BỔ ĐỀ VỀ TỔNG BÌNH PHƯƠNG VÀ SỐ NGUYÊN TỐ

(Nguyễn Đăng Khải Hoàn-11 Toán,Chuyên Lương Thế Vinh,Đồng Nai)

Số nguyên tố từ lâu đã trở thành một vấn đề quan trọng và hấp dẫn trong lí thuyết số.Những tính chất và định lí về số nguyên tố luôn làm đóng vai trò cầu nối và thiết yếu trong việc giải toán số học nói riêng và toán học nói chung.Trong muôn vàn những tính chất đẹp đẽ và kì ảo ấy,có một bổ đề được phát biểu và chứng minh rất đơn giản nhưng lại có nhiều ứng dụng hay và hữu ích khi giải quyết các bài toán về phương trình nghiệm nguyên,các bài toán về số chính phương... Ngoài ra đây còn là một tính chất đẹp,là một viên ngọc sáng thể hiện mối liên giữa số chính phương và số nguyên tố-hai vấn đề thú vị của số học.

Trong bài viết nhỏ này,tôi xin được trình bày về bổ đề nêu trên.

I-BỔ ĐỀ VỀ TỔNG HAI BÌNH PHƯƠNG VÀ TRƯỜNG HỢP TỔNG QUÁT.

1.Bổ đề về tổng hai bình phương:

Cho p là số nguyên tố dạng $4k+3$.Khi đó:$x^2+y^2 \vdots p$ khi và chỉ khi $x \vdots p$ và $y \vdots p$.

***Chứng minh:**

Ta sẽ chứng minh bằng phản chứng.

Bỏ qua trường hợp đơn giản:Trong hai số x và y tồn tại một số chia hết cho p.Ta giả sử cả x và y đều không chia hết cho p.

Từ điều kiện giả sử,theo định lí Fermat nhỏ ta có:

$x^{p-1} \equiv 1(modp)$ và $y^{p-1} \equiv 1(modp)$

Suy ra:$x^{p-1}+y^{p-1} \equiv 2(modp)$

hay $x^{4k+2}+y^{4k+2} \equiv 2(modp)$

$\leftrightarrow (x^2)^{2k+1}+(y^2)^{2k+1} \equiv 2(modp).(*)$

Mặt khác: $(x^2)^{2k+1}+(y^2)^{2k+1} \vdots (x^2+y^2) \vdots p$.Mâu thuẫn với (*).

Vậy ta có đpcm.

***Hệ quả:**

+)Với mọi số nguyên x,k và k không có ước nguyên tố dạng $4k+3$ thì x^2+k^2 không có ước dạng $4k+3$.

+)Cho các số nguyên dương x,y thỏa $gcd(x,y)=1$, khi đó mọi ước nguyên tố của x^2+y^2 không có dạng $4k+3$.

Các hệ quả này ứng dụng nhiều trong chứng minh các bài toán vô nghiệm và không tồn tại trong số học.

2.Tổng quát:

Giả sử $p=k.2^t+1$ là một số nguyên tố,t là số nguyên dương và k là số tự nhiên lẻ.Giả thiết x và y là các số tự nhiên mà $(x^{2^t}+y^{2^t}) \vdots p$.Ta có đồng thời x và y chia hết cho p.

*Cách chứng minh trường hợp tổng quát hoàn toàn tương tự cách chứng minh bổ đề trên.

Một số trường hợp đặc biệt:

+)Với $t=1$ ta có ngay đây là trường hợp bổ đề ta nói đến.

+)Với $t=2$ thì ta có:Với số nguyên tố p có dạng $4k+1$ thì $x^4+y^4 \vdots p \leftrightarrow x \vdots p$ và $y \vdots p$.

II-MỘT SỐ ÁP DỤNG.

1-Các bài toán về phương trình nghiệm nguyên.

Ví dụ 1:Chứng minh các phương trình sau không có nghiệm nguyên dương.

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

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

***Lời giải:**

Đây là hai phương trình nghiệm nguyên khá nổi tiếng và được đề cập nhiều trong các tài liệu toán học.Đây cũng là các ví dụ "kinh điển" của việc ứng dụng bổ đề trên.

a)Ta viết lại phương trình dưới dạng:

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

Từ đẳng thức trên ta có:$(2y)^2 + 1$ phải có ước dạng $4k+3$,theo hệ quả của bổ đề trên thì điều này vô lí,nên ta có ngay phương trình vô nghiệm.

b)*Nếu y chẵn thì ta có:$x \equiv 3(mod 4)$,điều này vô lí vì $x \equiv 0, 1(mod 4)$.

Do đó y lẻ.

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

vì y lẻ nên $y^2 - 2y + 4 \equiv 3(mod 4)$.Theo hệ quả thì suy ra điều này vô lí.

Vậy ta có ngay phương trình vô nghiệm.

Nhận xét:

Từ hai ví dụ trên ta có thể nhận thấy rằng,để chứng minh một phương trình vô nghiệm nguyên thì ta có thể sử dụng hệ quả của bổ đề trên bằng cách:ở một vế tạo ra 2 tổng bình phương,thường là $x^2 + 1$,$x^2 + 4$...vế còn lại là một tích,xét các trường hợp theo modulo 4 để tìm ra điều mâu thuẫn hoặc vô lí.

Ở phương trình b),dạng tổng quát của nó là $x^2 = y^3 + k$ (trường hợp này $k = 7$),được gọi là phương trình Mordell.Nó có rất nhiều điều thú vị trong lớp bài toán Diophante,vì với mỗi k bất kì thì cách giải có thể sẽ khác nhau.Xin mời các bạn thử giải trong trường hợp $k = 16$ và $k = -4$.

Ví dụ 2:Giải phương trình nghiệm nguyên sau:$(x+y)^2 + 2 = 2x + 2013y$.

Lời giải:

Cũng hoàn toàn với tư tưởng như 2 bài toán trên ta sẽ đưa về tổng bình phương và áp dụng bổ đề.

PT $\Leftrightarrow (x + y - 1)^2 + 1 = 2011y$.

vì $2011 \equiv 3(mod 4)$ nên vô nghiệm theo hệ quả.

Ví dụ 3:Tìm các số nguyên (x, y) **sao cho** $\frac{x^2+1}{y^2-5}$ **cũng là số nguyên.**

Lời giải:

Giả sử tồn tại các số nguyên x, y sao cho $\dfrac{x^2+1}{y^2-5} \in Z$

Ta có: $y^2 \equiv 0, 1\ (mod\ 4) \Rightarrow y^2 - 5 \equiv 3, 0\ (mod\ 4)$

Nếu $y^2 - 5 \equiv 0\ (mod\ 4) \Rightarrow 4 \mid x^2 + 1 \Rightarrow x^2 \equiv 3\ (mod\ 4)$, điều này vô lí.

Nếu $y^2 - 5 \equiv 3\ (mod\ 4)$ thì $y^2 - 5$ có ít nhất một ước nguyên tố p có dạng $4k + 3$, suy ra $p \mid x^2 + 1$, điều này mâu thuẫn với hệ quả của bổ đề.

Kết luận : Không tồn tại số nguyên x, y nào thỏa mãn đề bài.

*Với những bài toán phương trình nghiệm nguyên như trên thì ta có thể chế biến ra rất nhiều bài toán tương tự bằng cách thay đổi số liệu nhưng không đổi các tính chất về modulo.Các kĩ thuật giải phương trình nghiệm nguyên như những ví dụ đã nêu cũng đã trở nên quen thuộc và tự nhiên trong lớp bài toán về phương trình nghiệm nguyên.

2-Các bài toán về số chính phương.

Ví dụ 1:Tìm các số nguyên dương a,b,c sao cho $a^2 = b^c - 3$. **với** $c \equiv 3(mod4)$
Lời giải:
Ta tiếp tục với cấu trúc một vế là 2 bình phương vế còn lại là tích.
Giả sử tồn tại các số nguyên dương a, b, c thỏa mãn.
Ta viết đẳng thức lại thành:$a^2 + 4 = (b + 1)(b^{c-1} - b^{c-2} + .. + b - 1)$.
*Nếu $b = 4k + 2$ thì $b + 1 = 4k + 3$, dễ có ngay điều vô lí theo bổ đề.
*Nếu $b = 4k + 1$ thì $b + 1 \equiv 2(mod4)$ và $(b^{c-1} - b^{c-2} + .. + b - 1) \equiv 1(mod4)$.
Từ đó $VT \equiv VP \equiv 2(mod4)$ hay $x^2 \equiv 2(mod4)$.Vô lí.
*Nếu $b = 4k + 3$ và $c \equiv 3(mod4)$ nên $(b^{c-1} - b^{c-2} + .. + b - 1) \equiv -1(mod4)$.
Theo bổ đề dễ có điều vô lí.
*Nếu $b = 4k$ thì $b^c \equiv 0(mod8)$.khi đó: $b^c - 3 \equiv -3(mod8)$,vô lí vì một scp chia 8 không có số dư là -3.
Vậy không tồn tại các số nguyên dương a, b, c thỏa mãn.

Ví dụ 2:Chứng minh rằng:không tồn tại số nguyên tố p sao cho:$3^p + 19(p - 1)$ **là số chính phương.**
Lời giải:
Tiếp tục phản chứng nào...
Giả sừ tồn tại số nguyên tố p thỏa mãn.
Đặt $3^p + 19(p - 1) = n^2$ (n là một số nguyên).
*Nếu $p = 2, 3$.Dễ có không có số nguyên n nào thỏa mãn.
*Nếu $p > 3$,p lẻ.
+)$p = 4k + 1$:
Ta có: $3 \equiv -1(mod4)$
nên $3^p \equiv -1(mod4)$.
và $19 \equiv 3(mod4); p - 1 \equiv 0(mod4)$
Do đó $VT \equiv VP \equiv -1(mod4)$(Vô lí!!)
+)$p = 4k + 3$:
Theo định lí Fermat ta có:
$3^p \equiv 3(modp)$.
và: $19(p - 1) \equiv -19(modp)$.
nên $VT \equiv -16(modp)$.
Do đó $n^2 + 16 \vdots p$.
Từ bổ đề,ta có:$4 \vdots p$. (vô lí vì 4 không có ước dạng $4k + 3$).
Vậy ta có đpcm.

Ví dụ 3:.Chứng minh rằng:Không tồn tại số tự nhiên n sao cho n^7+7 là số chính phương.

Giả sử tồn tại n thỏa mãn,khi đó $n^7+7=m^2$,với m là một số tự nhiên.

Ta có:$n^7+2^7=m^2+11^2$

$\rightarrow (n+2)(n^6-2n^5+4n^4-8n^3+16n^2-32n+2^6)=m^2+11^2$.

vì $m^2\equiv 0,1(mod4)$ và $11^2\equiv 1(mod4)$ nên ta suy ra $VP\equiv 1,2(mod4)$.

Lại có:$2^7\equiv 0(mod4)$ và $n^7\equiv 0,1,-1(mod4)$ nên $VT\equiv 0,1,-1(mod4)$.

Do đó $VT\equiv VP\equiv 1(Mod4)$ và $n\equiv 1(mod4)$.

Từ đó $n+2\equiv 3(mod4)$ nên $n+2$ sẽ có ước nguyên tố $p=4i+3$.

Theo bổ đề thì $11\vdots p$,nên $p=11,m=11k$

$\rightarrow VP\vdots 11^2$ nên $VT\vdots 11^2$.

Ta lại có:$n^6-2n^5+...+2^6\equiv 8(mod11)$ (vì $n\equiv -2(mod11)$).

nên $n+2\vdots 11^2\rightarrow n=11^2h-2$ và h là ước dương của k^2+1.

Suy ra $h\equiv 1(mod4)$,Vì vậy $n\equiv 3(mod4)$ (vô lí).

Vậy ta có đpcm.

3-Các bài toán về dãy số.

Ví dụ 1:Cho dãy số xác định như sau:$a_1=5,a_{n+1}=a_n^3-2a_n^2+2$**,với mọi** $n\geq 2$**.Cho** p **là số nguyên tố dạng** $4k+3$ **và** $a_{2011}+1\vdots p$**.Chứng minh rằng** $p=3$.

Ta có: $a_{n+1}-2=a_n^3-2a_n^2$

$=a_n^2(a_n-2)$

$=a_n^2.a_{n-1}^2.(a_{n-1}-2)$

$=...=a_n^2.a_{n-1}^2...a_2^2(a_1-2)$

$=t^2.3(t^2=a_n^2.a_{n-1}^2...a_2^2)$

Từ đó suy ra: $a_{n+1}+1=3t^2+3=3(t^2+1)$

Nếu $p=4k+3|a_{n+1}+1$ thì $3(t^2+1)\vdots p$ nên $3\vdots p$ hay $p=3$.

Vậy $p=3$.

Nhận xét:Từ công thức truy hồi của dãy số chúng ta tạo ra một qui trình lặp để đưa về đẳng thức $a_{n+1}-2=3.t^2$.Kĩ thuật này rất hay và được sử dụng nhiều trong các bài toán số học dãy số.Vì vậy cần chú ý đề thêm bớt vào 2 vế và biến đổi để có được các đẳng thức phù hợp.

Ví dụ 2:Cho dãy $\{u_n\}$ **thoả mãn** $u_1=2013,u_{n+1}=u_n^3-4u_n^2+5u_n\ \forall n\in\mathbb{N}^*$**. Tìm tất cả các số nguyên tố** p **là ước của** $(u_{2014}+2009)$ **và** $p\equiv 3\pmod 4$**.**

Lời giải:

Ta tiếp tục sử dụng kĩ thuật như ví dụ trên.

Ta có $u_{n+1}-2=u_n^3-4u_n^2+5u_n-2$

$=(u_{n-1}-1)^2(u_{n-1}-2)$

$=(u_{n-1}-1)^2.(u_{n-2}-1)^2.(u_{n-2}-1)=...=(u_{n-1}-1)^2.(u_{n-2}-1)^2....(u_2-1)^2.(u_1-2)$

$=(u_{n-1}-1)^2.(u_{n-2}-1)^2....(u_2-1)^2.2011.$

Từ đây, ta có: $u_{2014}-2=(u_{2013}-1)^2.(u_{2012}-1)^2....(u_2-1)^2.2011$

$\Leftrightarrow u_{2014}+2009=(u_{2013}-1)^2.(u_{2012}-1)^2....(u_2-1)^2.2011+2011$

$= 2011((u_{2013}-1)^2.(u_{2012}-1)^2....(u_2-1)^2+1)$.
Vì $((u_{2013}-1)^2.(u_{2012}-1)^2....(u_2-1)^2+1)$ có dạng a^2+b^2 với $(a,b)=1$ nên nó không có ước nguyên tố dạng $4k+3$. Vậy từ đó $p=2011$

4-Các dạng toán khác.

Ví dụ 1:Cho $T=(x,y)|x,y\epsilon\mathbb{N}, 0\leq 2x<y\leq 100, x^4+y^4\vdots 49$**.Tìm |T|.**
Lời giải:
Ta có: $x^4+y^4\vdots 49\rightarrow (x^2)^2+(y^2)^2\vdots 7$.
Theo bổ đề ta có: $x^2\vdots 7$ và $y^2\vdots 7$.
Suy ra:$x\vdots 7$ và $y\vdots 7$.
Đặt $x=7a, y=7b$,(a,b là các số tự nhiên).Ta có:$0\leq 14a<7b\leq 14$
Suy ra: $0\leq a\leq 6$.Khi đó:$b=14-2a$.
Số bộ (a,b) thỏa là:$\sum_{a=0}^{6}(14-2a)=56$.

Ví dụ 2:Tìm n **nguyên dương để tập** $\{n,n+1,n+2,n+3,n+4,n+5\}$ **có thể phân hoạch thành 2 tập** A **và** B **sao cho tích của tất cả các phần tử ở tập này bằng tích của tất cả các phần tử ở tập kia.**
Lời giải:
Giả sử tập ban đầu được phân hoạch thành hai tập A và B.
Trong 6 số nguyên liên tiếp thì tồn tại nhiều nhất một số chia hết cho 7.
Nếu trong 6 số $n,n+1,..,n+5$ có một số chia hết cho 7 thì khi lấy tích các phần tử của A và B sẽ có 1 tích chia hết cho 7, một tích không chia hết cho 7. Loại.
Do đó cả 6 số đều không chia hết cho 7.
Suy ra tích $P=n(n+1)..(n+5)\equiv 1.2.3.4.5.6\equiv 6(mod 7)$
Điều này vô lí vì P phải là số chính phương mà số chính phương chỉ chia 7 dư $0,1,2,4$.
Vậy không tồn tại n thỏa mãn.
Tổng quát:
Chứng minh rằng tồn tại vô số nguyên tố p thỏa mãn tính chất : Không tồn tại tập hợp gồm $p-1$ phần tử là $p-1$ số nguyên dương liên tiếp mà có thể chia tập này thành hai tập con, trong đó tích các phần tử của mỗi tập con là bằng nhau.

Ví dụ 3:.Chứng minh rằng với mọi số nguyên tố p **thì** $p^3+\frac{p-1}{2}$ **không là tích hai số tự nhiên liên tiếp.**
Lời giải:
Từ đề bài dễ có p lẻ.
Đặt $p^3+\frac{p-1}{2}=n(n+1)$.(n là số tự nhiên).
$+)p=4k+1$:Khi đó dễ có VT lẻ.(vô lí vì tích hai số liên tiếp luôn chẵn).
$+)p=4k+3$:
Từ đẳng thức ta biến đổi thành:
$4p^3+2p=(2n+1)^2+1$.
suy ra $(2n+1)^2+1\vdots p$.Vô lí theo hệ quả.
Vậy ta có đpcm.

III-Một số bài toán luyện tập.

Bài tập 1:Giải phương trình nghiệm nguyên: $x^{2002}+y^{2002}=2003^{2001}(x^3+y^3)$

Bài tập 2:Cho k là số nguyên dương cho trước.Tìm nghiệm nguyên dương của phương trình: $x^2+y^2=2011^{2003^k+1}(10-z)$.

Bài tập 3:Chứng minh rằng với mọi số nguyên tố p **thì** $7p+3^p-4$ **không là số chính phương.**

Bài tập 4:Tìm số nguyên dương n **sao cho luôn tồn tại số nguyên** m **thỏa mãn** $2^n-1 \mid m^2+9$.

Bài tập 5:Tìm số nguyên dương lẻ n **để** $n^{11}+199$ **là một số chính phương.**

Bài tập 6:Cho p **là số nguyên tố dạng** $4k+3$**.Cho** x,y,z,t **là các số nguyên dương thỏa:**$x^{2p}+y^{2p}+z^{2p}=t^{2p}$**.Chứng minh rằng ít nhất trong các số** x,y,z,t **chia hết cho** p.

IV-Hướng dẫn-Gợi ý

Bài tập 1:Giải phương trình nghiệm nguyên:$x^{2002}+y^{2002}=2003^{2001}(x^3+y^3)$

Gợi ý:

Nhận thấy rằng 2003 là số nguyên tố có dạng $4k+3$.

Áp dụng bổ đề ta suy ra $2003|x$ và $2003|y$.

Đặt $x=2003x_1, y=2003y_1$ và thay vào phương trình :

$2003^{2002}(x_1^{2002}+y_1^{2002})=2003^{2004}(x_1^3+y_1^3) \Leftrightarrow x_1^{2002}+y_1^{2002}=2003^2(x_1^3+y_1^3)$

Từ đây lại có $2003|x_1, 2003|y_1$. Đặt $x_1=2003x_2, y_1=2003y_2$, được :

$2003^{1997}(x_2^{2002}+y_2^{2002})=x_2^3+y_2^3$

Rõ ràng $VT \geq VP$ và đẳng thức chỉ xảy ra khi $x=y=0$

Phương trình có nghiệm nguyên duy nhất $(0,0)$.

Bài tập 2:Cho k là số nguyên dương cho trước.Tìm nghiệm nguyên dương của phương trình: $x^2+y^2=2011^{2003^k+1}(10-z)$.

Gợi ý:

Do $2011 \equiv 3(mod 4)$ nên theo bổ đề ta có:

$x=2011x_1$,$y=2011y_1$.(x_1, y_1 là các số nguyên dương.)

Vì 2003^k+1 là số chẵn nên đặt $2n=2003^k+1$.Từ đó ta có phương trình:

$x_1^2+y_1^2=2011^{2n-2}(10-z)$.

Lặp lại qui trình trên n lần ta đi đến được phương trình sau:

$x_n^2+y_n^2=10-z$.(với $x=2011^n x_n$ và $y=2011^n y_n$).(*)

Dễ có (*) có các nghiệm nguyên dương sau:$(x_n,y_n,z)=(1,1,8);(1,2,5);(2,1,5);(2,2,2)$.

Từ đó phương trình đã cho có các nghiệm nguyên dương là:

$(2011^n,2011^n,8);(2011^n,2.2011^n,5);(2.2011^n,2011^n,5);(2.2011^n,2.2011^n,2)$.

Bài tập 3:Chứng minh rằng với mọi số nguyên tố p thì $7p+3^p-4$ không là số chính phương.

Gợi ý:

Giả sử $7p+3^p-4$ là số chính phương. Khi đó:

$7p+3^p-4=x^2$

$\Leftrightarrow 7p+3^p-3=x^2+1$.

Dễ thấy với $p=2$ và $p=3$ không thỏa mãn.

TH1: $p \equiv 1(mod 4)$.

Ta có $3^p-3 \equiv 0(mod 4)$ và $7p \equiv 3(mod 4)$

$\Rightarrow 7p+3^p-3 \equiv 3(mod 4)$

Vì $7p+3^p-3 \equiv 3(mod 4)$ nên nó phải có 1 ước nguyên tố $q=4k+3$ nên $x^2+1 \vdots q$.

Áp dụng bổ đề có $1 \vdots q$ (vô lí).

TH2: $p \equiv 3(mod 4)$

Khi đó theo định lí Fermat nhỏ, ta có $7p+3^p-3 \vdots p \Rightarrow x^2+1 \vdots p$ và theo bổ đề có $1 \vdots p$ (vô lí).

Vậy ta có đpcm.

Bài tập 4:Tìm số nguyên dương n sao cho luôn tồn tại số nguyên m thỏa mãn $2^n - 1 \mid m^2 + 9$.

Gợi ý:

Nếu $n = 1$ thì hiển nhiên với mọi m đều thỏa mãn.

Nếu $n > 1$ thì $2^n - 1 \equiv 3 \ (mod\ 4)$, gọi p là ước nguyên tố dạng $4k + 3$ của $2^n - 1$ thì $p = 3$, tức là $3|2^n - 1$, suy ra n chẵn.

Gọi q là ước nguyên tố lẻ của n. Thì $2^q - 1|2^n - 1 \wedge 3 \nmid 2^q - 1$.

Nhưng rõ ràng điều này vô lí vì $2^q - 1|m^2 + 9 \wedge 2^q - 1 \equiv 3 \ (mod\ 4) \Rightarrow 3|2^q - 1$

Do đó n không có ước nguyên tố lẻ, $n = 2^k$. Bây giờ ta sẽ chứng minh với $n = 2^k$ thì luôn tồn tại số m thỏa mãn đề bài.

Thật vậy,

$$2^n - 1 = 3(2^{2^1} + 1)(2^{2^2} + 1)...(2^{2^{k-1}} + 1)$$

Xét hệ :

$$\begin{cases} x \equiv 3.2^{2^0} \ (mod\ 2^{2^1} + 1) \\ x \equiv 3.2^{2^1} \ (mod\ 2^{2^2} + 1) \\ \qquad ... \\ x \equiv 3.2^{2^{k-2}} \ (mod\ 2^{2^{k-1}} + 1) \end{cases}$$

Rõ ràng $gcd(2^{2^i} + 1, 2^{2^j} + 1) = 1 \ \forall i \neq j, i, j \in \{0, 1, 2, ..., k - 1\}$ vì chúng là các số $Fermat$

Theo định lí phần dư Trung Hoa thì hệ trên chắc chắn có nghiệm x_0

Khi đó

$$\begin{cases} x_0^2 \equiv 9.2^{2^1} \equiv -9 \ (mod\ 2^{2^1} + 1) \\ x_0^2 \equiv 9.2^{2^2} \equiv -9 \ (mod\ 2^{2^2} + 1) \\ \qquad ... \\ x_0^2 \equiv 2^{2^{k-1}} \equiv -9 \ (mod\ 2^{2^{k-1}} + 1) \end{cases} \Rightarrow x_0^2 + 9 \equiv 0 \ (mod\ 2^n - 1)$$

Kết luận : $n = 2^k$

Bài tập 5:Tìm số nguyên dương lẻ n để $n^{11} + 199$ là một số chính phương.

Gợi ý:

Đặt $n^{11} + 199 = m^2$, $m \in \mathbb{N}$

Vì n lẻ nên $n \equiv 1; 3(mod 4)$

Nếu $n \equiv 3(mod 4) \Rightarrow m^2 \equiv 3^{11} + 199 \equiv 2(mod 4)$ (vô lí) Do đó $n \equiv 1(mod 4)$

Ta có : $n^{11} + 199 = m^2 \Leftrightarrow n^{11} + 2^{11} = m^2 + 43^2 \Leftrightarrow (n + 2)(n^{10} - 2n^9 + ... - 512n + 1024) = m^2 + 43^2 \Leftrightarrow (n + 2).b = m^2 + 43^2$ $\quad (*)$ Vì $n \equiv 1(mod 4) \Rightarrow b = n^{10} - n^9.2 + ... - n.2^9 + 2^{10} \equiv 3(mod 4) \Rightarrow b$ có ít nhất một ước nguyên tố $p \equiv 3(mod 4)$.

Theo bổ đề thì $b|(a^2 + 43^2) \Rightarrow p|(a^2 + 43^2) \Rightarrow p|43 \Rightarrow p = 43 \Rightarrow 43|b$

Nếu $43|(n + 2) \Rightarrow n \equiv -2(mod 43) \Rightarrow b = n^{10} - 2n^9 + 4n^8 - 8n^7 + 16n^6 - 32n^5 + 64n^4 - 128n^3 + 256n^2 - 512n + 1024 \equiv 8(mod 43)$.

Điều này là vô lí vì $43|b$. Suy ra $43 \nmid (n + 2)$.

Ta có $a^2 + 43^2 = (n + 2).b \vdots 43 \Rightarrow a \vdots 43 \Rightarrow (a^2 + 43^2) \vdots 43^2 \Rightarrow b(n + 2) \vdots 43^2$. Vì $43 \nmid (n + 2)$ nên $b = 43^2.m$ $\quad (m \in \mathbb{N}, gcd(m, 2) = 1)$

Hơn nữa vì $a \vdots 43 \Rightarrow a = 43q \qquad (q \in \mathbb{N})$

Do đó $(n+2).b = a^2 + 43^2 = 43^2.(q^2+1) \Leftrightarrow (n+2).43^2.m = 43^2(q^2+1) \Leftrightarrow q^2+1 = m(n+2)$

Vì $gcd(1,q) = 1$ nện theo bổ đề thì q^2+1 không có ước nguyên tố nào có dạng $4k+3$, nhưng $n+2 \equiv 3(mod 4)$ (vì $n \equiv 1(mod 4)$)

Điều này mâu thuẫn.

Kết luận : Không tồn tại số n thỏa mãn đề bài.

Bài tập 6:Cho p là số nguyên tố dạng $4k+3$.Cho x,y,z,t là các số nguyên dương thỏa:$x^{2p}+y^{2p}+z^{2p}=t^{2p}$.Chứng minh rằng ít nhất trong các số x,y,z,t chia hết cho p.

Gợi ý:

Ta chứng minh bằng phản chứng,giả sử trong 4 số x,y,z,t không tồn tại số nào chia hết cho p. Không mất tính tổng quát,ta giả sử $gcd(x,y,z,t) = 1$.Khi đó cả 4 số x,y,z,t không thể cùng chẵn.Giả sử z lẻ.

Ta có:

$x^{2p}+y^{2p} = t^{2p}-z^{2p} = (t^2-z^2)\left(\frac{t^{2p}-z^{2p}}{t^2-z^2}\right)$

Chú ý rằng:$\frac{t^{2p}-z^{2p}}{t^2-z^2} = (t^2)^{p-1}+(t^2)^{p-2}(z^2)+\cdots+(z^2)^{p-1} \equiv p \equiv 3 \pmod 4$

Vì vậy tồn tại số nguyên tố $q \equiv 3(mod 4)$ sao cho:$q^{\text{lẻ}} \parallel \frac{t^{2p}-z^{2p}}{t^2-z^2}$.

Vì:$q|x^{2p}+y^{2p}$ và $q \equiv 3 \pmod 4$ nên ta có:$q^{\text{chẵn}} \parallel x^{2p}+y^{2p}$

Suy ra:$q|t^2-z^2$

Ta có:$\frac{t^{2p}-z^{2p}}{t^2-z^2} \equiv (t^2)^{p-1}+(t^2)^{p-2}(z^2)+\cdots+(z^2)^{p-1} \equiv (t^2)^{p-1}p \equiv 0 \pmod q$

Vì vậy:$q|pt$.

Nếu:$q=p$ thì ta có:$p|(x^p)^2+(y^p)^2$,suy ra $p|x,y$,vô lí với điều ta giả sử.

Do đó $q|t$,vì:$q|t^2-z^2$ nên $q|z$,và vì:$q|(x^p)^2+(y^p)^2$ nên $q|x,y$ vì vậy:$\gcd(x,y,z,t) \geq q > 1$,vô lí!

Vậy ta có đpcm.

Cuối cùng xin gửi tới mọi người bài toán sau,rất mong nhận được sự đóng góp ý kiến từ bạn đọc,bài toán này có liên quan đến số nguyên tố dạng $4k+3$,tác giả cũng chưa giải quyết hoàn toàn bài toán:

Bài toán:Tìm các bộ số (x,y) nguyên thỏa:$y^2 = x^3 - p^2x$ với p là số nguyên tố dạng $4k+3$.

Trên đây là bài viết về những ứng dụng của bổ đề tổng hai bình phương và số nguyên tố,rất mong bài viết này có thể giúp bạn đọc thêm yêu thích môn toán và nắm được những kĩ thuật cơ bản khi đối mặt với các bài toán số học.

Dù tác giả đã rất cố gắng trong quá trình làm việc,nhưng thiếu sót là điều khó tránh khỏi,rất mong nhận được những ý kiến đóng góp từ bạn đọc.

Mọi đóng góp xin được thảo luận tại:**http://forum.mathscope.org/showthread.php?t=46184** hoặc gửi về email:**Cuoichutdi@yahoo.com.vn.**

Xin chân thành cám ơn các thành viên diễn đàn **Mathscope.org** đã giúp đỡ tác giả hoàn thành bài viết,đặc biệt xin cám ơn các thành viên:**Juliel** và **Quocbaoct10** đã nhiệt tình đóng góp và ủng hộ tác giả hoàn thành chuyên đề nhỏ này.