TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA KHOA HỌC MÁY TÍNH

————-oOo————-

BÀI TẬP VỀ NHÀ
MÔN ĐẠI SỐ MÁY TÍNH

BÀI TẬP BUỔI 2
SỐ HỌC

Lớp: CS522.M11

Giảng viên giảng dạy: TS. Nguyễn Đình Hiển

Nhóm sinh viên thực hiện:

1. Phan Thanh Hải 18520705
2. Trần Ngọc Sương 18521353

TP. HỒ CHÍ MINH, 10/2021

Mục lục

Bài 1.

(a) (Định lí Wilson) Chứng minh rằng:

$$\forall p \text{ là số nguyên tố}, \big(p-1\big)! \equiv -1 \pmod{p}$$

(b) (Định lí Fermat nhỏ) Chứng minh rằng:

$$\forall p \text{ là số nguyên tố}, a \text{ là số nguyên sao cho } \big(a,p\big) = 1.$$

$$\text{Khi đó: } a^{p-1} \equiv 1 \pmod{p}$$

Bài làm:

(a) **Chứng minh định lí Wilson**

(1) Nếu $\big(p-1\big)! \equiv -1 \pmod{p}$ **thì** p **là số nguyên tố**

Ta có: $\big(p-1\big)! \equiv -1 \pmod{p}$

$\Rightarrow \big(p-1\big)! + 1 \equiv 0 \pmod{p}$ hay $\big(p-1\big)! + 1$ chia hết cho p.

$\Rightarrow 1.2.3.4.5....\big(p-1\big) + 1 \vdots p$

Vì khi đó p sẽ nguyên tố cùng nhau với các số $1, 2, 3, 4, 5, ...\big(p-1\big)$, nên không thể tồn tại ước k nào khác ngoài 1 và chính nó, hay nói cách khác, p là số nguyên tố.

Vậy ta chứng minh được mệnh đề (1).

(2) Nếu $p = 2$**:** dễ thấy được $\big(2-1\big)! = 1 \equiv -1 \pmod{2}$ (Đúng)

(3) Nếu p **là số nguyên tố** $\big(p > 2\big)$ **thì** $\big(p-1\big)! + 1$ **chia hết cho** p

Để chứng minh mệnh đề trên, trước tiên ta cần chứng minh: Cho $A = \{2, 3, 4, ..., p-2\}$.

$\forall a \in A$, tồn tại duy nhất $m \in A$ sao cho $m.a \equiv -1 \pmod{p}$(*)

(3.1) Xét dãy $a, 2a, 3a, 4a, ..., \big(p-1\big)a$, có thể thấy:

- Các số khác nhau từng đôi một.
- Không có hai số nào đồng dư theo module p.

$\big($Giả sử $\exists\ ma \equiv na \pmod{p}$ (với $n \in A$)

$\Rightarrow \big(m-n\big)a \equiv 0 \pmod{p}$

$\Rightarrow \big(m-n\big) \vdots p$ (Vì $a \not\vdots p$)

Vì $m, n < p$ nên để $\big(m - n\big) \vdots p$ thì $m = n$ (Điều này không đúng với điều kiện $m, n \in A$).

Do đó không tồn tại hai số nào trong dãy trên đồng dư theo module $p\big)$.

(3.2) Giả sử $\exists\, m$, $1 \leq m \leq p-1$ sao cho $ma \equiv 1 \pmod p$

- Nếu $m = 1$ thì $a = 1$ (Sai)
- Nếu $m = p-1$ thì: $m \equiv p-1 \equiv -1 \pmod p \Rightarrow a \equiv -1 \pmod p \Rightarrow a = p-1$ (Sai)

$\Rightarrow 1 < m < p-1$

Ta chứng minh được mệnh đề (*).

Chia tập A thành các cặp (a, m) sao cho $ma \equiv 1 \pmod p$

Ta có: $2.3.4....(p-2) \equiv 1 \pmod p$

$\Rightarrow (p-2)! \equiv 1 \pmod p$

$\Rightarrow (p-2)!(p-1) \equiv (p-1).1 \pmod p$

$\Rightarrow (p-1)! \equiv p-1 \equiv -1 \pmod p$ (đpcm)

Như vậy ta đã chứng minh được định định lí Wilson.

(b) **Chứng minh định lí Fermat nhỏ**

Xét dãy số $a, 2a, 3a, 4a, ..., (p-1)a$:

- Vì $a \not\vdots p$ nên các số trong dãy trên cũng không chia hết cho p
- Không tồn tại hai số nào đồng dư theo module p

Giả sử các số $a, 2a, 3a, 4a, ..., (p-1)a$ chia cho p được các số dư là $r_1, r_2, r_3, ..., r_{p-1}$.

Khi đó, $r_1, r_2, r_3, ..., r_{p-1}$ khác nhau đôi một. (*)

$\big($Giả sử $\exists\, r_i = r_j$ $(1 \leq i \leq j \leq p-1)$

Ta có $ia \equiv ij \pmod p \Leftrightarrow a(i-j) \equiv 0 \pmod p$

Điều này không hợp lý vì $a \not\vdots p$, $i - j \not\vdots p$.

Do đó ta chứng minh được (*)$\big)$.

Từ (*) suy ra các số dư lần lượt là $1, 2, 3, 4, ..., p-1$

Hay $r_1.r_2.r_3....r_{p-1} = (p-1)!$

$\Rightarrow a.2a.3a.4a....(p-1)a \equiv (p-1)! \pmod p$

$\Rightarrow a^{p-1}.(p-1)! \equiv (p-1)! \pmod{p}$

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$ (đpcm)

Như vậy ta đã chứng minh được định lí Fermat nhỏ.

Bài 2.

Dễ thấy rằng: $\lim\limits_{n\to\infty} \dfrac{\log n}{n^\alpha} = 0, \forall\, \alpha > 0.$

Nghĩa là: $\forall\, \alpha > 0, \exists\, N_\alpha > 0$ sao cho: $\log n < n^\alpha, \forall\, n > N_\alpha$.

Cho $\alpha = 10^{-4}$, hãy tìm giá trị của N_α.

Bài làm:

Giả sử $\log n$ là logarit cơ số e.

$\forall\, \alpha > 0$, ta có: $\log n < n^\alpha$

$\Leftrightarrow n^{-\alpha} \log n < 1$ (nhân cả 2 vế với $n^{-\alpha} > 0$ nên không thay đổi chiều BĐT)

$\Leftrightarrow n^{-\alpha} \log\left(n^{-\alpha}\right) > -\alpha$ (nhân cả 2 vế với $-\alpha < 0$ nên thay đổi chiều BĐT)

$\Leftrightarrow \log\left(n^{-\alpha}\right) \exp\left[\log\left(n^{-\alpha}\right)\right] > -\alpha$

$$\Leftrightarrow \left[\begin{array}{l} \log\left(n^{-\alpha}\right) > W_0(-\alpha) \\ \log\left(n^{-\alpha}\right) < W_{-1}(-\alpha) \end{array}\right.$$

$$\Leftrightarrow \left[\begin{array}{l} \log n < -\dfrac{1}{\alpha} W_0(-\alpha) \\ \log n > -\dfrac{1}{\alpha} W_{-1}(-\alpha) \end{array}\right.$$

$$\Leftrightarrow \left[\begin{array}{l} n < \exp\left[-\dfrac{1}{\alpha} W_0(\alpha)\right] \\ n > \exp\left[-\dfrac{1}{\alpha} W_{-1}(\alpha)\right] \end{array}\right.$$

Với $\alpha = 10^{-4}$, ta được:

$$\left[\begin{array}{l} n < \exp\left[-\dfrac{1}{10^{-4}} W_0\left(10^{-4}\right)\right] \\ n > \exp\left[-\dfrac{1}{10^{-4}} W_{-1}\left(10^{-4}\right)\right] \end{array}\right. \Leftrightarrow \left[\begin{array}{l} n < 2,71855 \\ n > 4,31133.10^{50669} \end{array}\right.$$

Vậy ta có thể chọn một giá trị bất kì của $N_\alpha \in \left[4,31133.10^{50669}; +\infty\right)$.

Bài 3

(a) Chứng minh rằng: Tồn tại vô số cặp số nguyên (m, n) sao cho $ma + nb = \gcd\big(a, b\big)$.

(b) Cài đặt thuật toán Euclid để tìm UCLN của hai số nguyên a và b.

(c) Cài đặt thuật toán Euclid mở rộng để xác định giá trị $\big(m, n\big)$ sao cho: $\gcd\big(a, b\big) = ma + nb$.

Bài làm:

(a) Với thuật toán Euclid mở rộng, ta tìm được một nghiệm $\big(m, n\big)$ thỏa mãn phương trình $ma + nb = \gcd\big(a, b\big)$ $\big(1\big)$.

Với $k \in \mathbb{Z}$, ta có: $ma + nb = ma + nb + kab - kab = a\big(m - kb\big) + b\big(n + ka\big)$.

Ta nhận thấy nếu $\big(m, n\big)$ là một nghiệm của phương trình $\big(1\big)$ thì $\big(m - kb, n + ka\big)$ cũng là một nghiệm của phương trình $\big(1\big)$. Vì có vô số giá trị $k \in \mathbb{Z}$ nên ta cũng có vô số cặp $\big(m - kb, n + ka\big)$ là nghiệm của phương trình $\big(1\big)$.

Vậy ta chứng minh được tồn tại vô số cặp số nguyên $\big(m, n\big)$ sao cho $ma + nb = \gcd\big(a, b\big)$.

(b)

Mã giả của thuật toán:

Thuật toán 1: Thuật toán Euclid để tìm UCLN

Đầu vào: 2 số nguyên không âm a, b.

Đầu ra : Số nguyên không âm d sao cho $d = \gcd\big(a, b\big)$.

```
while b ≠ 0 do
    r ← a mod b
    a ← b
    b ← r
return a
```

Hiện thực thuật toán trên Maple:

Ta định nghĩa thủ tục (procedure) `GCD`$\big(x, y\big)$ như trong hình bên dưới. Sau đó, ta chạy thử thuật toán để tìm UCLN của các cặp số sau:

$$\big(8, 0\big), \big(11, 0\big), \big(13, 13\big), \big(37, 600\big), \big(20, 100\big), \big(624129, 2061517\big)$$

```
> GCD := proc(x, y)
    local a, b, r;
    a := x;
    b := y;
    while b ≠ 0 do
      r := a mod b;
      a := b;
      b := r;
    end do;
    return a;
  end proc;
GCD := proc(x, y)
  local a, b, r;
  a := x; b := y; while b <> 0 do r := a mod b; a := b; b := r end do; return a
end proc
> GCD(8, 0)
                                  8
> GCD(11, 0)
                                 11
> GCD(13, 13)
                                 13
> GCD(37, 600)
                                  1
> GCD(20, 100)
                                 20
> GCD(624129, 2061517)
                              18913
```

(c)

Mã giả của thuật toán:

Thuật toán 2: Thuật toán Euclid mở rộng

Đầu vào: 2 số nguyên không âm a, b.

Đầu ra : 3 số nguyên m, n, d sao cho $ma + nb = \gcd(a, b) = d$.

$(m, n, d) \leftarrow (1, 0, a)$
$(u_1, u_2, u_3) \leftarrow (0, 1, b)$
while $u_3 \neq 0$ **do**
    $q \leftarrow \left\lfloor \frac{d}{u_3} \right\rfloor$
    $(v_1, v_2, v_3) \leftarrow (m, n, d) - q(u_1, u_2, u_3)$
    $(m, n, d) \leftarrow (u_1, u_2, u_3)$
    $(u_1, u_2, u_3) \leftarrow (v_1, v_2, v_3)$
return m, n, d

Hiện thực thuật toán trên Maple:

Ta định nghĩa thủ tục (procedure) `ExtendedGCD`(a, b) như trong hình bên dưới. Sau đó, ta chạy thử thuật toán để tìm giá trị m, n, d của các cặp số sau:

$$(29, 8), (1398, 324)$$

```
> ExtendedGCD := proc(a, b)
    local m_n_d, u, q, v;
    m_n_d := (1, 0, a);
    u := (0, 1, b);
    while u[3] ≠ 0 do
      q := floor( m_n_d[3] / u[3] );
      v := m_n_d − q·u;
      m_n_d := u;
      u := v;
    end do;
    return m_n_d;
  end proc;
```

```
ExtendedGCD := proc(a, b)
  local m_n_d, u, q, v;
  m_n_d := 1, 0, a;
  u := 0, 1, b;
  while u[3] <> 0 do
    q := floor(m_n_d[3]/u[3]); v := m_n_d − q*u; m_n_d := u; u := v
  end do;
  return m_n_d
end proc
```

```
> ExtendedGCD(29, 8)
                                  −3, 11, 1
> ExtendedGCD(1398, 324)
                                  −19, 82, 6
```

Bài 4

Giải hệ phương trình đồng dư sau:

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 9 \\ x \equiv 8 \pmod{11} \\ x \equiv 13 \pmod{13} \end{cases}$$

Bài làm:

Để giải hệ phương trình đồng dư tuyến tính, ta sẽ sử dụng định lí số dư Trung Hoa.

Mã giả của thuật toán:

Thuật toán 3: Giải hệ phương trình đồng dư sử dụng định lí số dư Trung Hoa

Đầu vào: $a = (a_1, a_2, ..., a_k)$ là k số nguyên tùy ý và k số nguyên dương đôi một nguyên tố cùng nhau $m = (m_1, m_2, ..., m_k)$. Khi đó ta có hệ phương trình đồng dư tuyến tính sau:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

Đầu ra : 2 số nguyên dương b, c sao cho $x \equiv b \pmod c$ là nghiệm của hệ trên.

$S \leftarrow 0$
$N \leftarrow 0$
$N^{-1} \leftarrow 0$
$b \leftarrow 0$
for $i \leftarrow 1$ **to** `len`(a) **do**
    `/* Hàm Remove dùng để loại bỏ phần tử thứ i trong a */`
    $S \leftarrow$ `Remove`(a, i)
    `/* Hàm Multiply dùng để tính tích các phần tử trong S */`
    $N \leftarrow$ `Multiply`(S)
    `/* Lấy nghịch đảo module sử dụng thuật toán Euclid mở rộng trong bài 3c */`
    $N^{-1} \leftarrow$ `ExtendedGCD`(N, m_i)
    $b \leftarrow b + a_i.N.N^{-1}$
return b, `Multiply`(m)

Giải tay:

Ta có:

$$N_1 = 9.11.13 = 1287 \equiv 2 \pmod 5 \Rightarrow N_1^{-1} = 3$$

$$N_2 = 5.11.13 = 715 \equiv 4 \pmod 9 \Rightarrow N_2^{-1} = 7$$

$$N_3 = 5.9.13 = 585 \equiv 2 \pmod{11} \Rightarrow N_3^{-1} = 6$$

$$N_4 = 5.9.11 = 495 \equiv 1 \pmod{13} \Rightarrow N_4^{-1} = 1$$

Vậy nghiệm của hệ phương trình là:

$$x = 2.1287.3 + 5.715.7 + 8.585.6 + 13.495.1 = 67262 \equiv 2912 \pmod{5.9.11.13 = 6435}$$

Hiện thực thuật toán trên Maple:

Ta định nghĩa thủ tục (procedure) `ChineseRemainder`(a, m) như trong hình bên dưới. Sau đó, ta chạy thử thuật toán tìm nghiệm của 2 hệ phương trình đồng dư sau:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases} \quad (1)$$

và

$$\begin{cases} x \equiv 6 \pmod{11} \\ x \equiv 13 \pmod{16} \\ x \equiv 9 \pmod{21} \\ x \equiv 19 \pmod{25} \end{cases} \quad (2)$$

```
> ChineseRemainder := proc(a, m)
    local i, S, N, inverse_N, solution; solution := 0;
    for i from 1 to numelems(a) do
      S := subsop(i = NULL, m);
      N := convert(S, `*`);
      inverse_N := ExtendedGCD(N, m[i])[1] mod m[i];
      solution := solution + a[i]·N·inverse_N;
    end do;
    return solution mod convert(m, `*`), convert(m, `*`);
  end proc;
ChineseRemainder := proc(a, m)
  local i, S, N, inverse_N, solution;
  solution := 0;
  for i to numelems(a) do
    S := subsop(i = NULL, m);
    N := convert(S, `*`);
    inverse_N := ExtendedGCD(N, m[i])[1] mod m[i];
    solution := solution + a[i]*N*inverse_N
  end do;
  return solution mod convert(m, `*`), convert(m, `*`)
end proc
> a := [2, 3, 5]; m := [3, 5, 7]
                                  a := [2, 3, 5]
                                  m := [3, 5, 7]
> ChineseRemainder(a, m)
                                  68, 105
> a := [6, 13, 9, 19]; m := [11, 16, 21, 25]
                                  a := [6, 13, 9, 19]
                                  m := [11, 16, 21, 25]
> ChineseRemainder(a, m)
                                  89469, 92400
```

Như vậy ta thấy nghiệm của hệ phương trình (1) là $x \equiv 68 \pmod{105}$, nghiệm của hệ phương trình (1) là $x \equiv 89469 \pmod{92400}$.

Bây giờ, ta đi tìm nghiệm của hệ phương trình đồng dư của **bài 4** sử dụng thủ tục (procedure) `ChineseRemainder`(a, m) đã được định nghĩa trong **Maple** như ở trên.

```
> a := [2, 5, 8, 13]; m := [5, 9, 11, 13]
                                  a := [2, 5, 8, 13]
                                  m := [5, 9, 11, 13]
> ChineseRemainder(a, m)
                                  2912, 6435
```

Vậy nghiệm của hệ phương trình đồng dư ở **bài 4** là $x \equiv 2912 \pmod{6435}$.

Bài 5

(a) Giải phương trình nghiệm nguyên: $a^2 + b^2 = c^2$.

(b) Chứng minh rằng phương trình sau không có nghiệm nguyên: $a^4 + b^4 = c^4$.

Bài làm:

(a)

Ta giả sử a, b, c nguyên tố cùng nhau và khi đó, chúng đôi một nguyên tố cùng nhau.

Ta nhận thấy rằng a và b không thể đồng thời là số chẵn (vì a và b nguyên tố cùng nhau như đã nói ở trên). Ngoài ra, a và b cũng không thể đồng thời là số lẻ (vì nếu a và b là số lẻ thì ta biểu diễn $a = 2k+1, b = 2l+1 \rightarrow a^2+b^2 = \big(2k+1\big)^2 + \big(2l+1\big)^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 4\big(k^2 + k + l^2 + l\big) + 2$ chia 4 dư 2 nhưng c^2 thì lại chia hết cho 4).

Ta giả sử a lẻ và b chẵn (Trường hợp ngược lại là a chẵn và b lẻ thì ta cũng sẽ xét tương tự). Ta có:

$$a^2 = c^2 - b^2 = \big(c + b\big)\big(c - b\big)$$

Ta thấy $c + b$ và $c - b$ là các số lẻ và chúng nguyên tố cùng nhau. Hai số nguyên dương $c+b$ và $c-b$ nguyên tố cùng nhau và có tích là số chính phương a^2 nên mỗi số $c + b$ và $c - b$ cũng là số chính phương.

Ta đặt $c + b = m^2, c - b = n^2$, với m, n là các số lẻ và nguyên tố cùng nhau, $m > n$. Ta được:

$$\begin{cases} a = mn \\ b = \dfrac{m^2 - n^2}{2} \\ c = \dfrac{m^2 + n^2}{2} \end{cases}$$

Vì m, n là các số lẻ nên $m^2 - n^2$ và $m^2 + n^2$ là các số chẵn. Do đó b và c ra kết quả là số nguyên.

Ta thử thay bộ 3 số $\big(a, b, c\big)$ vào vế trái của phương trình $a^2 + b^2 = c^2$. Ta được:

$$a^2 + b^2 = \big(mn\big)^2 + \left(\frac{m^2 - n^2}{2}\right)^2 = \frac{\big(m^2 - n^2\big)^2 + 4m^2n^2}{2^2}$$
$$= \frac{\big(m^2\big)^2 + 2m^2n^2 + \big(n^2\big)^2}{2^2} = \left(\frac{m^2 + n^2}{2}\right)^2 = c^2$$

Vậy với bộ 3 số $\big(a, b, c\big)$ ở trên thì ta chứng minh được phương trình $a^2 + b^2 = c^2$ có nghiệm nguyên.

(b)

Đầu tiên, phương trình $a^4 + b^4 = c^4$ (1) có nghiệm tầm thường khi $a = 0$ hoặc $b = 0$, tương ứng với từng trường hợp thì $c = \pm b$ hoặc $c = \pm a$. Nói cách khác, (1) có các nghiệm tầm thường tổng quát là $(0, b, b)$, $(0, b, -b)$, $(a, 0, a)$, $(a, 0, -a)$. Ta cần chứng minh phương trình (1) không có nghiệm nguyên nào khác ngoài các nghiệm tầm thường này.

Ta có thể chứng minh phương trình (1) không có nghiệm nguyên thông qua việc chứng minh phương trình $a^4 + b^4 = c^2$ (2) không có nghiệm nguyên. Điều này hợp lý vì nếu tồn tại một nghiệm (a, b, c) của phương trình (2) thì có thể dẫn đến một nghiệm (a, b, c^2) cho phương trình (1).

Để chứng minh phương trình $a^4 + b^4 = c^2$ không có nghiệm nguyên, ta sử dụng **phương pháp lùi vô hạn**. Đây là phương pháp chứng minh bằng phản chứng, bằng cách chứng minh rằng giả sử tồn tại một bộ nghiệm nhỏ nhất, có thể tìm được bộ nghiệm nhỏ hơn. Điều này dẫn đến việc lùi vô hạn và cuối cùng là sự mâu thuẫn.

Giả sử (2) có bộ nghiệm nhỏ nhất (x, y, z), sao cho $x^4 + y^4 = z^2$ và $\gcd(x, y, z) = 1$. Khi đó x hoặc y sẽ là số chẵn, giả sử x chẵn, y lẻ (trong trường hợp x lẻ và y chẵn thì cũng xét tương tự, và tính tổng quát vẫn được bảo toàn).

Dễ thấy, (x^2, y^2, z) là một bộ ba số Pytago. Như đã biết, theo công thức tổng quát của bộ ba số Pytago, thì tồn tại hai số nguyên dương m và n, với $m > n$,

$\gcd(m, n) = 1$, sao cho:

$$\begin{cases} x^2 = m^2 - n^2 \ (3) \\ y^2 = 2mn \ (4) \\ z = m^2 + n^2 \ (5) \end{cases}$$

Từ $x^2 = m^2 - n^2$ ta suy ra được $x^2 + n^2 = m^2$. Tương tự, (x, n, m) là một bộ ba số Pytago, với x chẵn và n lẻ. Do đó, tồn tại hai số nguyên dương p và q, với $p > q$, $\gcd(p, q) = 1$, sao cho:

$$\begin{cases} x = p^2 - q^2 \ (6) \\ n = 2pq \ (7) \\ m = p^2 + q^2 \ (8) \end{cases}$$

Thay (7) và (8) vào (4) ta được: $y^2 = 4pq(p^2 + q^2)$ (9).

Tuy nhiên, vì p, q nguyên tố cùng nhau, suy ra $\gcd(p^2, q^2) = 1$, dẫn đến các số p, q, $p^2 + q^2$ sẽ nguyên tố cùng nhau từng đôi một. Hay nói cách khác, $(p, q) = 1$, $(p, (p^2 + q^2)) = 1$, $(q, (p^2 + q^2)) = 1$. Kết hợp với (9), ta có thể suy ra $p, q, (p^2 + q^2)$ đều là các số chính phương.

Khi đó, tồn tại các số nguyên r, s, t sao cho:

$$\begin{cases} p = r^2 \\ q = s^2 \\ p^2 + q^2 = t^2 \end{cases}$$

Ta có $t^2 = p^2 + q^2 \Rightarrow t^2 = r^4 + s^4$.

Có thể thấy $0 < t \leq m \leq m^2 + n^2 = z$, do đó ta có thêm một bộ nghiệm (r, s, t), với r, s, t nguyên tố cùng nhau từng đôi một, và r, s, t nhỏ hơn x, y, z. Tuy nhiên, điều này ngược lại với giả thiết ban đầu là (x, y, z) là bộ nghiệm nhỏ nhất. Vì vậy, (2) không có nghiệm nguyên ngoài nghiệm tầm thường và điều này dẫn đến (1) cũng không có nghiệm nguyên khác ngoài nghiệm tầm thường.

Như vậy, với việc chứng minh phản chứng bằng phương pháp lùi vô hạn, ta đã chứng minh được phương trình $a^4 + b^4 = c^4$ không có nghiệm nguyên.