ĐỊNH LÝ FERMAT NHỎ VÀ MỘT SỐ BÀI TOÁN ỨNG DỤNG

I. NỘI DUNG ĐỊNH LÝ

"Nếu a là một số nguyên dương và p là một số nguyên tố thì $\boxed{a^p \equiv a \pmod p}$ "

Chứng minh 1. Sử dụng phương pháp quy nạp theo a.

Với $a = 1$ thì mệnh đề luôn đúng.

Giả sử mệnh đề đúng đến a tức là $p \mid a^p - a$.

Ta sẽ chứng minh mệnh đề đúng đến $a + 1$. Thật vậy:

$$(a+1)^p - (a+1) = (a^p - a) + \sum_{k=1}^{p-1} C_p^k\, a^k$$

Sử dụng $p|C_p^k$ với $1 \le k \le p-1$ và giả thiết quy nạp ta suy ra

$p|(a+1)^p - (a+1)$. Khi đó $(a+1)^p \equiv (a+1) \pmod p$.

Vậy ta hoàn tất chứng minh.

Chứng minh 2. Giả sử rằng $\gcd(a, p) = 1$ và cần chứng minh rằng $a^{p-1} \equiv 1 \pmod p$.

Xét các số nguyên $a, 2a, \ldots, (p-1)a$ mà các số dư khi chia cho p phân biệt (nếu không thì, với $ia \equiv ja \pmod p$ thì $p|(i-j)a$ hay là $p|i-j$, dấu "=" xảy ra chỉ nếu $i = j$).

Do đó $a.(2a) \ldots (p-1)a \equiv 12 \ldots (p-1) \pmod p$.

Vì $\gcd(p, (p-1)!) = 1$ nên ta suy ra điều phải chứng minh.

Lưu ý. Định lý này có thể biết gọn dưới dạng: $\boxed{a^{p-1} \equiv 1 \pmod p}$

II. BÀI TẬP VẬN DỤNG

Bài 1. Cho p, q là hai số nguyên tố phân biệt. Chứng minh rằng $p^{q-1} + q^{p-1} - 1$ chia hết cho pq.

Lời giải

Áp dụng **định lý Fermat nhỏ** ta có $(p^q - p) \vdots q \Rightarrow p(p^{q-1} - 1) \vdots q$ (do q nguyên tố). (1)

Vì p, q là các số nguyên tố nên $\gcd(p, q)$=1.

Từ (1) suy ra $(p^{q-1} - 1) \vdots q$ (2)

Từ (2) suy ra $(p^{q-1} + q^{p-1} - 1) \vdots q$ (3)

Vì p và q có vai trò như nhau nên $(p^{q-1} + q^{p-1} - 1) \vdots p$ (4)

Lại vì $\gcd(p, q) = 1$ nên từ (3) và (4) ta suy ra điều phải chứng minh.

Bài 2. a) Cho a là một số nguyên dương. Chứng minh rằng bất cứ thừa số nguyên tố nào lớn hơn 2 của $a^2 + 1$ đều có dạng $4m + 1$.

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

Lời giải

a) Giả sử rằng: $p|a^2 + 1$ và $= 4m + 3, \forall\, m \in \mathbb{Z}$.
Thế thì $a^2 \equiv -1(\text{mod } p)$ và $a^{p-1} = (a^2)^{2m+1} \equiv (-1)^{2m+1} \equiv -1(\text{mod } p)$, mâu thuẫn với **định lý Fermat nhỏ**.

b) Số nguyên $(n!)^2 + 1$ có dạng $4m + 1$. Do đó tất cả các thừa số nguyên tố của nó cũng có dạng này. Giả sử rằng bất kì số nguyên tố p có dạng $4m + 1$, $(p!)^2$+1 là một số nguyên tố hoặc có một thừa số nguyên tố $p_1 > p$.

Bài 3. Chứng minh rằng với bất kì số nguyên tố p, $p^{p+1} + (p + 1)^p$ không phải là một số chính phương.

Lời giải

Với $p = 2$ thì $p^{p+1} + (p + 1)^p = 17$ không phải là số chính phương.

Giả sử ngược lại, $p \geq 3$ và $p^{p+1} + (p + 1)^p = t^2$ với mọi t nguyên dương.

Giả sử rằng $\left(t + p^{\frac{p+1}{2}}\right)\left(t - p^{\frac{p+1}{2}}\right) = (p + 1)^p$, do đó $t \pm p^{\frac{p+1}{2}} = 2^{p-1}u^p$ và $t \mp p^{\frac{p+1}{2}} = 2v^p$ với mọi u, v nguyên dương sao cho $2uv = p + 1$ và $(u, v) = 1$. Ta có: $p^{\frac{p+1}{2}} = |2^{p-2}u^p - v^p|$.

Sử dụng **định lý Fermat nhỏ** ta có $u^p \equiv u$ (mod p). $v^p \equiv v$ (mod p) và $2^{p-1} \equiv 1$ (mod p).

Vì vậy $u \equiv 2v$ (mod p). Từ $2uv = p + 1$ ta nhận được $u = 2v$ và cuối cùng $v = 1$ và $p = 3$. Dẫn đến $t^2 = 145$, một điều vô lý.

Bài 4. Cho $n \geq 2, a \geq 0$ là số nguyên dương và p là một số nguyên tố sao cho $a^p \equiv 1$ (mod p^n). Chứng tỏ rằng nếu $p > 2$ thì $a \equiv 1$ (mod p^{n-1}) và nếu $p = 2$ thì $a \equiv \pm 1$(mod 2^{n-1}).

Lời giải

Ta có $a^p \equiv 1$ (mod p^n) với $n \geq 2$, vì vậy $a^p \equiv 1$ (mod p).

Nhưng từ **định lý Fermat nhỏ**, $a^p \equiv a$ (mod p), do đó $a \equiv 1$ (mod p).

Với $a = 1$, kết quả là rõ ràng; nếu không, đặt $a = 1 + kp^d$, ở đây $d \geq 1$ và k không chia hết cho p.

Thế thì $p > 2$, $a^p = 1 + kp^{d+1} + Mp^{2d+1}$ với M là một số nguyên.

Do đó $d + 1 \geq n$ và vì vậy $s \equiv 1$ (mod p^{n-1}). Trong trường hợp $p = 2$, ta có $2^n | a^2 - 1 = (a - 1)(a + 1)$. Vì $a - 1 \neq 2, a + 1 \neq 2$ nên cả hai không thể là bội của 4. Do đó một trong hai $a + 1$ hoặc $a - 1$ chia hết cho 2^{n-1}, tức là $a \equiv \pm 1$ (mod 2^{n-1}) là như mong muốn.

Bài 5. (Bulgarian MO 1995). Tìm tất cả các số nguyên $n > 1$ sao cho $a^{25} - a$ chia hết cho n với mỗi số nguyên a.

Lời giải

Cho n là số thỏa mãn yêu cầu bài toán. Thế thì p^2 (p là một số nguyên tố) không chia hết n vì p^2 không chia hết $p^{25} - p$. Do đó n là bội của các số nguyên tố phân biệt. Mặt khác $a^{25} - 2 = 2.3^2.5.7.13.17.241$. nhưng n không chia hết cho 17 và 241 vì $3^{25} \equiv -3$ (mod 17) và $3^{25} \equiv 32$ (mod 241). Theo **định lý Fermat nhỏ** suy ra rằng $a^{25} \equiv a$ (mod p) khi $p \in \{2; 3; 5; 7; 13\}$. Như vậy n sẽ bằng với các ước của 2.3.5.7.13 , khác nhau từ 1 và có $2^5 - 1 = 31$ của chúng.

Bài 6. (6^{th}IMO).

a) Tìm tất cả các số nguyên dương n sao cho 7 chia hết $2^n - 1$.

b) Chứng minh rằng với mỗi số nguyên dương n số $2^n + 1$ không thể chia hết cho 7.

Lời giải

Định lý Fermat nhỏ cho ta: $2^6 \equiv 1$ (mod 7).

a) Từ $7|(2^3 - 1)(2^3 + 1)$ suy ra rằng $2^3 \equiv 1$ (mod 7).Do đó tất cả các số n mà chia hết cho 3 đều thỏa mãn yêu cầu bài toán.

b) Cho $n = 3k + r$ với $r = 1$ hoặc $r = 2$.

Thế thì $2^n = 2^{3k+r} \equiv (2^3)^k.2^r \equiv 2$ hoặc 4 (mod 7).

Do đó không thể có được $2^n \equiv -1$ (mod 7).

Bài 7. Tìm tất cả các số nguyên tố p sao cho $5^{p^2} + 1 \equiv 0$ (mod p^2).

Lời giải

Giả sử số nguyên tố p thỏa mãn điều kiện đã cho.

Khi đó $5^{2p^2} \equiv 1$ (mod p).

Vì $(p^2 - 1) \vdots p - 1$ nên theo **định lý Fermat nhỏ** ta có : $5^{2(p^2-1)} \equiv 1$ (mod p).

Từ đó suy ra $5^2 \equiv 1$ (mod p) nên $p \in \{2: 3\}$. Thử trực tiếp ta tìm được $p = 3$ thỏa mãn yêu cầu bài toán.

Bài 8. Chứng minh rằng với mọi số nguyên tố p, tồn tại vô số số nguyên dương n thỏa mãn: $(2^n - n) \vdots p$.

Lời giải

Nếu $p = 2$ thì mọi n chẵn đều thỏa mãn điều kiện đề bài nên không giảm tính tổng quát ta giả sử $p > 2$. Khi đó theo **định lý Fermat nhỏ** ta có: $2^{m(p-1)} \equiv 1$ (mod p).

Lấy $n = m(p-1)$ với $m \equiv -1 \pmod{p}$ ta có: $n = m(p-1) \equiv 1 \pmod{p}$ và

$2^n - n \equiv 2^n - 1 \equiv 0 \pmod{p}$.

Do có vô số số nguyên dương m sao cho $m \equiv -1 \pmod{p}$ nên tồn tại vô số số nguyên dương n thỏa mãn điều kiện đã cho. Điều phải chứng minh.

Bài 9. Cho p là số nguyên tố khác 2 và a, b là hai số tự nhiên lẻ sao cho $a+b$ chia hết cho p và $a-b$ chia hết cho $p-1$. Chứng minh rằng: $a^b + b^a$ chia hết cho $2p$.

Lời giải

Giả sử $a \geq b$.

Gọi r là dư trong phép chia a cho p thì $a \equiv r \pmod{p}$.

Do $(a+b) \vdots p$ nên $b \equiv -r \pmod{p}$.

Suy ra: $a^b + b^a \equiv r^b - r^a \pmod{p}$ hay $a^b + b^a \equiv r^b(1 - r^{a-b}) \pmod{p}$.

Mặt khác: $(a-b) \vdots (p-1)$ nên $a - b = k(p-1)$.

Vì r không chia hết cho p nên theo **định lý Fermat nhỏ** ta có:

$r^{p-1} \equiv 1 \pmod{p} \Longrightarrow r^{k(p-1)} \equiv 1 \pmod{p} \Longrightarrow r^{a-b} \equiv 1 \pmod{p}$.

Từ đó suy ra: $a^b + b^a \equiv 0 \pmod{p}$ tức là: $(a^b + b^a) \vdots p$.

Ngoài ra a^b, b^a là các số nguyên lẻ nên $(a^b + b^a) \vdots 2$.

Vậy $(a^b + b^a) \vdots 2p$.

Bài 10. Cho $p > 7$ là một số nguyên tố. Chứng minh rằng: $(3^p - 2^p - 1) \vdots 42p$.

Lời giải

Theo **định lý Fermat nhỏ** ta có:

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

Mặt khác $3^p - 2^p - 1 = [(3^p - 1) - 2^p] \vdots 2$.

Vì $p > 7$ là số nguyên tố nên p lẻ.

Khi đó $3^p - 2^p - 1 \equiv -(-1)^p - 1 \equiv 0 \pmod{3}$.

Cần chứng minh $3^p - 2^p - 1 \vdots 7$.

Ta có : $3^p - 2^p - 1 = 3.3^{p-1} - 2^p - 1 = 3.9^{\frac{p-1}{2}} - 2^p - 1 \equiv 3.2^{\frac{p-1}{2}} - 2^p - 1 \pmod{7}$.

Mà $3.2^{\frac{p-1}{2}} - 2^p - 1 = (2+1).2^{\frac{p-1}{2}} - 2^p - 1 = 2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1$ nên

$3^p - 2^p - 1 \equiv\ 2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1$ (mod 7).

Vì $(p, 3) = 1$ nên $p = 3k + 1, p = 3k + 2$.

Với $p = 3k + 1\ thì\ \ 2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1 = 8^k - 1 - 2^{\frac{p+1}{2}} - 2^p \equiv 2^p - 2^{\frac{p+1}{2}}$ (mod 7).

$2^p - 2^{\frac{p+1}{2}} = 2^{\frac{p+1}{2}}\left(2^{\frac{p-1}{2}} - 1\right) = 2^{\frac{p+1}{2}}(8^k - 1) \equiv 0$ (mod 7).

Suy ra $2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1 \equiv 0$ (mod 7).

Với $p = 3k + 2$ ta chứng minh tương tự như trên và thu được $2^{\frac{p+1}{2}} + 2^{\frac{p-1}{2}} - 2^p - 1 \equiv 0$ (mod 7).

Vậy ta hoàn tất chứng minh.

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

Lời giải

Ta có: $m = \frac{9^p-1}{8} = \frac{3^p-1}{2}.\frac{3^p+1}{4}$.

Vì $\frac{3^p-1}{2}.\frac{3^p+1}{4}$ đều là những số nguyên lớn hơn 1 nên m là hợp số.

Lại có $m = \frac{9^p-1}{8} = \frac{9^p-1}{9-1} = 9^{p-1} + 9^{p-2} + \cdots + 9 + 1 \equiv 1$ (mod 3), tức m không chia hết cho 3.

Hơn nữa, do p là số nguyên tố lẻ nên $p - 1$ là số chẵn. Để ý rằng 9^k có tận cùng là 9 nếu k lẻ và có tận cùng là 1 nếu k chẵn.

Thế thì $9^{p-1} + 9^{p-2} + \cdots + 9 = (9^{p-1} + 9^{p-2}) + (9^{p-3} + 9^{p-4}) + \cdots + (9^2 + 9^1)$.

Rõ ràng mỗi tổng trong dấu ngoặc có tận cùng là chữ số 0. Như vậy, m có tận cùng là chữ số 1 nên m lẻ.

Theo **định lý Fermat nhỏ** thì $9^p \equiv 9$ (mod p).

Vì $9^p \equiv 9$ (mod 8) và $(p; 8) = 1$ nên $9^p \equiv 9$ (mod $8p$).

Điều này nghĩa là $m - 1 = \frac{9^p-9}{8} \vdots p$.

Do m lẻ nên $m - 1$ chẵn và $(2, p) = 1$ dẫn đến $(m - 1) \vdots 2p$.

Vì lý do đó mà $(3^{m-1} - 1) \vdots (2^{2p} - 1) \Longrightarrow (3^{m-1} - 1) \vdots m$ (do $(3^{2p} - 1) \vdots 8m$).

Nói cách khác $3^{m-1} \equiv 1$ (mod m).

Bài 12. Cho p là số nguyên tố bất kỳ khác 2 và khác 5. Chứng minh rằng trong dãy 9,99,999,9999,… có vô số số hạng chia hết cho p.

Lời giải

Do p là số nguyên tố khác 2 và khác 5 nên gcd$(p, 10)$=1. (1)

Vì p là số nguyên tố nên theo **định lý Fermat nhỏ**, ta có:

$(10^p - 10) \vdots p \Longrightarrow 10(10^{p-1} - 1) \vdots p$ (2)

Từ (1) và (2) suy ra: $(10^{p-1} - 1) \vdots p \Longrightarrow 10^{p-1} \equiv 1$ (mod p).

Do đó, với mọi n nguyên dương thì $10^{n(p-1)} \equiv 1$ (mod p) $\Longrightarrow \left(10^{n(p-1)} - 1\right) \vdots p$ với n nguyên dương.

Mặt khác, $10^{n(p-1)} - 1 = \underbrace{99 \ldots 9}_{n(p-1)}$. Từ đó suy ra tồn tại vô số số hạng của dãy 9,99,999,9999,… chia hết cho p.

Bài 13. (Gặp gỡ Toán học năm 2011). Chứng minh rằng:

a) Số nguyên dạng $x^2 + 1$ không có ước nguyên tố dạng $4k + 3$

b) Số nguyên dạng $x^2 + 3$ không có ước nguyên tố dạng $6k + 5$

Lời giải

a) Giả sử tồn tại $p = 4k + 3$ sao cho $(x^2 + 1) \vdots p$. Điều này có nghĩa là $x^2 \equiv -1(mod\, p)$.

Suy ra $(x^2)^{2k+1} \equiv -1(mod\, p)$ hay $x^{4k+2} \equiv -1(mod\, p)$, mâu thuẫn với **định lý Fermat nhỏ**. Vậy ta suy ra điều phải chứng minh.

b) Giả sử ngược lại, tồn tại x và $p = 6k + 5$ sao cho $x^2 + 3 \equiv 0(mod\, p)$. $(*)$

Nếu x thỏa $(*)$ thì $x + p$ cũng thỏa $(*)$. Khi đó ta có thể giả sử x lẻ, tức là $x = 2y + 1$.

Suy ra $4y^2 + 4y + 4 \equiv 0(mod\, p)$.

Do $\gcd(p, 4) = 1$ nên $y^2 + y + 1 \equiv 0(mod\, p)$.

Dẫn đến $y^3 \equiv 1(mod\, p) \Rightarrow y^{6k+3} = 1(mod\, p)$.

Mặt khác, theo **định lý Fermat nhỏ** thì $y^{6k+4} \equiv 1(mod\, p)$.

Suy ra $y \equiv 1(mod\, p) \Rightarrow 3 \equiv 0(mod\, p)$, mâu thuẫn.

Vậy điều giả sử ở trên là sai và ta đi đến điều phải chứng minh.

Bài 14. (IMO 2015). Xét dãy số $a_1, a_2, \ldots$ xác định bởi $a_n = 2^n + 3^n + 6^n - 1$ với tất cả số nguyên dương n. Xác định tất cả các số nguyên dương nguyên tố cùng nhau với mỗi số hạng của dãy.

Lời giải

Ta thấy rằng mỗi số nguyên tố $p | a_n$ với mọi số nguyên dương n. Để ý rằng cả $p = 2$ và $p = 3$ đều chia hết $a_2 = 2^2 + 3^2 + 6^2 - 1 = 48$.

Bây giờ giả sử rằng $p \geq 5$. Áp dụng **định lý Fermat nhỏ** ta có:

$2^{p-1} \equiv 3^{p-1} \equiv 6^{p-1} \equiv 1(mod\, p)$.

Khi đó $3.2^{p-1} + 2.3^{p-1} + 6^{p-1} \equiv 3 + 2 + 1 \equiv 6(mod\, 6)$ hay $6(2^{p-2} + 3^{p-2} + 6^{p-2} - 1) \equiv 0(mod\, p)$. Suy ra $6a_{p-2} \vdots p$.

Vì $\gcd(p, 6) = 1, a_p \vdots p$ nên ta suy ra điều phải chứng minh.

Bài 15. Cho p là một số nguyên tố. Chứng minh rằng $(xy^p - yx^p) \vdots p$ với mọi a, b nguyên.

Lời giải

Để ý rằng $xy^p - yx^p = xy(y^{p-1} - x^{p-1})$.

Nếu $p|xy$ thì $p|xy^p - x^py$; nếu $p \nmid xy$ thì $\gcd(p, x) = gcd(p, y) = 1$ và vì vậy $y^{p-1} \equiv x^{p-1} \equiv 1(mod\, p)$ (theo **định lý Fermat nhỏ**).

Do đó $p \mid y^{p-1} - x^{p-1}$. Suy ra rằng $p + xy^p - yx^p$. Vậy thì $p \mid xy^p - x^py$ với mọi p.

Bài 16. (Turkish MO 1995). Chứng minh rằng các mệnh đề sau đây là tương đương:

(i). Với bất kì số nguyên dương $a, n \mid a^n - a$;

(ii). Với bất kì ước số nguyên tố p của $n, p^2 \nmid n$ và $p - 1 \mid n - 1$.

Lời giải

Trước hết, giả sử ta có (i). Nếu $p^2|n$ với mọi số nguyên tố p thì ta phải có

$$p^2 \mid (p+1)^{p^2} - (p+1) = p^2 - p + \sum_{k=2}^{p^2} C_{p^2}^k p^k.$$

Tất cả số hạng mà đầu tiên chia hết cho p^2, mâu thuẫn với điều giả sử.

Do đó $p^2 \nmid n$. Ngoài ra, nếu a là một căn nguyên thủy modulo p thì

$a^{n-1} \equiv 1(mod\, p) \Rightarrow p - 1 \mid n - 1$.

Mặt khác, nếu n là số không chính phương và $p - 1 \mid n - 1$ với mọi số nguyên tố $p \mid$ n, khi đó với bất kì a, hoặc $p|a$ hoặc $a^{p-1} \equiv 1(mod\, p)$; hoặc trong trường hợp $a^n \equiv a(mod\, p)$ với tất cả $p \mid$ n.

Vậy ta hoàn tất chứng minh.

Bài 17. (VMO 2011).

Cho dãy số nguyên $\{u_n\}$ xác định bởi:

$u_{0=1, u_1=-1, u_n} = 6u_{n-1} + 5u_{n-2} \quad \forall n \geq 2.$

Chứng minh rằng: $u_{2012} - 2010$ chia hết cho 2011.

Lời giải 1

Xét số nguyên $\{v_n\}$ xác định bởi: $v_0 = 1, v_1 = -1$ và

$v_n = 6v_{n-1} + 2016v_{n-2} \forall n \geq 2.$

Dễ thấy $\forall n \epsilon \mathbb{N}$ ta có: $u_n \equiv v_n (mod\, 2011)$.

Phương trình đặc trưng của dãy $\{v_n\}$ có dạng:

$\lambda^2 - 6\lambda - 2016 = 0 \Leftrightarrow \left[\begin{smallmatrix}\lambda=-42\\ \lambda=48\end{smallmatrix}\right.$.

Số hạng tổng quát của dãy $\{v_n\}$ có dạng: $v_n = A.(-42)^n + B.48^n$.

Từ các điều kiện ban đầu của dãy $\{v_n\}$ ta suy ra: $A = \frac{49}{90}, B = \frac{41}{90}$.

Như vậy $v_n = \frac{49.(-42)^n + 41.48^n}{90}\ \forall n \in \mathbb{N}$.

Vì 2011 là số nguyên tố nên theo **định lý Fermat nhỏ** ta có:

$(-42)^{2010} \equiv 48^{2010} \equiv 1 (mod\, 2011)$.

Do đó:

$90\mathrm{v}_{2012} \equiv 49.(-42)^{2012} + 41.48^{2012} \equiv 49.(-42)^2 + 41.48^2 \equiv 90\mathrm{v}_2 (\mathrm{mod}\, 2011)$.

Suy ra: $\mathrm{V}_{2012} \equiv \mathrm{v}_2 (\mathrm{mod}\, 2011)$ (vì $(90{,}2011) = 1$).

Mà $v_2 = 6v_1 + 2016v_0 = 2010$ nên $v_{2012} \equiv 2010 (\mathrm{mod}\, 2011)$. Vì thế

$u_{2012} \equiv 2010 (mod\, 2011)$.

Lời giải 2

Số hạng tổng quát của dãy $\{u_n\}$ là:

$u_n = \left(\frac{1}{2} - \frac{2}{\sqrt{14}}\right)\left(3 + \sqrt{14}\right)^n + \left(\frac{1}{2} + \frac{2}{\sqrt{14}}\right)\left(3 - \sqrt{14}\right)^n$.

Đặt $p = 2011$, ta có:

$u_{p+1} = \left(\frac{1}{2} - \frac{2}{\sqrt{14}}\right)\left(3 + \sqrt{14}\right)^{p+1} + \left(\frac{1}{2} + \frac{2}{\sqrt{14}}\right)\left(3 - \sqrt{14}\right)^{p+1}$.

Do $\left(3 + \sqrt{14}\right)^{p+1} = A_{p+1} + B_{p+1}.\sqrt{14}$; $\left(3 - \sqrt{14}\right)^{p+1} = A_{p+1} - B_{p+1}.\sqrt{14}$,

trong đó: $A_{p+1} = \sum_{i=0}^{\frac{p+1}{2}} C_{p+1}^{2i}.3^{2i}.14^{\frac{p+1}{2}-i}$; $B_{p+1} = \sum_{i=0}^{\frac{p+1}{2}} C_{p+1}^{2i-1}.3^{2i-1}.14^{\frac{p+1}{2}-i}$,

nên $u_{p+1} = A_{p+1} - 4B_{p+1}$.

Do p là số nguyên tố nên $C_p^k \equiv 0 (mod\, p) \forall k = \overline{1, p-1}$.

Vì thế, từ $C_{p+1}^k = C_p^k + C_p^{k-1}$ suy ra $c_{p+1}^k \equiv 0 (mod\, p) \forall k = \overline{2, p-1}$.

Khi đó: $A_{p+1} \equiv \left(14^{\frac{p+1}{2}} + 3^{p+1}\right)(mod\, p)$;

$B_{p+1} \equiv 3(p+1)\left(14^{\frac{p-1}{2}} + 3^{p-1}\right) \equiv 3\left(14^{\frac{p-1}{2}} + 3^{p-1}\right)(mod\, p)$.

Để ý rằng:$45^2 \equiv 14(mod\ p), (45, p) = 1$ nên theo **định lý Fermat nhỏ** ta có:

$3^p \equiv 3(mod\ p)$ và $14^{\frac{p-1}{2}} \equiv 45^{p-1} \equiv 1(mod\ p)$.

Vậy $u_{2012} = u_{p+1} \equiv -3 + 2 = -1 \equiv 2010(mod\ 2011)$.

Bài 18. Cho dãy số $\{u_n\}$ được xác định bởi công thức: $\begin{cases} u_1 = 5, u_2 = 7 \\ u_{n+1} = u_n^3 + 6u_{n-1} + 3.2^{2008} \end{cases}$.

Chứng minh rằng $\{u_n\}$ không thể biểu diễn được dưới dạng tổng lũy thừa bậc 6 của ba số nguyên dương.

Lời giải

Xét $A = a^6 + b^6 + c^6$.

Theo **định lý Fermat nhỏ** ta có: $x^{13} \equiv x(mod\ p) \Leftrightarrow x(x^6 - 1)(x^6 + 1) \equiv 0(mod\ 13) \Leftrightarrow \left[\begin{array}{l} x^6 \equiv 0 \\ x^6 \equiv 1 \\ x^6 \equiv -1 \end{array}\right. (mod\ 13)$.

Vậy bô thặng dư của A mod 13 là: $S = \{0; \pm 1; \pm 2; \pm 3\}$.

Ta có: $\begin{cases} u_3 \equiv 382 \equiv 5(mod\ 13) \\ u_4 \equiv 176 \equiv 7(mod\ 13) \end{cases} \Rightarrow$ số dư của u_n khi chia cho 13 tuần hoàn với chu kì 2. $\Leftrightarrow u_n \equiv u_{n-2}(mod\ 13) \Leftrightarrow \begin{cases} u_{2n} \equiv u_2 \equiv 7(mod\ 13) \\ u_{2n+1} \equiv u_1 \equiv 5(mod\ 13) \end{cases} \Rightarrow \left[\begin{array}{l} u_n \equiv 5 \\ u_n \equiv 7 \end{array}\right.(mod\ 13)$.

Mà 5;7 ∉ S.

Vậy u_n không thể biểu diễn được dưới dạng tổng lũy thừa bậc 6 của 3 số nguyên dương.

Bài 19. Tìm các cặp số nguyên x, y sao cho $101 \mid (x^2 + xy + y^2 + 14(x + y) + 2018)$.

Lời giải

Vì gcd(4,101) = 1 nên điều kiện đã cho tương đương với

$101 \mid (4(x^2 + xy + y^2 + 14(x + y) + 2018)) \Leftrightarrow 101 \mid ((2x + y + 14)^2 + 3y^2 + 28y + 7876 - 202y - 5353) \Leftrightarrow 101 \mid (2x + y + 14)^2 + 3(y - 29)^2$ (1)

Đặt $u = 2x + y + 14, v = y - 29$.

Khi đó (1) trở thành $101 \mid u^2 + 3v^2 \Leftrightarrow u^2 \equiv -3v^2(mod\ 101)$ (2)

Giả sử $\gcd(u, 101) = 1$ tức là u không chia hết cho 101. Do 101 là số nguyên tố nên từ (2) suy ra y không chia hết cho 101, tức là $\gcd(v, 101) = 1$. Lúc này theo **định lý Fermat nhỏ** ta có: $(u^{101} - u) \vdots 101 \Rightarrow u(u^{100} - 1) \vdots 101$.

Vì $\gcd(u, 101) = 1$ nên $(u^{100} - 1) \vdots 101$ hay $1 \equiv u^{100}(mod\ 101)$.

Từ (2) suy ra $u^{100} \equiv (-3y)^{50} \equiv (-3)^{50}v^{100} \equiv (-3)^{50} \equiv -1(mod\ 101)$.

Như vậy $1 \equiv -1(mod\ 101)$ là một điều vô lý, cho nên $\gcd(u, 101) > 1$.

Khi đó (2)$\Leftrightarrow u \equiv v(mod\ 101) \Leftrightarrow \begin{cases} 2x + y + 14 \equiv 0(mod\ 101) \\ y - 29 \equiv 0(mod\ 101) \end{cases}$.

Từ $y \equiv 29(mod\ 101)$ thay lại hệ thức ở trên ta thu được:

$2x \equiv -43 \equiv 58(mod\ 101) \Leftrightarrow x \equiv 29(mod\ 101)$.

Do đó (2)$\Leftrightarrow x \equiv y \equiv 29(mod\ 101)$.

Vậy $(x, y) = (29 + 101t; 29 + 101s)$ với t, s là các số nguyên.

Bài 20. (diendantoanhoc.net 2014). Giả sử phương trình $x^{2017} + ax^2 + bx + c = 0$ với các hệ số nguyên a, b, c có 3 nghiệm nguyên là x_1, x_2, x_3. Chứng minh rằng:

$(a + b + c + 1)(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ chia hết cho 2017.

Lời giải

Phương trình đã cho tương đương với:

$(x^{2017} - x) + [ax^2 + (b + 1)x + c] = 0$.

Đặt $f(x) = ax^2 + bx + c$.

Theo **định lý Fermat nhỏ** ta có$(x_i^{2017} - x_i) \vdots 2017$ với mọi $i = 1,2,3$ cho nên $f(x) \vdots 2017$ với mọi $i = 1,2,3$.

Nếu $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \vdots 2017$ thì bài toán được chứng minh.

Nếu $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \quad 2017$ thì theo chứng minh trên suy ra:

$\begin{cases} \left(f(x_1) - f(x_2)\right) \vdots 2017 \\ \left(f(x_2) - f(x_3)\right) \vdots 2017 \end{cases} \Leftrightarrow \begin{cases} (x_1 - x_2)[a(x_1 + x_2) + b + 1] \vdots 2017 \\ (x_2 - x_1)[a(x_2 + x_3) + b + 1] \vdots 2017 \end{cases}$.

Suy ra $\begin{cases} [a(x_1 + x_2) + b + 1] \vdots 2017 \\ [a(x_2 + x_3) + b + 1] \vdots 2017 \end{cases} \Rightarrow a(x_3 - x_1) \vdots 2017 \Rightarrow a \vdots 2017$.

Từ đó suy ra $(b + 1) \vdots 2017$ mà $f(x) = [ax^2 + (b + 1)x + c] \vdots 2017$ nên $c \vdots 2017$.

Từ đó suy ra $(a + b + c + 1) \vdots 2017$.

Tóm lại, $(a + b + c + 1)(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \vdots 2017$.