Generate
Private-roots of Prime-number

素数の原始根を生成するプログラム

https://github.com/uchuukaeru/private-roots

プログラムについて
-About the Program-

Language : C#

I wanted to use “ulong”type variables,which are not available in java.

In the end , the “ulong”type variables is no longer needed and can be implemented the same way in java (I think).

言語：C#

“ulong”型変数※が使いたかった。

が、結局使わずに実装できたため、ほぼそのままjavaでも実装可能。（だと思う）（気が向いたら実装する予定）

※”ulong”型：符号なし64ビット整数型

プログラムの概要1
-Overview 1-

```
Main(){
    Input;
    Calcul(Input);
    Output;
}
```

プログラムの概要2
-Overview 2-

```
Calcul(Input){
    For(i:2=>Input-1){
        For(n;1=>Input-1){
            Calcul_roots(i,n,Input);
        }
    }
    Return(ans);
}
```

プログラムの概要3
-Overview 3-

Calcul_roots(i,n,Input){

If($i^n > 2^{64} - 1$){

It = Calcul_roots(i,$\lfloor n/2 \rfloor$,Input);

Nt = Calcul_roots(i,$\lceil n/2 \rceil$.floor,Input);

m = $(It \times Nt)\ mod\ (Input)$;

}Else{

m = $i^n mod\ (Input)$;

}

Return(m);

}

計算のアルゴリズム1
-Calculation Algorithm 1-

A,n,m,l:整数-integer

$$A^n mod\ l = B$$

$$A^m mod\ l = C$$

$$t = n + m$$

$$A^t = A^{n+m} = A^n \times A^m$$

$$A^{2n} mod\ l = (A^n \times A^n) mod\ l = \left(\left((A^n) mod\ l\right)^2\right) mod\ l$$

$$= (B^2)\ mod\ l$$

$$A^t mod\ l = (A^n \times A^m) mod\ l$$

$$= \left(\left((A^n) mod\ l\right) \times \left((A^m) mod\ l\right)\right) mod\ l = (B \times C) mod\ l$$

計算のアルゴリズム2
-Calculation Algorithm 2-

$$A = 5, l = 11, n = [2,3,4,6,8]$$

$$5^2 = 25 \qquad 5^2 \; mod \; 11 = 25 \; mod \; 11 = 3$$

$$5^3 = 125 \qquad 5^3 \; mod \; 11 = 125 \; mod \; 11 = 4$$

$$5^4 = 625 \qquad 5^4 \; mod \; 11 = 625 \; mod \; 11 = 9$$

$$5^6 = 15625 \qquad 5^6 \; mod \; 11 = 15625 \; mod \; 11 = 5$$

$$5^8 = 390625 \qquad 5^8 \; mod \; 11 = 390625 \; mod \; 11 = 4$$

計算のアルゴリズム3
-Calculation Algorithm 3-

$$5^2 \; mod \; 11 = 25 \; mod \; 11 = 3 \cdots t$$

$$5^4 = 625 \quad 5^4 \; mod \; 11 = 625 \; mod \; 11 = 9$$

$$5^4 \; mod \; 11 = 5^{2+2} \; mod \; 11$$
$$= \big((5^2 \; mod \; 11) \times (15^2 \; mod \; 11)\big) mod \; 11 = (3 \times 3) \; mod \; 11$$
$$= 9 \; mod \; 11 = 9$$

計算のアルゴリズム4
-Calculation Algorithm 4-

$$5^2\ mod\ 11 = 25\ mod\ 11 = 3$$
$$5^3\ mod\ 11 = 125\ mod\ 11 = 4$$
$$5^6 = 15625 \qquad 5^6\ mod\ 11 = 15625\ mod\ 11 = 5$$

$$5^6\ mod\ 11 = 5^{2+2+2}\ mod\ 11$$
$$= \big((5^2\ mod\ 11) \times (5^2\ mod\ 11) \times (5^2\ mod\ 11)\big) mod\ 11$$
$$= (3 \times 3 \times 3) mod\ 11 = 27\ mod\ 11 = 5$$

$$5^6\ mod\ 11 = 5^{3+3}\ mod\ 11 = \big((5^3\ mod\ 11) \times (5^3\ mod\ 11)\big) mod\ 11$$
$$= (4 \times 4) mod\ 11 = 16\ mod\ 11 = 5$$

計算のアルゴリズム5
-Calculation Algorithm 5-

$$A = 5, l = 11, n = [2,3,4,6,8]$$
$$5^2 \; mod \; 11 = 25 \; mod \; 11 = 3$$
$$5^3 \; mod \; 11 = 125 \; mod \; 11 = 4$$

$$5^8 = 390625 \qquad 5^8 \; mod \; 11 = 390625 \; mod \; 11 = 4$$

$$5^8 \; mod \; 11 = 5^{2+3+3} \; mod \; 11$$
$$= \big((5^2 \; mod \; 11) \times (5^3 \; mod \; 11) \times (5^3 \; mod \; 11)\big) mod \; 11$$
$$= (3 \times 4 \times 4) mod \; 11 = 48 \; mod \; 11 = 4$$

アルゴリズムの数学的証明について
-On Mathematical Proofs of Algorithms-

I don’t know if the algorithm I just described has been proved.

This came to me by accident while I was programming.

I’m not a mathematician , and I’m not good at theory ,

so I’m not going to bother with proofs.

数学的に証明されているかは知らない。

プログラミングしているときに突然思いついた。

自力で証明するつもりはない。証明は苦手だし、数学者ではないので。

終

-fin-