Problem Solving Homework (Week 13)

161180162 Xu Zhiming

2018 年 6 月 26 日

JH Chapter 5

5.3.2.5

使用下面 5.3.3.10 中的算法

5.3.3.2

2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20, 22, 23, 25, 26, 29, 31, 32, 34, 37, 38, 40, 41, 43, 44, 46, 47, 50, 52, 53, 55, 58, 59, 61, 62.

The code for computing these values is listed below:

```
#include <cstdio>
#include <cmath>
#include <set>
using namespace std;
inline int resq(int a, int b, int p)
{
    int c = a, d = 1;
    for(int i=0;b;++i)
    {
        if(b&0x1)
        {
            d = d * c % p;
            c = c * c % p;
        }
        b>>=1;
    }
    return d;
}
int n = 63;
int main()
{
    set<int> s;
    for(int i=1;i<n;++i)
    {
        int tmp = resq(i, (n-1) / 2, n);
        if(tmp!=1&&tmp!=-1)
        {
            for(int j=1;j<n;++j)
            {
                if(i*j%n==1)
                {
                    s.insert(i);
                    s.insert(j);
                }
            }
        }
    }
    set<int>::iterator iter;
    for(iter = s.begin(); iter!=s.end(); ++iter)
    printf("%d ", *iter);
    return 0;
}
```

5.3.3.9

All the numbers below satisfy **Definition 5.3.3.7**.

证明. (i)

$$\because a^2 \cdot b^2 \mod p = a^2 \mod p \cdot b^2 \mod p$$
$$\therefore Leg\left[\frac{a \cdot b}{p}\right] = Leg\left[\frac{a}{p}\right] \cdot Leg\left[\frac{b}{p}\right]$$
$$\therefore Jac\left[\frac{a \cdot b}{p}\right] = Jac\left[\frac{a}{p}\right] \cdot Jac\left[\frac{b}{p}\right]$$

(ii)

$$\because a \equiv b \mod n$$
$$\therefore a^2 \equiv b^2 \mod n$$
$$\therefore Jac\left[\frac{a}{p}\right] = Jac\left[\frac{b}{p}\right]$$

(iii) Suppose $a = q_1^{j_1} \cdot q_2^{j_2} \cdot \cdots \cdot q_m^{j_m}$,$p_i$ is prime and j_i is positive interger.

$$\begin{aligned} Jac\left[\frac{n}{a}\right] &= \prod_{i=1}^{m} \left(Leg\left[\frac{n}{q_i}\right]\right)^{j_i} \\ &= \prod_{i=1}^{m} \left(n^{(q_i-1)/2} \mod q_i\right)^{j_i} \end{aligned}$$

(iv)

$$\because 1^2 = 1 \mod p$$
$$\therefore Leg\left[\frac{1}{n}\right] = 1$$
$$\therefore Jac\left[\frac{1}{n}\right] = 1$$

(v)

$$\because Jac\left[\frac{2}{n}\right] = \prod_{i=1}^{l} \left(Leg\left[\frac{a}{p_i}\right]\right)^{k_i},\ n = p_1^{k_1} p_2^{k_2} \cdot \cdots \cdot p_l^{k_l}$$
$$\begin{aligned} n = 8k+3, 8k+5, Jac\left[\frac{2}{n}\right] &= -Jac\left[\frac{n}{2}\right] \text{(iii)} \\ &= -Jac\left[\frac{1}{2}\right] \text{(ii)} \\ &= -1 \\ n = 8k+1, 8k+7, Jac\left[\frac{2}{n}\right] &= -Jac\left[\frac{n}{2}\right] \text{(iii)} \\ &= -Jac\left[\frac{1}{2}\right] \text{(ii)} \\ &= -1 \end{aligned}$$

□

5.3.3.10

证明. Since a and n are coprimes, we can first use property (iii), reducing to calculate $(-1)^{\frac{a-1}{2} \cdot \frac{n-1}{2}} \cdot Jac\left[\frac{n}{a}\right]$. The power of -1 can be easily computed in $O(1)$ times since we only need to determine whether the exponential is even or odd. $Jac\left[\frac{n}{a}\right] = Jac\left[\frac{n \mod a}{a}\right]$ according to property (ii). This time, again, use property (iii), reducing to compute $Jac\left[\frac{a}{n \mod a}\right]$, which is similar to what Eulerian-Algorithm does for calculating $\gcd(a, n)$, with time complexity in $O(\log n)$. In the end, $Jac\left[\frac{a}{n}\right]$ can be reduced in property (v)'s form, where only some powers of $-1/1$ are computed in $O(1)$. Therefore, for every odd n and every $a \in \{1, 2, \cdots, n-1\}$ with $\gcd(a, n) = 1$, $Jac\left[\frac{a}{n}\right]$ can be computed in polynomial time according to $\log_2 n$. □