CHINH PHỤC OLYMPIC TOÁN
TẠP CHÍ VÀ TƯ LIỆU TOÁN HỌC

NUMBER THEORY

Legendre SYMBOL

HAPPY NEW YEAR 2020

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

DOÃN QUANG TIẾN – NGUYỄN MINH TUẤN

LEGENDRE SYMBOL

Chịu trách nhiệm nội dung. Doãn Quang Tiến
Biên tập. Nguyễn Minh Tuấn

Ngày 24 tháng 1 năm 2020

Tóm tắt nội dung

Trong bài viết này, chúng tôi sẽ đề cập tới một vấn đề tương đối thú vị và có nhiều ứng dụng trong số học đó là kí hiệu Legendre hay thặng dư bình phương. Bài viết cung cấp cho bạn đọc lý thuyết đầy đủ cũng như các bài toán xuất hiện trong các kì thi chọn đội tuyển, olympic trong nước và khu vực, đồng thời chúng tôi có tham khảo một số nguồn tài liệu của các tác giả trong và ngoài nước, bạn đọc có thể xem ở phần tài liệu tham khảo. Bây giờ chúng ta sẽ bắt đầu tìm hiểu vấn đề này qua định nghĩa đầu tiên, đó là kí hiệu Legendre - Bài viết được trích từ cuốn **Khai thác một số chủ đề số học hay và khó, Doãn Quang Tiến ft Huỳnh Kim Linh.**

1 Lý thuyết

1.1 Kí hiệu Legendre

Định nghĩa 1

Cho số nguyên dương n, số nguyên a được gọi là thặng dư bình phương mod$n$ (hay số chính phương modulo n) nếu $(a,n)=1$ và phương trình $x^2 \equiv a \,(\mathrm{mod} n)$ có nghiệm.

Từ định nghĩa này ta có các các định lý sau.

Định lý

Định lý 1.Giả sử p là số nguyên tố lẻ, a là số nguyên không chia hết cho p.
Khi đó, phương trình trình $x^2 \equiv a(\mathrm{mod} p)$ hoặc vô nghiệm hoặc có 2 nghiệm không đồng dư modulo n.
Định lý 2. Nếu p là số nguyên tố lẻ thì trong các số $1,2,\ldots,p-1$ có đúng $\dfrac{p-1}{2}$ thặng dư bình phương mod$p$.

Chứng minh.
Ta sẽ tiến hành bình phương các số $1,2,...,p-1$ lên.
Giả sử a là một thặng dư bình phương mod n. Ta nhận thấy rằng, nếu T là một số trong các số $\{1,\ 2,...,\ p-1\}$ thì $T^2 \equiv (p-T)^2(\mathrm{mod} p)$.
Do đó, phương trình $x^2 \equiv a(\mathrm{mod} p)$ có đúng hai nghiệm mà bình phương có cùng thặng dư a. Mà có tổng cộng $p-1$ số nên sẽ có $\dfrac{p-1}{2}$ thặng dư bình phương mod$p$. □

Nhận xét. Giả sử p là số nguyên tố lẻ, a là số nguyên không chia hết cho p. Kí hiệu Legendre là $\left(\dfrac{a}{p}\right)$. Khi đó $\left(\dfrac{a}{p}\right)$ được xác định như sau.

Định nghĩa 2

Giả sử p là một số nguyên tố lẻ, a là số nguyên không chia hết cho p. Khi đó

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

Chứng minh.

Trước tiên, giả sử $\left(\frac{a}{p}\right) = 1$. Khi đó đồng dư $x^2 \equiv a(\mathrm{mod} p)$ có nghiệm $x = x_0$.

Theo ***định lý Fermat nhỏ***, ta có

$$a^{\frac{p-1}{2}} \equiv \left(x_0^2\right)^{\frac{p-1}{2}} \equiv 1 \, (\mathrm{mod} p)$$

Xét trường hợp $\left(\frac{a}{p}\right) = -1$. Khi đó , đồng dư $x^2 \equiv a(\mathrm{mod} p)$ vô nghiệm. Với mỗi i từ 1 đến $(p-1)$, tồn tại duy nhất j, $1 \leqslant j \leqslant p-1$ sao cho tích $i.j \equiv a(\mathrm{mod} p)$. Rõ ràng i khác j nên có thể nhóm các số từ 1 đến $p-1$ thành $\frac{p-1}{2}$ cặp, sao cho tích hai số trong mỗi cặp đều đồng dư a modulo p.

Nhân tất cả các số $1, 2, ..., p-1$, ta được

$$(p-1)! \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$$

Theo ***định lý Wilson***, thì $(p-1)! \equiv -1(\mathrm{mod} p)$.

Định lý được chứng minh. □

Từ ***tiêu chuẩn Euler*** và định nghĩa ***Legendre***, ta dễ dàng chứng minh các tính chất sau.

Định lý 3

Giả sử p là một số nguyên tố lẻ, a và b là những số nguyên không chia hết cho p. Khi đó thì

i. Nếu $a \equiv b(\mathrm{mod} p)$ thì $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

ii. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

iii. $\left(\frac{a^2}{p}\right) = 1$

(i) Nếu $a \equiv b(\mathrm{mod} p)$ thì $x^2 \equiv a(\mathrm{mod} p)$ có nghiệm khi và chỉ khi $x^2 \equiv b(\mathrm{mod} p)$ có nghiệm, do vậy ta được

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$

(ii) Theo ***tiêu chuẩn Euler*** ta có

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p), \left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} (\mathrm{mod} p), \left(\frac{ab}{p}\right) \equiv ab^{\frac{p-1}{2}} (\mathrm{mod} p)$$

Khi đó ta được

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) (\mathrm{mod} p)$$

Vì vậy giá trị của ***kí hiệu Legendre*** chỉ có thể là ± 1 nên ta có đẳng thức cần chứng minh.

(iii) Vì $\left(\frac{a}{p}\right) = \pm 1$ nên từ phần trên ta có

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1$$

Định lí trên cho thấy rằng tích của hai thặng dư bình phương hoặc hai không thặng dư bình phương là một thặng dư bình phương, tích của một thặng dư bình phương và một không thặng dư bình phương là một không thặng dư bình phương. Ngoài ra, nhờ ***tiêu chuẩn Euler***, ta cũng sẽ biết được khi nào -1 là một số chính phương modulo p. □

Định lý 4

Nếu p là một số nguyên tố lẻ thì

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{khi} \quad p \equiv 1(\text{mod}4) \\ -1 & \text{khi} \quad p \equiv -1(\text{mod}4) \end{cases}$$

Chứng minh.
Theo ***tiêu chuẩn Euler*** ta có

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}(\text{mod}p)$$

Nếu $p \equiv 1(\text{mod}4)$ thì $p = 4k+1$ với k là số nguyên nào đó. Như vậy ta có

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

Hay $\left(\frac{-1}{p}\right) = 1$. Tiếp tục xét trường hợp thứ 2.
Nếu $p \equiv -1(\text{mod}4)$ thì $p = 4k+3$ với k là số nguyên nào đó. Như vậy ta có

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

Hay $\left(\frac{-1}{p}\right) = -1$.
Vậy định lý được chứng minh. □

Định lý 5

Giả sử $(x;y) = 1, a, b, c$ là các số nguyên p là 1 ước nguyên tố của $ax^2+bxy+cy^2$, p không là ước của abc thì $D = b^2 - 4ac$ là thặng dư bậc 2 mod p. Đặc biệt nếu p là ước của $x^2 - Dy^2$ và $(x,y) = 1$ thì D là thặng dư bậc 2 mod p.

Chứng minh. Đặt $N = ax^2+bxy+cy^2$ thì từ $4aN = (2ax+by)^2 - Dy^2$ ta có

$$(2ax+by)^2 \equiv Dy^2(\text{mod}p)$$

Hơn nữa y không chia hết cho p; nếu không thì p chia hết cho $2ax+by$ và x, điều này trái với giả thiết. Vậy $(y,p) = 1$ nên tồn tại yy' sao cho $yy' \equiv 1(\text{mod}p)$, suy ra $(2axy'+byy')^2 \equiv D\,(yy')^2 \equiv D(\text{mod}p)$. Vậy D là thặng dư bình phương modulo p. Cho a là một số nguyên, p là một số nguyên tố sao cho $(a,p) = 1$. Với mỗi $k = 1, 2, \ldots, p'$ tồn tại $r_k \in \{\pm 1, \pm 2, \ldots, \pm p'\}$ sao cho $ka \equiv r_k(\text{mod}p)$, dễ thấy không tồn tại hai số r_k có cùng giá trị tuyệt đối, do đó $|r_1|, |r_2|, \ldots, |r_{p'}|$ là một hoán vị của tập hợp $\{1, 2, \ldots, p'\}$.
Cho k chạy rừ 1 đến p' rồi nhân các vế với nhau ta được

$$a^{p'} \equiv \frac{r_1 \ldots r_{p'}}{1.2 \ldots p'} = \frac{r_1 \ldots r_{p'}}{|r_1| \ldots |r_{p'}|}(\text{mod}p)$$

Đặt $\varepsilon_k = \dfrac{r_k}{|r_k|}; \varepsilon_k = \pm 1$ ta có $a^{p'} \equiv \varepsilon_{1...} \cdot \varepsilon_{p'} (\mathrm{mod} p)$. Ta có $\varepsilon_k = -1$ khi và chỉ khi phần dư khi chia ka cho p lớn hơn p', khi đó ta được

$$\frac{2ka}{p} = 2p + \frac{2r}{p} \Leftrightarrow \left[\frac{2ka}{p}\right] = 2\left[\frac{ka}{p}\right] + 1$$

Suy ra $r_k = (-1)^{\left[\frac{2ka}{p}\right]}$. Như vậy ta có

$$a^{p'} \equiv (-1)^{\sum\limits_{k=1}^{p'} \left[\frac{2ka}{p}\right]}$$

Định lý được chứng minh. □

Định lý 6

Bổ đề Gauss

Giả sử p là một số nguyên tố lẻ, a là số nguyên không chia hết cho p. Nếu trong số các thặng dư dương bé nhất của các số nguyên $a, 2a, 3a, ..., \dfrac{p-1}{2}a$ có s thặng dư lớn hơn $\dfrac{p}{2}$ thì

$$\left(\frac{a}{p}\right) = (-1)^s$$

Chứng minh.

Trong số các thặng dư dương bé nhất của các số nguyên $a, 2a, 3a, ..., \dfrac{p-1}{2}a$. Giả sử $u_1, u_2, ..., u_s$ là các thặng dư lớn hơn $\dfrac{p}{2}$ và $v_1, v_2, ..., v_t$ là các thặng dư bé hơn $\dfrac{p}{2}$.

Vì $(ja, p) = 1$ với mọi j, $1 \leqslant j \leqslant \dfrac{p-1}{2}$ nên mọi u_i, v_j đều khác 0, tức là thuộc tập hợp $1, 2, ..., p-1$. Ta sẽ chứng minh rằng, tập hợp $p-u_1, p-u_2, ..., p-u_s; v_1, v_2, ..., v_t$ chính là tập hợp các số $1, 2, ..., \dfrac{p-1}{2}$ xếp theo thứ tự nào đó. Rõ ràng không có hai số u_i nào, cũng như không có hai số v_j nào đồng dư modulo p.

Thật vậy, nếu ngược lại ta sẽ có $ma \equiv na (\mathrm{mod}\ p)$, mâu thuẫn. Tương tự như trên, có thể thấy rằng không có số $p - u_i$ nào đồng dư với v_j.

Như vậy ta có

$$(p-u_1)(p-u_2)...(p-u_s)v_1, v_2, ..., v_t \equiv \frac{p-1}{2}! \, (\mathrm{mod} p)$$

Mặt khác, vì $u_1, u_2, ..., u_s$; $v_1, v_2, ..., v_t$ là các thặng dư dương bé nhất của $a, 2a, 3a, ..., \dfrac{p-1}{2}a$ modulo p nên

$$u_1u_2...u_s.v_1v_2...v_t \equiv a^{\frac{p-1}{2}} \frac{p-1}{2}! \, (\mathrm{mod} p)$$

Như vậy ta có

$$(-1)^s a^{\frac{p-1}{2}} \frac{p-1}{2}! \equiv \frac{p-1}{2}! \, (\mathrm{mod} p)$$

Do p và $\dfrac{p-1}{2}!$ nguyên tố cùng nhau nên suy ra

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

Tức là $a^{\frac{p-1}{2}} \equiv (-1)^s \, (\mathrm{mod} p)$.

Định lí suy ra từ ***tiêu chuẩn Euler***. □

Định lý 7

Nếu p là số nguyên tố lẻ thì

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Như vậy, 2 là só chính phương modulo p khi và chỉ khi $p \equiv \pm 1 \,(\text{mod} 8)$

Chứng minh.

Áp dụng ***bổ đề Gauss***, ta cần tìm số thặng dư dương bé nhất lớn hơn $\frac{p}{2}$ của dãy số

$$1.2, 2.2, ..., \frac{p-1}{2}.2$$

Vì các số đều nhỏ hơn p nên đều trùng với thặng dư dương bé nhất của chúng. Như vậy, chỉ cần tính số các số của dãy lớn hơn $\frac{p}{2}$. Số các số như vậy là

$$s = \frac{p-1}{2} - \left[\frac{p}{4}\right]$$

Như vậy, ta có

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} - \left[\frac{p}{4}\right]}$$

Bằng cách xét các trường hợp $p \equiv 1, 3, 5, 7 \pmod 8$, dễ dàng chứng minh đồng dư

$$\frac{p-1}{2} - \left[\frac{p}{4}\right] \equiv \frac{p^2-1}{8} \,(\text{mod} 2)$$

Khi đó định lí suy ra từ ***bổ đề Gauss.*** □

Một số mở rộng.

1. -2 là số chính phương modulo p khi và chỉ khi $p \equiv 1, 3 \,(\text{mod} 8)$

2. 3 là số chính phương modulo p khi và chỉ khi $p \equiv \pm 1 \,(\text{mod} 12)$

3. -3 là số chính phương modulo p khi và chỉ khi $p \equiv 1 \,(\text{mod} 6)$

4. 5 là thặng dư bậc 2 mod p khi và chỉ khi $p \equiv \pm 1 (\text{mod} 10)$.

5. $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$

Định lý 8

Luật tương hỗ Gauss

Giả sử p và q là những số nguyên tố lẻ khác nhau. Khi đó, ta có

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

Chứng minh.

Để chứng minh định lí trên, trước hết ta cần chứng minh bổ đề sau.

Bổ đề. Giả sử p là số nguyên tố lẻ, a là số lẻ không chia hết cho p .

Khi đó $\left(\frac{a}{p}\right) = (-1)^{T(a,p)}$ trong đó $T(a,p) = \sum_{j=1}^{\frac{p-1}{2}} \left[\frac{ja}{p}\right]$.

Chứng minh.

Xét các thặng dư dương bé nhất của các số nguyên $a, 2a, 3a, ..., \frac{p-1}{2}a$. Như trước đây, kí hiệu $u_1, u_2, ..., u_s$; $v_1, v_2, ..., v_t$ là các thặng dư lớn hơn và bé hơn $\frac{p}{2}$, tương ứng.

Từ ***phép chia Euclide*** ta có

$$ja = p\left[\frac{ja}{p}\right] + \text{phần dư}$$

trong đó phần dư là một trong các số u_i hoặc v_j.
Cộng từng vế $\frac{p-1}{2}$ phương trình ta được

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ja}{p}\right] + \sum_{i=1}^{s} u_i + \sum_{j=1}^{t} v_j$$

Như đã chỉ ra trong chứng minh ***bổ đề Gauss***, tập hợp

$$p-u_1, p-u_2, ..., p-u_s; v_1, v_2, ..., v_t$$

chính là tập hợp các số $1, 2, ..., \frac{p-1}{2}$ xếp theo thứ tự nào đó.
Do đó ta có

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{s} (p-u_i) + \sum_{j=1}^{t} v_j = ps - \sum_{i=1}^{s} u_i + \sum_{j=1}^{t} v_j$$

Từ đó suy ra

$$\sum_{j=1}^{\frac{p-1}{2}} ja - \sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{\frac{p-1}{2}} p\left[\frac{ia}{p}\right] - ps + 2.\sum_{i=1}^{s} u_i$$

Từ công thức của $T(a,p)$ ta nhận được

$$(a-1)\sum_{j=1}^{\frac{p-1}{2}} j = pT(a,p) - ps + 2.\sum_{i=1}^{s} u_i$$

Do a, p lẻ nên suy ra $T(a,p) \equiv s \pmod 2$. Từ ***bổ đề Gauss*** ta có điều phải chứng minh.
Chứng minh luật thuận nghịch.
Xét các cặp số nguyên (x,y) với $1 \leqslant x \leqslant \frac{p-1}{2}$ và $1 \leqslant y \leqslant \frac{q-1}{2}$, có tất cả $\frac{p-1}{2}.\frac{q-1}{2}$ cặp như vậy. Ta sẽ chia các cặp đó thành hai nhóm, tùy thuộc độ lớn của px và qy. Do p, q là những số nguyên tố khác nhau nên $px \neq qy$ với mọi cặp (x,y).
Xét các cặp với $qx > py$. Với mỗi giá trị cố định của x , $1 \leqslant x \leqslant \frac{p-1}{2}$, tồn tại $\left[\frac{qx}{p}\right]$ số nguyên y thỏa mãn $1 \leqslant y \leqslant \frac{qx}{p}$. Như vậy, số các cặp đang xét là $\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right]$. Xét các cặp với $qx < py$. Tương tự như trên, số các cặp thỏa mãn điều kiện này là $\sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right]$. Vì có tất cả là $\frac{p-1}{2}.\frac{q-1}{2}$ cặp nên ta nhận được đẳng thức sau

$$\sum_{j=1}^{\frac{p-1}{2}} \left[\frac{jq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] = \frac{p-1}{2}.\frac{q-1}{2}$$

Từ định nghĩa của $T(p,q)$ ta có

$$(-1)^{T(p,q)+T(q,p)} = (-1)^{\frac{p-1}{2}.\frac{q-1}{2}}$$

Định lí suy ra từ bổ đề. □
Nhận xét. Qua các định lí trên, chúng ta có thể chứng minh được một số là số chính phương modulo p. Tuy nhiên, các định lí trên cũng có một điểm bất lợi là chỉ áp dụng được cho những số nguyên tố lẻ. Còn hợp số thì sao? Đối với trường hợp đó, chúng ta sẽ sử dụng một kí hiệu mạnh hơn cả ***kí hiệu Legendre***. Đó là ***kí hiệu Jacobi***.

1.2 Kí hiệu Jacobi

Định lý 1

Kí hiệu Jacobi
Giả sử $n > 0$ là số tự nhiên lẻ và $p_1^{\alpha_1}.p_2^{\alpha_2}...p_k^{\alpha_k}$ là dạng phân tích tiêu chuẩn của n.
Với số nguyên a bất kỳ và $(a, n) = 1$, kí hiệu *Jacobi* là

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i^{a_i}}\right) = \prod \left(\frac{a}{p_i}\right)^{a_i}$$

trong đó tất cả các kí hiệu bên vế phải là ***kí hiệu Legendre***.

Do ***kí hiệu Jacobi*** chỉ là mở rộng của kí hiệu ***Legendre*** nên hầu hết các định lí trên vẫn đúng cho ***kí hiệu Jacobi***.

1. Nếu n là số nguyên tố thì ***kí hiệu Jacobi*** là ***kí hiệu Legendre***.
2. $\left(\frac{a}{n}\right) \in \{0, 1, -1\}$
3. $\left(\frac{a}{n}\right) = 0$ khi $\gcd(a, n) \neq 1$.
4. $\left(\frac{ab}{n}\right) \equiv \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.
5. $\left(\frac{a}{mn}\right) \equiv \left(\frac{a}{m}\right)\left(\frac{b}{n}\right)$, điều này dẫn tới $\left(\frac{a}{n^2}\right)$ là 0 hoặc 1.
6. Nếu $a \equiv (\mathrm{mod} n)$, thì $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.
7. $\left(\frac{1}{n}\right) = 1$.
8. $\left(-\frac{1}{n}\right) = (-1)^{\frac{n-1}{2}} \begin{cases} 1 & \text{khi} \quad n \equiv 1\,(\mathrm{mod} 4) \\ -1 & \text{khi} \quad n \equiv 3\,(\mathrm{mod} 4) \end{cases}$.
9. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & \text{khi} \quad n \equiv 1, 7\,(\mathrm{mod} 8) \\ -1 & \text{khi} \quad n \equiv 3, 5\,(\mathrm{mod} 8) \end{cases}$.
10. $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{(m-1)(n-1)}{4}}$.

Trong trường hợp n là số nguyên tố thì ***kí hiệu Jacobi*** trùng với ***kí hiệu Legendre***. Tuy nhiên khác với ***kí hiệu Legendre***, khi n là hợp số, ***kí hiệu Jacobi*** không cho biết phương trình đồng dư $x^2 \equiv a(\mathrm{mod} p)$ có nghiệm hay không. Mặc dù vậy, ***kí hiệu Jacobi*** có nhiều tính chất tương tự như ***kí hiệu Legendre.*** Ta chú ý rằng

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

không thể chỉ ra rằng a là không thặng dư bình phương modulo n. Thật vậy, nếu $\left(\frac{a}{n}\right) = -1$ thì từ định nghĩa $\left(\frac{a}{p_i}\right) = -1$ thì ít nhất p_i là ước của n; hơn nữa a là không thặng dư bình phương modulo p_i . Tuy vậy điều ngược lại thì không đúng, ta có thể xét ví dụ sau.
Ví dụ. Ta có

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$$

Ta thấy 2 là không thặng dư bình phương modulo 15, cũng là không thặng dư bình phương modulo 3 và 5. Do vậy, ta chưa thể kết luận được nếu p không là số nguyên tố.

Tính chất thứ hai không thể mở rộng gắn với ***đồng dư thức Euler*** $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$ với số nguyên tố p và số nguyên a bất kỳ. Một cách tự nhiên ***đồng dư thức Euler*** mở rộng từ ***kí hiệu Legendre*** sang ***kí hiệu Jacobi*** là $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} (\mathrm{mod} p)$ với hợp số lẻ dương n. Tuy nhiên đồng dư thức này là sai với ít nhất một nửa của các a mod n khi n là hợp số.

Định lý 2

Cho a là số nguyên và b là số nguyên dương, và b có phân tích ra thừa số nguyên tố $p = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ thì a là thặng dư bình phương modulo b nếu và chỉ nếu a là thặng dư bình phương modulo p^{α_i} với mỗi $i = 1, 2, \dots, r$.

Chứng minh.
Nếu a là thặng dư bình phương modulo b, thì hiển nhiên nó là thặng dư bình phương modulo với mỗi $p^{\alpha_i}; i = 1, 2, \dots, r$. Khi đó tồn tại x_i là số nguyên sao cho $x_i^2 \equiv a (\mathrm{mod} p^{\alpha_i})$. Theo ***định lý phần dư Trung Hoa*** thì có số x sao cho $x \equiv x_i (\mathrm{mod} p^{\alpha_i})$. Khi đó ta được

$$x^2 \equiv x_i^2 \equiv a (\mathrm{mod} p^{\alpha_i})$$

điều này chứng tỏ $x \equiv a (\mathrm{mod} b)$. □

Định lý 3

Số thặng dư bình phương modulo $p^n (n > 0)$, được tính bởi công thức

$$\left[\frac{2^{n-1} - 1}{3}\right] + 2 \text{ với } p = 2, \text{ và } \left[\frac{p^{n+1} - 1}{2(p+1)}\right] + 1 \text{ với } p > 2$$

Chứng minh.
Đặt k_n là số thặng dư bình phương modulo $p^n (n > 0)$.

(i) Cho p là số lẻ và $n \geqslant 2$. Số a là một thặng dư bình phương modulo p^n nếu và chỉ nếu p không là ước của a và a là một thặng dư bình phương modulo p, hoặc p^2 là ước của a và $\frac{a}{p^2}$ là một thặng dư bình phương modulo p^{n-2}. Từ đó suy ra

$$k_n = k_{n-2} + p' p^{n-1}$$

(ii) Cho $p = 2$ và $n \geqslant 3$. Số a là một thặng dư bình phương modulo 2^n nếu và chỉ nếu một trong hai khả năng sau xảy ra $a \equiv 1 (\mathrm{mod} 8)$ hoặc 4 là ước của a và $\frac{a}{4}$ là thặng dư bình phương modulo 2^{n-2}. Từ đó suy ra

$$k_n = k_{n-2} + 2^{n-3}$$

Sử dụng quy nạp ta dễ dàng chứng minh được các mệnh đề trên. □

1.3 Một vài tổng của kí hiệu Legendre

Việc tìm số nghiệm của một đồng dư thường quy về đếm các giá trị $x \in \{0, 1, \dots, p-1\}$ sao cho đa thức đã cho $f(x)$ với hệ số nguyên nào đó là thặng dư bình phương modulo một số nguyên tố lẻ p.

Câu trả lời hiển nhiên là có liên hệ với giá trị của tổng $\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)$. Trong phần này chúng ta quan tâm đến những tổng thuộc loại này. Đối với một đa thức tuyến tính f, tổng đang xét rất dễ đánh giá.

Định lý 1

Với các số nguyên a, b tùy ý và số nguyên tố $p \nmid a$, ta có

$$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=0$$

Chứng minh.

Do p không là ước của a, các số $ax+b$, với $x=0,1,\ldots,p-1$ lập nên hệ thặng dư đầy đủ modulo p. Có đúng $\frac{p-1}{2}$ là thặng dư bình phương, $\frac{p-1}{2}$ là không thặng dư bình phương, và một trong số đó chia hết cho p. Nghĩa là

$$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right)=\frac{p-1}{2}\cdot 1+\frac{p-1}{2}\cdot(-1)+0=0$$

Để đánh giá tổng của các đa thức bậc hai, chúng ta cần sử dụng định lí sau.

Định lý 2

Giả sử $f(x)^{p'}=a_0+a_1x+\ldots+a_{kp'}x^{kp'}$ với k là bậc của đa thức f. Đặt $k'=\left[\frac{k}{2}\right]$ thì ta có

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\equiv-\left(a_{p-1}+a_{2(p-1)}+\cdots+a_{k'(p-1)}\right)(\mathrm{mod}p)$$

Chứng minh.

Ta đặt $S_n=\sum_{x=0}^{p-1}x^n$ với n là số tự nhiên và $S_0=p$, bây giờ ta sẽ chỉ ra rằng $S_n\equiv -1(\mathrm{mod}\,p)$ với $n>0$ và $p-1|n$ và $S_n\equiv 0(\mathrm{mod}p)$ nếu ngược lại. Theo ***tiêu chuẩn Euler*** ta có

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right)\equiv\sum_{x=0}^{p-1}f(x)^{p'}=\sum_{i=0}^{kp'}a_iS_i\equiv-\left(a_{p-1}+a_{2(p-1)}+\cdots+a_{k'p-1}\right)(\mathrm{mod}p)$$

Như vậy định lý được chứng minh. □

Định lý 3

Với mọi số nguyên dương a, b, c và số nguyên tố $p \nmid a$, khi đó tổng

$$\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)$$

bằng $-\left(\frac{a}{p}\right)$ nếu $p \nmid b^2-4ac$ và $(p-1)\left(\frac{a}{p}\right)$ nếu $p|b^2-4ac$.

Chứng minh.

Ta đặt $D = b^2 - 4ac$, khi đó ta có

$$\left(\frac{4a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{(2ax+b)^2-D}{p}\right)$$

Do các số $ax+b$ trong đó $x = 0, 1, \ldots, p-1$ lập thành hệ thặng dư đầy đủ modulo p, do vậy ta được

$$\left(\frac{a}{p}\right)\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{x^2-D}{p}\right) = S$$

Theo như ***định lý 2*** thì $S \equiv -1 (\mathrm{mod} p)$, mặt khác $|S| \leqslant p$ lại cho ta $S = -1$ hoặc $S = p-1$, lúc này ta giả sử $S = p-1$, khi đó những số $\left(\frac{x^2-D}{p}\right)$ nhận giá tri bằng 1, khi $x = x_0$ thì nó nhận giá trị bằng 0, nghĩa là p là ước của $x_0^2 - D$. Do p là ước của $(-x_0)^2 - D = x_0 - p$ ta phải có $x_0 = 0$ do đó p là ước của D. Ngược lại, nếu p là ước của D, ta có $S = p-1$, mặt khác $S = -1$, đó là điều phải chứng minh. □

Ví dụ. Số nghiệm của phương trình đồng dư $x^2 - y^2 \equiv D (\mathrm{mod} p)$ với $D \not\equiv 0 (\mathrm{mod} p)$ bằng $p-1$.

Chứng minh. Đây chính là hệ quả được suy ra trực tiếp của định lí trên vì khi cố định x thì số các nghiệm y của đồng dư $y^2 \equiv x^2 - D (\mathrm{mod} p)$ bằng

$$\left(\frac{x^2-D}{p}\right) + 1$$

Đến đây bài toán đã được giải quyết. □

Nhận xét. Đánh giá tổng của ***kí hiệu Legendre*** đối với đa thức $f(x)$ bậc lớn hơn hai có ý nghĩa đặc biệt và khó. Trong phần này chúng ta xét trường hợp đa thức bậc ba thuộc một kiểu nào đó. Cho số nguyên a, ta đặt

$$K(a) = \sum_{x=0}^{p-1}\left(\frac{x\left(x^2+a\right)}{p}\right)$$

Giả sử p không là ước của a. Dễ suy ra rằng với mỗi số nguyên t, ta có

$$K\left(at^2\right) = \left(\frac{t}{p}\right)\sum_{x=0}^{p-1}\left(\frac{\frac{x}{t}\left(\left(\frac{x}{t}\right)^2+a\right)}{p}\right) = \left(\frac{t}{p}\right)K(a)$$

Do đó $|K(a)|$ chỉ phụ thuộc vào việc a có là thặng dư bình phương modulo p hay không. Bây giờ chúng ta đưa ra một chứng minh không tiêu chuẩn rằng mỗi số nguyên tố $p \equiv 1 (\mathrm{mod} 4)$ là tổng của hai bình phương.

Định lý 4

Đồng nhất thức Jacobstal - Jacobstal's identity

Giả sử a và b là một thặng dư bình phương và một không thặng dư bình phương modulo số nguyên tố p có dạng $4k+1$. Khi đó $|K(a)|$ và $|K(b)|$ là những số nguyên chẵn và thỏa mãn

$$\left(\frac{1}{2}|K(a)|\right)^2 + \left(\frac{1}{2}|K(b)|\right)^2 = p$$

Chứng minh.

Do $K(0) = 0$ nên ta có

$$p'\left(K(a)^2 + K(b)^2\right) = \sum_{n=1}^{p-1}K(n)^2 = \sum_{n=0}^{p-1}K(n)^2$$

Tiếp theo ta sẽ đi tính $\sum_{n=0}^{p-1} K(n)^2$, với mỗi số tự nhiên n ta có

$$K(n)^2 = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy\left(x^2+n\right)\left(y^2+n\right)}{p}\right)$$

Từ đây suy ra được

$$\sum_{n=0}^{p-1} K(n)^2 = \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right)\sum_{n=0}^{p-1}\left(\frac{\left(n+x^2\right)\left(n+y^2\right)}{p}\right)$$

Đến đây ra chú ý rằng, theo ***định lý 2*** thì $\sum_{n=0}^{p-1}\left(\frac{\left(n+x^2\right)\left(n+y^2\right)}{p}\right)$ bằng $p-1$ nếu $x=\pm y$ và bằng -1 trong trường hợp ngược lại. Do vậy mà

$$\sum_{n=0}^{p-1} K(n)^2 = p(2p-2) - \sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right) = 4pp'$$

Chúng ta thấy được rằng $K(a)^2 + K(b)^2 = 4p$ hơn nữa $K(a)^2 + K(b)^2 \vdots 4$ nên cả $K(a)^2$ và $K(b)^2$ đều chẵn.

Định lý được chứng minh. □

Sau đây ta sẽ cùng tìm hiểu một số định lý mở rộng có liên quan đến vài tổng của ***kí hiệu Legendre*** này.

Định lý 5

Với p là số nguyên tố lẻ và c là số nguyên dương, ta có

$$\sum_{x=0}^{p-1}\left(\frac{x^n+c}{p}\right) \equiv \begin{cases} \displaystyle\sum_{k=1}^{\left\lfloor\frac{\gcd(p-1,n)}{2}\right\rfloor}\binom{\frac{p-1}{2}}{k\frac{p-1}{\gcd(p-1,n)}}c^{\left(\frac{p-1}{2}k\frac{p-1}{\gcd(p-1,n)}\right)}, & \text{nếu } p\nmid c \\ -1, & \text{nếu } p|c \text{ và } n\equiv 0\,(\mathrm{mod}2) \\ 0, & \text{nếu } p|c \text{ và } n\equiv 1\,(\mathrm{mod}2) \end{cases}$$

Chứng minh.

Gọi S là tổng ta cần tính. Khi đó $S \equiv \sum_{x=0}^{p-1}(x^n+c)^{\frac{p-1}{2}} \pmod p$.

Nếu $p|c$ thì ta được $S = \sum_{x=0}^{p-1}\left(\frac{x^n}{p}\right) \mod p$, do vậy

$$S = \begin{cases} \displaystyle\sum_{x=0}^{p-1}\left(\frac{x^2}{p}\right) = p-1, & \text{nếu } n\equiv 0(\mathrm{mod}2) \\ \displaystyle\sum_{x=0}^{p-1}\left(\frac{x}{p}\right) = 0, & \text{nếu } n\equiv 1(\mathrm{mod}2) \end{cases}$$

Bây giờ ta xét $p\nmid c$, ta lấy giới hạn từ $x=1$ đến $x=p$ và sử dụng khai triển ***nhị thức Newton*** ta có được

$$S \equiv \sum_{x=1}^{p}\sum_{r=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{r}c^{\left(\frac{p-1}{2}-r\right)}x^{nr}(\mathrm{mod}p)$$

Thay đổi vị trí của các tổng ta được

$$S \equiv \sum_{r=0}^{\frac{p-1}{2}} \left(\binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2}-r\right)} \sum_{x=1}^{p} x^{nr} \right) (\mathrm{mod} p)$$

Giá trị của tổng $\sum_{x=1}^{p} x^{nr}$ modulo p là -1 nếu $(p-1)|nr$ và là 0 trong trường hợp còn lại, với mọi $r \geqslant 1$.
Với $r = 0$ thì giá trị của modulo p hiển nhiên bằng 0, do đó

$$S \equiv - \sum_{r \geqslant 1, (p-1)|nr}^{r \leqslant \frac{p-1}{2}} \binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2}-r\right)} (\mathrm{mod} p)$$

Nếu $(p-1)|nr$ thì $\dfrac{p-1}{\gcd(p-1,n)}|r$, do vậy các giá trị có thể có của r là $k\dfrac{p-1}{\gcd(p-1,n)}$, trong đó k là số nguyên dương thỏa mãn $1 \leqslant k \leqslant \left\lfloor \dfrac{\gcd(p-1,n)}{2} \right\rfloor$, do vậy ta có

$$S \equiv \sum_{k=1}^{\left\lfloor \frac{\gcd(p-1,n)}{2} \right\rfloor} \binom{\frac{p-1}{2}}{k\frac{p-1}{\gcd(p-1,n)}} c^{\left(\frac{p-1}{2} k \frac{p-1}{\gcd(p-1,n)}\right)} \pmod p$$

Định lý được chứng minh. □

Định lý 6

Ta đặt $\xi(a,b,c) = \sum_{x=0}^{p-1} \left(\dfrac{ax^2+bx+c}{p} \right) x$ thì khi đó ta có

$$2a \left(\frac{a}{p} \right) \xi(a,b,c) \equiv b \pmod p$$

Chứng minh.
Đầu tiên ta biến đổi

$$\begin{aligned} 2a \left(\frac{a}{p} \right) \xi(a,b,c) &= \sum_{x=0}^{p-1} \left(\frac{(2ax+b)^2 + \left(4ac-b^2\right)}{p} \right) 2ax \\ &= \sum_{x=0}^{p-1} \left(\frac{(2ax+b)^2 + \left(4ac-b^2\right)}{p} \right) (2ax+b) - b \sum_{x=0}^{p-1} \left(\frac{(2ax+b)^2 + \left(4ac-b^2\right)}{p} \right) \end{aligned}$$

Vì tập hợp các số nguyên dương $2ax+b$ tạo thành một hệ thặng dư đầy đủ nên

$$2a \left(\frac{a}{p} \right) \xi(a,b,c) \equiv \sum_{x=0}^{p-1} \left(\frac{x^2 + \left(4ac-b^2\right)}{p} \right) x - b \sum_{x=0}^{p-1} \left(\frac{l^2 + \left(4ac-b^2\right)}{p} \right) (\mathrm{mod} p)$$

Từ ***định lý 3*** ta có

$$\sum_{x=0}^{p-1} \left(\frac{x^2 + \left(4ac-b^2\right)}{p} \right) \equiv -1 \pmod p$$

Từ điều này suy ra được

$$2a \left(\frac{a}{p} \right) \xi(a,b,c) \equiv \sum_{x=0}^{p-1} \left(\frac{x^2 + \left(4ac-b^2\right)}{p} \right) x + b \equiv \xi\left(1,0,4ac-b^2\right) + b (\mathrm{mod} p) \qquad (1)$$

Ta chú ý rằng

$$\xi\left(1,0,4ac-b^2\right)=\sum_{x=0}^{p-1}\frac{x^2+\left(4ac-b^2\right)}{p}x\equiv\sum_{x=1}^{p}\left(x^2+\left(4ac-b^2\right)\right)^{\frac{p-1}{2}}x(\mathrm{mod}p)$$

Từ đây, sử dụng khai triển ***nhị thức Newton*** ta có

$$\xi\left(1,0,4ac-b^2\right)\equiv\sum_{x=1}^{p}\sum_{r=0}^{\frac{p-1}{2}}\binom{\frac{p-1}{2}}{r}\left(4ac-b^2\right)^{\left(\frac{p-1}{2}-r\right)}x^{2r+1}\quad(\mathrm{mod}p)$$

Ta sắp xếp lại ví trí các tổng, ta có được

$$\xi\left(1,0,4ac-b^2\right)\equiv\sum_{r=0}^{\frac{p-1}{2}}\left(\binom{\frac{p-1}{2}}{r}\left(4ac-b^2\right)^{\left(\frac{p-1}{2}-r\right)}\sum_{x=1}^{p}x^{2r+1}\right)\quad(\mathrm{mod}p)$$

Ta thấy rằng tổng $\sum_{x=1}^{p}x^{2r+1}$ có giá trị bằng -1 modulo p nếu $(p-1)|(2r+1)$ và là 0 trong trường hợp còn lại. Mặt khác $p-1$ là số chẵn và $2r+1$ là số lẻ nên $(p-1)\nmid(2r+1)$ và $\sum_{x=1}^{p}x^{2r+1}$ có giá trị là 0 modulo p với mọi r. Suy ra

$$\xi\left(1,0,4ac-b^2\right)\equiv0\quad(\mathrm{mod}p)$$

Từ đây theo (1) ta được

$$2a\left(\frac{a}{p}\right)\xi(a,b,c)\equiv b\quad(\mathrm{mod}p)$$

Như vậy định lý được chứng minh. □

Nhận xét. Từ định lý này ta có thể suy ra được kết quả sau.

Kết quả. Ta có $\xi(ka,kb,kc)=\left(\frac{k}{p}\right)\xi(a,b,c)$ với mọi số nguyên dương k.

Định lý 7

Đặt $S(a,b,c)=\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)$, với m là số nguyên dương thì ta có

$$\xi\left(a,b+2ma,m^2a+mb+c\right)=\xi(a,b,c)+p\sum_{r=0}^{m-1}\left(\frac{r^2a+rb+c}{p}\right)-mS(a,b,c)$$

Chứng minh.

Ta sẽ sử dụng phương pháp quy nạp. Ta có

$$\begin{aligned}\xi(a,b+2a,a+b+c) &= \sum_{x=0}^{p-1}\left(\frac{ax^2+(b+2a)x+(a+b+c)}{p}\right)x\\ &= \sum_{x=0}^{p-1}\left(\frac{a(x+1)^2+b(x+1)+c}{p}\right)(x+1)-S(a,b,c)\\ &= \sum_{x=1}^{p}\left(\frac{ax^2+bx+c}{p}\right)x-S(a,b,c)\\ &= \sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)x+p\left(\frac{c}{p}\right)-S(a,b,c)\\ &= \xi(a,b,c)+p\left(\frac{c}{p}\right)-S(a,b,c)\end{aligned}$$

Với $m=1$ thì đương nhiên thỏa mãn. Ta giả sử giả thiết quy nạp đúng với $m-1$, bây giờ ta sẽ đi chứng minh nó đúng với m. Ta đặt $B=b+2(m-1)a$ và $C=(m-1)^2a+(m-1)b+c$, khi đó ta có

$$\xi\left(a,b+2ma,m^2a+mb+c\right)=\xi(a,B+2a,a+B+C)=\xi(a,B,C)+p\left(\frac{C}{p}\right)-S(a,B,C)$$

Bây giờ sử dụng giả thiết quy nạp trên $\xi(a,B,C)$ ta có thể viết lại

$$\begin{aligned}\xi\left(a,b+2ma,m^2a+mb+c\right) &= \xi(a,b,c)+p\sum_{r=0}^{m-2}\left(\frac{r^2a+rb+c}{p}\right)-(m-1)S(a,b,c)\\ &\quad +p\left(\frac{(m-1)^2a+(m-1)b+c}{p}\right)-S(a,B,C)\end{aligned}$$

Ta có $4aC-B^2=4ac-b^2$, đến đây sử dụng ***định lý 3*** thì $S(a,b,c)=S(a,B,C)$. Điều này ám chỉ rằng

$$\xi\left(a,b+2ma,m^2a+mb+c\right)=\xi(a,b,c)+p\sum_{r=0}^{m-1}\left(\frac{r^2a+rb+c}{p}\right)-mS(a,b,c)$$

Như vậy định lý được chứng minh. □

Định lý 8

Với p là số nguyên tố và c, $n\geqslant 1$ và $k\geqslant 1$ là số nguyên dương

$$\sum_{x=0}^{p-1}\left(\frac{x^n+c}{p}\right)x^k\equiv\begin{cases}\displaystyle\sum_{0\leqslant r\leqslant\frac{p-1}{2};(p-1)|(nr+k)}\binom{\frac{p-1}{2}}{r}c^{\left(\frac{p-1}{2}-r\right)}, & \text{nếu} \quad p\nmid c\\ -1, & \text{nếu} \quad p|c \text{ và } (p-1)\left|\left(n\left(\frac{p-1}{2}\right)+k\right)\right.\\ 0, & \text{nếu} \quad p|c \text{ và } (p-1)\nmid\left(n\left(\frac{p-1}{2}\right)+k\right)\end{cases}$$

Chứng minh.

Đặt η là tổng ta đang cần tính. Nếu $p|c$, khi đó tổng trở thành

$$\eta\equiv\sum_{x=0}^{p-1}x^{n\left(\frac{p-1}{2}\right)+k}\pmod p$$

Tổng này có giá trị bằng 0 nếu $(p-1) \nmid \left(n\left(\frac{p-1}{2}\right)+k\right)$, và -1 trong các trường hợp còn lại. Tiếp theo ta xét $p \nmid c$, tiến hành theo cách tương tự như trong chứng minh ***định lý 5***, chúng ta thu được

$$\eta \equiv \sum_{r=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2}-r\right)} \sum_{x=1}^{p} x^{nr+k} (\mathrm{mod} p)$$

Tổng $\sum_{x=1}^{p} x^{nr+k}$ modulo p có giá trị là 0 khi $(p-1) \nmid (nr+k)$ và -1 trong các trường hợp còn lại. Do đó

$$\eta \equiv \sum_{0 \leqslant r \leqslant \frac{p-1}{2}; (p-1) \mid (nr+k)} \binom{\frac{p-1}{2}}{r} c^{\left(\frac{p-1}{2}-r\right)} \pmod{p}$$

Như vậy định lý được chứng minh. □

Nhận xét. Từ định lý này ta có các hệ quả sau.

(i) Nếu n là số chẵn và k là số lẻ thì $\eta \equiv 0 \pmod{p}$.

(ii) Với mọi số nguyên tố p lẻ, khi đó $S_p(1,b)$ chia hết cho p.

1.4 Số giả nguyên tố Euler

Giả sử p là số nguyên tố lẻ và b là số nguyên không chia hết cho p.
Khi đó theo ***tiêu chuẩn Euler*** ta có

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{p}\right) (\mathrm{mod} p)$$

Như vậy để kiểm tra n có phải là số nguyên tố hay không, ta có thể lấy một số b nguyên tố cùng nhau với n, và kiểm tra đồng dư sau có nghiệm hay không

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{n}\right) (\mathrm{mod} n)$$

trong đó vế phải là ***kí hiệu Jacobi***. Nếu đồng dư thức không đúng thì n phải là hợp số, ngược lại chưa kết luận được nhưng nhiều khả năng n là nguyên tố.

Định nghĩa 1

Số nguyên dương n được gọi là ***số giả nguyên tố Euler*** cơ sở b nếu nó là hợp số và đồng dư sau nghiệm đúng

$$b^{\frac{p-1}{2}} \equiv \left(\frac{b}{n}\right) (\mathrm{mod} n)$$

Từ định nghĩa này ta suy ra được mọi ***số giả nguyên tố Euler*** cơ sở b đều là số giả nguyên tố cơ sở b. Ta cùng tìm hiểu chủ đề này qua các định lý sau.

Định lý 1

Mọi số giả nguyên tố mạnh cơ sở b đều là số giả nguyên tố Euler cơ sở b.

Chứng minh.
Cho n là số giả nguyên tố mạnh cơ sở b. Khi đó, nếu $n-1 = 2^s t$, t thì, hoặc $b^t \equiv 1 (\mathrm{mod} n)$, hoặc $b^{2^r t} \equiv -1 (\mathrm{mod}\, n)$, trong đó r thỏa mãn $0 \leqslant r \leqslant s-1$. Ta giả sử rằng $\prod_{j=1}^{m} p_j^{a_j}$ là phân tích của n thành thừa số nguyên tố. Ta xét hai trường hợp.

(i) Nếu $b' \equiv 1(\mathrm{mod} n)$, ta giả sử p là một ước nguyên tố của n. Khi đó $ord_d p$ là ước của t, suy ra $ord_p b$ là số lẻ. Mặt khác thì $ord_d p$ là ước của $\phi(p) = p-1$, nên nó phải là ước của $\dfrac{p-1}{2}$. Do đó ta được

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

Theo ***tiêu chuẩn Euler*** ta có $\left(\dfrac{b}{p}\right) = 1$ và $\left(\dfrac{b}{n}\right) = 1$. Mặt khác ta lại có

$$b^{\frac{n-1}{2}} = \left(b^t\right)^{2^s-1} \equiv 1(\mathrm{mod} p)$$

Như vậy thì n là số giả nguyên tố Euler cơ sở b.

(ii) Nếu $b^{2^{r+1}t} \equiv -1(\mathrm{\ mod\ } n)$. Với p là một ước nguyên tố của n thì $b^{2^{r+1}t} \equiv -1(\mathrm{\ mod\ } p)$. Bình phương cả hai vế của đồng dư thức này ta được

$$b^{2^{r+1}t} \equiv 1(\mathrm{mod} p)$$

Như vậy ta suy ra được $ord_d p$ là ước của $2^{r+1}t$, nhưng $ord_d p$ không là ước của $2^r t$, suy ra $ord_d p = 2^{r+1}c$, trong đó c là một số nguyên lẻ. Mặt khác, vì $ord_d p$ là ước của $p-1$, 2^{r+1} là ước của $ord_d p$ nên 2^{r+1} là ước của $p-1$. Từ đó ta có $p = 2^{r+1}d + 1$, trong đó d là số nguyên. Vì

$$b^{\frac{ord_p b}{2}} \equiv 1(\mathrm{mod} p)$$

nên ta có được

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} = b^{\frac{ord_p b}{2}\frac{p-1}{ord_p b}} \equiv (-1)^{\frac{p-1}{ord_p b}} = (-1)^{\frac{p-1}{2^{r+1}}c}(\mathrm{mod} p)$$

vì c lẻ nên từ đó suy ra $\left(\dfrac{b}{p}\right) = (-1)^d$. Bây giờ ta giả sử có phân tích thành thừa số nguyên tố dạng $n = \prod_{j=1}^{m} p_j^{a_j}$. Theo chứng minh phần trên, các ước nguyên tố p_i có dạng $p_i = 2^{r+1}d_i + 1$, và đồng thời

$$\left(\frac{b}{m}\right) = \prod_{i=1}^{m}\left(\frac{b}{p_i}\right)^{a_i} = (-1)\sum_{i=1}^{m} a_i d_i$$

Mặt khác, dễ thấy rằng

$$n \equiv 1 + 2^{r+1}\sum_{i=1}^{m} a_i d_i \left(\mathrm{mod} 2^{2r+2}\right)$$

Do đó ta được

$$t2^{s-1} = \frac{n-1}{2} \equiv 2^r \sum_{i=1}^{m} a_i d_i \left(\mathrm{mod} 2^{r+1}\right)$$

tức là $t2^{s-1-r} \equiv \sum_{i=1}^{m} a_i d_i (\mathrm{mod} 2)$ và

$$b^{\frac{n-1}{2}} = \left(b^{2^r t}\right)^{2^{s-1-r}} = (-1)^{\sum_{i=1}^{m} a_i d_i}(\mathrm{mod} n)$$

Như vậy

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right)(\mathrm{mod} n)$$

và n là số giả nguyên tố Euler cơ sở b. Định lí được chứng minh. □

Nhận xét. Chú ý rằng, điều ngược lại không phải luôn luôn đúng: tồn tại những số nguyên tố giả Euler cơ sở b không là số giả nguyên tố mạnh cơ sở đó. Ví dụ $n = 1105, b = 2$. Tuy nhiên, với những điều kiện bổ sung, một số giả nguyên tố Euler sẽ là số giả nguyên tố mạnh cùng cơ sở. Ta có định lí sau.

Định lý 2

Số n giả nguyên tố Euler cơ sở b là số giả nguyên tố mạnh cơ sở b nếu $n \equiv 3(\text{mod}4)$, hoặc $\left(\frac{b}{n}\right) = -1$.

Chứng minh.

Trường hợp 1. Nếu $n \equiv 3(\text{mod}4)$. Khi đó $n - 1 = 2t$ và t lẻ. Vì n là số giả nguyên tố Euler cơ sở b nên

$$b' = b^{\frac{p-1}{2}} \equiv \left(\frac{b}{n}\right) (\text{mod}\, n)$$

Như vậy, n là số giả nguyên tố mạnh cơ sở b.

Trường hợp 2. Nếu $\left(\frac{b}{n}\right) = -1$, khi đó ta viết $n - 1 = 2^s t$, trong đó t lẻ, s là số nguyên dương. Vì n là số giả nguyên tố mạnh cơ sở b nên

$$b^{2^{s-1}t} = b^{\frac{p-1}{2}} \equiv \left(\frac{b}{n}\right) (\text{mod}\, n)$$

Theo giả thiết ta có $b^{2^{s-1}t} \equiv -1(\text{mod}n)$.

Do $\left(\frac{b}{n}\right) = \pm 1$ nên hoặc $b' \equiv 1(\text{mod}n)$ hoặc $b' \equiv -1(\text{mod}n)$.

Vậy n là số giả nguyên tố mạnh cơ sở b. □

Nhận xét. Dùng số giả nguyên tố Euler, ta có thể xây dựng thuật toán xác suất để kiểm tra một số nguyên tố hay không. Thuật toán này được Solovay và Strassen tìm ra đầu tiên năm 1977. Ta bắt đầu bằng bổ đề sau.

Bổ đề 1.

Giả sử n là một số nguyên dương lẻ không chính phương. Khi đó tồn tại ít nhất một số b với $1 < b < n$ và $(b, n) = 1$, sao cho $\left(\frac{b}{n}\right) = -1$.

Chứng minh.

Nếu n là số nguyên tố thì số b tồn tại. Khi n là hợp số không chính phương, ta viết $n = rs$, trong đó $(r, s) = 1$ và $r = p^e$ với p là một số nguyên tố lẻ và e là số nguyên dương lẻ. Bây giờ giả sử t là một không thặng dư bình phương của số nguyên tố p. Ta dùng ***định lí phần dư Trung Hoa*** để tìm số nguyên b sao cho $1 < b < n, (b, n) = 1$ và $b \equiv t(\text{mod}r), b \equiv 1(\text{mod}s)$. Khi đó ta có

$$\left(\frac{b}{r}\right) = \left(\frac{b}{p^e}\right) = (-1)^e = -1 = -1, \quad \left(\frac{b}{s}\right) = 1$$

Đồng nghĩa với $\left(\frac{b}{n}\right) = -1$. Bổ đề được chứng minh. □

Bổ đề 2.

Với mỗi hợp số lẻ n, tồn tại ít nhất một số b sao cho $1 < b < n, (b, n) = 1$ và

$$b^{\frac{n-1}{2}} \not\equiv \left(\frac{b}{n}\right) (\text{mod}n)$$

Chứng minh.
Giả sử ngược lại, với mọi số nguyên không vượt quá n và nguyên tố cùng nhau với n, ta có

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) (\mathrm{mod} n)$$

Từ đó suy ra, nếu $(b,n)=1$ thì $b^{n-1} \equiv 1(\mathrm{mod} n)$.
Như vậy, n phải là **số Carmichael**, và do đó, $n = q_1 q_2 \dots q_r$ là tích của các số nguyên tố lẻ khác nhau. Ta sẽ chỉ ra rằng

$$b^{\frac{n-1}{2}} \equiv 1(\mathrm{mod} n)$$

đối với số nguyên tố b không vượt quá n và nguyên tố cùng nhau với n. Giả sử ngược lại, tồn tại b thỏa mãn $b^{\frac{n-1}{2}} \equiv -1(\mathrm{mod} n)$. Theo ***định lý phần dư Trung Hoa*** ta tìm được số a $1 < a < n, (a,n) = 1$ sao cho $a \equiv b\,(\mathrm{mod} q_1)\,, a \equiv 1\,(\mathrm{mod} q_1 q_2 \dots q_r)$. Như vậy thì

$$a^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} \equiv -1\,(\mathrm{mod} q_1)\,, a^{\frac{n-1}{2}} \equiv 1\,(\mathrm{mod} q_1 q_2 \dots q_r)$$

Do đó $a^{\frac{n-1}{2}} \not\equiv \pm 1\,(\mathrm{mod} q_1 q_2 \dots q_r)$, trái với giả thiết phản chứng.
Như vậy với mọi $b, 1 < a < n, (b,n) = 1$ ta có $b^{\frac{n-1}{2}} \equiv 1(\mathrm{mod} n)$. Từ đồng dư trên và giả thiết của bổ đề, ta có

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) \equiv 1(\mathrm{mod} n)$$

Điều này mâu thuẫn với bổ đề 1 nên bổ đề 2 được chứng minh. □
Nhận xét.

(i) Một số p là số giả nguyên tố cơ sở a với mọi a nguyên tố cùng nhau với p được gọi là ***số Carmichael*** (chẳng hạn 561).

(ii) Định lí trên đây được dùng làm cơ sở cho một thuật toán kiểm tra xác suất số nguyên tố. Ta có định lí sau.

Định lý 3

Đối với mỗi hợp số lẻ n, tồn tại không quá $\dfrac{\phi(n)}{2}$ số nguyên dương b nhỏ hơn n, nguyên tố cùng nhau với n, sao cho n là số giả nguyên tố Euler cơ sở b.

Chứng minh.
Theo ***bổ đề 2***, tồn tại số b thỏa mãn $(b,n) = 1; 1 < a < n$, sao cho $b^{\frac{n-1}{2}} \not\equiv \left(\dfrac{b}{n}\right) (\mathrm{mod} n)$. Đến đây ta giả sử rằng $a_1, a_2, \dots, a_m$ là các số thỏa mãn $1 \leqslant a_j < n, (a_j, n) = 1$ và

$$a_j^{\frac{n-1}{2}} \equiv \left(\frac{a_j}{n}\right) = (\mathrm{mod} n)$$

Giả sử $r_1, r_2, \dots, r_m$ là thặng dư dương bé nhất của các số $ba_1, ba_2, \dots, ba_m$. Các số r_j khác nhau và nguyên tố cùng nhau với n. Ta sẽ chứng tỏ rằng chúng không thỏa mãn đồng dư thức như đối với các số a_j. Thật vậy, nếu ngược lại

$$r_j^{\frac{n-1}{2}} \equiv \left(\frac{r_j}{n}\right) = 1(\mathrm{mod} n)$$

thì ta có $ba_j^{\frac{n-1}{2}} \equiv \left(\dfrac{ba_j}{n}\right) = 1(\mathrm{mod} n)$ và như vậy

$$b^{\frac{n-1}{2}} a_j^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right)\left(\frac{ba_j}{n}\right) (\mathrm{mod} n)$$

Từ đó suy ra $b^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) (\mathrm{mod} n)$, mâu thuẫn với tính chất của b. Như vậy, tập hợp các số a_j và r_j không giao nhau. Gộp cả hai tập hợp này ta được $2m$ số khác nhau, bé hơn n và nguyên tố cùng nhau với n. Từ đó suy ra $m < \frac{\phi(n)}{2}$, định lí được chứng minh. □

Nhận xét. Từ định lí trên ta thấy rằng, nếu n là một hợp số lẻ, b là số chọn nhẫu nhiên trong các số $1, 2, ..., n-1$, thì xác suất để n là số giả nguyên tố Euler cơ sở b sẽ bé hơn $\frac{1}{2}$. Ta có định lí sau.

Thuật toán kiểm tra nguyên tố xác suất Solovay-Strassen. Cho n là số nguyên dương, ta chọn ngẫu nhiên k số $b_1, b_2, \ldots, b_k$ từ các số $1, 2, \ldots, n-1$. Đối với mỗi số nguyên b_j, xét đồng dư thức

$$b_j^{\frac{n-1}{2}} \equiv \left(\frac{b_j}{n}\right) (\mathrm{mod} n)$$

Ta có kết luận sau

1. Nếu một trong các đồng dư thức đó không nghiệm đúng thì n là hợp số.
2. Nếu n là nguyên tố thì mọi đồng dư thức đều nghiệm đúng.
3. Nếu n là hợp số, thì xác suất để mọi đồng dư thức nghiệm đúng là bé hơn $\frac{1}{2^k}$.

Như vậy, nếu k đủ lớn, và n trải qua được kiểm tra xác suất trên đây, thì "hầu như chắc chắn" n là số nguyên tố.

2 Các ví dụ minh họa

Bài 1

Tìm các số nguyên dương x, y sao cho $x^2+1 \vdots y^2-5$

Lời giải

Gọi p là ước nguyên tố của y^2-5 thì ta có

$$x^2+1 \vdots p \Rightarrow x^2 \equiv -1\,(\mathrm{mod} p) \Rightarrow \left(\frac{-1}{p}\right)=1 \Rightarrow (-1)^{\frac{p-1}{2}}=1 \Rightarrow p \equiv 1\,(\mathrm{mod} 4)$$

Do đó ta phải có

$$y^2-5 \equiv 1\,(\mathrm{mod} 4) \Rightarrow y^2 \equiv 6 \equiv 2\,(\mathrm{mod}\,4)$$

ta dễ thấy điều này vô lý.
Như vậy không tồn tại các số nguyên x, y thỏa mãn đề bài. □

Bài 2

Việt Nam TST 2004
Cho số nguyên dương n. Chứng minh rằng 2^n+1 không có ước nguyên tố dạng $8k+7$.

Lời giải

Gọi p à ước nguyên tố của 2^n+1. Giả sử $p \equiv 7(\mathrm{mod} 8)$.
i. Nếu n là số chẵn thì ta có

$$2^n \equiv -1\ (\mathrm{mod}\ p) \Rightarrow \left(\frac{-1}{p}\right)=1 \Rightarrow (-1)^{\frac{p-1}{2}}=1 \Rightarrow \frac{p-1}{2} : 2 \Rightarrow p \equiv 1\ (\mathrm{mod}\ 4)$$

Ta thấy điều này mâu thuẫn với giả thiết phản chứng là $p \equiv 7\ (\mathrm{mod}\ 8)$.
ii. Nếu n là số lẻ thì ta có

$$2^{n+1} \equiv -2\ (\mathrm{mod}\ p) \Rightarrow \left(\frac{-2}{p}\right)=1 \Rightarrow \left(\frac{-1}{p}\right).\left(\frac{2}{p}\right)=1 \Rightarrow (-1)^{\frac{p-1}{2}}.(-1)^{\frac{p^2-1}{8}}=1 \qquad (1)$$

Nhưng mà do

$$p \equiv 7(\mathrm{mod} 8) \Rightarrow \begin{cases} (-1)^{\frac{p-1}{2}}=1 \\ (-1)^{\frac{p^2-1}{8}}=-1 \end{cases}$$

Từ đây kéo theo

$$(-1)^{\frac{p-1}{2}}.(-1)^{\frac{p^2-1}{8}}=-1,$$

mâu thuẫn với (1).
Như vậy giả thiết phản chứng là sai nên ta có điều phải chứng minh. □

Bài 3

Indonesia TST 2009
Chứng minh rằng tồn tại vô hạn số nguyên dương n sao cho n^2+1 không là ước của n !.

Lời giải

Trước hết ta sử dụng bổ đề quen thuộc sau đây.
Bổ đề. Tồn tại vô hạn số nguyên tố có dạng $4k+1,\ k$ là số nguyên dương.
Bổ đề này khá là quen thuộc nên chúng tôi không nêu chứng minh ở đây.
Ta quay lại với bài toán. Giả sử ta xét p là số nguyên tố có dạng $4k+1$.
Theo định lý ***tiêu chuẩn Euler*** ta có

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

Hay -1 là số chính phương mod p.
Từ đó tồn tại $n^{'} \in \{1,\ 2,\ 3,..., p-1\}$ sao cho

$$\left(n^{'}\right)^2 + 1 \equiv 0 \ (\text{mod } p).$$

Lại dễ thấy $(n')!$ không chia hết cho p nên ta suy ra ngay $\left(n^{'}\right)^2 + 1$ không là ước của $(n')!$.
Bây giờ ta chỉ cần chứng tỏ sự tồn tại vô hạn của $n^{'}$ là xong.
Thật vậy, có

$$\left(n'\right)^2 + 1 \geqslant p \Rightarrow n' \geqslant \sqrt{p-1}$$

Theo ***bổ đề*** thì có vô hạn số nguyên tố có dạng $4k+1$ nên ta có thể chọn vô số số $n^{'}$ như vậy. Tức là tồn tại vô hạn số nguyên dương n sao cho n^2+1 không là ước của n !. □

Bài 4

Cho n là số nguyên dương lẻ và u là một ước nguyên dương lẻ của 3^n+1. Chứng minh rằng $u-1$ chia hết cho 3. Chứng minh rằng tồn tại vô hạn số nguyên dương n sao cho n^2+1 không là ước của n !.

Lời giải

Ta gọi p là ước nguyên tố lẻ của 3^n+1, ta có

$$3^n + 1 \equiv 0(\text{mod}p) \Rightarrow 3^{n+1} \equiv -3(\text{mod}p)$$

Vì n lẻ nên $n+1$ chẵn, từ đó suy ra -3 là số chính phương mod p hay

$$\left(\frac{-3}{p}\right) = 1 \qquad (*)$$

Theo định lý ***tiêu chuẩn Euler*** ta có

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

Theo ***luật tương hỗ Gauss*** ta có

$$\left(\frac{3}{p}\right).\left(\frac{p}{3}\right) = (-1)^{\frac{(p-1)(3-1)}{4}} = (-1)^{\frac{p-1}{2}} \Rightarrow \left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}.\left(\frac{p}{3}\right) \qquad (2)$$

Từ (1) và (2) suy ra

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

Nếu $p \equiv 2 \ (\text{mod } 3) \Rightarrow \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1$,từ đây kéo theo

$$\left(\frac{-3}{p}\right) = -1,$$

điều này mâu thuẫn với $(*)$.

Mặt khác ta dễ thấy $p \neq 3$, do vậy $p \equiv 1(\text{mod}3) \Rightarrow u - 1 \vdots 3$
Từ đây ta có điều phải chứng minh. □

Bài 5

Tìm tất cả các số nguyên dương n thỏa mãn $3^n - 1 \vdots 2^n - 1$.

Lời giải

Nếu n là số chẵn thì

$$2^n - 1 \equiv 0 \ (\text{mod } 3) \Rightarrow 3^n - 1 \equiv 0 \ (\text{mod } 3),$$

điều này mâu thuẫn. Do đó n phải là số lẻ.
Ta gọi p là một ước nguyên tố lẻ của $2^n - 1$. Hiển nhiên $p \neq 3$. Nếu $n > 3$ thì ta có

$$3^n - 1 \equiv 0 \ (\text{mod } p) \Rightarrow 3^n \equiv 1 \ (\text{mod } p) \Rightarrow 3^{n+1} \equiv 3 \ (\text{mod } p) \Rightarrow \left(\frac{3}{p}\right) = 1.$$

$$2^n - 8 = 8.\left(2^{n-3} - 1\right) \equiv 0 \ (\text{mod } 12) \Rightarrow 2^n - 1 \equiv 7 \ (\text{mod } 12) \tag{1}$$

Áp dụng định lý ***luật tương hỗ Gauss*** thì ta có

$$\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right).\left(\frac{3}{p}\right) = (-1)^{\frac{(p-1)(3-1)}{4}} = (-1)^{\frac{p-1}{2}}.$$

Nếu $p \equiv 2 \ (\text{mod } 3) \Rightarrow \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1$, kéo theo

$$\frac{p-1}{2} \not\vdots 2 \Rightarrow p \equiv 3 \ (\text{mod } 4).$$

Ta được $p \equiv -1 \ (\text{mod } 12)$.
Nếu $p \equiv 1 \ (\text{mod } 3) \Rightarrow \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1$, kéo theo

$$\frac{p-1}{2} \vdots 2 \Rightarrow p \equiv 1 \ (\text{mod } 4).$$

Ta được $p \equiv 1 \ (\text{mod } 12)$. Tóm lại là ta có $p \equiv \pm 1(\text{mod } 12)$. Do vậy chỉ có thể là $2^n - 1 \equiv \pm 1(\text{mod } 12)$, nhưng điều này lại mâu thuẫn với (1). Suy ra $n \leqslant 3$, thử trực tiếp ta được $n = 1$.
Vậy $n = 1$ là đáp số duy nhất của bài toán. □

Bài 6

Tạp chí Pi số tháng 8.2017
Chứng minh rằng không tồn tại số nguyên $n > 5$, sao cho $3^n + 5^n$ chia hết cho $n^2 - 25$.

Lời giải

Giả sử ngược lại, tồn tại số nguyên $n > 5$ sao cho $3^n + 5^n$ chia hết cho $n^2 - 25$. Giả sử n là số chẵn. Khi đó $n^2 - 25 \equiv 3(\text{mod } 4)$. Từ đó, do $n^2 - 25 > 1$ nên $n^2 - 25$ có ước nguyên tố p mà $p \equiv 3(\text{mod } 4)$. Hơn nữa, vì $3^n + 5^n \vdots p$ nên $p \neq 3, \ 5$. Ta có $5^n \equiv -3^n(\text{mod } p)$. Từ đó, với lưu ý $\frac{p-1}{2}$ là số lẻ, suy ra

$$5^{\frac{n(p-1)}{2}} \equiv -3^{\frac{n(p-1)}{2}}(\text{mod} p).$$

Mặt khác vì $p \neq 3,\ 5$ nên theo ***định lý Fermat*** nhỏ ta có

$$5^{\frac{n(p-1)}{2}} \equiv 1 \equiv 3^{\frac{n(p-1)}{2}} (\text{mod} p).$$

Do đó, $2.3^{\frac{n(p-1)}{2}} \equiv 0(\text{ mod } p)$, mâu thuẫn với các tính chất đã nêu của p. Vậy n là số nguyên dương lẻ.
Xét ước nguyên tố p tùy ý của n^2-25 thì ta có $3^n+5^n \vdots p$. Do đó $\left(\frac{3^n}{p}\right) = \left(\frac{-5^n}{p}\right)$ suy ra

$$1 = \left(\frac{3^n}{p}\right).\left(\frac{-5^n}{p}\right) = \left(\frac{3^n.(-5^n)}{p}\right).$$

Từ đó vì n là số lẻ nên ta có $\left(\frac{-15}{p}\right) = 1$.
Suy ra theo ***luật tương hỗ bậc hai***, ta có

$$1 = \left(\frac{-15}{p}\right) = \left(\frac{-1}{p}\right).\left(\frac{3}{p}\right).\left(\frac{5}{p}\right) = \left(\frac{p}{3}\right).\left(\frac{p}{5}\right).$$

Suy ra p đồng dư với $1,\ 2,\ 4,\ 8$ theo mod 15. Như vậy, mọi ước nguyên tố của n^2-25 đều có dạng $15k+r$ với $r \in \{1,\ 2,\ 4,\ 8\}$. Do đó, mọi ước nguyên tố của $n+5$ và $n-5$ đều có dạng vừa nêu. Mà tích của hai số nguyên có dạng $15k+r$ với $r \in \{1,2,4,8\}$ cũng là một số có dạng như vậy, nên suy ra $n+5$ và $n-5$ đều đồng dư với $\{1,\ 2,\ 4,\ 8\}$ theo mod 15. Tuy nhiên, điều này là không thể vì hiệu của hai số tùy ý thuộc tập hợp $\{1,2,4,8\}$ đều khác 10 hoặc -10.
Mâu thuẫn nhận được chứng tỏ giả sử ở đầu lời giải là sai và do đó kết luận của bài toán được chứng minh. □

Bài 7

Có tồn tại hay không một tập hợp gồm 16 số nguyên dương liên tiếp mà không có số nguyên dương nào có dạng

$$7x^2+9xy-5y^2\ (x,y \in \mathbb{Z}).$$

Lời giải

Gọi p là ước nguyên tố của

$$A = 7x^2+9xy-5y^2\ (x,y \in \mathbb{Z})$$

- Nếu một trong hai số $x,\ y$ chia hết cho p thì x và y cùng chia hết cho p, do đó $A \vdots p^2$.
- Nếu $(x,\ p) = (y,\ p) = 1$ thì

$$A \vdots p \Rightarrow 20\left(7x^2+9xy-5y^2\right) \equiv 0\ (\text{mod } p) \Rightarrow 221x^2 \equiv (9x-10y)^2 (\text{mod } p).$$

Suy ra 221 là số chính phương mod p.
Theo ***kí hiệu Jacobi*** và ***luật tương hỗ Gauss*** ta có

$$1 = \left(\frac{221}{p}\right) = \left(\frac{13}{p}\right).\left(\frac{17}{p}\right) = \left(\frac{p}{13}\right).\left(\frac{p}{17}\right) \quad (*)$$

Do đó, nếu $(x,\ p) = (y,\ p) = 1$ thì A chỉ chứa các ước nguyên tố p mà $\left(\frac{p}{13}\right).\left(\frac{p}{17}\right) = 1$ tức là các số nguyên tố p mà là số chính phương mod 13 và không là số chính phương mod 17 và ngược lại. Dễ dàng kiểm chứng được

- Nếu p là số chính phương mod$13 \Leftrightarrow p \equiv r\ (\text{mod} p)$ với $r \in \{1,3,4,9,10,12\}$.

- Nếu p là số chính phương mod $17 \Leftrightarrow p \equiv r \pmod{p}$, với $r \in \{1,2,4,8,9,13,15,16\}$.

Từ đó, ta dễ dàng tìm được 16 số nguyên tố thỏa mãn

$$\left(\frac{p}{13}\right).\left(\frac{p}{17}\right) = -1$$

là $T = \{p_1,\ p_2, ..., p_{16}\} = \{2,3,13,17,19,23,29,47,59,61,67,79,83,89,107,113\}$.
Theo định lý ***thặng dư Trung Hoa*** thì tồn tại số nguyên dương n để

$$n \equiv -i + p_i \pmod{p_i^2},\ i = \overline{1,\ 16}.$$

Khi đó ta xét tập $S = \{n+1, n+2, ..., n+16\}$ thì tập này thỏa mãn.
Thật vậy, phản chứng, giả sử tồn tại số j và $x,\ y$ để

$$B = n + j = 7x^2 + 9xy - 5y^2.$$

Khi đó, ta có $B \equiv p_j \pmod{p_j^2}$. Nếu $x \vdots p_j$ thì $y \vdots p_j$ và do đó $B \vdots p_j^2$. Điều này mâu thuẫn với $B \equiv p_j \pmod{p_j^2}$. Nếu $(x,\ p_j) = 1$ thì theo $(*)$ suy ra

$$\left(\frac{p_j}{13}\right).\left(\frac{p_j}{17}\right) = 1$$

nhưng điều này lại mâu thuẫn với $p_j \in T$.
Vậy tập S này thỏa mãn và đáp án của bài toán là tồn tại.
Bình luận. Bài toán này hoàn toàn là một bài toán số học đơn thuần chứ không phải là một bài toán tổ hợp. Kiến thức để nói về bản chất của bài toán này chính là ***luật tương hỗ Gauss***. □

Bài 8

Chứng minh rằng không tồn tại các số nguyên dương $a,\ b,\ c$ sao cho $a^2 + b^2 + c^2$ chia hết cho $3(ab + bc + ca)$.

Lời giải

Giả sử tồn tại các số nguyên dương $a,\ b,\ c,\ n$ sao cho

$$a^2 + b^2 + c^2 = 3n.(ab + bc + ca) \Leftrightarrow (a+b+c)^2 = (3n+2).(ab + bc + ca).$$

Vậy tồn tại một ước nguyên tố p của $3n+2$ sao cho $p \equiv 2 \pmod{3}$ và $v_p(3n+2)$ lẻ.
Giả sử $p^{2i-1} \parallel (3n+2)$, $i \in \mathbb{N}^*$ nào đó. Ta có

$$(a+b+c)^2 \vdots (3n+2) \Rightarrow (a+b+c)^2 \vdots p^{2i-1}$$

Ta suy ra được

$$(a+b+c) \vdots p^i \Rightarrow (a+b+c)^2 \vdots p^{2i} \Rightarrow (ab+bc+ca) \vdots p$$

$$\Leftrightarrow [ab + c(a+b)] \vdots p \Rightarrow [ab + (-a-b)(a+b)] \vdots p$$

do $a+b+c \vdots p$ suy ra $\Leftrightarrow a^2 + ab + b^2 \vdots p$. Từ đó suy ra

$$4\left(a^2+ab+b^2\right) \vdots p \Leftrightarrow (2a+b)^2 + 3b^2 \vdots p \Rightarrow \left(\frac{-3}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod{6},$$

điều này mâu thuẫn. Vậy điều giả sử là sai.
Hay không tồn tại các số nguyên dương $a,\ b,\ c,\ n$ thỏa mãn yêu cầu bài toán.

Nhận xét. Bài toán trong kì thi ***Iran TST 2013***: Tìm tất cả các số nguyên dương a, b, c thỏa mãn $a^2+b^2+c^2$ chia hết cho $2013.(ab+bc+ca)$, đây là trường hợp đặc biệt của bài toán này với $n=671k$, với $k\in\mathbb{N}^*$. □

Bài 9

Chuyên KHTN Hà Nội

Cho (a_n) xác định bởi công thức sau

$$\begin{cases} a_0=1, a_1=4 \\ a_{n+1}=2a_n+3a_{n-1} \end{cases} (n\in\mathbb{N}^*).$$

Chứng minh rằng trong dãy số trên không có số nào là bội của 2017.

Lời giải

Phương trình đặc trưng của dãy số là $\lambda^2-2\lambda-3=0$.

Do đó ta tìm được công thức tổng quát là $a_n=\frac{5}{4}.3^n-\frac{1}{4}.(-1)^n$, với $n\geqslant 0$. Do đó ta thu được dãy chẵn và dãy lẻ như sau

$$\begin{cases} a_{2k}=\frac{5}{4}.3^{2k}-\frac{1}{4} \\ a_{2k+1}=\frac{5}{4}.3^{2k+1}+\frac{1}{4} \end{cases}$$

Ta cần chứng minh

$$\begin{cases} 5.3^{2k}-1\not\equiv 0\,(\mathrm{mod}2017) \\ 5.3^{2k+1}+1\not\equiv 0\,(\mathrm{mod}2017) \end{cases}$$

Tức là ta cần chứng minh $3^{2k}\not\equiv -807\,(\mathrm{mod}2017)$ hay ta sẽ đi chứng minh $\left(\frac{-807}{2017}\right)=-1$.

Mà ta có

$$-1=\left(\frac{-807}{2017}\right)=\left(\frac{-1}{2017}\right).\left(\frac{807}{2017}\right)=(-1)^{\frac{2017-1}{2}}.\left(\frac{807}{2017}\right)=\left(\frac{807}{2017}\right).$$

Nên ta chỉ cần đi chứng minh là đủ $\left(\frac{807}{2017}\right)=-1$. Ta có $\left(\frac{807}{2017}\right)=\left(\frac{3}{2017}\right).\left(\frac{269}{2017}\right)$,

Mà theo ***luật tương hỗ Gauss*** thì

$$\left(\frac{3}{2017}\right).\left(\frac{2017}{3}\right)=(-1)^{\frac{(2017-1)(3-1)}{4}}=1$$

và

$$\left(\frac{269}{2017}\right).\left(\frac{2017}{269}\right)=(-1)^{\frac{(2017-1)(269-1)}{4}}=1$$

Do đó,

$$\begin{aligned}\left(\frac{807}{2017}\right)&=\left(\frac{3}{2017}\right).\left(\frac{269}{2017}\right)=\left(\frac{2017}{3}\right).\left(\frac{2017}{269}\right)\\&=\left(\frac{2016+1}{3}\right).\left(\frac{1883+134}{269}\right)=\left(\frac{1}{3}\right).\left(\frac{134}{269}\right)\end{aligned}$$

Mà $134\equiv-\frac{1}{2}\pmod{269}$ do đó $\left(\frac{134}{269}\right)=\left(\frac{-2}{269}\right)$.

Mà 269 không có dạng $8k+1$, $8k-1$ nên 2 không là số chính phương mod 269 nên

$$\left(\frac{-2}{269}\right)=-1$$

Tức là ta có $\left(\frac{807}{2017}\right) = -1$, do đó ta suy ra điều phải chứng minh.

Nhận xét. Đây là một bài toán thuộc dạng dãy số số học, ngoài việc vận dụng linh hoạt các tính chất của dãy số thì biến đổi số học là điều tối quan trọng để giải quyết nhưng bài toán dạng này. Và những kiến thức về thặng dư bình phương là một vũ khí mạnh để vận dụng trong các biến đổi số học đó. □

Bài 10

Cho dãy số nguyên (a_n) xác định bởi

$$\begin{cases} a_0 = 1, a_1 = -1 \\ a_{n+2} = 6a_{n+1} + 5a_n \end{cases} \quad (n \in \mathbb{N})$$

Tìm tất cả các số nguyên tố $p > 5$ sao cho 14 là số chính phương mod p và $a_{p+1} + 1 \vdots p$.

Lời giải

Trước tiên ta tìm tất cả các số nguyên tố $p > 5$ sao cho 14 là số chính phương mod p.
Do 14 là số chính phương.

Trường hợp 1. Nếu $\left(\frac{7}{p}\right) = \left(\frac{2}{p}\right) = 1$, khi đó ta có

$$1 = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \Leftrightarrow p \equiv \pm 1 \pmod 8$$

từ đây xảy ra hai khả năng.

- *Khả năng 1.* Nếu $p = 56k + 8r + 1\,(k, r \in \mathbb{N}, r = 0, 1, 2, ..., 6)$ thì ta có

$$\left(\frac{7}{p}\right) = (-1)^{\frac{(7-1)(p-1)}{4}} . \left(\frac{p}{7}\right) = \left(\frac{r+1}{7}\right) = 1 \Leftrightarrow r \in \{0, 1, 3, 6\}$$

  khi đó ta được $p \equiv 1, 9, 25, 49\,(\text{mod}56)$.

- *Khả năng 2.* Nếu $p = 56k + 8r - 1\,(k, r \in \mathbb{N}, r = 0, 1, 2, ..., 6)$ thì ta có

$$\left(\frac{7}{p}\right) = (-1)^{\frac{(7-1)(p-1)}{4}} . \left(\frac{p}{7}\right) = \left(\frac{r-1}{7}\right) = 1 \Leftrightarrow r \in \{1, 2, 3, 5\}$$

  ta được $p \equiv 7, 15, 23, 39\,(\text{mod}56)$.

Trường hợp 2. Nếu $\left(\frac{7}{p}\right) = \left(\frac{2}{p}\right) = -1$, khi đó ta có

$$-1 = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \Leftrightarrow p \equiv \pm 3 \pmod 8$$

từ đây xảy ra hai khả năng.

- *Khả năng 1.* Nếu $p = 56k + 8r + 3\,(k, r \in \mathbb{N}, r = 0, 1, 2, ..., 6)$ thì ta có

$$\left(\frac{7}{p}\right) = (-1)^{\frac{(7-1)(p-1)}{4}} . \left(\frac{p}{7}\right) = \left(\frac{r+3}{7}\right) = -1 \Leftrightarrow r \in \{0, 2, 3\}$$

  khi đó ta được $p \equiv 3, 19, 27\,(\text{mod}56)$.

- *Khả năng 2.* Nếu $p = 56k + 8r - 3\,(k, r \in \mathbb{N}, r = 0, 1, 2, ..., 6)$ thì ta có

$$\left(\frac{7}{p}\right) = (-1)^{\frac{(7-1)(p-1)}{4}} \cdot \left(\frac{p}{7}\right) = \left(\frac{r-3}{7}\right) = -1 \Leftrightarrow r \in \{1, 2, 3, 6\}$$

Khi đó ta được $p \equiv 5, 13, 21, 45\,(\mathrm{mod} 56)$.

Vậy tất cả các số nguyên tố cần tìm có dạng

$$p \equiv 1,\ 3,\ 5,\ 7,\ 9,\ 13,\ 15, 19, 23, 25, 27, 35, 39, 45, 49\ \ (\mathrm{mod}\ 56)$$

Trong đó riêng trường hợp $p \equiv 21\ \ (\mathrm{mod}\ 56)$, loại.
Các số nguyên tố trên tồn tại do theo ***định lý Dirichlet*** với hai số nguyên dương nguyên tố cùng nhau (a, b) thì tồn tại vô hạn các số nguyên tố cùng nhau có dạng $an + b$. Trở lại với bài toán. Do 14 là số chính phương mod p nên tồn tại số nguyên dương m sao cho $m^2 \equiv 14\,(\mathrm{mod} p)$.
Xét dãy số (b_n) xác định như sau

$$\begin{cases} b_0 = 0, b_1 = -1 \\ b_{n+2} = 6b_{n+1} + \left(m^2 - 9\right) b_n \end{cases} (n \in \mathbb{N}),$$

dễ thấy m là số thỏa mãn thì $(2m,\ p) = 1$.
Khi đó phương trình đặc trưng của (b_n) là $x^2 - 6x + 9 - m^2 = 0$ có nghiệm

$$x_1 = 3 + m,\ x_2 = 3 - m$$

Suy ra $b_n = c_1.(3+m)^n + c_2.(3-m)^n$, kết hợp với $b_0 = 0,\ b_1 = -1$ thì ta suy ra được

$$2mb_n = (m+4).(3+m)^n + (m-4).(3-m)^n.$$

Suy ra

$$\begin{aligned} 2mb_{p+1} &= (m+4).(3+m)^{p+1} + (m-4).(3-m)^{p+1} \\ &\equiv (m+4).(3+m)^2 + (m-4).(3-m)^2\,(\mathrm{mod} p) \end{aligned}$$

Điều này tương đương với

$$\Leftrightarrow 2m\left(b_{p+1} + 1\right) \equiv 2m\left(m^2 - 14\right)\ \ (\mathrm{mod}\ p) \Rightarrow b_{p+1} + 1 \equiv m^2 - 14 \equiv 0\ \ (\mathrm{mod}\ p) \qquad (1)$$

Bằng quy nạp ta chứng minh được

$$a_n \equiv b_n\,(\mathrm{mod} p), \forall n \geqslant 0 \qquad (2)$$

Từ (1) và (2) ta được $a_{p+1} + 1 \equiv 0\ \ (\mathrm{mod}\ p)$.
Vậy tất cả các số nguyên tố $p > 5$ thỏa mãn yêu cầu bài toán là

$$p \equiv 1, 3, 5, 7, 9, 13, 15, 19, 23, 25, 27, 35, 39, 45, 49\,(\mathrm{mod} 56)$$

Nhận xét. Bài toán trên được xây dựng trên ý tưởng của ***bài 6 VMO 2011*** sử dụng số chính phương mod$p$ để chứng minh cho bài toán chia hết. □

Bài 11

Cho đa thức $P(x) = x^8 - 16$. Chứng minh rằng với mọi số nguyên tố p đều tìm được số nguyên dương n sao cho $P(n) \vdots p$.

Lời giải

Từ

$$P(x)=x^8-16=\left(x^4-4\right).\left(x^4+4\right)=\left(x^2-2\right).\left(x^2+2\right).\left[\left(x^2+2\right)^2-4x^2\right]$$
$$=\left(x^2-2\right).\left(x^2+2\right).\left(x^2-2x+2\right).\left(x^2+2x+2\right)$$

Từ đó suy ra được

$$P(x)=\left(x^2-2\right).\left(x^2+2\right).\left[(x-1)^2+1\right].\left[(x+1)^2+1\right]$$

- Nếu 2 là số chính phương mod p thì tồn tại $n\in\mathbb{N}^*:P(n)=0$, từ đây suy ra điều phải chứng minh.
- Nếu -2 là số chính phương mod p thì tồn tại $n\in\mathbb{N}^*:P(n)=0$, từ đây suy ra điều phải chứng minh.
- Nếu -1 là số chính phương mod p thì tồn tại $n\in\mathbb{N}^*:P(n)=0$, từ đây suy ra điều phải chứng minh.
- Nếu $-2,-1,2$ đều không là số chính phương mod p hay là

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

  Nhưng rõ ràng ta có

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

  điều này vô lý.

Từ đây ta suy ra kết luận của bài toán.

Nhận xét. Từ cách giải của bài toán trên, ta có thể giải được bài toán tương tự sau. Cho đa thức

$$P(x)=\left(x^2-a\right).\left(x^2-b\right).\left(x^2-ab\right),$$

trong đó $a,\ b$ là hai số nguyên tố phân biệt. Chứng minh rằng với mọi số nguyên tố p, đều tìm được số nguyên dương n sao cho $P(n)\vdots p$. □

Bài 12

Cho $f(x)$ là một tam thức bậc hai với hệ số nguyên thỏa mãn, với mọi số nguyên tố p đều tồn tại ít nhất một số nguyên n sao cho $f(n)\vdots p$. Chứng minh rằng $f(x)$ có nghiệm hữu tỉ.

Lời giải

Bổ đề. Cho a là một số nguyên dương không chính phương. Khi đó tồn tại vô số số nguyên tố p sao cho a không là số chính phương mod p.

Chứng minh. Bạn đọc xem ở **bài 31.**

Đặt $f(x)=ax^2+bx+c\ (a,\ b,\ c\in\mathbb{Z},\ a\neq 0)$.

Ta chỉ cần chứng minh $\Delta=b^2-4ac$ là số chính phương.

Chọn p là một số nguyên tố bất kì theo giả thiết tồn tại số nguyên n sao cho

$$f(n)\vdots p\Leftrightarrow an^2+bn+c\equiv 0\,(\mathrm{mod}p)\Leftrightarrow b^2-4ac\equiv(2an+b)^2\,(\mathrm{mod}p)$$

Do đó $\left(\dfrac{b^2-4ac}{p}\right)=1$. Khi đó theo Bổ đề thì ta có $\Delta=b^2-4ac$ là số chính phương.

Từ đây suy ra điều phải chứng minh của bài toán. □

Bài 13

1998 Bulgarian MO

Cho $m,\ n$ là hai số nguyên dương thỏa mãn $A = \dfrac{(m+3)^n + 1}{3m}$ là số nguyên. Chứng minh rằng A là số lẻ.

Lời giải

- Nếu m là số lẻ thì $(m+3)^n + 1$ và $3m$ là các số lẻ nên suy ra A là số lẻ.
- Nếu m là số chẵn. Do A là số nguyên nên suy ra

$$0 \equiv (m+3)^n + 1 \equiv m^n + 1 \pmod 3.$$

Suy ra n phải là số lẻ.

Đặt $n = 2t+1,\ t \in N^*$ và

$$m \equiv -1 \pmod 3 \qquad (*)$$

Khi đó ta xét các trường hợp sau.

Trường hợp 1. Nếu $m = 8m_1, m_1 \in \mathbb{N}^*$ Khi đó ta có

$$(m+3)^n + 1 \equiv 3^n + 1 \equiv 4 \,(\text{mod}8) \Rightarrow (m+3)^n + 1 = 8M + 4, M \in \mathbb{N}^*$$

và mẫu số

$$3m \equiv 0 \,(\text{ mod } 8) \Rightarrow 3m = 8M', M' \in \mathbb{N}^*$$

điều này mâu thuẫn với giả thiết A là số nguyên.

Trường hợp 2. Nếu $m = 8m_1 + 2,\ m_1 \in \mathbb{N}^*$ và $m = 8m_1 + 6,\ m_1 \in \mathbb{N}^*$ hay $m \equiv 2 \,(\text{mod}4)$

Khi đó

$$(m+3)^n + 1 \equiv (2+3)^n + 1 \equiv 2 \pmod 4 \Rightarrow (m+3)^n + 1 = 4M + 2, M \in \mathbb{N}^*$$

và mẫu số $3m \equiv 2 \,(\text{mod}4) \Rightarrow 3m = 4M' + 2, M' \in \mathbb{N}^*$ với A là số lẻ.

Trường hợp 3. Nếu $m = 8m_1 + 4, m_1 \in \mathbb{N}^*$ kết hợp với $(*)$ nên $m_1 \equiv -1 \pmod 3$.

Do vậy tồn tại số nguyên tố p là ước của m_1 sao cho

$$p \equiv -1 \pmod 3 \qquad (**)$$

Do $A \in \mathbb{Z} \Rightarrow 0 \equiv (m+3)^n + 1 \equiv 3^n + 1 \equiv 3^{2k+1} + 1 \,(\text{mod } m)$

$$3^{2k+1} \equiv -1 \pmod{m} \Rightarrow 3^{2k+1} \equiv -1 \,(\text{mod}p)$$

$$\Rightarrow \left(3^{k+1}\right)^2 \equiv -3 \pmod p \Rightarrow \left(\frac{-3}{p}\right) = 1 \Rightarrow p \equiv 1 \,(\text{mod}6)$$

điều này mâu thuẫn với $(**)$.

Từ đây suy ra điều phải chứng minh của bài toán.

Nhận xét. Ngoài cách giải trên ta có thể chứng minh được rằng "Mọi ước lẻ của $3^n + 1, n$ lẻ đều có dạng $6k+1, k \in \mathbb{N}$" và sử dụng điều đó kết hợp với việc chia các trường hợp m là số chẵn ta có điều phải chứng minh. □

Bài 14

Chứng minh rằng phương trình $x^2 + 5 = y^3$ không có nghiệm nguyên.

Lời giải

Giả sử phương trình $x^2+5=y^3$ có nghiệm nguyên $(x,\ y)$.
Nếu y chẵn thì

$$x^2+5\equiv 0\pmod 8\Rightarrow x^2\equiv 3\pmod 8,$$

điều này vô lý. Do đó y phải là số lẻ.
Xét phương trình

$$x^2+5=y^3\Leftrightarrow x^2-3=y^3-8=(y-2).\left(y^2+2y+4\right),$$

do y là số lẻ nên y^2+2y+4 lẻ, gọi p là một ước nguyên tố bất kì của y^2+2y+4 suy ra p lẻ và

$$p\equiv 3\pmod 4 \qquad (*)$$

Từ điều kiện

$$y^2+2y+4\equiv 0\pmod p\Rightarrow (y+1)^2+3\equiv 0\pmod p\Rightarrow \left(\frac{-3}{p}\right)=1.$$

Mặt khác

$$x^2-3=(y-2).\left(y^2+2y+4\right)\Rightarrow x^2-3\equiv 0\pmod p\Rightarrow \left(\frac{3}{p}\right)=1.$$

Nên ta có

$$1=\left(\frac{-3}{p}\right)=\left(\frac{3}{p}\right).\left(\frac{-1}{p}\right)=\left(\frac{-1}{p}\right)\Rightarrow p\equiv 1\pmod 4 \qquad (**)$$

Vậy $(*)$ và $(**)$ mâu thuẫn với nhau suy ra điều giả sử là sai hay phương trình

$$x^2+5=y^3$$

không có nghiệm nguyên
Nhận xét. Ta có thể giải bài toán trên thông qua việc sử dụng ***kí hiệu Jacobi*** như sau. Do y là số lẻ, nếu

$$y\equiv 3\pmod 4\Rightarrow x^2=y^3-5\equiv 3^3-5\equiv 2\pmod 4,$$

điều này vô lý. Suy ra

$$y\equiv 1\pmod 4\Rightarrow y=4z+1,\ z\in\mathbb{Z}.$$

Khi đó ta có

$$x^2+4=y^3-1=(y-1).\left(y^2+y+1\right)=4z.\left(16z^2+12z+3\right).$$

Suy ra

$$x^2+4\equiv 0\ \left(\mathrm{mod}\ 16z^2+12z+3\right)\Rightarrow x^2\equiv -4\ \left(\mathrm{mod}\ 16z^2+12z+3\right).$$

Sử dụng ***kí hiệu Jacobi*** ta được

$$\left(\frac{-4}{16z^2+12z+3}\right)=\left(\frac{-1}{16z^2+12z+3}\right)=-1,$$

vô lí vì $16z^2+12z+3\equiv 3\pmod 4$.
Vậy phương trình không có nghiệm nguyên. □

Bài 15

2008 Serbia MO
Tìm tất cả các nghiệm nguyên không âm của phương trình $12^x+y^4=2008^z$.

Lời giải

Nếu $z > 0$ thì $y > 0$.
Nếu x là số chẵn thì vế trái của phương trình có dạng

$$a^2 + b^2,\ a, b \in \mathbb{N}^* \tag{1}$$

Nếu x là số lẻ thì vế trái của phương trình có dạng

$$a^2 + 3b^2,\ a, b \in \mathbb{N}^* \tag{2}$$

Mà $2008 = 251.8, p = 251$ là số nguyên tố và a, b đều không chia hết cho 251.
Từ (1) ta suy ra

$$a^2 \equiv -b^2 \,(\text{mod}251) \Rightarrow \left(\frac{-1}{251}\right) = 1$$

Từ (2) ta suy ra

$$a^2 \equiv -3b^2 \,(\text{mod}251) \Rightarrow \left(\frac{-3}{251}\right) = 1.$$

Mặt khác ta có

$$\left(\frac{-1}{251}\right) = (-1)^{\frac{251-1}{2}} = 1,$$

điều này vô lý và

$$\left(\frac{-3}{251}\right) = \left(\frac{-1}{251}\right).\left(\frac{3}{251}\right) = -\left(\frac{3}{251}\right) = -(-1)^{\frac{251-1}{2}}.\left(\frac{251}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

điều này vô lý.
Vậy $z = 0 \Rightarrow x = y = 0$.
Phương trình có nghiệm duy nhất là $x = y = z = 0$. □

Bài 16

Cho số nguyên dương $k, p = 4k + 1\,(k \in \mathbb{N}^*)$ là một số nguyên tố. Chứng minh rằng $k^k - 1$ chia hết cho p.

Lời giải

Ta có

$$p = 4k + 1 \Rightarrow k = \frac{p-1}{4} = -\left(\frac{p-1}{2}\right)^2 + p.\left(\frac{p-1}{4}\right) = -\left(\frac{p-1}{2}\right)^2 + kp$$

Suy ra

$$k \equiv -\left(\frac{p-1}{2}\right)^2 (\text{mod}p) \Rightarrow \left(\frac{p-1}{2}\right)^2 \equiv -k \,(\text{mod}p)$$

$$\Leftrightarrow \left(\frac{-k}{p}\right) = 1 \Leftrightarrow (-k)^{\frac{p-1}{2}} \equiv 1 \,(\text{mod}p) \tag{1}$$

Mặt khác

$$(-k)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}}.k^{\frac{p-1}{2}} \equiv k^{\frac{p-1}{2}} \,(\text{mod}p) \tag{2}$$

Từ (1) và (2) suy ra

$$k^{\frac{p-1}{2}} \equiv 1 \,(\text{mod}p)$$

Mà ta có

$$k^k \equiv (-1)^k.\left(\frac{p-1}{2}\right)^{2k} \equiv (-1)^k.2^{\frac{p-1}{2}}.k^{\frac{p-1}{2}} \equiv (-1)^k.2^{\frac{p-1}{2}} \,(\text{mod}p)$$

Nếu k là số chẵn, $k=2t, t\in\mathbb{N}^*$ suy ra

$$p=8t+1\Rightarrow\left(\frac{2}{p}\right)=1\Leftrightarrow 2^{\frac{p-1}{2}}\equiv 1\,(\mathrm{mod}p)\,,(-1)^k=1.$$

Vậy $k^k\equiv 1\,(\mathrm{mod}p)\Leftrightarrow k^k-1\vdots p$.
Nếu k là số lẻ, $k=2t+1, t\in\mathbb{N}^*$ suy ra

$$p=8t+5\Rightarrow\left(\frac{2}{p}\right)=-1\Leftrightarrow 2^{\frac{p-1}{2}}\equiv -1\,(\mathrm{mod}p)\,,(-1)^k=-1.$$

Vậy $k^k\equiv 1\,(\mathrm{mod}p)\Leftrightarrow k^k-1\vdots p.$.
Từ đây ta suy ra kết luận của bài toán. □

Bài 17

Gabriel Dospinescu

Cho p là số nguyên tố có dạng $4k+1,\ k\in\mathbb{N}^*$, sao cho $2^p-2\vdots p^2$. Chứng minh rằng ước nguyên tố lớn nhất q của 2^p-1 thỏa mãn bất đẳng thức $2^q>(6p)^p$.

Lời giải

Giả sử rằng

$$2^p-1=q_1^{k_1}.q_2^{k_2}...q_m^{k_m}.$$

Trong đó

$$q_i\in P,\ k_i\in\mathbb{N}^*,\forall i=\overline{1,\ m},\ q_1<q_2<...<q_m.$$

Lại đặt $q_i=1+x_ip\,(x_i\in\mathbb{N})\,,\forall i=\overline{1,\ m}$.
Ta có

$$2^p-1=(1+x_1p)^{k_1}.(1+x_2p)^{k_2}...(1+x_mp)^{k_m}.$$

Theo giả thiết ta có

$$2^p-2\equiv 0\left(\mathrm{mod}p^2\right)\Rightarrow 1\equiv\prod_{i=1}^{m}(1+x_ip)^{k_i}\left(\mathrm{mod}p^2\right)$$

Để ý rằng ta có

$$(1+x_ip)^{k_i}=1+\frac{k_i}{1}.x_ip+\frac{k_i\,(k_i-1)}{2}.x_i^2p^2+...+x_i^{k_i}p^{k_i}\equiv 1+k_ix_ip\ \left(\mathrm{mod}p^2\right)$$

Do vậy mà

$$\begin{aligned}\prod_{i=1}^{m}(1+k_ix_ip)\equiv 1\left(\mathrm{mod}p^2\right)&\Rightarrow 1+\sum_{i=1}^{m}k_ix_ip\equiv 1\left(\mathrm{mod}p^2\right)\\&\Rightarrow\sum_{i=1}^{m}k_ix_i\equiv 0\,(\mathrm{mod}p)\\&\Rightarrow x_m\sum_{i=1}^{m}k_i>\sum_{i=1}^{m}x_ik_i\geqslant p.\end{aligned}$$

Ta cũng có

$$\begin{aligned}2^p-1\equiv 0\,(\mathrm{mod}p_i)\Rightarrow 2^{p+1}\equiv 2\ \ (\mathrm{mod}q_i)\Rightarrow\left(\frac{2}{q_i}\right)&=1\\\Leftrightarrow q_i\equiv\pm 1\ \ (\mathrm{mod}8)\Rightarrow 1+x_ip&\equiv\pm 1\,(\mathrm{mod}\ 8)\\\Rightarrow x_i\vdots 8\vee x_ip&\equiv 6\,(\mathrm{mod}8)\\\Rightarrow x_i\vdots 8\vee x_i&\equiv 6\,(\mathrm{mod}8)\Rightarrow x_i\geqslant 6.\end{aligned}$$

Từ đó dẫn đến

$$2^p-1=\prod_{i=1}^{m}(1+x_ip)^{k_i}>(6p)^{k_1+k_2+...+k_m}\Rightarrow 2^{px_m}>(6p)^{x_m(k_1+k_2+...+k_m)}>(6p)^p.$$

Hay

$$2^{q-1}=2^{q_m-1}>(6p)^p\Rightarrow 2^q>2.(6p)^p.$$

Từ đây bài toán được giải quyết trọn vẹn và ta suy ra điều phải chứng minh. □

Bài 18

Chứng minh rằng không tồn tại nghiệm nguyên dương của phương trình sau

$$4xyz-x-y=t^2$$

Lời giải

Giả sử phương trình tồn tại nghiệm nguyên dương là (x,y,z,t). Khi đó, ta có

$$\begin{aligned}4xyz-x-y=t&\Leftrightarrow 16xyz^2=4xz+4yz+4zt^2\\&\Leftrightarrow 4zt^2+1=(4xz-1)(4yz-1)\\&\Rightarrow (2zt)^2\equiv -z\,(\mathrm{mod}\,(4yz-1))\end{aligned}\qquad(*)$$

Giả sử $z=2^kb$ với k là số nguyên không âm và b lẻ.
Từ $(*)$, sử dụng các tính chất của ***kí hiệu Jacobi***

$$\begin{aligned}1&=\left(\frac{-z}{4yz-1}\right)=\left(\frac{-1}{4yz-1}\right)\left(\frac{2^k}{4yz-1}\right)\left(\frac{b}{4yz-1}\right)=-\left(\frac{2}{4yz-1}\right)^k\left(\frac{-1}{b}\right)(-1)^{\frac{b-1}{2}}\\&=-\left(\frac{2}{4yz-1}\right)^k\left(\frac{(4.2^ky)\,b-1}{b}\right)(-1)^{\frac{b-1}{2}}=-\left(\frac{2}{4yz-1}\right)^k\left(\frac{-1}{b}\right)(-1)^{\frac{b-1}{2}}=-\left(\frac{2}{4yz-1}\right)^k=T\end{aligned}$$

Nếu k chẵn thì $T=-1$, vô lý.
Nếu k lẻ thì $k\geqslant 1$. Do đó

$$4yz-1=\left(4.2^k\right)by-1\equiv -1\,(\mathrm{mod}8)\Rightarrow\left(\frac{2}{4yz-1}\right)=1\Rightarrow T=-1$$

Điều này vô lý. Vậy phương trình không có nghiệm nguyên dương. □

Bài 19

Cho hai hàm số $f,g:\mathbb{N}^*\to\mathbb{N}^*$ thỏa mãn đồng thời hai điều kiện
i. g là toàn ánh
ii. $2f(n)^2=n^2+g(n)^2,\forall n\in\mathbb{N}$
Chứng minh rằng nếu $|f(n)-n|\leqslant 2013\sqrt{n},\forall n\in\mathbb{N}^*$ thì f có vô số điểm bất động.

Lời giải

Theo **định lý Dirichlet**, tồn tại vô hạn các số nguyên tố (p_i) với p_i có dạng $8k+3$.
Vì g là toàn ánh nên tồn tại vô hạn các số nguyên dương $\{x_n\}$ sao cho $g(x_n)=p_n\ \forall n$.
Theo điều kiện **ii** ta có

$$2f(x_n)^2={x_n}^2+g(x_n)^2={x_n}^2+{p_n}^2\equiv {x_n}^2\,(\mathrm{mod}p_n)$$

Do $p_n \equiv 3 \,(\text{mod}8)$ nên 2 là số không chính phương $(\text{mod}p_n)$.
Do đó tồn tại vô hạn hai dãy số nguyên dương $\{a_n\}, \{b_n\}$ sao cho

$$\begin{cases} x_n = a_n p_n \\ f(x_n) = b_n p_n \end{cases} \quad \forall n = 1, 2, ...$$

Khi đó ta có

$$2{b_n}^2 {p_n}^2 = {a_n}^2 {p_n}^2 + {p_n}^2 \Rightarrow 2{b_n}^2 = {a_n}^2 + 1 \Rightarrow \frac{b_n}{a_n} = \frac{\sqrt{{a_n}^2 + 1}}{\sqrt{2a_n}}$$

Mà $\lim\limits_{n \to +\infty} x_n = +\infty$, theo giả thiết, ta có

$$|f(n) - n| \leqslant 2013\sqrt{n} \Rightarrow \frac{2013}{\sqrt{x_n}} \geqslant \left| \frac{f(x_n)}{x_n} - 1 \right| = \left| \frac{b_n}{a_n} - 1 \right| = \left| \frac{1}{\sqrt{2}} \sqrt{\frac{{a_n}^2 + 1}{{a_n}^2}} - 1 \right|$$

$$\Rightarrow 0 \leqslant \lim \left| \frac{1}{\sqrt{2}} \sqrt{\frac{{a_n}^2 + 1}{{a_n}^2}} - 1 \right| \leqslant \lim \frac{2013}{\sqrt{x_n}} = 0$$

Do đó $\lim\limits_{n \to \infty} \sqrt{\dfrac{{a_n}^2 + 1}{{a_n}^2}} = \sqrt{2} \Rightarrow \lim a_n = 1$.
Mà $\{a_n\}$ là dãy vô hạn số nguyên dương nên $\exists N_0 \in \mathbb{N}^* : a_n = 1 \forall n \geqslant N_0 \Rightarrow b_n = 1 \forall n \geqslant N_0$.
Do vậy $f(p_n) = f(x_n) = p_n \forall n \geqslant N_0$ hay hàm f có vô số điểm bất động. □

Bài 20

Cho dãy $\{u_n\}$ xác định bởi

$$\begin{cases} u_1 = 1, u_2 = 11 \\ u_{n+2} = u_{n+1} + 5u_n \, \forall n \in \mathbb{N}^* \end{cases}$$

Chứng minh rằng u_n không là số chính phương $\forall n \geqslant 3$.

Lời giải

Bằng phương pháp quy nạp, ta sẽ chứng minh

$$u_{n+2k} = -(-5)^k u_n + u_{n+k} \forall k \in \mathbb{N}^* \qquad (*)$$

Dễ chứng minh được rằng

$$u_{6k+2} \equiv u_{6k+4} \equiv -1 \,(\text{mod}4), u_{6k} \equiv 2 \,(\text{mod}4), \forall k \in \mathbb{N}$$

Với $k = 0$ ta thấy $(*)$ đúng. Giả sử $(*)$ đúng k với.
Xét với $k + 1$, ta có

$$u_{6(k+1)} = u_{6k+6} = 11u_{6k+4} - 25u_{6k+2} \equiv -11 + 25 \equiv 2 \,(\text{mod}4)$$
$$u_{6(k+1)+2} = u_{6k+8} = 11u_{6k+6} - 25u_{6k+4} \equiv 11.2 + 25 \equiv -1 \,(\text{mod}4)$$
$$u_{6(k+1)+4} = u_{6k+10} = 11u_{6k+8} - 25u_{6k+6} \equiv -11 - 25.2 \equiv -1 \,(\text{mod}4)$$

Như vậy $(*)$ cũng đúng với $k + 1$.
Trước tiên, ta đi chứng minh u_{4k+1} không là số chính phương với mọi $n \in \mathbb{N}^*$. Giả sử tồn tại m sao cho $m \in \mathbb{N}^*, m \equiv 1 \,(\text{mod}4)$ thỏa mãn u_m là số chính phương. Đặt $m = 1 + 3^r.2k, r \in \mathbb{N}, k \in \mathbb{N}^*, 2|k, 3 \nmid k$.
Ta có

$$u_m = u_{1+3^r.2k} \equiv (-5)^{2k} u_{1+(3^r-2).2k}$$
$$\equiv ... \equiv -(-5)^{3^r.k} u_1 \equiv -(-5)^{3^r k} \,(\text{mod}u_k)$$

Gọi p là một ước nguyên tố bất kì của u_k, vì $(u_n, 5) = 1 \forall n \in \mathbb{N}^*$ nên ta suy ra $(u_k, 5) = 1$.
Ta có $u_m \equiv -(-5)^{3^r.k} \,(\mathrm{mod} p)$, mà k chẵn, u_m là số chính phươmg, nên

$$\left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \,(\mathrm{mod} 4) \Rightarrow u_k \equiv 1 \,(\mathrm{mod} 4)$$

Điều này vô lý vì k chẵn nên $u_k \equiv 1, 2 \,(\mathrm{mod} 4)$. Bằng cách chứng minh tương tự, ta chỉ ra được rằng u_{4k+3} cũng không là số chính phương.
Vậy u_n không là số chính phương với mọi $n \geqslant 3$. □

Bài 21

Giả sử rằng $a_1, a_2, ..., a_{2004}$ là các số nguyên âm thỏa mãn $a_1^n + a_2^n + ... + a_{2004}^n$ là số chính phương với mọi số nguyên dương n . Tìm số nhỏ nhất các số bằng 0 trong các số $a_1, a_2, ..., a_{2004}$.

Lời giải

Lấy số nguyên tố $p > N = \max\{2004, a_i | i = 1, 2, ..., 2004\}$ và lấy $n = p - 1$. Khi đó ta có

$$\sum_{i=1}^{2004} {a_i}^n = \sum_{i=1}^{2004} {a_i}^{p-1} \equiv k \,(\mathrm{mod} p)$$

trong đó k là số số hạng của dãy $a_1, a_2, ..., a_{2004}$ mà không chia hết cho p.
Ta có $0 < k < p$. Mà $\sum_{i=1}^{n} {a_i}^n$ là số chính phương nên ta có $\left(\frac{k}{p}\right) = 1 \ \forall p$ nguyên tố lớn hơn N hay k là số chính phương. Đặt $k = l^2$, từ đây suy ra

$$l^2 \leqslant 2004 \Rightarrow l \leqslant 44 \Rightarrow k \leqslant 44^2 = 1936$$

Do vậy, có ít nhất $2004 - 1936 = 68$ số bằng 0 trong dãy $a_1, a_2, ..., a_{2004}$. Mặt khác ta xét dãy

$$a_i = m^2 \forall i = \overline{1, 1936}; a_i = 0 \forall i = \overline{1937, 2004}$$

Khi đó ta được

$$\sum_{i=1}^{n} {a_i}^n = 1936\left(m^2\right)^n = (44m^n)^2$$

Vậy 68 là số cần tìm. □

Bài 22

Chứng minh rằng tồn tại vô hạn số nguyên dương n sao cho $n^2 + 1$ có ước nguyên tố lớn hơn $2n + \sqrt{10n}$.

Lời giải

Xét p là một số nguyên tố có dạng $8k + 1$, khi đó -1 là số chính phương mod p, hay phương trình đồng dư $x^2 = -1 \,(\mathrm{mod} p)$ có hai nghiệm thuộc $[1; p - 1]$. Ta gọi 2 nghiệm đó là x_1, x_2 sao cho

$$1 \leqslant x_1 \leqslant \frac{p-1}{2} < x_2 \leqslant p - 1$$

Chọn $n = x_1$, khi đó ta có $p | n^2 + 1, n \leqslant \frac{p-1}{2}$. Ta sẽ đi chứng minh $p > 2n + \sqrt{10n}$.

Do $1 \leqslant n \leqslant \dfrac{p-1}{2}$ nên ta đặt $n = \dfrac{p-1}{2} - u, 0 \leqslant u < \dfrac{p-1}{2}$, ta có

$$\begin{aligned} n^2 &\equiv -1 \,(\mathrm{mod} p) \\ &\Rightarrow \left(\frac{p-1}{2} - u\right)^2 \equiv -1 \,(\mathrm{mod} p) \\ &\Rightarrow (p-1-2u) + 4 \equiv 0 \,(\mathrm{mod} p) \\ &\Rightarrow (2u+1)^2 + 4 \equiv 0 \,(\mathrm{mod} p) \\ &\Rightarrow \exists r \in \mathbb{N}^* : (2u+1)^2 + 4 = rp \end{aligned}$$

Mặt khác ta lại có

$$\begin{aligned} (2u+1)^2 + 4 = 4u(u+1) + 1 \equiv 1 \,(\mathrm{mod} 8) &\Rightarrow rp \equiv 5 \,(\mathrm{mod} 8) \\ &\Rightarrow r \equiv 5 \,(\mathrm{mod} 8) \\ &\Rightarrow r \geqslant 5(2u+1)^2 + 4 \geqslant 5p \\ &\Rightarrow u \geqslant \frac{1}{2}\left(\sqrt{5p-4} - 1\right) \end{aligned}$$

Đặt $\sqrt{5p-4} = v \Rightarrow u \geqslant \dfrac{1}{2}(v-1)$, ta có

$$\begin{aligned} n = \frac{p-1}{2} - u &\leqslant \frac{p-1}{2} - \frac{1}{2}(v-1) \\ &= \frac{1}{2}(p-v) = \frac{1}{2}\left(\frac{v^2+4}{5} - v\right) \\ &\Rightarrow v^2 - 5v + 4 - 10n \geqslant 0 \\ &\Rightarrow (2v-5)^2 \geqslant 40n + 9 \\ &\Rightarrow v \geqslant \frac{1}{2}\left(5 + \sqrt{40n+9}\right) \end{aligned}$$

Mặt khác, do

$$n \leqslant \frac{1}{2}(p-v) \Rightarrow p \geqslant 2n + v \geqslant 2n + \frac{1}{2}\left(5 + \sqrt{40n+9}\right) > 2n + \sqrt{10n}$$

Do có vô hạn số nguyên tố p có dạng $8k+1$ nên bài toán được chứng minh. □

Bài 23

Cho $P(x)$ và $Q(x)$ là hai đa thức hệ số nguyên, nguyên tố cùng nhau trên $\mathbb{Q}$. Giả sử rằng với mọi $n \in \mathbb{Z}$ thì $P(n), Q(n)$ nguyên dương và $2^{Q(n)} - 1$ chia hết cho $3^{P(n)} - 1$. Chứng minh rằng $Q(x)$ là một đa thức hằng.

Lời giải

Do $P(x), Q(x) \in \mathbb{Z}[x]$ và nguyên tố cùng nhau trên $\mathbb{Q}[x]$ nên tồn tại các đa thức $u(x), v(x) \in \mathbb{Z}[x]$ và số nguyên dương d sao cho

$$P(x)u(x) + Q(x)v(x) = d \Rightarrow \gcd(P(n), Q(n)) \leqslant d \forall n \in \mathbb{Z}$$

Giả sử $Q(x)$ không là hằng số. Khi đó dãy $\{Q(n) | n \in \mathbb{Z}\}$ không bị chặn, mà ta lại có

$$Q(n) \in \mathbb{N}^* \forall n \in \mathbb{Z}$$

nên $\deg Q$ chẵn và hệ số bậc cao nhất của $Q(x)$ dương. Từ đó ta có thể chọn $m \in \mathbb{Z}$ sao cho

$$M = 2^{Q(m)} - 1 \geqslant 3^{\max\{P(0), P(1), P(2), \ldots, P(d)\}}$$

Ta có

$$M = 2^{Q(m)} - 1 | 3^{P(m)} - 1 \qquad (*)$$

nên $(M, 2) = (M, 3) = 1$. Gọi a, b tương ứng là bậc của $2, 3$ modulo M. Từ (*) ta có

$$a | Q(m), b | P(m) \Rightarrow \gcd(a, b) \leqslant \gcd(Q(m), P(m)) \leqslant d$$

Đặt $\gcd(a, b) = s$, khi đó tồn tại các số nguyên x_0, y_0 sao cho $s = ax_0 + by_0$.
Do $1 \leqslant s < d$ nên tồn tại $k \in \mathbb{N}, 0 \leqslant k < d$ sao cho $s = d - k$. Ta sẽ chứng minh rằng tồn tại các số nguyên x, y sao cho $0 \leqslant m + ax + by \leqslant \mathrm{d}$. Chọn $x = tx_0, y = ty_0$, ta có

$$0 \leqslant m + ax + by \leqslant \mathrm{d} \Leftrightarrow 0 \leqslant \mathrm{m{+}t}(ax_0 + by_0) \leqslant d$$

Điều này tương đương với

$$0 \leqslant m + t(d - k) \leqslant d \Leftrightarrow \frac{-m}{d-k} \leqslant t \leqslant \frac{d-m}{d-k}$$

Do $\dfrac{d-m}{d-k} - \dfrac{-m}{d-k} = \dfrac{d}{d-k} \geqslant 1$ nên tồn tại số nguyên t thỏa mãn. Ta có $Q(x) \in \mathbb{Z}[x]$ nên

$$\begin{aligned} Q(m + ax) \equiv Q(m) (\mathrm{mod} a) &\Rightarrow 2^{Q(m+ax+by)} \equiv 2^{Q(m)} \equiv 1 (\mathrm{mod} M) \\ &\Rightarrow M | 2^{Q(m+ax)} - 1 | 3^{P(m+ax)} - 1 \end{aligned}$$

Tương tự, ta có

$$\begin{aligned} P(m + ax + by) &\equiv P(m + ax) (\mathrm{mod} b) \\ &\Rightarrow 3^{P(m+ax+by)} \equiv 3^{P(m+ax)} \equiv 1 (\mathrm{mod} M) \\ &\Rightarrow M \leqslant 3^{P(m+ax+by)} - 1 \leqslant 3^{\max\{P(0), P(1), P(2), \ldots P(d)\}} - 1 \\ &\leqslant 2^{Q(m)} - 2 = M - 1 \end{aligned}$$

điều này là vô lý. Vậy $Q(x) = const.$ □

Bài 24

Iran TST 2004

Cho số nguyên tố p và số nguyên dương k, chứng minh rằng tồn tại số nguyên dương n sao cho

$$\left(\frac{n}{p}\right) = \left(\frac{n+k}{p}\right)$$

Lời giải

Bài toán tương đương với việc chứng minh tồn tại số nguyên dương n để

$$\left(\frac{n(n+k)}{p}\right) = 1$$

Ta giả sử tồn tại $1 \leqslant k \leqslant p - 1$ sao cho

$$\left(\frac{n(n+k)}{p}\right) = -1, \forall 1 \leqslant n \leqslant p - 1$$

Vì với mỗi số nguyên tố p bất kì, có đúng $\dfrac{p-1}{2}$ số không chính phương $(\mathrm{mod} p)$.
Do đó nếu $f(n, k, p) = n(n + k) (\mathrm{mod} p)$ nhận nhiều hơn $\dfrac{p-1}{2}$ giá trị phân biệt thì theo ***định lý***

Dirichlet, tồn tại ít nhất một số chính phương $(\mathrm{mod} p)$. Như vậy, tập giá trị của $f(n,k,p)$ nhận không quá $\dfrac{p-1}{2}$ phần tử, do đó ta có ít nhất ba số x,y,z nguyên phân biệt sao cho

$$\begin{cases} 1 \leqslant x,y,z \leqslant p-1 \\ f(x,k,p) = f(y,k,p) = f(z,k,p) \end{cases} \Rightarrow x(x+k) \equiv y(y+k) \equiv z(z+k) \,(\mathrm{mod} p)$$

$$\Leftrightarrow \begin{cases} p|x+y+k \\ p|y+z+k \\ p|z+x+k \end{cases} \Leftrightarrow x \equiv y \equiv z \,(\mathrm{mod} p)$$

Điều này vô lí vì x,y,z phân biệt và $1 \leqslant x,y,z \leqslant p-1$.
Bài toán được chứng minh. □

Bài 25

Korea Final 2000

Cho số nguyên tố $p = 4k+1$, tính $\displaystyle\sum_{x=1}^{p-1} \left(\left\lfloor \frac{2x^2}{p} \right\rfloor - 2 \left\lfloor \frac{x^2}{p} \right\rfloor \right)$.

Lời giải

Ta dễ thấy $\lfloor 2x \rfloor - 2\lfloor x \rfloor \leqslant 1 \forall x \in \mathbb{R}$.
Đẳng thức xảy ra khi và chỉ khi $\{x\} \geqslant \dfrac{1}{2}$. Ta sẽ đi tìm số đồng dư của một số chính phương khi chia cho số nguyên tố $p = 4k+1$ sao cho nó lớn hơn $\dfrac{p-1}{2}$. Theo tính chất số (1) của thặng dư bình phương, ta có đúng $\dfrac{p-1}{2}$ số chính phương $(\mathrm{mod} p)$. Vì $p = 4k+1$ nên ta suy ra

$$\left(\frac{-1}{p}\right) = 1 \Rightarrow \left(\frac{-a^2}{p}\right) = 1 \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{p-a}{p}\right)$$

Như vậy, ta sẽ có đúng $\dfrac{p-1}{4}$ số chính phương $(\mathrm{mod} p)$ không lớn hơn $\dfrac{p-1}{2}$ và đúng $\dfrac{p-1}{4}$ số chính phương $(\mathrm{mod} p)$ lớn hơn $\dfrac{p-1}{2}$. Do đó

$$\sum_{x=1}^{p-1} \left(\left\lfloor \frac{2x^2}{p} \right\rfloor - 2 \left\lfloor \frac{x^2}{p} \right\rfloor \right) = \frac{p-1}{2}$$

vì nếu $\begin{cases} \forall i,j \in \mathbb{N} \\ 1 \leqslant i,j \leqslant p-1 \\ i+j = p \end{cases}$ thì $i^2 \equiv j^2 \,(\mathrm{mod} p)$.
Bài toán được giải quyết. □

Bài 26

a) Chứng minh rằng số $2^n + 1$ không có ước nguyên tố dạng $8k-1$.
b) Chứng minh rằng với mọi số nguyên dương n, số $2^{3^n} + 1$ có ít nhất n ước nguyên tố có dạng $8k+3$.

Lời giải

a) Giả sử rằng tồn tại số p nguyên tố có dạng $8k-1$ sao cho $p|(2^n+1)$.

- Nếu n chẵn thì
$$-1 \equiv \left(2^{\frac{n}{2}}\right)^2 (\mathrm{mod} p) \Rightarrow \left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 (\mathrm{mod} 4)$$
điều này mâu thuẫn.

- Nếu n lẻ, do $p \equiv -1 (\mathrm{mod} 8)$ nên
$$-2 \equiv \left(2^{\frac{n+1}{2}}\right)^2 (\mathrm{mod} p) \Rightarrow 1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}} = -1$$
điều này cũng mâu thuẫn.

Vậy số $2^n + 1$ không có ước nguyên tố dạng $8k - 1$.
b) Từ chứng minh ở câu a, ta nhận thấy
"Nếu n lẻ thì $2^n + 1$ không có ước nguyên tố dạng $8k + 5$."
Do đó mọi ước nguyên tố của $2^{3^n} + 1$ đều đồng dư 1 hoặc 3 (mod8). Ta có
$$2^{3^n} + 1 = (2+1)\left(2^2 - 2 + 1\right)\left(2^{2.3} - 2^3 + 1\right) ... \left(2^{2.3^{n-1}} - 2^{3^{n-1}} + 1\right)$$
Đặt $s_i = 2^{2.3^i} - 2^{3^i} + 1, \forall 1 \leqslant i \leqslant n-1$. Ta sẽ chứng minh rằng $\forall 1 \leqslant i \leqslant j \leqslant n-1$ thì $\gcd(s_i, s_j) = 3$.
Dễ thấy
$$s_i \equiv 1 - (-1) + 1 \equiv 3 (\mathrm{mod} 9) \Rightarrow 3 || s \forall i$$
Gọi p là một số nguyên tố chia hết $\gcd(s_i, s_j)$. Khi đó
$$p | s_i | \left(2^{3^{i+1}} + 1\right) \Rightarrow 2^{3^j} = \left(2^{3^{i+1}}\right)^{3^{j-i-1}} \equiv (-1)^{3^{j-i-1}} \equiv -1 (\mathrm{mod} p)$$
$$\Rightarrow 0 \equiv s_j = 2^{2.3^j} - 2^{3^j} + 1 \equiv 1 - (-1) + 1 \equiv 3 (\mathrm{mod} p) \Rightarrow p = 3$$
Vậy $\gcd(s_i, s_j) = 3 \forall 1 \leqslant i \leqslant j \leqslant n-1$. Lấy $i \in \{1, 2, ..., n-1\}$.
Nếu mọi ước nguyên tố của s_i (trừ 3) đều có dạng $8k+1$ thì $s_i \equiv 3 (\mathrm{mod} 8)$. Điều này vô lý vì $3 || s_i \forall i$.
Do vậy mỗi s_i đều có ít nhất một ước nguyên tố x p_i dạng $8k+3$ mà $p_i \neq 3$.
Do $\gcd(s_i, s_j) = 3$ nên $p_i \neq p_j \forall 1 \leqslant i < j \leqslant n-1$. Như vậy $2^{3^n} + 1$ có ít nhất n ước nguyên tố dạng $8k+3$ là $3, p_1, p_2, ..., p_{n-1}$. □

Bài 27

Cho số nguyên dương a. Xét dãy số nguyên $\{x_n\}$ xác định bởi $x_1 = a, x_{n+1} = 2x_n + 1 \forall n \geqslant 1$. Đặt $y_n = 2^{x_n} - 1$. Tìm số nguyên dương k lớn nhất sao cho tồn tại số nguyên dương a để $y_1, y_2, ..., y_k$ đều là số nguyên tố.

Lời giải

Nhận xét 1. Nếu $2^m - 1$ là số nguyên tố thì m cũng là số nguyên tố.
Nhận xét 2. Nếu p là số nguyên tố có dạng $4m+3$ và $q = 2p+1$ cũng là số nguyên tố thì $q | 2^p - 1$.
Chứng minh.
Theo ***định lý Fermat*** ta có
$$q | 2^{q-1} - 1 = 2^{2p} - 1 = (2^p - 1)(2^p + 1)$$
Gọi $\alpha = \mathrm{ord}_q(2)$, suy ra $\alpha | 2p \Rightarrow \alpha \in \{2, p, 2p\}$. Ta xét 2 trường hợp.

- Nếu $\alpha = 2 \Rightarrow q | 2^2 - 1 = 3 \Rightarrow 1 = 3 \Rightarrow p = 1$, điều này là vô lý.

- Nếu $\alpha = 2p$, từ đây suy ra $q \not| 2^p - 1 \Rightarrow q | 2^p + 1 \Rightarrow -2 \equiv \left(2^{\frac{p+1}{2}}\right)^2 (\mathrm{mod} q)$ hay $\left(\frac{-2}{q}\right) = 1$ nhưng $q = 2p + 1 = 8m + 7$, điều này là vô lý.

Vậy $\alpha = p \Rightarrow q|2^p - 1$.

Trở lại bài toán.

Với $k = 2$, chọn $a = 2$ ta được $y_1 = 2, y_2 = 31, y_3 = 2047 = 23.89$. Giả sử tồn tại $k \geqslant 3$ sao cho tồn tại $a \in \mathbb{N}^*$ thỏa mãn $y_1, y_2, ..., y_k$ đều là các số nguyên tố. Khi đó theo **nhận xét 1** ta có $x_1, x_2, ..., x_k$ cũng là số nguyên tố. Nói riêng y_3 là số nguyên tố nên theo trên ta có $a \geqslant 3$, mà $a = x_1$ nguyên tố nên a lẻ, suy ra

$$x_n \equiv 3 \,(\mathrm{mod} 4) \,\forall n \geqslant 2$$

Ta có $x_2 \equiv 3 \,(\mathrm{mod} 4)\,, x_3 = 2x_2 + 1$, x_2, x_3 nguyên tố nên theo **nhận xét 2**, ta có $x_3|2^{x_2} - 1$ nhưng $2^{x_2} - 1 = y_2$ là số nguyên tố nên

$$x_3 = 2^{x_2} - 1 \Rightarrow 4a + 3 = 2^{2a+1} - 1$$

Điều này vô lý vì $a \geqslant 3$.

Vậy $k = 2$ là giá trị lớn nhất cần tìm. □

Bài 28

Tìm tất cả các số nguyên dương k thỏa mãn với k số nguyên tố lẻ đầu tiên $p_1, p_2, ..., p_k$, tồn tại các số nguyên dương $a, n\,(n > 1)$ sao cho $p_1p_2...p_k = a^n + 1$.

Lời giải

Giả sử k là số nguyên dương sao cho tồn tại các số nguyên dương $a, n\,(n > 1)$ thỏa mãn $p_1p_2...p_k = a^n+1$ với $p_1, p_2, ..., p_k$ là k số nguyên tố lẻ đầu tiên.

- Xét n chẵn, ta có $-1 \equiv \left(a^{\frac{n}{2}}\right)^2 (\mathrm{mod} p_i)\,\forall i = \overline{1,k}$, từ đây suy ra

$$\left(\frac{-1}{p_i}\right) = 1 \forall i = \overline{1,k} \Rightarrow \left(\frac{-1}{3}\right) = 1$$

  điều này là vô lý.

- Xét n lẻ, giả sử tồn tại $i \in \{1, 2, ..., k\}$ sao cho $p_i|n$. Khi đó ta có

$$p_i|a^n + 1 = \left(a^{\frac{n}{p_i}}\right)^{p_i} + 1$$

  Mà theo ***định lý Fermat*** nhỏ thì

$$p_i|\left(a^{\frac{n}{p_i}}\right)^{p_i} - a^{\frac{n}{p_i}} \Rightarrow p_i|a^{\frac{n}{p_i}} + 1$$

  Do đó ta được

$$v_{p_i}\left(a^n + 1\right) = v_{p_i}\left(\left(a^{\frac{n}{p_i}}\right)^{p_i} + 1\right) = v_{p_i}\left(a^{\frac{n}{p_i}} + 1\right) + v_{p_i}\left(p_i\right) \geqslant 2 \Rightarrow {p_i}^2|a^n + 1$$

  Suy ra ${p_i}^2|p_1p_2...p_k$. Vô lý vì các p_j nguyên tố đôi một phân biệt. Kết hợp với n lẻ, $n > 1$ ta suy ra tất cả các ước nguyên tố của n đều lớn hơn p_k. Do đó $n > p_k$. Giả sử a không có ước nguyên tố lẻ thì $a = 2^m, m \in \mathbb{N}^*$, ta suy ra $p_1p_2...p_k = 2^{mn} + 1$. Ta xét 2 trường hợp.

  – Nếu m chẵn thì $\left(\frac{-1}{p_i}\right) = 1 \forall i = \overline{1,k}$, điều này là vô lý.

  – Nếu m lẻ thì $2x^2 + 1 \equiv 0 \,(\mathrm{mod} 5)$,vì dễ thấy $k \geqslant 2$, với $x = 2^{\frac{2^{mn}-1}{2}}$, ta suy ra

$$x^2 \equiv 2 \,(\mathrm{mod} 5) \Rightarrow \left(\frac{2}{5}\right) = 1$$

  điều này vô lý.

Vậy tồn tại p nguyên tố lẻ sao cho $p|a$ mà $(a,p_i)=1 \forall i=\overline{1,k}$ nên $p>p_k$, suy ra

$$p_i p_2 ... p_k = a^n + 1 > {p_k}^{p_k}$$

Vậy không tồn tại số nguyên dương k thỏa mãn bài toán. □

Bài 29

Cho số nguyên tố $p>3, p=4n+1$. Tính $S_1=\sum_{i=1}^{n}\left[\sqrt{ip}\right]$.

Lời giải

Trước tiên ta phát biểu và chứng minh bổ đề sau.

Bổ đề. Với p là một số nguyên tố lẻ thì trong tập $S=\{1,2,...,p-1\}$ có $\frac{p-1}{2}$ số chính phương mod$p$ và $\frac{p-1}{2}$ số không chính phương mod$p$.

Chứng minh.

Với mỗi $i \in S_1=\left\{1,2,...,\frac{p-1}{2}\right\}$, gọi $r_i \in S$ là số duy nhất mà $i^2 \equiv r_i \,(\text{mod}p)$. Dễ thấy $r_j \neq r_j \forall i \neq j$, khi đó tập hợp $A=\left\{r_i : r_i \in S, i^2 \equiv r_i \,(\text{mod}p), i \in S_1\right\}$ có đúng $\frac{p-1}{2}$ phần tử. Ta chứng minh rằng A là tập tất cả các số chính phương mod$p$ trong S. Giả sử $a \in S$ sao cho tồn tại $k \in S$ thỏa mãn $a \equiv k^2 \,(\text{mod}p)$.

- Nếu $k \in S_1 \Rightarrow a=r_k \in A$.
- Nếu $k \notin S_1 \Rightarrow h=p-k \in S_1; a \equiv h^2 \,(\text{mod}p) \Rightarrow a=r_h \in A$.

Bổ đề được chứng minh.

Trở lại bài toán.

Đặt $S=\sum_{i=1}^{n}\left[\sqrt{ip}\right]$. Dễ thấy $\left[\sqrt{np}\right]=2n$. Cho x nhận lần lượt các giá trị $1,2,...,n$ và với mỗi x như thế, tương ứng ta cho y nhận các giá trị

$$\left[\sqrt{(x-1)p}\right]+1, \left[\sqrt{(x-1)p}+2\right], ..., [\sqrt{xp}]$$

Đặt $r=r(x,y)=xp-y^2$ ta suy ra $r \in (0,p)$.

Dễ thấy $-r=y^2-xp \equiv y^2 \,(\text{mod}p) \Rightarrow \left(\frac{-r}{p}\right)=1$. Mà $p \equiv 1 \,(\text{mod}4)$ nên

$$\left(\frac{-1}{p}\right)=1 \Rightarrow \left(\frac{r}{p}\right)=1$$

Giả sử ta có $r(x_1,y_1)=r(x_2,y_2)$, suy ra

$${x_1 p - {y_1}}^2 = {x_2 p - {y_2}}^2 \Rightarrow p|(y_1-y_2)(y_1+y_2)$$

Mà $0<y_1+y_2<2\left[\sqrt{np}\right]=4n<p$ và $-p<y_1-y_2<p$ nên $y_1-y_2=0$ hay $y_1=y_2, x_1=x_2$, hay $r(x,y)$ đôi một phân biệt. Như vậy ta có các số $r(x,y)$ là

$$N=\sum_{x=1}^{n}\left([\sqrt{xp}]-\left[\sqrt{(x-1)p}\right]\right)=[\sqrt{np}]=2n=\frac{p-1}{2}=$$

số thặng dư bình phương mod$p$ trong tập $\{1,2,...,p-1\}$. Do $p \equiv 1 \,(\text{mod}4)$ nên

$$\left(\frac{r}{p}\right)\left(\frac{p-r}{p}\right) \equiv r^{\frac{p-1}{2}}.(p-r)^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}}.(-r)^{\frac{p-1}{2}} = r^{p-1} \equiv 1 \,(\text{mod}p)$$

$$\Rightarrow \left(\frac{r}{p}\right)=1 \Leftrightarrow \left(\frac{p-r}{p}\right)=1$$

Mà rõ ràng $r \neq p-r$ nên tập các thặng dư bình phương mod$p$ trong tập $\{1,2,...,p-1\}$ có thể phân hoạch thành $\dfrac{p-1}{4}$ cặp, mỗi cặp có tổng bằng p, suy ra

$$\sum r(x,y) = \frac{p(p-1)}{4} \qquad (*)$$

Mặt khác ta lại có

$$\begin{aligned}
\sum r(x,y) &= \sum_{x=1}^{n}\left(\sum_{y=\left[\sqrt{(x-1)p}\right]+1}^{[\sqrt{xp}]} r(x,y)\right) = \sum_{x=1}^{n}\left(\sum_{y=\left[\sqrt{(x-1)p}\right]+1}^{[\sqrt{xp}]}\left(xp-y^2\right)\right) \\
&= \sum_{x=1}^{n}\left(\left([\sqrt{xp}]-\left[\sqrt{(x-1)p}\right]\right)xp - \sum_{y=\left[\sqrt{(x-1)p}\right]+1}^{[\sqrt{xp}]} y^2\right) \\
&= p\sum_{x=1}^{n}\left(x\left([\sqrt{xp}]-\left[\sqrt{(x-1)p}\right]\right)\right) - \sum_{y=1}^{2n} y^2 \\
&= p\left(-S+(n+1)[\sqrt{np}]\right) - \frac{2n(2n+1)(4n+1)}{6} \\
&= -pS + 2n(n+1)p - \frac{n(2n+1)(4n+1)}{3} \qquad (**)
\end{aligned}$$

Từ (*) và (**), với $p = 4n+1$ ta suy ra $S = \dfrac{p^2-1}{12}$.

Bài toán được giải quyết. □

Bài 30

IMO Shortlist 2009 N7

Cho a, b là hai số nguyên dương thỏa mãn ab không là số chính phương. Chứng minh rằng tồn tại vô hạn số nguyên dương n sao cho $(a^n-1)(b^n-1)$ không là số chính phương.

Lời giải

Bổ đề. Cho a là một số nguyên dương không chính phương. Khi đó tồn tại vô hạn số nguyên tố p sao cho a không là số chính phương mod$p$.

Chứng minh. Do a là một số nguyên dương không chính phương nên ta đặt $a = b^2c$, trong đó $b \in \mathbb{N}^*, c = q_1q_2...q_m\ (m \geqslant 1)$ với q_i nguyên tố và đoi một phân biệt. Khi đó với mỗi số nguyên tố lẻ p mà $(p,a)=1$, ta có

$$\left(\frac{a}{p}\right) = \left(\frac{b^2c}{p}\right) = \left(\frac{c}{p}\right) = \prod_{i=1}^{m}\left(\frac{q_i}{p}\right)$$

Xét các khả năng sau.

Khả năng 1. Nếu q_1 lẻ. Chọn $r_1, r_2, ..., r_m$ thỏa mãn r_1 không là số chính phương modq_1 và r_i là số chính phương modq_i với mọi $i = 2,...,m$. Theo định lý thặng dư Trung Hoa, tồn tại số nguyên p_0 thỏa mãn

$$\begin{cases} p_0 \equiv r_i \,(\mathrm{mod} q_i)\ \forall i = 1,2,..,m \\ p_0 \equiv 1\,(\mathrm{mod}4) \end{cases} \qquad (*)$$

Dễ thấy $(p_0,q_i) = (p_0,4) = 1, \forall i = 1,2,...,m \Rightarrow (p_0, 4q_1q_2...q_m) = 1$. Mà ta có $p = p_0 + (4q_1q_2...q_m)t$ cũng là nghiệm của (*) với mọi $t \in \mathbb{N}$. Nhưng theo ***định lý Dirichlet***, ta có thể chọn được vô hạn t

sao cho p là số nguyên tố, hay tồn tại vô hạn số nguyên tố p thỏa mãn

$$\begin{cases} p \equiv r_i \,(\mathrm{mod} q_i)\, \forall i = 1,2,...,m \\ p \equiv 1 \,(\mathrm{mod} 4) \end{cases} \Rightarrow \left(\frac{p}{q_i}\right) = \left(\frac{r_i}{q_i}\right) = \begin{cases} -1 khi i = 1 \\ 1 khi i = 2,...,m \end{cases}$$

Do $p \equiv 1 \,(\mathrm{mod} 4)$ nên theo ***luật tương hỗ Gauss***, ta có $\left(\frac{p}{q_i}\right) = \left(\frac{q_i}{p}\right) \forall i = 1,2,...,m$, suy ra

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{m} \left(\frac{q_i}{p}\right) = \prod_{i=1}^{m} \left(\frac{p}{q_i}\right) = -1$$

Khả năng 2. Nếu $q_1 = 2$. Chọn r_i là số chính phương $\mathrm{mod} p_i$ với mọi $i = 2,...,m$. Tương tự ta có vô hạn số nguyên tố p thỏa mãn

$$\begin{cases} 1 \leqslant x, y, z \leqslant p-1 \\ f(x,k,p) = f(y,k,p) = f(z,k,p) \\ p \equiv r_i \,(\mathrm{mod} q_i)\, \forall i = 2,...,m \\ p \equiv 5 \,(\mathrm{mod} 8) \end{cases}$$

Từ đây ta suy ra

$$\left(\frac{p}{q_i}\right) = \left(\frac{r_i}{q_i}\right) = 1 \forall i = 2,..,m$$

Do $p \equiv 5 \,(\mathrm{mod} 8)$ nên

$$p \equiv 1 \,(\mathrm{mod} 4) \Rightarrow \left(\frac{q_i}{p}\right) = \left(\frac{p}{q_i}\right) = 1 \forall i = 2,...,m \Rightarrow \left(\frac{a}{p}\right) = \prod_{i=1}^{m} \left(\frac{q_i}{p}\right) = -1$$

Bổ đề được chứng minh.

Trở lại bài toán.

Theo giả thuyết ta có ab không là số chính phương nên theo bổ đề ta có tồn tại vô hạn số nguyên tố p sao cho

$$\left(\frac{ab}{p}\right) = -1 \Rightarrow \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -1$$

Từ đó không mất tính tổng quát ta có thể giả sử $\left(\frac{a}{p}\right) = 1; \left(\frac{b}{p}\right) = -1$, hay

$$a^{\frac{p-1}{2}} \equiv 1 \,(\mathrm{mod} p)\,; b^{\frac{p-1}{2}} = -1 \,(\mathrm{mod} p)$$

Suy ra p không chia hết $b^{\frac{p-1}{2}} - 1$. Xét các khả năng sau

- Nếu $v_p\left(a^{\frac{p-1}{2}} - 1\right)$ lẻ. Khi đó

  $$v_p\left(\left(a^{\frac{p-1}{2}} - 1\right)\left(b^{\frac{p-1}{2}} - 1\right)\right)$$

  lẻ, do đó $\left(a^{\frac{p-1}{2}} - 1\right)\left(b^{\frac{p-1}{2}} - 1\right)$ không là số chính phương.

- Nếu $v_p\left(a^{\frac{p-1}{2}} - 1\right)$ chẵn. Theo định lý về số mũ đúng ta có

  $$v_p\left(a^{\frac{p-1}{2}p} - 1\right) = v_p\left(a^{\frac{p-1}{2}} - 1\right) + 1$$

  là một số lẻ. Hơn nữa ta lại có $b^{\frac{p-1}{2}p} - 1 \equiv (-1)^p - 10 \,(\mathrm{mod} p)$ nên ta suy ra

  $$v_p\left(\left(a^{\frac{p-1}{2}p} - 1\right)\left(b^{\frac{p-1}{2}p} - 1\right)\right)$$

  lẻ, do đó $\left(a^{\frac{p-1}{2}p} - 1\right)\left(b^{\frac{p-1}{2}p} - 1\right)$ không là số chính phương.

Bài toán được giải quyết. □

Bài 31

Chứng minh rằng với mỗi số nguyên dương n, đều tồn tại các số nguyên > 1, đôi một nguyên tố cùng nhau $k_0, k_1, ..., k_n$ sao cho $k_0k_1...k_n - 1$ là tích của hai số nguyên liên tiếp.

Lời giải

Bổ đề. Cho p là một số nguyên tố có dạng $3k + 1$. Khi đó tồn tại số nguyên dương r sao cho $p|\left(r^2 + r + 1\right)$.

Chứng minh. Do p là một số nguyên tố dạng $3k+1$ nên $p \equiv 1 \,(\text{mod}6)$, suy ra -3 là số chính phương mod$p$, hay tồn tại số nguyên dương x sao cho

$$(x + kp)^2 \equiv -3 \,(\text{mod}p) \,\forall k \in \mathbb{N}$$

Rõ ràng tồn tại $k \in \mathbb{N}$ sao cho $x + kp = 2r + 1$, với r nguyên dương nào đó. Suy ra

$$p|(2r + 1)^2 + 3 = 4\left(r^2 + r + 1\right) \Rightarrow p|\left(r^2 + r + 1\right)$$

Trở lại bài toán.

Với mỗi số nguyên dương n, rõ ràng tồn tại các số nguyên tố dôi một phân biệt $p_0, p_1, ..., p_n$ có dạng $3k + 1$. Khi đó theo bổ đề, ta gọi $r_0, r_1, ..., r_n$ là các số nguyên dương thỏa mãn

$$p_i|\left({r_i}^2 + r_1 + 1\right) \forall i = 0, 1, ..., n$$

Theo ***định lý thặng dư Trung Hoa***, tồn tại số nguyên dương a thỏa mãn

$$a \equiv r_i \,(\text{mod}p_i) \,\forall i = 0, 1, ..., n$$

Suy ra $p_0p_1...p_n|\left(a^2 + a + 1\right)$. Với mỗi i , lấy k_i là lũy thừa lớn nhất của p_i chia hết $a^2 + a + 1$ và đặt $k_0 = \dfrac{a^2 + a + 1}{k_1...k_n}$. Khi đó rõ ràng $k_0, k_1, ..., k_n$ đôi một nguyên tố cùng nhau và

$$k_0k_1...k_n - 1 = a^2 + a = a\,(a + 1)$$

Bài toán được giải quyết. □

Bài 32

Với p là một số nguyên tố lẻ và a là số nguyên dương thỏa mãn $1 \leqslant a \leqslant p - 1$. Chứng minh rằng

$$\sum_{n=0}^{p-1} \left(\frac{n^2 + a}{p}\right) = -1$$

Lời giải

Đây là một bài toán tương đối khó. Ta sẽ xét các trường hợp sau.

Trường hợp 1. Nếu $\left(\dfrac{a}{p}\right) = -1$, với $n \neq 0$ ta có

$$\left(\frac{n^2 + a}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{an^2 + a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a + \left(an^{-1}\right)^2}{p}\right)$$

Do vậy

$$\sum_{n \in \mathbb{F}_p^\times} \left(\frac{n^2 + a}{p}\right) = \left(\frac{a}{p}\right) \sum_{n \in \mathbb{F}_p^\times} \left(\frac{a + \left(an^{-1}\right)^2}{p}\right) = \left(\frac{a}{p}\right) \sum_{n \in \mathbb{F}_p^\times} \left(\frac{a + n^2}{p}\right).$$

Vì $\left(\frac{a}{p}\right) = -1$ nên ta có $\sum_{n\in\mathbb{F}_p^\times}\left(\frac{n^2+a}{p}\right) = 0$ và đồng thời

$$\sum_{n\in\mathbb{F}_p}\left(\frac{n^2+a}{p}\right) = 0 + \left(\frac{a}{p}\right) = -1\,.$$

Trường hợp 2. Nếu $\left(\frac{a}{p}\right) = +1$, ta viết lại $a \equiv x^2 \pmod p$, do đó suy ra

$$\begin{aligned}\sum_{n\in\mathbb{F}_p}\left(\frac{n^2+a}{p}\right) &= \sum_{n\in\mathbb{F}_p^\times}\left(\frac{n^2+x^2}{p}\right)+1 = \sum_{n\in\mathbb{F}_p^\times}\left(\frac{\left(nx^{-1}\right)^2+1}{p}\right)+1\\ &= \sum_{n\in\mathbb{F}_p^\times}\left(\frac{n^2+1}{p}\right)+1 = \sum_{n\in\mathbb{F}_p}\left(\frac{n^2+1}{p}\right).\end{aligned}$$

Đến đây có 2 khả năng xảy ra là $\left(\frac{-1}{p}\right) = +1$ và $\left(\frac{-1}{p}\right) = -1$.

(i) Với $\left(\frac{-1}{p}\right) = +1$, ta có $k^2 \equiv -1 \pmod p$, đến đây ta sẽ chứng minh một kết quả.

Bổ đề. Với p là số nguyên tố lẻ và $(a,p) = (b,p) = 1$, khi đó thì

$$\sum_{x=1}^{p-1}\left(\frac{x(ax+b)}{p}\right) = -\left(\frac{a}{p}\right)$$

Chứng minh. Với x^{-1} là nghịch đảo của x modulo p thì ta có

$$\begin{aligned}\sum_{x=1}^{p-1}\left(\frac{x(ax+b)}{p}\right) &= \sum_{x\in\mathbb{F}_p^\times}\left(\frac{x}{p}\right)\left(\frac{ax+b}{p}\right) = \sum_{x\in\mathbb{F}_p^\times}\left(\frac{x^{-1}}{p}\right)\left(\frac{ax+b}{p}\right)\\ &= \sum_{x\in\mathbb{F}_p^\times}\left(\frac{x^{-1}(ax+b)}{p}\right) = \sum_{x\in\mathbb{F}_p^\times}\left(\frac{a+bx^{-1}}{p}\right)\end{aligned}$$

Do vậy ta suy ra

$$\sum_{x=1}^{p-1}\left(\frac{x(ax+b)}{p}\right) = \sum_{y\in\mathbb{F}_p^\times}\left(\frac{a+by}{p}\right) = \sum_{y\in\mathbb{F}_p}\left(\frac{a+by}{p}\right) - \left(\frac{a}{p}\right).$$

Vì $p \nmid b$ nên ta có $\{a+by | y\in\mathbb{F}_p\}$ là một hệ thặng dư đầy đủ modulo p, do vậy

$$\sum_{y\in\mathbb{F}_p}\left(\frac{a+by}{p}\right) = 0$$

Từ đây bổ đề được chứng minh.

Quay lại trường hợp đang xét. Áp dụng ***bổ đề*** trên ta có

$$\begin{aligned}\sum_{n\in\mathbb{F}_p}\left(\frac{n^2+a}{p}\right) &= \sum_{n\in\mathbb{F}_p}\left(\frac{n^2+1}{p}\right) = \sum_{n\in\mathbb{F}_p}\left(\frac{n^2-k^2}{p}\right)\\ &= \sum_{n\in\mathbb{F}_p}\left(\frac{n-k}{p}\right)\left(\frac{n+k}{p}\right) = \sum_{n\in\mathbb{F}_p}\left(\frac{n}{p}\right)\left(\frac{n+2k}{p}\right)\\ &= \sum_{n\in\mathbb{F}_p}\left(\frac{n(n+2k)}{p}\right) = -\left(\frac{1}{p}\right) = -1\,,\end{aligned}$$

Như vậy với trường này thì bài toán được chứng minh.

(ii) Với $\left(\frac{-1}{p}\right)=-1$, ta chú ý rằng

$$\begin{aligned}\sum_{n\in\mathbb{F}_p}\left(\frac{n^2+a}{p}\right)&=\sum_{n\in\mathbb{F}_p}\left(\frac{n^2+1}{p}\right)=1+2\sum_{\left(\frac{x}{p}\right)=+1}\left(\frac{x+1}{p}\right)\\&=1+2\left(\sum_{x\in\mathbb{F}_p}\left(\frac{x+1}{p}\right)-\left(\frac{1}{p}\right)-\sum_{\left(\frac{x}{p}\right)=-1}\left(\frac{x+1}{p}\right)\right)\\&=1+2\left(0-1-\sum_{\left(\frac{x}{p}\right)=-1}\left(\frac{x+1}{p}\right)\right)\\&=-1+2\sum_{\left(\frac{x}{p}\right)=-1}\left(\frac{-x-1}{p}\right)\\&=-1+2\sum_{\left(\frac{x}{p}\right)=+1}\left(\frac{x-1}{p}\right)=-1+\sum_{n\in\mathbb{F}_p^\times}\left(\frac{n^2-1}{p}\right).\end{aligned}$$

Đến đây tiếp tục sử dụng ***bổ đề*** đã chứng minh ở trên ta có

$$\sum_{n\in\mathbb{F}_p^\times}\left(\frac{n^2-1}{p}\right)=\sum_{n\in\mathbb{F}_p}\left(\frac{n^2-1}{p}\right)+1=\sum_{n\in\mathbb{F}_p}\left(\frac{n(n+2)}{p}\right)+1=-\left(\frac{1}{p}\right)+1=0.$$

Như vậy, từ các trường hợp đã xét, ta có điều phải chứng minh. □

Bài 33

IMO 2016

Một tập hợp các số nguyên dương được gọi ***tập hương*** nếu có ít nhất hai phần tử và mỗi phần tử của nó có ước nguyên tố chung với ít nhất với một trong các phần tử còn lại. Đặt $P(n)=n^2+n+1$. Tìm số nguyên dương b nhỏ nhất sao cho tồn tại số nguyên không âm a để tập hợp $\{P(a+1),...,P(a+b)\}$ là ***tập hương***.

Lời giải

Phân tích. Ta phải xác định

1. Dạng của ước nguyên tố của $P(n)=n^2+n+1$.
2. Ước nguyên tố chung của $P(n)$ và $P(n+m)$, $m\geqslant 1$.

Với ý thứ nhất, $P(n)$ là biểu thức bậc hai, ta có thể sử dụng thặng dư bậc hai để xác định

$$4P(n)=4n^2+4n+4=(2n+1)^2+3$$

Từ đó ta suy ra

$$p|P(n)\Leftrightarrow p|4P(n)\Leftrightarrow(2n+1)^2\equiv -3\,(\mathrm{mod}\,p)\Rightarrow\left(\frac{-3}{p}\right)=1$$

Nếu $p>3$, đặt $p=3k+r, 0<r<3$. Ta có

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

Vì $\left(\frac{-1}{p}\right)=\begin{cases}1 & \text{khi} \quad p\equiv 1\,(\text{mod}4)\\ -1 & \text{khi} \quad p\equiv -1\,(\text{mod}4)\end{cases}$ và $\left(\frac{2}{3}\right)=1$ nên

$$\left[\begin{array}{l}p=4s+1, r=1\\ p=4s+3, r=1\end{array}\right.$$

Suy ra $p=6h+1$ hoặc $p=3$.
Với ý 2, p là ước nguyên tố chung của $P(n)$ và $P(n+m)$, như vậy ta có được

$$\begin{cases}p|P(n)\\ p|P(n+m)-P(n)\end{cases}\Rightarrow\begin{cases}p|n^2+n+1\\ p|m(2n+m+1)\end{cases}\Rightarrow\begin{cases}p|(2n+1)^2+3\\ \left[\begin{array}{l}p|m\\ p|2n+m+1\end{array}\right.\end{cases}$$

Nếu $m=3$ thì $\left[\begin{array}{l}\begin{cases}p|2(n+2)\\ p|n^2+n+1\end{cases}\\ \begin{cases}p=3\\ 3|2n+1\end{cases}\end{array}\right.$. Mặt khác ta lại có

$$n^2+n+1=(n+2)(n-1)+3\Rightarrow\begin{cases}n=3k+1\\ p=3\end{cases}$$

Vậy $(P(x),P(x+3))>1,(P(y),P(y+3))>1$ khi và chỉ khi $3|x-y$.
Nếu $m=1$ thì $\begin{cases}p|2n+2\\ p|n^2+n+1\end{cases}$, mà $n^2+n+1=n(n+1)+1$ nên $p|1$, điều này là vô lý.
Nếu $m=2$ thì $\begin{cases}p|(2n+3)\\ p|4n^2+4n+4\end{cases}$. Mặt khác ta lại có

$$4n^2+4n+4=(2n+3)(2n-1)+7\Rightarrow\begin{cases}n=7k+2\\ p=7\end{cases}$$

Vậy nếu $(P(x),P(x+2))>1,(P(y),P(y+2))>1$ thì $7|x-y$.
Nếu $m=4$, thì $\begin{cases}p|(2n+5)\\ p|4n^2+4n+4\end{cases}$. Mặt khác ta lại có

$$4n^2+4n+4=(2n+5)(2n-3)+19\Rightarrow\begin{cases}n=19k+7\\ p=19\end{cases}$$

Từ nhận xét trên, suy ra các tập $\{P(a+1),P(a+2)\},\{P(a+1),P(a+2),P(a+3)\}$ không là ***tập hương*** với mọi a vì $P(a+2)$ không có ước nguyên tố chúng với 2 phần tử còn lại trong tập.
Vậy tập $\{P(a+1),P(a+2)\},\{P(a+1),P(a+2),P(a+3)\}$ không là ***tập hương***. Giả sử tồn tại a để tập $\{P(a+1),P(a+2),P(a+3),P(a+4)\}$ là ***tập hương***, vậy

$$\begin{cases}(P(a+2),P(a+4))>1\\ (P(a+3),P(a+1))>1\end{cases}\Rightarrow 7|(a+2)-(a+1),$$

điều này là vô lý. Giả sử tồn tại a để tập $\{P(a+1),P(a+2),P(a+3),P(a+4),P(a+5)\}$ là ***tập hương***.

1. Nếu $(P(a+1),P(a+3))>1$ thì $a+1=7k+2$ nên $(P(a+2),P(a+4))>1$, suy ra

$$(P(a+2),P(a+5))>1$$

Do đó $a+2=3q+1$ hay $a=3q-1$. Nhưng lúc này $(P(a+1),P(a+4))=1$ nên $P(a+4)$ không có ước nguyên tố với bất kì phần tử nào còn lại của tập hợp, điều này là mâu thuẫn.

2. Nếu $(P(a+3), P(a+5)) > 1$ thì $a+3 = 7k+2$ nên $(P(a+1), P(a+3)) = 1$, suy ra

$$(P(a+2), P(a+4)) = 1$$

Suy ra hoặc $(P(a+1), P(a+4)) > 1$ hoặc $(P(a+1), P(a+5)) > 1$.
Điều này dẫn đến hoặc $a+1 = 3q+1$ hoặc $a+1 = 19q+7$.
Cả hai điều này ta đều được $(P(a+2), P(a+5)) = 1$ do đó $P(a+2)$ không có ước nguyên tố chung với bất kì phần tử nào còn lại, điều này mâu thuẫn.

Với $b = 6$, trong quá trình xét các trường hợp ở trên, ta có thể dự đoán

$$\begin{cases} (P(a+1), P(a+4)) > 1 \\ (P(a+2), P(a+6)) > 1 \\ (P(a+3), P(a+5)) > 1 \end{cases}$$

Để được điều này, ta cần

$$\begin{cases} a+1 = 3k+1 \\ a+2 = 19q+7 \\ a+3 = 7s+2 \end{cases} \Rightarrow \begin{cases} a \equiv 0 \pmod 3 \\ a \equiv 5 \pmod{19} \\ a \equiv 6 \pmod 7 \end{cases}$$

Theo ***định lý phần dư Trung Hoa*** thì hệ này có nghiệm.
Vậy $b = 6$ là giá trị cần tìm. □

Bài 34

Cho a, b, c là các số nguyên và $p > 3$ là một số nguyên tố lẻ. Chứng minh rằng nếu $f(x) = ax^2 + bx + c$ là số chính phương tại $\dfrac{p+5}{2}$ giá trị nguyên liên tiếp của x thì $p \mid (b^2 - 4ac)$.

Lời giải

Với bài toán này ta sử dụng tới ***định lý 2,3*** của phần **Một vài tổng của kí hiệu Legendre**. Giả sử rằng tồn tại số nguyên x_0 sao cho $f(x_0), f(x_0+1), ..., f\left(x_0 + \dfrac{p+1}{2}\right)$ đều là các số chính phương. Xét các khả năng sau

1. Với $a \vdots p$. Nếu bp thì tập $\left\{bx + c : x = x_0, x_0+1, ..., x_0 + \dfrac{p+3}{2}\right\}$ là một hệ thặng dư không đầy đủ modulo p gồm $\dfrac{p+5}{2}$ phần tử mà $f(x) \equiv bx + c \pmod p$ nên tập

$$\left\{f(x) : x = x_0, x_0+1, ..., x_0 + \frac{p+3}{2}\right\}$$

cũng là một hệ thặng dư không đầy đủ modulo p gồm $\dfrac{p+5}{2}$ phần tử. Nhưng rõ ràng một số chính phương chỉ có thể đồng dư với đúng một số trong $\dfrac{p+1}{2}$ số là $0^2, 1^2, ..., \left(\dfrac{p-1}{2}\right)^2$, mâu thuẫn. Do đó $b \vdots p \Rightarrow p \mid b^2 - 4ac$.

2. Với $a \not\vdots p$. Giả sử rằng $pb^2 - 4ac$. Khi đó theo ***định lý 3*** ta có

$$\sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p}\right) = -\left(\frac{a}{c}\right)$$

$$\Rightarrow \sum_{x=x_0}^{x_0+p-1}\left(\frac{ax^2+bx+c}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=-\left(\frac{a}{p}\right)\leqslant 1$$

Mặt khác dễ dàng thấy rằng không tồn tại 3 số nguyên phân biệt

$$x_1,x_2,x_3\in\{x_0,x_0+1,...,x_0+p-1\}$$

sao cho $ax_i{}^2+bx_i+c\vdots p\forall i=1,2,3$ nên

$$\sum_{x=x_0}^{x_0+p-1}\left(\frac{ax^2+bx+c}{p}\right)\geqslant\left(\frac{p+5}{2}-2\right)-\left(p-\frac{p+5}{2}\right)=3>1$$

Điều này mâu thuẫn. Như vậy bài toán đã hoàn toàn được chứng minh. □

Bài 35

Với mỗi số nguyên a, hãy tính số nghiệm (x,y,z) của phương trình đồng dư

$$x^2+y^2+z^2\equiv 2axyz\,(\mathrm{mod}p)$$

Lời giải

Ta có

$$x^2+y^2+x^2\equiv 2axyz\,(\mathrm{mod}p)\Leftrightarrow(z-axy)^2\equiv\left(a^2x^2-1\right)y^2-x^2\,(\mathrm{mod}p)\qquad(1)$$

Suy ra với mỗi cặp x,y cố định thuộc tập $\{0,1,...,p-1\}$ thì số nghiệm $z\in\{0,1,...,p-1\}$ thỏa mãn điều kiện (1) là

$$1+\left(\frac{\left(a^2x^2-1\right)y^2-x^2}{p}\right)$$

Do vậy số nghiệm của phương trình $x^2+y^2+z^2\equiv 2axyz\,(\mathrm{mod}p)$ là

$$N=p^2+\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{\left(a^2x^2-1\right)y^2-x^2}{p}\right)$$

Xét các khả năng sau.

Khả năng 1. Nếu $a\vdots p$, khi đó sử dụng ***định lý 3*** như bài ở trên thì ta được

$$\begin{aligned}N=p^2+\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{-y^2-x^2}{p}\right)&=p^2+\left(\frac{-1}{p}\right)\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{y^2+x^2}{p}\right)\\&=p^2+\left(\frac{-1}{p}\right)\left(\sum_{y=0}^{p-1}\left(\frac{y^2}{p}\right)+\sum_{x=1}^{p-1}\sum_{y=0}^{p-1}\left(\frac{y^2+x^2}{p}\right)\right)\\&=p^2+\left(\frac{-1}{p}\right)\left((p-1)+\sum_{x=1}^{p-1}\left(-\left(\frac{1}{p}\right)\right)\right)\\&=p^2+\left(\frac{-1}{p}\right)((p-1)+(-p+1))=p^2\end{aligned}$$

Khả năng 2. Nếu $a\not\vdots p$. Dễ thấy tồn tại duy nhất các số nguyên $x_1,x_2\in\{1,2,...,p-1\}$ sao cho

$$\begin{cases}ax_1\equiv 1\,(\mathrm{mod}p)\\ax_2\equiv -1\,(\mathrm{mod}p)\end{cases}\Rightarrow p|a^2x_1{}^2-1,p|a^2x_2{}^2+1$$

Do vậy $p \not| x^2\left(a^2x^2-1\right), \forall x \in \{0,1,...,p-1\} \setminus \{0,x_1,x_2\}$. Chú ý rằng $\left(\frac{\alpha}{p}\right)=0$ nếu $\alpha \vdots p$, ta được

$$\begin{aligned}
N &= p^2+\sum_{y=0}^{p-1}\left(\frac{-y^2}{p}\right)+\sum_{y-0}^{p-1}\left(\frac{\left(a^2{x_1}^2-1\right)y^2-{x_1}^2}{p}\right)+\sum_{y-0}^{p-1}\left(\frac{\left(a^2{x_2}^2-1\right)y^2-{x_2}^2}{p}\right)\\
&+\sum_{\substack{x=1\\x\neq x_1,x_2}}^{p-1}\sum_{y-0}^{p-1}\left(\frac{\left(a^2x^2-1\right)y^2-x^2}{p}\right)\\
&=p^2+(p-1)\left(\frac{-1}{p}\right)+2p\left(\frac{-1}{p}\right)+\sum_{\substack{x=1\\x\neq x_1,x_2}}^{p-1}-\left(\frac{a^2x^2-1}{p}\right)\\
&=p^2+p\left(\frac{-1}{p}\right)+2p\left(\frac{-1}{p}\right)-\sum_{x=0}^{p-1}\left(\frac{a^2x^2-1}{p}\right)=p^2+3p\left(\frac{-1}{p}\right)+\left(\frac{a^2}{p}\right)\\
&=p^2+3p\left(\frac{-1}{p}\right)+1
\end{aligned}$$

Vậy $N=\begin{cases} p^2 & \text{khi} \quad a \vdots p \\ p^2+3p\left(\frac{-1}{p}\right)+1 & \text{khi} \quad a \not\vdots p \end{cases}$

Bài 36

Xét đa thức $P(x)=x^3+14x^2-2x+1$. Chứng minh rằng tồn tại số tự nhiên n sao cho với mọi $x \in \mathbb{Z}$, ta có $101 | \underbrace{P(P(...P}_{n}(x)...)-x$.

Lời giải

Xét hai số nguyên x,y bất kỳ. Ta sẽ chứng minh rằng

$$x \equiv y \,(\text{mod}101) \Leftrightarrow P(x) \equiv P(y)\,(\text{mod}101) \tag{1}$$

Do $P(x)=x^3+14x^2-2x+1$ nên ta có

$$\begin{aligned}
4\left(P(x)-P(y)\right) &= 4(x-y)\left(x^2+xy+y^2+14x+14y-2\right)\\
&=(x-y)\left((2x+y+14)^2+3(y-29)^2\right)\\
&\Rightarrow P(x) \equiv P(y)\,(\text{mod}101)\\
&\Leftrightarrow \left[\begin{array}{l} x \equiv y\,(\text{mod}101)\\ (2x+y+14)^2+3(y-129) \equiv 0\,(\text{mod}101)\end{array}\right.
\end{aligned} \tag{2}$$

Xét (2), ta có

(i) Nếu $\gcd(y-29,101)=1$ thì $\left(\frac{-3}{101}\right)=1 \Rightarrow 101 \equiv 1\,(\text{mod}6)$. Vô lý.

(ii) Nếu $101|(y-29) \Rightarrow 101|(2x+y+14) \Rightarrow x \equiv y \equiv 29\,(\text{mod}101)$.

Do đó ta luôn có $x \equiv y\,(\text{mod}101)$, (1) được chứng minh. Xét 102 số

$$P(x), P(P(x)), P(P(P(x))), ..., \underbrace{P(P(...P}_{102}(x)...)$$

Theo ***Định lí Dirichlet***, tồn tại $m, n \in \{1, 2, ..., 102\}, m > n$ sao cho

$$\underbrace{P(P(...P}_{m}(x)...) \equiv \underbrace{P(P(...P}_{n}(x)...) \,(\mathrm{mod}101)$$

Từ nhận xét trên ta suy ra $\underbrace{P(P(...P}_{m-n}(x)...) \equiv x \,(\mathrm{mod}101)\, \forall x \in \mathbb{Z}$. Bài toán được chứng minh. □

Bài 37

Cho p là một số nguyên tố lẻ và đặt $f(x) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^{x^{i-1}}$.

(i) Chứng minh rằng $f(x)$ chia hết cho $(x-1)$ nhưng không chia hết cho $(x-1)^2$ nếu và chỉ nếu $p \equiv 3(\mathrm{mod}4)$.

(ii) Chứng minh rằng nếu $p \equiv 5(\mathrm{mod}8)$ thì $f(x)$ chia hết cho $(x-1)^2$ nhưng không chia hết cho $(x-1)^3$.

Lời giải

(i) Từ giả thiết ta có $f(1) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right) = 0$. Ta có nhận xét đã được chứng minh sau.

Nhận xét. Với p là một số nguyên tố lẻ thì trong tập $S = \{1, 2, \ldots, p-1\}$, có $\frac{p-1}{2}$ số chính phương modulo p và $\frac{p-1}{2}$ số không chính phương modulo p.

Áp dụng nhận xét này ta suy ra được $f(x)$ chia hết cho $(x-1)$. Ta có

$$\begin{aligned} f'(1) &= \sum_{i=1}^{p-1}(i-1)\left(\frac{i}{p}\right) = \sum_{i=1}^{p-1} i\left(\frac{i}{p}\right) - f(1) = \sum_{i=1}^{p-1} i\left(\frac{i}{p}\right) \\ &= \sum_{i=1}^{p-1}(p-i)\left(\frac{p-i}{p}\right) = \sum_{i=1}^{p-1}(p-i)\left(\frac{-i}{p}\right) = (-1)^{\frac{p-1}{2}}\sum_{i=1}^{p-1}(p-i)\left(\frac{i}{p}\right) \\ &= (-1)^{\frac{p-1}{2}}\left(pf(1) - \sum_{i=1}^{p-1} i\left(\frac{i}{p}\right)\right) = (-1)^{\frac{p+1}{2}} f'(1) \end{aligned}$$

Nếu $p \equiv 1(\mathrm{mod}4)$ thì theo trên ta có $f'(1) = -f'(1) \Rightarrow f'(1) = 0$.
Mà $f(1) = 0$ nên $f(x)$ chia hết cho $(x-1)^2$.
Nếu $p \equiv 3(\mathrm{mod}4)$, với chú ý $\left(\frac{i}{p}\right) \equiv 1(\mathrm{mod}2), \forall i = 1, 2, \ldots, p-1$ ta có

$$f'(1) = \sum_{i=1}^{p-1} i\left(\frac{i}{p}\right) \equiv \sum_{i=1}^{p-1} i = \frac{p(p-1)}{2} \equiv 1(\mathrm{mod}2) \Rightarrow f'(1) \neq 0$$

Mà $f(1) = 0$ nên $f(x) \vdots (x-1)$ nhưng $f(x) \not\vdots (x-1)^2$. Do đó $f(x)$ chia hết cho $(x-1)$ nhưng không chia hết cho $(x-1)^2$ nếu và chỉ nếu $p \equiv 3(\mathrm{mod}4)$.
(ii) Ta nhận thấy rằng

$$\begin{aligned} f''(1) &= \sum_{i=1}^{p-1}(i-1)(i-2)\left(\frac{i}{p}\right) = \sum_{i=1}^{p-1}\left(i^2 - 3i + 2\right)\left(\frac{i}{p}\right) \\ &= \sum_{i=1}^{p-1} i^2\left(\frac{i}{p}\right) - 3\sum_{i=1}^{p-1} i\left(\frac{i}{p}\right) + 2f(1) = \sum_{i=1}^{p-1} i^2\left(\frac{i}{p}\right) - 3\sum_{i=1}^{p-1} i\left(\frac{i}{p}\right) \end{aligned}$$

Ta giả sử rằng $p \equiv 5(\text{mod}8)$, khi đó theo câu (i) ta có $f(x) \vdots (x-1)^2$ và $\sum_{i=1}^{p-1} i\left(\frac{i}{p}\right) = f'(1) = 0$, từ đây ta suy ra được

$$f''(1) = \sum_{i=1}^{p-1} i^2\left(\frac{i}{p}\right) = \sum_{i=1}^{\frac{p-1}{2}} (2i)^2\left(\frac{2i}{p}\right) + \sum_{i=1}^{\frac{p-1}{2}} (2i-1)^2\left(\frac{2i-1}{p}\right)$$

Mặt khác do $p \equiv 5(\text{mod}8)$ nên $\left(\frac{2}{p}\right) = -1, \left(\frac{-1}{p}\right) = 1$, khi đó ta có

$$\sum_{i=1}^{\frac{p-1}{2}} (2i)^2\left(\frac{2i}{p}\right) = 4\left(\frac{2}{p}\right)\sum_{i=1}^{\frac{p-1}{2}} i^2\left(\frac{i}{p}\right) \equiv -4\sum_{i=1}^{\frac{p-1}{2}} i^2 \equiv -4\sum_{i=1}^{\frac{p-1}{2}} i = -4\frac{p^2-1}{8} \equiv -4(\text{mod}8)$$

và đồng thời

$$\sum_{i=1}^{\frac{p-1}{2}} (2i-1)^2\left(\frac{2i-1}{p}\right) \equiv \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{2i-1}{p}\right)(\text{mod}8)$$

Mặt khác lại do $f(1) = 0$ nên ta có

$$\begin{aligned} -\sum_{i=1}^{\frac{p-1}{2}} \left(\frac{2i-1}{p}\right) &= \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{2i}{p}\right) = \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{2i}{p}\right) = \left(\frac{p-1}{p}\right) + \sum_{i=1}^{\frac{p-3}{2}} \left(\frac{2i}{p}\right) \\ &= 1 + \sum_{i=1}^{\frac{p-3}{2}} \left(\frac{2\left(\frac{p-1}{2} - i\right)}{p}\right) = 1 + \sum_{i=1}^{\frac{p-1}{3}} \left(\frac{p-2i-1}{p}\right) \\ &= 1 + \sum_{i=1}^{\frac{p-1}{3}} \left(\frac{2i+1}{p}\right) = \sum_{i=1}^{\frac{p-1}{2}} \left(\frac{2i-1}{p}\right) \end{aligned}$$

Từ đây ta suy ra được

$$\sum_{i=1}^{\frac{p-1}{2}} \left(\frac{2i-1}{p}\right) = 0 \Rightarrow \sum_{i=1}^{p-1} (2i-1)^2\left(\frac{2i-1}{p}\right) \equiv \sum_{i=1}^{p-1} \left(\frac{2i-1}{p}\right) = 0(\text{mod}8)$$

Do vậy ta có

$$f''(1) \equiv -4(\text{mod}8) \Rightarrow f''(1) \neq 0 \Rightarrow f(x) \not\vdots (x-1)^3$$

Vậy nếu $p \equiv 5(\text{mod}8)$ thì $f(x)$ chia hết cho $(x-1)^2$ nhưng không chia hết cho $(x-1)^3$.
Bài toán được giải quyết. □

Bài 38

Cho $k = 2^{2^n} + 1$ với n nguyên dương. Chứng minh rằng k là một số nguyên tố (số nguyên tố Fermat, lưu ý $2^{2^5} + 1 \vdots 641$) 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 $3^{\frac{k-1}{2}} \equiv -1\,(\text{mod}k)$. Do đó $3^{k-1} \equiv 1\,(\text{mod}k)$. Mà cấp của 3 modulo k chính là $k-1$. Từ đó suy ra $k-1 | \varphi(k)$ với $\varphi(k)$ là ***phi hàm Euler*** của k.
Nếu k không là số nguyên tố, thì nhận thấy ngay $\varphi(k) > k-1$. Do đó k là một số nguyên tố. Đảo lại, cho k là một số nguyên tố, theo luật thuận nghịch và giả thiết $k = 2^{2^n} + 1$, ta có

$$\left(\frac{3}{k}\right) = \left(\frac{k}{3}\right) = \left(\frac{2}{3}\right) = -1$$

Do đó

$$3^{\frac{k-1}{2}} \equiv \left(\frac{3}{k}\right) \equiv -1 \,(\mathrm{mod} k)$$

Như vậy bài toán được chứng minh. □

Bài 39

Tìm mọi cặp số nguyên (a, b) sao cho với mọi số nguyên dương n, ta có $n|a^n + b^{n+1}$.

Lời giải

Cho $n = p$ với p là số nguyên tố lẻ đủ lớn, ta có

$$a^p + b^{p+1} \equiv a + b^2 \equiv 0 \,(\mathrm{mod} p) \Rightarrow \left(\frac{-a}{p}\right) = 1, \forall p \geqslant p_0$$

Với p_0 là số nguyên tố lẻ đủ lớn thỏa mãn $\gcd(a, p_0) = 1$. Mà theo bổ đề quen thuộc là nếu x không là số chính phương thì tồn tại vô số số nguyên tố p sao cho $\left(\frac{x}{p}\right) = -1$, do đó ta phải có $-a$ là một số chính phương. Tương tự, chọn $n = 2p$ với p là số nguyên tố lẻ đủ lớn thì ta có

$$\left(\frac{-b^{2p+1}}{p}\right) = 1, \forall p \geqslant p_0 \Rightarrow \left(\frac{-b}{p}\right) = 1, \forall p \geqslant p_0$$

Từ đây suy ra $-b$ là một số chính phương.
Tiếp tục chọn $n = p$ với p là số nguyên tố lẻ, đặt $-a = k^2, -b = l^2$, theo ***định lý Fermat nhỏ*** ta có

$$\left(-k^2\right)^p + \left(-l^2\right)^{p+1} \vdots p \Leftrightarrow l^4 - k^2 \equiv 0 \,(\mathrm{mod} p)$$

Do đó ta lại có $l^2 \pm k \equiv 0 \,(\mathrm{mod} p)$ với vô số số nguyên tố p, vì vậy ta lại tiếp tục suy ra $(\pm k)^2$ là một lũy thừa bậc 4. Tương tự chọn $n = 2p$ với p là số nguyên tố lẻ, ta lại có $(\pm k)^2$ là một lũy thừa bậc 4. Lặp lại quá trình này vô hạn lần, ta có $-a, -b$ là lũy thừa bậc 2^t tùy ý. Do đó

$$\left[\begin{array}{l} -a = -b = 1 \\ -a = -b = 0 \end{array}\right.$$

Vậy $(a, b) \in \{(0, 0), (-1, -1)\}$. □

Bài 40

Korean National Olympiad 2nd Round 2019
Giả sử rằng các số nguyên dương m, n, k thỏa mãn các phương trình $m^2+1 = 2n^2, 2m^2+1 = 11k^2$. Tìm phần dư khi chia n cho 17.

Lời giải

Dễ thấy $(k, m, n) = (3, 7, 5)$ là một nghiệm của bài toán. Ta gọi hai dãy $\{m_i\}_{i=1}^{\infty}$ và $\{n_i\}_{i=1}^{\infty}$ được xác định như sau

$$m_1 = n_1 = 1, m_{i+1} = 3m_i + 4n_i, n_{i+1} = 2m_i + 3n_i (i \geqslant 1)$$

Bằng bổ đề nổi tiếng của ***phương trình Pell***, ta biết rằng $(m, n) = (m_j, n_j)$ với $j \geqslant 1$.
Dễ thấy $n^2 \equiv 3 (\mathrm{mod} 11) \Rightarrow n \equiv \pm 5 (\mathrm{mod} 11)$. Ta sẽ kiểm tra số dư của (m_i, n_i) mod11.

$$(1, 1) \to (7, 5) \to (8, 7) \to (8, 4) \to (7, 6) \to (1, -1) \to (-1, -1)$$

$$\to (-7, -5) \to (-8, -7) \to (-8, -4) \to (-7, 5) \to (-1, 1) \to (1, 1) \to \ldots$$

Điều này có nghĩa là $j \equiv 2 \pmod 3$. Ta tiếp tục kiểm tra số dư của (m_i, n_i) cho 17.

$$(1,1) \to (7,5) \to (7,12) \to (1,-1) \to (-1,-1) \to (-7,12) \to (-7,5) \to (-1,1-) \to (1,1) \to ...$$

Để ý rằng $(2n-1)(2n+1) = 4n^2 - 1 = 11k^2$, khi đó ta có $\begin{cases} 2n-1 = 11u^2 \\ 2n+1 = v^2 \end{cases}$ hoặc $\begin{cases} 2n+1 = 11u^2 \\ 2n-1 = v^2 \end{cases}$.

(i) Trường hợp $\begin{cases} 2n-1 = 11u^2 \\ 2n+1 = v^2 \end{cases}$ $\Rightarrow 11u^2 + 2 = v^2$. Mâu thuẫn vì $\left(\dfrac{2}{11}\right) = -1$.

(ii) Trường hợp $\begin{cases} 2n+1 = 11u^2 \\ 2n-1 = v^2 \end{cases}$, suy ra $n \equiv 5 \pmod{11} \Rightarrow j \equiv 2, 11 \pmod{12}$ hoặc $j \equiv 2, 3 \pmod 4$
$\Rightarrow n \equiv \pm 5 \pmod{17}$

Nếu $n \equiv -5 \pmod{17} \Rightarrow v^2 = 2n - 1 \equiv 6 \pmod{17}$. Điều này là vô lý vì $\left(\dfrac{6}{17}\right) = -1$.

Vậy $n \equiv 5 \pmod{17}$. □

3 Bài tập tự luyện.

Bài 1. Cho 3 số nguyên a, b, c, chứng minh rằng a, b, c, abc không là số chính phương khi và chỉ khi tồn tại vô số số nguyên tố p sao cho

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = \left(\frac{c}{p}\right)$$

Bài 2. Chứng minh rằng tồn tại số nguyên dương n sao cho với mọi số nguyên dương k thì $k^2 + k + n$ không có ước nguyên tố nhỏ hơn 2008.

Bài 3. Cho p là số nguyên tố lớn hơn 3 và có dạng $3k + 1$. Chứng minh rằng ta luôn có

$$\prod_{i=1}^{p} \left(i^2 + i + 1\right) \equiv 0 (\mathrm{mod} p)$$

Bài 4. Cho đa thức $P(x) = \left(x^2 - 2\right)\left(x^2 - 3\right)\left(x^2 - 6\right)$. Chứng minh rằng với mọi số nguyên tố p luôn tìm được số nguyên dương n sao cho $P(n)$ chia hết cho p.

Bài 5. Gọi F_n là số ***Fibonacci*** thứ n, chứng minh rằng với $p > 5$ là số nguyên tố thì $p \mid \left(F_p - \left(\frac{p}{5}\right)\right)$, trong đó $\left(\frac{p}{5}\right)$ là ***kí hiệu Legendre***.

Bài 6. Với p và q là 2 số nguyên tố phân biệt, chứng minh rằng

$$\sum_{x_1 + x_2 + \cdots + x_q \equiv q \ (\mathrm{mod}\ p), 1 \leqslant x_i \leqslant p-1} \left(\frac{x_1 \cdot x_2 \cdots x_q}{p}\right) \equiv 1 \, (\mathrm{mod} q) \, .$$

Bài 7. Với p là số nguyên tố lẻ và h nguyên dương thỏa mãn $1 \leqslant h \leqslant p$, chứng minh rằng

$$\sum_{n=1}^{p} \left(\sum_{m=1}^{h} \left(\frac{m+n}{p}\right)\right)^2 = h(p-h)$$

Bài 8. Với p là số nguyên tố, chứng minh rằng

$$\sum_{i=1}^{p-1} \left(\frac{i^3 + 6i^2 + i}{p}\right)$$

Bài 9. Với mọi số nguyên x, chứng minh rằng

$$\left(\frac{-4}{16x^2 + 12x + 3}\right) = \left(\frac{-1}{16x^2 + 12x + 3}\right)$$

Bài 10. Cho p là số nguyên tố thỏa mãn $p \equiv 3 (\mathrm{mod} 4)$. Chứng minh rằng

$$\sum_{k=1}^{p-1} k^2 \left(\frac{k}{p}\right) = p \sum_{k=1}^{p-1} k \left(\frac{k}{p}\right)$$

Bài 11. Cho k là số tự nhiên khác 0. Chứng minh rằng

$$1 + \sum_{x=0}^{p-1} \left(\frac{x^4 + k}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x(x^2 + k)}{p}\right)$$

Bài 12. Cho cặp số nguyên dương (m, n) thỏa $\phi\left(5^m - 1\right) = 5^n - 1$, chứng minh rằng $\gcd(m, n) > 1$.

Bài 13. Với p là số nguyên tố có dạng $4k + 1$. Giả sử r là một thặng dư bậc 2 của p và s là không thặng dư của p. Chứng minh rằng $p = a^2 + b^2$, trong đó

$$a = \frac{1}{2} \sum_{i=1}^{p-1} \left(\frac{i(i^2 - r)}{p}\right), b = \frac{1}{2} \sum_{i=1}^{p-1} \left(\frac{i(i^2 - s)}{p}\right).$$

và $\left(\frac{k}{p}\right)$ là ***kí hiệu Legendre***.

Bài 14. Với p là một số nguyên tố có dạng $4k+1$ và $\frac{m}{n}$ là phân số tối giản thỏa mãn

$$\sum_{a=2}^{p-2} \frac{1}{a^{\frac{p-1}{2}} + a^{\frac{p+1}{2}}} = \frac{m}{n}.$$

Chứng minh rằng $p|m+n$.

Bài 15. Chứng minh rằng với mọi số nguyên tố p thì tồn tại ít nhất $\frac{p+1}{2}$ số nguyên dương d thỏa mãn $0 \leqslant d < p$ sao cho phương trình đồng dư $x^3 + x \equiv d \pmod{p}$ có ít nhất 1 nghiệm modulo p.

Tài liệu

[1] Cấp của số nguyên, căn nguyên thủy và ứng dụng - Phạm Xuân Thịnh, THPT Chuyên Hạ Long, Quảng Ninh.

[2] Đa thức chia đường tròn - Luận văn thạc sỹ toán học, Nguyễn Thị Thùy Linh, Đại học Thái Nguyên.

[3] Vận dụng phương pháp LTE vào giải các bài toán số học, Phạm Quang Toàn.

[4] Problems and solutions from winter schools of mathematics in Vietnam - Blog Toán học cho mọi người.

[5] Đa thức chia đường tròn - ứng dụng vào các bài toán số học - Nguyễn Đình Minh, THPT Chuyên Lê Quý Đôn, Khánh Hòa.

[6] Cấp của số nguyên, căn nguyên thủy và ứng dụng - Phạm Xuân Thịnh, THPT Chuyên Hạ Long, Quảng Ninh.

[7] Cấp và căn nguyên thủy, Lê Xuân Đại, THPT Chuyên Vĩnh Phúc, tỉnh Vĩnh Phúc.

[8] Hà Duy Hưng, Một số phương pháp giải toán số học sơ cấp.

[9] Nguyễn Duy Liên: Chuyên đề: Cấp số nguyên, căn nguyên thủy và ứng dụng.

[10] Tạp chí Pi, Tạp chí Toán học tuổi trẻ.

[11] Một số tính chất và ứng dụng của hàm định giá p-adic, Dương Thái Bảo - THPT Chuyên Nguyễn Quang Diêu, Đồng Tháp.

[12] Các phương pháp giải toán qua các kì thi Olympic năm 2013, Trần Nam Dũng - Võ Quốc Bá Cẩn - Lê Phúc Lữ, NXB Đại học Quốc gia TP.HCM.

[13] Ứng dụng hàm định giá để giải một số bài toán số học, Trần Thanh Nhã, THPT Chuyên Lê Quý Đôn - Bình Định.

[14] Thặng dư bình phương, số giả nguyên tố Euler và ứng dụng, Trần Quang Huy, Đại học Thái Nguyên.

[15] Thặng dư bình phương, Nguyễn Văn Sơn - THPT Chuyên Phan Bội Châu, Nghệ An.

[16] Kí hiệu Legendre, các số nguyên đại số và ứng dụng vào phương trình Diophantine, Đào Phương Bắc, ĐHQG Hà Nội.

[17] Nguyễn Văn Mậu (Chủ biên), Trần Nam Dũng, Đặng Hùng Thắng, Đặng Huy Ruận: Một số vấn đề Số học chọn lọc. Nhà Xuất bản Giáo dục, 2008.

[18] Phan Huy Khải - Các bài toán về hàm số học - NXB Giáo dục, tháng 3 năm 2009.

[19] Nguyễn Vũ Lương - Nguyễn Lưu Sơn - Nguyễn Ngọc Thắng - Phạm Văn Hùng - Các bài giảng về số học - NXB Đại học Quốc Gia Hà Nội, Quý 4 năm 2006.

[20] Đặng Hùng Thắng - Nguyễn Văn Ngọc - Vũ Kim Thủy - Bài giảng số học - Xí nghiệp in đường sắt Hà Nội, tháng 05/1997.

[21] Các hàm số học, Luận văn thạc sỹ toán học - Đỗ Cao Sơn, Đại học Thái Nguyên.

[22] Đột Phá Đỉnh Cao Bồi Dưỡng Học Sinh Giỏi Chuyên Đề Số Học - Văn Phú Quốc - Nhà xuất bản Đại Học Quốc Gia Hà Nội.

[23] Một số bài toán số học và dãy số - Lê Văn Tài - Đại học KHTN - Đại học Quốc Gia Hà Nội.

[24] Chuyên khảo dãy số - Nguyễn Tài Chung - Nhà xuất bản Đại học Quốc Gia Hà Nội.

[25] Blog Cao Đình Huy - https://julielltv.wordpress.com/category/day-so-so-hoc/.

[26] Hàm phần nguyên và ứng dụng, Nguyễn Thị Hồng Hạnh, Đại học Thái Nguyên.

[27] Tính chất số học trong các bài toán về đa thức - Phạm Viết Huy - THPT Chuyên Lê Khiết - Quảng Ngãi.

[28] Chuyên đề đa thức và số học - Nguyễn Thành Nhân - Chuyên Hùng Vương - Bình Dương.

[29] Tài liệu ôn đội tuyển VMO 2015 - Thầy Trần Minh Hiền - Chuyên Quang Trung - Bình Phước.

[30] Tuyển chọn các bài toán trong kì thi chọn đội tuyển của các tỉnh, thành phố năm học 2016 - 2017 - Toán học cho mọi người.

[31] Định hướng bồi dưỡng học sinh năng khiếu toán - Nhà xuất bản Giáo dục Việt Nam.

[32] Nguyễn Văn Mậu (1997), "Phương trình hàm", NXB Giáo dục.

[33] Nguyễn Trọng Tuấn (2004), "Bài toán hàm số qua các kì thi Olympic", NXB Giáo dục.

[34] Nguyễn Tài Chung, Lê Hoành Phò (2013), "Chuyên khảo phương trình hàm" Nhà xuất bản Đại học quốc gia Hà Nội.

[35] Trần Nam Dũng, Dương Bửu Lộc - Chuyên đề Phương trình hàm trên tập số nguyên.

[36] Các bài toán về hệ số nhị thức, Nguyễn Nguyễn, Chuyên đề toán học số 11 - Trường Phổ Thông Năng Khiếu, TP.HCM.

[37] Số học của hệ số nhị thức, Nguyễn Chu Gia Vượng, Viện Toán học.

[38] Đẳng thức tổ hợp, Diễn đàn toán học Việt Nam - VMF.

[39] Định lý lớn Fermat, Blog Toán học cho mọi người - https://blogm4e.wordpress.com/2017/02/06/dinh-ly-lon-fermat/.

[40] Chuyên đề bồi dưỡng học sinh giỏi đa thức, Nguyễn Tài Chung, NXB Đại học Quốc Gia Hà Nội.

[41] On the converse of Wolstenholme's Theorem, Richard J. McIntosh (Regina, Sask.).

[42] H. W. Brinkmann, Problem E.435, Amer. Math. Monthly 48 (1941), 269–271.

[43] Mestrovic R. On the mod p^7 determination of $\binom{2p-1}{p-1}$ - https://arxiv.org/pdf/1108.1174v1.pdf

[44] J. Wolstenholme, On certain properties of prime numbers, Quart. J. Pure Appl. Math. 5 (1862), 35–39.

[45] On binomial coefficients modulo squares of primes, Darij Grinberg, January 10, 2019

[46] Darij Grinberg, The Lucas and Babbage congruences, 10 January 2019. http://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf

[47] Darij Grinberg, Notes on the combinatorial fundamentals of algebra, 10 January 2019. https://github.com/darijgr/detnotes/releases/tag/2019-01-10

[48] R.J. McIntosh, On the converse of Wolstenholme's Theorem, Acta Arith. 71 (1995), 381–389.

[49] The Lucas and Babbage congruences, Darij Grinberg, January 10, 2019.

[50] Richard Stanley, Enumerative Combinatorics, volume 1, Second edition, version of 15 July 2011. Available at `http://math.mit.edu/~rstan/ec/`

[51] Olympiad Number Theory Through Challenging Problems, Justin Stevens

[52] Mathematical Excalibur, Vol.18, No.3, Nov.13.

[53] Some identities involving the partial sum of q-binomial coefficients, Bing He, Department of Mathematics, Shanghai Key Laboratory of PMMP East China Normal University

[54] Number Theory Structures, Examples, and Problems - Titu Andreescu , Dorin Andrica

[55] On Wolstenholme's Theorem and its converse, Charles Helou - Guy Terjanian, Journal of Number Theory 128(2008) 475-499

[56] Congruences identifying the primes, Crux Mathematicorum 20 (1994), 33–35.

[57] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers. 6th Edition. Edited by A. Wiles, R. Heath-Brown, J. Silverman. Oxford University Press 2008.

[58] K. Ireland, M. Rosen, A classical introduction to modern number theory. Second edition. Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990. xiv+389 pp.

[59] Titu Andreescu, Zuming Feng, A Path to Combinatorics for Undergraduates Counting Strategies, Birkhauser 2004, 43 – 68.

[60] Analogues Of The Binomial Coefficient Theorems Of Gauss And Jacobi, Abdullah Al-Shaghay, Dalhousie University Halifax, Nova Scotia March 2014.

[61] `http://www-users.math.umn.edu/~garrett/m/algebra/notes/08.pdf`

[62] `http://faculty.bard.edu/~belk/math318/CyclotomicPolynomials.pdf`

[63] `https://www.whitman.edu/Documents/Academics/Mathematics/2015/Final`

[64] Andreescu, T.; Feng, Z., 101 Problems in Algebra from the Training of the USA IMO Team, Australian Mathematics Trust, 2001.

[65] Andreescu, T, Number theory Structures Examples and Problems.

[66] Andreescu, T.; Andrica, D.; Feng, Z., 104 Number Theory Problems From the Training of the USA IMO Team, 2006.

[67] N. Koblizt, p-adic numbers, p-adic Analysis, And Zeta-functions, second edition, Springer - Verlag, 1984.

[68] Dusan Djukic, Quadratic Congruences - Olympiad Training Materials.

[69] J. Stevens, Olympiad Number Theory Through Challenging Problems, Third edition.

[70] On Certain Sums with Quadratic Expressions Involving the Legendre Symbol, Ram Krishna Pandey, Department of Mathematics, Journal of Integer Sequences, Vol. 21 (2018),

[71] A primality test for Fermat numbers faster than Pépin test? - Tony Reix.

[72] A comprehensive course in number theory - Alan Baker - Cambridge University Press (2012).

[73] Problem - Solving and Selected Topics in Number Theory - In the Spirit of the Mathematical Olympiads - Michael Th. Rassias-Springer - Verlag New York (2011).

[74] Number Theory A Historical Approach - John J.Watkins.

[75] Number theory and polynomials (London Mathematical Society Lecture Note Series) - James McKee, Chris Smyth - CUP (2008).

[76] An Introduction to Theory of Functional Equations - Marek Kuczma, Attila Gilányi and Inequalities.

[77] The IMO Compendium. A Collection of Problems Suggested for The International Mathematical Olympiads: 1959 - 2009 - Djukic D., Vladimir Jankovic, Ivan Matic, Nikola Petrovic - Springer (2011).

[78] Problem - Solving and Selected Topics in Number Theory - Michael Th. Rassias.

[79] 104 Number Theory Problems: From the Training of the USA IMO Team - Titu Andreescu, Dorin Andrica, Zuming Feng.

[80] A Computational Introduction To Number Theory And Algebra - Victor Shoups.

[81] J.Aczél (1966), "Lectures on functional equations and their applications", ACADEMIC PRESS New York San Francisco London.

[82] Stevo Stevic (2004), "Periodic Character of a Class of Difference Equation", Taylor and Francis Group.

[83] Valentine Boju, Luis Funar - The Math Problems Notebook.

[84] Titu Andreescu, Razvan Gelca – Birkhauser Mathematical Olympiad Challenges and Inequalities.

[85] Edward Lozansky , Cecil Rousseau – Winning Solutions.

[86] (Developments in Mathematics 39) Saïd Abbas, Mouffak Benchohra – Advanced.

[87] Functional Evolution Equations and Inclusions-Springer International Publishing (2015).

[88] Aczel – Lectures on functional equations and their applications – Academic Press (1966).

[89] Analytic Solutions of Functional Equations – Sui Sun Cheng, Wenrong Li.

[90] Functional Analysis, Sobolev Spaces and Partial Differential Equations – Haim Brezis.

[91] Topics in Algebra and Analysis Preparing for the Mathematical Olympiad –Radmila.

[92] Bulajich Manfrino, José Antonio Gómez Ortega, Rogelio Valdez Delgado-Birkhäuser Basel (2015)..

[93] 101 Problems in Algebra from the training of the USA IMO team – T Andreescu, Z Feng.

[94] Diễn đàn AoPS Online `https://artofproblemsolving.com/community`.

[95] Diễn đàn toán học Việt Nam - VMF, `https://diendantoanhoc.net/`.