

Trích và dịch từ bài chứng minh của bạn Phương về FLT

Bổ đề

Cho a chẵn, b lẻ. Nếu tồn tại các số nguyên e, f, g, h khác zero sao cho

$$2(fg + eh) = a(a - b)$$

$$2(eg - fh) = ab$$

$$e^2 + f^2 - g^2 - h^2 = b(a - b)$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab$$

Hoặc

$$2(fg + eh) = ab$$

$$2(eg - fh) = a(a - b)$$

$$e^2 + f^2 - g^2 - h^2 = b(a - b)$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab$$

, vậy thì tồn tại 2 số chẵn lẻ nguyên tố với nhau i, j để mà $i^2 + j^2$ là một ước số chung của a và b .

Chứng minh

Xét hệ sau

$$2(fg + eh) = a(a - b) \tag{0.1}$$

$$2(eg - fh) = ab \tag{0.2}$$

$$e^2 + f^2 - g^2 - h^2 = b(a - b) \tag{0.3}$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab \tag{0.4}$$

Cộng (0.3) & (0.4),

$$2(e^2 + f^2) = a^2 \tag{0.5}$$

Hay

$$(e + f)^2 + (e - f)^2 = a^2 \quad (0.6)$$

Giải (0.6) ,

$$e + f = k(i^2 - j^2) \quad (0.7)$$

$$e - f = k(2ij) \quad (0.8)$$

$$a = k(i^2 + j^2) \quad (0.9)$$

trong đó i, j là 2 số chẵn lẻ nguyên tố với nhau và $k = GCD(e + f, e - f)$.

Suy ra

$$e = \frac{k}{2}(i^2 - j^2 + 2ij) \quad (0.10)$$

$$f = \frac{k}{2}(i^2 - j^2 - 2ij) \quad (0.11)$$

Cộng (0.1) & (0.2) ,

$$2(e + f)g + 2(e - f)h = a^2 \quad (0.12)$$

Giải (0.12)

$$h = \frac{a^2 - 2(e + f)g}{2(e - f)} \quad (0.13)$$

Thay giá trị $e + f, e - f$ và a vào (0.13) ,

$$h = \frac{k(i^2 + j^2)^2 + 2(j^2 - i^2)g}{4ij} \quad (0.14)$$

Từ (0.2) ,

$$b = \frac{2(eg - fh)}{a} \quad (0.15)$$

Thay giá trị e, f, a và h vào (0.15) ,

$$b = \frac{(i^2 + j^2)(kj^2 + 2kij - ki^2 + 2g)}{4ij} \quad (0.16)$$

Bởi vì $GCD(i, j) = 1$ và i, j chẵn lẻ khác nhau nên $GCD(i^2 + j^2, 4ij) = 1$. Suy ra $kj^2 + 2kij - ki^2 + 2g = l(4ij)$, trong đó l là một số nguyên khác zero.

Vậy thì

$$b = l(i^2 + j^2) \quad (0.17)$$

nên $i^2 + j^2$ là một ước số chung của a và b .

Hệ sau cũng cho cùng kết quả.

$$2(fg + eh) = ab$$

$$2(eg - fh) = a(a - b)$$

$$e^2 + f^2 - g^2 - h^2 = b(a - b)$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab$$

Bổ đề được chứng minh.

Định lý

Với bất kỳ số tự nhiên $n > 2$, đường cong $x^n + y^n - 1 = 0$ không có điểm hữu tỷ khác zero.

Chứng minh

Rõ ràng chỉ cần chứng minh định lý cho 2 trường hợp sau:

1) n là một số lẻ lớn hơn 2.

2) $n = 4$.

Giả sử với bất kỳ số lẻ n lớn hơn 2 hay bằng 4, đường cong $(L): x^n + y^n - 1 = 0$ có một điểm hữu tỷ khác zero $M_0(x_0, y_0)$. Không mất tính tổng quát, giả sử $x_0 = \frac{a}{c}$, $y_0 = \frac{b}{c}$, trong đó a, b, c là những số nguyên khác zero và nguyên tố từng đôi.

Đặt $m = \frac{x_0}{y_0} = \frac{a}{b}$. Dễ thấy $m \neq 0, m \neq 1$ and $m \neq -1$.

Trong mặt phẳng Oxy , gọi (C) là vòng tròn tâm O đi qua $M_0(x_0, y_0)$. Vậy thì phương trình tiếp tuyến (δ) với (C) tại $M_0(x_0, y_0)$ là $y = -m(x - x_0) + y_0$. Ta cũng có phương trình tiếp tuyến (Δ) với (L) tại $M_0(x_0, y_0)$ là $y = -m^{n-1}(x - x_0) + y_0$.

Nếu (Δ) trùng với (δ) thì

$$-m^{n-1} = -m \quad (0.18)$$

Hay

$$m^{n-2} - 1 = 0 \quad (0.19)$$

Nghiệm hữu tỷ của (0.19) nếu có chỉ có thể là $m = 1$ hay $m = -1$. Vì điều kiện trên, (Δ) phải cắt (C) tại 2 điểm phân biệt $M_0(x_0, y_0)$ và $M_1(x_1, y_1)$ có các tọa độ là

$$x_1 = \frac{(m^{2n-2} - 1)x_0 + 2m^{n-1}y_0}{m^{2n-2} + 1} \quad (0.20)$$

$$y_1 = \frac{2m^{n-1}x_0 + (1 - m^{2n-2})y_0}{m^{2n-2} + 1} \quad (0.21)$$

Từ (0.20) & (0.21) và $y_0 \neq 0$,

$$\frac{x_1}{y_0} = \frac{m^{2n-1} + 2m^{n-1} - m}{m^{2n-2} + 1} \quad (0.22)$$

$$\frac{y_1}{y_0} = \frac{-m^{2n-2} + 2m^n + 1}{m^{2n-2} + 1} \quad (0.23)$$

Nếu $x_1 = 0$ thì $m^{2n-2} + 2m^{n-1} - m = 0$. Phương trình này không có nghiệm hữu tỷ.

Nếu $y_1 = 0$ thì $m^{2n-2} - 2m^n - 1 = 0$. Phương trình này không có nghiệm hữu tỷ.

Vì vậy $x_1 \neq 0$ and $y_1 \neq 0$.

Thay $m = \frac{a}{b}$ vào (0.22) & (0.23),

$$\frac{x_1}{y_0} = \frac{a(a^{2n-2} + 2a^{n-2}b^n - b^{2n-2})}{b(a^{2n-2} + b^{2n-2})} \quad (0.24)$$

$$\frac{y_1}{y_0} = \frac{-a^{2n-2} + 2a^n b^{n-2} + b^{2n-2}}{a^{2n-2} + b^{2n-2}} \quad (0.25)$$

Bởi vì $M_0(x_0, y_0)$ and $M_1(x_1, y_1)$ cùng ở trên (C) nên

$$x_1^2 + y_1^2 = x_0^2 + y_0^2 \quad (0.26)$$

Chia 2 vế (0.26) cho $y_0^2 \neq 0$,

$$\left(\frac{x_1}{y_0}\right)^2 + \left(\frac{y_1}{y_0}\right)^2 = \left(\frac{x_0}{y_0}\right)^2 + 1 \quad (0.27)$$

Thay giá trị $\frac{x_1}{y_0}$ và $\frac{y_1}{y_0}$ vào (0.27),

$$\left(\frac{ap}{bq}\right)^2 + \left(\frac{r}{q}\right)^2 = \left(\frac{a}{b}\right)^2 + 1 \quad (0.28)$$

trong đó dễ thấy $p = a^{2n-2} + 2a^{n-2}b^n - b^{2n-2}$, $q = a^{2n-2} + b^{2n-2}$ và $r = -a^{2n-2} + 2a^n b^{n-2} + b^{2n-2}$ là những số nguyên khác zero.

Bởi vì $(bq)^2 \neq 0$ từ (0.28) suy ra

$$(ap)^2 + (br)^2 = (a^2 + b^2)q^2 \quad (0.29)$$

Nhân cả 2 vế (0.29) với $a^2 + b^2 \neq 0$,

$$(a^2 + b^2)\{(ap)^2 + (br)^2\} = \{(a^2 + b^2)q\}^2 \quad (0.30)$$

Rồi cộng 2 vế (0.30) với $-2ab\{(ap)^2 + (br)^2\}$

$$(a^2 + b^2 - 2ab)\{(ap)^2 + (br)^2\} = \{(a^2 + b^2)q\}^2 - 2ab\{(ap)^2 + (br)^2\} \quad (0.31)$$

Từ (0.29) & (0.31),

$$(a-b)^2 \{(a^2 + b^2)q^2\} = \{(a^2 + b^2)q\}^2 - 2ab\{(a^2 + b^2)q^2\} \quad (0.32)$$

Hay

$$(a-b)^2 (a^2 + b^2)q^2 = \{(a^2 + b^2 - ab)q\}^2 - (ab)^2 q^2 \quad (0.33)$$

Bởi vì $q^2 \neq 0$ từ (0.33) chúng ta được

$$\{a(a-b)\}^2 + (ab)^2 + \{b(a-b)\}^2 = (a^2 + b^2 - ab)^2 \quad (0.34)$$

Bởi vì $GCD(a, b) = 1$ nên chỉ có 2 trường hợp sau:

a) a, b chẵn lẻ khác nhau.

b) a, b đều lẻ.

Xét trường hợp a và với bất kỳ n lẻ lớn hơn 2 hay bằng 4. Luôn giả sử được rằng a chẵn, b lẻ. Từ đây $a(a-b)$, ab chẵn còn $b(a-b)$, $a^2 + b^2 - ab$ lẻ. Vì vậy, từ (0.34) ta thấy bộ 4 $[a(a-b), ab, b(a-b), a^2 + b^2 - ab]$ là một nghiệm nguyên khác zero của phương trình $x^2 + y^2 + z^2 = w^2$. Hơn nữa do $GCD(b(a-b), a^2 + b^2 - ab) = 1$ nên $[a(a-b), ab, b(a-b), a^2 + b^2 - ab]$ là một bộ 4 nguyên thủy của phương trình $x^2 + y^2 + z^2 = w^2$. Nếu vậy thì sẽ tồn tại các số nguyên e, f, g, h khác zero sao cho

$$2(fg + eh) = a(a-b) \quad (0.35)$$

$$2(eg - fh) = ab \quad (0.36)$$

$$e^2 + f^2 - g^2 - h^2 = b(a-b) \quad (0.37)$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab \quad (0.38)$$

hay

$$2(fg + eh) = ab \quad (0.39)$$

$$2(eg - fh) = a(a-b) \quad (0.40)$$

$$e^2 + f^2 - g^2 - h^2 = b(a-b) \quad (0.41)$$

$$e^2 + f^2 + g^2 + h^2 = a^2 + b^2 - ab \quad (0.42)$$

Mặt khác từ bổ đề trên sẽ có $i^2 + j^2$ là một ước số chung của a và b . Điều này trái với giả thiết $GCD(a, b) = 1$.

Xét trường hợp b, nếu n là một số lẻ lớn hơn 2 thì từ $a^n + b^n = c^n$ chúng ta có $a^n = c^n + (-b)^n$. Đặt $A = c$, $B = -b$, $C = a$ thì $A^n + B^n = C^n$, trong đó A, B chẵn lẻ khác nhau. Điều này mâu thuẫn với trường hợp a.

Xét trường hợp b và với $n = 4$. Khi đó từ $a^4 + b^4 = c^4$ ta có c là số chẵn. Đặt $c = 2l$ với l là một số nguyên khác zero. Từ đây suy ra $\frac{a^4 + b^4}{2} = 8l^4$. Điều này vô lý vì $\frac{a^4 + b^4}{2}$ lẻ còn $8l^4$ chẵn.

Định lý được chứng minh.