

# 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 $\exists 0 \leq i < r, s.t. a^{d \times 2^i} \equiv -1 \pmod{n}$

# 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

- HDU 2138
- Luogu 3383
- BZOJ 4802

# 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 $\gcd(f_i - f_j, p) \neq 1$ ，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
- 没计算连续一段的乘积 然后再做 $gcd$ 是一样的效果
- 1、枚举 $i \in [2^j, 2^{j+1})$ , 计算所有 $(f_i - f_{2^j})$ 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

- BZOJ 3667
- Luogu 4718
- Bzoj 4522
- 都是裸题

# 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

# BZOJ 1420

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

# BZOJ 1420

- 求出原根 $g$
- 假设 $x = g^y, a = g^z$
- 则原方程变为
- $g^{ky} \equiv g^z \pmod{p}$
- $ky \equiv z \pmod{p-1}$
- EXGCD解之即可
- BZOJ 1319双倍经验

# BSGS

- 求  $a^x \equiv b \pmod p$  的一组解
- $p \leq 10^9$  且是质数



# P136 T3 改

- 求斐波那契数列关于给定数 $p$ 的循环节长度
- $p \leq 10^6$

# P136 T3 改

- 应用BSGS至矩阵乘法
- 不需要矩阵求逆
- 类似的题 BZOJ 4128

# HDU 2815

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

# HDU 2815

- 令  $A^x = Ct + B, g = \gcd(A, C)$
- 若  $B \bmod g \neq 0$  则无解
- 则式子变化为
- $\frac{A}{g} \cdot A^{x-1} = \frac{C}{g}t + \frac{B}{g} \Rightarrow \frac{A}{g} \cdot A^{x-1} = \frac{B}{g} \left( \bmod \frac{C}{g} \right)$
- 则转化为了原来的问题
- 双倍经验 SPOJ 3105

# 拓展中国剩余定理

- ~~• 其实我完全不知道中国剩余定理有拓展一说~~
- ~~• 我所知道的方法是可以解决模数不互质等情况的~~
- 问题定义：
- 给定 $N$ 个方程
- $x \equiv b_i \pmod{m_i}$
- 求 $x$

# 方法一：大数翻倍法

- 考虑合并两个方程
- $x \equiv b_1 \pmod{p_1}, x \equiv b_2 \pmod{p_2}, p_1 > p_2$
- 则暴力枚举
- $b_1, b_1 + p_1, b_1 + 2p_1, \dots$
- 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
- $x \equiv b_1 \pmod{p_1}, x \equiv b_2 \pmod{p_2}$
- 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
- $\frac{p_1}{g} k_1 \equiv \frac{b_2 - b_1}{g} \pmod{\frac{p_2}{g}}$
- 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 (线性筛法)

```
1: for (int i = 2; i <= n; ++ i) {  
2:     if (!not_prime[i]) prime[++ prime_cnt] = i;  
3:     for (int j = 1; j <= prime_cnt; ++ j) {  
4:         if (prime[j] * i > n) break;  
5:         not_prime[prime[j] * i] = true;  
6:         if (i % prime[j] == 0) break;  
7:     }  
8: }
```



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

# 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 $g$
- $\sum_{i=1}^n (f * g)(i) = \sum_{i=1}^n \sum_{d|i} g(d) f\left(\frac{i}{d}\right)$
- $= \sum_{d=1}^n g(d) \sum_{i=1}^{\lfloor \frac{n}{d} \rfloor} f(i) = \sum_{d=1}^n g(d) S\left(\left\lfloor \frac{n}{d} \right\rfloor\right)$

# 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
- $f * g = n^2 \sum_{d|n} \phi(d) = n^3$

# HDU 4610

- 4个条件： $N$ 是质数、 $N$ 的因子个数是质数、 $N$ 的所有因子之和是质数、 $N$ 的所有因子的乘积是一个完全平方数
- 一个数每满足一个条件加一分
- 给定 $N$ 个不超过 $10^6$ 的数，从里面选 $K$ 个使得分数的和最大
- $N \leq 10^4$

# HDU 4610

- 核心问题只有第三点比较麻烦
- 使用miller rabin解决第三点即可

# BZOJ 2257

- 给定 $N$ 个数，要求从这 $N$ 个数中找 $K$ 个数，使得这 $K$ 个数的最大公因数最大
- $N \leq 1000$

# BZOJ 2257

- 质因数分解统计次数
- 排序选最大即可

# BZOJ 1129

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



# BZOJ 1129

- 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

# BZOJ 2005

- 求  $\sum_{i=1}^n \sum_{j=1}^m \gcd(i, j)$
- $n, m \leq 10^6$

# BZOJ 2005

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

51NOD 1237

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

- $n, m \leq 10^{10}$

# 51NOD 1237

- 先转化式子

- $\sum_{i=1}^n \sum_{j=1}^n \gcd(i, j) = \sum_{d=1}^n d \sum_{i=1}^{i \times d \leq n} \sum_{j=1}^{j \times d \leq n} [\gcd(i, j) = 1]$

- $= \sum_{d=1}^n d \sum_{i=1}^{i \times d \leq n} \sum_{j=1}^{j \times d \leq n} \sum_{k|i, k|j} \mu(k)$

- $= \sum_{d=1}^n d \sum_{k=1}^{k \times d \leq n} \mu(k) \left\lfloor \frac{n}{kd} \right\rfloor^2$

- $= \sum_{s=1}^n \left\lfloor \frac{n}{s} \right\rfloor^2 \sum_{t|s} t \mu\left(\frac{s}{t}\right) = \sum_{s=1}^n \left\lfloor \frac{n}{s} \right\rfloor^2 \phi(s)$

# 51NOD 1237

- 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 $\phi$ 的区间和

# BZOJ 2219

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

# BZOJ 2219

- 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
- $B \equiv 0 \pmod{p^k}$
- $\gcd(B, p^k) > 1$
- $\gcd(B, p^k) = 1$



# BZOJ 2219

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

# BZOJ 2219

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

# BZOJ 2219

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

如果我们有时间 我们再讲这个

# 組合數求模

## Example

組合數的定義想必大家都是知道的：

$$C_m^n = \frac{n!}{m!(n-m)!}$$

給出非負整數  $n, m$  和正整數  $k$ , 求  $C_m^n \bmod k$ 。

## Solution

先來一些簡單點的情況。

- $k = 1$ , 這種情況過於困難, 不用管了。
- $k > 1, 0 \leq nm \leq 10^7$ 。  $O(nm)$  遞推。
- $n \leq 10^9, m \leq 10^4, k \leq 10^9$ , 由於  $C_m^n = \frac{n(n-1)(n-2)\cdots(n-m+1)}{m!}$ , 可以發現分子分母的項數都是可以接受的, 這就又有兩種方法:
  - 對每個數字分解素因子, 合併後用快速幂。
  - 對每個數字值分解  $k$  所含有的素因子, 分母剩餘的部分用逆元解決。

# 組合數求模

## Solution

然後我們稍微增加點難度。

- $n, m \leq 10^6, k \leq 10^9$ , 對  $n!$  分解素因子, 大致複雜度是  $O(n)$ 。
- $n, m \leq 10^{10}, k$  是素數且較小, 使用 *Lucas* 定理。

## Theorem (Lucas 定理)

$$C_m^n \bmod p = \prod_{i=0}^h C_{m_i}^{n_i} \bmod p$$

這裏  $n_i$  和  $m_i$  表示把  $n$  和  $m$  分解為  $p$  進制時第  $i$  位的值。

## Solution

最後考慮這麼一種數據範圍,  $n, m \leq 10^9, k \leq 10^5$ 。

首先,我們可以利用中國剩餘定理,可以發現問題等價於求  $C_m^n \bmod p^c$ ,  $p$  是素數,  $c \geq 1$ 。

我們考慮計算  $n!$ , 把中間的  $p$  都除開算出一個值, 同時算出除開的  $p$  的個數。  
例如  $n = 19, p = 3, c = 2$ , 考慮  $19!$ :

$$19! = (1 \times 2 \times 4 \times 5 \times 7 \times \cdots \times 16 \times 17 \times 19) \times 3^6 \times (1 \times 2 \times 3 \times \cdots \times 6)$$

令  $f(n)$  表示  $n!$  中除去  $p$  因子後模  $p^c$  的值。若要求  $f(19)$ , 那麼就是上式的前半部分, 然後  $3^6$  提出來, 最後一部分對答案的貢獻是  $f(6)$ , 即  $f(\lfloor \frac{n}{p} \rfloor)$ 。對於前面, 又有:

$$1 \times 2 \times 4 \times 5 \times 7 \times 8 \equiv 10 \times 11 \times 13 \times 14 \times 16 \times 17 \pmod{9}$$

這是有週期的, 而且乘積的項數也不會超過  $p^c$ , 所以可以進行預處理。然後從  $f(n)$  遞歸到  $f(\lfloor \frac{n}{p} \rfloor)$ , 層數  $O(\log_p n)$ 。