「学习总结」数论再探

Jiayi Su (ShuYuMo)

2021-03-06 18:58:03

结束了「学习总结」整数模 n 乘法群 之后，发现数论还有很多东西妹学。(T___T). 一直没有发表

数论初探

「学习总结」数论

整数模 **n** 乘法群

「学习总结」整数模 n 乘法群

库默尔定理

令 $V_p(n)$ 表示 n 中素因子 P 的次数，有：

$$V_p\left(\binom{n}{m}\right)$$

的值为 m 与 $n-m$ 在 P 进制下加法的进位次数。

另一个事实是，$n!$ 中质因子 p 的幂次为：

$$\frac{n-f_p(n)}{p-1}$$

$f_p(n)$ 为 n 在 p 进制下的数位和。

二次剩余

一个数 a，如果不是 p 的倍数且模 p 同余于某个数的平方，则称 a 为模 p 的 二次剩余。

而一个不是 p 的倍数的数 b，不同余于任何数的平方，则称 b 为模 p 的 非二次剩余。

勒让德符号

$$\left(\frac{n}{p}\right)=\begin{cases}1 & p\nmid n且n是p的二次剩余\\ -1 & p\nmid n且n不是p的二次剩余\\ 0 & p\mid n\end{cases}$$

欧拉准则

$$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}}\pmod p$$

剩余系开根

Cipolla 算法

给出正整数 n 求出模 p 意义下的 $\sqrt{n}$。

背过程：

随机一个 n 的剩余系下整数 a ，满足 a^2-n 不是二次剩余。

设剩余系下虚数单位 $\mathbf{i}=\sqrt{a^2-n}$

则 $\sqrt{n}\equiv(a+\mathbf{i})^{\frac{p+1}{2}} \pmod p$

一道例题 Code+#7 同余方程

```
int np[_], prime[_], tot, d[_], x;
void Prime(int n) {
    for(int i = 2; i <= n; i++){
        if(!np[i]) prime[++tot] = i, d[i] = i;
        for(int j = 1; j <= tot && (x = prime[j] * i) <= n; j++){
            np[x] = 1; d[x] = prime[j];
            if(i % prime[j] == 0) break;
        }
    }
}
pair<int, int> IN[_];
int main(){
    int n; IO >> n; int MAX = 0;
    for(int i = 1; i <= n; i++) (IO >> IN[i].first >> IN[i].second), MAX = max(MAX, IN[i].first) ;
    Prime(MAX + 1);
    for(int i = 1; i <= n; i++) {
        int p = IN[i].first, x = IN[i].second; LL ret = 1;
        while(p != 1){
            int now = d[p];
            if(x % now == 0) ret *= (now % 4 == 1 ? ((now << 1) - 1) : 1);
            else ret *= (((now % 4 == 1) ? -1 : 1) + now);
            p /= d[p];
        }
        printf("%lld\n", ret);
    }
    return 0;
}
```