**★★☆☆☆**

**題組：Problem Set Archive with Online Judge**

**題號：11287 –Pseudoprime Numbers**

**解題者：謝孟唐**

**解題日期：2013年5月2日**

**題意：**

每次給定一組數字 p (2 < p ≦ 109)、a (1 < a < p)。

ap == a (mod p) 且 p 不為質數，

則我們將 p 稱為 base-a pseudoprime。

如果 p 是 base-a pseudoprime，則輸出yes，否則輸出no。

**題意範例：**

23 % 3 == 2

310 % 10 == 9

2341 % 341 == 2

.

.

.

input a=0, p=0時結束

no

no

yes

no

yes

yes

3 2

10 3

341 2

341 3 🡪

1105 2

1105 3

0 0

**解法：**

其中比較核心的部分是要計算 ap (mod p)，又 p 值很大

直接算會TLE。

原理: (x \* y) % n = (x % n \* y % n) % n

ans = xy mod n

= (…((((x mod n)\*x)mod n)\*x)mod n…\*x)mod n    (共y個x)

ans = 1;

temp\_p = p;

while( temp\_p != 0)

{

if( temp\_p % 2 == 1)

ans = ans \* a % p;

a = a \* a % p;

temp\_p = temp\_p / 2;

}

**解法範例：**

ex. 213

1310 = 11012

ans = 20 a = 21 temp\_p = 13

ans = 21 a = 22  temp\_p = 6

ans = 21 a = 24 temp\_p = 3

ans = 24+1 a = 28 temp\_p = 1

ans = 28+4+1 a = 216 temp\_p = 0

**討論：**

1. 因為測資範圍最多到109，所以變數型態需用long long。

**程式：**

#include <stdio.h>

#include <stdlib.h>

#include <math.h>

long F(long, long);

bool is\_prime(int);

int main(void)

{

long p, a;

while(scanf("%ld %ld", &p, &a))

{

if(p == 0 && a == 0)

break;

if(is\_prime(p) == true)

printf("no\n");

else

{

if(F(p, a) == a)

printf("yes\n");

else

printf("no\n");

}

}

return 0;

}

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

long F(long p, long a)

{

long count = p, temp = 1;

while(count != 0)

{

if(count % 2 == 1)

temp = temp \* a % p;

a = a \* a % p;

count = count / 2;

}

return temp % p;

}

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/

bool is\_prime(int p)

{

for(int i = 2; i <= sqrt(p); i ++)

{

if(p % i == 0)

return false;

}

return true;

}

/\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*/