên, ta còn có thể sử dụng phép quy nạp để chứng minh định lí thặng dư Trung Hoa.

2. Định lí Thặng dư Trung Hoa khẳng định về sự tồn tại duy nhất của một lớp thặng dư các số nguyên thỏa mãn đồng thời nhiều đồng dư tuyến tính. Do đó có thể dùng định lí để giải quyết những bài toán về sự tồn tại và đếm các số nguyên thỏa mãn một hệ các

điều kiện quan hệ, chia hết,..., hay đếm số nghiệm của phương trình đồng dư. Việc sử dụng hợp lý các bộ và (trong định lý) cho ta rất nhiều kết quả thú vị và từ đó có thể đưa ra nhiều bài toán hay và khó.

Ví dụ 6.12. *Cho $m_1, m_2, ..., m_n$ là các số nguyên dương, $r_1, r_2, ..., r_n$ là các số nguyên bất kì. Chứng minh rằng điều kiện cần và đủ để hệ phương trình đồng dư*

$$\begin{aligned} x &\equiv r_1 \pmod{m_1} \\ x &\equiv r_2 \pmod{m_2} \\ &... \\ x &\equiv r_n \pmod{m_n} \end{aligned}$$

có nghiệm là $r_i \equiv r_j \pmod{GCD\,(m_i, m_j)};\ \forall 1 \le i < j \le n.$

Nếu x_0 và x_1 là hai nghiệm thỏa mãn hệ phương trình trên thì $x_0 \equiv x_1 \pmod{m}$ với $m = LCM(m_1, m_2, ..., m_n)$. Tức là hệ phương trình đã cho có nghiệm duy nhất theo module m. △

Lời giải. Trước hết ta giả sử hệ phương trình đã cho có nghiệm x_0. Đặt $GCD\,(m_i, m_j) = d$, ta có:

$$\begin{aligned} x_o - r_i &\equiv 0 \pmod{m_i} \\ x_o - r_j &\equiv 0 \pmod{m_j} \end{aligned}$$

Suy ra $r_i \equiv r_j \bmod (GCD\,(m_i, m_j))$. Do i, j tùy chọn nên $r_i \equiv r_j \pmod{GCD(m_i, m_j)}, \forall 1 \le i < j \le n$. Đây là điều kiện cần để hệ phương trình có nghiệm.

Ngược lại, ta sẽ chứng minh bằng quy nạp theo n rằng nếu điều kiện trên được thỏa mãn thì hệ phương trình luôn có nghiệm duy nhất theo module m với $m = LCM\,(m_1, m_2, ..., m_n)$.

Với trường hợp $n = 2$, đặt $GCD\,(m_1, m_2) = d \Rightarrow m_1 = dd_1;\ m_2 = dd_2$ với $GCD\,(d_1, d_2) = 1$.

Suy ra $r_i \equiv r_j \equiv r \pmod{d}$. Đặt $r_1 = r + k_1 d;\ r_2 = r + k_2 d$.

Ta có:

$$\left\{\begin{array}{ll} x\equiv r_1 & (\text{mod } m_1)\\ x\equiv r_2 & (\text{mod } m_2)\end{array}\right. \Leftrightarrow \left\{\begin{array}{l} (x-r)-k_1d\vdots dd_1\\ (x-r)-k_2d\vdots dd_2\end{array}\right.$$

$$\Leftrightarrow \left\{\begin{array}{ll} \dfrac{x-r}{d}\equiv k_2 & (\text{mod } d_1)\\ \dfrac{x-r}{d}\equiv k_2 & (\text{mod } d_2)\end{array}\right. \tag{6.13}$$

Do $(d_1,d_2)=1$ nên theo định lí Thặng dư Trung Hoa, tồn tại một số dương $\overline{x}$ sao cho $\overline{x}\equiv k_1 \pmod{d_1}$; $\overline{x}\equiv k_2 \pmod{d_2}$. Vì $\overline{x}$ và $\dfrac{x-r}{d}$ là hai nghiệm của phương trình $\left\{\begin{array}{ll} x\equiv k_1 & (\text{mod } d_1)\\ x\equiv k_2 & (\text{mod } d_2)\end{array}\right.$ nên $\dfrac{x-r}{d}\equiv \overline{x}$ (mod d_1d_2) hay $x\equiv \overline{x}d+r \pmod{dd_1d_2}$.
Do $m=LCM\,(m_1,m_2)=dd_1d_2$ nên theo định lí Thặng dư Trung Hoa, hệ có nghiệm duy nhất module m.
Giả sử định lí đúng đến $n-1$. Ta sẽ chứng minh định lí đúng đến n.
Đặt $m_1^{'}=LCM\,(m_1,m_2,...,m_{n-1})$; $m_2'=m_n$; $r_2'=r_n$. Vì $r_i\equiv r_j(\text{mod}GCD\,(m_i,m_j))$ với mọi $1\le i<j\le n$ nên theo giả thiết quy nạp, hệ phương trình $\left\{\begin{array}{l} x\equiv r_i \pmod{m_i}\\ i=\overline{1,n-1}\end{array}\right.$ có duy nhất nghiệm $x\equiv r_1'$ (mod m_1').
Mặt khác từ $r_i\equiv r_j(\text{mod } GCD(m_i,m_j))$ với mọi $1\le i<j\le n$ suy ra $r_1^{'}\equiv r_2^{'} \pmod{GCD(m_1',m_2^{'})}$.
Theo chứng minh trên cho trường hợp $n=2$ ta có hệ phương trình $\left\{\begin{array}{ll} x\equiv r_1' & (\text{mod } m_1')\\ x\equiv r_2' & (\text{mod } m_2')\end{array}\right.$ có nghiệm duy nhất theo module

$$m=LCM\left(m_1',m_2'\right)=LCM\,(m_1,m_2,...,m_n)$$

. Theo nguyên lí quy nạp ta có điều phải chứng minh. ■

Nhận xét. Đây chính là định lí Thặng dư Trung Hoa dạng mở rộng, nó hoàn toàn chứng minh dựa trên cơ sở định lí Thặng dư Trung Hoa. Trong bài viết này, ta sẽ không đi sâu vào tìm hiểu định lí dạng mở rộng mà chỉ đi sâu vào các ứng dụng của định lí Thặng dư Trung Hoa (dạng thường).

6.3.2 Ứng dụng

Trong Lý thuyết số

Ví dụ 6.13. *Chứng minh rằng với mỗi số tự nhiên n, tồn tại n số tự nhiên liên tiếp mà mỗi số trong n số đó đều là hợp số.* △

Lời giải. Ý tưởng: ta sẽ tạo ra một hệ phương trình đồng dư gồm n phương trình đồng dư. Dựa vào định lí thặng dư Trung Hoa, ta kết luận được sự tồn tại nghiệm của hệ đó.
Giả sử $p_1, p_2, ..., p_n$ là n số nguyên tố khác nhau từng đôi một.
Xét hệ phương trình đồng dư $x \equiv -k \pmod{p_k^2} (k = 1, 2, ..., n)$.
Theo định lí thặng dư Trung Hoa, tồn tại $x_0 \in \mathbb{N}^*$ sao cho $x_0 \equiv -k \pmod{p_k^2}, \forall k = 1, 2, ..., n$.
Khi đó các số $x_0 + 1; x_0 + 2, ...; x_0 + n$ đều là hợp số.(đpcm) ■

Ví dụ 6.14. *Chứng minh rằng với mọi số tự nhiên n, tồn tại n số tự nhiên liên tiếp sao cho bất kì số nào trong các số đó cũng đều không phải lũy thừa (với số mũ nguyên dương) của một số nguyên tố.* △

Nhận xét. Bài này cũng gần tương tự với ý tưởng của bài toán ở ví dụ củng cố. Tuy nhiên việc tìm ra hệ phương trình đồng dư khó hơn một chút.

Lời giải. Với mỗi số tự nhiên n, xét n số nguyên tố khác nhau từng đôi một $p_1, p_2, ..., p_n$.
Theo định lí Thặng dư Trung Hoa, tồn tại $a \in \mathbb{N}^*$ sao cho $a \equiv p_k - k \pmod{p_k^2}$ $(k = 1, 2, ..., n)$.
Khi đó dễ thấy rằng các số $a + 1, a + 2, ..., a + n$ đều không phải lũy thừa với số mũ nguyên dương của một số nguyên tố (đpcm). ■

Ví dụ 6.15. *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.* △

Lời giải. Xét dãy $F_n = 2^{2^n} + 1, (n = 0, 1, 2, ...)$. Dễ chứng minh bổ đề sau:

Bổ đề 6.4– *Nếu $n \neq m$ thì $(F_n, F_m) = 1$.* □

Áp dụng định lí Thặng dư Trung Hoa cho n số nguyên tố cùng nhau $F_1^s, F_2^s, ..., F_n^s$ và n số $r_i = -i (i = 1, 2, .., n)$ ta có tồn tại số nguyên c sao cho $c + i \vdots F_i^s$.
Vậy dãy $\{c + i\}_{i=1}^n$ là n số nguyên dương liên tiếp, số hạng thứ i chia hết cho F_i^s. ■

Ví dụ 6.16. *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 $P(x)$ chia hết cho n.* △

Lời giải. Ta có thể xét đa thức $P(x) = (3x + 1)(2x + 1)$.
Với mỗi số nguyên dương n, ta biểu diễn n dưới dạng $n = 2^k(2m + 1)$.
Vì $GCD(2^k, 3) = 1$ nên tồn tại a sao cho $3a \equiv 1 \pmod{2^k}$. Từ đó

$$3x \equiv -1 \pmod{2^k} \Leftrightarrow x \equiv -a \pmod{2^k}$$

Tương tự $GCD\ (2, 2m+1) = 1$ nên tồn tại b sao cho $2b \equiv 1 \pmod{(2m+1)}$. Từ đó

$$2x \equiv -1 \pmod{(2m + 1)} \Leftrightarrow x \equiv -b \pmod{(2m + 1)}$$

Cuối cùng, do $GCD\ (2^k, 2m+1) = 1$ nên theo định lý Thặng dư Trung Hoa, tồn tại số nguyên x là nghiệm của hệ:

$$\begin{cases} x \equiv -a \pmod{2^k} \\ x \equiv -b \pmod{(2m + 1)} \end{cases}$$

Và theo lý luận trên, $P(x) = (3x + 1)(2x + 1) \vdots n$. ■

Ví dụ 6.17. *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 từ O nếu đoạn thẳng OA không chứa điểm nguyên nào khác ngoài A, O. Chứng minh rằng với mọi n nguyên dương lớn tùy ý, tồn tại hình vuông $n \times n$ có các đỉnh nguyên, hơn nữa tất cả các điểm nguyên nằm bên trong và trên biên của hình vuông đều không nhìn thấy được từ O.* △

Lời giải. Dễ thấy điều kiện cần và đủ để điểm $A(x_0, y_0)$ nhìn thấy được từ O là $\gcd(x_0, y_0) = 1$.
Để giải quyết bài toán, ta sẽ xây dựng một hình vuông $n \times n$ với n nguyên dương lớn tùy ý sao cho với mọi điểm nguyên (x, y) nằm trong hoặc trên hình vuông đều không thể nhìn thấy được từ O.
Thật vậy, chọn p_{i_j} là các số nguyên tố đôi một khác nhau với $0 \leq i, j \leq n$. Xét hai hệ đồng dư sau:

$$\begin{cases} x \equiv 0 \pmod{p_{0_1}p_{0_2}...p_{0_n}} \\ x+1 \equiv 0 \pmod{p_{1_1}p_{1_2}...p_{1_n}} \\ x+2 \equiv 0 \pmod{p_{2_1}p_{2_2}...p_{2_n}} \\ ... \\ x+n \equiv 0 \pmod{p_{n_1}p_{n_2}...p_{n_n}} \end{cases}$$

và

$$\begin{cases} y \equiv 0 \pmod{p_{0_1}p_{0_2}...p_{0_n}} \\ y+1 \equiv 0 \pmod{p_{1_1}p_{1_2}...p_{1_n}} \\ y+2 \equiv 0 \pmod{p_{2_1}p_{2_2}...p_{2_n}} \\ ... \\ y+n \equiv 0 \pmod{p_{n_1}p_{n_2}...p_{n_n}} \end{cases}$$

Theo định lý Thặng dư Trung Hoa thì tồn tại (x_0, y_0) thỏa mãn hai hệ đồng dư trên.
Khi đó, rõ ràng $\gcd(x_0 + i, y_0 + i) > 1, \ \forall i, j = 0, 1, 2, ..., n$.
Điều đó có nghĩa là mọi điểm nằm bên trong hoặc trên biên hình vuông $n \times n$ xác định bởi điểm phía dưới bên trái là (x_0, y_0) đều không thể nhìn thấy được từ O. Bài toán được chứng minh. ■

Trong tìm số lượng nghiệm nguyên của một phương trình nghiệm nguyên

Ví dụ 6.18. *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:*

$$x^2 + x \equiv 0 \pmod{n}$$

Lời giải. Ta có:

$$x^2+x\equiv 0 \pmod n \Leftrightarrow \begin{cases} x(x+1)\equiv 0 \pmod{p_i^{\alpha_i}} \\ i=\overline{1,k} \end{cases}$$
$$\Leftrightarrow \begin{cases} \left[\begin{array}{rcl} x &\equiv& 0 \pmod{p_i^{\alpha^i}} \\ x &\equiv& -1 \pmod{p_i^{\alpha^i}} \end{array}\right. \\ i=\overline{1,k} \end{cases} \tag{6.14}$$

Theo định lí Thặng dư Trung Hoa, mỗi hệ phương trình $x^2+x\equiv 0 \pmod n \Leftrightarrow \begin{cases} x\equiv a_i \pmod{p_i^{\alpha_i}} \\ a_i\in\{-1;0\} \\ i=\overline{1,k} \end{cases}$ có duy nhất một nghiệm 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 đã cho có đúng 2^k nghiệm. ■

Ví dụ 6.19. *Cho $m=2007^{2008}$. Hỏi có tất cả bao nhiêu số tự nhiên $n<m$ sao cho $m|n(2n+1)(5n+2)$.* △

Lời giải. Dễ thấy $GCD\ (m;10)=1$. Do đó:

$$\begin{array}{rcl} n(2n+1)(5n+2) &\equiv& 0 \pmod m \\ \Leftrightarrow 10n(10n+5)(10n+4) &\equiv& 0 \pmod m \end{array} \tag{6.15}$$

Ta có: $m=3^{4016}.223^{2008}$. Để cho thuận tiện, đặt $10n=x$; $3^{4016}=q_1$; $223^{2008}=q_2$.
Khi đó $GCD\ (q_1,q_2)=1$ nên (6.15) tương đương với:

$$x(x+5)(x+4)\equiv 0 \pmod{q_1} \tag{6.16}$$
$$x(x+5)(x+4)\equiv 0 \pmod{q_2} \tag{6.17}$$

Dễ thấy:

- (6.16) xảy ra khi và chỉ khi $x\equiv 0 \pmod{q_1}$ hoặc $x\equiv -5 \pmod{q_1}$ hoặc $x\equiv -4 \pmod{q_1}$.
- (6.17) xảy ra khi và chỉ khi $x\equiv 0 \pmod{q_2}$ hoặc $x\equiv -5 \pmod{q_2}$ hoặc $x\equiv -4 \pmod{q_2}$.

Do đó từ (6.16) và (6.17), với lưu ý rằng $x \equiv 0 \pmod{10}$, suy ra n là số tự nhiên thỏa mãn các điều kiện đề bài khi và chỉ khi $n = \dfrac{x}{10}$, với x là số nguyên thỏa mãn hệ điều kiện sau:

$$\begin{cases} x \equiv 0 \pmod{10} \\ x \equiv 1 \pmod{q_1} \\ x \equiv r_2 \pmod{q_2} \\ 0 \le x < 10q_1q_2 \\ r_1, r_2 \in \{0; -4; -5\} \end{cases} \tag{6.18}$$

Vì 10; q_1; q_2 đôi một nguyên tố cùng nhau nên theo định lí Thặng dư Trung Hoa, hệ (6.18) có nghiệm duy nhất.
Dễ thấy sẽ có 9 số x là nghiệm của 9 hệ (6.18) tương ứng. Vì mỗi số x cho ta một số n và hai số x cho hai số n khác nhau nên có 9 số n thỏa mãn các điều kiện đề bài. ■

Nhận xét. Ví dụ 6.19 chính là trường hợp đặc biệt của bài toán tổng quát sau:

Ví dụ 6.20. *Cho số nguyên dương n có phân tích tiêu chuẩn $n = p_1^{\alpha_1}p_2^{\alpha_2}...p_k^{\alpha_k}$. Xét đa thức $P(x)$ có hệ số nguyên. Nghiệm x_0 của phương trình đồng dư $P(x) \equiv 0 \pmod{n}$ là lớp đồng dư $\overline{x_0} \in \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\}$ thỏa mãn $P(x_0) \equiv 0 \pmod{n}$. Khi đó, điều kiện cần và đủ để phương trình $P(x) \equiv 0 \pmod{n}$ có nghiệm là với mỗi $i = 1, 2, ..., s$, phương trình $P(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ có nghiệm. Hơn nữa, nếu với mỗi $i = 1, 2, ..., s$, phương trình $P(x) \equiv 0 \pmod{p_i^{\alpha_i}}$ có r_i nghiệm module $p_i^{\alpha_i}$ thì phương trình có $r = r_1r_2...r_s$ nghiệm module n.* △

6.4 Bài tập đề nghị & gợi ý – đáp số

Bài tập đề nghị

Bài 1. a. Chứng minh rằng: Nếu $(a, m) = 1$ và x chạy qua một hệ thặng dư đầy đủ modulo m thì $ax + b$, với b là một số nguyên tùy ý, cũng chạy qua một hệ thặng dư đầy đủ module m.

b. Chứng minh rằng: Nếu $(a, m) = 1$ và x chạy qua một hệ thặng dư thu gọn modulo m thì ax cũng chạy qua một hệ thặng dư thu gọn module m.

Bài 2. Mỗi số nguyên dương T được gọi là số tam giác nếu nó có dạng $T = \dfrac{k(k+1)}{2}$, trong đó k là một số nguyên dương. Chứng minh rằng tồn tại một HĐĐ module n gồm n số tam giác.

Bài 3. a. Cho m_1, m_2 là hai số nguyên dương nguyên tố cùng nhau. Chứng minh rằng:

$$\Phi(m_1 m_2) = \Phi(m_1).\Phi(m_2)$$

b. Giả sử số nguyên dương m có phân tích chính tắc thành tích các thừa số nguyên tố $m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Chứng minh rằng:

$$\Phi(m) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} ... p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 2)...(p_k - 1)$$

Bài 4. Tính tổng sau:

$$S = \sum_{k=6}^{2012} \left[\frac{17^k}{11} \right]$$

Bài 5. Cho số nguyên dương n và số nguyên tố p lớn hơn $n+1$. Chứng minh rằng đa thức $P(x) = 1 + \dfrac{x}{n+1} + \dfrac{x^2}{2n+1} + ... + \dfrac{x^p}{pn+1}$ không có nghiệm nguyên.

Bài 6. Cho p là số nguyên tố có dạng $3k + 2$ (k nguyên dương). Tìm số dư khi chia $S = \sum_{k=1}^{p} (k^2 + k + 1)$ cho p.

Bài 7. Cho các số nguyên dương a, b thỏa mãn $(a, b) = 1$. Chứng minh rằng phương trình $ax + by = 1$ có vô số nghiệm nguyên (x, y) và $(x, a) = (y, b) = 1$.

Bài 8. Tìm số nguyên dương nhỏ nhất có tính chất: chia 7 dư 5, chia 11 dư 7, chia 13 dư 3.

Bài 9. Chứng minh rằng tồn tại một dãy tăng $\{a_n\}_{n=1}^{\infty}$ các số tự nhiên sao cho với mọi số tự nhiên k, dãy $\{k + a_n\}$ chỉ chứa hữu hạn các số nguyên tố.

Bài 10. Số nguyên dương n được gọi là có tính chất P nếu như với các số nguyên dương a, b mà $a^3b + 1 \vdots n$ thì $a^3 + b \vdots n$. Chứng minh rằng số các số nguyên dương có tính chất P không vượt quá 24.

Bài 11. Tìm tất cả các số tự nhiên n thỏa mãn $2^n - 1$ chia hết cho 3 và có một số nguyên m mà $\dfrac{2^n - 1}{3} | 4m^2 + 1$.

Bài 12. Chứng minh rằng tồn tại số tự nhiên k sao cho tất cả các số $k.2^n + 1$ $(n = 1, 2, ...)$ đều là hợp số.

Gợi ý – đáp số

Bài 1. Chứng minh trực tiếp dựa vào định nghĩa.

Bài 2. Ta chứng minh n phải có dạng $n = 2^k$. Phản chứng, giả sử $n = 2^k.m$ với m lẻ và $m > 1$. Sử dụng tính chất hệ thặng dư đầy đủ.

Bài 3. Ta có thể chứng minh dựa vào kiến thức về hệ thặng dư đầy đủ, cũng có thể chứng minh dựa vào định lí Thặng dư trung Hoa.

Bài 4. Sử dụng HTG.

Bài 5. Biểu diễn $P(x)$ dưới dạng $P(x) = a_p x^p + a_{p-1}x^{p-1} + ... + a_2x^2 + a_1x + a_0$. Phản chứng, giả sử $P(x)$ có nghiệm nguyên $x = u$. Suy ra mâu thuẫn.

Bài 6. Tiến hành tương tự Ví dụ 6.7.

Bài 7. Sử dụng kiến thức HĐĐ.

Bài 8. Đáp số: 887.

Bài 9. Gọi p_k là số nguyên tố thứ k, $k > 0$. Theo định lí Thặng dư Trung Hoa, tồn tại dãy số $\{a_n\}_{n=1}^{\infty}$ thỏa mãn $a_1 = 2; a_n = -k(\mathrm{mod} p_{k+1}), \forall k \leq n$.

Bài 10. Định lý Thặng dư Trung Hoa.

Bài 11. Chứng minh n có dạng 2^k. Sử dụng tính chất của số Fecma (xem lại Ví dụ 6.15).

Bài 12. Ví dụ 6.15 và Bài 3.

Chương

7 Một số bài toán số học hay trên VMF

Phần này gồm một số bài toán hay được thảo luận nhiều trên Diễn đàn Toán học. Bạn đọc có thể vào trực tiếp topic của bài toán đó trên Diễn đàn Toán học, bằng cách click vào tiêu đề của bài toán đó.

7.1 $m^3 + 17 \vdots 3^n$

Bài toán 7.1. *Chứng minh rằng với mọi số nguyên dương n, tồn tại một số tự nhiên m sao cho*

$$\left(m^3 + 17\right) \vdots 3^n$$

. △

Đầu tiên, chúng ta đến với chứng minh đề xuất cho bài toán đầu bài.
Chứng minh. Ta sẽ chứng minh bài toán bằng quy nạp.
Với $n = 1$, ta chọn $m = 4$.
Với $n = 2$, ta chọn $m = 1$.

Giả sử bài toán đúng đến $n = k$, hay $\exists m \in \mathbb{N} : m^3 + 17 \vdots 3^k$
Ta chứng minh rằng đối với trường hợp $n = k+1$ cũng đúng tức là tồn tại một số m' sao cho $m'^3 + 17 \vdots 3^{k+1}$.

Đặt $m^3 + 17 = 3^k.n \Rightarrow n \not\vdots 3$.

$$\Rightarrow \left[\begin{array}{l} n\equiv 2 \\ n\equiv 1 \end{array}\right. (\text{mod} 3) \Rightarrow \left[\begin{array}{l} m^3+17\equiv 2.3^k \\ m^3+17\equiv 3^k \end{array}\right. \left(\text{mod} 3^{k+1}\right)$$

• ***Trường hợp 1:*** $m^3+17\equiv 2.3^k \pmod{3^{k+1}}$
Xét:

$$(m+3^{k-1})^3 = m^3+m^2 3^k+m3^{2k-1}+3^{3k-3} \equiv m^3+m^2 3^k \pmod{3^{k+1}}$$

(Do $k\geq 2 \Rightarrow 3^{2k-1}\vdots 3^{k+1}$ và $3^{3k-3}\vdots 3^{k+1}$).
Suy ra:

$$\left(m+3^{k-1}\right)^3+17 \equiv m^3+m^2.3^k+17 \equiv 2.3^k+m^2.3^k \equiv 0 \pmod{3^{k+1}}$$

(vì $m \not\vdots 3 \Rightarrow m^2\equiv 1 \pmod 3 \Rightarrow 2+m^2\vdots 3 \Rightarrow (2+m^2).3^k\vdots 3^{k+1}$).

Như vậy, ở trường hợp 1, ta có: $\left(m+3^{k-1}\right)^3+17\vdots 3^{k+1}$.

• ***Trường hợp 2:*** $m^3+17\equiv 3^k \pmod{3^{k+1}}$.
Xét:

$$\left(m-3^{k-1}\right)^3 = m^3-m^2 3^k+m3^{2k-1}-3^{3k-3} \equiv m^3-m^2 3^k \pmod{3^{k+1}}$$

(Do $k\geq 2 \Rightarrow 3^{2k-1}\vdots 3^{k+1}$ và $3^{3k-3}\vdots 3^{k+1}$).
Suy ra:

$$\left(m-3^{k-1}\right)^3+17 \equiv m^3-m^2 3^k+17 \equiv 3^k-m^2 3^k \equiv 0 \pmod{3^{k+1}}$$

(vì $m \not\vdots 3 \Rightarrow m^2\equiv 1 \pmod 3 \Rightarrow 1-m^2\vdots 3 \Rightarrow \left(1-m^2\right).3^k\vdots 3^{k+1}$).

Như vậy, ở trường hợp 2 ta có: $\left(m-3^{k-1}\right)^3+17\vdots 3^{k+1}$.

Tóm lại, ta đều tìm được số nguyên $t \not\vdots 3$ mà $t^3+17\vdots 3^{k+1}$.
Ta đã chứng minh được vấn đề đúng trong trường hợp $n=k+1$.
Theo nguyên lý quy nạp, ta có đpcm.

Mấu chốt bài toán này là bổ đề sau:

Bổ đề 7.1– *Cho a, b, q là các số nguyên thỏa $(a; q) = 1$ và $q > 0$. Khi ấy, luôn tồn tại $k \in \mathbb{Z}$ sao cho $ak \pm b \vdots q$.* □

Chứng minh. Ta chứng minh đại diện cho trường hợp $ak + b \vdots q$. Trường hợp còn lại tương tự.
Xét $A = \{1; 2; 3; ...; q\}$ là 1 hệ đầy đủ HDD mod q.
Theo tính chất của Hệ thặng dư, ta có tập $B = \{a; 2a; 3a; ...; qa\}$ cũng là HDD mod q.
$\Rightarrow C = \{a + b; 2a + b; 3a + b; ...; qa + b\}$ cũng là HDD mod q.

Do đó, tồn tại $k \in [1; q]$ sao cho $ak + b \vdots q$. ■

Nhận xét. Bài toán đã cho thực chất là yêu cầu tìm 1 số x nguyên sao cho $x + 17 \vdots 3^n$ và x là lập phương 1 số nguyên. Bổ đề trên đã cho thấy sự tồn tại của x nguyên để $x + 17 \vdots 3^n$. Còn việc tìm x để là x là lập phương 1 số nguyên thì ta sẽ dùng phương pháp quy nạp như trên.
Đối với 1 người yêu toán, ta phải không ngừng sáng tạo. Ta hãy thử tổng quát bài toán đã cho:

- thay vì m^3, ta thử thay m^k với k là số nguyên dương cố định.
- thay vì 3^n, ta thử thay p^n với p là 1 số nguyên tố.
- thay số 17 bởi $y \in \mathbb{N}$ với y cố định.

Kết hợp các thay đổi trên, ta có 1 bài toán "tổng quát" hơn

Dự đoán 7.1– *Cho p là số nguyên tố. $y, k \in \mathbb{N}$ và y, k cố định. Khẳng định hoặc phủ định mệnh đề sau*

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^k + y \vdots p^n \tag{7.1}$$

Ta thử thay một vài giá trị p, k, y vào để thử xem (7.1) có đúng không.

Khi thay $k = 2, y = 1, p = 3$ thì mệnh đề (7.1) trở thành

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^2 + 1 \vdots 3^n \tag{7.2}$$

Rất tiếc, khi này, (7.2) lại sai!!!. Ta sẽ chứng minh (7.2) sai khi $n \geq 1$.

Thật vậy, để chứng minh dự đoán 7.1 sai, ta cần có bổ đề sau

Bổ đề 7.2– *Cho p là số nguyên tố dạng $4k+3$ và $a, b \in \mathbb{Z}$. Khi đó*

$$a^2 + b^2 \vdots p \Leftrightarrow (a \vdots p) \wedge (b \vdots p)$$

Từ (7.2), suy ra $x^2 + 1 \vdots 3$. Áp dụng bổ đề 7.2 với $p = 3$, ta suy ra $1 \vdots 3$: vô lý.

Vậy khi $n \geq 1$ thì $\nexists x \in \mathbb{Z} : x^2 + 1 \vdots 3^n$.

Không nản lòng, ta thử thêm một vài điều kiện để (7.1) trở nên chặt hơn và đúng. Nếu bạn đọc có ý kiến nào hay, xin hãy gửi vào topic này để thảo luận. Sau khi thêm một số điều kiện, ta có 1 bài toán hẹp hơn nhưng luôn đúng.

Định lý 7.1– *Cho p nguyên tố lẻ. $y, k \in \mathbb{N}$ và y, k cố định.*
Biết rằng $gcd(k, p) = gcd(k, p-1) = gcd(y, p) = 1$.
Chứng minh rằng:

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^k + y \vdots p^n \tag{7.3}$$

Chứng minh. Trước hết, để chứng minh (7.3), ta cần có bổ đề sau

Bổ đề 7.3– *Cho p là số nguyên tố lẻ. k nguyên dương thỏa*

$$(k; p) = (k-1; p) = 1$$

Khi đó, $\{1^k; 2^k; ...; (p-1)^k\}$ là HTG mod$p$. □

Chứng minh. Gọi g là căn nguyên thủy của p tức là $ord_p(g) = p-1$. Khi đấy thì $g^1, g^2, ..., g^{p-1}$ lập thành 1 HTG mod$p$ và rõ ràng $g^{a_1}, g^{a_2}, ..., g^{a_{p-1}}$ là HTG mod$p \Leftrightarrow a_1, a_2, .., a_{p-1}$ là HĐD của $p-1$. Với $1 \leq i \leq p-1$ thì tồn tại a_i để mà $i \equiv g^{a_i} \pmod p$ và rõ ràng a_i lập thành 1 HTG mod$p$ nên hệ $1^k, 2^k, .., (p-1)^k$ có thể viết lại là $g^k, g^{2k}, ..., g^{(p-1)k}$, nó là HTG mod$p$ khi và chỉ khi $k, 2k, ..., (p-1)k$ là hệ thặng dư đầy đủ của $p-1$, tức là k nguyên tố cùng nhau với $p-1$. Bổ đề được chứng minh. ■

Quay lại bài toán. Ta chứng minh (7.3) bằng phương pháp quy nạp.
Với $n = 1$, theo bổ đề 7.3 thì

$$\exists x_0 \in \{1; 2; ...; p-1\} : x_0^k \equiv -y \pmod{p} \Rightarrow x_0^k + y \vdots p$$

Giả sử bài toán đúng đếnn hay tồn tại $x^k + y \vdots p^n$

Ta sẽ chứng minh $n+1$ cũng đúng hay tồn tại $x_0^k + y \vdots p^{n+1}$
Thật vậy, từ giả thiết quy nạp suy ra $x^k + y = p^n.q$

- Trường hợp 1: $q \vdots p \Rightarrow$ đpcm
- Trường hợp 2:

$$gcd(q, p) = 1 \tag{7.4}$$

Khi đó ta chọn $x_0 = v.p^n + x$
Do đó

$$\begin{aligned} & x_0^k + y = (v.p^n + x)^k + y \\ &= v^k.p^{nk} + \binom{1}{k}.v^{k-1}.p^{n(k-1)}.x + ... + \binom{k-1}{k}.v.p^n.x^{k-1} + (x^k + y) \end{aligned} \tag{7.5}$$

Dễ dàng chứng minh

$$p^{n+1} \mid v^k.p^{nk} + \binom{1}{k}.v^{k-1}.p^{n(k-1)}.x + ... \binom{k-2}{k}.v^2.p^{2n}.x^{k-2}$$

Do vậy ta xét

$$\binom{k-1}{k}.v.p^n.x^{k-1} + (x^k + y) = k.v.p^n.x^{k-1} + p^n.q = p^n(k.v.x^{k-1} + q)$$

Nhận thấy giả sử $k.x^{k-1} \equiv t \pmod{p}$ mà $gcd(k, p) = 1$ và $x^k + y \vdots p \Rightarrow gcd(x, p) = 1$ (do $gcd(y, p) = 1$) suy ra $gcd(t, p) = 1$
Do đó $(k.v.x^{k-1} + q) \equiv tv + q \pmod{p}$ mà từ (7.4) ta đã có $gcd(q, p) = 1$

Cho nên luôn tồn tại v thỏa mãn $tv + q \vdots p$. Do đó bài toán được khẳng đinh với $n+1$.
Theo nguyên lý quy nạp, bài toán đã được chứng minh.

Chưa dừng lại ở đây, nếu trong (7.3), ta thay k bởi x, ta sẽ được 1 bài toán khác:

Định lý 7.2– *Cho p nguyên tố lẻ. $y \in \mathbb{N}$ và y cố định. Biết rằng $gcd(y, p) = 1$. Khi đó:*

$$\forall n \in \mathbb{N}, \exists x \in \mathbb{N} : x^x + y \vdots p^n \tag{7.6}$$

Chứng minh. Ta chứng minh bài toán này bằng phương pháp quy nạp. Ta coi định lý 7.1 như 1 bổ đề. Dễ thấy nếu x thỏa (7.6) thì $gcd(x; p) = 1$.
Khi đó, với $n = 1$, ta xét hệ đồng dư (I)

$$\begin{cases} x \equiv k \pmod{(p-1)} \\ x \equiv x_0 \pmod{p} \end{cases}$$

trong đó, $x_0; k \in \mathbb{N}$ thỏa $x_0^k + y \vdots p$.
Do $gcd(p-1; p) = 1$ nên theo định lý Thặng dư Trung Hoa thì hệ (I) luôn có nghiệm x'.
Chọn $x = x'$, ta chứng minh x thỏa (7.6) khi $n = 1$. Thật vậy

$$\begin{aligned} gcd(x; p) = 1 \Rightarrow x^{p-1} \equiv 1 \pmod{p} \Rightarrow x^k \equiv x^x \pmod{p} \\ \Rightarrow x^x + y \equiv x^k + y \equiv x_0^k + y \equiv 0 \pmod{p} \end{aligned}$$

Vậy $\exists x \in \mathbb{N} : x^x + y \vdots p$.

Giả sử (7.6) đúng đến $n-1$, tức là tồn tại x_0 để ${x_0}^{x_0} + y \vdots p^{n-1}$.
Theo cách chứng minh quy nạp ở (7.6), ta chọn được $x_n = ap^n + x_0$ thỏa $x_n^{x_0} + y \vdots p^n$.
Khi đó, dễ nhận thấy $x_n \equiv x_0 \pmod{p^{n-1}}$. Ta xét hệ đồng dư (II)

$$\begin{cases} X \equiv x_0 \pmod{(p^{n-1}(p-1))} \\ X \equiv x_n \pmod{p^n} \end{cases}$$

Do $gcd(p^{n-1}(p-1); p^n) = 1$ nên theo định lý Thặ ng dư Trung hoa, hệ (II) có nghiệm X. Ta chứng minh $x = X$ thỏa (7.6). Thật vậy
Do $(p-1)p^{n-1} = \phi(p^n) \Rightarrow X^X \equiv X^{x_0} \pmod{p^n}$ (định lý Euler).

Mặt khác $X^{x_0} \equiv {x_n}^{x_0} \pmod{p^n}$ (do cách chọn trong hệ (II)).

$$\Rightarrow X^X + y \equiv {x_n}^{x_0} + y \equiv 0 \pmod{p^n}$$

Theo nguyên lý quy nạp, bài toán đã được chứng minh. ■

Mở rộng của bài toán đầu đề vẫn còn nhiều, như tăng thêm điều kiện để chặn như $(m^3+17\vdots 3^n) \wedge (m^3+17 \not\vdots 3^{n+1})$, v.v. Rất mong nhận được ý kiến đóng góp cho việc mở rộng.

Lời cảm ơn

Rất cảm ơn Nguyen Lam Thinh, Karl Heinrich Marx,nguyenta98, The Gunner đã đóng góp ý kiến và mở rộng cho bài viết này.

7.2 $c(ac+1)^2=(5c+2)(2c+b)$

Bài toán 7.2. *Cho 3 số nguyên dương $a;b;c$ thoả mãn đẳng thức:*

$$c(ac+1)^2=(5c+2b)(2c+b) \tag{7.7}$$

Chứng minh rằng : c là số chính phương lẻ. △

Nhận xét. Thoạt nhìn vào bài toán, thật khó để tìm 1 phương pháp cho loại này. Nhận xét trong giả thiết ở VP (7.7), thì b xuất hiện với bậc là 2. Thế là ta có 1 hướng nghĩ là dùng tam thức bậc 2 cho bài toán này. Ta không nên chọn c vì bậc của c là 3, không chọn a vì phương trình mới theo a hiển nhiên trở lại (7.7)

Chứng minh (Chứng minh 1).

$$\begin{aligned}
&c\left(ac+1\right)^2=\left(5c+2b\right)\left(2c+b\right)\\
&\Leftrightarrow 2b^2+9bc+10c^2-c\left(ac+1\right)^2=0\\
&\Delta_b=81c^2-4.2.\left(10c^2-c\left(ac+1\right)^2\right)=c^2+8c\left(ac+1\right)^2\\
&\Rightarrow \Delta_b=c\left[c+8\left(ac+1\right)^2\right]=x^2,(x\in\mathbb{N}^*)
\end{aligned}$$

Đặt $\left.\begin{array}{l} d=GCD(c;c+8(ac+1)^2)\Rightarrow d|8\left(ac+1\right)^2\\ d|c\Rightarrow\left(\left(ac+1\right)^2;d\right)=1\end{array}\right\}\Rightarrow d|8$

- Trường hợp 1: $\boxed{\text{d=8}}\Rightarrow\left(\frac{c}{8};\frac{c}{8}+\left(ac+1\right)^2\right)=1$

$$\begin{aligned}
&c\left[c+8\left(ac+1\right)^2\right]=x^2(x\in\mathbb{N})\Leftrightarrow\frac{c}{8}.\left(\frac{c}{8}+\left(ac+1\right)^2\right)=\left(\frac{x}{8}\right)^2\\
&\Rightarrow 8|x\Rightarrow x=8x_2\,(x_2\in\mathbb{N}^*)\Rightarrow\frac{c}{8}.\left(\frac{c}{8}+\left(ac+1\right)^2\right)=x_2^2\\
&\Rightarrow\left\{\begin{array}{ll}\dfrac{c}{8}=t^2 & \left(\begin{array}{l}t;p\in\mathbb{N}^*\\(t;p)=1\end{array}\right)\\ \dfrac{c}{8}+\left(ac+1\right)^2=p^2 & \end{array}\right.\\
&\Rightarrow\left\{\begin{array}{l}c=8t^2\\ t^2+\left(8t^2a+1\right)^2=p^2\end{array}\right.
\end{aligned}$$

Mà dễ chứng minh

$$\begin{aligned}
&\left(8t^2a+1\right)^2<t^2+\left(8t^2a+1\right)^2<\left(8t^2a+2\right)^2\\
&\Rightarrow\left(8t^2a+1\right)^2<p^2<\left(8t^2a+2\right)^2:\text{ mâu thuẫn}
\end{aligned}$$

Do đó, $d=8$ bị loại.

• Trường hợp 2: d=4 $\Rightarrow \left(\frac{c}{4};\frac{c}{4}+2\left(ac+1\right)^2\right)=1$

$\Rightarrow \frac{c}{4};\frac{c}{4}+2\left(ac+1\right)^2$ là những số chính phương (*)

Nếu $\frac{c}{4}$ là số chẵn $\Rightarrow \frac{c}{4}+2\left(ac+1\right)^2 \vdots 2$

$\Rightarrow \left(\frac{c}{4};\frac{c}{4}+2\left(ac+1\right)^2\right)=2$: mâu thuẫn.

Do đó, $\frac{c}{4}$ là số lẻ. Mà $\frac{c}{4}$ là số chính phương $\Rightarrow \frac{c}{4}\equiv 1 \pmod 4$

Mặt khác, do c chẵn nên $ac+1$ là số lẻ $\Rightarrow (ac+1)^2\equiv 1 \pmod 4$

$\Rightarrow \frac{c}{4}+2\left(ac+1\right)^2\equiv 1+2.1\equiv 3 \pmod 4$: vô lý do (*).

Do đó, $d=4$ bị loại.

• Trường hợp 3: d=2.

Tương tự tự Trường hợp 2, ta có $\frac{c}{2}$ lẻ $\Rightarrow \frac{c}{2}\equiv 1 \pmod 8$

c chẵn nên $ac+1$ lẻ $\Rightarrow (ac+1)^2\equiv 1 \pmod 8$

$$\Rightarrow \frac{c}{2}+4(ac+1)^2\equiv 1+4.1\equiv 5 \pmod 8 : \text{ vô lý}$$

Do đó, $d=2$ bị loại.

• Trường hợp 4: d=1

Tương tự trường hợp 2, ta có ngay c lẻ và do $(c;c+8(ac+1)^2)=1$ nên c là số chính phương.

Vậy ta có đpcm. ■

Nhận xét. Ta thấy trong bài này, b và c có 1 mối liên quan khá chặt chẽ với nhau nên ta thử giải theo b,c sử dụng kĩ thuật GCD tức là đặt $d=GCD(b;c)$ ta có cách chứng minh thứ 2.

Chứng minh (Chứng minh 2). Đặt $d=(b;c)\Rightarrow \left\{\begin{array}{l} c=dm \\ b=dn \end{array}\right. \left(\begin{array}{l} m;n\in\mathbb{N}^* \\ (m;n)=1 \end{array}\right)$

Khi đó

$$\begin{aligned}
&(7.7)\Leftrightarrow m\left(dam+1\right)^2=d\left(5m+2n\right)\left(2m+n\right)\\
&\left.\begin{array}{l}\Rightarrow d|m\left(dam+1\right)^2\\(d;dam+1)=1\end{array}\right\}\Rightarrow d|m\Rightarrow m=dp\Rightarrow(p;n)=(d;n)=1\\
&(7.7)\Leftrightarrow p\left(d^2ap+1\right)^2=\left(5dp+2n\right)\left(2dp+n\right)\\
&\left.\begin{array}{l}\Rightarrow p|\left(5dp+2n\right)\left(2dp+n\right)\\(p;2dp+n)=1\end{array}\right\}\Rightarrow p|5dp+2n\Rightarrow p|2n\\
&(p;n)=1\Rightarrow p|2\Rightarrow p\in\{1;2\}
\end{aligned}$$

• Trường hợp 1: $\boxed{\text{p=2}}$, khi đó $2\left(2ad^2+1\right)^2=\left(10d+2n\right)\left(4d+n\right)$, suy ra $\left(2ad^2+1\right)^2=\left(5d+n\right)\left(4d+n\right)$. Nhưng vì $\left(5d+n;4d+n\right)=\left(d;4d+n\right)=(d;n)=1$ Cho nên ta phải có

$$\left\{\begin{array}{l}5d+n=x^2\\4d+n=y^2\end{array}\right.\qquad(x;y\in\mathbb{N}^*,(x;y)=1)$$

Suy ra $d=x^2-y^2$. Mặt khác

$$2ad^2+1=xy\Leftrightarrow a=\frac{xy-1}{2d^2}=\frac{xy-1}{2\left(x^2-y^2\right)^2}$$

Ta chứng minh $2\left(x^2-y^2\right)^2>\left(x+y\right)^2>xy-1$
Thật vậy

$$\begin{aligned}
&\left(x+y\right)^2\geq4xy>xy-1\\
&2\left(x^2-y^2\right)^2-\left(x+y\right)^2=\left(x+y\right)^2\left(2\left(x-y\right)^2-1\right)>0\\
&\Rightarrow2\left(x^2-y^2\right)^2>xy-1\Rightarrow a<1:\text{ Trái gt}
\end{aligned}$$

Vậy $p=2$ bị loại.
• Trường hợp 2: $\boxed{\text{p=1}}$

$$\begin{aligned}
&\Rightarrow d=m\Rightarrow\left\{\begin{array}{l}c=d^2,(i)\\b=dn\end{array}\right.\\
&(7.7)\Leftrightarrow d^2\left(ad^2+1\right)^2=\left(5d^2+2dn\right)\left(2d^2+dn\right)\\
&\qquad\Leftrightarrow\left(ad^2+1\right)^2=\left(5d+2n\right)\left(2d+n\right)\qquad(7.8)
\end{aligned}$$

$$(5d+2n;2d+n)=(d;2d+n)=(d;n)=1$$
$$\Rightarrow \left\{\begin{array}{l} 5d+2n=x^2 \\ 2d+n=y^2 \end{array}\right. \left(\begin{array}{l} x;y\in\mathbb{N}^* \\ (x;y)=1 \end{array}\right) \Rightarrow \left\{\begin{array}{l} d=x^2-2y^2 \\ n=5y^2-2x^2 \end{array}\right.$$

Nếu $x=2z$ với $z\in\mathbb{N}^* \Rightarrow \left\{\begin{array}{l} d=4z^2-2y^2 \\ n=5y^2-8z^2 \end{array}\right.$

$$(7.8)\Leftrightarrow \left(ad^2+1\right)^2=4z^2y^2 \Leftrightarrow a\left(4z^2-2y^2\right)^2+1=2zy$$

Phương trình cuối cùng vô nghiệm nguyên do 2 vế khác tính chẵn lẻ.
Suy ra, x lẻ $\Rightarrow d$ lẻ $\Rightarrow c$ lẻ. (ii)
Kết luận: $(i),(ii)\Rightarrow c$ là số chính phương lẻ. ■

Không ngừng tìm kiếm, ta sẽ tìm một lời giải khác súc tích hơn. Nếu ta biết đến công cụ $v_p(n)$ thì sẽ thấy nó sẽ rất hiệu quả cho bài toán này, ta có cách chứng minh thú vị sau.

Chứng minh (Chứng minh 3). Giả sử c chẵn khi đó ta có:

$$v_2(c)=v_2(5c+2b)+v_2(2c+b)$$

Nếu b lẻ thì ta có $v_2(c)=v_2(5c+2b)=v_2(5c)\Rightarrow v_2(5c)<v_2(2b)=1$.
Điều này vô lí!
Do đó c lẻ. Xét $p|c$ là một ước nguyên tố của c.
Ta có $v_p(c)=v_p(5c+2b)+v_p(2c+b)$.
Ta thấy rằng $v_p(c)>v_p(5c+2b), v_p(2c+b)>0$.
Do đó $v_p(5c+2b)=min[v_p(c);v_p(4c+2b)]$
$\Rightarrow v_p(5c+2b)=v_p(4c+2b)=v_p(2c+b)$
$\Rightarrow v_p(c)=2v_p(5c+2b)$: số chẵn nên suy ra c là số chính phương. ■

Và hi vọng còn những lời giải khác hay hơn, sáng tạo hơn từ các bạn. Mong bạn đọc thảo luận thêm và đóng góp ý kiến cho bài toán.

Lời cảm ơn

Rất cảm ơn Karl Heinrich Marx,nguyenta98, Vương Nguyễn Thùy Dương và perfectstrong đã đóng góp ý kiến cho bài viết này.

Tài liệu tham khảo

[1] Vũ Hữu Bình,*Phương trình nghiệm nguyên và kinh nghiệm giải*

[2] Phan Huy Khải, *Các chuyên đề bồi dưỡng học sinh giỏi toán trung học. Chuyên đề 5: Phương trình nghiệm nguyên*

[3] Phạm Minh Phương và nhóm tác giả chuyên toán Đại học Sư phạm Hà Nội, *Các chuyên đề Số học bồi dưỡng học sinh giỏi Trung học cơ sở*

[4] Titu Andreescu, Dorin Andrica, *Number Theory: Structures, Examples and Problems*

[5] Tạp chí Toán Tuổi Thơ, Toán học và Tuổi trẻ, Mathematical Reflections, v.v

[6] Các đề thi học sinh giỏi, tuyển sinh vào THPT, TST, IMO,v.v

[7] Tài nguyên Internet, đặc biệt: HTTP://DIENDANTOANHOC.NET/FORUM/, HTTP://WWW.ARTOFPROBLEMSOLVING.COM/, HTTP://BOXMATH.VN

[8] Gv THPT chuyên ĐHKHTN Hà Nội,*Bài giảng Số học*

[9] Đặng Hùng Thắng, *Đồng dư và phương trình đồng dư*

[10] Phan Huy Khải, *Các bài toán cơ bản của Số học*

[11] Hà Huy Khoái, *Chuyên đề bồi dưỡng HSG THPT Số Học*

[12] Kỷ yếu của các hội thảo Toán học, Tạp chí Toán học và Tuổi trẻ, tạp chí Crux,v.v

[13] Nguyễn Trọng Nam, *Lý thuyết đồng dư và ứng dụng trong mã sửa sai*