**CHỨNG MINH MỆNH ĐỀ**

**MỆNH ĐỀ: chứng minh rằng trong dãy số Fibonacci, F[y]|F[x] ⬄ y|x với mọi 3<=x<=y  
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~**

**<> Quy ước chung:**

K=y div x

R=y mod x

F[0]=0; F[1]=F[2]=1;

“|” là dấu chia hết

Trong các phép chứng minh, i,n,t được dùng như biến đếm, không phải kết quả của 1 biểu thức cụ thể như k, r,…

Gọi M[i]=F[i] mod F[x];

Để cho tiện ta sẽ quy ước luôn: các phép tính trên M[.] ta sẽ ngầm hiểu là đồng dư.

VD: M[i]=M[i-1] + M[i-2] (không cần ghi mod F[x])

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

**<> định lý 1: gcd(F[i],F[i+1]) = 1 với mọi i>0**

Chứng minh:

- Dễ thấy ĐL1 đúng với n=1 vì F[1]=F[2]=1

- Giả sử ĐL1 đúng với n=i tức là có gcd(F[i],F[i+1])=1

- Ta chứng minh ĐL1 đúng với n=i+1

+ Thật vậy, giả sử gcd(F[i+1],F[i+2]) = t >1  
+ ta có F[i+2]=F[i] + F[i+1]. Nếu F[i+2], F[i+1] cùng chia hết cho t, thì F[i] cũng phải chia hết cho t điều này ngược với giả thuyết quy nạp 🡪 vô lý

🡪 gcd(F[i+1],F[i+2])=1

🡪 ĐL1 đúng với mọi i

\* **hệ quả**:

1/ M[i] và M[i+1] không thể đồng thời bằng 0, vì x>=3 nên F[x]>1 mà F[i] và F[i+1] không thể đồng thời chia hết cho 1 số lớn hơn 1

2/ M[i]=0 ⬄ M[i+1] = M[i+2] ≠ 0

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Giả sử có F[i] và F[i+1], chắc chắn F[i+t] tồn tại được 1 phép phân tích thành a.F[i] + b.F[i+1] (phương trình diophantos tuyến tính bậc nhất luôn có nghiệm nguyên nếu vế phải là bội của ước chung lớn nhất các hệ số bên vế trái)

Thật vậy, ta chỉ cần đặt F[i], F[i+1] là ẩn, sau đó cộng dồn các hệ số. xem bảng sau:

|  |  |  |
| --- | --- | --- |
| F[.] | a | b |
| i | 1 | 0 |
| i+1 | 0 | 1 |
| i+2 | 1 | 1 |
| i+3 | 1 | 2 |
| i+4 | 2 | 3 |
| i+5 | 3 | 5 |
| … | … | … |

Đến đây ta lại nhận thấy a từ chỗ i+1 trở đi có dạng 0;1;1;2;3;5;… chính là dãy fibonacci. Tương tự b từ chỗ i cũng có dạng này.

Như vậy ta dẫn đến 1 định lý sau đây:

**<> Định lý 2: F[i+t] = F[t-1].F[i] + F[t].F[i+1]**

Chứng minh:

- với t=0 rõ ràng F[i] = 1.F[i] + 0.F[i+1] = F[-1].F[i] + F[0].F[i+1]

- với t=1 ta cũng có F[i+1] = 0.F[i] + 1.F[i+1] = F[0].F[i] + F[1].F[i+1]

- giả sử mệnh đề đúng với t=x và t=x+1, tức là:

F[i+x] = F[x-1].F[i] + F[x].F[i+1]

F[i+x+1] = F[x].F[i] + F[x+1].F[i+1]

Ta chứng minh mệnh đề cũng đúng với t=x+2. Tức là chứng minh:

F[i+x+2] = F[x+1].F[i] + F[x+2].F[i+1]

Thật vậy:

F[i+x+2] = F[i+x] + F[i+x+1]

= F[x-1].F[i] + F[x].F[i+1] + F[x].F[i] + F[x+1].F[i+1]

= (F[x-1] + F[x]).F[i] + (F[x] + F[x+1]).F[i+1]

= F[x+1].F[i] + F[x+2].F[i+1]

🡪 định lý được chứng minh.

**\* Hệ quả:** điều này cũng đúng với phép toán trên M

*M[i+t] = M[t-1].M[i] + M[t].M[i+1]*

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

**<> định lý 3: F[kx] | F[x] với mọi k>=0**theo định nghĩa F[kx] | F[x] ⬄ M[kx] = 0  
vậy ta sử dụng M để chứng minh.

- Với k=0, hiển nhiên M[0.x]= F[0] mod F[x] = 0 🡪 như vậy ĐL3 đúng với k=0

- Với k=1, M[1.x]= F[x] mod F[x] = 0 🡪 ĐL3 đúng với k=1

- Giả sử ĐL3 đúng với k=i. tức là M[ix]=0

- ta chứng minh ĐL3 đúng với k=i+1

Thật vậy:

*M[(i+1)x]*

*= M[ ix + x]*

*= M[ (ix + 1) + (x – 1) ]*

*= M[x-2].M[ix + 1] + M[x-1].M[ix + 2] (\*)*

*Mà theo hệ quả 2 của định lý 1, M[ix + 1] = M[ix + 2]*

*🡪 (\*) = M[ix + 1] . ( M[x-2] + M[x-1] )*

*= M[ix + 1].M[x]*

*= 0*

Như vậy ĐL3 đúng với mọi k>=0

Ta đã chứng minh được chiều ngược của mệnh đề ban đầu!

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

**<> định lý 4: nếu gcd(a,c)=1 và b không chia hết cho c. thì a.b không chia hết cho c**

Chỉ có 3 trường hợp để a.b | c  
1: a|c (vô lý vì gcd(a,c)=1 )

2: b|c (vô lý, gt)

3: tồn tại số tự nhiên d,e sao cho:

+ a = da’

+ b = eb’

+ c = de

- ta thấy rằng d cùng là ước của a, c, vậy nó phải là 1 (gt) ⬄ e=c ⬄ b|c, vô lý!

🡪 định lý được chứng minh

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

**<> định lý 5: F[kx+r] không chia hết cho F[x] (0<r<x)**

- tương tự định lý 3, ta đi chứng minh trên M.

- ở định lý 3, ta đã chứng minh được F[kx] | F[x] 🡪 M[kx+1] = M[kx+2]

*M[ kx + r ]*

*= M[ (kx+1) + (r-1) ]*

*= M[r-2].M[kx + 1] + M[r-1].M[kx + 2 ]*

*= M[kx+1] . ( M[r-1] + M[r-2] )*

*= M[kx+1] . M[r]*

- Vì 0<r<x nên 0<F[r]<F[x] 🡪 F[r] không chia hết cho F[x]

- Từ định lý 1 ta lại có có gcd(F[kx], F[kx + 1]) = 1. Mà F[x] là ước F[kx] nên gcd(F[x], F[kx +1]) = 1 (hiển nhiên vì việc chia bớt không thể làm xuất hiện thêm thừa số nguyên tố chung)

🡪 từ 2 điều và từ định lý 4 trên ta dễ dàng suy ra được F[kx+1] . F[r] không chia hết cho F[x]

🡪 (F[kx+1].F[r]) mod F[x] ≠ 0

🡪 M[kx + r] ≠ 0

🡪 F[kx + r] không chia hết cho F[x]

**\* hệ quả: chiều ngược lại của mệnh đề: nếu F[y] | F[x] 🡪 y|x**

**-** giả sử y không chia hết cho x 🡪 theo ĐL5 F[y] không chia hết cho F[x] mâu thuẫn với điều kiện đề cho

🡪 chứng minh chiều xuôi của mệnh đề ban đầu

🡪 mệnh đề đã được chứng minh hoàn toàn □

QTN