Thặng dư bình phương

Nguyễn Văn Sơn A1K40
Trường THPT chuyên Phan Bội Châu Nghệ An

Chuyên đề này viết về một khái niệm khá thú vị của số học, đó là Thặng dư bình phương. Chuyên đề trình bày một số khái niệm cơ bản, các ví dụ minh họa cùng các ứng dụng của lý thuyết Thặng dư bình phương.
Các bài tập được chuẩn bị tương đối kỹ lưỡng và hạn chế trình bày lại các tính chất, các định lý cùng các bổ đề cơ bản. Vì thế đối tượng đọc cần có và nằm vững được những kiến thức nhất định về lý thuyết này. Bên cạnh đó cũng phải có các kiến thức về bậc, căn nguyên thủy, số mũ đúng, phương trình đồng dư, hệ thặng dư, định lý phần dư Trung Hoa.

I. Một số tính chất cần biết.

1) Định nghĩa 1: Cho số nguyên dương n, số nguyên a được gọi thặng dư bình phương $\bmod n$ (hay số chính phương $\bmod n$) nếu tồn tại số nguyên x sao cho: $x^2 \equiv a \pmod{n}$.

2) Định nghĩa 2: Giả sử p là một số nguyên tố lẻ, a là một số nguyên. Kí hiệu Legendre $\left(\frac{a}{p}\right)$ được xác định như sau:

$$\left(\frac{a}{p}\right)=\begin{cases}1 \text{ nếu } (a,p)=1 \text{ và } a \text{ là số chính phương } \bmod p\\ -1 \text{ nếu } (a,p)=1 \text{ và } a \text{ không là số chính phương } \bmod p\\ 0 \text{ nếu } a \vdots p\end{cases}$$

3) Định lý 1 (tiêu chuẩn Euler): Cho p là một số nguyên tố và a là một số nguyên. Khi đó ta có: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Chứng minh: Gọi g là một căn nguyên thủy modulo p. Khi đó tập $\{1,g,g^2,...,g^{p-2}\}$ là hệ thặng dư thu gọn modulo p. Do đó ta chỉ cần chứng minh cho $a \in \{1,g,g^2,...,g^{p-2}\}$.

Giả sử $a = g^i, i \in \{0,1,2,...,p-2\}$. Ta cần chứng minh rằng: $a^{\frac{p-1}{2}} = 1 \Leftrightarrow \left(\frac{a}{p}\right) = 1$.

Thật vậy, giả sử :

$a^{\frac{p-1}{2}} = \left(g^i\right)^{\frac{p-1}{2}} \equiv 1 \left(\mathrm{mod}\, p\right) \Rightarrow i.\frac{p-1}{2} \equiv 0 \left(\mathrm{mod}\, p-1\right) \Rightarrow i \equiv 0 \left(\mathrm{mod}\, 2\right)$

Suy ra tồn tại $j \in \mathbb{N}^* : i = 2j \Rightarrow a = \left(g^j\right)^2 \Rightarrow \left(\frac{a}{p}\right) = 1$

Ngược lại, nếu $\left(\frac{a}{p}\right) = 1$ thì tồn tại $j \in \{0,1,...,p-2\}$ sao cho

$a \equiv \left(g^j\right)^2 \left(\mathrm{mod}\, p\right) \Rightarrow g^i \equiv \left(g^j\right)^2 \left(\mathrm{mod}\, p\right) \Rightarrow i \equiv 2j \left(\mathrm{mod}\, p-1\right) \Rightarrow i \equiv 0 \left(\mathrm{mod}\, 2\right)$ Do đó $a^{\frac{p-1}{2}} = \left(g^i\right)^{\frac{p-1}{2}} = g^{(p-1)k} \equiv 1 \left(\mathrm{mod}\, p\right)$

Vậy định lý trên được chứng minh.

4) Định lý 2 (bổ đề Gauss): Cho p là một số nguyên tố và a là một số nguyên. Khi đó ta có: $a^{\frac{p-1}{2}} \equiv (-1)^{\sum_{k=1}^{\frac{p-1}{2}} \left[\frac{ka}{p}\right]} \left(\mathrm{mod}\, p\right)$.

5) Luật tương hỗ Gauss (luật thuận nghịch bình phương): Cho p,q là hai số nguyên tố lẻ phân biệt. Khi đó:

1. Nếu có ít nhất một trong hai số có dạng $4k+1$ thì p là số chính phương $\left(\mathrm{mod}\, q\right)$ khi và chỉ khi q là số chính phương $\left(\mathrm{mod}\, p\right)$.

2. Nếu cả hai số đều có dạng $4k+3$ thì p là số chính phương $\left(\mathrm{mod}\, q\right)$ khi và chỉ khi q là số không chính phương $\left(\mathrm{mod}\, p\right)$.

Và dưới kí hiệu Legendre, Luật tương hỗ Gauss được viết dưới dạng:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}$$

Chứng minh:

Đặt $A=\left\{a\mid (a,pq)=1,1\le a\le \frac{pq-1}{2}\right\}, B=\prod_{x\in A} x$

Nhận xét 1: $\begin{cases} B\equiv (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right)(\mathrm{mod}\, p) \\ B\equiv (-1)^{\frac{q-1}{2}}\left(\frac{p}{q}\right)(\mathrm{mod}\, q) \end{cases}$

Đặt $C=\left\{a\mid (a,p)=1,1\le a\le \frac{pq-1}{2}\right\}, D=\left\{q,q.2,\ldots,q.\frac{p-1}{2}\right\}$

Nhận thấy C là hợp rời của A và D nên:

$$\prod_{x\in C} x\equiv B.q^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\, p)\equiv B.\left(\frac{q}{p}\right)\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\, p)$$

Mà $\prod_{x\in C} x=\left[(p-1)!\right]^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\, p)\equiv (-1)^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\, p)$

nên $B.\left(\frac{q}{p}\right)\left(\frac{p-1}{2}\right)!\ \equiv (-1)^{\frac{q-1}{2}}\left(\frac{p-1}{2}\right)!\ (\mathrm{mod}\, p)\Rightarrow B\equiv (-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right)(\mathrm{mod}\, p)$

Tương tự ta có: $B\equiv (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right)(\mathrm{mod}\, q)$

Vậy nhận xét 1 được chứng minh.

Từ đây ta có: nếu $B\equiv \pm 1(\mathrm{mod}\, pq)$ thì $(-1)^{\frac{p-1}{2}}\left(\frac{q}{p}\right)=(-1)^{\frac{q-1}{2}}\left(\frac{p}{q}\right)$ hay

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

Nhận xét 2: $B\equiv \pm 1(\mathrm{mod}\, pq)\Leftrightarrow p\equiv q\equiv 1(\mathrm{mod}\, 4)$

Với $a\in A$, tồn tại duy nhất $a'\in A$ và $S_a\in\{-1;1\}$ thỏa mãn:

$a.a'\equiv S_a(\mathrm{mod}\, pq)$. Đây là song ánh trên A nên $B=\prod_{x\in A} x=\pm\delta$, trong đó δ là tích các phần tử của tập $E=\{a\in A\mid a=a'\}$.

Theo định lý phần dư Trung Hoa thì phương trình $x^2 \equiv 1(\mod pq)$ có 4 nghiệm 1,-1,N,–N $(N \neq \pm 1)$.

Giả sử $p \equiv q \equiv 1(\mod 4)$. Khi đó phương trình đồng dư $x^2 \equiv -1(\mod pq)$ có nghiệm I và từ đó suy ra toàn bộ nghiệm vủa nó là: $I, -I, NI, -NI$. Do đó $B \equiv \pm(1.N.I.NI.) \equiv \pm 1(\mod pq)$.

Giả sử $(p,q) \neq (1,1)(\mod 4)$. Khi đó phương trình đồng dư $x^2 \equiv -1(\mod pq)$ vô nghiệm. Do đó $B \equiv \pm(1..N.) \neq \pm 1(\mod pq)$

Nhận xét 2 được chứng minh.

Như vậy nếu $(p,q) \neq (1,1)(\mod 4)$ thì

$$B \neq \pm 1(\mod pq) \Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) \neq (-1)^{\frac{p-1}{2}+\frac{q-1}{2}} \Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -(-1)^{\frac{p-1}{2}+\frac{q-1}{2}}$$

Nhưng dễ thấy rằng nếu $(p,q) = (1,1)(\mod 4)$ thì $(-1)^{\frac{p-1}{2}+\frac{q-1}{2}} = 1 = (-1)^{\frac{(p-1)(q-1)}{4}}$

và nếu $(p,q) \neq (1,1)(\mod 4)$ thì $(-1)^{\frac{p-1}{2}+\frac{q-1}{2}} = -1 = (-1)^{\frac{(p-1)(q-1)}{4}}$

Do vậy ta luôn có $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Ngoài ra định lý trên còn được chưng minh bằng bổ đề Gauss, bạn đọc có thể xem chứng minh ấy tại $[5]$.

Luật tương hỗ Gauss có ý nghĩa vô cùng quan trọng trong các bài toán về thặng dư bình phương và đặc biệt nó giúp ta biến đổi và tính toán các ký hiệu Legendre một cách hợp lý. Điều này sẽ được thể hiện rõ trong các ví dụ và bài tập ở phần sau.

6) Định nghĩa 3: Cho a là một số nguyên và b là một số nguyên dương lẻ. Giả sử $b = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ là sự phân tích chính tắc của b. Kí hiệu Jakobi đươc xác định như sau:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1}\left(\frac{a}{p_2}\right)^{\alpha_2} \ldots \left(\frac{a}{p_r}\right)^{a_r}$$

và $\left(\frac{a}{p_i}\right)$ được xác định theo kí hiệu Legendre như trên.

Chú ý: Kí hiệu Jakobi có đầy đủ các tính chất như kí hiệu Legendre. Đặc biệt Luật tương hỗ Gauss được mở rộng dưới kí hiệu Jakobi như sau:

Nếu m,n là các số nguyên dương lẻ và nguyên tố cùng nhau. Khi đó:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right)=(-1)^{\frac{(m-1)(n-1)}{4}}$$

7) Tính chất: Giả sử n là một số nguyên lẻ và a là số nguyên với $(a,n)=1$. Khi đó ta có:

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

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

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

iv. $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$

v. 2 là số chính phương mod p khi và chỉ khi $p\equiv\pm1(\mod 8)$

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

vii. 3 là số chính phương mod p khi và chỉ khi $p\equiv\pm1(\mod 12)$

viii. -3 là số chính phương mod p khi và chỉ khi $p\equiv 1(\mod 6)$

II. Một số bài toán ứng dụng.

Bài toán 1. Cho đa thức $P(x)=(x^2-2)(x^2-3)(x^2-6)$. Chứng minh rằng với mọi số nguyên tố p, đều tìm được số nguyên dương n sao cho $P(n)\vdots p$.

Lời giải:

Với $p=2,3$ tương ứng ta chọn $n=2,3$, hiển nhiên thỏa mãn.

Giả sử tồn tại số nguyên tố $p>3$ sao cho $P(n)\not\vdots p \quad \forall n\in\mathbb{Z}$.

hay $(n^2-2)(n^2-3)(n^2-6)\not\equiv 0 \pmod p \quad \forall n\in\mathbb{Z}$.

Suy ra $2,3,6$ đều không là số chính phương $(\mathrm{mod}\, p)$, hay

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

Nhưng rõ ràng $6^{\frac{p-1}{2}}=2^{\frac{p-1}{2}}.3^{\frac{p-1}{2}}\equiv(-1).(-1)\equiv 1(\mathrm{mod}\, p)$

Vô lý vì p nguyên tố >3.

Bài toán 2. 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:

$101 \mid \underbrace{P(P(...P}_{n}(x)...)-x$

Lời giải:

Xét hai số nguyên x,y bất kỳ.

Ta sẽ chứng minh rằng $x\equiv y(\mathrm{mod}\, 101)\Leftrightarrow P(x)\equiv P(y)(\mathrm{mod}\, 101)(1)$

Hiển nhiên $x\equiv y(\mathrm{mod}\, 101)\Rightarrow P(x)\equiv P(y)(\mathrm{mod}\, 101)$

Do $P(x)=x^3+14x^2-2x+1$ nên ta có:

$4[P(x)-P(y)]=4(x-y)(x^2+xy+y^2+14x+14y-2)$

$=(x-y)\left[(2x+y+14)^2+3(y-29)^2\right]$

Suy ra: $P(x)\equiv P(y)(\mathrm{mod}\, 101)\Leftrightarrow\left[\begin{array}{l}x\equiv y(\mathrm{mod}\, 101)\\(2x+y+14)^2+3(y-29)^2\equiv 0(\mathrm{mod}\, 101)(2)\end{array}\right.$

Xét (2):

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

Nếu $101\mid(y-29)\Rightarrow 101\mid(2x+y+14)\Rightarrow x\equiv y\equiv 29(\mathrm{mod}\, 101)$

Như vậy ta luôn có $x\equiv y(\mathrm{mod}\, 101)$.

Do đó (1) được chứng minh.

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

Theo nguyên lý Drichlet, 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 3.Chứng minh rằng phương trình $x^2 = y^3 - 5$ không có nghiệm nguyên.

Lời giải:

Giả sử phương trình $x^2 = y^3 - 5$ có nghiệm nguyên (x, y).

Nếu y chẵn thì $x^2 = y^3 - 5 \equiv -5 \equiv 3 (\mathrm{mod}\, 8)$. Vô lý vì một số chính phương chỉ có thể đồng dư 0,1,4 theo modulo 8.

Do đó y lẻ.

Nếu $y \equiv 3 (\mathrm{mod}\, 4) \Rightarrow x^2 \equiv 3^3 - 5 \equiv 2 (\mathrm{mod}\, 4)$. Vô lý.

Suy ra $y \equiv 1 (\mathrm{mod}\, 4) \rightarrow y = 4z + 1$, $z \in \mathbb{Z}$.

Khi đó ta có :

$x^2 + 4 = y^3 - 1 = (4z+1)^3 - 1 = 64z^3 + 48z^2 + 12z = 4z(16z^2 + 12z + 3)$

Suy ra: $x^2 \equiv -4 \mathrm{mod}(16z^2 + 12z + 3)$

Sử dụng ký hiệu Jakobi ta được :

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

$(\text{vì } 16z^2 + 12z + 3 \equiv 3 (\mathrm{mod}\, 4))$,vô lý.

Vậy phương trình đã cho không có nghiệm nguyên.

Bài toán 4 .Chứng minh rằng phương trình sau không có nghiệm nguyên dương: $4xyz - x - y = t^2$

Lời giải:

Giả sử tồn tại bộ số nguyên dương (x,y,z,t) thỏa mãn:

$4xyz - x - y = t^2 \Leftrightarrow 16xyz^2 = 4xz + 4yz + 4zt^2$

$\Leftrightarrow 4zt^2 + 1 = (4xz-1)(4yz-1) \Rightarrow (2zt)^2 \equiv -z \bmod (4yz-1)(*)$

Giả sử rằng $z = 2^k b$, với k là số nguyên không âm và b là một số nguyên dương lẻ. Từ $(*)$, sử dụng các tính chất của ký hiệu Jakobi ta được:

$$1 = \left(\frac{-z}{4yz-1}\right) = \left(\frac{-1}{4yz-1}\right)\left(\frac{2^k}{4yz-1}\right)\left(\frac{b}{4yz-1}\right) = -\left(\frac{2}{4yz-1}\right)^k \left(\frac{4yz-1}{b}\right)(-1)^{\frac{b-1}{2}}$$

$$= -\left(\frac{2}{4yz-1}\right)^k \left(\frac{(4.2^k y)b-1}{b}\right)(-1)^{\frac{b-1}{2}} = -\left(\frac{2}{4yz-1}\right)^k \left(\frac{-1}{b}\right)(-1)^{\frac{b-1}{2}}$$

$$= -\left(\frac{2}{4yz-1}\right)^k = T$$

Nếu k chẵn thì $T = -1$. Vô lý.

Nếu k lẻ thì nói riêng: $k \geq 1$.

Suy ra: $4yz - 1 = (4.2^k)by - 1 \equiv -1 (\bmod 8) \Rightarrow \left(\frac{2}{4yz-1}\right) = 1 \Rightarrow T = -1$

Vô lý.

Vậy phương trình đang xét không có nghiệm nguyên.

Chú ý rằng các phương trình sau cũng không có nghiệm nguyên dương:

a) $4xy - x - 1 = z^2$

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

Bài toán 5. Chứng minh rằng số $4kxy - 1$ không chia hết số $x^m + y^m$ với mọi x,y,k,m nguyên dương.

Lời giải:

Giả sử tồn tại các số nguyên dương x,y,k,m sao cho:

$(4kxy-1) \mid (x^m + y^m)$.

Chú ý rằng: $4kxy - 1, x^m, y^m$ đôi một nguyên tố cùng nhau.

Đặt $m_1 = \left[\frac{m}{2}\right], n_1 = \left[\frac{n}{2}\right]$. Xét các khả năng sau:

a) $m = 2m_1, n = 2n_1$

Khi đó: $(4kxy-1) \mid \left(x^{m_1}\right)^2 + \left(y^{m_1}\right)^2 \Rightarrow \left(\frac{-1}{4kxy-1}\right) = 1$

Vô lý vì $4kxy - 1 \equiv 3 \pmod 4$.

b) $m = 2m_1, n = 2n_1 + 1$

(trường hợp $m = 2m_1 + 1, n = 2n_1$ hoàn toàn tương tự)

Ta có: $4kxy - 1 \mid x^m + y^m = \left(x^{m_1}\right)^2 + y\left(y^{n_1}\right)^2 \Rightarrow \left(\frac{-y}{4kxy-1}\right) = 1$

Nếu y lẻ, ta có:

$$\left(\frac{-y}{4kxy-1}\right) = \left(\frac{-1}{4kxy-1}\right)\left(\frac{y}{4kxy-1}\right) = -(-1)^{\frac{y-1}{2}}\left(\frac{4kxy-1}{y}\right)$$

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

Mâu thuẫn.

Nếu y chẵn. Ta đặt $y = 2^t y_1$, với $t \in N^*$, y_1 lẻ.

Khi đó tương tự trường hợp y lẻ, ta có:

$$\left(\frac{2}{4kxy-1}\right) = (-1)^{\frac{(4kxy-1)^2-1}{8}} = 1 \text{ và } \left(\frac{-y_1}{4kxy-1}\right) = \left(\frac{-y_1}{2^t.4kxy_1-1}\right) = 1$$

Suy ra: $\left(\frac{-y}{4kxy-1}\right) = \left(\frac{2^t(-y_1)}{4kxy-1}\right) = \left(\frac{2}{4kxy-1}\right)^t\left(\frac{-y_1}{4kxy-1}\right) = (1)^t(-1) = -1$

Mâu thuẫn.

c) $m = 2m_1 + 1, n = 2n_1 + 1$.

Ta có: $4kxy - 1 \mid x^m + y^m = x\left(x^{m_1}\right)^2 + y\left(y^{n_1}\right)^2 \Rightarrow \left(\frac{-xy}{4kxy-1}\right) = 1$

Mặt khác theo trường hợp b) ta có :

$$\left(\frac{-xy}{4kxy-1}\right) = \left(\frac{-1}{4kxy-1}\right)\left(\frac{x}{4kxy-1}\right)\left(\frac{y}{4kxy-1}\right) = (-1).(-1).(-1) = -1$$

Mâu thuẫn.

Vậy giả thiết phản chứng là sai.

Bài toán 6. 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 $\bmod p$ và $\frac{p-1}{2}$ số không chính phương $\bmod p$.

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 $i^2 \equiv r_i \left(\bmod p\right)$. Dễ thấy $r_i \neq r_j \forall i \neq j$. Khi đó tập hợp $A = \left\{r_i : r_i \in S, i^2 \equiv r_i \left(\bmod p\right), i \in S_1\right\}$ có đúng $\frac{p-1}{2}$ phần tử.

Ta chứng minh rằng A là tập tất cả số chinh phương $\bmod p$ trong S.

Thật vậy, rõ ràng mỗi số thuộc thuộc A đều là số chính phương $\bmod p$. Giả sử $a \in S$ sao cho tồn tại $k \in S$ thỏa mãn: $a \equiv k^2 \left(\bmod p\right)$

Nếu $k \in S_1$ thì $a = r_k \in A$.

Nếu $k \notin S_1$ thì $h = p - k \in S_1$ và $a \equiv h^2 \left(\bmod p\right) \Rightarrow a = r_h \in A$

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

Khi đó đặt $r = r(x,y) = xp - y^2$ thì ta có $r \in (0,p)$.

Rõ ràng: $-r = y^2 - xp \equiv y^2 \left(\bmod p\right) \Rightarrow \left(\frac{-r}{p}\right) = 1$

Mà $p \equiv 1(\mod 4)$ nên $\left(\frac{-1}{p}\right) = 1 \Rightarrow \left(\frac{r}{p}\right) = 1$.

Nhận xét: các số $r(x,y)$ đôi một phân biệt.

Thật vậy giả sử : $r(x_1,y_1) = r(x_2,y_2)$

Suy ra: $x_1 p - y_1^2 = x_2 p - y_2^2 \Rightarrow p \mid (y_1 - y_2)(y_1 + y_2)$

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 $y_1 = y_2, x_1 = x_2$

Như vậy ta có số các số $r(x,y)$ là:

$N = \sum_{x=1}^{n}\left(\left[\sqrt{xp}\right] - \left[\sqrt{(x-1)p}\right]\right) = \left[\sqrt{np}\right] = 2n = \frac{p-1}{2}$ = số thặng dư bình phương $\mod p$ trong tập $\{1,2,...,p-1\}$ (theo bổ đề).

Do $p \equiv 1(\mod 4)$ nên

$\left(\frac{r}{p}\right)\left(\frac{p-r}{p}\right) \equiv r^{\frac{p-1}{2}}.(p-r)^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}}.(-r)^{\frac{p-1}{2}} = r^{p-1} \equiv 1(\mod p)$ Suy ra :

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

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 $\frac{p-1}{4}$ cặp, mỗi cặp có tổng bằng p. Suy ra : $\sum r(x,y) = \frac{p(p-1)}{4}(*)$.

Mặt khác ta lại có :

$$\sum r(x,y)=\sum_{x=1}^{n}\left(\sum_{y=\left[\sqrt{(x-1)p}\right]+1}^{\left[\sqrt{xp}\right]} r(x,y)\right)=\sum_{x=1}^{n}\left(\sum_{y=\left[\sqrt{(x-1)p}\right]+1}^{\left[\sqrt{xp}\right]}\left(xp-y^2\right)\right)$$

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

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

$$=p\left(-S+(n+1)\left[\sqrt{np}\right]\right)-\frac{2n(2n+1)(4n+1)}{6}$$

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

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

Nhận xét: Lời giải trên thực sự ấn tượng nhưng ta đều nhận thấy nó khá khó về mặt ý tưởng và sự kết nối các sự kiện là hơi mất tự nhiên.Tuy nhiên bằng một cách tư duy đơn giản hơn và sử dụng nhuần nhuyễn các tính chất của hàm phần nguyên ta có thể đi đến lời giải sau :

Lời giải 2:

Giả sử P là mệnh đề nào đó, ta đưa vào ký hiệu sau :

$$\{P\}=\begin{cases}1 \text{ nếu P là mệnh đề đúng}\\ 0 \text{ nếu P là mệnh đề sai}\end{cases}$$

Từ đó với mỗi $i\in\mathbb{Z},1\le i\le n$ ta có :

$$\left[\sqrt{ip}\right]=\sum_{x\in\mathbb{N}}\left\{x\le\sqrt{ip}\right\}=\sum_{x\in\mathbb{N}}\left\{x^2\le ip\right\}$$

Vì $i\le n$ nên $ip\le np$. Do đó nếu $x\ge 2n+1$ thí

$$x^2\ge(2n+1)^2=4n^2+4n+1>n(4n+1)=np\ge ip$$

Suy ra: $\sum_{x\in\mathbb{N}}\left\{x^2\le ip\right\}=\sum_{x=0}^{2n}\left\{x^2\le ip\right\}=\sum_{x=1}^{2n}\left(1-\left\{x^2\ge ip\right\}\right)$

$$=2n-\sum_{x=1}^{2n}\left\{x^2\ge ip\right\}=2n-\sum_{x=1}^{2n}\left\{i\le\frac{x^2}{p}\right\}$$

Do vậy:

$$\sum_{i=1}^{n}\left[\sqrt{ip}\right]=\sum_{i=1}^{n}\left(2n-\sum_{x=1}^{2n}\left\{i\le\frac{x^2}{p}\right\}\right)=2n^2-\sum_{i=1}^{n}\sum_{x=1}^{2n}\left\{i\le\frac{x^2}{p}\right\}$$

$$=2n^2-\sum_{x=1}^{2n}\sum_{i=1}^{n}\left\{i\le\frac{x^2}{p}\right\}=2n^2-\sum_{x=1}^{2n}\sum_{i\in\mathbb{N}}\left\{i\le\frac{x^2}{p}\right\}$$

$$=2n^2-\sum_{x=1}^{2n}\left[\frac{x^2}{p}\right]=2n^2-\sum_{x=1}^{\frac{p-1}{2}}\left[\frac{x^2}{p}\right]$$

Như vậy ta chỉ cần tính tổng $T=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{k^2}{p}\right]$ với p là một số nguyên tố có dạng $4n+1$.

Tính chất cơ bản : Cho a,b là hai số thực thỏa mãn $(a+b)\in\mathbb{Z},ab\notin\mathbb{Z}$. Khi đó ta có : $[a]+[b]=a+b-1$.

Xét bổ đề sau : Cho p là một số nguyên tố có dạng $4k+1$ và m là một số nguyên dương nguyên tố cùng nhau với p. Khi đó ta có :

$$\sum_{i=1}^{p-1}\left[\frac{mi^2}{p}\right]=\sum_{i=1}^{p-1}\frac{mi^2}{p}-\frac{p-1}{2}$$

Chứng minh :

Do p là một số nguyên tố có dạng $4k+1$ nên với mỗi $i\in\{1,2,...,p-1\}$, tồn tại duy nhất $j\in\{1,2,...,p-1\},j\ne i$ sao cho $i^2+j^2\equiv 0(\mathrm{mod}\,p)$. Như vậy tập $\{1,2,...,p-1\}$ được phân hoạch thành $\frac{p-1}{2}$ cặp như thế. Khi đó với chú ý $(m,p)=1$, áp dụng tính chất trên, ta được :

$$\left[\frac{mi^2}{p}\right]+\left[\frac{mj^2}{p}\right]=\frac{mi^2}{p}+\frac{mj^2}{p}-1.$$

Suy ra :

$$\sum_{i=1}^{p-1}\left[\frac{mi^2}{p}\right]=\sum_{(i,j)}\left(\left[\frac{mi^2}{p}\right]+\left[\frac{mj^2}{p}\right]\right)=\sum_{(i,j)}\left(\frac{mi^2}{p}+\frac{mj^2}{p}-1\right)$$

$$=\sum_{i=1}^{p-1}\frac{mi^2}{p}-\frac{p-1}{2}$$

Áp dụng bổ đề với $m=1$ ta được :

$$\sum_{k=1}^{p-1}\left[\frac{k^2}{p}\right]=\sum_{k=1}^{p-1}\frac{k^2}{p}-\frac{p-1}{2}=\frac{(p-1)p(2p-1)}{6p}-\frac{p-1}{2}=\frac{(p-1)(p-2)}{3}$$

Mặt khác ta lại có :

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

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

Do đó:

$$2T+\frac{(p-1)^2}{4}=\frac{(p-1)(p-2)}{2}\Rightarrow T=\frac{(p-1)(p-5)}{24}$$

$$\text{Vậy } M=2n^2-T=2n^2-\frac{(p-1)(p-5)}{24}=2\left(\frac{p-1}{4}\right)^2-\frac{(p-1)(p-5)}{24}=\frac{p^2-1}{12}$$

Chú ý rằng kết quả $T=\frac{(p-1)(p-5)}{24}$ với $p\equiv 1(\mod 4)$ chính là tổng quát 'nhỏ' của VietnamTST2005 bài 5b), bài đó yêu cầu tính $P=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{k^2}{p}\right]$ với $p\equiv 1(\mod 8)$ cũng cho $P=\frac{(p-1)(p-5)}{24}$.

Bài toán 7.

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

Nếu n chẵn, ta có: $-1 \equiv \left(2^{\frac{n}{2}}\right)^2 \pmod p \Rightarrow \left(\frac{-1}{p}\right) = -1 \Rightarrow p \equiv 1 \pmod 4$. Mâu thuẫn.

Nếu n lẻ, ta có :

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

(do $p \equiv -1 \pmod 8$). Vô lý.

Vậy số 2^n+1 không có ước nguyên tố dạng $8k-1$.

b) Từ chứng minh trên ta nhận thấy : nếu n lẻ thì 2^n+1 không có ước nguyên tố dạng $8k+5$.

Như vậy mọi ước nguyên tố của $2^{3^n}+1$ đều đồng dư 1 hoặc 3 $\bmod 8$.

Ta có : $2^{3^n}+1 = (2+1)\left(2^2-2+1\right)\left(2^{2.3}-2^3+1\right)\ldots\left(2^{2.3^{n-1}}-2^{3^{n-1}}+1\right)$

Đặt $s_i = 2^{2.3^i}-2^{3^i}+1, \quad 1 \le i \le n-1$

Ta sẽ chứng minh rằng : $\forall 1 \le i < j \le n-1$ thì $\gcd(s_i, s_j) = 3$.

Để ý rằng $s_i \equiv 1-(-1)+1 \equiv 3 \pmod 9 \Rightarrow 3 \,||\, s_i \forall i$

Gọi p là một số nguyên tố chia hết $\gcd(s_i, s_j)$. Khi đó

$$p \mid s_i \mid \left(2^{3^{i+1}}+1\right) \Rightarrow 2^{3^j} = \left(2^{3^{i+1}}\right)^{3^{j-i-1}} \equiv (-1)^{3^{j-i-1}} \equiv -1 \pmod p$$

$$\Rightarrow 0 \equiv s_j = 2^{2.3^j}-2^{3^j}+1 \equiv 1-(-1)+1 \equiv 3 \pmod p \Rightarrow p = 3$$

Vậy $\gcd(s_i, s_j) = 3 \quad \forall 1 \le i < j \le n-1$

Bây giờ lấy $i \in \{1, 2, \ldots, n-1\}$. Nếu mọi ước nguyên tố của s_i (trừ 3) đều có dạng $8k+1$ thì $s_i \equiv 3 \pmod 8$ (chú ý rằng $3 \,||\, s_i \forall i$). Vô lý.

Do vậy mỗi s_i đều có ít nhất một ước nguyên tố p_i dạng $8k+3$ mà $p_i \ne 3$. Do $\gcd(s_i, s_j) = 3$ nên $p_i \ne p_j \forall 1 \le i < j \le n-1$.

Suy ra $2^{3^n}+1$ có ít nhất n ước nguyên tố dạng $8k+3$ là :

$3, p_1, p_2, \ldots, p_{n-1}$.

Bài toán 8. 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 $\bmod p$, hay phương trình đồng dư $x^2 \equiv -1 (\bmod p)$ có hai nghiệm thuộc $[1, p-1]$, ta gọi hai nghiệm đó là x_1, x_2 với

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

Chọn $n = x_1$. Khi đó ta có $p \mid n^2+1,\ n \le \frac{p-1}{2}$.

Ta sẽ chứng minh rằng: $p > 2n+\sqrt{2n}$.

Thật vậy do $1 \le n \le \frac{p-1}{2}$ nên ta đặt $n = \frac{p-1}{2} - l,\ 0 \le l < \frac{p-1}{2}$.

Do $n^2 \equiv -1 (\bmod p)$ nên:

$$\left(\frac{p-1}{2} - l\right)^2 \equiv -1 (\bmod p) \Rightarrow (p-1-2l) + 4 \equiv 0 (\bmod p)$$

Suy ra: $(2l+1)^2 + 4 \equiv 0 (\bmod p) \Rightarrow \exists r \in \mathbb{N}^* : (2l+1)^2 + 4 = rp$.

mà $(2l+1)^2 = 4l(l+1) + 1 \equiv 1 (\bmod 8) \Rightarrow rp \equiv 5 (\bmod 8)$

Suy ra: $r \equiv 5 (\bmod 8) \Rightarrow r \ge 5(2l+1)^2 + 4 \ge 5p \Rightarrow l \ge \frac{1}{2}\left(\sqrt{5p-4} - 1\right)$

Đặt $\sqrt{5p-4} = u \to l \ge \frac{1}{2}(u-1)$, ta có

$$n = \frac{p-1}{2} - l \le \frac{p-1}{2} - \frac{1}{2}(u-1) = \frac{1}{2}(p-u) = \frac{1}{2}\left(\frac{u^2+4}{5} - u\right) \Rightarrow$$

$$u^2 - 5u + 4 - 10n \ge 0 \Rightarrow (2u-5)^2 \ge 40n+9 \Rightarrow u \ge \frac{1}{2}\left(5 + \sqrt{40n+9}\right)$$

Mặt khác do $n \le \frac{1}{2}(p-u)$ nên

$$p \ge 2n + u \ge 2n + \frac{1}{2}\left(5 + \sqrt{40n+9}\right) > 2n + \sqrt{10n}.$$

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

Nhận xét: Với bài toán trên ta đã có một tổng quát cho bài toán sau: Xét mệnh đề : $P(n)$: n^2+1 chia hết $n!$. Chứng minh rằng tồn tại vô hạn số nguyên dương n sao cho $P(n)$ đúng và cũng tồn tại vô hạn số nguyên dương n sao cho $P(n)$ sai. (Romania National Olympiad 2008).

Bài toán 9. Tìm tất cả các số nguyên dương n sao cho $(2^n-1)\,|\,(3^n-1)$.

Lời giải:

Ta sẽ chứng minh rằng $n=1$ nghiệm duy nhất của bài toán.

Thật vậy giả sử tồn tại số nguyên $n>1$ sao cho $2^n-1\,|\,3^n-1$.

Khi đó rõ ràng $3\not\vdots(2^n-1)$ nên n lẻ, do đo:

$$n\geq 3\Rightarrow 2^n-8=8\left(2^{n-3}-1\right)\vdots 4.3=12\Rightarrow 2^n-1\equiv 7\pmod{12}$$

Suy ra 2^n-1 có ít nhất một ước nguyên tố p có dạng $12k+5$ hoặc $12k+7$.

Hơn nữa ta lại có:

$$p\,|\,(2^n-1)\,|\,(3^n-1)\Rightarrow 3\equiv\left(3^{\frac{n+1}{2}}\right)^2\pmod p\Rightarrow\left(\frac{3}{p}\right)=1\Rightarrow p\equiv\pm1\pmod{12}$$ Mâu thuẫn.

Vậy $n=1$ là số nguyên dương duy nhất thỏa mãn.

Bài toán 10. 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 $3^{P(n)}-1$.

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:

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

Giả sử $Q(x)$ không là hằng số. Khi đó dãy $\{Q(n) \mid n \in \mathbb{Z}\}$ 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 chon $m \in \mathbb{Z}$ sao cho :

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

Ta có $M = 2^{Q(m)}-1 \mid 3^{P(m)}-1$ $(*)$ nên $(M,2)=(M,3)=1$

Gọi a,b tương ứng là bậc của $2,3$ modulo M. Từ $(*)$ ta suy ra

$a \mid Q(m), b \mid P(m) \Rightarrow \gcd(a,b) \le \gcd(Q(m),P(m)) \le d$

Đặt $\gcd(a,b)=s$. Khi đó tồn tại các số nguyên x_0,y_0 sao cho

$s = ax_0+by_0$.

Do $1 \le s \le d$ nên tồn tại $k \in \mathbb{N}, 0 \le k < d$ sao cho $s = d-k$.

Ta sẽ chứng tỏ rằng tồn tại các số nguyên x,y sao cho:

$0 \le m+ax+by \le d$. Thật vậy chọn $x = tx_0, y = ty_0$.

Ta có :$0 \le m+ax+by \le d \Leftrightarrow 0 \le m+t(ax_0+by_0) \le d$ hay

$0 \le m+t(d-k) \le d \Leftrightarrow \dfrac{-m}{d-k} \le t \le \dfrac{d-m}{d-k}$

Do $\dfrac{d-m}{d-k}-\dfrac{-m}{d-k}=\dfrac{d}{d-k} \ge 1$ nên tồn tại số nguyên t thỏa mãn.

Nhận xét trên được chứng minh.

Ta có $Q(x) \in \mathbb{Z}[x]$ nên :

$Q(m+ax) \equiv Q(m) \pmod a \Rightarrow 2^{Q(m+ax)} \equiv 2^{Q(m)} \equiv 1 \pmod M$

hay $M \mid 2^{Q(m+ax)}-1 \mid 3^{P(m+ax)}-1$

Tương tự , ta có :

$P(m+ax+by) \equiv P(m+ax) \pmod b \Rightarrow 3^{P(m+ax+by)} \equiv 3^{P(m+ax)} \equiv 1 \pmod M$Suy ra :$M \le 3^{P(m+ax+by)}-1 \le 3^{\max\{P(0),P(1),\ldots,P(d)\}}-1 \le 2^{Q(m)}-2 = M-1$. Vô lý.

Vậy $Q(x) \equiv \text{Const}$.

Bài toán 11. Cho a,b là hai số nguyên dương thoả mãn ab không là số chính phương. Chứng minh rằng tồn tại vô hạn số nguyên dương n sao cho $\left(a^n-1\right)\left(b^n-1\right)$ 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 $\bmod p$.

Chứng minh :

Do a là một số nguyên dương không chính phương nên ta đặt : $a=b^2c$, trong đó $b\in\mathbb{N}^*, c=q_1q_2...q_m\left(m\geq 1\right)$, với q_i nguyên tố, đôi một phân biệt.

Khi đó với mỗi số nguyên tố lẻ p mà $\left(p,a\right)=1$, 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 :

1) q_1 lẻ

Chọn $r_1,r_2,...,r_m$ thỏa mãn r_1 không là số chính phương $\bmod q_1$ và r_i là số chính phương $\bmod q_i$ với mọi $i=2,...,m$.

Theo định lý thặng dư Trung Hoa, tồn tại số nguyên p_0 thỏa mãn:

$$\begin{cases}p_0\equiv r_i\left(\bmod q_i\right)\forall i=1,2,...,m\\ p_0\equiv 1\left(\bmod 4\right)\end{cases}\left(I\right)$$

Dễ thấy $\left(p_0,q_i\right)=\left(p_0,4\right)=1\forall i=1,2,..,m\Rightarrow\left(p_0,4q_1q_2...q_m\right)=1$

Mà ta có $p=p_0+\left(4q_1q_2...q_m\right)t$ cũng là nghiệm của $\left(I\right)$ với mọi $t\in\mathbb{N}$.

Nhưng theo định lý Drichlet, 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: $\begin{cases}p\equiv r_i\left(\bmod q_i\right)\forall i=1,2,...,m\\ p\equiv 1\left(\bmod 4\right)\end{cases}$

Suy ra: $\left(\frac{p}{q_i}\right)=\left(\frac{r_i}{q_i}\right)=\begin{cases}-1, \text{ khi } i=1\\ 1, \text{ khi } i=2,\ldots,m\end{cases}$

Do $p\equiv 1\pmod 4$ nên theo luật tương hỗ Gauss, ta có: $\left(\frac{p}{q_i}\right)=\left(\frac{q_i}{p}\right)\forall i=1,2,\ldots,m$

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

2) $q_1=2$

Chọn r_i là số chính phương $\bmod p_i$ với mọi $i=2,\ldots,m$

Tương tự ta có vô hạn số nguyên tố p thỏa mãn:

$\begin{cases}p\equiv r_i\pmod{q_i}\forall i=2,..,m\\ p\equiv 5\pmod 8\end{cases}$

Suy ra: $\left(\frac{p}{q_i}\right)=\left(\frac{r_i}{q_i}\right)=1\forall i=2,\ldots,m$

Do $p\equiv 5\pmod 8$ nên $p\equiv 1\pmod 4\Rightarrow\left(\frac{q_i}{p}\right)=\left(\frac{p}{q_i}\right)=1\forall i=2,\ldots,m$

Mà $\left(\frac{q_1}{p}\right)=\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}=-1$ (do $p\equiv 5\pmod 8$)

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

Bổ đề được chứng minh.

Trở lại bài toán.

Theo giả thiết 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 $a^{\frac{p-1}{2}}\equiv 1\pmod p, b^{\frac{p-1}{2}}\equiv -1\pmod p$

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

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

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

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 : $b^{\frac{p-1}{2}p}-1\equiv(-1)^p-1\not\equiv 0(\mathrm{mod}\,p)$

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.

Chú ý rằng một trong hai khả năng sẽ xảy ra với vô hạn p.

Vấn đề mở rộng: Cho a,b là hai số nguyên dương phân biệt >1, chứng minh rằng tồn tại số nguyên dương n sao cho $\left(a^n-1\right)\left(b^n-1\right)$ không là số chính phương.

Nhận xét: Bổ đề được phát biểu và chứng minh trong lời giải trên thực sự tốt và có nhiều ứng dụng để giải các bài toán "đẹp" về thặng dư bình phương. Sau đây là một số ví dụ minh họa.

Bài toán 12. Cho $f(x)$ là một tam thức bậc 2 với hệ số nguyên thỏa mãn với mọi số nguyên tố p đều tồn tại ít nhất một số nguyên n sao cho $p\mid f(n)$. Chứng minh rằng $f(x)$ có nghiệm hữu tỉ.

Lời giải:

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

Rõ ràng ta chỉ cần chứng minh rằng : b^2-4ac là số chính phương.

Lấy p là một số nguyên tố bất kỳ, theo giả thiết tồn tại số nguyên n sao cho :

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

Do đó: $\left(\frac{b^2 - 4ac}{p}\right) = 1$. Khi đó theo bổ đề bài 11 ta có $b^2 - 4ac$ là số chính phương.

Do vậy $f(x)$ có nghiệm hữu tỉ.

Bài toán 13: Giả sử rằng $a_1, a_2, ..., a_{2004}$ là các số nguyên không 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 $p > N = \max\{2004, a_i \mid i = 1, 2, ..., 2004\}$ 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 $a_1, a_2, ..., a_{2004}$ không chia hết cho p. Theo trên 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.

Áp dụng bổ đề bài 11 ta được k là số chính phương.

Đặt $k = l^2 \Rightarrow l^2 \le 2004 \Rightarrow l \le 44 \Rightarrow k \le 44^2 = 1936$.

Do đó 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 $\sum_{i=1}^{n} a_i^n = 1936 (m^2)^n = (44m^n)^2$.

Vậy 68 là giá trị nhỏ nhất cần tìm.

Bài toán 14. Cho a, b, c là các số nguyên và p là một số nguyên tố lẻ > 3. Chứng minh rằng nếu $f(x) = ax^2 + bx + c$ là số chính phương tại $\frac{p+5}{2}$ giá trị nguyên liên tiếp của x thì $p \mid (b^2 - 4ac)$.

Lời giải:

Bổ đề 1: Cho $f(x)$ là một đa thức hệ số nguyên có $\deg f = k$. Đặt $r = \frac{p-1}{2}$, và $f(x)^r = a_0 + a_1 x + ... + a_{kr} x^{kr}$. Khi đó ta có:

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right) \equiv -\left(a_{p-1} + a_{2(p-1)} + ... + a_{l(p-1)}\right)(\mathrm{mod}\, p),\ l = \left[\frac{k}{2}\right].$$

Chứng minh:

Đặt $s_n = \sum_{x=0}^{p-1} x^n, (n \in \mathbb{N})$.

Dễ thấy $s_0 = p,\ s_n \equiv p-1 \equiv -1\ (\mathrm{mod}\, p)$ với $n > 0$ và $p-1 \mid n$.

Xét $n > 0$ vµ $n \not\vdots (p-1)$, ta gọi g là một căn nguyên thủy của p, khi đó $\{g, g^2, g^3, ..., g^{p-1}\} \equiv \{1, 2, ..., p-1\}(\mathrm{mod}\, p)$, $g^{p-1} \equiv 1 (\mathrm{mod}\, p)$ và $g^n - 1 \not\equiv 0 (\mathrm{mod}\, p)$.

Suy ra: $s_n = \sum_{x=0}^{p-1} x^n \equiv \sum_{i=1}^{p-1} g^{ni} = g^n \sum_{i=0}^{p-2} (g^n)^i = g^n . \frac{g^{n(p-1)} - 1}{g^n - 1} \equiv 0 (\mathrm{mod}\, p)$.

VËy $s_n \equiv \begin{cases} -1\ (\mathrm{mod}\, p) \text{ khi } n > 0,\ n \vdots (p-1) \\ 0\ (\mathrm{mod}\, p) \text{ khi } n=0 \ \vee\ n > 0,\ n \not\vdots (p-1) \end{cases}$

Do đó:

$$\sum_{x=0}^{p-1}\left(\frac{f(x)}{p}\right) \equiv \sum_{x=0}^{p-1} (f(x))^r = \sum_{x=0}^{p-1} \left(a_0 + a_1 x + ... + a_{kr} x^{kr}\right) = \sum_{i=0}^{kr} a_i s_i$$

$$\equiv -\left(a_{p-1} + a_{2(p-1)} + ... + a_{l(p-1)}\right)$$

Bổ đề 1 được chứng minh.

Bổ đề 2: Cho a, b, c là các số nguyên bất kỳ và p là một số nguyên tố không chia hết a. Khi đó ta có:

$$\sum_{x=0}^{p-1}\left(\frac{ax^2 + bx + c}{p}\right) = \begin{cases} -\left(\frac{a}{p}\right) & \text{khi } b^2 - 4ac \not\vdots p \\ (p-1)\left(\frac{a}{p}\right) & \text{khi } b^2 - 4ac \vdots p \end{cases}$$

Chứng minh. Ta có:

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

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

Đặt $S=\sum_{x=0}^{p-1}\left(\frac{x^2-D}{p}\right)$. Áp dụng bổ đề 1 cho $f(x)=x^2-D$ ta được:

$S\equiv -(a_{p-1})=-1(\mathrm{mod}\,p)$, mà $|S|\le p$ nên $S\in\{-1,p-1\}$.

Nếu $S=p-1$, thì có duy nhất một số $x_0\in\{0,1,...,p-1\}$ sao cho

$$\left(\frac{x_0^2-D}{p}\right)=0\Rightarrow\begin{cases}p\mid(x_0^2-D)\\ p\mid((p-x_0)^2-D)\end{cases}$$

Suy ra nếu $x_0\neq 0$ thì $(p-x_0)\in\{0,1,...,p-1\}$ và $(p-x_0)\neq x_0$. Mâu thuẫn tính duy nhất của x_0. Do đó $x_0=0\Rightarrow p\mid D$.

Ngược lại nếu $p\mid D$, suy ra $S=\sum_{x=0}^{p-1}\left(\frac{x^2}{p}\right)=p-1$.

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

Nếu $S=-1$ thì $D\not\vdots p$ và $\sum_{x=0}^{p-1}\left(\frac{ax^2+bx+c}{p}\right)=-\left(\frac{a}{p}\right)$.

Bổ đề 2 được chứng minh.

Trở lại bài toán.

Giả sử rằng tồn tại số nguyên x_0 sao cho:

$f(x_0), f(x_0+1),...,f\left(x_0+\frac{p+1}{2}\right)$ đều là số chính phương. Xét các khả năng sau:

1) a chia hết cho p.

Nếu b không chia hết cho p thì tập $\left\{bx+c:\ x=x_0,x_0+1,...,x_0+\frac{p+3}{2}\right\}$ là một hệ thặng dư không đầy đủ modulo p gồm $\frac{p+5}{2}$ phần tử mà

$f(x) \equiv bx + c \pmod p$ nên tập $\left\{ f(x) :\ x = x_0, x_0 + 1, \ldots, x_0 + \frac{p+3}{2} \right\}$ cũng là một hệ thặng dư không đầy đủ modulo p gồm $\frac{p+5}{2}$ phần tử nhưng rõ ràng một số chính phương chỉ có thể đồng dư với đúng một số trong $\frac{p+1}{2}$ số là $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$. Như vậy ta có điều mâu thuẫn.

Do đó b chia hết cho p. Vậy $p \mid b^2 - 4ac$.

2) a chia hết cho p.

Giả sử rằng: p không chia hết $b^2 - 4ac$.

Khi đó theo bổ đề 2, ta có: $\sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right) = -\left(\frac{a}{p} \right)$.

Suy ra: $\sum_{x=x_0}^{x_0+p-1} \left(\frac{ax^2 + bx + c}{p} \right) = \sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right) = -\left(\frac{a}{p} \right) \le 1$.

Mặt khác dễ dàng thấy rằng không tồn tại 3 số nguyên phân biệt $x_1, x_2, x_3 \in \{x_0, x_0 + 1, \ldots, x_0 + p - 1\}$ sao cho $(ax_i^2 + bx_i + c) \vdots p \forall i = 1,2,3$ nên $\sum_{x=x_0}^{x_0+p-1} \left(\frac{ax^2 + bx + c}{p} \right) \ge \left(\frac{p+5}{2} - 2 \right) - \left(p - \frac{p+5}{2} \right) = 3 > 1$. Mâu thuẫn.

Chú ý rằng: Đây là một mở rộng khá mạnh của bài IMO Shortlist năm 1991 do Polish đề nghị như sau:

Cho a, b, c là các số nguyên và p là một số nguyên tố lẻ. Chứng minh rằng nếu $f(x) = ax^2 + bx + c$ là số chính phương tại $2p - 1$ giá trị nguyên liên tiếp của x thì $p \mid (b^2 - 4ac)$.

Bài toán 15. Với mỗi số nguyên a, hãy tính số nghiệm (x, y, z) của phương trình đồng dư: $x^2 + y^2 + z^2 \equiv 2axyz \pmod p$

Lời giải:

Ta có :

$x^2+y^2+z^2\equiv 2axyz\pmod p\Leftrightarrow (z-axy)^2\equiv (a^2x^2-1)y^2-x^2\pmod p$ (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 (1) là: $1+\left(\frac{(a^2x^2-1)y^2-x^2}{p}\right)$.

Do vậy số nghiêm của phương trình $x^2+y^2+z^2\equiv 2axyz\pmod p$ là:

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

Xét các khả năng sau:

1) a chia hết cho p.

Khi đó áp dụng bổ đề 2 Bài 14 ta có:

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

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

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

2) a không chia hết cho p.

Dễ thấy tồn tại duy nhất các số nguyên $x_1,x_2\in\{1,2,...,p-1\}$ sao cho:

$$\begin{cases}ax_1\equiv 1\pmod p\\ ax_2\equiv -1\pmod p\end{cases}\Rightarrow p\mid a^2x_1^2-1,\ p\mid a^2x_2^2-1$$

Do vậy p không chia hết $4x^2(a^2x^2-1)$ $\forall x\in\{0,1,...,p-1\}\setminus\{0,x_1,x_2\}$

Từ đó áp dụng bổ đề 2 Bài 14, với chú ý $\left(\frac{\alpha}{p}\right)=0$ nếu $\alpha\vdots p$, ta được:

$$N = p^2 + \sum_{y=0}^{p-1}\left(\frac{-y^2}{p}\right) + \sum_{y=0}^{p-1}\left(\frac{\left(a^2x_1^2-1\right)y^2 - x_1^2}{p}\right) + \sum_{y=0}^{p-1}\left(\frac{\left(a^2x_2^2-1\right)y^2 - x_2^2}{p}\right)$$

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

$$= p^2 + p\left(\frac{-1}{p}\right) + 2p\left(\frac{-1}{p}\right) - \sum_{x=0}^{p-1}\left(\frac{a^2x^2-1}{p}\right) = p^2 + 3p\left(\frac{-1}{p}\right) + \left(\frac{a^2}{p}\right)$$

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

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

Bài toán 16. 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 $p \mid \left(r^2 + r + 1\right)$.

Chứng minh: p là một số nguyên tố có dạng $3k+1$ nên $p \equiv 1 \left(\mod 6\right)$, suy ra -3 là số chính phương $\mod p$, hay tồn tại số nguyên dương x sao cho: $\left(x + kp\right)^2 \equiv -3 \left(\mod p\right)\ \forall k \in \mathbb{N}$.

Rõ ràng tồn tại $k \in \mathbb{N}$ sao cho: $x + kp = 2r + 1$, với r nguyên dương nào đó. Suy ra: $p \mid \left(2r+1\right)^2 + 3 = 4\left(r^2 + r + 1\right) \Rightarrow p \mid \left(r^2 + r + 1\right)$.

Trở lại bài toán.

Với mỗi số nguyên dương n, rõ ràng tồn tại các số nguyên tố đôi 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: $p_i \mid \left(r_i^2 + r_i + 1\right)\ \forall i = 0, 1, ..., n$.

Theo định lý thặng dư Trung Hoa, tồn tại số nguyên dương a thỏa mãn: $a \equiv r_i \left(\mod p_i\right)\ \forall i = 0,1,...,n$

Suy ra: $p_0 p_1 ... p_n \mid \left(a^2 + a + 1\right)$

Với mỗi $i : 1 \le i \le n$, 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 $k_0 k_1 ... k_n - 1 = a^2 + a = a\left(a + 1\right)$

Nhận xét: Bằng các tính chất của Thặng dư bình phương và định lý Thặng dư Trung Hoa ta đã cho một lời giải đẹp với bài toán trên. Tuy nhiên dễ dàng nhận thấy ý tưởng trên chỉ nhằm mục đích đưa về kết quả sau:

Đặt $f\left(x\right) = x^2 + x + 1$. Khi đó tồn tại vô hạn số nguyên tố p sao cho phương trình đồng dư: $f\left(x\right) \equiv 0 \left(\mod p\right)$ có nghiệm.

Ta chứng minh kết quả này.

Giả sử ta đã có m số nguyên tố thỏa mãn là: $p_1, p_2, ..., p_m$.

Theo định lý Thặng dư Trung Hoa ta tìm được số nguyên dương b sao cho: $f\left(b\right) \equiv 0 \left(\mod p_i\right)\ \forall i = 1,2,...,m$.

Ta có: $\gcd\left(f\left(b\right), f\left(b+1\right)\right) = \gcd\left(b^2 + b + 1, b^2 + 3b + 3\right) = 1$

Mà $f\left(b+1\right) > 1$ nên nó có một ước nguyên tố p_{m+1} mà $p_{m+1} \ne p_i\ \forall i = 1,2,...,m$. Đpcm.

Ta có kết quả tổng quát: Cho đa thức hệ số nguyên $f\left(x\right)$ khác hằng số. Khi đó tồn tại vô hạn số nguyên tố p sao cho phương trình đồng dư: $f\left(x\right) \equiv 0 \left(\mod p\right)$ có nghiệm.

Hiển nhiên với kết quả này bài toán ban đầu của ta có thể được mở rộng thành tích của k số nguyên liên tiếp, với k là số nguyên dương tùy ý.

Bài toán 17. Cho các số nguyên dương m,n thoả mãn: $A=\dfrac{(m+3)^n+1}{3m}$ là số nguyên. Chứng minh rằng A lẻ.

Lời giải:

Nếu m lẻ thì $(m+3)^n+1$ lẻ, suy ra A lẻ.

Nếu m chẵn thì do A là số nguyên nên

$0\equiv(m+3)^n+1\equiv m^n+1\pmod 3\Rightarrow \gcd(m,3)=1$

suy ra: $n=2k+1,\ m\equiv -1\pmod 3$.

Ta xét các khả năng sau:

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

$(m+3)^n+1\equiv 3^n+1=3^{2k+1}+1\equiv 4\pmod 8$ và $3m_1\equiv 0\pmod 8$. mâu thuẫn với A là số nguyên.

2) $m=8m_1+2\ \vee\ 8m_1+6$, hay $m\equiv 2\pmod 4$. Khi đó ta có:

$(m+3)^n+1\equiv(2+3)^n+1\equiv 2\pmod 4$ và $3m\equiv 2\pmod 4$. Suy ra A lẻ.

3) $m=8m_1+4$. Khi đó do $m\equiv -1\pmod 3$ nên $m_1\equiv -1\pmod 3$, suy ra tồn tại số nguyên tố p là ước của m_1 sao cho $p\equiv -1\pmod 3$. Do A là số nguyên nên

$0\equiv(m+3)^n+1\equiv 3^n+1=3^{2k+1}+1\pmod m\Rightarrow 3^{2k+1}\equiv -1\pmod p$

hay $-3\equiv(3^{k+1})^2\pmod p\Rightarrow\left(\dfrac{-3}{p}\right)=1\Rightarrow p\equiv 1\pmod 6$, mâu thuẫn.

Bài toán 18. Chứng minh rằng không tồn tại các số nguyên dương a,b,c sao cho $\dfrac{a^2+b^2+c^2}{3(ab+bc+ca)}$ là một số nguyên.

Lời giải:

Giả sử rằng tồn tại các số nguyên dương a,b,c,n sao cho :

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

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

Ta có :

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

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

$\Leftrightarrow p \mid (ab+(-a-b)(a+b))$ $(\text{do } p \mid (a+b+c))$

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

Mâu thuẫn.

Nhận xét : Đây là một bài toán khá cũ nhưng vừa rồi nó lại xuất hiện trong kỳ thi Iran TST 2013 : Tìm tất các số nguyên dương a,b,c thỏa mãn :

$a^2+b^2+c^2$ chia hết cho $2013(ab+bc+ca)$.

Bài toán 19. 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 các khả năng sau:

1) n chẵn. Ta có

$-1 \equiv \left(a^{\frac{n}{2}}\right)^2 \pmod{p_i}$ $\forall i = \overline{1,k} \Rightarrow \left(\frac{-1}{p_i}\right) = 1$ $\forall i = \overline{1,k} \Rightarrow \left(\frac{-1}{3}\right) = 1$. Vô lý.

2) n lẻ.

Giả sử tồn tại $i \in \{1,2,...,k\}$ sao cho $p_i \mid n$.

Khi đó ta có: $p_i \mid a^n+1 = \left(a^{\frac{n}{p_i}}\right)^{p_i}+1$

Mà theo định lý nhỏ Fecma ta có: $p_i \mid \left(a^{\frac{n}{p_i}}\right)^{p_i} - a^{\frac{n}{p_i}} \Rightarrow p_i \mid a^{\frac{n}{p_i}} + 1$

Do đó: $v_{p_i}\left(a^n + 1\right) = v_{p_i}\left(\left(a^{\frac{n}{p_i}}\right)^{p_i} + 1\right) = v_{p_i}\left(a^{\frac{n}{p_i}} + 1\right) + v_{p_i}\left(p_i\right) \geq 2 \Rightarrow p_i^2 \mid a^n + 1$

Suy ra: $p_i^2 \mid p_1 p_2 ... p_k$. 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 $a = 2^m, m \in \mathbb{N}^* \Rightarrow p_1 p_2 ... p_k = 2^{mn} + 1$

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

Nếu m lẻ, ta có: $2x^2 + 1 \equiv 0 \left(\mathrm{mod}\, 5\right)$ (vì dễ thấy $k \geq 2$), với $x = 2^{\frac{mn-1}{2}}$

Suy ra: $x^2 \equiv 2 \left(\mathrm{mod}\, 5\right) \Rightarrow \left(\frac{2}{5}\right) = 1$. Vô lý.

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

Suy ra: $p_1 p_2 ... p_k = a^n + 1 > p_k^{p_k}$. Vô lý.

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

Bài toán 20. Cho số nguyên dương a. Xét dãy số nguyên $\left\{x_n\right\}$ xác định bởi: $x_1 = a, \ x_{n+1} = 2x_n + 1 \ \forall n \geq 1$. 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 phải là số nguyên tố.

Nhận xét 2: Nếu p là số nguyên tố có dạng $4m + 3$ và $q = 2p + 1$ cũng là một số nguyên tố thì $q \mid 2^p - 1$.

Chứng minh:

Theo định lý nhỏ Fecma ta có: $q \mid 2^{q-1}-1=2^{2p}-1=\left(2^p-1\right)\left(2^p+1\right)$

Gọi $\alpha=\text{ord}_q(2) \Rightarrow \alpha \mid 2p \Rightarrow \alpha \in \{2,p,2p\}$.

Nếu $\alpha=2 \Rightarrow q \mid 2^2-1=3 \Rightarrow q=3 \Rightarrow p=1$. Vô lý.

Nếu $\alpha=2p \Rightarrow q \not| 2^p-1 \Rightarrow q \mid 2^p+1 \Rightarrow -2 \equiv \left(2^{\frac{p+1}{2}}\right)^2 \pmod q$ hay $\left(\frac{-2}{q}\right)=1$

nhưng $q=2p+1=8m+7$. Vô lý.

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

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 $k \geq 3$ sao cho tồn tại $a \in \mathbb{N}^*$ thỏa mãn $y_1, y_2, \ldots, y_k$ đều là số nguyên tố. Khi đó theo nhận xét 1 ta có $x_1, x_2, \ldots, x_k$ cũng là số nguyên tố. Nói riêng y_3 là số nguyên tố nên theo trên ta có: $a \geq 3$ mà $a=x_1$ nguyên tố nên a lẻ, suy ra $x_n \equiv 3 \pmod 4 \ \forall n \geq 2$.

Ta có: $x_2 \equiv 3 \pmod 4, x_3=2x_2+1$, x_2, x_3 nguyên tố nên theo nhận xét 2 ta có: $x_3 \mid 2^{x_2}-1$ nhưng $2^{x_2}-1=y_2$ là số nguyên tố nên $x_3=2^{x_2}-1 \Rightarrow 4a+3=2^{2a+1}-1$. Vô lý vì $a \geq 3$.

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

Bài toán 21: Cho dãy $\{u_n\}_{n=1}^{+\infty}$ 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 với mọi $n \geq 3$.

Lời giải:

Trước tiên bằng quy nạp ta chứng minh được rằng: với mỗi số nguyên dương n ta có: $u_{n+2k}=-(-5)^k u_n+u_{n+k}u_k \ \forall k \in \mathbb{N}^*$.

Tiếp tục ta chứng minh bằng quy nạp các kết quả sau:

$u_{6k+2}=u_{6k+4} \equiv -1 \pmod 4, u_{6k} \equiv 2 \pmod 4 \ \forall k \in \mathbb{N}$.

Với $k=0$, dễ thấy đúng

Giả sử đúng với k. Xét với $k+1$, ta có:

$u_{6(k+1)} = u_{6k+6} = 11u_{6k+4} - 25u_{6k+2} \equiv -11 + 25 \equiv 2 \pmod 4$

$u_{6(k+1)+2} = u_{6k+8} = 11u_{6k+6} - 25u_{6k+4} \equiv 11.2 + 25 \equiv -1 \pmod 4$

$u_{6(k+1)+4} = u_{6k+10} = 11u_{6k+8} - 25u_{6k+6} \equiv -11 - 25.2 \equiv -1 \pmod 4$

Như vậy kết quả trên cũng đúng với $k+1$.

Do đó u_{2n} không là số chính phương với mọi $n \in \mathbb{N}^*$.

Ta sẽ chứng minh u_{4n+1} không là số chính phương với mọi $n \in \mathbb{N}^*$.

Thật vậy giả sử tồn tại $m \in \mathbb{N}^*, m \equiv 1 \pmod 4$ sao cho u_m là số chính phương.

Đặt $m = 1 + 3^r.2k,\ r \in \mathbb{N}, k \in \mathbb{N}^*, 2 \mid k, 3 \not\mid k$. Ta có:

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

$\equiv -(-5)^{3^r k} \pmod{u_k}$

Gọi p là một ước nguyên tố bất kỳ của $u_k \Rightarrow (p,5) = 1$

(vì $(u_n, 5) = 1\ \forall n \in \mathbb{N}^*$)

Ta có: $u_m \equiv -(-5)^{3^r k} \pmod p$ mà k chẵn, u_m là số chính phương nên $\left(\frac{-1}{p}\right) = 1 \Rightarrow p \equiv 1 \pmod 4 \Rightarrow u_k \equiv 1 \pmod 4$. Vô lý vì k chẵn nên $u_k \equiv 1, 2 \pmod 4$.

Ta sẽ chứng minh u_{4n+3} không là số chính phương với mọi $n \in \mathbb{N}$

Thật vậy giả sử tồn tại $m \in \mathbb{N}^*, m \equiv 3 \pmod 4$ sao cho u_m là số chính phương.

Đặt $m = 3 + 3^r.2k,\ r \in \mathbb{N}, k \in \mathbb{N}^*, 2 \mid k, 3 \not\mid k$. Ta có:

$u_m = u_{3+3^r.2k} \equiv -(-5)^k u_{3+(3^r-1).2k} \equiv (-5)^{2k} u_{3+(3^r-2).2k} \equiv ... \equiv -(-5)^{3^r k} u_3$

$\equiv -16.(-5)^{3^r k} \pmod{u_k}$

Gọi p là một ước nguyên tố bất kỳ của $u_k \Rightarrow (p,5) = 1, (p,2) = 1$

(vì $(u_n,5)=1\ \forall n\in\mathbb{N}^*$ và $2\mid k,3\not\mid k\Rightarrow k\equiv 2,4(\mathrm{mod}\,6)\Rightarrow u_k$ lẻ)

Ta có: $u_m\equiv -16.(-5)^{3^r k}(\mathrm{mod}\,p)$ mà k chẵn, u_m là số chính phương nên $\left(\frac{-1}{p}\right)=1\Rightarrow p\equiv 1(\mathrm{mod}\,4)\Rightarrow u_k\equiv 1(\mathrm{mod}\,4)$. Vô lý vì k chẵn nên $u_k\equiv 1,2(\mathrm{mod}\,4)$.

Vậy u_n không là số chính phương với mọi $n\geq 3$.

Bài toán 22. Cho hai hàm số $f,g:\mathbb{N}^*\to\mathbb{N}^*$ thoả mãn đồng thời:

i) g là toàn ánh.

ii) $2f(n)^2=n^2+g(n)^2\ \forall n\in\mathbb{N}^*$

Chứng minh rằng nếu $|f(n)-n|\leq 2013\sqrt{n}\forall n\in\mathbb{N}^*$ thì f có vô số điểm bất động.

Lời giải:

Theo định lý Dirichlet, tồn tai dãy vô hạn các số nguyên tố (p_i) với p_i có dạng $8k+3$.

Vì g là toàn ánh nên ta tìm được dãy vô hạn các số nguyên dương $\{x_n\}_{n=1}^{\infty}$ 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 $p_n\equiv 3(\mathrm{mod}\,8)$ nên 2 là số không chính phương $\mathrm{mod}\,p_n$

Suy ra : $f(x_n)\equiv x_n\equiv 0(\mathrm{mod}\,p_n)$.

Do đó tồn tại 2 dãy vô hạn các số nguyên dương $\{a_n\}_{n=1}^{\infty},\{b_n\}_{n=1}^{\infty}$ sao cho : $\begin{cases}x_n=a_np_n\\ f(x_n)=b_np_n\end{cases}\ \forall n=1,2,\ldots$

Khi đó ta có : $2b_n^2p_n^2=a_n^2p_n^2+p_n^2\Rightarrow 2b_n^2=a_n^2+1\Rightarrow\frac{b_n}{a_n}=\frac{\sqrt{a_n^2+1}}{\sqrt{2}a_n}$

Để ý rằng $\lim x_n=+\infty$.

Theo giả thiết ta có :

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

Suy ra: $0 \le \lim\left|\frac{1}{\sqrt{2}}\sqrt{\frac{a_n^2+1}{a_n^2}}-1\right| \le \lim\frac{2013}{\sqrt{x_n}} = 0$

Do đó: $\lim\sqrt{\frac{a_n^2+1}{a_n^2}} = \sqrt{2} \Rightarrow \lim a_n = 1$

Mà (a_n) là dãy vô hạn gồm các số nguyên dương nên

$\exists N_0 \in \mathbb{N}^* : a_n = 1 \ \forall n \ge N_0 \Rightarrow b_n = 1 \ \forall n \ge N_0$.

Do vậy : $f(p_n) = f(x_n) = p_n \ \forall n \ge N_0$, tức là hàm f có vô số điểm bất động.

Bài toán 23. Cho p là một số nguyên tố lẻ và đặt: $f(x) = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)x^{i-1}$

a) Chứng minh rằng $f(x)$ chia hết cho $(x-1)$ nhưng không chia hết cho $(x-1)^2$ nếu và chỉ nếu $p \equiv 3 \pmod 4$.

b) Chứng minh rằng nếu $p \equiv 5 \pmod 8$ thì $f(x)$ chia hết cho $(x-1)^2$ nhưng không chia hết cho $(x-1)^3$.

Lời giải:

a) Do $f(x) = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)x^{i-1}$ nên $f(1) = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right) = 0$ (Với p là một số nguyên tố lẻ thì trong tập $S = \{1,2,...,p-1\}$ có $\frac{p-1}{2}$ số chính phương $\bmod p$ và $\frac{p-1}{2}$ số không chính phương $\bmod p$ –Bổ đề bài 5a). Suy ra $f(x)$ chia hết cho $(x-1)$.

Ta có:

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

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

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

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 $\left(\frac{i}{p}\right)\equiv 1(\mathrm{mod}\,2)\ \forall i=1,2,...,p-1$,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 $f(x)\not\vdots(x-1)^2$.

Như vậy $f(x)$ chia hết cho $(x-1)$ nhưng không chia hết cho $(x-1)^2$ nếu và chỉ nếu $p\equiv 3\ (\mathrm{mod}\,4)$.

b) Ta nhận thấy rằng :

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

$$=\sum_{i=1}^{p-1}i^2\left(\frac{i}{p}\right)-3\sum_{i=1}^{p-1}i\left(\frac{i}{p}\right)+2f(1)=\sum_{i=1}^{p-1}i^2\left(\frac{i}{p}\right)-3\sum_{i=1}^{p-1}i\left(\frac{i}{p}\right)\ (\text{do } f(1)=0)$$

Giả sử rằng $p\equiv 5(\mathrm{mod}\,8)$. Khi đó theo câu a) ta có : $f(x)\vdots(x-1)^2$ và $\sum_{i=1}^{p-1}i\left(\frac{i}{p}\right)=f'(1)=0$

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

Mặt khác do $p\equiv 5(\mathrm{mod}\,8)$ nên $\left(\frac{2}{p}\right)=-1$, $\left(\frac{-1}{p}\right)=1$. Khi đó :

$$\begin{cases}\sum_{i=1}^{\frac{p-1}{2}}(2i)^2\left(\frac{2i}{p}\right)=4\left(\frac{2}{p}\right)\sum_{i=1}^{\frac{p-1}{2}}i^2\left(\frac{i}{p}\right)\equiv -4\sum_{i=1}^{\frac{p-1}{2}}i^2\equiv -4\sum_{i=1}^{\frac{p-1}{2}}i=-4\frac{p^2-1}{8}\equiv -4\pmod 8\\ \sum_{i=1}^{\frac{p-1}{2}}(2i-1)^2\left(\frac{2i-1}{p}\right)\equiv\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i-1}{p}\right)\pmod 8\end{cases}$$

Hơn nữa do $f(1)=0$ nên ta có :

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

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

Suy ra : $\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i-1}{p}\right)=0$.

Do đó : $\sum_{i=1}^{\frac{p-1}{2}}(2i-1)^2\left(\frac{2i-1}{p}\right)\equiv\sum_{i=1}^{\frac{p-1}{2}}\left(\frac{2i-1}{p}\right)=0\pmod 8$

Như vậy $f''(1)\equiv -4\pmod 8\Rightarrow f''(1)\neq 0\Rightarrow f(x)\not\vdots (x-1)^3$

Vậy nếu $p\equiv 5\pmod 8$ thì $f(x)$ chia hết cho $(x-1)^2$ nhưng không chia hết cho $(x-1)^3$.

IV. Bài tập tự luyện

Bài toán 1. Có tồn tại hay không một tam thức bậc hai $f(x)$ với hệ số nguyên sao cho với mỗi số tự nhiên n, tất cả các ước nguyên tố của $f(n)$ đều có dạng $4k+3$.

Bài toán 2. Cho cặp số nguyên dương (m,n) thỏa mãn: $\phi(5^m-1)=5^n-1$. Chứng minh rằng $\gcd(m,n)>1$.

Bài toán 3. Cho n,a là các số nguyên dương.

Chứng minh rằng: $(2a+3)^n+1 \vdots 6a \Leftrightarrow n$ lẻ và $a \mid \frac{3^n+1}{4}$.

Bài toán 4. Cho dãy $\{x_n\}$ được xác định bởi: $x_1=7$ và $x_{n+1}=2x_n^2-1 \ \forall n \geq 1$. Chứng minh rằng 2003 không chia hết bất kỳ số hạng nào của dãy trên.

Bài toán 5. Cho dãy số $\{L_i\}_{i=0}^{+\infty}$ được xác định như sau:

$$\begin{cases} L_0=2, L_1=1 \\ L_{n+2}=L_{n+1}+L_n, n=0,1,... \end{cases}$$

Chứng minh rằng với $n>1$ thì L_n là số chính phương khi và chỉ khi $n=3$.

Bài toán 6. Cho dãy số $\{x_n\}_{n=0}^{\infty}$ được xác định bởi: $\begin{cases} x_0=3 \\ x_{n+1}=2x_n^2-1 \end{cases}$.

chứng minh rằng với mỗi số nguyên dương n, nếu p là một ước nguyên tố của x_n thì $p \equiv 1 \pmod{2^{n+2}}$

Bài toán 7. Cho dãy số $\{x_n\}_{n=0}^{\infty}$ được xác định bởi: $\begin{cases} x_1=4 \\ x_{n+1}=x_n^2-2 \end{cases}$

Cho $n \geq 3$, n lẻ, chứng minh rằng $x_{n-1} \vdots 2^n-1 \Leftrightarrow 2^n-1$ là số nguyên tố.

Bài toán 8. Cho a,b là hai số nguyên dương nguyên tố cùng nhau và $\{a_n\},\{b_n\}$ là dãy các số nguyên dương thỏa mãn:

$\left(a+b\sqrt{2}\right)^{2n}=a_n+b_n\sqrt{2}$. Tìm tất cả các số nguyên tố p sao cho tồn tại số nguyên dương $n \leq p$ thỏa mãn b_n chia hết cho p

HOC247

Vững vàng nền tảng, Khai sáng tương lai

Website **HOC247** cung cấp một môi trường **học trực tuyến** sinh động, nhiều **tiện ích thông minh**, nội dung bài giảng được biên soạn công phu và giảng dạy bởi những **giáo viên nhiều năm kinh nghiệm, giỏi về kiến thức chuyên môn lẫn kỹ năng sư phạm** đến từ các trường Đại học và các trường chuyên danh tiếng.

I. Luyện Thi Online

Học mọi lúc, mọi nơi, mọi thiết bi – Tiết kiệm 90%

- **Luyên thi ĐH, THPT QG:** Đội ngũ **GV Giỏi, Kinh nghiệm** từ các Trường ĐH và THPT danh tiếng xây dựng các khóa **luyện thi THPTQG** các môn: Toán, Ngữ Văn, Tiếng Anh, Vật Lý, Hóa Học và Sinh Học.
- **Luyện thi vào lớp 10 chuyên Toán:** Ôn thi **HSG lớp 9** và **luyện thi vào lớp 10 chuyên Toán** các trường *PTNK, Chuyên HCM (LHP-TĐN-NTH-GĐ), Chuyên Phan Bội Châu Nghệ An* và các trường Chuyên khác cùng *TS.Trần Nam Dũng, TS. Pham Sỹ Nam, TS. Trịnh Thanh Đèo và Thầy Nguyễn Đức Tấn.*

II. Khoá Học Nâng Cao và HSG

Học Toán Online cùng Chuyên Gia

- **Toán Nâng Cao THCS:** Cung cấp chương trình Toán Nâng Cao, Toán Chuyên dành cho các em HS THCS lớp 6, 7, 8, 9 yêu thích môn Toán phát triển tư duy, nâng cao thành tích học tập ở trường và đạt điểm tốt ở các kỳ thi HSG.
- **Bồi dưỡng HSG Toán:** Bồi dưỡng 5 phân môn **Đại Số, Số Học, Giải Tích, Hình Học** và **Tổ Hợp** dành cho học sinh các khối lớp 10, 11, 12. Đội ngũ Giảng Viên giàu kinh nghiệm: *TS. Lê Bá Khánh Trình, TS. Trần Nam Dũng, TS. Pham Sỹ Nam, TS. Lưu Bá Thắng, Thầy Lê Phúc Lữ, Thầy Võ Quốc Bá Cẩn* cùng đôi HLV đạt thành tích cao HSG Quốc Gia.

III. Kênh học tập miễn phí

HOC247 NET cộng đồng học tập miễn phí
HOC247 TV kênh Video bài giảng miễn phí

- **HOC247 NET:** Website hoc miễn phí các bài học theo **chương trình SGK** từ lớp 1 đến lớp 12 tất cả các môn học với nội dung bài giảng chi tiết, sửa bài tập SGK, luyện tập trắc nghiệm mễn phí, kho tư liệu tham khảo phong phú và cộng đồng hỏi đáp sôi động nhất.
- **HOC247 TV:** Kênh **Youtube** cung cấp các Video bài giảng, chuyên đề, ôn tập, sửa bài tập, sửa đề thi miễn phí từ lớp 1 đến lớp 12 tất cả các môn Toán- Lý - Hoá, Sinh- Sử - Địa, Ngữ Văn, Tin Học và Tiếng Anh.