Lời nói đầu

Số học là một phần rất quan trọng trong chương trình Toán phổ thông. Trong hầu hết các đề thi học sinh giỏi thì bài Số học thường xuyên xuất hiện và luôn là một thách thức lớn đối với học sinh.

Hiện nay, không còn hệ chuyên cấp Trung học cơ sở nên các em học sinh chuyên Toán cũng không được học nhiều về phần này nên thường gặp rất nhiều khó khăn khi giải các bài toán đó. Vì vậy, tôi biên soạn tài liệu này nhằm giải quyết phần nào những khó khăn đó cho các em học sinh chuyên Toán.

Chuyên đề gồm ba chương:

-Chương I. Các bài toán chia hết

-Chương II. Các bài toán đồng dư

-Chương III. Các bài toán khác.

Ở mỗi bài đều được trình bày ba phần: Hệ thống lí thuyết; hệ thống các ví dụ và cuối cùng là hệ thống các bài tập tự giải. Các ví dụ và bài tập luôn được sắp xếp với độ khó tăng dần - theo quan điểm của tác giả.

Tuy nhiên, do trình độ có hạn nên không thể tránh khỏi nhiều thiếu sót, rất mong được các thầy cô đóng góp để hoàn thiện hơn. Xin chân thành cảm ơn!

NGUYỄN VĂN THẢO

Chương I

CÁC BÀI TOÁN VỀ CHIA HẾT

I.1 Chia hết

I.1.1 Lí thuyết

I.1.1.1 Định nghĩa

Cho m và n là hai số nguyên , $n \neq 0$. Ta nói rằng m chia hết cho n (hay n chia hết m) nếu tồn tại một số nguyên k sao cho $m = kn$.

Kí hiệu: $m \vdots n$, (đọc là m chia hết cho n) hay $n \mid m$, (đọc là n chia hết m).

I.1.1.2 Các tính chất cơ bản

Cho các số nguyên x, y, z. Ta có:

a) $x \vdots x$, $x \neq 0$.

b) Nếu $x \vdots y$ và $x \neq 0$ thì $|x| \geq |y|$.

c) Nếu $x \vdots z$, $y \vdots z$ thì $ax + by \vdots z$ với mọi số nguyên a, b.

d) Nếu $x \vdots z$ và $x \mp y \vdots z$ thì $y \vdots z$

e) Nếu $x \vdots y$ và $y \vdots x$ thì $|x| = |y|$.

f) Nếu $x \vdots y$ và $y \vdots z$ thì $x \vdots z$.

g) Nếu $x \mid y$ và $y \neq 0$ thì $\frac{y}{x} \mid y$.

Chứng minh

a) $x = 1.x$ nên $x \vdots x$ với mọi $x \neq 0$.

b) Nếu $x \vdots y$, $x \neq 0$ thì tồn tại $k \in Z$ sao cho $x = ky$, $k \neq 0$

$\Rightarrow |x| = |k||y| \geq |y|$ do $|k| \geq 1$.

Các phần còn lại cũng khá đơn giản, việc chứng minh xin nhường lại cho bạn đọc.

I.1.2 Các ví dụ

Ví dụ 1. Cho n là một số tự nhiên lớn hơn 1. Chứng minh rằng

a) 2^n là tổng của hai số lẻ liên tiếp.

b) 3^n là tổng của ba số tự nhiên liên tiếp.

Lời giải

a) Ta có $2^n = (2^{n-1} - 1) + (2^{n-1} + 1)$ suy ra đpcm.

b) Ta có $3^n = (3^{n-1} - 1) + (3^{n-1}) + (3^{n-1} + 1)$ suy ra đpcm.

Ví dụ 2. Chứng minh rằng:

a) nếu $m - n$ chia hết $mp + nq$ thì $m - n$ cũng chia hết $mq + np$.

b) nếu m – n chia hết mp thì m – n cũng chia hết np.

Lời giải

Nhận xét: *Hai biểu thức (mp + nq) và (mq + np) là hai biểu thức có hình thức giống như "đối xứng loại hai" vì vậy khi xét các biểu thức loại này thường người ta kiểm tra hiệu của chúng.*

a) Ta có $(mp + nq) - (mq + np) = (m - n)(p - q) \vdots (m - n)$

Nên nếu $(mp + nq) \vdots (m - n)$ thì hiển nhiên $(mq + np) \vdots (m - n)$.

b) Chứng minh tương tự.

Ví dụ 3. Chứng minh rằng nếu $a^3 + b^3 + c^3$ chia hết cho 9 thì một trong ba số *a, b, c* phải chia hết cho 3.

Lời giải

Nhận xét: *Với những bài toán chứng minh a chia hết cho một số cụ thể luôn khá đơn giản! Ta có thể xét hết các trường hợp xảy ra của số dư khi a chia cho số đó. (Công viêc đó chính là xét về hệ thặng dư đầy đủ - đây là tập hữu hạn nên có thể thử trực tiếp)*

Giả sử không có số nào trong ba số *a, b, c* chia hết cho 3. Khi đó

$a = 3m \pm 1; b = 3n \pm 1; c = 3p \pm 1$

Do đó $a^3 + b^3 + c^3 = (3m \pm 1)^3 + (3n \pm 1)^3 + (3p \pm 1)^3$

$$= \begin{bmatrix} 9A+3 \\ 9a+1 \\ 9a-3 \\ 9A-1 \end{bmatrix}$$ không thể chia hết cho 9.

Từ đó suy ra đpcm.

Ví dụ 4.

Chứng minh rằng nếu $a^2 + b^2$ chia hết cho 3 thì cả *a* và *b* đều chia hết cho 3.

Lời giải

TH1: có 1 số không chia hết cho 3, giả sử là *a*

Khi đó $a = 3k \pm 1; b = 3q$ suy ra $a^2 + b^2 = (3k \pm 1)^2 + (3q)^2$

$= 3(3k^2 \pm 2k + 3q^2) + 1$ không chia hết cho 3.

TH2: cả hai số không chia hết cho 3.

Khi đó $a = 3k \pm 1; b = 3q \pm 1$ suy ra $a^2 + b^2 = 3A + 2$

Do đó cả *a* và *b* phải chia hết cho 3.

Ví dụ 5. Chứng minh rằng với mọi số tự nhiên chẵn *n* và mọi số tự nhiên lẻ *k* thì

$S = 1^k + 2^k + \ldots + n^k$ luôn chia hết cho $n + 1$.

Lời giải

Ta có $2S = (1^k + n^k) + (2^k + (n - 1)^k) + \ldots \vdots n + 1$

Mà n chẵn nên $n + 1$ lẻ nên $(2, n+ 1) = 1$

Do đó $S \vdots n + 1$.

Ví dụ 6. Cho p là s ố nguyên tố, $p > 3$ v à $n = \dfrac{2^{2p} - 1}{3}$ .Chứng minh rằng

$$2^n - 2 \vdots n.$$

Lời giải

Vì p là số nguyên tố và $p>3 \Rightarrow 2^{p-1} \equiv 1 (\mathrm{mod}\, 3)$

Mặt khác $(2, p) = 1$ nên theo định lí Fermat ta có

$$2^{p-1} \equiv 1 (\mathrm{mod}\, p)$$

Do đó $2^{p-1} - 1 \vdots 3p$

Ta có

$$n - 1 = \frac{2^{2p} - 1}{3} - 1 = \frac{4^p - 4}{3} = \frac{4(2^{p-1} + 1)(2^{p-1} - 1)}{3}$$

suy ra $n - 1 \vdots 2p \Rightarrow 2^{n-1} - 1 \vdots 2^{2p} - 1$

Vì $n = \dfrac{2^{2p} - 1}{3} \Rightarrow 2^{2p} - 1 \vdots n \Rightarrow 2^{n-1} - 1 \vdots n \Rightarrow 2^n - 2 \vdots n.$

Từ đó suy ra điều phải chứng minh.

Ví dụ 7. Cho x, y là hai số nguyên khác -1 sao cho

$$\frac{x^3 + 1}{y + 1} + \frac{y^3 + 1}{x + 1} \quad \text{là một số nguyên}$$

Chứng minh rằng $x^{2004} - 1$ chia hết cho $y+1$.

Lời giải

Trước hết ta đặt $\dfrac{x^3 + 1}{y + 1} = \dfrac{a}{b}$; $\dfrac{y^3 + 1}{x + 1} = \dfrac{c}{d}$

với a, b, c, d nguyên và $b > 0, d > 0, (a,b) = 1, (c,d) = 1$.

Ta có

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad \text{nguyên}$$

Do đó

$$ad+bc \ \vdots\ \text{bd} \Rightarrow \text{ad}+\text{bc}\vdots\text{b} \Rightarrow \text{ad}\vdots\text{b} \Rightarrow \text{d}\vdots\text{b} \quad \text{vì } (a,b)=1 \qquad (1)$$

Mặt khác

$$\frac{a}{b}.\frac{c}{d}=\frac{x^3+1}{y+1}.\frac{y^3+1}{x+1}=(x^2-x+1)(y^2-y+1)\in Z$$

$$\Rightarrow \text{ac}\vdots\text{bd} \Rightarrow \text{ac}\vdots\text{d} \Rightarrow \text{a}\vdots\text{d} \qquad (2)$$

Vì $(c,d)=1$ nên từ (1) và (2) suy ra

$$a\vdots b \quad \text{suy ra } b=1 \text{ vì } (a,b)=1$$

Vì

$$\frac{x^3+1}{y+1}=\frac{a}{b} \Rightarrow \text{x}^3+1=a(y+1) \Rightarrow \text{x}^3+1\ \vdots\ \text{y}+1 \qquad (3)$$

Mà $x^{2004}-1=(\text{x}^3)^{664}\text{-}1\vdots\ \text{x}^3+1$

Kết hợp với (3) suy ra điều phải chứng minh.

Ví dụ 8. Cho $\text{n}\geq 5$ là số tự nhiên .Chứng minh rằng

$$\left[\frac{(n-1)!}{n}\right]\ \vdots\ \text{n-1}\ .$$

Lời giải

a) Trường hợp 1. n là số nguyên tố

Theo định lý Winson $(n\text{-}1)!\equiv\text{-}1(\text{mod } n)$ suy ra $((n\text{-}1)!+1\ \vdots n$

Ta có

$$\left[\frac{(n-1)!}{n}\right]=\left[\frac{(n-1)!+1}{n}-\frac{1}{n}\right]=\frac{(n-1)!+1}{n}-1 \quad (\text{vì } 0<\frac{1}{n}<1)$$

$$=\frac{(n-1)!-(n-1)}{n}\ \vdots\ (\text{n}-1) \quad \text{vì } (\text{n},\ \text{n}-1)=1$$

b) Trường hợp 2. n là hợp số

+) n không là bình phương của một số nguyên tố.

Khi đó $n=rs$ với $1<r<s<n$.

Do $(n,n\text{-}1)=1$ suy ra $s<n\text{-}1 \Rightarrow (n\text{-}1)!=kn(n\text{-}1)$

suy ra

$$\left[\frac{(n-1)!}{n}\right]=k(n-1)\vdots(n-1).$$

+) $n=p^2$ với p là một số nguyên tố.

Do $p^2 = n, n \geq 5$ suy ra $p \geq 3 \Rightarrow p^2 \geq 3p > 2p+1$

$\Rightarrow 2p < p^2 - 1$ hay 2p < n-1.

Nên $1 < p < 2p < n-1$

Suy ra $(n-1)! \vdots p.2p.(n-1) = 2n(n-1)$.

Từ đo suy ra $\left[\frac{(n-1)!}{n}\right] \vdots (n-1)$.

Vậy ta có điều phải chứng minh.

Ví dụ 9

Tồn tại hay không một số nguyên x sao cho $x^2 + x + 1 \vdots 2003$?

Lời giải

Ta có 2003 là số nguyên tố có dạng $3k + 2$.

Giả sử tồn tại x nguyên thỏa mãn $x^2 + x + 1 \vdots 2003$

Từ đó suy ra tồn tại $a \in \{1,2,....,2002\}$ thỏa mãn $a^2 + a + 1 \vdots 2003$ $(*)$

Ta có

$$a^3 - 1 = (a-1)(a^2 + a + 1) \vdots 2003$$

$$\Rightarrow a^{2001} - 1 \vdots 2003 \quad hay \quad a^{2001} \equiv 1 \ (\text{mod } 2003)$$

$$\Rightarrow a^{2002} \equiv a \ (\text{mod } 2003) \quad (1)$$

Theo định lí Fermat ta có

$$a^{2002} \equiv 1 \ (\text{mod } 2003) \quad (2)$$

Từ (1) và (2) ta có $a \equiv 1 \ (\text{mod } 2003)$ suy ra $a = 1$ (vô lí)

Vậy không tồn tại x nguyên sao thỏa mãn đầu bài.

Ví dụ 10. (30 - 4 - 2006) Chứng minh rằng với mọi m, tồng tại một số nguyên n sao cho

$$n^3 - 11n^2 - 87n + m$$

Chia hết cho 191.

Lời giải

Đặt $P(x) = x^3 - 11x^2 - 87x + m$.

Ta chứng, tồn tại a, b nguyên để $P(x) \equiv (x+a)^3 + b \ (\text{mod } 191)$

$$\Leftrightarrow x^3 + 3ax^2 + 3a^2x + a^3 + b \equiv x^3 - 11x^2 - 87x + m \ (\text{mod } 191)$$

Chọn a nguyên sao cho $3a \equiv -11 \ (\text{mod } 191)$

$$\Leftrightarrow 3a \equiv 180 \ (\text{mod } 191)$$

$$\Leftrightarrow a \equiv 60 \ (\text{mod } 191), \text{ do } (3, 191) = 1,$$

$$\Rightarrow 3a^2 \equiv 3.60^2 \pmod{191} \equiv -87 \pmod{191}$$

Vậy với mọi m, chỉ cần chon $b \equiv m - a^3 \pmod{191}$

là được $P(x) \equiv (x + a)^3 + b \pmod{191}$.

Ta có, với mọi i, j nguyên thì $P(i) \equiv P(j) \pmod{191}$

$$\Leftrightarrow (i + a)^3 \equiv (j + a)^3 \pmod{191}$$

$$\Rightarrow (i + a)^{3.63}(j + a)^2 \equiv (j + a)^{3.63+2} \pmod{191}$$

$$\equiv (j + a) \pmod{191}$$

$$\Rightarrow (j + a)^2 \equiv (i + a)^{189}(j + a)^3 \pmod{191}$$

$$\equiv (i + a)^{192} \pmod{191}$$

$$\equiv (i + a)^2 \pmod{191}$$

$$\Rightarrow (i + a)^{3.63}(j + a)^2 \equiv (i + a)^{189}.(i + a)^2 \pmod{191}$$

$$\equiv i + a \pmod{191}$$

Từ đó suy ra

$$P(i) \equiv P(j) \pmod{191} \Leftrightarrow i = j \pmod{191}$$

Từ đó suy ra tập {P(1), P(2), ..., P(191)} có 191 số dư khác nhau khi chia cho 191

Do đó phải tồn tại một số nguyên $n \in \{1, 2, ..., n\}$ sao cho P(n) ⋮ 191

Vậy ta có điều phải chứng minh.

I.1.3 Bài tập

Bài 1. Chứng minh rằng với mọi số nguyên *m, n* ta có:

1) $n^3 + 11n \vdots 6$

2) $mn(m^2 - n^2) \vdots 3$

3) $n(n + 1)(2n + 1) \vdots 6$.

4) $n^3 + (n + 1)^3 + (n + 2)^3 \vdots 9$.

5) $n^2(n^2 - 12) \vdots 12$

6) $mn(m^4 - n^4) \vdots 30$

7) $n^5 - n \vdots 30$

8) $n^4 + 6n^3 + 11n^2 + 6n \vdots 24$

9) $n^4 - 4n^3 - 4n^2 + 16n \vdots 384$ (n chẵn và $n > 4$)

10) $n^2 + 4n + 3 \vdots 8$

11) $n^3 + 3n^2 - n - 3 \vdots 48$

12) $n^{12} - n^8 - n^4 + 1 \vdots 512$

13) $n^8 - n^6 - n^4 + n^2 \vdots 1152$.

14) $n^3 - 4n \vdots 48$ (n chẵn)

15) $n^2 - 3n + 5$ không chia hết cho 121.

16) $(n + 1)(n + 2)\ldots(2n) \vdots 2n$

17) $n^6 - n^4 - n^2 + 1 \vdots 128$ (n lẻ)

Bài 2. Chứng minh rằng tích của n số nguyên lien tiếp luôn chia hết cho $n!$

Bài 3. Cho p là số nguyên tố lẻ. Chứng minh rằng với mọi $k \in N$, ta luôn có

$S = 1^{2k+1} + 2^{2k+1} + \ldots + (p - 1)^{2k+1}$ chia hết cho p.

Bài 4. Chứng minh rằng nếu $a^3 + b^3 + c^3$ chia hết cho 9 thì một trong ba số *a, b, c* phải chia hết cho 9.

Bài 5. Cho *a, b* nguyên. Chứng minh rằng nếu $a^n \vdots b^n$ thì $a \vdots b$.

Bài 6. Tìm số nguyên dương n sao cho n chia hết cho mọi số nguyên dương không vượt quá $\sqrt{n}$.

Bài 7. Chứng minh rằng $a^2 + b^2 + c^2$ không thể đồng dư với 7 modulo 8.

Bài 8. Tổng n số nguyên liên tiếp có chia hết cho n hay không? tại sao?

Bài 9. Chứng minh rằng không tồn tại cặp số nguyên (x, y) nào thỏa mãn một trong những đẳng thức sau:

a) $x^2 + 1 = 3y$

b) $x^2 + 2 = 5y$.

Bài 10. Chứng minh rằng với $n \geq 1$ thì

$$(n + 1)(n + 2) \ldots (n + n)$$

chia hết cho 2^n.

Bài 11. Tìm chữ số tận cùng của số Fermat $F_n = 2^{2^n} + 1$, $n \geq 2$.

Bài 12. Tìm các số nguyên dương p, q, r sao cho

$$pqr - 1 \vdots (p - 1)(q - 1)(r - 1).$$

Bài 13. Chứng minh rằng tồn tại một số tự nhiên có 1997 chữ số gồm toàn chữ số 1 và 2 sao cho số đó chia hết cho 2^{1997}.

Bài 14. Cho a là một số nguyên dương và $a > 2$. Chứng minh rằng tồn tại vô số số nguyên dương n thỏa mãn

$$a^n - 1 \vdots n.$$

Bài 15. Chứng minh rằng tồn tại vô số số nguyên dương n sao cho

$$2^n + 1 \vdots n.$$

Bài 16. Chứng minh rằng trong 12 số nguyên tố phân biệt bất kì luôn chon ra được 6 số $a_1, a_2, \ldots, a_6$ sao cho

$$(a_1 - a_2)(a_3 - a_4)(a_5 + a_6) \vdots 1800.$$

Bài 17. Cho a, b, c, d nguyên bất kì. Chứng minh rằng

$$(a - b)(a - c)(a - d)(b - c)(b - d)(c - d) \vdots 12.$$

Bài 18. Tìm số tự nhiên n sao cho $2^n - 1$ chia hết cho 7. Chứng minh rằng với mọi số tự nhiên n thì $2^n + 1$ không thể chia hết cho 7.

Bài 19. Tìm số tự nhiên n sao cho $n^5 - n$ chia hết cho 120.

Bai 20. Tìm tất cả các cặp số nguyên $x > 1$, $y > 1$ sao cho

$$\begin{cases} 3x + 1 \vdots y \\ 3y + 1 \vdots x. \end{cases}$$

Bài 21. Cho x_1, x_2 là hai nghiệm của phương trình $x^2 - mx + 1 = 0$ với m là số nguyên lớn hơn 3. Chứng minh rằng với mọi số nguyên dương n thì $S_n = x_1^n + x_2^n$ là một số nguyên và không chia hết cho $m - 1$.

Bài 22. Tìm tất cả các cặp số nguyên dương a, b sao cho

$$\frac{a^2 - 2}{ab + 2}$$

là một số nguyên.

Bài 23. (30.4.2003) Tìm ba số nguyên dương đôi một phân biệt sao cho tích của hai số bất kì đều chia hết cho số thứ 3.

B ài 24. Chứng minh rằng với mọi số tự nhiên n thì giữa n^2 và $(n + 1)^2$ luôn tồn tại ba số tự nhiên phân biệt a, b, c sao cho $a^2 + b^2 \vdots c^2$.

Bài 25. Cho số tự nhiên A_n = 19981998...1998 (gồm n số 1998 viết liền nhau)

a) Chứng minh rằng tồn tại số nguyên dương $n < 1998$ sao cho $A_n \vdots 1999$.

b) Gọi k là số nguyên dương nhỏ nhất sao cho $A_k \vdots 1999$. Chứng minh rằng

$$1998 \vdots 2k.$$

Bài 26. Cho hai số nguyên dương m và n sao cho $n + 2 \vdots m$. Hãy tính số các bộ ba số nguyên dương (x, y, z) sao cho $x + y + z \vdots$ m trong đó mỗi số x, y, z đều không lớn hơn n.

Bài 27. (APMO 98) Tìm số nguyên dương n lớn nhất sao cho n chia hết cho mọi số nguyên dương nhỏ hơn $\sqrt[3]{n}$.

Bài 28. Tìm tất cả các số nguyên dương m, n sao cho $n^3 + 1$ chia hết cho $mn - 1$.

Bài 29. Tìm tất cả các cạp số nguyên dương a, b sao cho

$$\frac{a^2 + b}{ab^2 - 1}$$

là một số nguyên.

Bài 30. Tìm tất cả các cặp số nguyên dương sao cho

$$\frac{a^2b + a + b}{ab^2 + b + 7}$$

là một số nguyên.

Bài 31. Cho n là số nguyên dương lớn hơn 1. p là một ước nguyên tố của số Fermat F_n. Chứng minh rằng $p - 1$ chia hết cho 2^{n+2}.

Bài 32. Cho x, y, p là các số nguyên và $p > 1$ sao cho x^{2002} và y^{2002} đều chia hết cho p. Chứng minh rằng $1 + x + y$ không chia hết cho p.

Bài 33. (USA - 98) Chứng minh rằng với mỗi số nguyên dương $n \geq 2$, tồn tại một tập hợp n số nguyên sao cho với hai số a, b bất kì $(a \neq b)$ thuộc tập đó thì $(a - b)^2$ chia hết ab.

Bài 34. Giả sử tập S = {1, 2, 3, ..., 1998} được phân thành các cặp rời nhau $\{a_i, b_i | 1 \leq i \leq 1998\}$ sao cho $|a_i - b_i|$ bằng 1 hoặc bằng 6. Chứng minh rằng

$$\sum_{i=1}^{999} |a_i - b_i| = 10k + 9.$$

Bài 35. Tìm tất cả các cặp số nguyên dương a, b sao cho

$$\frac{a^2 - 2}{ab + 2}$$

là một số nguyên.

Bài 36. Chứng minh rằng với mọi $n \in N^*$ luôn tồn tại số tự nhiên a sao cho

$$64a^2 + 21a + 7 \vdots 2^n.$$

Bài 37. (Nga - 1999) Cho tập A là tập con của tập các số tự nhiên n sao cho trong 1999 số tự nhiên liên tiếp bất kì luôn có ít nhất một số thuộc A.

Chứng minh rằng tồn tại hai số m, n thuộc A sao cho $m \vdots n$.

Bài 38. Tìm x, y, z nguyên dương và $x < y < z$ sao cho

$$2^x + 2^y + 2^z = 2336.$$

Bài 39. Cho x, y, z là các số nguyên dương thỏa mãn

$$(x - y)(y - z)(z - x) = x + y + z.$$

Chứng minh rằng $x + y + z$ chia hết cho 27.

Bài 40. Cho m, n là các số nguyên dương sao cho $m \le \frac{n^2}{4}$ và mọi ước số nguyên tố của m đều nhỏ hơn hoặc bằng n. Chứng minh rằng

$$n! \vdots m.$$

Bài 41. Tìm tất cả các cặp số nguyên dương a, b sao cho

$$\frac{a^2 + b}{b^2 - a}; \quad \frac{b^2 + a}{a^2 - b}$$

là các số nguyên.

Bài 42. Cho x, y là hai số nguyên dương sao cho $x^2 + y^2 + 1$ chia hết cho xy.

Chứng minh rằng

$$\frac{x^2 + y^2 + 1}{xy} = 3.$$

Bài 43. Cho hàm số $f(x) = x^3 + 17$. Chứng minh rằng mỗi số nguyên dương n luôn tồn tại một số nguyên dương x sao cho $f(x)$ chia hết cho 3^n nhưng không chia hết cho 3^{n+1}.

Bài 44. Cho p là số nguyên tố lớn hơn 2 và $p - 2$ chia hết cho 3. Chứng minh rằng trong tập hợp các số có dạng $x^3 - y^2 + 1$, với x, y là các số nguyên không âm nhỏ hơn p có nhiều nhất $p - 1$ số chia hết cho p.

Bài 45. Chứng minh rằng với mọi n nguyên dương luôn tồn tại một số tự nhiên có n chữ số chia hết cho 2^n và số này chỉ gồm các chữ số 1 và 2.

Bài 46. Cho số nguyên dương $n > 1$, thỏa mãn $3^n - 1$ chia hết cho n. Chứng minh rằng n là số chẵn.

I.2 Ước số chung lớn nhất - Bội số chung nhỏ nhất

I.2.1. Lí thuyết

I.2.1.1. Ước số chung lớn nhất

I.2.1.1.1 Định nghĩa 1

Cho *a, b* là hai số nguyên. Số nguyên dương *d* lớn nhất chia hết cả *a* và *b* được gọi là ước chung lớn nhất của *a* và *b.*

Kí hiệu: d = (*a, b*) hoặc *d* = gcd(*a, b*)

Nếu *d* = 1 thì ta nói *a* và *b* là hai số nguyên tố cùng nhau.

I.2.1.1.2. Các tính chất của ước chung lớn nhất

a) Nếu *p* là một số nguyên tố thì (*p,m*) = *p* hoặc (*p, m*) = 1.

b) Nếu (*a, b*) = *d* thì *a* = *dm*, *b* = *dn* và (*m, n*) = 1.

c) Nếu (*a, b*) = *d, a* = *d'm*, *b* = *d'n* và (*m, n*) = 1 thì *d* = *d'*.

d) Nếu *m* là một ước chung của *a* và *b* thì *m* | (*a,b*).

e) Nếu $p^x \,||\, m$ và $p^y \,||\, n$ thì $p^{\min(x,y)} \,||\, (m, n)$.

f) Nếu *a* = *bq* + *r* thì (*a, b*) = (*r, b*).

g) Nếu *c* | *ab* và (*a,c*) = 1 thì *c* | *b*.

h) Nếu (*a, c*) = 1 thì (*ab, c*) = (*b, c*).

I.2.1.2 Bội số chung nhỏ nhất.

I.2.1.2.1 Định nghĩa.

Cho *a, b* là hai số nguyên. Số nguyên dương nhỏ nhất chia hết cho cả *a* và *b* được gọi là bội số chung nhỏ nhất của *a* và *b*.

Kí hiệu: [*a,b*] hay lcm(*a,b*).

I.2.1.2.2. Các tính chất của bội chung nhỏ nhất.

a) Nếu [*a, b*] = *m* và *m* = *a.a'* = *b.b*' thì (*a', b'*) = 1.

b) Nếu *m'* = *a.a'* = *b.b'* và (*a', b'*) = 1 thì [*a, b*] = *m*.

c) Nếu m = [a, b] và m' là một bội chung của a và b thì m | m'.

d) Nếu *a* | *m* và *b* | *m* thì [*a, b*] | *m.*

e) Cho *n* là một số nguyên dương, ta luôn có *n*[*a, b*] = [*na, nb*].

f) Nếu $a = p_1^{n_1}.p_2^{n_2}...p_k^{n_k}$; $b = p_1^{m_1}.p_2^{m_2}...p_k^{m_k}$

Thì $[a, b] = \prod_{i=1}^{k} p_i^{\min(n_i, m_i)}$.

I.2.1.3 Định lí Bézout

Phương trình $mx + ny = (m,n)$ luôn có vô số nghiệm nguyên.

Nhận xét: Phương trình $ax + by = c$ có nghiệm nguyên khi và chỉ khi c là bội của (a, b).

Phương trình $ax + by = 1$ có nghiệm nguyên khi và chỉ khi $(a, b) = 1$.

I.2.1.4 Mối quan hệ giữa ước số chung lớn nhất và bội số chung nhỏ nhất

Cho a và b là các số nguyên khác 0, ta có

$$[a,b] = \frac{ab}{(a,b)}$$

I.2.2 Các ví dụ

Ví dụ 1. Chứng minh rằng với mọi số nguyên a, b ta luôn có

$$(3a + 5b, 8a + 13b) = (a, b).$$

Lời giải

Ta có $(3a + 5b, 8a + 13b) = (3a + 5b, 8a + 13b - 2(3a + 5b))$

$= (3a + 5b, 2a + 3b) = (a + 2b, 2a + 3b)$

$= (a + 2b, b) = (a, b)$.

Đpcm.

Ví dụ 2. Nếu $(a, b) = d$ thì $(a + b, a - b)$ có thể nhận những giá trị nào?

Lời giải

Ta có $m = (a + b, a - b) = (a + b, 2a) = (a + b, 2b)$.

Do đó m là ước chung của $2a$ và $2b$ và $a + b$.

Nếu a + b lẻ thì (a + b, a - b) = d

Nếu $a + b$ chẵn thì $(a + b, a - b) = 2d$.

Ví dụ 3. Chứng minh rằng phân số sau tối giản

$$\frac{21n + 4}{14n + 3}$$

Lời giải

Ta có $(21n + 4, 14n + 3) = (7n + 1, 14n + 3)$

$= (7n + 1, 14n + 3 – 2(7n + 1))$

$= (7n + 1, 1) = 1$

Từ đó suy ra điều phải chứng minh.

Ví dụ 4. Cho a, b là các số nguyên dương phân biệt sao cho $ab(a + b)$ chia hết cho $a^2 + ab + b^2$. Chứng minh rằng

$$| a – b | > \sqrt[3]{ab}$$

Lời gải

Đặt $g = (a, b) \Rightarrow a = xg$ và $b = yg$ với $(x, y) = 1$.

Khi đó

$$\frac{ab(a+b)}{a^2+ab+b^2} = \frac{gxy(x+y)}{x^2+xy+y^2}$$

là một số nguyên.

Ta có $(x^2 + xy + y^2, x) = (y^2, x) = 1$

$(x^2 + xy + y^2, y) = 1$.

Vì $(x + y, y) = 1$ nên ta có

$(x^2 + xy + y^2, x + y) = (y^2, x + y) = 1$

Do đó $x^2 + xy + y^2 \mid g$

Suy ra $g \geq x^2 + xy + y^2$

Mặt khác $|a - b|^3 = g^3|x - y|^3$

$= g^2|x - y|^3 g$

$\geq g^2.1. (x^2 + xy + y^2) = ab.$

Từ đó ta có điều phải chứng minh.

Ví dụ 5. Cho n là một số nguyên dương, $d = (2n + 3, n + 7)$.

Tìm giá trị lớn nhất của d.

Lời giải

Ta có

$(2n + 3, n + 7) = (2(n + 7) – 2n -3, n + 7)$

$= (11, n + 7) \leq 11.$

Mặt khác khi $n = 11k + 4$ thì $n + 7 = 11(k + 1)$

$\Rightarrow (11, n + 4) = 11.$

Do đó giá trị lớn nhất của d là 11.

Ví dụ 6. (India 1998) Tìm tất cả các bộ (x, y, n) nguyên dương sao cho

$$(x, n+1) = 1 \quad (1)$$

$$\text{và } x^n + 1 = y^{n+1}. \quad (2)$$

Lời giải

Từ (2) ta có

$$x^n = y^{n+1} - 1$$
$$= (y - 1)(y^n + y^{n-1} + \ldots + 1) \quad (*)$$

Đặt $m = y^n + y^{n-1} + \ldots + 1$

Suy ra $x^n \vdots m$

Mà $(x, n+1) = 1$ nên ta phải có $(m, n+1) = 1$

Ta lại có

$$m = y^n - y^{n-1} + 2(y^{n-1} - y^{n-2}) + \ldots + n(y - 1) + n + 1$$
$$= (y - 1)(y^{n-1} + 2y^{n-2} + \ldots + n) + n + 1$$
$$\Rightarrow n + 1 \vdots (m, y - 1)$$

Mà $(m, n + 1) = 1 \Rightarrow (m, y - 1) = 1$ (**)

Từ (*) và (**) suy ra m phải là luỹ thừa n của một số nguyên dương.

Tức là $m = q^n$ với q là một số nguyên dương nào đó

Vì $y > 0$ nên ta có $y^n < y^n + y^{n-1} + \ldots + 1 < y^n + C_n^1 y^{n-1} + \ldots + C_n^n$ với mọi n > 1

hay $y^n < q^n < (y + 1)^n$ với mọi n > 1 (vô lí)

Vậy $n = 1 \Rightarrow x = y^2 - 1$

Vì $(x, n+1) = (x, 2) = 1$ nên $x = 2k + 1 \Rightarrow y$ chẵn

Do đó $(x, y, n) = (4a^2 - 1, 2a, 1)$ với a nguyên dương.

Ví dụ 7. Chứng minh rằng nếu một số nguyên dương có số ước số là lẻ thì đó phải là số chính phương.

Lời giải

Gọi n là số tự nhiên như vậy.

Nhận thấy, nếu d là một ước số của n thì $\frac{n}{d}$ cũng là một ước số của n.

Do vậy nếu với mọi d mà $d \neq \frac{n}{d}$ thì số ước của n phải là chẵn.

Nên tồn tại d là ước của n sao cho $d = \frac{n}{d} \Leftrightarrow n = d^2$ (đpcm).

Ví dụ 8. (APMO - 1999) Tìm số nguyên dương n lớn nhất sao cho n chia hết cho mọi số tự nhiên nhỏ hơn $\sqrt[3]{n}$.

Lời giải

Câu trả lời là 420.

Thật vậy, ta có

$$[1, 2, 3, 4, 5, 6, 7] = 420.\ 7 < \sqrt[3]{420} < 8.$$

Giả sử $n > 420$ và thỏa mãn điều kiện đầu bài $\Rightarrow \sqrt[3]{n} > 7 \Rightarrow n \vdots 420$.

Do đó $n \geq 2.420 = 480 \Rightarrow \sqrt[3]{n} \geq 9$.

Ta có

$$[1, 2, ..., 9] = 2520 \Rightarrow n \vdots 2520 \Rightarrow \sqrt[3]{n} > 13.$$

Gọi m là số nguyên dương lớn nhất nhỏ hơn $\sqrt[3]{n} \Rightarrow n \geq 13$ và $m^3 < n \leq (m+1)^3$.

Do $n \vdots [1, 2, ..., m] \Rightarrow n \vdots [m - 3, m - 2, m - 1, m]$

Mặt khác

$$[m-3, m-2, m-1, m] \geq \frac{m(m-1)(m-2)(m-3)}{6}$$

nên

$$\frac{m(m-1)(m-2)(m-3)}{6} \leq n \leq (m+1)^3$$

suy ra

$$m \leq \frac{6(m+1)^3}{(m-1)(m-2)(m-3)}$$

$$\Leftrightarrow m \leq 6\left(1+\frac{2}{m-1}\right)\left(1+\frac{3}{m-2}\right)\left(1+\frac{4}{m-3}\right)$$

$$\Leftrightarrow f(m) = m - 6\left(1+\frac{2}{m-1}\right)\left(1+\frac{3}{m-2}\right)\left(1+\frac{4}{m-3}\right) \leq 0$$

Mở rộng tập xác định của m trên tập số thực ta dễ dàng chứng minh được f(m) là hàm số đồng biến trên tập $[13; +\infty)$

Do đó với mọi $m \geq 13$ thì $f(m) \geq f(13) > 0$ (vô li)

nên điều giả sử là sai.Từ đó suy ra điều phải chứng minh.

I.2.3 Bài tập

Bài 1. Cho *m, n* là hai số nguyên dương phân biệt và *(m, n) = d.*

Tính $(2006^m + 1, 2006^n + 1)$.

Bài 2. Chứng minh rằng nếu các số *a, b, c* đôi một nguyên tố cùng nhau thì

$$(ab + bc + ca, abc) = 1.$$

Bài 3. Tìm

a) $(21n + 4, 14n + 3)$

b) $(m^3 + 2m, m^4 + 3m^2 + 1)$

c) $[2^n - 1, 2^n + 1]$.

Bài 4. Chứng minh rằng $(2^p - 1, 2^q - 1) = 2^{(p, q)} - 1$.

Bài 5. Cho *a, m, n* là các số nguyên dương, $a > 1$ và $(m, n) = 1$. Chứng minh rằng

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

Bài 6. Chứng minh rằng

$$[1, 2, ..., 2n] = (n +1, n + 2, ..., 2n)$$

Bài 6. Chứng minh rằng với mọi số nguyên dương $m > n$ ta có

$$[m,n]+[m+1,n+1]>\frac{2mn}{\sqrt{m-n}}.$$

Bài 7. Chứng minh rằng dãy 1, 11, 111, ... chứa vô hạn cặp (x_n, x_m) nguyên tố cùng nhau.

Bài 8. Cho *n* là một số nguyên dương, *a* và *b* nguyên dương và nguyên tố cùng nhau. Chứng minh rằng $(\frac{a^n - b^n}{a-b}, a-b)$ bằng 1 hoặc *n*.

Bài 9. Cho *m, n* là các số nguyên dương, *a* là một số nguyên dương lớn hơn 1.

Chứng minh rằng

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

Bài 10. (Hàn Quốc 1998) Tìm tất cả các số nguyên dương *l, m, n* đôi một nguyên tố cùng nhau sao cho

$$(l + m + n)(\frac{1}{l} + \frac{1}{m} + \frac{1}{n})$$

là một số nguyên.

Bài 11. (Canada - 97)Tìm số các cặp số nguyên *a, b* $(a \le b)$ thoả mãn

$$\begin{cases}(a,b)=5!\\ [a,b]=50!\end{cases}$$

Bài 12. (Hungari - 1998) Tìm n nguyên dương sao cho tồn tại các cặp số nguyên a, b thỏa mãn

$$(a, b) = 1998 \text{ và } [a, b] = n!$$

Bài 13. (Nga - 2000) Cho 100 số nguyên dương nguyên tố cùng nhau xếp trên một vòng tròn. Xét phép biến đổi như sau: Với mỗi số nguyên trên vòng tròn ta có thể cộng thêm ước chung lớn nhất của hai số kề bên nó. Chứng minh rằng sau một số hữu hạn phép biến đổi đó, ta có thể thu được các số mới đôi một nguyên tố cùng nhau.

Bài 14. (Hungari - 1997) Cho tập A gồm 1997 số nguyên phân biệt sao cho bất kì 10 số nào trong A cũng có bội chung nhỏ nhất như nhau. Tìm số lớn nhất các số đôi một nguyên tố cùng nhau có thể có trong A.

Bài 15. Cho s và t là các số nguyên dương khác 0. Với cặp (x, y) bất kì, gọi T là phép biến đổi (x, y) thành cặp $(x - t, y - s)$. Cặp (x, y) được gọi là "Tốt" nếu sau hữu hạn phép biến đổi T ta thu được cặp mới nguyên tố cùng nhau.

a) Tìm (s, t) sao cho (s, t) là một cặp "Tôt"

b) Chứng minh rằng với mọi s, t thì luôn tồn tại cặp (x, y) không "Tôt".

Bài 16. Tồn tại hay không các cặp số nguyên dương a, b sao cho

$$(30a + b)(30b + a) = 4^{2001}?$$

I.3. Số nguyên Tố

I.3.1. Lí thuyết

I.3.1.1 Định nghĩa

Một số nguyên dương p được gọi là số nguyên tố, nếu nó chỉ có hai ước số dương là 1 và chính nó.

Nếu p không phải số nguyên tố thì p được gọi là hợp số.

Nhận xét: 2 là số nguyên tố chẵn duy nhất.

I.3.1.2 Định lý 1 (Định lý cơ bản của số học)

Mọi số tự nhiên lớn hơn 1 đều có thể phân tích một cách duy nhất thành tích các thừa số nguyên tố.

I.3.1.3. Định lý 2

Tập hợp các số nguyên tố là vô hạn.

I.3.1.3. Định lý 3

Cho p là một số nguyên tố. Nếu $p \mid ab$ thì $p \mid a$ hoặc $p \mid b$.

(Việc chứng minh các định lý trên khá đơn giản và ta có thể tìm được trong bất kì một quyển sách số học nào, vì vậy sẽ không được trình bày tại đây)

I.3.2 Các ví dụ

Ví dụ 1. Tìm tất cả các số nguyên dương n sao cho các số $3n - 4$, $4n - 5$, $5n - 3$ đều là các số nguyên tố.

Lời giải

Ta có $(3n - 4) + (5n - 3) = 8n - 7$ là số lẻ

Do đó trong hai số trên phải có một số chẵn và một số lẻ.

Nếu $3n - 4$ chẵn thì $3n - 4 = 2 \Leftrightarrow n = 2 \Rightarrow 4n - 5 = 3$ và $5n - 3 = 7$ đều là các số nguyên tố.

Nếu $5n - 4$ chẵn thì $5n - 3 = 2 \Leftrightarrow n = 1 \Rightarrow 3n - 4 = -1$ (loại)

Vậy $n = 2$.

Ví dụ 2. Tìm số nguyên tố p sao cho $8p^2 + 1$ và $8p^2 - 1$ cũng là những số nguyên tố.

Lời giải

Nếu $p = 2$ thì $8p^2 + 1 = 33 \vdots 3$ nên không thỏa mãn.

Nếu $p = 3$ thì $8p^2 + 1 = 73$ và $8p^2 - 1 = 71$ đều là số nguyên tố nên $p = 3$ thỏa mãn

Nếu $p > 3$ và p nguyên tố nên p không chia hết cho 3.

Do đó $p = 3k + 1$ hoặc $p = 3k - 1$

+) $p = 3k + 1 \Rightarrow 8p^2 + 1 = 8(3k + 1)^2 + 1$

$= 72k^2 + 48k + 9 \vdots 3$

Và hiển nhiên $8p^2 + 1 > 3$ nên $8p^2 + 1$ là hợp số.

+) $p = 3k - 1 \Rightarrow 8p^2 + 1 \vdots 3$ và $8p^2 - 1 > 3$ nên không thỏa mãn.

Vậy $p = 3$.

Ví dụ 3. Cho $p \geq 5$ thỏa mãn p và $2p + 1$là số nguyên tố. Chứng minh rằng $4p + 1$ là hợp số.

Lời giải.

+) $p = 3k + 2 \Rightarrow 4p + 1 = 4(3k + 2) + 1 = 12k + 9 \vdots 53 \Rightarrow$ $4p + 1$ là hợp số.

+ $p = 3k + 1 \Rightarrow 2p + 1 = 2(3k + 1) + 1 = 6k + 3 \vdots 3$ (vô lí vì $2p + 1$ là số nguyên tố lớn hơn 11.)

Ví dụ 4. Tìm số nguyên tố p sao cho $2p + 1$ là lập phương của một số tự nhiên.

Lời giải

Ta có $2p + 1 = n^3 \Leftrightarrow 2p = n^3 - 1 = (n - 1)(n^2 + n + 1)$ (*)

Do với mọi số tự nhiên n thì $n^2 + n + 1 > n - 1$ và mọi số nguyên tố p thì $p \geq 2$

Nên từ (*) ta có $\begin{cases} n-1=2 \\ n^2+n+1=p \end{cases}$

Từ đó tìm được $p = 13$.

Ví dụ 5. Chứng minh rằng với mọi số nguyên dương $a > 2$, tồn tại vô số số nguyên dương n sao cho: $a^n - 1 \vdots n$.

Lời giải

Xét dãy số $x_0 = 1, x_{n+1} = a^{x_n} - 1$

Ta sẽ chứng minh với mọi $k \in N$ thì $a^{x_k} - 1 \vdots k$ (*)

+) $n = 0$, hiển nhiên (*)đúng.

+) Giả sử (*)đúng tới $n \le k$, ta có

$a^{x_k} - 1 = m.x_k \Rightarrow a^{x_{x+1}} - 1 = a^{(a^{x_k}-1)} - 1 = a^{mx_k} - 1$

$= (a^{x_k})^m - 1 \vdots a^{x_k} - 1 = x_{k+1}$

Từ đó suy ra (*)được chứng minh.

Do $a > 2$ nên (x_n) là dãy số tăng suy ra (x_n) là dãy số vô hạn.

Đpcm.

Ví dụ 6. Cho p, q là hai số nguyên tố phân biệt. Chứng minh rằng

$$p^{q-1} + q^{p-1} - 1 \vdots pq.$$

Lời giải

Do p và q là hai số nguyên tố phân biệt nên $(p, q) = 1$

Theo định lí Fermat nhỏ ta có $p^{q-1} - 1 \vdots q \Rightarrow p^{q-1} + q^{p-1} - 1 \vdots q$.

Tương tự ta cũng có $p^{q-1} + q^{p-1} - 1 \vdots q$

Do đó ta có điều phải chứng minh.

Ví dụ 7. Biết rằng $2^n - 1$ là một số nguyên tố. Chứng minh rằng n là số nguyên tố.

Lời giải

Do $2^n - 1$ là số nguyên tố nên $n > 1$.

Giải sử n là hợp số

Khi đó $n = pq$ trong đó p và q đều lớn hơn $1 \Rightarrow 2^n - 1 = 2^{pq} - 1 \vdots 2^p - 1$ và $2^q - 1$

Mà $2^p - 1$ và $2^q - 1$ đều lớn hơn 1 nên $2^n - 1$ không phải số nguyên tố (mâu thuẫn)

Vậy ta có điều phải chứng minh.

Ví dụ 8. Chứng minh rằng $a^n + 1$ (a và n nguyên dương) là số nguyên tố thì $n = 2^k$.

Lời giải

Giả sử $n \neq 2^k$ thì $n = 2^m.q$ trong đó q là một số nguyên dương lẻ .

Khi đó $a^n + 1 = a^{2^m q} + 1 = (a^{2^m})^q + 1 = (a^{2^m} + 1)(a^{2^m(q-1)} + ... + 1)$

Suy ra $a^n + 1$ không thể là số nguyên tố (Mâu thuẫn)

Vậy ta có điều phải chứng minh.

Ví dụ 9. Tìm tất cả các số nguyên tố p và q sao cho $p + q = (p - q)^3$.

Lời giải

Vì $(p - q)^3 = p + q \neq 0$ nên p và q phân biệt và $(p, q) = 1$.

Mặt khác ta lại có $p - q \equiv 2p \pmod{p + q}$

Suy ra $8p^3$ chia hết cho $p + q$

Lại có $1 = (p, q) = (p + q, p)$ do đó p^3 và $p + q$ cũng nguyên tố cùng nhau

Nên $8 \vdots p+q \Rightarrow \begin{cases} \left[\begin{array}{l} p+q=2 \\ p+q=4 \\ p+q=8 \end{array}\right. \\ p,q<8. \end{cases}$

Thử trực tiếp được $p = 5$, $q = 3$.

Ví dụ 10. (Baltic 2001). Cho a là số nguyên dương lẻ, m và n là hai số nguyên dương phân biệt. Chứng minh rằng: $(a^{2^n} + 2^{2^n}, a^{2^m} + 2^{2^m}) = 1$.

Lời giải

Giả sử $m > n > 0$.

Gọi p là một ước nguyên tố của $a^{2^n} + 2^{2^n} \Rightarrow a^{2^n} \equiv -2^{2^n} \pmod{p}$ (*)

Bình phương hai vế của (*) $m - n$ lần ta được:

$$a^{2^m} \equiv 2^{2^m} \pmod{p}$$

Do đó $a^{2^m} + 2^{2^m} \equiv 2.2^{2^m} \pmod{p}$ nên p không thể là ước của $a^{2^m} + 2^{2^m}$.

Từ đó suy ra điều phải chứng minh.

Ví dụ 11. (Nga - 2001) Tìm số nguyên dương lẻ $n > 1$ sao cho a và b là hai ước nguyên tố cùng nhau bất kì của n thì $a + b - 1$ cũng là ước của n.

Lời giải

TH1: $n = p^k$ trong đó p là một số nguyên tố thì n thỏa mãn yêu cầu.

TH2: n không là luỹ thừa của một số nguyên tố.

Gọi p là một ước nguyên tố nhỏ nhất của n. Khi đó $n = p^k.s$ và $(p,s) = 1$.

$\Rightarrow p + s - 1 \mid n$

Gọi q là một ước nguyên tố của s thì $q > p$.

Dễ thấy $s < s + p - 1 < s + q \Rightarrow s + p - 1$ không thể chia hết cho q

Từ đó suy ra $(s, s + p - 1) = 1$. Do đó $s + p - 1$ chỉ có ước nguyên tố là p

$$\Rightarrow s + p - 1 = p^c \Rightarrow s = p^c - p + 1$$

Do $p^c \mid n$ và $(p^c, s) = 1$ nên $p^c + s - 1$ là ước của n

$$\Rightarrow 2p^c - p \mid n$$

Vì $(2.p^c - 1, p) = 1$ nên $2p^c - 1$ là ước của s.

Mặt khác ta dễ dàng chứng minh được

$$\frac{p-1}{2} < \frac{p^c - p + 1}{2p^c - 1} < \frac{p+1}{2}$$

Hay

$$\frac{p-1}{2} < \frac{s}{2p^c - 1} < \frac{p+1}{2} = \frac{p-1}{2} + 1$$

Suy ra s không thể chia hết cho $2p^c - 1$.

(mâu thuẫn với giả thiết)

Vậy $n = p^k$ với p là số nguyên tố.

I.3.3 Bài tập

Bài 1. Cho $a \in N^*$. Chứng minh rằng nếu $a^m + 1$ là số nguyên tố thì $m = 2^n$. Điều ngược lại có đúng không?

Bài 2. Giả sử phương trình $x^2 + ax + b + 1 = 0$ ($a, b \in Z$) có nghiệm nguyên. Chứng minh rằng $a^2 + b^2$ là hợp số.

Bài 3. Cho a, b, c là các số nguyên khác 0 và $a \neq c$ thỏa mãn

$$\frac{a}{c} = \frac{a^2 + b^2}{c^2 + b^2}$$

Chứng minh rằng $a^2 + b^2 + c^2$ không phải là số nguyên tố.

Bài 4. Tìm n sao cho $n^4 + 4^n$ là một số nguyên tố.

Bài 5. Cho p là số *n*guyên tố. Chứng minh rằng số

$$\underbrace{11\ldots1}_{p}\underbrace{22\ldots2}_{p}\ldots\underbrace{99\ldots9}_{p} - 123456789$$

chia hết cho p.

Bài 6. Tìm số tự nhiên n sao cho

$$A = n^{2005} + n^{2006} + n^2 + n + 2$$

là một số nguyên tố.

Bài 7. Tìm n nguyên dương để mỗi số sau đây là số nguyên tố:

a) $n^4 + 4$

b) $n^4 + n^2 + 1$.

Bài 8. Chứng minh rằng nếu p là một số nguyên tố lớn hơn 3 thì

$$p^2 - 1 \vdots 24.$$

Bài 9. Cho $2^m - 1$ là một số nguyên tố. Chứng minh rằng m là một số nguyên tố.

Bài 10. Tìm số nguyên tố p sao cho $2p + 1 = a^3$, với a nguyên dương.

Bài 11. Tìm số nguyên tố p sao cho $p + 4$ và $p + 8$ cũng là số nguyên tố.

Bài 12. Tìm số nguyên tố p sao cho $8p^2 + 1$ và $8p^2 - 1$ là những số nguyên tố.

Bài 13. Cho p là một số nguyên tố và $p = 30k + r$. Chứng minh rằng

$r = 1$ hoặc r là một số nguyên tố.

Bài 14. Cho $a \in N^*$, a > 1. Chứng minh rằng $a^n + 1$ là một số nguyên tố thì $n = 2^k$.

Bài 15. (Iran 1998) Cho a, b, x là các số nguyên dương thỏam mãn

$$x^{a+b} = a^b b.$$

Chứng minh rằng $x = a$ và $b = x^x$.

Bài 16. Chứng minh rằng tồn tại một dãy vô hạn $\{p_n\}$ các số nguyên tố phân biệt sao cho $p_n \equiv 1 \pmod{1999^n}$ với mọi $n = 1, 2, ...$

Bài 17. Tìm tất cả các số nguyên tố p sao cho

$$f(p) = (2 + 3) - (2^2 + 3^2) + ... - (2^{p-1} + 3^{p-1}) + (2^p + 3^p) \text{ chia hết cho } 5.$$

Bài 18. (Trung Quốc 2001) Cho các số nguyên dương a, b, c sao cho $a, b, c, a + b - c, c + a - b, b + c - a$ và $a + b + c$ là bảy số nguyên tố phân biệt. d là số các số nguyên phân biệt nằm giữa số bé nhất và lớn nhất trong bảy số đó. Giả sử rằng số 800 là một phần tử của tập $\{a + b, b + c, c + a\}$. Tìm giá trị lớn nhất của d.

Bài 19. Chứng minh rằng với mọi số nguyên a thì luôn tồn tại một dãy vô hạn $\{a_k\}$ sao cho dãy $\{a_k + a\}$ chứa hữu hạn số nguyên tố.

Bài 20. Chứng minh rằng mỗi số tự nhiên đều biểu diễn được dưới dạng hiệu của hai số tự nhiên có cùng số ước nguyên tố.

Bài 21. Cho p là số nguyên tố lẻ và $a_1, a_2, ..., a_{p-2}$ là dãy các số nguyên dương sao cho p không là ước của a_k và $a_k^k - 1$ với mọi $k = 1, 2, ..., p - 2$.

Chứng minh rằng tồn tại một số phần tử trong dãy trên có tich khi chia cho p dư 2.

Bài 22. Chứng minh rằng nếu ước số nguyên tố nhỏ nhất p của số nguyên dương n không vượt quá $\sqrt[3]{n}$ thì $\frac{n}{p}$ là số nguyên tố.

Bài 23. (Balan 2000) Cho dãy các số nguyên tố $p_1, p_2, ...$ thỏa mãn tính chất: p_n là ước nguyên tố lớn nhất của $p_{n-1} + p_{n-2} + 2000$. Chứng minh rằng dãy số trên bị chặn.

Bài 24. Cho $a_1, a_2, ..., a_n$ là các số tự nhiên đôi một khác nhau và có ước nguyên tố không lớn hơn 3. Chứng minh rằng

$$\frac{1}{a_1} + \frac{1}{a_2} + ... + \frac{1}{a_n} < 3.$$

Bài 25. Gọi A là tập các số nguyên tố p sao cho phương trìn

$$x^2 + x + 1 = py$$

có nghiệm nguyên x, y. Chứng minh rằng A là tập vô hạn.

Bài 26. Chứng minh rằng tồn tại vô số số k nguyên dương sao cho $p^2 + k$ là hợp số với mọi số nguyên tố p.

Bài 27. Cho n là số nguyên dương sao cho $n^2 + n + 1$ phân tích được thành tích của 4 số nguyên tố. Chứng minh rằng $n \geq 67$.

Bài 28. Chứng minh rằng không thể phân tích bất kì số nguyên tố nào thành tổng bình phương của hai sô tự nhiên theo hai cách khác nhau.

Bài 29. Tìm ba số nguyên tố p, q, r sao cho $p^2 + q^2 + r^2$ cũng là số nguyên tố.

Bài 30. Tìm các số nguyên tố p sao cho 2^{11p-2} chia hết cho $11p$.

Chương II
CÁC BÀI TOÁN VỀ ĐỒNG DƯ

II.1. Định nghĩa và các tính chất cơ bản của đồng dư

II.1.1. Lí thuyết

II.1.1.1 Định nghĩa

Cho ba số nguyên *a, b, m* ($m \neq 0$). Ta nói *a* đồng dư với *b* theo modulo *n* nếu a – b chia hết cho *m.*

Kí hiệu: $a \equiv b \pmod m$.

II.1.1.2 Các tính chất

a) $a \equiv b \pmod m \Leftrightarrow a - b \vdots m$

b) Nếu $a_i \equiv b_i \pmod m$ với mọi $i = 1, 2, \ldots, n$ thì $\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod m$.

c) Nếu $a \equiv b \pmod m$ và $c \equiv d \pmod m$

thì $a - c \equiv b - d \pmod m$.

d) $a \equiv b \pmod m$ và $b \equiv c \pmod m \Rightarrow a \equiv c \pmod m$.

e) Nếu $a_i \equiv b_i \pmod m$ với mọi $i = 1, 2, \ldots, n$ thì $\prod_{i=1}^{n} a_i \equiv \prod_{i-1}^{n} b_i \pmod m$

f) Nếu $a \equiv b \pmod m$ thì $a^n \equiv b^n \pmod m$.

g) Cho $P(x)$ là đa thức tuỳ ý với hệ số nguyên

nếu $a \equiv b \pmod m$ thì $P(a) \equiv P(b) \pmod m$

Chứng minh

a) Hiển nhiên

b) Do $a_i \equiv b_i \pmod m$ nên ta có $a_i - b_i \vdots m$

Mà $\sum_{i=1}^{n} a_i - \sum_{i=1}^{n} b_i = \sum_{i=1}^{n} (a_i - b_i) \vdots m$

Từ đó suy ra đpcm.

c) Do $a \equiv b \pmod m$ và $c \equiv d \pmod m$

nên $a - b$ và $c - d$ đều chia hết cho m

Mà $(a - c) - (b - d) = (a - b) - (c - d) \equiv o \pmod m$

Suy ra đpcm.

d) Giả sử $a = mq + r$

Vì $a \equiv b \pmod{m}$ nên $b = mp + r$

Vì $b \equiv c \pmod{m}$ nên $c = ml + r$

$\Rightarrow a \equiv b \pmod{m}$.

(Các phần còn lại xin nhường bạn đọc)

II.1.2. Các ví dụ

Ví dụ 1. A và B là hai số có 7 chữ số khác nhau từ 1 đến 7 và $A > B$.

Chứng minh rằng A không chia hết cho B.

Lời giải

Kí hiệu S(n) là tổng các chữ số của n.

Khi đó $S(A) = S(B) = 1 + 2 + \ldots + 7 = 28$.

Mà $A \equiv S(A) \pmod 9$; $B \equiv S(B) \pmod 9$.

Từ đó suy ra $A \equiv B \equiv 1 \pmod 9$.

Giả sử $A \vdots B$ hay $A = pB$, p nguyên dương.

Do $A > B$ nên $p > 1$.

Vì A và B có 7 chữ số khác nhau từ 1 đến 7 nên

$$1111111 < B < A < 7777777$$

Suy ra

$$\frac{A}{B} < 7$$

Từ đó suy ra $1 < p < 7$

Mà $B \equiv 1 \pmod 9$ nên $B = 9k + 1 \Rightarrow A = p(9k + 1) \equiv p \pmod 9$

Mặt khác $A \equiv 1 \pmod 9$ nên $p \equiv 1 \pmod 9$. Vô lí vì $1 < p < 7$.

Vậy điều giả sử là sai.

Suy ra A không chia hết cho B.

Ví dụ 2. Chứng minh rằng 10^{3n+1} không thể biểu diễn thành tổng hai lập phương.

Lời giải

Ta thấy với mọi số nguyên a thì $\left[\begin{array}{l} a^3 \equiv 0 \pmod 7 \\ a^3 \equiv 1 \pmod 7 \\ a^3 \equiv -1 \pmod 7 \end{array}\right.$

Do đó với mọi a, b nguyên thì $\left[\begin{array}{l} a^3 + b^3 \equiv 0 \pmod 7 \\ a^3 + b^3 \equiv \pm 1 \pmod 7 \\ a^3 + b^3 \equiv \pm 2 \pmod 7 \end{array}\right.$

Mà $10^{3n+1} \equiv 3.3^{3n} \equiv 3.27^n \equiv 3(-1)^n \equiv \pm\ 3 \pmod 7$

Nên suy ra đpcm.

Ví dụ 3. Cho 11 số nguyên dương $a_1, a_2, \ldots, a_{11}$. Chứng minh rằng luôn tồn tại các số $x_i \in \{-1, 0, 1\}$, $i = 1, 2, \ldots, 11$ không đồng thời bằng 0 sao cho:

$$x_1a_1 + x_2a_2 + \ldots + x_{11}a_{11} \text{ chia hết cho } 2047.$$

Lời giải

Đặt $S = \{b_1a_1 + b_2a_2 + \ldots + b_{11}a_{11} | \ b_i \in \{0, 1\}\}$.

Khi đó $|S| = 2048$

Do đó khi chia các số của S cho 2047 phải có 2048 số dư.

Vì vậy phải tồn tại hai số trong S mà khi chia cho 2047 có cùng số dư

Giả sử hai số đó là

$$A_m = \sum_{i=1}^{11} b_i a_i, A_n = \sum_{i=1}^{11} c_i a_i \ .$$

Ta có $A_m - A_n \vdots 2047$.

Mà $A_m - A_n = \sum_{i=1}^{11} (b_i - c_i)a_i = \sum_{i=1}^{11} x_i a_i$

Vì $b_i, c_i \in \{0, 1\}$ nên $x_i \in \{-1, 0, 1\}$

Lại có $(b_1, b_2, \ldots, b_{11}) \neq (c_1, c_2, \ldots, c_{11})$ nên x_i không đồng thời bằng 0.

Đpcm.

Ví dụ 4. Xét 100 số tự nhiên liên tiếp 1, 2, …, 100.

Gọi A là số thu được bằng cách xếp một cách tuỳ ý 100 số đó thành một dãy, B là số thu được bằng cách đặt một cách tuỳ ý các dấu cộng vào giữa các chữ số của A. Chứng minh rằng cả A và B đều không chia hết cho 2010.

Lời giải

Kí hiệu $S(n)$ là tổng các chữ số của số tự nhiên n.

Ta thấy từ 1 đến 100 xuất hiện 21 chữ số 1, 20 chữ số 2, 3, 4, 5, 6, 7, 8, 9.

Do đó $S(A) = 21.1 + 20(2 + 3 + \ldots + 9) = 901$

Mà $A \equiv S(A) \equiv 1 \pmod 3$

Nên A không chia hết cho 3 do đó A không chia hết cho 2010.

Giả sử sau khi đã đặt các dấu cộng vào giữa các chữ số của A ta được

$$B = b_1 + b_2 + \ldots + b_n.$$

Khi đó

$$B = b_1 + b_2 + \ldots + b_n \equiv S(b_1) + S(b_2) + \ldots + S(b_n) \pmod 3.$$

Mà $S(b_1) + S(b_2) + \ldots + S(b_n) = S(A) \equiv 1 \pmod 3$

Suy ra $B \equiv 1 \pmod 3$. Do đó B không chia hết cho 2010.

Ví dụ 5. Chứng minh rằng $11^{n+2} + 12^{2n+1}$ chia hết cho 133 với mọi số tự nhiên n.

Lời giải

Ta có $11^{n+2} + 12^{2n+1} = 121.11^n + 12.144^n$

$= 133.11^n + 12(144^n - 11^n)$

Mà $144^n - 11^n \vdots 144\text{-}11 = 133$

Nên ta có đpcm.

Ví dụ 6. Chứng minh rằng $19.8^n + 17$ là hợp số với mọi số tự nhiên n.

Lời giải

Ta có

$$19.8^n + 17 \equiv 19.(-1)^n + 17 \pmod 3$$

Nếu n chẵn thì

$$19.(-1)^n + 17 \equiv 19 + 17 \equiv 0 \pmod 3$$

Mà $19.8^n + 17 > 3$ nên $19.8^n + 17$ là hợp số khi n chẵn.

Nếu $n = 4k + 1$

Ta có

$$\begin{aligned} 19.8^n + 17 &= 19.8^{4k+1} + 17 \\ &\equiv 48.64^{2k} + 17 \pmod{13} \\ &\equiv 48.(-1)^{2k} + 17 \pmod{12} \\ &\equiv 0 \pmod{13} \end{aligned}$$

Do đó $19.8^n + 17$ là hợp số.

Nếu $n = 4k + 3$ thì

$$19.8^{4k+3} + 17 \equiv 0 \pmod 5$$

Tóm lại với mọi n thì $19.8^n + 17$ là hợp số.

Ví dụ 7.(Nga 2000) Tìm các số nguyên tố p và q sao cho $p + q = (p - q)^3$.

Lời giải

Ta có

$$(p - q)^3 = p + q \neq 0$$

Nên p và q là hai số nguyên tố phân biệt.

Ta có

$$\begin{aligned} p - q &\equiv 2p \pmod{p + q} \\ \Rightarrow (p - q)^3 &\equiv 8p^3 \pmod{p + q} \\ \Rightarrow \quad 8p^3 &\equiv 0 \pmod{p + q}. \qquad (*) \end{aligned}$$

Do $(p, q) = 1 \Rightarrow (p, p + q) = 1$

$\Rightarrow (p^3, p + q) = 1$

Từ (*) $\Rightarrow 8 \vdots p + q$

$\Rightarrow p + q \le 8$

Mà $p, q \ge 2$ nên $2 \le q < p \le 5$

Do đó $(p, q) = (5, 3)$.

Ví dụ 8. Cho a là một số nguyên dương lẻ. Chứng minh rằng

$$a^{2^n} + 2^{2^n}, a^{2^m} + 2^{2^m}$$

nguyên tố cùng nhau với moi số nguyên dương $m \neq n$.

Lời giải

Giả sử $m > n$

Gọi p là một ước nguyên tố của $a^{2^n} + 2^{2^n}$

Ta có

$$a^{2^n} \equiv -2^{2^n} \pmod{p} \qquad (*)$$

Bình phương hai vế của (*) $m - n$ lần ta được:

$$a^{2^m} \equiv 2^{2^m} \pmod{p}$$

Do đó $a^{2^m} + 2^{2^m} \equiv 2.2^{2^m} \pmod{p}$ nên p không thể là ước của $a^{2^m} + 2^{2^m}$.

Từ đó suy ra điều phải chứng minh.

II.1.3. Bài tập

Bài 1. Chứng minh rằng với mọi n nguyên dương ta có:

a) $4^{2^n} + 2^{2^n} + 1 \equiv 0 \pmod 7$

b) $2^{2n} + 15n - 1 \equiv 0 (\mathrm{mod}\, 9)$.

Bài 2. Tìm các số tự nhiên *x, y, z* thỏa mãn

$$2^x.3^y + 1 = 17^z.$$

Bài 3. Tìm tất cả các số nguyên dương *n* sao cho $5^n \equiv -1 \pmod{7^{2000}}$.

Bài 4. Chứng minh rằng với mọi *n* lẻ thì

$$1^n + 2^n + ... + n^n \vdots 1 + 2 + ... + n.$$

Bài 5. Cho *p* là số nguyên tố. *a, b* là hai số nguyên bất kì. Chứng minh rằng

$$(a + b)^p \equiv a^p + b^p \pmod p.$$

Bài 6. Cho *a, n* nguyên dương, *p* nguyên tố thỏa mãn

$$2^p + 3^p = a^n$$

Chứng minh rằng $n = 1$.

Bài 7. Tìm *x* nguyên sao cho $|x| \le 1997$ sao cho $x^2 + (x + 1)^2 \vdots 1997$.

Bài 8. Tìm số nguyên dương $n = 2^p 3^q$ sao cho $n + 25$ là một số chính phương.

Bài 9. Cho các số nguyên không âm a_1 , $a_2 < ... < a_{101} < 5050$. Chứng minh rằng tồn tại bốn số nguyên phân biệt sao cho

$$(a_k + a_l - a_m - a_n) \vdots 5050.$$

Bài 10. Chứng minh rằng tồn tại số nguyên dương *a* sao cho mọi số nguyên *k* thì các số $m = k^2 + k - 3a$ và $n = k^2 + k + 1 - 3a$ đều không chia hết cho 2000^{2001}.

Bài 11. Chứng minh rằng tồn tại một số tự nhiên 2001 chữ số gồm toàn chữ số 1, 2 và chia hết cho 2^{2001}.

Bài 12. Chứng minh rằng từ 11 số tự nhiên tuỳ ý luôn chon được ra hai số sao cho hiệu bình phương của chúng chia hết cho 20.

II.2. Định lý Fermat, định lý euler và định lý Wilson

II.2. 1. Hệ thặng dư đầy đủ và hệ thặng dư thu gọn.

II.2.1.1 Định nghĩa 1

Nếu $x \equiv y \pmod m$ ta nói y là một thặng dư của x modulo m.

Tập $S = \{x_1, x_2, \ldots, x_m\}$ được gọi là một hệ thặng dư đầy đủ modulo m nếu mỗi số nguyên y tuỳ ý đều tồn tại duy nhất một số x_i sao cho $y \equiv x_i \pmod m$.

II.2.1.2 Các tính chất cơ bản

+) Tập $\{1, 2, \ldots, m - 1\}$ là một hệ thặng dư đầy đủ modulo m.

+) Mọi hệ thặng dư đầy đủ modulo m đều có đúng m phần tử.

+) Một hệ gồm m phần tử là hệ thặng dư đầy đủ modulo m khi và chỉ khi hai phần tử khác nhau bất kì của nó không đồng dư với nhau modulo m.

+) Mỗi số nguyên m luôn có vô số hệ thặng dư đầy đủ.

+) Với mỗi số nguyên a, $m > 0$. Tập tất cả các số x nguyên thoả mãn $x \equiv a \pmod m$ lập thành một cấp số cộng. Tập hợp này đựpc gọi là một lớp thặng dư modulo m.

+) Với mỗi số nguyên dương m thì luôn có m lớp thặng dư modulo m.

II.2.1.3 Định lí 1

Cho a, b, m là các số nguyên. Khi đó $a \equiv b \pmod m$ thì $(a, m) = (b, m)$.

Chứng minh

Ta có $a \equiv b \pmod m \Rightarrow a - b \equiv 0 \pmod m \Rightarrow a = b + mq$

$\Rightarrow (a, m) = (b + mq, m) = (b, m)$.

Đpcm.

II.2.1.4 Định nghĩa 2

Tập $S = \{x_1, x_2, \ldots, x_n\}$ với các số x_i phân biệt gọi là một hệ thặng dư thu gọn modulo m nếu $(x_i, m) = 1$ với mọi $i = 1, 2, \ldots, n$ và mọi số nguyên y nguyên tố cùng nhau với m đều tồn tại số x_i sao cho $y \equiv x_i \pmod m$.

Nhận xét:

+) Ta có thể thu được một hệ thặng dư thu gọn bằng cách loại ra khỏi hệ thặng dư đầy đủ những số không nguyên tố cùng nhau với m.

+) Mọi hệ thặng dư đầy đủ đều có cùng số phần tử, số phần tử của một hệ thặng dư thu gọn kí hiệu là $\varphi(m)$. $\varphi(m)$ gọi là phi hàm Euler.

+) Nêu p là số nguyên tố thì $\varphi(p) = p - 1$.

+) $\varphi(m)$ bằng số các số nguyên không vượt quá m và nguyên tố cùng nhau với m.

II.2.1.5 Định lí 2

Cho $(a, m) = 1$. Nếu $S = \{x_1, x_2, \ldots, x_n\ 1\}$ là một hệ thặng dư thu gọn (hoặc đầy đủ) modulo m thì $aS = \{ax_1, ax_2, \ldots, ax_n\}$ cũng là một hệ thặng dư thu gọn (hoặc tương ứng đầy đủ) modulo m.

Chứng minh

Ta có $(a, m) = 1 \Rightarrow$ Nếu $ax_i \equiv ax_j \pmod m$ thì $x_i \equiv x_j \pmod m$

Do đó/ với $i \neq j$ thì x_i không đồng dư với $x_j \Rightarrow ax_i$ cũng không đồng dư với $ax_j \pmod m$.

Suy ra các phần tử của của aS đôi một phân biệt theo modulo m.

Mà S và aS có cùng số phần tử do đó nếu S là hệ thặng dư đầy đủ thì aS cũng là hệ thặng dư đầy đủ.

Nếu S là hệ thặng dư thu gọn thì ta chỉ cần chứng minh các phần tử của aS đều nguyên tố cùng nhau với m.

Thật vậy, vì $(a, m) = 1$ và $(x_i, m) = 1$ với mọi $i \Rightarrow (ax_i, m) = 1 \Rightarrow aS$ là hệ thặng dư thu gọn modulo m.

II.2.1.6 Định lí Eurler

Cho a, m là các số nguyên thoả mãn $(a, m) = 1$. Khi đó

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$$

Chứng minh

Gọi $y_1, y_2, \ldots, y_{\varphi(m)}$ là môt hệ thặng dư thu gọn modulo m.

Vì $(a, m) = 1$ nên $ay_1, ay_2, \ldots, ay_{\varphi(m)}$ cũng là một hệ thặng dư thu gọn modulo m.

Do đó, với mọi $i \in \{1, 2, \ldots, \varphi(m)\}$ đều tồn tại duy nhất $j \in \{1, 2, \ldots, \varphi(m)\}$ sao cho $y_i \equiv ay_j \pmod m$.

Từ đó ta có

$$\prod_{i=1}^{\varphi(m)} y_i \equiv \prod_{i=1}^{\varphi(m)} (ay_i) = a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} y_i \pmod m$$

Mà $(y_i, m) = 1$ với mọi i = 1, 2, …, φ (m)

Suy ra $a^{\varphi(m)} \equiv 1 \pmod m$.

II.2.1.7 Định lí Fermat

Cho p là một số nguyên tố, a là một số nguyên bất kì không chia hết cho p. Khi đó

$$a^{p-1} \equiv 1 \pmod p.$$

Chứng minh

Do a không chia hết cho p nên $(a, p) = 1$. Do đó, theo định lí Euler ta có

$$a^{\varphi(p)} \equiv 1 \pmod{p}$$

Mà p là số nguyên tố nên $\varphi(p) = p - 1 \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

đpcm.

+) Nhận xét

Từ định lí Fermat suy ra với mọi số nguyên a và số nguyên tố p thì

$$a^p \equiv a \pmod{p}.$$

II.2.1.7 Định lí Wilson

Cho p là một số nguyên tố. Khi đó

$$(p - 1)! \equiv -1 \pmod{p}$$

(Phần chứng minh của định lí khá đơn giản, xin nhường cho bạn đọc)

II.2.2. Các ví dụ

Ví dụ 1. Cho n là một số tự nhiên bất kì. Chứng minh rằng

$$n^7 - n \equiv 0 \pmod{42}.$$

Lời giải

Do 7 là một số nguyên tố nên, theo định lí Fermat, ta có

$$n^7 - n \equiv 0 \pmod 7. \quad (1)$$

Ta lại có

$$n^7 - n = n(n^6 - 1) = (n - 1)n(n + 1)(n^4 + n^2 + 1) \equiv 0 \pmod 6 \quad (2)$$

Mà (6, 7) = 1 nên từ (1) và (2) suy ra đpcm.

Ví dụ 2. Cho p là một số nguyên tố lớn hơn 7. Chứng minh rằng

$$(3^p - 2^p - 1) \vdots 42p.$$

Lời giải

Ta có

$$3^p - 2^p - 1 = (3^p - 3) - (2^p - 2) \equiv 0 \pmod p. \quad (1)$$

Mặt khác

$$3^p - 2^p - 1 = (3^p - 1) - 2^p \vdots 2 \quad (2)$$

Mà $p > 7 \Rightarrow p$ lẻ

Do đó

$$3^p - 2^p - 1 \equiv - (-1)^p - 1 \equiv 0 \pmod 3 \quad (3)$$

Bây giờ ta cần chứng minh $3^p - 2^p - 1 \vdots 7$

Ta có

$$3^p - 2^p - 1 = 3.3^{p-1} - 2^p - 1$$

$$= 3.9^{\frac{p-1}{2}} - 2^p - 1 \equiv 3.2^{\frac{p-1}{2}} - 2^p - 1 \pmod 7$$

$$= 2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1$$

Do $(p, 3) = 1$ nên $p = 3k + 1$ hoặc $p = 3k + 2$

Nếu $p = 3k + 1$ thì

$$2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1 = 8^k - 1 + 2^{\frac{p+1}{2}} - 2^p \equiv 2^p - 2^{\frac{p+1}{2}} \pmod 7$$

$$= 2^{\frac{p+1}{2}}(2^{\frac{p-1}{2}} - 1) = 2^{\frac{p+1}{2}}(8^k - 1) \equiv 0 \pmod 7$$

Nếu $p = 3k + 2$ ta chứng minh tương tự.

Từ đó suy ra đpcm.

Ví dụ 3. Cho x là một số nguyên tố. Khi đó, phương trình $x^2 \equiv -1 \pmod{p}$ (1) có nghiệm khi và chỉ khi $p = 2$ hoặc $p \equiv 1 \pmod 4$.

Lời giải

Nếu $p = 2$, phương trình có nghiệm $x = 1$.

Nếu $p \equiv 1 \pmod 4 \Rightarrow \frac{p-1}{2}$ là số chẵn

Khi đó ta sẽ chứng minh $x = (\frac{p-1}{2})!$ là một nghiệm của (1).

Thật vậy, ta có

$$\begin{cases} 1 \equiv -(p-1) \pmod p \\ 2 \equiv -(p-2) \pmod p \\ ... \\ \frac{p-1}{2} \equiv -(\frac{p+1}{2}) \pmod p \end{cases}$$

Do đó

$$(\frac{p-1}{2})! \equiv (-1)^{\frac{p-1}{2}} (p-1)(p-1)...\frac{p+1}{2} \pmod{\text{p}}$$

$$\Rightarrow (\frac{p-1}{2}!)^2 \equiv (-1)^{\frac{p-1}{2}}.1.2...(\frac{p-1}{2}).\frac{p+1}{2}...(p-1) \pmod p$$

$$= (-1)^{\frac{p-1}{2}} (p-1)!$$

Mà theo định lí Wilson ta có $(p - 1)! \equiv -1 \pmod p$

$p \equiv 1 \pmod 4$ nên $\frac{p-1}{2}$ là số chẵn

Từ đó suy ra $(-1)^{\frac{p-1}{2}} (p-1)! \equiv -1 \pmod p$

Do đó $x = \frac{p-1}{2}!$ là một nghiệm của (1).

Ngược lại, nếu p là số nguyên tố lẻ và (1) có nghiệm

Khi đó, gọi a là một nghiệm của (1)

Ta có

$$a^{p-1} = (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

Mà theo định lí Fermat, ta có $a^{p-1} \equiv 1 \pmod p$ nên

$$1 \equiv (-1)^{\frac{p-1}{2}} \pmod p$$

suy ra $\frac{p-1}{2}$ chẵn hay $p \equiv 1 \pmod 4$

đpcm.

Ví dụ 4. Cho a, b là hai số nguyên thỏa mãn $24a^2 + 1 = b^2$. Chứng minh rằng có một và chỉ một trong hai số đó chia hết cho 5.

Lời giải

Ta có $24a^2 – b^2 = 1$ không chia hết cho 5 nên a và b không thể cùng chia hết cho 5.

Giả sử a và b cùng không chia hết cho 5

Theo định lí Fermat ta có

$$a^4 – 1 \equiv 0 \pmod 5$$

$$b^4 – 1 \equiv 0 \pmod 5$$

Do đó

$$(a^2 – b^2)(a^2 + b^2) = a^4 – b^4 \equiv 0 \pmod 5$$

Nếu $a^2 + b^2 \equiv 0 \pmod 5$ thì $25a^2 + 1 = a^2 + b^2 \equiv 0 \pmod 5$ (vô lí)

Vậy $a^2 – b^2 \equiv 0 \pmod 5$

$\Rightarrow 23a^2 + 1 = b^2 – a^2 \equiv 0 \pmod 5 \Rightarrow 23a^2 + 1 \equiv 0 \pmod 5$

Vì $(a, 5) = 1$ nên $a \equiv \pm 1 \pmod 5$ hoặc $a \equiv \pm 2 \pmod 5$

Nếu $a \equiv \pm 1 \pmod 5$ thì

$$0 \equiv 23a^2 + 1 \equiv 23(\pm 1)^2 + 1 \equiv -1 \pmod 5 \text{ (vô lí)}$$

Nếu $a \equiv \pm 2 \pmod 5$ thì

$$0 \equiv 23a^2 + 1 \equiv 23(\pm 2)^2 + 1 \equiv 3 \pmod 5 \text{ (vô lí).}$$

Vậy điều giả sử là sai

Từ đó ta có đpcm.

Ví dụ 5. Cho p là một số nguyên tố, a và b là hai số nguyên dương.Chứng minh rằng:

$$ab^p – ba^p \equiv 0 \pmod p.$$

Lời giải

Ta có

$$ab^p – ba^p = ab(b^{p-1} – a^{p-1})$$

Nếu $ab \vdots p$ thì hiển nhiên $ab^p - ba^p \vdots p$.

Nếu ab không chia hết cho $p \Rightarrow (a, p) = (b, p) = 1$

$$\Rightarrow a^{p-1} - 1 \equiv 0 \pmod{p} \text{ và } b^{p-1} - 1 \equiv 0 \pmod{p}$$

$$\Rightarrow a^{p-1} - b^{p-1} \equiv 0 \pmod{p}$$

$$\Rightarrow ab^p - ba^p \equiv 0 \pmod{p}$$

đpcm.

Ví dụ 6. Cho a là một số nguyên. Chứng minh rằng $a^2 + 1$ không có ước nguyên tố dạng $4k + 3$. Từ đó suy ra các phương trình sau không có nghiệm nguyên dương.

a) $4xy - x - y = z^2$

b) $x^2 - y^3 = 7$.

Lời giải

Giả sử $a^2 + 1$ có ước nguyên tố $p = 4k + 3 \Rightarrow (a, p) = 1$.

Khi đó

$$a^{p-1} + 1 = a^{4k+2} + 1 = (a^2)^{2k+1} + 1 \vdots a^2 + 1 \quad (1)$$

Mặt khác, theo định lí Fermat, ta có

$$a^{p-1} - 1 \vdots p \quad (2)$$

Từ (1) và (2) suy ra $2 \vdots p \Rightarrow p = 2$ (vô lí vì 2 không có dạng $4k + 3$)

Vậy $a^2 + 1$ không có ước nguyên tố dạng $4k + 3$.

Áp dụng

a) Ta có

$$4xy - x - y = z^2$$

$$\Leftrightarrow (4x - 1)(4y - 1) = 4z^2 + 1$$

$$\Leftrightarrow (4x - 1)(4y - 1) = (2z)^2 + 1$$

Do $4x - 1 \geq 3$ với mọi x nguyên dương và có dạng $4k + 3$ nên nó có ít nhất một ước nguyên tố dạng $4k + 3$

Mà $(2z)^2 + 1$ không có ước nguyên tố dạng $4k + 3$ nên phương trình trên vô nghiệm.

b) Ta có

$$x^2 - y^3 = 7 \Leftrightarrow x^2 + 1 = y^3 + 8$$

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

Nếu y chẵn thì

$$(y + 2)(y^2 - 2y + 4) \vdots 4$$

$$\Rightarrow x^2 + 1 \vdots 4 \Rightarrow x^2 \equiv -1 \pmod 4 \text{ vô lí}$$

Do đó y lẻ $\Rightarrow y = 4k + 1$ hoặc $y = 4k + 3$

Nếu $y = 4k + 1$

$\Rightarrow y + 2 = 4k + 3$ nên có có ít nhất một ước nguyên tố dạng $4k + 3$.

Mà $x^2 + 1$ không có ước nguyên tố dạng $4k + 3 \Rightarrow$ phương trình trên không có nghiệm trong trường hợp này.

Nếu $y = 4k + 3 \Rightarrow y^2 - 2y + 4 \equiv (-1)^2 - 2(-1) \pmod 4 \equiv 3 \pmod 4$

nên phương trình trên cũng vô nghiệm trong trường hợp này.

Từ đó ta có đpcm.

Ví dụ 7. Cho a, b là các số nguyên. p là một số nguyên tố có dạng 4k + 3. Chứng minh rằng nếu $x^2 + y^2 \vdots p$ thì $x \vdots p$ và $y \vdots p$. Từ đó suy ra phương trình sau vô nghiệm nguyên:

$$x^2 + 2y + 4y^2 = 37$$

Lời giải

Giả sử $p = 4k + 3$ là số nguyên tố thỏa mãn $x^2 + y^2 \vdots p$ nhưng x không chia hết cho $p \Rightarrow x^2$ không chia hết cho $p \Rightarrow y$ không chia hết cho p.

Theo định lí Fermat ta có

$$x^{p-1} - 1 \vdots p \Rightarrow (x^2)^{2k+1} - 1 \vdots p$$

Tương tự, ta cung có

$$(y^2)^{2k+1} - 1 \vdots p$$

suy ra

$$(x^2)^{2k+1} + (y^2)^{2k+1} \equiv 2 \pmod p$$

Mà $(x^2)^{2k+1} + (y^2)^{2k+1} \vdots x^2 + y^2 \vdots p \Rightarrow 2 \vdots p \Rightarrow p = 2$ (vô lí)

Vậy $x \vdots p$ và $y \vdots p$.

Áp dụng

Ta có

$$x^2 + 2x + 4y^2 = 37$$

$$\Leftrightarrow (x+1)^2 + (2y)^2 = 38 \vdots 19 = 4.4 + 3$$

Do đó $x + 1 \vdots 19$ và $2y \vdots 19$.

Vì $x + 1$ và $2y$ không thể cùng bằng 0 nên $|x + 1| \geq 19$ hoặc $|2y| \geq 19$

Khi đó $(x + 1)^2 + (2y)^2 \geq 19^2 > 38$ nên phương trình trên vô nghiệm.

Ví dụ 8. Cho $p \geq 7$, p nguyên tố. Chứng minh rằng số S = 11…1 ($p - 1$ chữ số 1) chia hết cho p.

Lời giải

Ta có

$$S = \frac{10^{p-1} - 1}{9}$$

Vì $p \geq 7$ nên $(10, p) = 1$

Do đó

$$10^{p-1} - 1 \vdots p$$

$$10^{p-1} - 1 \vdots (10 -) = 9$$

Mà $(p, 9) = 1$ nên $10^{p-1} - 1 \vdots 9p$

Từ đó suy ra $S \vdots p$.

đpcm.

Ví dụ 9. [IMO - 2005] Cho dãy số (a_n) xác định như sau

$$a_n = 2^n + 3^n + 6^n - 1 \text{ với } n = 1, 2, \ldots$$

Tìm số tự nhiên nguyên tố cùng nhau với mọi số hạng của dãy trên.

Lời giải

Ta sẽ chứng minh rằng với mọi số nguyên tố p đều tồn tại một số hạng a_n chia hết cho p.

Thật vậy, ta có $a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$ chia hết cho 2 và 3.

Xét $p \geq 5$

Ta có

$$(2, p) = 1; (3, p) = 1; (6, p) = 1$$

Do đó, từ định lí Fermat suy ra

$$2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod{p}$$

Từ đó dễ dàng chứng minh được $6a_{p-2} \vdots p$

Mà $(p, 6) = 1$ nên $a_{p-2} \vdots p$

Do đó chỉ có số 1 là số tự nhiên duy nhất nguyên tố cùng nhau với mọi số hạng của dãy (a_n).

Ví dụ 10. [IMO - 2003] Tìm số nguyên dương k nhỏ nhất sao cho tồn tại các số $x_1, x_2, \ldots, x_k$ sao cho:

$$x_1^3 + x_2^3 + \ldots + x_k^3 = 2002^{2002}.$$

Lời giải

Ta có $2002 \equiv 4 \pmod 9 \Rightarrow 2002^3 \equiv 4^3 \equiv 1 \pmod 9$

$2002^{2002} = (2002^3)^{667}.2002 \equiv 2002 \pmod 9 \equiv 4 \pmod 9$

Mặt khác, với mọi số nguyên a ta có

$$a^3 \equiv \pm 1 \pmod 9 \text{ hoặc } a^3 \equiv 0 \pmod 9$$

Do đó

x_1^3 ; $x_1^3 + x_2^3$; $x_1^3 + x_2^3 + x_3^3$ không thể đồng dư với 4 modulo 9 được.

Tức là với $k \le 3$ thì phương trình trên không có nghiệm nguyên.

Ta sẽ chứng minh $k = 4$ là giá trị cần tìm.

Thật vậy, ta có $2002 = 10^3 + 10^3 + 1^3 + 1^3$

Mà $2002 = 3.667 + 1$

$$\Rightarrow 2002^{2002} = 2002.(2002^{667})^3$$
$$= (10^3 + 10^3 + 1^3 + 1^3)(2002^{667})^3$$
$$= (10.2002^{667})^3 + (10.2002^{667})^3 + (2002^{667})^3 + (2002^{667})^3$$

Vậy với $k = 4$ thì phương trình trên có nghiệm.

KL: $k = 4$ là giá trị cần tìm.

Ví dụ 11. (Balan - 98) Cho dãy số (a_n) được xác định như sau:

$$a_1 = 1, \quad a_n = a_{n-1} + a_{[\frac{n}{2}]} \text{ với mọi } n \ge 2.$$

Chứng minh rằng dãy (a_n) có vô số số hạng chia hết cho 7.

Lời giải

Giả sử trong dãy trên có hữu hạn số hạng chia hết cho 7.

Khi đó gọi a_k là số hạng cuối cùng của dãy chia hết cho 7.

Điều này là tồn tại vì có $a_5 = 7 \vdots 7$.

Ta có

$$a_{2k} = a_{2k-1} + a_k; \quad a_{2k+1} = a_{2k} + a_k.$$

Do đó

$$a_{2k+1} \equiv a_{2k} \equiv a_{2k-1} \equiv x \pmod 7.$$

Với $x \vdots 7$.

Mặt khác

$$a_{4k-2} = a_{4k-3} + a_{2k-1} \equiv a_{4k-3} + x \pmod 7$$
$$a_{4k-1} = a_{4k-2} + a_{2k-1} \equiv a_{4k-2} + x \pmod 7 \equiv a_{4k-3} + 2x \pmod 7$$
$$a_{4k} = a_{4k-1} + a_{2k} \equiv a_{4k-3} + 3x \pmod 7$$
$$a_{4k+1} = a_{4k} + a_{2k} \equiv a_{4k-3} + 4x \pmod 7$$
$$a_{4k+2} = a_{4k+1} + a_{2k+1} \equiv a_{4k-3} + 5x \pmod 7.$$

$$a_{4k+3} = a_{4k+2} + a_{2k+1} \equiv a_{4k-3} + 6x \pmod 7$$

Ta có $a_{4k-3} \vdots 7$ và $x \vdots 7$ nên trong các số $a_{4k-3} + ix$ (i = 1, 2, …, 6.) phải có số chia hết cho 7 nên trong các số a_{4k-3+i}, i = 1, 2, …, 6 phải có số chia hết cho 7.

Vậy điều giả sử là sai

Từ đó ta có điều phải chứng minh.

Ví dụ 12. Chứng minh rằng nếu p là một số nguyên tố thì $(p - 2)! - 1 \vdots p$.

Nếu $p > 5$ thì $(p - 2)! - 1$ không là luỹ thừa của p.

Lời giải

Theo định lí Wilson ta có

$$(p - 1)! \equiv -1 \pmod p \equiv p - 1 \pmod p$$

$$\Leftrightarrow (p - 1)(p - 2)! \equiv p - 1 \pmod p \quad (*)$$

Do $(p, p - 1) = 1$ nên

$$(*) \Leftrightarrow (p - 2)! \equiv 1 \pmod p$$

Với $p > 5$, giả sử $(p - 2)! - 1 = p^n$

Ta có

$$(p - 2)! \vdots p - 1 \Rightarrow p^n + 1 \vdots p - 1$$

Mà

$$p^n + 1 = (p^n - 1) + 2 \equiv 2 \pmod{p - 1}$$

$$\Rightarrow 2 \equiv 0 \pmod{p - 1}$$

Vô lí vì $p > 5$

Vậy có điều phải chứng minh.

Ví dụ 13.

a) Cho a là một số nguyên dương. Chứng minh rằng mọi ước nguyên tố p của $a^2 + 1$ với $p > 2$ thì p đều có dạng $4k + 1$.

b) Chứng minh rằng có vô số số nguyên tố có dạng $4k + 1$.

Lời giải

1) Giả sử p là số nguyên tố dạng $4k + 3$ và $p \mid a^2 + 1$

Khi đó

$$a^2 \equiv -1 \pmod p \Rightarrow (a^2)^{\frac{p-1}{2}} = (a^2)^{2k+1} \equiv -1 \pmod p$$

Mặt khác theo định lí Fermat, ta có

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

Do đó

$$2 \equiv 0 \pmod{p}$$

Vô lí vì $p > 2$

Vậy có điều phải chứng minh

b) Theo phần a) ta có mọi ước nguyên tố của $(n!)^2 + 1$ đều có dạng $4k + 1$

Giả sử có hữu hạn ước nguyên tố dạng $4k + 1$ khi đó gọi p là số nguyên tố lớn nhất có dạng $4k + 1$.

Ta có mọi ước nguyên tố lớn hơn 2 của $(p!)^2 + 1$ đều có dạng $4k + 1$ và đều không lớn hơn p (do p lớn nhất dạng $4k + 1$)

$((p!)^2 + 1, q) = 1$ với mọi $q \le p$ dó đó $(p!)^2 + 1$ không có ước nguyên tố nhỏ hơn hoặc bằng p (vô lí)

Vậy ta có điều phải chứng minh.

Ví dụ 14. Chứng minh rằng với mọi số nguyên tố p, tồn tại vô hạn các số nguyên dương n sao cho

$$2^n - n \vdots p \qquad (*)$$

Lời giải

Nếu $p = 2$ thì mọi n chẵn đều thỏa mãn (*)

Nếu $p > 2$, theo định lí Fermat, ta có

$$2^{p-1} \equiv 1 \pmod{p}$$

$$\Leftrightarrow 2^{m(p-1)} \equiv 1 \bmod p$$

Chọn $m = kp - 1$, $n = m(p - 1) = (kp - 1)(p - 1) \equiv 1 \pmod{p}$

Khi đó

$$2^n - n = 2^{m(p-1)} - n \equiv 1 - 1 \equiv 0 \pmod{p}$$

Từ đó suy ra đpcm.

Ví dụ 15. (Bulgarian – 95) Tìm số các số tự nhiên $n > 1$ sao cho

$$a^{25} - a \equiv 0 \pmod{n}$$

Với mọi số tự nhiên a.

Lời giải

Với mọi số nguyên tố p thì

$$(p^2, p^{25} - p) = p \Rightarrow p^{25} - p \vdots p$$

Do đó $n \vdots p^2$ với mọi p nguyên tố.

suy ra n là tích của các số nguyên tố phân biệt

(Số tự nhiên như vậy được gọi là số **squarefree**)

Mặt khác

$$2^{25} - 2 = 2.3^2.5.7.13.17.241$$

Nhưng n không thể chia hết cho 17 và 241 vì

$$3^{25} - 3 \equiv -6 \pmod{17}$$

$$\text{và } 3^{25} - 3 \equiv 29 \pmod{241}$$

Bây giờ ta xét $p = 2, 3, 5, 7, 13$.

+) $p = 2$, ta có với mọi a nguyên thì $a^{25} - a \vdots 2$.

+) $p = 3$. Nếu $a \vdots 3$ thì $a^{25} - a \vdots 3$

Nếu $a \vdots 3 \Rightarrow a^2 \equiv 1 \pmod 3 \Rightarrow a^{25} = (a^2)^{12}.\, a \equiv a \pmod 3$

$\Rightarrow a^{25} - a \vdots 3.$

Tương tự cho $p = 5, 7, 13$ thì $a^{25} - a \vdots p$ với mọi a nguyên.

Do đó n chính là tích của k $(1 \le k \le 5)$ số trong 5 số trên

Từ đó suy ra có $2^5 - 1 = 31$ số tự nhiên như vậy

Ví dụ 16. Cho $n \ge 5$ là số tự nhiên .Chứng minh rằng

$$\left[\frac{(n-1)!}{n}\right] \vdots\ n\text{-}1\ .$$

Lời giải

a) Trường hợp 1. n là số nguyên tố

Theo định lý Winson $(n\text{-}1)! \equiv -1 \pmod n$ suy ra $((n\text{-}1)!+1 \vdots n$

Ta có

$$\left[\frac{(n-1)!}{n}\right] = \left[\frac{(n-1)!+1}{n} - \frac{1}{n}\right] = \frac{(n-1)!+1}{n} - 1 \quad (\text{vì } \ 0 < \frac{1}{n} < 1)$$

$$= \frac{(n-1)!-(n-1)}{n} \ \vdots (\text{n - 1}) \qquad \text{vì } (n,\ n - 1) = 1$$

b) Trường hợp 2. n là hợp số

+) n không là bình phương của một số nguyên tố.

Khi đó $n = rs$ với $1 < r < s < n$.

Do $(n,n\text{-}1)=1$ suy ra $s < n\text{-}1 \Rightarrow$ $(n\text{-}1)! \vdots rs(n\text{-}1) = n(n\text{-}1)$ hay $(n\text{-}1)! = kn(n\text{-}1)$

suy ra

$$\left[\frac{(n-1)!}{n}\right] = k(n-1) \vdots (n-1).$$

+) $n = p^2$ với p là một số nguyên tố.

Do $p^2 = n, n \geq 5$ suy ra $p \geq 3$ $\Rightarrow p^2 \geq 3p > 2p+1$

$\Rightarrow 2p < p^2 - 1$ hay $2p < n$-1

Nên $1 < p < 2p < n$-1

Suy ra $(n$-1)! ⋮ $p.2p.(n$-1) = $2n(n$-1).

Từ đo suy ra $\left[\frac{(n-1)!}{n}\right] \vdots (n-1)$.

Vậy ta cố điều phải chứng minh.

II.2.3. Bài tập

Bài 1.

a) Cho a là số nguyên sao cho $(a, 7) = 1$. Chứng minh rằng

$$a^{12} - 1 \vdots 7.$$

b) a là số nguyên dương sao cho $(a, 240) = 1$. Chứng minh rằng

$$a^4 - 1 \vdots 240.$$

Bài 2. Cho $a_1 + a_2 + ... + a_n \vdots 30$, và $a_1, a_2, ..., a_n$ nguyên. Chứng minh rằng

$$a_1^5 + a_2^5 + ... + a_n^5 \vdots 30.$$

Bài 3. Chứng minh rằng

$$n^7 - n \vdots 42$$

với mọi số nguyên n.

Bài 4. Cho n nguyên dương. Chứng minh rằng

a) $2^{3^{4n+1}} + 3 \vdots 11$.

b) $2^{2^{10n+1}} + 19 \vdots 23$.

c) $2^{2^{6n+2}} \equiv 16 \pmod{37}$.

Bài 5. Cho p là số nguyên tố lớn hơn 17. Chứng minh rằng

$$P^{16} \equiv 1 \pmod{16320}.$$

Bài 6. Cho p là số nguyên tố lẻ. Chứng minh rằng

$$2(p-3)! \equiv -1 \pmod{p}.$$

Bài 7. Cho n là hợp số, $n \neq 4$. Chứng minh rằng $(n - 1)! \equiv 0 \pmod{n}$.

Bài 8. Cho p và q là hai số nguyên tố phân biệt. Chứng minh rằng

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

Bài 9. Cho a, b là các số nguyên, p là số nguyên tố. Chứng minh rằng

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

Bài 10. Chứng minh rằng n và $n + 2$ là cặp số nguyên tố sinh đôi khi và chỉ khi

$$4[(n - 1)! + 1] + n \equiv 0 \pmod{n(n + 2)}.$$

Bài 11. Cho p là một số nguyên tố lẻ. Chứng minh rằng số $m = \dfrac{9^p - 1}{8}$ là một hợp số lẻ, không chia hết cho 3 và $3^{m-1} \equiv 1 \pmod{m}$.

Bài 12. Chứng minh rằng với mọi số nguyên tố p, tồn tại vô hạn số nguyên dương n thỏa mãn

$$2^n - n \vdots p.$$

Bài 13. Tìm tất cả các số nguyên tố p sao cho

$$5^{2p^2} \equiv 1 (\bmod p)$$

Bài 14. Cho a, b là hai số nguyên dương sao cho $2a - 1$, $2b - 1$ và $a + b$ đều là các số nguyên tố. Chứng minh rằng $a^a + b^b$ và $a^b + b^a$ đều không chia hết cho $a + b$.

Bài 15. Tìm số nguyên dương n sao cho $n = a^2 + b^2$ với a, b là hai số nguyên dương nguyên tố cùng nhau và ab chia hết cho mọi số nguyên tố nhỏ hơn hoặc bằng $\sqrt{n}$.

Bài 16. Cho p là một số nguyên tố lẻ. Chứng minh rằng không tồn tại x, y nguyên thỏa mãn hệ thức

$$x^p + y^p = p[(p - 1)!]^p.$$

Bài 17. Tìm ba số nguyên tố p, q, r sao cho $p^2 + q^2 + r^2$ cũng là số nguyên tố.

II.3. Số chính phương mod p

II.3.1. Lí thuyết

II.3.1.1 Định nghĩa 1

Cho số nguyên tố p. Số nguyên a được gọi là số chính phương (mod p) nếu tồn tại số nguyên x sao cho $x^2 \equiv a \pmod p$.

Nhận xét:

+) Mọi số chính phương đều là số chính phương (mod p)

+) $a \equiv 0 \pmod p$ thì $a^2 \equiv a \pmod p$ nên mọi $a \equiv 0 \pmod p$ đều là số chính phương (mod p). Do đó, từ đây về sau, ta chỉ xét số nguyên a sao cho $(a, p) = 1$.

+) Mọi số nguyên lẻ đều là số chính phương (mod 2)

II.3.1.2 Kí hiệu Legendre

Cho p là số nguyên tố lẻ.

$\left(\frac{a}{p}\right) = 1$ nếu a là số chính phương mod p

$\left(\frac{a}{p}\right) = -1$ nếu a không là số chính phương mod p.

Kí hiệu trên gọi là kí hiệu **Legendre**.

II.3.1.3 Định lí 1

Cho p là một số nguyên tố lẻ. Khi đó

$$\left(\frac{a}{p}\right) = 1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p \quad (1)$$

$$\left(\frac{a}{p}\right) = -1 \Leftrightarrow a^{\frac{p-1}{2}} \equiv -1 \pmod p \quad (2)$$

Chứng minh

Giả sử a là số chính phương mod p, khi đó, tồn tại số tự nhiên x sao cho

$$x^2 \equiv a \pmod p$$

Do $(a, p) = 1$ nên $(x, p) = 1$.

Theo định lí Fermat ta có

$$1 \equiv x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod p$$

Ngược lại, nếu có (1) thì với mỗi $k \in \{1, 2, \ldots, p - 1\}$ có duy nhất một số $k' \in \{1, 2, \ldots, p - 1\}$ sao cho $k.k' \equiv a \pmod p$

Nếu tồn tại $k = k'$ thì $k.k' = k^2 \equiv a \pmod p \Rightarrow a$ là số chính phương (mod p).

Trái lại, tập $\{1, 2, \ldots, p - 1\}$ được chia thành $\frac{k-1}{2}$ tập con $\{k, k'\}$ rời nhau sao cho $k.k' \equiv a \pmod p$. $\Rightarrow (p - 1)! \equiv a^{\frac{p-1}{2}} \equiv 1 \pmod p$

Mặt khác, theo định lí Wilson, ta có

$$(p - 1)! \equiv -1 \pmod p$$

Từ đó suy ra

$$1 \equiv -1 \pmod p \Rightarrow p = 2 \text{ (vô lí vì } p \text{ lẻ)}$$

Vậy (1) được chứng minh xong.

Theo định lí Fermat, ta có $a^{p-1} \equiv 1 \pmod p$

$$\Rightarrow \left[\begin{array}{l} a^{\frac{p-1}{2}} \equiv 1 \pmod p \\ a^{\frac{p-1}{2}} \equiv -1 \pmod p \end{array}\right.$$

Do đó, (2) được chứng minh.

II.3.1.4 Định lí 2 (Bổ đề Gauss)

Cho p là số nguyên tố lẻ, a là số nguyên, $(a, p) = 1$. Xét tập

$$\{ka \mid k = 1, 2, \ldots, \frac{p-1}{2}\}.$$

Gọi $r_k \equiv ka \pmod p$, $1 \le r_k \le p$.

Gọi n là số các số r_k thuộc khoảng $(\frac{p}{2}; p)$. Khi đó $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$.

(n chính là số bội số của a trong khoảng $(\frac{p}{2}; p)$)

Chứng minh

Ta có

$$ka \equiv r_k \pmod p$$

Cho k chạy từ 1 đến $(p - 1)/2$ rồi nhân các đẳng thức đó lại ta được:

$$\frac{p-1}{2}! a^{\frac{p-1}{2}} \equiv \prod_{k=1}^{\frac{p-1}{2}} r_k \pmod p$$

Gọi $A = \left\{ r_k \mid r_k > \frac{p}{2} \right\}$; $B = \left\{ r_k \mid r_k < \frac{p}{2} \right\}$

Khi đó

$$\prod_{k=1}^{\frac{p-1}{2}} r_k = \prod_{r_k \in A} r_k \prod_{r_k \in B} r_k \equiv (-1)^n \prod_{r_k \in A} (p - r_k) \prod_{r_k \in B} r_k \pmod p$$

Ta có với mọi $r_k \in A$ thì $p - r_k \le \frac{p-1}{2}$.

Mặt khác Nếu $r_i \in A$, $r_j \in B$ thì $p - r_i \ne r_j$ vì nếu $p - r_i = r_j$ thì $r_i + r_j = p$

$\Rightarrow a(i + j) \equiv 0 \pmod p \Rightarrow i + j \equiv 0 \pmod p$.

Điều này không thể vì i và j thuộc $(1; \frac{p-1}{2})$ nên $1 < i + j < p$.

Từ đó suy ra $\frac{p-1}{2}! a^{\frac{p-1}{2}} \equiv \prod_{k=1}^{\frac{p-1}{2}} r_k \equiv (-1)^n \frac{p-1}{2}!$ (*)

Mà $(\frac{p-1}{2}!, p) = 1$ nên từ (*) suy ra $a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$

đpcm.

Từ đó ta có một số hệ quả quan trọng sau.

Hệ quả 1. Cho p là số nguyên tố lẻ. Gọi n là số các số chẵn thuộc $(\frac{p}{2}; p)$ thì ta có

$$2^{\frac{p-1}{2}} \equiv (-1)^n \pmod p.$$

Chứng minh

Từ định lí 2, cho $a = 2$ ta có điều phải chứng minh.

Hệ quả 2. Cho p là số nguyên tố lẻ. Khi đó

$$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$$

Chứng minh

(Hiển nhiên)

Hệ quả 3. Cho p là số nguyên tố lẻ. Khi đó

$$(\frac{2}{p}) = 1 \Leftrightarrow p \equiv \pm 1 \pmod 8$$

$$\text{và} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Chứng minh

Giả sử $p = 4k + 1$, tập các số chẵn trong khoảng $(0; p)$ là $\{2i \mid 1 \le i \le 2k\}$

Khi đó, số các số chẵn trong khoảng $(\frac{p}{2}; p)$ là $n = k$.

Tương tự như vậy, nếu $p = 4k - 1$ thì ta cũng tính được số các số chẵn trong khoảng $(\frac{p}{2}; p)$ là $n = k$.

Do đó, theo hệ quả 1, ta có

$$2^{\frac{p-1}{2}} \equiv (-1)^n (\text{mod } p) \equiv (-1)^k (\text{mod p})$$

2 là số chính phương mod $p \Leftrightarrow 1 \equiv 2^{\frac{p-1}{2}} \equiv (-1)^k (\text{mod } p)$

$\Leftrightarrow k$ chẵn $\Leftrightarrow$ p $\equiv \pm 1$ (mod p).

2 không là số chính phương mod $p \Leftrightarrow k$ lẻ $\Leftrightarrow p \equiv \pm 3 (\text{mod } p)$

đpcm.

Hệ quả 4. Cho p là số nguyên tố lẻ. Gọi n là số các bội của 3 trong khoảng $(\frac{p}{2}; p)$. Khi đó

$$3^{\frac{p-1}{2}} \equiv (-1)^n (\text{mod } p)$$

Chứng minh

Được suy ra hiển nhiên từ định lí, trong trường hợp $a = 3$.

Hệ quả 5. Cho p là số nguyên tố có dạng $6k \pm 1$. Khi đó, 3 là số chính phương mod p khi và chỉ khi $p \equiv \pm 1 (\text{mod } 12)$.

Chứng minh

Giả sử $p = 6k + 1$. Tập hợp các số là bội của 3 trong khoảng $(0; p)$ là

$$\{3i \mid 1 \le i \le 2k\}$$

Mà

$$3i > \frac{p}{2} \Leftrightarrow i > \frac{p}{6} = k + \frac{1}{6} \Leftrightarrow i \ge k + 1$$

Do đó, số các số là bội của 3 trong khoảng $(\frac{p}{2}; p)$ là $n = k$.

Tương tự khi $p = 6k - 1$, ta cũng chứng minh được $n = k$.

Vậy trong cả hai trường hợp ta đều chứng minh được số các số là bội của 3 trong khoảng $(\frac{p}{2}; p)$ là $n = k$.

Vì vậy, theo hệ quả 4, ta có

$$3^{\frac{p-1}{2}} \equiv (-1)^n \pmod p \equiv (-1)^k \pmod p$$

$$\Rightarrow (\frac{3}{p}) = 1 \Leftrightarrow (-1)^k \equiv 1 \pmod p$$

$$\Leftrightarrow k \text{ chẵn}$$

$$\Leftrightarrow p \equiv \pm 1 \pmod{12}.$$

đpcm.

II.3.1.5 Định lí 2

Cho p là số nguyên tố. $a \equiv b \pmod p$, $(a, p) = (b, p) = 1$. Khi đó

$$(\frac{a}{p}) = (\frac{b}{p}).$$

Chứng minh

Do $a \equiv b \pmod p \Rightarrow a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod p \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$

đpcm.

II.3.1.5 Định lí 4

Cho p là một số nguyên tố. $a_1, a_2, \ldots, a_n$ là các số nguyên không chia hết cho p. Khi đó

$$(\frac{a_1 a_2 \ldots a_n}{p}) = (\frac{a_1}{p})(\frac{a_2}{p})\ldots(\frac{a_n}{p})$$

Chứng minh

(Phần chứng minh khá đơn giản, xin nhường cho bạn đọc)

II.3.1.6 Định lí 5

Cho p là số nguyên tố lẻ, a là số nguyên không chia hết cho p. Khi đó

$$a^{\frac{p-1}{2}} \equiv (-1)^s \pmod p$$

Với s = $\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]$

Chứng minh

Gọi *n* là số các bội của a trong khoảng $(\frac{p}{2}; p)$, theo định lí 2, ta có

$$a^{\frac{p-1}{2}} \equiv (-1)^n \pmod p$$

Vì vậy, ta chỉ cần chứng minh $s - n$ là số chẵn.

(Phần này khá đơn giản, xin nhường lại cho bạn đọc).

II.3.1.6 Định lí 7 (Luật tương hỗ Gauss)

Cho *p, q* là hai số nguyên tố lẻ phân biệt.

Khi đó:

a) Nếu có ít nhất một trong hai số có dạng $4k + 1$ thì

$$(\frac{p}{q}) = (\frac{q}{p}).$$

b) Nếu cả hai số có dạng $4k + 3$ thì

$$(\frac{p}{q}) = -(\frac{q}{p}).$$

Chứng minh

a) Đặt

$$s_1 = \sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right]; \quad s_2 = \sum_{i=1}^{\frac{q-1}{2}} \left[\frac{ip}{q}\right]$$

Khi đó

$$s_1 + s_2 = (\frac{p-1}{2})(\frac{q-1}{2})$$

(tính chất này đã được chứng minh trong tài liệu "Một số bài toán về phần nguyên " của cùng tác giả).

Do *p* hoặc *q* có dạng $4k + 1$ nên $(\frac{p-1}{2})(\frac{q-1}{2})$ là số chẵn.

Nên s_1 và s_2 có cùng tính chẵn lẻ.

Theo định lí 5, ta có

$$q^{\frac{p-1}{2}} \equiv (-1)^{s_1} \pmod p$$

$$p^{\frac{q}{2}} \equiv (-1)^{s_2} \pmod q$$

Từ đó dễ dàng suy ra điều phải chứng minh.

b) Chứng minh tương tự.

II.3.2. Các ví dụ

Ví dụ 1. Cho p là số nguyên tố có dạng $8k + 5$ hoặc $8k + 7$. x, y là hai số nguyên thỏa mãn $x^2 + 2y^2$ chia hết cho p.

Chứng minh rằng $x \vdots p$ và $y \vdots p$.

Lời giải

Giả sử ngược lại $x \not\vdots p \Rightarrow 2y^2 \not\vdots p \Rightarrow y \not\vdots p$.

Mà

$$x^2 + 2y^2 \vdots p \Rightarrow x^2 \equiv -2y^2 \pmod p$$

$$\Rightarrow \left(\frac{x^2}{p}\right) = \left(\frac{-2y^2}{p}\right)$$

$$\Rightarrow 1 = \left(\frac{-2}{p}\right)\left(\frac{y^2}{p}\right) = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right). \quad (1)$$

Nếu $p = 8k + 5 \Rightarrow \begin{cases} \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \\ \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1 \end{cases}$

Thay vào (1) được 1 = -1 (vô lí).

Nếu $p = 8k + 1 \Rightarrow \begin{cases} \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = -1 \\ \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = 1 \end{cases}$ cũng không thoả mãn (1)

Vậy điều giả sử là sai

Từ đó suy ra đpcm.

Ví dụ 2. Cho $k = 2^{2^n} + 1$ với n nguyên dương. Chứng minh rằng k là số nguyên tố khi và chỉ khi k là ước của $3^{\frac{k-1}{2}} + 1$.

Lời giải

Nếu k là ước của $3^{\frac{k-1}{2}} + 1$ thì ta có

$$3^{\frac{k-1}{2}} \equiv -1 \pmod{k} \quad (1)$$

$$\Leftrightarrow 3^{k-1} \equiv 1 \pmod{k} \quad (2)$$

Gọi d là bậc của 3 modulo k

Từ (1) và (2) ta có $d \mid k-1$ nhưng d lại không chia hết $\frac{k-1}{2}$

$\Rightarrow d = k-1 \Rightarrow k$ là số nguyên tố.

Ngược lại, k là số nguyên tố

Ta có k là số nguyên tố dạng $4l+1$ nên theo luật tương hỗ Gauss ta có

$$(\frac{3}{k}) = (\frac{k}{3})$$

Mà $k \equiv 2 \pmod 3$ nên $(\frac{k}{3}) = (\frac{2}{3}) = -1$ (do 2 không phải số chính phương mod 3).

Từ đó suy ra

$$3^{\frac{k-1}{2}} \equiv -1 (\mathrm{mod}\, k) \Leftrightarrow 3^{\frac{k-1}{2}} + 1 \equiv 0 (\mathrm{mod}\, k).$$

đpcm.

Ví dụ 3. Chứng minh rằng với mọi n nguyên dương, số $2^n + 1$ không có ước nguyên tố dạng $8k + 7$.

Lời giải

Giả sử tồn tại số nguyên tố $p = 8k + 7$ sao cho $p \mid 2^n + 1$

Nếu n chẵn, ta có

$$2^n \equiv -1 \pmod{p}$$

Suy ra -1 là số chính phương mod p

Do đó

$$1 = (\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = (-1)^{4k+3} = -1 \text{ (vô lí)}$$

Nếu n lẻ, ta có

$$2^n \equiv -1 \pmod p \Rightarrow 2^{n+1} \equiv -2 \pmod p$$

Suy ra -2 là số chính phương mod p

Do đó, ta có

$$1 = (\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = -1.1 = -1. \text{ (vô lí)}$$

Vậy ta có điều phải chứng minh.

Ví dụ 4. Tìm x, n nguyên dương sao cho

$$x^3 + 2x + 1 = 2^n. \quad (1)$$

Lời giải

Do x nguyên dương nên $x^3 + 2x + 1 \geq 4 \Rightarrow n \geq 2$.

Nếu $n = 2$, ta dễ dàng tìm được $x = 1$.

Xét $n \geq 3$

$(1) \Leftrightarrow x(x^2 + 2) = 2^n - 1$ là số lẻ nên x lẻ

Do đó, $x^2 + 2 \vdots 3 \Rightarrow 2^n \equiv (1 \bmod 3) \Leftrightarrow (-1)^n \equiv 1 \pmod 3$

Từ đó suy ra n chẵn.

Mặt khác

$$x^3 + 2x + 1 = 2^n$$
$$\Leftrightarrow x^3 + 2x + 3 = 2^n + 2$$
$$\Leftrightarrow (x + 1)(x^2 - x + 3) = 2^n + 2.$$

Giả sử p là một ước nguyên tố của $x^2 - x + 3 \Rightarrow p$ lẻ

Khi đó

$$2^n + 2 \equiv 0 \pmod p \Leftrightarrow 2^n \equiv -2 \pmod p$$

Mà n chẵn suy ra $(\frac{-2}{p}) = 1$

Ta có

$$1 = (\frac{-2}{p}) = (\frac{-1}{p})(\frac{2}{p}) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p^2-1}{8}}$$

Từ đó suy ra $p = 8k + 1$ hoặc $p = 8k + 3$.

Mà $n \geq 3 \Rightarrow 2^n = 8.2^{n-3} \equiv 0 \pmod 8$

Do đó ta suy ra

$$x^3 + 2x + 1 \equiv 0 \pmod 8.$$

Mà x lẻ $\Rightarrow x = 8k \pm 1, x = 8k \pm 3$

Nếu $x = 8k \pm 1 \Rightarrow x^3 + 2x + 1 \equiv (\pm 1)^3 + 2(\pm 1) + 1 \equiv 0 \pmod 8$ (vô lí)

Nếu $x = 8k + 3$ thì $x^3 + 2x + 1$ cũng không thể chia hết cho 8.

Nếu $x = 8k + 5$ thì thỏa mãn.

Khi đó

$$x^2 - x + 3 \equiv 5^2 - 5 + 3 \equiv 7 \pmod 8$$

Hay

$$x^2 - x + 3 = 8l + 7$$

Mà số dạng $8l + 7$ thì không thể có ước nguyên tố dạng $8k + 1$ hoặc $8k + 3$

Do đó (1) vô nghiệm khi $n \geq 3$.

Vậy $x = 1, n = 2$.

Ví dụ 5. Cho p là số nguyên tố dạng $12k - 1$. Tìm x, y, n nguyên không âm sao cho

$$3a^2 + b^2 \vdots p^n \quad (1)$$

Với a và b không chia hết cho p.

Lời giải

Nếu $n = 0$ thì mọi a, b nguyên không âm và $a \not\vdots p, b \not\vdots p$ đều thỏa mãn (1)

Nếu $n \neq 0 \Rightarrow a > 0 \Rightarrow 3a^2 + b^2 \vdots p$

Do đó

$$b^2 \equiv -3a^2 \pmod p$$

$$\Rightarrow (b^2)^{\frac{p-1}{2}} \equiv (-3)^{\frac{p-1}{2}} (a^2)^{\frac{p-1}{2}} \pmod p$$

$$\Rightarrow b^{p-1} \equiv (-3)^{\frac{p-1}{2}} a^{p-1} \pmod p$$

Mà

$$(a, p) = (b, p) = 1 \Rightarrow a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$$

Suy ra

$$(-3)^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Mặt khác

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{3}{p}\right) = (-1)^{6k-1} \left(\frac{3}{p}\right) = -\left(\frac{3}{p}\right) \ (*)$$

Lại có $p = 12k - 1$ nên 3 là số chính phương mod p hay $(\frac{3}{p}) = 1$

Thay vào (*) ta được 1 = -1 (vô lí)

Vậy khi $n > 0$ thì không tồn tại a, b, n thỏa mãn.

Ví dụ 6. (Serbi - 2008) Giải phương trình

$$12^x + y^4 = 2008^z$$

Với x, y, z là các số nguyên không âm.

Lời giải

Nếu $z = 0 \Rightarrow x = y = 0$.

Nếu $z > 0 \Rightarrow y > 0$ vì $12^x \vdots 251$ mà $2008 = 251.8$

TH1: x chẵn

Ta có $12^x + y^4 = (12^{\frac{x}{2}})^2 + (y^2)^2 = a^2 + b^2$

Với $a = 12^{x/2}$, $b = y^2$.

Vì $2008 = 251.8 \Rightarrow a^2 + b^2 \vdots 251$

Mà 251 là số nguyên tố và $251 = 4k + 3$ nên cả a và b đều phải chia hết cho 251

Vô lí vì $12^{x/2} \vdots 251$.

TH2. x lẻ làm tương tự.

Vậy phương trình có nghiệm duy nhất $x = y = z = 0$.

II.3.3. Bài tập

Bài 1. Chứng minh rằng mọi ước nguyên tố của $n^4 - n^2 + 1$ đều có dạng $12k + 1$.

Bài 2. (Ba Lan 2007) Chứng minh rằng phương trình $x^2 + 5 = y^3$ không có nghiệm nguyên.

Bài 3. Chứng minh rằng với mỗi số nguyên tố p thì tồn tại các số nguyên *a, b* sao cho $a^2 + b^2 + 1$ chia hết cho *p*.

Bài 4. Cho số nguyên tố *p*. Chứng minh rằng $3^p + 7p - 4$ không là bình phương của một số nguyên.

Bài 5. (IMO 2006) Tìm tất cả các nghiệm nguyên của phương trình

$$1 + 2^x + 2^{2x+1} = y^2.$$

Bài 6. Cho *m, n* là các số nguyên sao cho $A = \dfrac{(m+3)^n + 1}{3m}$ là một số nguyên. Chứng minh rằng *A* là số lẻ.

Bài 7. (Đề nghị IMO 2004)Chứng minh rằng $2^n + 1$ không có ước nguyên tố dạng $8k + 7$.

Chứng minh rằng $2^{3^n} + 1$ có ít nhất n ước nguyên tố dạng $8k + 3$.

Bài 8. Tìm tất cả các số nguyên dương *n* sao cho $3^n - 1 \vdots 2^n - 1$.

II. 4. Định lí thặng dư Trung Hoa

II.4.1 Lí thuyết

II.4.1.1. Định lí 1 (Định lí thặng dư Trung Hoa)

Cho hệ phương trình

$$\begin{cases} x \equiv r_1 (\text{mod}\, m_1) \\ x \equiv r_2 (\text{mod}\, m_2) \\ ... \\ x \equiv r_n (\text{mod}\, m_n) \end{cases} \quad (1)$$

Trong đó $m_1, m_2, \ldots, m_n$ là các số nguyên đôi một nguyên tố cùng nhau. Khi đó hệ phương trình trên luôn có nghiệm. Nếu x_1 và x_0 là hai nghiệm của (1) thì $x_1 \equiv x_0 \pmod{m_1 m_2 \ldots m_n}$.

Chứng minh

Đặt $s_i = \dfrac{\prod_{k=1}^{n} m_k}{m_i}$.

Do $m_1, m_2, \ldots, m_n$ đôi một nguyên tố cùng nhau nên $(s_i, m_i) = 1$.

Nên với mỗi số nguyên dương s_i luôn tồn tại một số nguyên h_i sao cho

$$s_i h_i \equiv 1 \pmod{m_i}.$$

Đặt $x_0 = \sum_{i=1}^{n} s_i h_i r_i$

Vì $s_i \vdots m_j$ với mọi $j \neq i$ nên

$$x_0 \equiv s_i h_i r_i \pmod{m_i} \equiv r_i \pmod{m_i}$$

Do đó x_0 chính là một nghiệm của (1).

Giả sử x_1 cũng là một nghiệm của (1)

Ta có

$$x_1 \equiv x_0 \pmod{m_i} \Rightarrow x_1 - x_0 \vdots m_i \text{.với mọi } i$$

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

$$x_1 - x_o \vdots m_1 m_2 \ldots m_n.$$

Từ đó suy ra điều phải chứng minh.

II.4.1.2. Định lí 2

Cho hệ phương trình

$$\begin{cases} x \equiv r_1 (\text{mod}\, m_1) \\ x \equiv r_2 (\text{mod}\, m_2) \\ ... \\ x \equiv r_n (\text{mod}\, m_n) \end{cases} \quad (1)$$

Điều kiện cần và đủ để hệ trên có nghiệm là

$$r_i \equiv r_j \ (\text{mod}\ (m_i, m_j)).$$

Khi đó hệ trên có nghiệm duy nhất theo modulo $[m_1, m_2, \ldots, m_n]$.

Chứng minh

(xin nhường cho bạn đọc)

II.4.1.3. Phương pháp giải hệ (1) trong trường hợp các số m_i đôi một nguyên tố cùng nhau.

Bước 1. Đặt $m = m_1 m_2 \ldots m_n = M_i m_i$ với i = 1, 2, …,*n*.

Bước 2. Tìm các số N_i nghiệm đúng phương trình

$$M_i x \equiv 1 \ (\text{mod}\ m)$$

Bước 3. Tìm được một nghiệm của hệ là

$x_0 = \sum_{i=1}^{n} M_i N_i r_i$ là một nghiệm của hệ

Bước 4. Kết luận $x = x_0 + mt$.

II.4.2 Các ví dụ

Ví dụ 1. Giải hệ

$$\begin{cases} x \equiv 4(\text{mod}11) \\ x \equiv 3(\text{mod}17) \end{cases}$$

Lời giải

Xét phương trình

$$17y \equiv 1(\text{mod } 11)$$

$$\Leftrightarrow 6y \equiv 1 \ (\text{mod } 11)$$

Ta dễ dàng tìm được một nghiệm là $N_1 = 2$.

Xét phương trình

$$11y \equiv 1 \ (\text{mod } 17)$$

Ta cũng dễ dàng tìm được một nghiệm là $N_2 = 14$.

Suy ra một nghiệm là $x_0 = 17.2 \ .4 + 11.14.3$

Từ đó tìm được nghiệm của hệ là $x = 17.2.4 + 11.14. \ 3 + 11.17t$.

Ví dụ 2. Giải hệ

$$\begin{cases} x \equiv 1(\text{mod}\,2) \\ x \equiv 2(\text{mod}\,3) \\ x \equiv 3(\text{mod}\,5) \end{cases}$$

Lời giải

Xét phương trình

$$15y \equiv 1 \ (\text{mod } 2)$$

Phương trình này có một nghiệm là $N_1 = 1$

Xét phương trình

$$10y \equiv 1 \ (\text{mod } 3)$$

Cũng dễ dàng tìm được một nghiệm là $N_2 = 1$.

Xét phương trình

$$6y \equiv 1 \ (\text{mod } 5)$$

Cũng tìm được $N_3 = 1$ là một nghiệm.

Vậy $x_0 = 15.1.1 + 10.1.2 + 6.1.3 = 53$ là một nghiệm của hệ

Do đó hệ phương trình đã cho có nghiệm là

$$x \equiv 53 \ (\text{mod } 30) \equiv 23 \ (\text{mod } 30)$$

Ví dụ 3. Giải hệ

$$\begin{cases} x \equiv 0(\text{mod}\,2) \\ x \equiv 0(\text{mod}\,3) \\ x \equiv 1(\text{mod}\,5) \\ x \equiv 6(\text{mod}\,7) \end{cases}$$

Lời giải

Xét phương trình

$$42y \equiv 1 \ (\text{mod } 5)$$

$$\Leftrightarrow 2y \equiv 1 \ (\text{mod } 5)$$

Tìm được $N_3 = 3$.

Xét phương trình

$$30y \equiv 1 \ (\text{mod } 7)$$

$$\Leftrightarrow 2y \equiv 1 \ (\text{mod } 7)$$

Tìm được $N_3 = 4$

Từ đó suy ra $x_0 = 42.3.1 + 30.4.6$ là một nghiệm của hệ

Vậy hệ có nghiệm là x ≡

Ví dụ 4. Chứng minh rằng với mọi số nguyên dương k tuỳ ý luôn tồn tại k số nguyên liên tiếp toàn hợp số.

Lời giải

Gọi $p_1 < p_2 < ... < p_k$ là các số nguyên tố tuỳ ý. Khi đó, theo định lí thặng dư Trung Hoa, luôn tồn tại n sao cho

$$\begin{cases} n \equiv -1(\text{mod}\,p_1) \\ n \equiv -2(\text{mod}\,p_2) \\ ... \\ n \equiv -k(\text{mod}\,p_k) \end{cases}$$

Do đó với mọi $i = 1, 2, ..., k$ thì $n + i \vdots p_k$.

Do đó chỉ cần chọn $n > p_k$ thì dãy $\{n + i | \ i = 1, 2, ..., n\}$ luôn là hợp số.

Ví dụ 5. (VMO - 2008) Cho $m = 2007^{2008}$. Hỏi có tất cả bao nhiêu số tự nhiên $n<m$ sao cho $m \mid n(2n+1)(5n+2)$?

Lời giải

Ta có $m = 3^{2008}.223^{2008}$.

Ta lại có $(n, 2n + 1) = 1$; $(n, 5n + 2) = (n, 2) \le 2$

$(2n + 1; 5n + 2) = (2n + 1, n) = 1$

Do đó $m \mid n(2n + 1)(5n + 2)$ khi và chỉ khi xảy ra một trong các trường hợp sau:

1) $m \mid n$

2) $m \mid 2n + 1$

3) $m \mid 5n + 2$

4) $3^{4096} \mid n$ và $223^{2008} \mid 2n + 1$

5) $3^{4096} \mid n$ và $233^{2008} \mid 5n + 2$

6) $3^{4096} \mid 5n + 2$ và $223^{2008} \mid 2n + 1$

7) $3^{4096} \mid 5n + 2$ và $233^{2008} \mid n$

8) $3^{4096} \mid 2n + 1$ và $223^{2008} \mid 5n + 2$

9) $3^{4096} \mid 2n + 1$ và $223^{2008} \mid n$

Trong mỗi trường hợp ấy, theo định lí thặng dư Trung hoa, có duy nhất một số tự nhiên n (modulo m) thỏa mãn.

Nên có tất cả 9 số tự nhiên thỏa mãn đề bài.

Ví dụ 6. (Đề nghị IMO 2002) Trong lưới điểm nguyên của mặt phẳng tọa độ Oxy, một điểm có tọa độ là các số nguyên $A(x, y) \in Z^2$ được gọi là nhìn thấy được từ O nếu trên đoạn OA không có điểm nào thuộc Z^2, trừ O và A. Chứng minh rằng với mọi số tự nhiên n tuỳ ý, luôn tồn tại hình vuông n x n có các đỉnh nguyên và mọi điểm nguyên bên trong và trên biên của hình vuông đều không nhìn thấy được từ O.

Lời giải

Ta có nếu $(x, y) = d$

thì điểm $M(\frac{x}{d};\frac{y}{d})$ là điểm nguyên thuộc đoạn OA với $A(x; y)$.

Do đó, $A(x, y)$ là điểm nhìn thấy được từ O khi và chỉ khi $(x, y) = 1$.

Gọi $p_{i,j}$ là các số nguyên tố đôi một khác nhau với $0 \le i, j \le n$

(có $(n +1)^2$ số nguyên tố như vậy)

Xét hai hệ sau:

$$\begin{cases} x \equiv 0(\text{mod}\, p_{0,0}p_{0,1}...p_{0,n}) \\ x \equiv -1(\text{mod}\, p_{1,0}p_{1,1}...p_{1,n}) \\ ... \\ x \equiv -n(\text{mod}\, p_{n,0}p_{n,1}...p_{n,n}) \end{cases}$$

$$\text{và } \begin{cases} x \equiv 0(\text{mod } p_{0,0}p_{1,0}...p_{n,0}) \\ x \equiv -1(\text{mod } p_{0,1}p_{1,1}...p_{n,1}) \\ ... \\ x \equiv -n(\text{mod } p_{0,n}p_{1,n}...p_{n,n}) \end{cases}$$

Theo định lí thặng dư Trung Hoa, tồn tại các số tự nhiên y như vậy.

Mà $x + i$ và $y + j$ đều chia hết cho $p_{i,j}$

Do đó, mọi điểm trong hình vuông n x n với $(n + 1)^2$ điểm nguyên $A_{i,j}(x + i, y + j)$ trên đều không nhìn thấy được từ O.

Ví dụ 8. (Nordic - 98) Tồn tại hay không một dãy cô hạn các số tự nhiên

$$\{x_1, x_2, ..., x_n, ...\} = \{1, 2, ..., n, ...\}$$

Sao cho $x_i \neq x_j$ với mọi $i \neq j$ và

$$x_1 + x_2 + ... + x_k \vdots k \text{ với mọi } k = 1, 2, ...$$

Lời giải

Ta xây dựng một dãy thỏa mãn đề bài như sau:

Chọn $x_1 = 1, x_2 = 3, x_3 = 2$.

Giả sử $x_1, x_2, ..., x_n$ là dãy số thỏa mãn

$$x_1 + x_2 + ... + x_k \vdots k \text{ với mọi } k = 1, 2, ..., n.$$

Gọi m là số nguyên dương bé nhất không nằm trong dãy $x_1, x_2, ..., x_n$.

Do $(n + 1, n + 2) = 1$ nên, theo định lí thặng dư Trung Hoa, tồn tại số nguyên x lớn hơn $\max\{x_1, x_2, ..., x_n\}$ và thỏa mãn

$$\begin{cases} x \equiv -s(\text{mod } n+1) \\ x \equiv -m - s(\text{mod } n+2) \end{cases} \text{ với } s = x_1 + x_2 + ... + x_n.$$

Khi đó, đặt $x_{n+1} = x, x_{n+2} = m$

Từ đó ta được dãy $x_1, x_2, ..., x_{n+1}, x_{n+2}$ thoả mãn

$$x_1 + x_2 + ... + x_n + x_{n+1} = s + x \vdots n + 1.$$

$$x_1 + x_2 + ... + x_{n+1} + x_{n+2} = s + x + n \vdots n + 2.$$

Do đó

$$x_1 + x_2 + ... + x_k \vdots k \text{ với mọi } k = 1, 2, ..., n + 2$$

Cứ tiếp tục như vậy ta thu được dãy số vô hạn thỏa mãn yêu cầu bài toán.

II.4.3. Bài tập

Bài 1. Giải các hệ phương trình sau:

a) $\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{7} \end{cases}$

b) $\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$

c) $\begin{cases} 5x \equiv 1 \pmod{12} \\ 5x \equiv 2 \pmod{8} \\ 7x \equiv 3 \pmod{11} \end{cases}$

Bài 2. (IMO 1989) Chứng minh rằng với mọi số tự nhiên *n,* luôn tồn tại *n* số tự nhiên liên tiếp mà cả *n* số đó đều không phải luỹ thừa của một số nguyên tố.

Bài 3. (Hàn Quốc 1999) Tìm tất cả các số tự nhiên *n* sao cho $2^n - 1$ chia hết cho 3 và tồn tại $m \in Z$ sao cho $4m^2 + 1$ chia hết cho $\frac{2^n - 1}{3}$.

Bài 4. Chứng minh rằng với mọi số nguyên dương *k* lớn tuỳ ý đều tồn tại *k* số nguyên liên tiếp gồm toàn hợp số.

Bài 5. Cho $S = \{a_1, a_2, ..., a_n\} \subset Z$. Chứng minh rằng tồn tại một số $b \in Z$ sao cho tập $b.S = \{ba_1, ba_2, ..., ba_n\}$ mà mọi phần tử của nó đều là luỹ thừa lớn hơn 1 của một số nguyên.

Bài 6. Cho *f(x)* là một đa thức với hệ số nguyên. Giả sử có một tập hữu hạn các số nguyên tố $\{p_1, p_2, ..., p_n\}$ mà với mọi *n* thì đều tồn tại $p_i \mid f(n)$. Chứng minh rằng tồn tại một số nguyên tố *p* sao cho với mọi *n* thì $f(n) \vdots p$.

Chương III

MỘT SỐ VẤN ĐỀ KHÁC

III.1. Luỹ thừa của một số nguyên

III.1.1 Số chính phương

III.1.1.1 Định nghĩa

Số tự nhiên n được gọi là một số chính phương nếu tồn tại m nguyên sao cho $n = m^2$.

Nhận xét: Nếu phân tích tiêu chuẩn $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$ thì:

+) n là số chính phương khi và chỉ khi α_i chẵn với mọi $i = 1, 2, ..., k$.

+) n là luỹ thừa s của một số nguyên khi và chỉ khi $\alpha_i \vdots s$ với mọi $i = 1, 2, ..., k$.

III.1.1.2 Các ví dụ

Ví dụ 1. Tìm tất cả các số chính phương có dạng $A = \overline{1985ab}$

Lời giải

Ta có

$$445^2 = 198025 < A < 198916 = 446^2$$

Từ đó suy ra không có số chính phương nào thỏa mãn yêu cầubài toán.

Ví dụ 2. Chứng minh rằng nếu $\overline{abc}$ là số nguyên tố thì $b^2 - 4ac$ không phải là số chính phương.

Lời giải

Giả sử $b^2 - 4ac$ là số chính phương thì

$$b^2 - 4ac = k^2, k \text{ nguyên dương.}$$

Ta có

$$\begin{aligned} 4a.\overline{abc} &= 400a^2 + 40ab + 4ac \\ &= 400a^2 + 40ab + b^2 - (b^2 - 4ac) \\ &= (20a + b)^2 - k^2 \\ &= (20a + b + k)(20a + b - k) \end{aligned}$$

Vì $\overline{abc}$ là số nguyên tố nên $c \neq 0 \Rightarrow ac > 0$

Do đó

$$b > k \Rightarrow 20a + b + k > 20a + b - k > 20a$$

Từ đó suy ra

$$\overline{abc} = \frac{(20a+b+k)(20a+b-k)}{4a} = m.n$$

Mà $20a + b + k$ và $20a + b - k$ đều lớn hơn $4a$ nên m và n đều lớn hơn 1

Nên $\overline{abc}$ là hợp số, trái với giả thiết

Từ đó ta có điều phải chứng minh.

Ví dụ 3. Chứng minh rằng một số chính phương luôn có số ước số nguyên dương là lẻ và ngược lại một số tự nhiên có số ước nguyên dương là lẻ thì số đó phải là số chính phương.

Lời giải

a) Nếu A là một số chính phương thì phân tích tiêu chuẩn của A là

$$A = p_1^{2k_1} p_2^{2k_2} ... p_n^{2k_n}$$

Từ đó suy ra số ước số nguyên dương của A là

$$(2k_1 + 1)(2k_2 + 1)...(2k_n + 1) \text{ là số lẻ.}$$

b) Ngược lại: Nếu A có số ước số là lẻ

Xét phân tích tiêu chuẩn của A

$$A = p_1^{k_1} p_2^{k_2} ... p_n^{k_n}$$

Từ đó suy ra số ước số của A là

$$(k_1 + 1)(k_2 + 1)...(k_n + 1) \text{ là số lẻ}$$

Do đó, tất cả các nhân tử trên đều lẻ

Suy ra k_i chẵn với mọi $i = 1, 2, ..., n$

Từ đó suy ra A là số chính phương.

Ví dụ 4. (Romani - 2004) Tìm tất cả các số không âm n sao cho tồn tại hai số nguyên a và b sao cho

$$n^2 = a + b \text{ và } n^3 = a^2 + b^2.$$

Lời giải

Ta có

$$2(a^2 + b^2) \geq (a + b)^2 \qquad \Rightarrow 2n^3 \geq n^4 \Leftrightarrow 0 \leq n \leq 2.$$

Nếu $n = 0$, chọn $a = b = 0$

Nếu $n = 1$, chọn được $a = 1, b = 0$.

Nếu $n = 2$, chọn được $a = b = 2$.

Vậy $n = 0$, $n = 1$, $n = 2$ là các giá trị cần tìm.

Ví dụ 5. Chứng minh rằng nếu $2n$ ($n \in N^*$) là tổng của hai số chính phương thì n cũng là tổng của hai số chính phương.

Lời giải

Gọi n là số tự nhiên thỏa mãn

$$2n = a^2 + b^2 \text{ với } a, b \in \mathrm{N}. \quad (1)$$

Từ (1) suy ra a và b cùng tính chẵn lẻ

Do đó $a + b$ và $a - b$ là số chẵn

Đặt

$$\begin{cases} a+b = 2x \\ a-b = 2y \end{cases}$$

Khi đó $a = x + y$ và $b = x - y$

Thay vào (1) ta được

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

Từ đó ta được điều phải chứng minh.

Ví dụ 6. Cho a, b là hai số nguyên dương sao cho $a^2 + b^2 \vdots ab + 1$.

Chứng minh rằng $\dfrac{a^2+b^2}{ab+1}$ là số chính phương.

Lời giải

Đặt

$$k = \frac{a^2+b^2}{ab+1} \quad (1)$$

Không mất tính tổng quát ta giả sử $a \geq b$.

Khi đó

$$(1) \Leftrightarrow a^2 + b^2 - kab - k = 0$$
$$\Leftrightarrow a^2 - kb.a + b^2 - k = 0.(*)$$

Giả sử rằng k không phải số chính phương. Xét phương trình

$$x^2 - 2bx + b^2 - k = 0 \quad (3)$$

Ta có a là một nghiệm của (3), gọi a_1 là một nghiệm còn lại

Khi đó

$$a + a_1 = kb$$

Do a, k, b nguyên nên suy ra a_1 cũng là số nguyên.

+) Nếu $a_1 = 0$ thì $k = b^2$, trái với điều giả sử.

+) Nếu $a_1 < 0$, ta có

$$a_1^2 - kba_1 + b^2 = k$$

Mà a_1 nguyên âm nên $a_1^2 - kba_1 + b^2 > -kba_1 = (-a_1 b)k > k$ (vô lí)

+) Do đo $a_1 > 0$ thì

$$a.a_1 = b^2 - k \Rightarrow a_1 = \frac{b^2 - k}{a} < a$$

Dặt $b_1 = b$ khi đó $a + b > a_1 + b_1$. ta có

$$a_1^2 - kb_1a_1 + b_1^2 - k = 0 \quad (4)$$

Lại xuất phát từ (4) suy ra phương trình (3) có nghiệm tự nhiên mới (a_2, b_2) mà

$$a_2 + b_2 < a_1 + b_1.$$

Từ đó suy ra phương trình hai biến (*) có vô hạn nghiệm tự nhiên thỏa mãn

$(a_1, b_1), (a_2, b_2)$, ... thỏa mãn $a_1 + b_1 > a_2 + b_2 >$ ...(vô lí)

Nên điều giả sử là sai.

Vậy ta có điều phải chứng minh.

Vídụ 7. Tìm n nguyên dương sao cho

$$A = 2^8 + 2^{11} + 2^n$$

là một số chính phương.

Lời giải

Nếu A là số chính phương thì

$$2^8 + 2^{11} + 2^n = x^2 \Leftrightarrow 2^n = (x - 48)(x + 48)$$

Với x là một số nguyên dương nào đó.

Khi đó

$$x - 48 = 2^s \text{ và } x + 48 = 2^{n-s},\ n > 2s$$

Từ đó suy ra

$$2^{n-s} - 2^s = 96 \Leftrightarrow 2^s(2^{n-2s} - 1) = 3.2^5.$$

Từ đó suy ra

$$\begin{cases} s = 5 \\ 2^{n-2s} - 1 = 3 \end{cases} \Leftrightarrow \begin{cases} s = 5 \\ n = 12 \end{cases}$$

KL: $n = 12$.

Ví dụ 8. Chứng minh rằng

$$A = 1^k + 9^k + 19^k + 2013^k$$

không phải số chính phương với mọi k nguyên dương lẻ.

Lời giải

Với mọi k nguyên dương lẻ, ta có

$$1^k \equiv 1 \pmod 4$$

$$9^k \equiv 1 \pmod 4$$

$$19^k \equiv -1 \pmod 4$$

$$2013^k \equiv 1 \pmod 4$$

Nên $A \equiv 2 \pmod 4$

Vậy A không thể là số chính phương.

Ví dụ 9. Tìm số tự nhiên n sao cho $n - 50$ và $n + 50$ đều là số chính phương.

Lời giải

Ta có

$$\begin{cases} n-50=a^2 \\ n+50=b^2 \end{cases}$$

với a, b nguyên dương và $a > b$.

Suy ra $b^2 - a^2 = 100 \Leftrightarrow (b - a)(b + a) = 2^2.5^2$.

Do $b - a < b + a$ và chúng có cùng tính chẵn lẻ nên $a + b$ và $b - a$ phải là các số chẵn. Do đó

$$\begin{cases} b-a=2 \\ b+a=50 \end{cases} \Leftrightarrow \begin{cases} a=24 \\ b=26 \end{cases}$$

Từ đó tìm được $n = 626$.

Ví dụ 10. Chứng minh rằng với mọi số nguyên dương n thì số

$$\frac{(17+12\sqrt{2})^n-(17-12\sqrt{2}^n)}{4\sqrt{2}}$$

là một số nguyên và không phải số chính phương.

Lời giải

Ta có $17+12\sqrt{2}=(\sqrt{2}+1)^4$ và $17-12\sqrt{2}=(\sqrt{2}-1)^4$

Do đó

$$\frac{(17+12\sqrt{2})^n-(17-12\sqrt{2}^n)}{4\sqrt{2}}=\frac{(\sqrt{2}+1)^{2n}+(\sqrt{2}-1)^{2n}}{2}.\frac{(\sqrt{2}+1)^{2n}-(\sqrt{2}-1)^{2n}}{2\sqrt{2}}$$

Đặt

$$A=\frac{(\sqrt{2}+1)^{2n}+(\sqrt{2}-1)^{2n}}{2} \text{ và } B=\frac{(\sqrt{2}+1)^{2n}-(\sqrt{2}-1)^{2n}}{2\sqrt{2}}$$

Sử dụng nhị thức Niutơn ta suy ra

$$(\sqrt{2}+1)^{2n} = x + y\sqrt{2} \text{ và } (\sqrt{2}-1)^{2n} = x - y\sqrt{2}$$

Với *x, y* là các số nguyên dương.

Từ đó suy ra

$$A=\frac{(\sqrt{2}+1)^{2n}+(\sqrt{2}-1)^{2n}}{2}=x \text{ và } B=\frac{(\sqrt{2}+1)^{2n}-(\sqrt{2}-1)^{2n}}{2\sqrt{2}}=y$$

Nên *A.B* là một số nguyên dương.

Mặt khác, ta lại có

$$A^2 - 2B^2 = (A - B\sqrt{2})(A + B\sqrt{2}) = (\sqrt{2}+1)^{2n}(\sqrt{2} - 1)^{2n} = 1$$

Do đó *A* và *B* nguyên tố cùng nhau.

Vậy để chứng minh *AB* không phải số chính phương ta chỉ cần chứng minh một trong hai số đó không phải là số chính phương.

Ta có

$$A=\frac{(\sqrt{2}+1)^{2n}+(\sqrt{2}-1)^{2n}}{2}=\frac{\left[(\sqrt{2}+1)^{n}+(\sqrt{2}-1)^{n}\right]^2}{2}-1$$

$$A=\frac{(\sqrt{2}+1)^{2n}+(\sqrt{2}-1)^{2n}}{2}=\frac{\left[(\sqrt{2}+1)^{n}-(\sqrt{2}-1)^{n}\right]^2}{2}+1$$

Tư đó dễ dàng suy ra được *A* không phải số chính phương

Vậy suy ra điều phải chứng minh.

Ví dụ 11. (Polish - 2001) Cho *a, b* là các số nguyên sao cho với mọi n thì $2^n a + b$ đều là số chính phương. Chứng minh rằng $a = 0$.

Lời giải

Giả sử $a \neq 0$.

Nếu $a \neq 0$, $b = 0$ thì $2^1 a + b$ và $2^2 a + b$ không thể đồng thời là số chính phương.

Do đó *a* và *b* đều phải khác 0.

Từ đó dễ dàng suy ra được a và b đều dương.

Xét hai dãy số (x_n) và (y_n) như sau

$$x_n = 2\sqrt{2^n a + b} \quad y_n = \sqrt{2^{n+2} a + b}$$

Dễ thấy (x_n) và (y_n) là hai dãy số nguyên dương, đơn điệu tăng vô hạn.

Ta có

$$(x_n + y_n)(x_n - y_n) = 3b$$

Suy ra $3b \vdots x_n + y_n$ với mọi $n \Rightarrow 3b \geq x_n + y_n$ với mọi n (vô lí)

Vậy điều giả sử là sai

Từ đó suy ra điều phải chứng minh.

Ví dụ 12. Tìm n nguyên dương sao cho

$$n^2 + 3^n$$

là số chính phương.

Lời giải

Giả sử

$$n^2 + 3^n = m^2$$

với m là một số nguyên dương nào đó.

Ta có

$$(m - n)(m + n) = 3^n$$

Từ đó suy ra

$$\begin{cases} m - n = 3^k \\ m + n = 3^{n-k} \end{cases} \quad (*)$$

Mà $m + n > m - n$ nên $n - 2k \geq 1$.

Nếu $n - 2k = 1$

Từ (*) suy ra $2n = 3^{n-k} - 3^k = 3^k(3^{n-2k} - 1) = 2.3^k$

$$\Leftrightarrow 3^k = n = 2k + 1 \Leftrightarrow k = 0, k = 1.$$

Từ đó tìm được $n = 1$, $n = 3$.

Nếu $n - 2k \geq 2 \Rightarrow k \leq n - k - 2$

Từ (*) suy ra $2n = 3^{n-k} - 3^k \geq 3^{n-k} - 3^{n-k-2} = 8.3^{n-k-2}$

Theo bất đẳng thức Bernoulli ta có

$$8.3^{n-k-2} = 8.(1 + 2)^{n-k-2} \geq 8[1 + 2(n - k - 2)]$$

$$= 16n - 16k - 24.$$

Do đó

$$2n \geq 16n - 16k - 24 \Leftrightarrow 8k + 12 \geq 7n .$$

Mà $n - 2k \geq 2$ nên $n \geq 2k + 2 \Rightarrow 7n \geq 14k + 14$

Từ đó suy ra $8k + 12 \geq 14k + 14$ vô lí vì $k \geq 0$.

KL: $n = 1$, $n = 3$.

III.1.2 Lập phương của một số nguyên

Ví dụ 1. Chứng minh rằng nếu n là lập phương của một số nguyên ($n \neq -1$) thì $n^2 + 3n + 3$ không thể là lập phương của một số nguyên.

Lời giải

$n = 0$ thì $n^2 + 3n + 3 = 3 \neq m^3$.

Giả sử $n^2 + 3n + 3 = k^3$ với k là một số nguyên nào đó

Vì n là lập phương của một số nguyên nên

$$n(n^2 + 3n + 3) = l^3$$

$$\Leftrightarrow (n + 1)^3 - 1 = l^3$$

Với $n \neq 0$, $n \neq 1$, n nguyên thì $0 < 3n^2 + 3n < 3n^2 + 3n + 1$

$$\Rightarrow n^3 < n^3 + 3n^2 + 3n < n^3 + 3n^2 + 3n + 1$$

$$\Leftrightarrow n^3 < n^3 + 3n^2 + 3n < (n + 1)^3$$

Do đó $n^3 + 3n^2 + 3n$ không thể là lập phương của một số nguyên.

Vậy điều giả sử là sai

Do đó ta có điều phải chứng minh.

Ví dụ 2. (Iran - 98)Chứng minh rằng không có số tự nhiên nào có dạng $\overline{abab}$ trong hệ cơ số 10 là lập phương của một số nguyên. Hãy tìm cơ số b nhỏ nhất saôch trong hệ cơ số b, có ít nhất một số có dạng $\overline{abab}$ là lập phương của một số nguyên.

Lời giải

Ta có $\overline{abab} = 101\,\overline{ab}$ là lập phương của một số nguyên thì

$$101 \mid \overline{ab} \text{ (vô lí)}$$

Vậy $\overline{abab}$ không thể là lập phương của một số nguyên.

Xét trong hệ cơ số b

Ta có

$$\overline{abab}_{(n)} = (n^2 + 1)\overline{ab}_{(n)} = (n^2 + 1)(an + b)$$

với $a, b < n$ và $n^2 + 1 > an + b$.

Nếu $n^2 + 1$ không chia hết cho một số chính phương nào thì $n^2 + 1 = p_1p_2...p_k$

Khi đó $an + b$ phải chia hết cho $(p_1p_2...p_k)^2$ vô lí

Vậy $n^2 + 1$ phải chia hết cho một số chính phương.

Thử trực tiếp thấy $n = 7$ là số nhỏ nhất như vậy ($n^2 + 1 = 50$)

Mặt khác thấy $\overline{2626}_{(7)} = 1000 = 10^3$.

Do đó $n = 7$ chính là số cần tìm.

Vídụ 3. Cho x, y là các số tự nhiên thỏa mãn $x^2 + y^2 + 6$ chia hết cho xy.

Chứng minh rằng $\frac{x^2 + y^2 + 6}{xy}$ là lập phương của một số tự nhiên.

Lời giải

Vì $x^2 + y^2 + 6 \vdots xy$ nên $x^2 + y^2 + 6 = pxy$ (1)

Gọi (x_0, y_0) là nghiệm của (1) và thỏa mãn $x_0 + y_0$ nhỏ nhất.

Không mất tính tổng quát, giả sử $x_0 \le y_0$

Xét phương trình

$$y^2 - px_0y + x_0^2 + 6 = 0 \quad (2)$$

Dễ thấy y_0 là một nghiệm của (2). Gọi y_1 là nghiệm còn lại

Khi đó, theo Viet ta có

$$\begin{cases} y_0 + y_1 = px_0 \\ y_0y_1 = x_0^2 + 6 \end{cases} \quad (3)$$

Dễ thấy $y_1 > 0$ nên (x_0, y_1) cũng là một nghiệm nguyên dương của (1)

Do đó

$$x_0 + y_0 \le x_0 + y_1 \Rightarrow y_0 \le y_1$$

Nếu $x_0 = y_0$ thì từ (1) ta có

$$p = \frac{2x_0^2 + 6}{x_0^2} = 2x_0 + \frac{6}{x_0^2} \in Z$$

$$\Leftrightarrow x_0 = 1 \Rightarrow p = 8 = 2^3$$

Nếu $x_0 < y_0$

+) $y_0 = y_1$ thì từ (3) suy ra $y_0^2 = x_0^2 + 6$

$$\Leftrightarrow (y_0 - x_0)(y_0 + x_0) = 6 \quad (4)$$

Mà VT(4) $\equiv 0 \pmod 4$ còn VP(4) $\equiv 2 \pmod 4$ nên (4) không xảy ra

+) $y_0 < y_1$ nên $x_0 < y_0 < y_1$

Ta có $y_0 \ge x_0 + 1 \Rightarrow y_1 \ge y_0 + 1 \ge x_0 + 2 \Rightarrow y_0y_1 \ge (x_0 + 1)(x_0 + 2)$

$$\Rightarrow x_0^2 + 6 \ge (x_0 + 1)(x_0 + 2)$$

$$\Leftrightarrow x_0 \le \frac{4}{3}$$

Vì x_0 nguyên dương nên $x_0 = 1$

Do đó $y_0.y_1 = x^2 + 6 = 7$

Do đó tìm được $y_0 = 1, y_1 = 7$ (không thỏa mãn điều kiên $x_0 < y_0$)

Vậy ta có $p = 8 = 2^3$ (điều phải chứng minh).

Ví dụ 4. Chứng minh rằng không tồn tại số tự nhiên n sao cho

$$2^{n+1} - 1 \text{ và } 2^{n-1}(2^n - 1)$$

đồng thời là lập phương của các số nguyên.

Lời giải

Giả sử ngược lại, tồn tại n sao cho $2^{n+1} - 1$ và $2^{n-1}(2^n - 1)$ đều là lập phương của các số nguyên.

Khi đó

$$2^{n-1}(2^n - 1) = k^3$$

Mà $2^n - 1$ không chia hết cho 2 nên 2^{n-1} cũng phải là lập phương của một số nguyên hay $n - 1 = 3m$.

Từ đó suy ra

$$a^3 = 2^{n+1} - 1 = 2^{3m+2} - 1 = 4.8^m - 1 \equiv 3 (\text{mod } 7)$$

Vô lí vì $a^3 \equiv 0; \pm 1 \text{ (mod } 7)$

Vậy ta có điều phải chứng minh.

Ví dụ 5. Chứng minh rằng với mọi số nguyên không âm n thì

$$A = 2^n + 3^n + 5^n + 6^n$$

không thể là lập phương của một số nguyên.

Lời giải

Ta có $2^6 \equiv 3^6 \equiv 5^6 \equiv 6^6 \equiv 1 \text{ (mod } 7)$

Mà $n = 6k + r$ với $r = 0, 1, 2, 3, 4, 5$

Nếu $r = 6k$ thì

$A \equiv 4 \text{ (mod } 7)$ do đó $A \neq m^3$.

Nếu $n = 6k + 1$ thì

$A = 2.(2^6)^k + 3.(3^6)^k + 5.(5^6)^k + 6(6^6)^k \equiv 2 + 3 + 5 + 6 \equiv 2 \text{ (mod } 7)$

nên $A \neq m^3$

Nếu $n = 6k + 2$ thì $A \equiv 2^2 + 3^2 + 5^2 + 6^2 \equiv 4 \text{ (mod } 7)$ nên $A \neq m^3$

Nếu $n = 6k + 3$ thì $A \equiv 2^3 + 3^3 + 5^3 + 6^3 \equiv 5 \text{ (mod } 7) \Rightarrow A \neq m^3$

Nếu $n = 6k + 4$ thì $A \equiv 2^4 + 3^4 + 5^4 + 6^4 \equiv 2 \text{ (mod } 7) \Rightarrow A \neq m^3$

Nếu $n = 6k + 5$ thì $A \equiv 2^5 + 3^5 + 5^5 + 6^5 \equiv 4 \text{ (mod } 7) \Rightarrow A \neq m^3$.

Vậy ta có điều phải chứng minh.

III.1.3 Các bài toán biểu diễn một số nguyên thành tổng các luỹ thừa

Ví dụ 1. Chứng minh rằng nếu $\frac{n^2-1}{3}$ là tích của hai số tự nhiên liân tiếp thì n là tổng bình phương của hai số nguyên liên tiếp.

Lời giải

Giả sử n là số tự nhiên mà

$$\frac{n^2-1}{3} = a(a+1) \qquad (1)$$

với a là một số tự nhiên nào đó.

Ta có

$$(1) \Leftrightarrow n^2 = 3a^2 + 3a + 1$$
$$\Rightarrow 4n^2 = 12a^2 + 12a + 4$$
$$\Rightarrow (2n - 1)(2n + 1) = 3(2a + 1)^2.$$

Do $2n - 1$ và $2n + 1$ là hai số lẻ liên tiếp và $(2n - 1, 2n + 1) = 1$ nên

$$\left[\begin{array}{l}\begin{cases}2n-1=3m^2\\2n+1=p^2\end{cases} (*)\\ \begin{cases}2n+1=3m^2\\2n-1=p^2\end{cases} (**)\end{array}\right.$$

Từ (*) suy ra $p^2 = 3m^2 + 2$ (vô lí vì số chính phương chia 3 chỉ dư 0 và 1)

Do đó, chỉ có (**) xảy ra.

Từ (**) suy ra m và p đều lẻ

Đặt $p = 2k + 1$ ta được

$$2n = p^2 + 1 = (2k+1)^2 + 1 = 4k^2 + 4k + 2$$
$$\Leftrightarrow n = (k+1)^2 + k^2.$$

Đó là điều phải chứng minh.

Ví dụ 2. (Nga - 1996) Cho x, y, p, n, k là các số tự nhiên thỏa mãn

$$x^n + y^n = p^k. \qquad (1)$$

Chứng minh rằng nếu $n > 1$, n lẻ và p là một số nguyên tố lẻ thì n là một luỹ thừa của p.

Lời giải

Đặt $m = (x, y)$ thì $x = ma$, $y = mb$ với $(a, b) = 1$.

Khi đó

$$(1) \Leftrightarrow m^n(a^n + b^n) = p^k. \quad (2)$$

Do p nguyên tố nên từ (2) suy ra $m = p^q$

Do đó

$$(2) \Leftrightarrow a^n + b^n = p^{k - nq}.$$

Mà n lẻ nên

$$a^n + b^n = (^{a + b})(a^{n - 1} - a^{n - 2}b + ... - ab^{n - 2} + b^{n - 1}) \quad (3)$$

$$= (a + b)A$$

Với $A = a^{n - 1} - a^{n - 2}b + ... - ab^{n - 2} + b^{n - 1}$.

Vì p lẻ nên $p > 2$ suy ra hai số x và y khác tính chẵn lẻ nên ít nhất một trong hai số a và b phải lớn hơn 1.

Do đó $a^n + b^n > a + b \Rightarrow A > 1$

Mà

$$A(a + b) = p^{k - nq} > 1$$

Suy ra A và $a + b$ đều chia hết cho p

Hay $a + b = p^r$

Từ đó suy ra

$$A = a^{n - 1} - a^{n - 2}(p^r - a) + ... - a(p^r - a)^{n - 2} + (p^r - a)^{n - 1} \quad = na^{n - 1} + Bp.$$

Mà $A \vdots p \Rightarrow na^{n - 1} \vdots p$

$a + b \vdots p$, $(a, b) = 1$ nên a không chia hết cho p

Do đó $n \vdots p \Rightarrow n = mp$

Thay vào (1) ta dễ dang suy ra được $n = p^l$

Ví dụ 3. Cho p là số nguyên tố và a, n là các số nguyên dương. Chứng minh rằng nếu

$$2^p + 3^p = a^n$$

thì $n = 1$.

Lời giải

Nếu $p = 2$ thì $2^p + 3^p = 13 \Rightarrow n = 1$

Nếu $p > 2 \Rightarrow p$ lẻ

Ta có

$$2^p + 3^p \equiv 2^p + (-2)^p \pmod 5 \equiv 0 \pmod 5$$

Do đó $a \vdots 5$

Giả sử $n > 1$.

Khi đó $a^n \vdots 25$ và $\frac{2^p + 3^p}{2+3} \vdots 5 \quad \Rightarrow 2^{p-1} - 2^{p-2}.3 + ... + 3^{p-1} \vdots 5$

Mà

$$2^{p-1} - 2^{p-2}.3 + ... + 3^{p-1} \equiv p.2^{p-1} \pmod 5$$

suy ra $p.2^{p-1} \vdots 5 \Rightarrow p = 5$ (do p là số nguyên tố)

Mà $2^5 + 3^5 = 753 \neq a^n$, (với n > 1)

Vậy điều giả sử là sai.

Từ đó ta có điều phải chứng minh.

III.1.4. Bài tập

Bài 1. Tìm các hàm số $f: N \to N$ thoả mãn đồng thời các điều kiện sau

i) $f(2n) = f(n) + n$

ii) $f(n)$ là số chính phương thì n là số chính phương

iii) f là hàm tăng nghiêm ngặt.

Bài 2. Tìm tất cả các số nguyên dương n sao cho $2n + 1$ và $3n + 1$ đều là số chính phương. Khi đó chứng minh rằng n chia hết cho 40.

Bài 3. Chứng minh rằng tổng của 3, 4, 5, hoặc 6 số nguyên liên tiếp không thể là số chính phương.

Bài 4. (IMO 86) Cho d là một số nguyên khác 2, 5, 13. Chứng minh rằng luôn tìm được hai số nguyên a, b phân biệt trong tập $\{2, 5, 13, d\}$ sao cho $ab - 1$ không phải số chính phương.

Bài 5. Tìm tất cả các số nguyên dương n sao cho luỹ thừa 4 của số ước của n chính bằng n.

Bài 6. Chứng minh rằng bình phương của một số nguyên lẻ luôn có dạng $8k + 1$.

Bài 7. (Hungari 1998) Cho x, y, z là các số nguyên và $z > 1$. Chứng minh rằng

$$(x + 1)^2 + (x + 2)^2 + ... (x + 99)^2 \neq y^z.$$

Bài 8. Chứng minh rằng với mọi số tự nhiên n thì giữa n^2 và $(n + 1)^2$ luôn tồn tại ba số tự nhiên phân biệt a, b, c sao cho $a^2 + b^2 \vdots c^2$.

Bài 9. Cho n là số tự nhiên có số ước số tự nhiên là s. Chứng minh rằng tích tất cả các ước số đó bằng $\sqrt[n]{n^s}$.

Bài 10. Tìm tất cả các cặp số nguyên dương x, y sao cho

$$(x + 1)^y - 1 = x!$$

Bài 11. Tìm các số nguyên tố p sao cho tồn tại các số nguyên dương n, x, y thỏa mãn

$$x^3 + y^3 = p^n.$$

Bài 12. Cho n là số nguyên dương. Chứng minh rằng nếu $2n+1$ và $3n+1$ là các số chính phương thì $5n+3$ không phải số nguyên tố.

Bài 13. Cho a và b là hai số nguyên dương. Số $(36a+b)(a+36b)$ có thể là luỹ thừa của 2 được hay không?

Bài 14. Cho tập A gồm các số nguyên dương và $|A| > 3$. Biết rằng tích ba phần tử bất kì của A đều là số chính phương. Chứng minh rằng mọi phần tử của A đều là số chính phương.

Bài 15. Cho n là một số nguyên dương sao cho $2\sqrt{28n^2+1}$ là một số nguyên. Chứng minh rằng $2+2\sqrt{28n^2+1}$ là một số chính phương.

Bài 16. Cho a, b, c là các số nguyên dương sao cho

$$0 < a^2 + b^2 - abc \le c$$

Chứng minh rằng $a^2 + b^2 - abc$ là một số chính phương.

Bài 17. Cho a và b là các số nguyên dương sao cho $a^2 + b^2$ chia hết cho $ab + 1$. Chứng minh rằng

$$\frac{a^2+b^2}{ab+1}$$

là một số chính phương.

Bài 18. Cho x, y, z là các số nguyên dương.

Chứng minh rằng $(xy+1)(yz+1)(zx+1)$ là các số nguyên dương khi và chỉ khi $xy+1$, $yz+1$, $zx+1$ đều là số chính phương.

Bài 19. Cho a và b là các số nguyên sao cho với mọi số không âm n thì $2^n a = b$ đều là số chính phương. Chứng minh rằng $a = 0$.

Bài 20. Cho p là một số nguyên dương lẻ. Chứng minh rằng tổng các luỹ thừa bậc p của p số nguyên liên tiếp chia hết cho p^2.

Bài 21. Tìm các số nguyên dương n sao cho $n.2^n + 3^n$ chia hết cho 5.

Bài 22. Tìm các số nguyên dương n sao cho $n.2^n + 3^n$ chia hết cho 25.

Bài 23. Tìm các số tự nhiên n sao cho $n^{n+1} + (n+1)^n$ chia hết cho 5.

Bài 24. Tìm các số nguyên dương m, n, k lớn hơn 1 sao cho

$$1! + 2! + \ldots + n! = m^k.$$

Bài 25. Tìm các số nguyên tố có dạng $2^{2002^n}+17$ (n là số tự nhiên) biểu diễn dưới dạng hiệu lập phương của hai số tự nhiên.

III. 2. Áp dụng tổ hợp vào các bài toán số học

III.2.1. Một số định lí cơ bản

III.2.1.1. Nhị thức Newton

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$$

với *a, b* là các số thực tuỳ ý, *n* nguyên dương. $C_n^k = \frac{n!}{k!(n-k)!}$

III.2.1.2. Định lí

Cho *p* là một số nguyên tố. Khi đó

$C_p^k \vdots p$ với mọi $p = 1, 2, ..., p - 1$.

Chứng minh

Ta có

$$C_n^p = \frac{p!}{k!(p-k)!} = \frac{p(p-1)...(p-k+1)}{k!}$$

Do *p* nguyên tố và $k \in \{1, 2, ..., p-1\}$ nên $(p, k!) = 1$

Mà C_p^k nguyên nên $(p-1)(p-2)...(p-k+1) \vdots k!$

Hay

$$\frac{(p-1)(p-2)...(p-k+1)}{k!} = a \in Z$$

Từ đó suy ra điều phải chứng minh.

III.2.1.3 Một số hệ thức cơ bản

1) $C_n^k = C_n^{n-k}$

2) $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$ (Hệ thức Pascal)

3) $C_n^0 < C_n^1 < ... < C_n^{\left[\frac{n-1}{2}\right]+1} = C_n^{\left[\frac{n}{2}\right]}$

4) $C_n^0 + C_n^1 + ... + C_n^n = 2^n$

5) $\sum_{i=0}^{k} C_n^i C_m^{k-i} = C_{m+n}^k$ (Hệ thức Vandermon)

III.2.2. Các ví dụ và bài tập

Ví dụ 1. Chứng minh rằng với *n* là số nguyên dương lẻ thì tập

$$S = \{C_n^1, C_n^2, ..., C_n^{\frac{n-1}{2}}\}$$

chứa lẻ các số lẻ.

Lời giải

Đặt

$$S_n = C_n^1 + C_n^2 + ... + C_n^{\frac{n-1}{2}}$$

Khi đó

$$2S_n = C_n^0 + C_n^1 + ... + C_n^n - 2 \quad = 2^n - 2.$$

$$\Rightarrow S_n = 2^{n-1} - 1 \text{ là số lẻ}$$

Vậy tập S phải chứa lẻ các số lẻ.

Ví dụ 2. (Trung Quốc - 1998) Tìm số tự nhiên $n \geq 3$ sao cho

$$2^{2000} \vdots 1 + C_n^1 + C_n^2 + C_n^3.$$

Lời giải

Theo bài ta có

$$1 + C_n^1 + C_n^2 + C_n^3 = 2^k \ (0 \leq k \leq 2000, k \text{ nguyên})$$

$$\Leftrightarrow \frac{(n+1)(n^2 - n + 6)}{6} = 2^k$$

$$\Leftrightarrow (n+1)(n^2 - n + 6) = 3.2^{k+1}$$

Đặt $m = n + 1$ $(m \geq 4)$

Khi đó ta có

$$m(m^2 - 3m + 8) = 3.2^{k+1}.$$

Do đó, chỉ có thể xảy ra một trong hai trường hợp sau:

+) Trường hợp 1: $m = 2^s$

Do $m \geq 4$ nên $s \geq 2$

$$\Rightarrow m^2 - 3m + 8 = 2^{2s} - 3.2^s + 8 = 3.2^{k+1-s}.$$

Nếu $s \geq 4$ thì $2^{2s} - 3.2^s + 8 \equiv 8 \pmod{16}$.

$$\Rightarrow 8 \equiv 3.2^{k+1-s} \pmod{16} \Rightarrow 2^{k+1-s} = 8 \Rightarrow m^2 - 3m + 8 = 24$$

(không có nghiệm nguyên)

Nếu $s = 2 \Rightarrow m = 4 \Rightarrow n = 3$ (thỏa mãn)

Nếu $s = 3 \Rightarrow m = 8 \Rightarrow n = 7$ (thỏa mãn)

+) Trường hợp 2. $m = 3.2^s$

Làm tương tự như trên, ta tìm được $n = 23$.

Vậy $n = 3$, $n = 7$, $n = 23$ là những giá trị cần tìm.

Ví dụ 3. Cho p là một số nguyên tố. Chứng minh rằng

$$C_{2p}^{p} \equiv 2(\text{mod } p^2)$$

Lời giải

Theo hệ thức Vandermon, ta có

$$C_{2p}^{p} = C_p^0 C_p^p + C_p^1 C_p^{p-1} + ... + C_p^p C_p^0$$

Mà C_p^k ⋮ p với mọi p = 1, 2, ..., p - 1.

Do đó

$$C_p^i C_p^{p-i} \text{ ⋮ } p^2 \text{ với mọi i} = 1, 2, ..., p - 1$$

Từ đó suy ra điều phải chứng minh.

Ví dụ 3. (Hungari - 2001) Cho m, n là các số nguyên dương và $1 \le m \le n$. Chứng minh rằng

$$n\sum_{1}^{m-1}(-1)^k C_n^k \text{ ⋮ } m.$$

Lời giải

Ta có

$$\begin{aligned} &C_n^0 - C_n^1 + C_n^2 - ...(-1)^{m-1} C_n^{m-1} \\ &= C_{n-1}^0 - (C_{n-1}^0 + C_{n-1}^1) + (C_{n-1}^1 + C_{n-1}^2) - ... + (-1)^{m-1}(C_n^{m-2} + C_{n-1}^{m-1}) \\ &= (-1)^{m-1} C_{n-1}^{m-1} \end{aligned}$$

Do đó

$$n\sum_{1}^{m-1}(-1)^k C_n^k = (-1)^{m-1} n C_{n-1}^{m-1} = (-1)^{m-1}.m C_n^m \text{ ⋮ } m.$$

Từ đó có điều phải chứng minh.

Ví dụ 4. (VMO - 2011) Cho dãy số nguyên (a_n) xác định bởi

$$a_0 = 1, a_1 = -1$$

$$a_n = 6a_{n-1} + 5a_{n-2}, \text{ với } n = 2, 3, ...$$

Chứng minh rằng $a_{2012} - 2010$ chia hết cho 2011.

Lời giải

Dễ dàng tìm được số hạng tổng quát của dãy số là

$$a_n = \frac{(7-2\sqrt{14})(3+\sqrt{14})^n + (7+2\sqrt{14})(3-\sqrt{14})^n}{14}$$

Do đó

$$a_{2012} = \frac{(7-2\sqrt{14})(3+\sqrt{14})^{2012} + (7+2\sqrt{14})(3-\sqrt{14})^{2012}}{14}$$

Mặt khác, theo khai triển Newton ta có

$$(3+\sqrt{14})^{2012} = \sum_{k=0}^{2012} C_{2012}^k 3^{2012-k}.(\sqrt{14})^k = A + B\sqrt{14}$$

$$(3-\sqrt{14})^{2012} = \sum_{k=0}^{2012} (-1)^k C_{2012}^k 3^{2012-k}.(\sqrt{14})^k = A - B\sqrt{14}.$$

Trong đó

$$A = C_{2012}^0 3^{2012} + C_{2012}^2 3^{2010}.14 + ... + C_{2012}^{2012} 14^{1006}.$$

$$B = C_{2012}^1 3^{2011} + C_{2012}^3 3^{2009}.14 + ... + C_{2012}^{2011}.3.14^{1005}.$$

Do đó

$$a_{2012} = \frac{(7-2\sqrt{14})(A+B\sqrt{14}) + (7+2\sqrt{14})(A-B\sqrt{14})}{14}$$

$$\Leftrightarrow a_{2012} = A + 4B.$$

Bây giờ ta chỉ cần chứng minh $A + 4B \equiv -1 \pmod{2011}$

Thật vậy, ta có

$C_{2012}^k = C_{2011}^k + C_{2011}^{k-1}$ với mọi k = 2, 3, ..., 2010

Mà 2011 là số nguyên tố nên $C_{2011}^k \vdots 2011$ với mọi k = 1, 2, ..., 2010.

Từ đó suy ra

$C_{2012}^k \vdots 2011$ với mọi k = 2, 3, ..., 2010.

Do đó $A + 4B \equiv 3^{2012} + 14^{1006} - 4(3^{2011} + 3.14^{1005}) \pmod{2011}$

$\equiv 2.\ 14^{1005} - 3^{2011} \pmod{2011}$

Mà $3^{2011} \equiv 3 \pmod{2011}$

$14^{1005} \equiv 2025^{1005} \equiv (45^2)^{1005} \equiv 45^{2010} \equiv 1 \pmod{2011}$.

Từ đó suy ra $A + 4B \equiv 2 - 3 \pmod{2011} \equiv -1 \pmod{2011}$

Vậy ta có điều phải chứng minh.

III.2.3 Bài tập

Bài 1. Tìm ước chung lớn nhất của

$$C_{2006}^{1}, C_{2006}^{3},..., C_{2006}^{2005}.$$

Bài 2. (T7/245) Cho các số tự nhiên *m, n, p* thỏa mãn điều kiện $p \le m + n$.

Chứng minh rằng $(m+n-b)!\,p!\sum_{i=a}^{b} C_n^i C_m^{p-i}$ chia hết cho $(m + n - a)!$

Trong đó $a = \max\{0, p - m\}$, $b = \min\{p, n\}$.

Bài 3. Cho $x_n = \left[(4+\sqrt{15})^n\right]$, với $[x]$ là phần nguyên của *x, n* là số tự nhiên.

Tìm số dư của x_n khi chia cho 8.

Bài 4. Chứng minh rằng số

$$S = \sum_{k=0}^{1004} C_{2009}^{2k} 2^{2008-2k} 3^k$$

là tổng của hai số chính phương liên tiếp.

Bài 5. Chứng minh rằng với mọi số nguyên dương *n* ta có

$$C_{2n}^{n} \vdots (n+1)$$

Bài 6. Tìm cặp số tự nhiên *n, k* sao cho

$$C_{3n}^{n} = (3n)^k.$$

Bài 7. Cho *m* và *n* là các số nguyên dương, *m* lẻ. Chứng minh rằng

$$\frac{1}{n.3^m}\sum_{k=0}^{m} C_{3m}^{3k}(3n-1)^k$$

là một số nguyên.

Bài 8. Chứng minh rằng với mọi số nguyên dương *n* thì số

$$\sum_{k=0}^{n} C_{2n+1}^{2k+1} 2^{3k}$$

không chia hết cho 5.

III. 3 Tính chất số học của dãy số nguyên

Trong phần này tôi xin giới thiệu cùng bạn đọc một số tính chất số học cơ bản của dãy số nguyên như tính chia hết, tính chính phương, tìm số hạng nguyên tố, ... Tuy nhiên, phần sâu hơn sẽ được tác giả giới thiệu trong chuyên đề tiếp theo, sẽ viết riêng về dãy số nguyên.

III.3.1. Tính chia hết trong dãy số nguyên.

Ví dụ 1. Cho dãy số $\{u_n\}$ thỏa mãn

$$\begin{cases} u_1 = 7, u_2 = 50 \\ u_{n+1} = 4u_n + 5u_{n-1} + 22, \quad n = 2,3,... \end{cases}$$

Chứng minh rằng u_{1996} chia hết cho 1997.

Lời giải

Xét dãy $\{v_n\}$ thỏa mãn $v_n = 4u_n + 11$ khi đó

$$\begin{cases} v_1 = 39, v_2 = 211 \\ v_{n+1} = 4v_n + 5v_{n-1}, \quad n = 2,3,... \end{cases}$$

Dựa vào phương trình đặc trưng của dãy $\{v_n\}$ ta dễ dàng xác định được số hạng tổng quát của dãy là

$$v_n = \frac{8(-1)^n + 25.5^n}{3}$$

Do đó

$$v_{1996} = \frac{8 + 25.5^{1996}}{3}$$

Vì 1997 là số nguyên tố nên theo định li Fermat, ta có

$$5^{1996} \equiv 1 \pmod{1997}$$

$$\Rightarrow 8 + 25.5^{1996} \equiv 8 + 25 \pmod{1997} \equiv 33 \pmod{1997}.$$

$$\Rightarrow 3v_{1996} \equiv 33 \pmod{1997}.$$

Mà $v_{1996} = 4u_{1996} + 11$ nên suy ra

$$12u_{1996} + 33 \equiv 33 \pmod{1997}$$

$$\Rightarrow 12u_{1996} \vdots 1997$$

Mặt khác (12, 1997) = 1 nên $u_{1996} \vdots 1997$.

Vậy ta có điều phải chứng minh.

Ví dụ 2. Cho dãy số $\{u_n\}$ xác định như sau

$$\begin{cases} u_1 = 0, \ u_2 = 14, u_3 = -18 \\ u_{n+1} = 7u_{n-1} - 6u_{n-2} \quad n = 3,4,... \end{cases}$$

Chứng minh rằng với mọi số nguyên tố p thì $u_p \vdots p$.

Lời giải

Theo cách xác định dãy số ta tìm được số hạng tổng quát của u_n là

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

Với mọi số nguyên tố p thì

$$2^p \equiv 2 \pmod p \text{ và } (-3)^p \equiv -3 \pmod p$$

Do đó

$$u_p = 1 + 2^p + (-3)^p \equiv 1 + 2 + (-3) \pmod p$$

Hay $u_p \vdots p$.

Vậy ta có điều phải chứng minh.

Nhận xét: Với những dãy số nguyên tuyến tính có phương trình đặc trưng có nghiệm nguyên thì ta dễ dàng sử dụng định lí Fermat trong chứng minh chia hết. Còn với những dãy nguyên tuyến tính có phương trình đặc trưng có nghiệm vô tỉ thì bao giờ ta cũng phải sử dụng nhị thức Newton để chứng minh chia hết.

Ví dụ 3. (VMO - 2011) Cho dãy số nguyên (a_n) xác định bởi

$$a_0 = 1, a_1 = -1$$

$$a_n = 6a_{n-1} + 5a_{n-2}, \text{ với } n = 2, 3, ...$$

Chứng minh rằng $a_{2012} - 2010$ chia hết cho 2011.

Lời giải

Dễ dàng tìm được số hạng tổng quát của dãy số là

$$a_n = \frac{(7 - 2\sqrt{14})(3 + \sqrt{14})^n + (7 + 2\sqrt{14})(3 - \sqrt{14})^n}{14}$$

Do đó

$$a_{2012} = \frac{(7 - 2\sqrt{14})(3 + \sqrt{14})^{2012} + (7 + 2\sqrt{14})(3 - \sqrt{14})^{2012}}{14}$$

Mặt khác, theo khai triển Newton ta có

$$(3 + \sqrt{14})^{2012} = \sum_{k=0}^{2012} C_{2012}^k 3^{2012-k}.(\sqrt{14})^k = A + B\sqrt{14}$$

$$(3 - \sqrt{14})^{2012} = \sum_{k=0}^{2012} (-1)^k C_{2012}^k 3^{2012-k}.(\sqrt{14})^k = A - B\sqrt{14}.$$

Trong đó

$$A = C_{2012}^0 3^{2012} + C_{2012}^2 3^{2010}.14 + ... + C_{2012}^{2012} 14^{1006}.$$

$$B = C_{2012}^1 3^{2011} + C_{2012}^3 3^{2009}.14 + ... + C_{2012}^{2011}.3.14^{1005}.$$

Do đó

$$a_{2012} = \frac{(7-2\sqrt{14})(A+B\sqrt{14})+(7+2\sqrt{14})(A-B\sqrt{14})}{14}$$

$\Leftrightarrow a_{2012} = A + 4B.$

Bây giờ ta chỉ cần chứng minh $A + 4B \equiv -1 \pmod{2011}$

Thật vậy, ta có

$$C_{2012}^{k} = C_{2011}^{k} + C_{2011}^{k-1} \text{ với mọi } k = 2, 3, ..., 2010$$

Mà 2011 là số nguyên tố nên $C_{2011}^{k} \vdots 2011$ với mọi $k = 1, 2, ..., 2010$.

Từ đó suy ra

$$C_{2012}^{k} \vdots 2011 \text{ với mọi } k = 2, 3, ..., 2010.$$

Do đó $A + 4B \equiv 3^{2012} + 14^{1006} - 4(3^{2011} + 3.14^{1005}) \pmod{2011}$

$\equiv 2.\ 14^{1005} - 3^{2011} \pmod{2011}$

Mà $3^{2011} \equiv 3 \pmod{2011}$

14 là số chính phương mod 2011 nên $14^{1005} = 14^{\frac{2011-1}{2}} \equiv 1 \pmod{2011}$.

Từ đó suy ra A + 4B ≡ 2 - 3 (mod 2011) ≡ -1 (mod 2011)

Vậy ta có điều phải chứng minh.

Ví dụ 4. Cho dãy số $\{u_n\}$ được xác định như sau

$$\begin{cases} u_1 = 2, u_2 = 6 \\ u_{n+1} = 2u_n + u_{n-1}, \quad n = 2, 3, ... \end{cases}$$

Tìm phần dư của u_{1024} chia cho 1023.

Lời giải

Dễ dàng tìm được số hạng tổng quát của dãy $\{u_n\}$ là

$$u_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n$$

Do đó

$$u_{1024} = (1+\sqrt{2})^{1024} + (1-\sqrt{2})^{1024}$$

Theo khai triển nhị thức Newton, ta có

$$(1+\sqrt{2})^{1024} = A + B\sqrt{2}, \quad (1-\sqrt{2})^{1024} = A - B\sqrt{2}$$

Với

$$A = C_{1024}^{0} + 2C_{1024}^{2} + 2^2 C_{1024}^{4} + ... + 2^{512} C_{1024}^{1024}$$

$$B = C_{1024}^{1} + 2C_{1024}^{3} + 2^2 C_{1024}^{5} + ... + 2^{512} C_{1024}^{1023}$$

Do đ ó $u_{1024} = 2A$

Ta có

$$C_{1024}^{k} = C_{1023}^{k} + C_{1023}^{k-1} \text{ với mọi k = 2, 3, ..., 1022.}$$

Mà 1023 là số nguyên tố nên $C_{1023}^{k} \vdots 1023$ với mọi k = 1, 2, ..., 1022.

Từ đó suy ra

$$C_{1024}^{k} \vdots 1023 \text{ với mọi k = 2, 3, ..., 1022.}$$

Nên

$$2A \equiv 2C_{1024}^{0} + 2^{513} C_{1024}^{1024} (\text{mod} 1023)$$

$$\equiv 2+2^{513} \text{ (mod 1023).}$$

Mặt khác

$$2^{10} \equiv 1 \text{ (mod 1023)} \Rightarrow 2^{513} = 8.(2^{10})^{51} \equiv 8 \text{ (mod 1023)}$$

Do đó $2A \equiv 10$ (mod 1023)

Vậy phần dư của phép chia u_{1024} cho 1023 là 10.

Nhận xét: Việc sử dụng nhị thức Newton rất có hiệu quả đối với các bài toán chứng minh một số hạng cụ thể của dãy chia hết cho p. Tuy nhiên nó thường không có tác dụng đối với việc chứng minh trong dãy số tồn tại một số hạng của dãy chia hết cho p hoặc tồn tại vô hạn số hạng của dãy chia hết cho p. Đối với những bài toán dạng này ta thường phải chứng minh dãy số dư của u_n cho p tuần hoàn kể từ một số hạng nào đó.

Ví dụ 5. Cho dãy số $\{u_n\}$ được xácđịnh như sau

$$\begin{cases} u_1 = 20, \quad u_2 = 100 \\ u_{n+1} = 4u_n + 5u_{n-1} - 1976, \quad n = 2, 3,... \end{cases}$$

Chứng minh rằng tồn tại ít nhất một số hạng của dãy chia hết cho 1996.

Lời giải

Xét dãy $\{v_n\}$ với v_n là phần dư của phép chia u_n cho 1996.

Hay $v_n \equiv u_n$ (mod 1996), $0 \le v_n \le 1995$.

Dễ thấy $v_{n+1} \equiv 4v_n + 5v_{n-1} - 1976$ (mod 1996)

Xét các cặp (v_1, v_2), (v_2, v_3), ..., (v_n, v_{n+1}), ...

Vì dãy $\{v_n\}$ là vô hạn mà số các cặp (a, b) với $0 \le a, b, \le 1995$ là hữu hạn nên phải tồn tại hai số tự nhiên i, j (i > j) sao cho

$$\begin{cases} v_i = v_j \\ v_{i+1} = v_{j+1} \end{cases}$$

Khi đó. Ta có

$$5(v_{i-1} - v_{j-1}) \equiv 5(v_{i+1} - 4v_i + 1976) - 5(v_{j+1} - 4v_j + 1996)$$
$$\equiv 5(v_{i+1} - v_{j+1}) - 20(v_i - v_j) \pmod{1996}$$
$$\equiv 0 \pmod{1996}$$

Mà (5, 1996) = 1 nên $v_{i-1} - v_{j-1} \equiv 0 \pmod{1996}$

Vì $0 \le v_{i-1}, v_{j-1} \le 1995$ nên $v_{i-1} = v_{j-1}$

Lí luận tương tự ta dẫn đến $v_{i-2} = v_{j-2}$

Cứ tiếp tục như vậy ta sẽ dẫn đến

$$\begin{cases} v_2 = v_{2+(i-j)} \\ v_1 = v_{1+(i-j)} \end{cases}$$

Bây giờ ta sẽ chứng minh $v_{i-j} = 0$

Thật vậy, ta có

$$5v_{i-j} \equiv v_{i-j+2} - 4v_{i-j+1} + 1976 \pmod{1996}$$
$$\equiv v_2 - 4v_1 + 1976 \pmod{1996}$$
$$\equiv u_2 - 4u_1 + 1976 \pmod{1996}$$
$$\equiv 100 - 4.20 + 1976 \pmod{1996}$$
$$\equiv 0 \pmod{1996}.$$

Vì (5, 1996) = 1 nên $v_{i-j} \equiv 0 \pmod{1996}$

Do đó $u_{i-j} \equiv 0 \pmod{1996}$

Vậy có điều phải chứng minh.

Ví dụ 6. (Chọn ĐT Khoa học tự nhiên - 2009)

Cho dãy $\{a_n\}$ được xác định

$$a_0 = 0, a_1 = 1, a_2 = 2, a_3 = 6$$
$$a_{n+4} = 2a_{n+3} + a_{n+2} - 2a_{n+1} - a_n, n = 0, 1, ...$$

a) Chứng minh rằng a_n chia hết cho n với mọi $n \ge 1$.

b) Chứng minh rằng dãy số $\left\{\frac{a_n}{n}\right\}$, $n = 1, 2, ...$ chứa vô số số hạng chia hết cho 2009.

Lời giải

a) Phương trình đặc trưng của dãy $\{a_n\}$ là

$$x^4 - 2x^3 - x^2 + 2x + 1 = 0$$
$$\Leftrightarrow (x^2 - x - 1)^2 = 0$$

$$\Leftrightarrow \begin{cases} x = \dfrac{1+\sqrt{5}}{2} = \alpha \\ x = \dfrac{1-\sqrt{5}}{2} = \beta \end{cases}$$

Khi đó số hạng tổng quát của dãy trên là

$$a_n = c_1\alpha^n + c_2\beta^n + n(c_3\alpha^n + c_4\beta^n)$$

Dễ dàng tìm được

$$c_1 = c_2 = 0,\ c_3 = \frac{1}{\sqrt{5}},\ c_4 = -\frac{1}{\sqrt{5}}.$$

Do đó

$$a_n = n(\frac{1}{\sqrt{5}}\alpha^n - \frac{1}{\sqrt{5}}\beta^n)$$

Từ đó suy ra $\dfrac{a_n}{n} = F_n$ với $\{F_n\}$ là dãy Fibonaci.

Do đó $a_n \vdots n$ với mọi n.

b) Bổ sung vào dãy $\{F_n\}$ một số hạng $F_0 = 0$ mà ta vẫn giữ được hệ thức

$$F_{n+1} = F_n + F_{n-1},\ n = 0, 1, ...$$

Xét dãy $\{v_n\}$ với v_n là phần dư của phép chia F_n cho 2009.

Hay $v_n \equiv u_n \pmod{2009}$, $0 \le v_n \le 2008$.

Dễ thấy $v_{n+1} \equiv v_n + v_{n-1} \pmod{2009}$

Xét các cặp $(v_1, v_2), (v_2, v_3), ..., (v_n, v_{n+1}), ...$

Vì dãy $\{v_n\}$ là vô hạn mà số các cặp (a, b) với $0 \le a, b \le 2008$ là hữu hạn nên phải tồn tại hai số tự nhiên i, j (i > j) sao cho

$$\begin{cases} v_i = v_j \\ v_{i+1} = v_{j+1} \end{cases}$$

Làm tương tự ví dụ 5, ta suy ra $0 = v_0 = v_{i-j}$

và dãy $\{v_n\}$ tuần hoàn với chu kì *(i - j)*.

Do đó $v_{k(i-j)} = 0$ hay $F_{k(i-j)} \equiv 0 \pmod{2009}$

Vậy ta có điều phải chứng minh.

III.3. 2. Dãy số và số chính phương

Ví dụ 1. Cho dãy số $\{a_n\}$ được xác định như sau

$$\begin{cases} a_0 = 0, a_1 = 1 \\ \dfrac{a_{n+1} - 3a_n + a_{n-1}}{2} = ((-1)^n, n = 1,2,... \end{cases}$$

Chứng minh rằng với mọi n thì a_n là số chính phương.

Lời giải

Ta sẽ chứng minh với mọi n thì $a_n = F_n^2$, trong đó $\{F_n\}$ là dãy Fibonaci

Thật vậy

$$a_0 = 1 = F_0^2, a_1 = 1 = F_1^2, a_2 = 4 = F_2^2.$$

Giả sử $a_k = F_k^2$ với mọi $k \le n$

Khi đó

$$a_n = F_n^2, a_{n-1} = (F_{n-1})^2, a_{n-2} = (F_{n-2})^2$$

Theo cách xác định dãy $\{a_n\}$ ta có

$$a_{n+1} - 3a_n + a_{n-1} = 2(-1)^n$$
$$a_n - 3a_{n-1} + a_{n-2} = 2(-1)^{n-1}$$

Từ đó ta suy ra

$$a_{n+1} - 2a_n - 2a_{n-1} + a_{n-2} = 0$$
$$\Leftrightarrow a_{n+1} = 2(F_n)^2 + 2(F_{n-1})^2 - (F_{n-2})^2$$
$$= (F_n + F_{n-1})^2 + (F_n - F_{n-1})^2 - (F_{n-2})^2$$
$$= (F_{n+1})^2 + (F_{n-2})^2 - (F_{n-2})^2 = (F_{n+1})^2$$

Từ đó suy ra diều phải chứng minh.

Ví dụ 2. Cho dãy số $\{a_n\}$ xác định như sau

$$\begin{cases} a_0 = 2, a_1 = 3 \\ a_{n+1} = 3a_n - a_{n-1}, \quad n = 1,2,... \end{cases}$$

Tìm n sao cho $5(a_n - 2)$ là một số chính phương.

Lời giải

Dễ dàng xác định được số hạng tổng quát của dãy trên là

$$a_n = (\frac{3+\sqrt{5}}{2})^n + (\frac{3-\sqrt{5}}{2})^n$$

Mặt khác ta cũng chứng minh được ngay

$$a_{2k} \equiv 2 \pmod 5 \text{ và } a_{2k+1} \equiv 3 \pmod 5.$$

Do đó $5(a_n - 2)$ là số chính phương thì $a_n - 2 \vdots 5 \Rightarrow n = 2k$.

Khi đó

$$a_{2k} = (\frac{3+\sqrt{5}}{2})^{2k} + (\frac{3-\sqrt{5}}{2})^{2k}$$

Khi đó

$$5(a_{2k} - 2) = 5\left((\frac{3+\sqrt{5}}{2})^{k} - (\frac{3-\sqrt{5}}{2})^{k}\right)^2$$

Theo khai triển Newton ta có

$$(\frac{3+\sqrt{5}}{2})^{k} = \frac{A+B\sqrt{5}}{2^k}, \quad (\frac{3-\sqrt{5}}{2})^{k} = \frac{A-B\sqrt{5}}{2^k}$$

Với

$$A = C_k^0 3^k + C_k^2 3^{k-2}.5 + ... + C_k^{2\left[\frac{k}{2}\right]} 3^{k-2\left[\frac{k}{2}\right]}.5^{\left[\frac{k}{2}\right]}$$

$$B = C_k^1 3^{k-1} + C_k^3 3^{k-3}.5 + ... + C_k^{2\left[\frac{k}{2}\right]-1} 3^{k-2\left[\frac{k}{2}\right]-1} 5^{\left[\frac{k}{2}\right]}$$

Khi đó $(\frac{3+\sqrt{5}}{2})^{k} - (\frac{3-\sqrt{5}}{2})^{k} = \frac{B\sqrt{5}}{2^{k-1}} = \sqrt{5}.c_k$ với c_k là số hữu tỉ.

$\Rightarrow a_{2k} - 2 = 5c_k^2$ nguyên nên c_k^2 là số nguyên

Mà c_k hữu tỉ nên $c_k \in Z$

Từ đó suy ra $5(a_{2k} - 2) = (5c_k)^2$ với $5c_k \in Z$

Vậy với mọi k thì $5(a_{2k} - 2)$ là số chính phương.

Ví dụ 3. Cho dãy số $\{a_n\}$ được xác định như sau

$$a_n = 2^8 + 2^{11} + 2^n, n = 1, 2, ...$$

Tìm n để a_n là một số chính phương.

Lời giải

Ta có

$$a_n = 2^8 + 2^{11} + 2^n = x^2$$

$$\Leftrightarrow 2^n = (x - 48)(x + 48)$$

Với x là một số nguyên dương nào đó.

Khi đó

$$x - 48 = 2^s \text{ và } x + 48 = 2^{n-s}, n > 2s$$

Từ đó suy ra

$$2^{n-s} - 2^s = 96.$$

$$\Leftrightarrow 2^s(2^{n-2s} - 1) = 3.2^5.$$

Từ đó suy ra

$$\begin{cases} s = 5 \\ 2^{n-2s} - 1 = 3 \end{cases} \Leftrightarrow \begin{cases} s = 5 \\ n = 12 \end{cases}$$

Vậy a_n là số chính phương khi và chỉ khi $n = 12$

Ví dụ 4. Cho dãy số $\{a_n\}$ được xác định như sau

$$\begin{cases} a_1 = 1, a_2 = 3 \\ a_{n+1} = (n+2)a_n - (n+1)a_{n-1} \quad n = 2, 3,... \end{cases}$$

Tìm n để a_n là luỹ thừa p của một số nguyên ($p \geq 2$).

Lời giải

Ta dễ dàng chứng minh được

$$a_n = 1! + 2! + ... + n!$$

Trường hợp 1: $p = 2$.

Ta có $n! \vdots 10$ với mọi $n \geq 5$

Do đó, nếu $n \geq 5$ thì $a_n \equiv 1! + 2! + 3! + 4! \pmod{10}$

$$\equiv (1 + 2 + 6 + 24) \pmod{10} \equiv 3 \pmod{10}$$

Từ đó suy ra a_n không thể là số chính phương nếu $n \geq 5$.

Với $1 \leq n \leq 4$, thử trực tiếp thấy $n = 1$ và $n = 3$ thỏa mãn.

Trường hợp 2. $n \geq 3$

Ta có $a_1 = 1 = 1^p$ với mọi p.

Với $n \geq 2$ thì $a_n = 1! + 2! + 3! + ... + n! \vdots 3$

Giả sử $a_n = b^p$ ($p \geq 3$) $\Rightarrow u_n \vdots 27$

Ta có $9! \vdots 27$ nên $k! \vdots 27$ với mọi $k \geq 9$.

Do đó

$$a_n \equiv a_8 \pmod{27} \text{ với } n \geq 9.$$

Mà

$$a_8 = 1! + 2! + ... + 8! = 46233 \equiv 1 \pmod{27}.$$

Nên a_n không chia hết cho 27 với mọi $n \geq 8$ hay $a_n \neq b^p$ với mọi $n \geq 8$.

Bằng cách thử trực tiếp $k = 2, 3, ..., 7$ thấy không có giá trị nào thỏa mãn.

Vậy $n = 1$ là giá trị cần tìm.

III.3.3. Dãy số nguyên số nguyên tố.

Ví dụ 1. Cho dãy số $\{u_n\}$ được xác định như sau

$$u_n = 3^n - 2^n - 1$$

Chứng minh rằng nếu p là số nguyên tố thì $u_p \vdots 42p$.

Lời giải

Ta có

$$u_p = 3^p - 2^p - 1 = (3^p - 3) - (2^p - 2) \equiv 0 \pmod p. \quad (1)$$

Mặt khác

$$3^p - 2^p - 1 = (3^p - 1) - 2^p \vdots 2 \quad (2)$$

Mà $p > 7 \Rightarrow p$ lẻ

Do đó

$$3^p - 2^p - 1 \equiv -(-1)^p - 1 \equiv 0 \pmod 3 \quad (3)$$

Bây giờ ta cần chứng minh $3^p - 2^p - 1 \vdots 7$

Ta có

$$3^p - 2^p - 1 = 3.3^{p-1} - 2^p - 1$$

$$= 3.9^{\frac{p-1}{2}} - 2^p - 1 \equiv 3.2^{\frac{p-1}{2}} - 2^p - 1 \pmod 7$$

$$= 2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1$$

Do $(p, 3) = 1$ nên $p = 3k + 1$ hoặc $p = 3k + 2$

Nếu $p = 3k + 1$ thì

$$2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1 = 8^k - 1 + 2^{\frac{p+1}{2}} - 2^p \equiv 2^p - 2^{\frac{p+1}{2}} \pmod 7$$

$$= 2^{\frac{p+1}{2}}(2^{\frac{p-1}{2}} - 1) = 2^{\frac{p+1}{2}}(8^k - 1) \equiv 0 \pmod 7$$

Nếu $p = 3k + 2$ ta chứng minh tương tự.

Từ đó suy ra đpcm.

Ví dụ 2. [IMO - 2005] Cho dãy số (a_n) xác định như sau

$$a_n = 2^n + 3^n + 6^n - 1 \text{ với } n = 1, 2, \ldots$$

Tìm số tự nhiên nguyên tố cùng nhau với mọi số hạng của dãy trên.

Lời giải

Ta sẽ chứng minh rằng với mọi số nguyên tố p đều tồn tại một số hạng a_n chia hết cho p.

Thật vậy, ta có $a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$ chia hết cho 2 và 3.

Xét $p \geq 5$

Ta có

$$(2, p) = 1; (3, p) = 1; (6, p) = 1$$

Do đó, từ định lí Fermat suy ra

$$2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1 \pmod{p}$$

Từ đó dễ dàng chứng minh được $6a_{p-2} \vdots p$

Mà $(p, 6) = 1$ nên $a_{p-2} \vdots p$

Do đó chỉ có số 1 là số tự nhiên duy nhất nguyên tố cùng nhau với mọi số hạng của dãy (a_n).

III.3.4 Bài tập

Bài 1. Cho x_1, x_2 là nghiệm của phương trình

$$x^2 - 6x + 1 = 0.$$

Chứng minh rằng với mọi $n \in N$ thì $x_1^n + x_2^n$ là một số nguyên và không chia hết cho 5.

Bài 2. Cho dãy $\{u_n\}$ thỏa mãn

$$\begin{cases} u_1 = 1, u_2 = 2, u_3 = 24 \\ u_n = \dfrac{6u_{n-1}^2 u_{n-3} - 8u_{n-1}u_{n-2}^2}{u_{n-2}u_{n-3}}, \quad n = 4, 5,... \end{cases}$$

Chứng minh rằng với mọi n thì u_n chia hết cho n.

Bài 3. (T6/254) Cho dãy số $\{x_n\}$ xác định như sau:

$$\begin{cases} x_0 = a, x_1 = b \\ x_{n+1} = 5x_n^2 - 3x_{n-1}, \quad n \geq 2. \end{cases}$$

với a, b là hai số nguyên cho trước. Chứng minh rằng dãy số trên hoặc không có số hạng nào chia hết cho 1997 hoặc có vô số số hạng chia hết cho 1997.

Bài 4. (T6/255) Cho dãy $\{a_n\}$ được xác định như sau

$$\begin{cases} a_1 = 1964, a_2 = 96 \\ a_{n+2} = 30a_{n+1}^2 - 75a_n a_{n+1} - 1994a_n, \quad n \geq 1. \end{cases}$$

Chứng minh rằng không tồn tại số hạng nào của dãy là tổng luỹ thừa bảy của ba số nguyên.

Bài 5. Cho dãy $\{u_n\}$ được xác định bởi:

$$\begin{cases} u_0 = 3, u_1 = 11 \\ u_{n+2} = 2u_{n+1} + 7u_n, \quad n \geq 0. \end{cases}$$

Tìm các số nguyên dương lẻ a sao cho với các số nguyên dương m và n tuỳ ý luôn tìm được số nguyên dương k sao cho $u_n^k - a$ chia hết cho 2^m.

Bài 6. Cho dãy $\{u_n\}$ được xác định như sau:

$$\begin{cases} u_0 = u_1 = 1 \\ u_{n+2} = 1999u_{n+1} - u_n, \quad n \geq 0 \end{cases}$$

Tìm các số tự nhiên n sao cho u_n là số nguyên tố.

Bài 7. (Bulgari 1999) Cho $\{a_n\}$ là dãy số nguyên thỏa mãn

$$(n - 1)a_{n+1} = (n + 1)a_n - 2(n - 1).$$

Biết rằng a_{1999} chia hết cho 2000. Tìm số nguyên dương $n \geq 2$ và n nhỏ nhất sao cho a_n chia hết cho 2000.

Bài 8. Cho một dãy số gồm $2n + 1$ số nguyên dương liên tiếp sao cho tổng bình phương của n +1 hạng đầu tiên bằng tổng bình phương của n số hạng còn lại. Hỏi trong dãy đó có số 2001 không?

Bài 9. Cho dãy $\{a_n\}$ xác định như sau

$$\begin{cases} a_0 = 0, a_1 = 1 \\ a_{n+2} = 2a_{n+1} + a_n, \quad n = 0,1,... \end{cases}$$

Chứng minh rằng a_n chia hết cho 2^k khi và chỉ khi n chia hết 2^k, với mọi k nguyên không âm.

Bài 10. Cho dãy số $\{u_n\}$ thỏa mãn

$$\begin{cases} u_1 = 3, u_2 = 11 \\ u_{n+2} = 2u_{n+1} + 7u_n \quad n \geq 1. \end{cases}$$

Tìm số nguyên dương lẻ a sao cho với mọi m, n nguyên dương tuỳ ý luôn tìm được số nguyên dương k sao cho $u_n^k - a$ chia hết cho 2^m.

Bài 11. Cho dãy $\{u_n\}$ được xác đin như sau

$$\begin{cases} u_0 = 0, u_1 = 1 \\ u_{n+2} = 1999u_{n+1} - u_n, \quad n = 0, 1, ... \end{cases}$$

Tìm các số tự nhiên n sao cho u_n là số nguyên tố.

TÀI LIỆU THAM KHẢO

[1] Đặng Hùng Thắng, Nguyễn Văn Ngọc, Vũ Kim Thuỷ - NXBGD, 1997.

[2] Nguyễn Vũ Lương, Nguyễn Ngọc Thắng, Nguyễn Lưu Sơn, Phạm Văn Hùng - NXB Đại Học Quốc Gia Hà Nội, 2006.

[3] Phan Huy Khải - Các chuyên đề Số học - NXBGD, 2005.

[4] Nguyễn Văn Mậu, Trần nam Dũng, Đặng Hùng Thắng, Đặng Huy Ruận - NXBGD, 2008.

[5] Nguyễn Sinh Nguyên, Nguyễn Văn Nho, Lê Hoành Phò - Tuyển tập các bài dự thi Olimpiad Toán học Quốc tế 1991 - 2001 - NXBGD, 2001.

[6] Titu Andreescu, Dorin Andrica, Zuming Feng - 104 Number theory problems from the training of the USA IMO team - NXB Birkhauser, 2006.

[5] Tạp chí Toán học và tuổi trẻ

[6] Các đề thi vô địch các nước.

[7] Các tài liệu trên mạng Internet.