初等数论

素数的判定（素性测试）

- Miller-Rabin素性测试
- 如果n为素数，取$a < n$,设$n - 1 = d \times 2^r$，则要么$a^d \equiv 1 \pmod n$，要么$\exists 0 \le i < r, s.t. a^{d \times 2^i} \equiv -1 \pmod n$

素数的判定

- 常规做法：选取k个不同的数进行miller-rabin素性测试
- 如果都通过则为质数

- 2,3,5,7,13,29,37,89

- $O(k\log n)$

Miller Rabin练习题

- https://noip.ac/show_problem/3156

Pollard-Rho

- 对大数p分解质因数

- 如果p为质数则停止（通过Miller rabin进行检验）
- 否则我们要尝试找到一个数a使得a为p的一个因子
- 问题可以转换为找到一个数a使得$\gcd(a, p) \neq 1$

Pollard-Rho

- 方案一：随机一个数a检查，复杂度?

- 方案二：利用生日悖论减少枚举量

- 生日悖论：从n个数中随机选取k个两两之差全部不等于c的概率约为$O\left(\frac{1}{n^{k^2}}\right)$

Pollard-Rho

- 核心问题：要找到k个数，检查这k个数两两的差与p的最大公因数

- 伪随机函数：$f_i = f_{i-1}^2 + c$

- 如果$\gcd\left(f_i - f_j, p\right) \neq 1$，则
- $f_{i+1} - f_{j+1} = (f_i - f_j)(f_i + f_j)$与$p$的最大公因数也不为1

Pollard-Rho

- 方法一：令$i = j = 0, v_1 = f_i, v_2 = f_j$
- 每次令$i += 1, j += 2$
- 检查$|v_1 - v_2|$和p的最大公因数
- 假设最大公因数$v \neq 1$，则说明找到了一个因子
- 此时继续对v和$\frac{p}{v}$进行分解即可

Pollard-Rho

- 方案一的弊端:
- 每次都需要进行一次log级别的gcd操作
- 操作次数取决于循环节的长度

- 优化：倍增+奇怪操作

Pollard-Rho

- （该方法没有任何理论依据 只是实践很有效果）

- 每次计算gcd是不必要的
- 每计算连续一段的乘积 然后再做gcd是一样的效果

- 1、枚举$i \in \left[2^j, 2^{j+1}\right)$,计算所有$\left(f_i - f_{2^j}\right)$的乘积，检查与$p$的$gcd$
- 2、但是这样长度太长才检查一次，所以再加一个每t次乘积之后就检查一次的条件，一般$t = 128$（此处无任何道理）

Pollard-Rho练习题

- https://noip.ac/show_problem/3157

逆元

- 如果$(a, m) = 1$且存在唯一的b使得$a \times b \equiv 1 \pmod{m}$且$1 \leq b < m$,则$b$为$a$在模$m$意义下的逆元
- 费马小定理 $a^{p-1} \equiv 1$
- 欧拉定理 $a^{\phi(m)} \equiv 1$

线性求逆元

- 求$1-n$所有数对p的逆元？

线性求逆元

- $\forall 1 \le i \le n, p = ki + r$
- $ki + r \equiv 0 (mod\ p)$
- $kr^{-1} + i^{-1} \equiv 0 (mod\ p)$
- $i^{-1} \equiv -kr^{-1} (mod\ p)$
- $i^{-1} \equiv -\left\lfloor \frac{p}{i} \right\rfloor (p\ mod\ i)^{-1}$

ExGCD

- 给定a, b
- 知道$g = \gcd(a, b)$
- 求x, y
- 使得
- $xa + yb = g$

ExGCD

Solution (扩展欧几里得算法)

```
int ExGcd(int a, int b, int &x, int &y) {
    if (b == 0) {
        x = 1, y = 0;
        return a;
    }
    else {
        int g = ExGcd(b, a % b, x, y);
        int t = x;
        x = y, y = t - a / b * x;
        return g;
    }
}
```

裴蜀定理

- 给定a, b, c，则$ax + yb = c$有整数解的充要条件是$\gcd(a, b) \mid c$。

原根

- 原根的定义：
- 如果a模m的阶等于$\phi(m)$，则a叫做m的原根

- 阶的定义：
- 找到一个最小的k，使得$a^k = a^0$，则k是a的阶

原根

- 对于正整数m，m有原根当且仅当$m = 2,4,p^a,2p^a$，其中p是奇素数

- 原根怎么求?
- 1、暴力
- 2、优化暴力

Problem 1

- 给定k, p, a
- 求$x^k \equiv a (mod\ p)$的所有解
- $p \leq 10^9$且是质数, $2 \leq k \leq 10^5$

Problem 1

- 求出原根g
- 假设$x = g^y, a = g^z$
- 则原方程变为
- $g^{ky} \equiv g^z (mod\, p)$
- $ky \equiv z (mod\, p - 1)$
- EXGCD解之即可

- https://noip.ac/show_problem/3158

BSGS

- 求$a^x \equiv b(mod\ p)$的一组解
- $p \le 10^9$且是质数

Problem 2

- 求斐波那契数列关于给定数p的循环节长度
- $p \leq 10^6$

Problem 2

- 应用BSGS至矩阵乘法
- 不需要矩阵求逆

- https://noip.ac/show_problem/3159

Problem 3

- 给定A, B, C
- 求$A^x \equiv B(mod\ C)$的最小非负整数解
- $A, B, C \leq 10^9$，无其他约束

Problem 3

- 令$A^x = Ct + B, g = \gcd(A, C)$
- 若$B \ mod \ g \neq 0$则无解
- 则式子变化为
- $\frac{A}{g} \cdot A^{x-1} = \frac{C}{g}t + \frac{B}{g} \Rightarrow \frac{A}{g} \cdot A^{x-1} = \frac{B}{g}\left(mod\,\frac{C}{g}\right)$
- 则转化为了原来的问题

- https://noip.ac/show_problem/3160

拓展中国剩余定理

- 问题定义：
- 给定N个方程
- $x \equiv b_i (mod\ m_i)$
- 求x

方法一：大数翻倍法

- 考虑合并两个方程
- $x \equiv b_1 (mod\ p_1), x \equiv b_2 (mod\ p_2), p_1 > p_2$
- 则暴力枚举
- $b_1, b_1 + p_1, b_1 + 2p_1, \cdots$
- 检查是否满足条件
- 至多只用枚举p_2次

- 复杂度?

方法二——拓展欧几里得

- 考虑合并两个方程
- $x \equiv b_1 (mod\ p_1), x \equiv b_2 (mod\ p_2)$
- 则
- $x = k_1 p_1 + b_1 = k_2 p_2 + b_2 \Rightarrow k_1 p_1 - k_2 p_2 = b_2 - b_1$
- 设$g = \gcd(p_1, p_2)$则
- $\frac{p_1}{g} k_1 \equiv \frac{b_2 - b_1}{g} \left(mod\ \frac{p_2}{g} \right)$
- 用扩欧解出k_1之后则有答案

筛法——线性筛

- 重中之重
- 必须掌握

Solution (線性篩法)

```
for (int i = 2; i <= n; ++ i) {
  if (!not_prime[i]) prime[++ prime_cnt] = i;
  for (int j = 1; j <= prime_cnt; ++ j) {
    if (prime[j] * i > n) break;
    not_prime[prime[j] * i] = true;
    if (i % prime[j] == 0) break;
  }
}
```

积性函数

- 如果函数f满足$\gcd(a,b)=1$时有$f(ab)=f(a)f(b)$，则f叫做积性函数
- 如果取消互质的条件则叫做完全积性函数

狄利克雷卷积

- 定义：
- $(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$

狄利克雷卷积

- 三个性质：
- 交换律：$f * g = g * f$
- 结合律：$(f * g) * h = f * (g * h)$
- 分配律：$(f + g) * h = f * h + g * h$
- 三个等式：
- $\mu * I = \epsilon$ （$\epsilon(n) = [n = 1], I(n) = 1$）
- $\phi * I = id$ （$id(n) = n$）
- $\mu * id = \phi$

莫比乌斯反演

- 如果$g(n) = \sum_{d|n} f(d)$
- 则$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$

莫比乌斯反演

- 如果$g(n) = \sum_{d|n} f(d)$
- 则$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$

- 证明:
- $g = f * I$
- $g * \mu = f * I * \mu = f * (I * \mu) = f * \epsilon$

Problem 4

- 求$\phi(1-n),\mu(1-n)$

Problem 5

- 求$\sum_{i=1}^{n}\sum_{j=1}^{m}\gcd(i,j)$

Problem 5

- $\sum_{i=1}^{n} \sum_{j=1}^{m} \gcd(i, j)$
- $= \sum_{i=1}^{n} \sum_{j=1}^{m} \sum_{d \mid \gcd(i,j)} \phi(d)$
- $= \sum_{d=1}^{n} \phi(d) \left\lfloor \frac{n}{d} \right\rfloor \left\lfloor \frac{m}{d} \right\rfloor$

Problem 6

- 求$\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j)=1]$

Problem 6

- 将上一题的ϕ换成μ即可

Problem 7

- 求当$a \leq x \leq b, c \leq y \leq d$时$\gcd(x, y) = 1$的$(x, y)$的个数。

Problem 7

- 四段前缀和
- $\sum_{i=1}^{n}\sum_{j=1}^{m}[\gcd(i,j)=1]=\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d\mid\gcd(i,j)}\mu(d)=\sum_{d=1}^{\min(n,m)}\mu(d)\times\frac{n}{d}\times\frac{m}{d}$
- 然后分块即可
- https://noip.ac/show_problem/3161

Problem 8

- 求当$a \le x \le b, c \le y \le d$时$\gcd(x, y)$是质数的$(x, y)$的个数。

Problem 8

- 类似可得
- $\sum_p \sum_{d=1}^{\min\left(\frac{n}{p},\frac{m}{p}\right)} \mu(d) \times \frac{n}{dp} \times \frac{m}{dp} = \sum_{x=1}^{\min(n,m)} \frac{n}{x} \times \frac{m}{x} \sum_{p|x} \mu\left(\frac{x}{p}\right)$
- https://noip.ac/show_problem/3162

筛法——杜教筛

- 目标是求某个积性函数f的前缀和
- 设前缀和为S，则考虑另外一个函数g
- $\sum_{i=1}^{n}(f*g)(i)=\sum_{i=1}^{n}\sum_{d|i}g(d)f\left(\frac{i}{d}\right)$
- $=\sum_{d=1}^{n}g(d)\sum_{i=1}^{\left\lfloor\frac{n}{d}\right\rfloor}f(i)=\sum_{d=1}^{n}g(d)\,S\left(\left\lfloor\frac{n}{d}\right\rfloor\right)$

杜教筛

- 目标：$g(1)S(n)$
- $g(1)S(n) = \sum_{i=1}^{n}(f * g)(i) - \sum_{d=2}^{n} g(d)\,S\left(\left\lfloor\frac{n}{d}\right\rfloor\right)$

- 使用杜教筛的条件：
- $f * g$的前缀和很好算
- g很好算

- 所以核心就是g的构造

杜教筛

```
long long get_s_n(unsigned int n)
{
    if (n<maxn) return sum[n];
    long long ans=f_g_sum(n);
    for (unsigned int l=2;l<=n;)
    {
        unsigned int r=n/(n/l)+1;
        ans -= (g_sum(r)-g_sum(l))*get_s_n(n/l);
        l=r;
    }
    return ans / g(1);
}
```

杜教筛练习

- 1、$\sum_{i=1}^{N} \mu_i$
- 2、$\sum_{i=1}^{N} \phi_i$
- 3、$\sum_{i=1}^{N} \phi_i \times i$
- 4、$\sum_{i=1}^{N} \phi_i \times i^2$

杜教筛练习

- 1、$\mu * I = \epsilon$
- 2、$\phi * I = id$
- 3、$f * g = \sum_{d|n} d \times \phi(d) g\left(\frac{n}{d}\right)$
- 只要使得$g\left(\frac{n}{d}\right)$里面出来一个除以$d$就可以把前面的$d$干掉了
- 另$g(n) = id(n) = n$，则
- $\sum_{d|n} d \times \phi(d) g\left(\frac{n}{d}\right) = n \sum_{d|n} \phi(d) = n^2$

杜教筛练习

- 4、 $f * g = \sum_{d|n} d^2 \times \phi(d) g\left(\frac{n}{d}\right)$
- 令$g(n) = n^2$则
- $f * g = n^2 \sum_{d|n} \phi(d) = n^3$

Problem 9

- 给定序列s
- 求序列s的字典序排名对m取模的值
- $n \leq 300000$
- $m \leq 10^9$
- $s_i \leq 300000$

Problem 9

- 考虑计算有多少个排列小于s
- 枚举第一位变小的地方
- 相当于是询问后半部分有多少比这个数小（树状数组）
- 需要除以每个数出现的次数的阶乘
- m不是质数，所以做质因数分解之后用中国剩余定理合并即可

- https://noip.ac/show_problem/3163

Problem 10

- 求$\sum_{i=1}^{n}\sum_{j=1}^{m}\gcd(i,j)$

- $n,m \leq 10^6$

Problem 10

- $\sum_{i=1}^{n}\sum_{j=1}^{n}\operatorname{gcd}(i,j)=\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{d\mid\operatorname{gcd}(i,j)}\phi(d)$
- $=\sum_{d=1}^{N}\phi(d)\sum_{i=1}^{i\times d\leq n}\sum_{j=1}^{j\times d\leq m}1$
- $=\sum_{d=1}^{N}\phi(d)\left\lfloor\frac{n}{d}\right\rfloor\left\lfloor\frac{m}{d}\right\rfloor$

- https://noip.ac/show_problem/3164

Problem 11

- 求$\sum_{i=1}^{n}\sum_{j=1}^{n}\gcd(i,j)$
- $n,m \le 10^{10}$

Problem 11

- 先转化式子
- $\sum_{i=1}^{n}\sum_{j=1}^{n}\gcd(i,j) = \sum_{d=1}^{n} d \sum_{i=1}^{i\times d\leq n}\sum_{j=1}^{j\times d\leq n}[\gcd(i,j) = 1]$
- $= \sum_{d=1}^{n} d \sum_{i=1}^{i\times d\leq n}\sum_{j=1}^{j\times d\leq n}\sum_{k|i,k|j}\mu(k)$
- $= \sum_{d=1}^{n} d \sum_{k=1}^{k*d\leq N}\mu(k)\left\lfloor\frac{n}{kd}\right\rfloor^2$
- $= \sum_{s=1}^{n}\left\lfloor\frac{n}{s}\right\rfloor^2\sum_{t|s} t\mu\left(\frac{s}{t}\right) = \sum_{s=1}^{n}\left\lfloor\frac{n}{s}\right\rfloor^2\phi(s)$

Problem 11

- 显然杜教筛
- 先外部用数论分块干掉$\left\lfloor \frac{n}{s} \right\rfloor$
- 然后用杜教筛求内部ϕ的区间和
- https://noip.ac/show_problem/3165

Problem 12

- 给定$x^A \equiv B(mod\ C)$
- 求x在$[0, C)$上整数解的个数
- $1 \le A, B, C \le 10^9$
- C是奇数

Problem 12

- 先做质因数分解，最后用中国剩余定理合并
- 则此时有$C = p^k$
- 分三种情况讨论
- $B \equiv 0\left(mod\ p^k\right)$
- $\gcd\left(B, p^k\right) > 1$
- $\gcd\left(B, p^k\right) = 1$

Problem 12

- $B \equiv 0 \pmod{p^k}$
- 这个时候只要保证x有至少$p^{\left\lceil \frac{k}{A} \right\rceil}$这个因子即可

Problem 12

- $\gcd(B, p^k) > 1$
- 则$B = p^r \times b$，则有$x^A \equiv p^r \times b (mod\ p^k)$
- 则必须有$A|r$
- 所以有$\left(p^{\frac{r}{A}} \cdot y\right)^A \equiv p^r \times b (mod\ p^k)$
- 所以有$y^A \equiv b (mod\ p^{k-r})$
- 转化为情况3

Problem 12

- $\gcd\left(B, p^k\right) = 1$
- 设原根为g
- 则$x = g^a, B = g^b$
- 所以$g^{aA} \equiv g^b \left(mod\ p^k\right)$
- $aA \equiv b\left(mod\ \phi\left(p^k\right)\right)$
- 然后就是小问题了

- https://noip.ac/show_problem/3166