Math in OI (Discrete Part)

吴克文

2018 年 1 月 23 日

Section 1

数论

引入题

从 1 至 N 中选出最多数量的数，使它们两两不存在整除关系

$N < 10^6$

辗转相除法

- $\gcd(a, b) = \gcd(b\%a, a)$
- $\gcd(a, b) = \gcd(a, b - a) = \cdots = \gcd(a, b\%a)$
- 复杂度

扩展欧几里得

设 $(a, b) = k$, 求满足 $ax + by = c$ 的解

hint

- $(b\%a)x' + ay' = 1$
- $(b - a\left\lfloor \frac{b}{a} \right\rfloor)x' + ay' = 1$
- $x = y' - \frac{b}{a}x', y = x'$
- 迭代求解

费马小定理

$a^{p-1} \equiv 1 \mod p,\ (a,p)=1$

欧拉定理

$a^{\phi(n)} \equiv 1 \mod n,\ (a,n)=1$

威尔逊定理

$(p-1)! \equiv -1 \mod p$

逆元

$ax \equiv 1 \mod b$

$ax \equiv c \mod b$

hint

EXGCD 或欧拉定理 (费马小定理)

线性求逆

线性求出 $1-n$ 对 p 的逆元

线性求逆

线性求出 $1-n$ 对 p 的逆元

轻而易举

$(ab)^{-1} \equiv a^{-1}b^{-1} \mod p$

素数分布 $\frac{n}{\ln n}$

欧拉线性筛 + 暴力求逆

再简单点?

$$x^{-1} \equiv (x!)^{-1} \times (x-1)! \mod p$$

再简单点?

$x^{-1} \equiv (x!)^{-1} \times (x-1)! \mod p$

一行搞定?

$$p = a\lfloor\frac{p}{a}\rfloor + p\%a$$

$$a\left\lfloor\frac{p}{a}\right\rfloor \equiv -(p\%a) \mod p$$

$$a\left\lfloor\frac{p}{a}\right\rfloor \times (-(p\%a)^{-1}) \equiv 1 \mod p$$

$$a^{-1} \equiv \left\lfloor\frac{p}{a}\right\rfloor \times (-(p\%a)^{-1}) \mod p$$

CRT

$$x \equiv a_i \mod b_i$$

b_i互质

CRT

$$x \equiv a_i \mod b_i$$

$$b_i\text{互质}$$

hint

$$B = \prod_{i=1}^{n} b_i \to B_i\text{为}\frac{B}{b_i}\text{对}b_i\text{的逆}$$

$$x \equiv \sum_{i=1}^{n} a_i \times \frac{B}{b_i} \times B_i \mod \left(\prod_{i=1}^{n} b_i\right)$$

模线性方程组的合并

$$x \equiv a_i \mod b_i$$

b_i不一定互质

模线性方程组的合并

$$x \equiv a_i \mod b_i$$

b_i不一定互质

hint

$$x \equiv r_1 \mod m_1$$

$$x \equiv r_2 \mod m_2$$

$$m_1 u + m_2 v = r_2 - r_1 \rightarrow u'$$

$$x \equiv u' \times m_1 + r_1 \mod lcm(m_1, m_2)$$

简单题

未知数 x, 给出 $x\%c_i$ 的结果 $\{b_i\}$
试确定是否能获得 $x\%y$ 的值

简单题

未知数 x, 给出 $x\%c_i$ 的结果 $\{b_i\}$
试确定是否能获得 $x\%y$ 的值

hint

$(a\%(b\times c))\%c = a\%c$

Lucas 定理

$$\binom{n}{k} \equiv \prod \binom{A_i}{B_i} \mod p$$

$\{A_n\}, \{B_n\}$ 分别为 n, k 的 p 进制各数位

$$(1+x)^{ap+b} \equiv (1+x)^{pa}(1+x)^b \equiv (1+x^p)^a(1+x)^b$$

$$\text{记} n = ap+b, k = cp+d$$

$$\binom{ap+b}{cp+d}x^k = \binom{a}{c}x^{cp}\binom{b}{d}x^d$$

原根

a 作为 p 的原根，则有 $a^x \equiv 1 \mod p$ 的最小正整数解为 $p-1$

性质

a 生成的乘法群包含所有 F_p 的非零元
乘法 $\Rightarrow$ 加法

BSGS

$$a^x \equiv b \mod c,\ (a, c) = 1$$

BSGS

$a^x \equiv b \mod c, \ (a, c) = 1$

hint

$x = u \lfloor \sqrt{\phi} \rfloor + v$

meet in the middle

BSGS+

$a^x \equiv b \mod c,\ (a, c) = t$

BSGS+

$a^x \equiv b \mod c,\ (a, c) = t$

hint

$$a^u a^v \equiv b \mod c$$

$$\text{使得}(a^v, c) = (a^{v+1}, c)$$

Miller-Robin 1

快速检验 p 是否为素数
利用 $a^{p-1} \% p = 1$，可以选取若干 a，利用快速幂判断模 p 后是否为 1
能骗过底数 a 的合数称为以 a 为底的伪素数
能骗过所有小于 p 的底数的合数称为 Carmichael 数 (561)
由于这类数的存在 (尽管稀疏)，还需加强测试

Miller-Robin 2

考虑到如下事实，如果 p 是素数，且 $x^2\%p = 1$，则 x 等于 1 或-1
因此将 p-1 分解为 $d2^r$，先计算 a^d，再逐步平方，检查每次平方结果是否为 1，若是，则判断前次结果是否为 ±1 (二次探测)
合起来就是完整 MR 素性测试
通过以 a 为底的 MR 测试的合数称作以 a 为底的强伪素数 (2,2047)
由于这类数的存在，需要多选取一些 a 进行测试

Miller-Robin 3

$2,7,61 \Rightarrow 4759123141$
$2,3,5,7,11,13,17 \Rightarrow 341550071728320$
$2,3,7,61,24251 \Rightarrow 10^{16}$ (除了 46856248255981)

可以近似认为 k 个底数的测试失误率约为 0.25^k

一般常用第三组

一道 NOIP--题

给出一个大整数 n，将它质因数分解

$n < 10^{18}$

Pollard-Rho

先素性测试
随机 m 个数，两两做差判断是否为 n 的因数，然后递归分解
当 $m \sim \sqrt{n}$ 时，概率约为 0.5

Pollard-Rho

先素性测试
随机 m 个数，两两做差判断是否为 n 的因数，然后递归分解
当 $m \sim \sqrt{n}$ 时，概率约为 0.5
随机 m 个数，两两做差与 n 求 gcd，然后递归分解，概率大大提升

Pollard-Rho

先素性测试
随机 m 个数，两两做差判断是否为 n 的因数，然后递归分解
当 $m \sim \sqrt{n}$ 时，概率约为 0.5
随机 m 个数，两两做差与 n 求 gcd，然后递归分解，概率大大提升
它的准确率之高甚至不需要两两做差
利用随机函数 $f(x) = x^2 + a \mod p$，每次生成两个随机数，做差求 gcd 即可

Pollard-Rho

先素性测试
随机 m 个数，两两做差判断是否为 n 的因数，然后递归分解
当 $m \sim \sqrt{n}$ 时，概率约为 0.5
随机 m 个数，两两做差与 n 求 gcd，然后递归分解，概率大大提升
它的准确率之高甚至不需要两两做差
利用随机函数 $f(x) = x^2 + a \mod p$，每次生成两个随机数，做差求 gcd 即可
循环怎么办？Floyd 判环法，利用一个两倍速指针，如果两个指针相遇，则已循环

算法流程：

1. 对 n 进行素性测试
2. 随机选取 a 和大素数 p
3. 随机启始点 x 和两倍速点 y
4. x=f(x)， y=f(f(y))
5. 如果 x=y 则已循环，重新尝试分解
6. 利用 x-y 与 n 做 gcd，如果可约则退出
   否则回到第 4 步

取整

$$\left\lceil \frac{A}{B} \right\rceil = \left\lfloor \frac{A+B-1}{B} \right\rfloor = \left\lfloor \frac{A-1}{B} \right\rfloor + 1 \tag{1}$$

$$\left\lfloor \frac{\left\lfloor \frac{A}{B} \right\rfloor}{C} \right\rfloor = \left\lfloor \frac{A}{B \times C} \right\rfloor \tag{2}$$

取模

$$(Ag)\%(Bg) = (A\%B) \times g$$

$$(A\%(BC))\%C = A\%C$$

$$A\%B = A - \left\lfloor \frac{A}{B} \right\rfloor \times B$$

快速幂 $\rightarrow$ 快速乘

μ 函数

$$\mu(x) = \begin{cases} (-1)^k & x = \prod_1^k p_i \\ 0 & \exists p^2 | x \end{cases}$$

$\mu(1) = 1$ 复杂度?

μ 函数

$$\mu(x) = \begin{cases} (-1)^k & x = \prod_1^k p_i \\ 0 & \exists p^2 | x \end{cases}$$

$\mu(1) = 1$ 复杂度?

反演公式

$F(n) = \sum_{d|n} G(d)$
$G(n) = \sum_{d|n} \mu(d) F(\frac{n}{d})$

直观理解? 容斥原理

$$\sum_{d|n}\mu(d)=\begin{cases}1 & n=1\\0 & n>1\end{cases}$$

反演的证明?

$$\sum_{d|n}\mu(d)=\begin{cases}1 & n=1\\ 0 & n>1\end{cases}$$

反演的证明?

$\sum_{d|n}\mu(d)F(\frac{n}{d})$
$=\sum_{d|n}\mu(d)\sum_{k|\frac{n}{d}}F(k)$
$=\sum_{k|n}G(k)\sum_{d|\frac{n}{k}}\mu(d)$

可见点

有个人站在原点向第一象限看去，求在坐标范围 $[1,n]\times[1,m]$ 间的可见整点数

可见点

有个人站在原点向第一象限看去，求在坐标范围 $[1,n]\times[1,m]$ 间的可见整点数

hint

μ 函数的常见用法：

$[gcd(a,b)=1]=\sum_{d|gcd(a,b)}\mu(d)=\sum_{d|a,d|b}\mu(d)$

$\sum_{d=1}^{n}\mu(d)[\frac{n}{d}][\frac{m}{d}]$

快速求解

$\sum_{d=1}^{n} \mu(d)[\frac{n}{d}][\frac{m}{d}]$

快速求解

$\sum_{d=1}^{n} \mu(d)[\frac{n}{d}][\frac{m}{d}]$

hint

$$\forall j \in \left[i, \left[\frac{n}{[\frac{n}{i}]}\right]\right], [\frac{n}{j}] \equiv k$$

另类 μ 函数

也许你们听说过集合逆卷积

$$\mu(S) = \sum_{S' \subset S} (-1)^{|S'|}$$

$$\sum_{S' \subset S} \mu(S') = \begin{cases} 1 & S = \varnothing \\ 0 & S \neq \varnothing \end{cases}$$

$$\begin{cases} F(S) = \sum_{S' \subset S} G(S') \\ G(S) = \sum_{S' \subset S} \mu(S') F(S - S') \end{cases}$$

二项式反演

$$\begin{cases} F(n) = \sum_{i=0}^{n} \binom{n}{i} G(i) \\ G(n) = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} F(i) \end{cases}$$

证明核心：

$$\sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \binom{i}{m} = \begin{cases} 1 & n = m \\ 0 & n > m \end{cases}$$

错位排列

求 n 个元素恰好 m 个错位的方案数

错位排列

求 n 个元素恰好 m 个错位的方案数

hint

$\sum_{k=0}^{n} \binom{n}{k} D_k = n!$
$D_m = m! \sum_{k=0}^{m} (-1)^k \frac{1}{k!}$

映射计数

求 m 元集到 n 元集的满射方案数

映射计数

求 m 元集到 n 元集的满射方案数

hint

$n^m = \sum_{k=0}^{n} \binom{n}{k} g(m,k)$

$g(m,n) = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^m$

Section 2

矩阵

定义

线性无关：一组向量 $\{v_k\}$，如果不存在非全零数列 $\{a_k\}$，使得 $\sum a_i v_i = 0$，则称这组向量线性无关
线性相关：存在非全零数列 $\{a_k\}$，使得 $\sum a_i v_i = 0$

example

$(1,0),(1,2)$ 线性无关
$(1,0,1),(2,3,3),(0,3,1)$ 线性相关

基底

基底：一组可以生成整个线性空间的线性无关组 (任何向量均可由基底线性表出)
$\mathbb{R}^n$ 是 n 维线性空间，它的一组基底由 n 个线性无关的向量组成
基向量的选取有很多种

example

以 $\mathbb{R}^3$ 为例，$(1,0,0),(0,1,0),(0,0,1)$ 是常见的选法
$(e,0,\pi),(2,3,3),(0,0,976528)$ 同样也是一组基

特殊线性空间

$\mathbb{F}_p$ 在 $\mathbb{F}_p^n$ 上的乘法作用生成的线性空间
特别的，$p = 2$ 时，乘法表现为 and 运算，加法表现为 xor 运算

example

0b101,0b011,0b001 是一组 $\mathbb{F}_2^3$ 的一组基

模板题

给出一组 $\mathbb{Q}$ 上线性方程组，求出它的一组解或判断无解

模板题

给出一组 $\mathbb{Q}$ 上线性方程组，求出它的一组解或判断无解

模板题 +

给出一组模线性方程组，求出它的一组解或判断无解

模板题

给出一组 $\mathbb{Q}$ 上线性方程组，求出它的一组解或判断无解

模板题 +

给出一组模线性方程组，求出它的一组解或判断无解

模板题 ++

给出一组 $\mathbb{Q}$ 上一组线性关系，求出它的线性基

简单题

给出一个矩阵 $A_{n\times n}$，求出它的逆矩阵或判断不可逆

一些结论

行向量线性无关 $\Rightarrow$ 矩阵有右逆
列向量线性无关 $\Rightarrow$ 矩阵有左逆
方阵 $\Rightarrow$ 行向量组线性无关等价于列向量组线性无关

定义

行列式仅对方阵有定义

$$\det A = \sum_{\pi} (-1)^{\sigma(\pi)} \prod_{i} A_{i,\pi(i)}$$

物理解释：n 维空间立方体的有向体积

人力算法

二阶矩阵：$ad - bc$(平行四边形面积)
三阶矩阵：看我画图 TAT

一些结论

某一行加上另一行的若干倍：行列式不变
某两行交换：行列式变号
某一行乘 k：行列式乘 k
矩阵转置：行列式不变
某一列 (行) 分裂：行列式分裂求和

均可以用粗略的物理直观解释

一些结论

某一行加上另一行的若干倍：行列式不变
某两行交换：行列式变号
某一行乘 k：行列式乘 k
矩阵转置：行列式不变
某一列 (行) 分裂：行列式分裂求和

均可以用粗略的物理直观解释

计算机算法

初等行列变换将矩阵消至上三角
记录过程中的变更信息
上三角矩阵的行列式求法?

行列式

给出一个 n 阶整系数矩阵的第一行，问是否有可能填充剩余位置，使得行列式为 K，并给出一个可行方案

$n < 200, K < 10^{18}$

基尔霍夫矩阵与生成树定理

$S = D - A$，D 为度数矩阵，A 为邻接矩阵，S 为基尔霍夫矩阵
无向图的生成树个数即为 S 任一个主子式的行列式

有向版本

$S = D - A$，D 为出度矩阵，A 为邻接矩阵，S 为基尔霍夫矩阵
有向图以 i 为根的内向树个数即为主子式 S_i 的行列式

简单题

$M \times M$ 的格状矩形，每个格子是房间或是柱子。相邻的格子之间都有墙隔着
你想要打通一些墙，使得所有房间能够互相到达。在此过程中，你不能把房子给打穿，或者打通柱子 (以及柱子旁边的墙)
同时，你希望任意两个房间之间都只有一条通路
统计一共有多少种可行的方案，对 $10^9 + 7$ 取模

$N, M < 10$

简单题

$M \times M$ 的格状矩形，每个格子是房间或是柱子。相邻的格子之间都有墙隔着

你想要打通一些墙，使得所有房间能够互相到达。在此过程中, 你不能把房子给打穿，或者打通柱子 (以及柱子旁边的墙)

同时, 你希望任意两个房间之间都只有一条通路

统计一共有多少种可行的方案，对 $10^9 + 7$ 取模

$N, M < 10$

简单题 +

方案数对 Q 取模

$N, M < 10, Q < 10^{18}$

特殊矩阵

- 稀疏矩阵 $\Rightarrow$ ijk 循环的顺序
- 循环矩阵 $\Rightarrow O(N^3)$?
- 对称矩阵 $\Rightarrow$ 乘一半
- 分块矩阵 $\Rightarrow$ 分块乘法

简单题

给出一个有向图，启始点为 1，求 k 步走到 n 号点的方案数

简单题

给出一个有向图，启始点为 1，求 k 步走到 n 号点的方案数

简单题 +

给出一个有向图，启始点为 1，求 k 步内走到 n 号点的方案数

简单题

给出一个有向图，启始点为 1，求 k 步走到 n 号点的方案数

简单题 +

给出一个有向图，启始点为 1，求 k 步内走到 n 号点的方案数

简单题 ++

给出一个有向图，启始点为 1，边权为转移概率，保证 $\sum_j p_{i,j} = 1$，求第 k 步在 n 号点的概率

递推求解

$A_n = uA_{n-1} + vA_{n-2}$，求 A_N
$N < 10^{18}$

递推求解

$A_n = uA_{n-1} + vA_{n-2}$，求 A_N

$N < 10^{18}$

递推求解 +

$A_n = \sum_i^M b_i \times A_{n-i} + A_{n-2}$，求 A_N

$N < 10^{18}, M < 100$

递推求解

$A_n = uA_{n-1} + vA_{n-2}$，求 A_N

$N < 10^{18}$

递推求解 +

$A_n = \sum_i^M b_i \times A_{n-i} + A_{n-2}$，求 A_N

$N < 10^{18}, M < 100$

递推求解 ++

$A_n = \sum_i^M b_i \times A_{n-i} + A_{n-2}$，求 A_N

$N < 2^{100}, M < 200$

CH 定理

矩阵的特征多项式是它的零化多项式

$f(x) = |xI - A| \implies f(A) = 0$

有啥用啊

矩阵的线性表出

N^2 阶 $\Rightarrow N$ 阶

Section 3

卷积

棣莫弗定理

$x^n = 1 \Rightarrow x_n^k = \xi_n^k = e^{2\pi i \times \frac{k}{n}}$

$\xi_n^k \times \xi_n^j = \xi_n^{k+j} = \xi_n^{(k+j)\%n}$

$\overline{\xi_n^k} = \xi_n^{n-k}$

$\sum_{k=0}^{n-1} \xi_n^k = 0$

多项式卷积

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$
$g(x) = b_0 + b_1 x + \cdots + b_m x^m$
求 $h(x) = f(x) \times g(x)$

hint

n 次多项式 $\Rightarrow$ n+1 个点唯一插值表示
(回忆拉格朗日插值法)
卷积 $\Rightarrow$ 点值乘法
系数表示法 $\Rightarrow$ 点值表示法

$$f(x) : (x_i, y_i), 0 \leqslant i \leqslant m+n$$
$$g(x) : (x_i, y_i'), 0 \leqslant i \leqslant m+n$$
$$h(x) : (x_i, y_i \times y_i'), 0 \leqslant i \leqslant m+n$$

算法思路

$f(x)$ 系数表示 $\Rightarrow f(x)$ 点值表示
$g(x)$ 系数表示 $\Rightarrow g(x)$ 点值表示
点值相乘 $\Rightarrow h(x)$ 点值表示 $\Rightarrow h(x)$ 系数表示

选取精妙的点
使得从系数表示到点值表示，以及从点值表示到系数表示的转换更快

系数转点值，不妨设 $n = 2^m$

$$
\begin{aligned}
f_n(\xi_n^k) &= a_0 + a_1\xi_n^k + a_2\xi_n^{2k} + \cdots + a_{2^m-1}\xi_n^{(2^m-1)k} \\
&= (a_0 + a_2\xi_n^{2k} + \cdots + a_{2^m-2}\xi_n^{(2^m-2)k}) + \\
&\quad \xi_n^k(a_1 + a_3\xi_n^{2k} + \cdots + a_{2^m-1}\xi_n^{(2^m-2)k}) \\
&= (a_0 + a_2\xi_{\frac{n}{2}}^k + \cdots + a_{2^m-2}\xi_{\frac{n}{2}}^{tk}) + \\
&\quad \xi_n^k(a_1 + a_3\xi_{\frac{n}{2}}^k + \cdots + a_{2^m-1}\xi_{\frac{n}{2}}^{tk}) \\
&= f_{\frac{n}{2}}(\xi_{\frac{n}{2}}^k) + \xi_n^k \times g_{\frac{n}{2}}(\xi_{\frac{n}{2}}^k)
\end{aligned}
$$

这为啥是 $N\log N$??

点值转系数 (IDFT)，同样假设 $n = 2^m$
记矩阵 $F = [\xi_n^{ij}]_{0\leqslant i,j\leqslant n-1}$

$$F = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \xi_n^1 & \xi_n^2 & \cdots & \xi_n^{n-1} \\ 1 & \xi_n^2 & \xi_n^4 & \cdots & \xi_n^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \xi_n^{n-1} & \xi_n^{2(n-1)} & \cdots & \xi_n^{(n-1)^2} \end{bmatrix}$$

则有

$$F\begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} f(\xi_n^0) \\ f(\xi_n^1) \\ \vdots \\ f(\xi_n^{n-1}) \end{bmatrix}$$

故系数矩阵即为 $F^{-1}X$

$$F^{-1}=\frac{1}{n}\overline{F}=\frac{1}{n}\begin{bmatrix}1 & 1 & 1 & \cdots & 1\\ 1 & \xi_n^{n-1} & \xi_n^{n-2} & \cdots & \xi_n^{1}\\ 1 & \xi_n^{n-2} & \xi_n^{n-4} & \cdots & \xi_n^{n-2(n-1)}\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ 1 & \xi_n^{n-(n-1)} & \xi_n^{n-2(n-1)} & \cdots & \xi_n^{n-(n-1)^2}\end{bmatrix}$$

可以画一个 F_5 验证一下

直观理解 $\overline{F}$?
除了第一行，后面的行成对交换！

$$记F=\begin{bmatrix} v_0 \\ v_1 \\ v_2 \\ \vdots \\ v_{n-1} \end{bmatrix},则\overline{F}=\begin{bmatrix} v_0 \\ v_{n-1} \\ v_{n-2} \\ \vdots \\ v_1 \end{bmatrix}$$

所以类似地对换 $f(\xi_n^k)$，将它当作系数做点值转换 (IDFT)，最后再对换回即可

多项式卷积

$f(x) = a_0 + a_1 x + \cdots + a_n x^n$

$g(x) = b_0 + b_1 x + \cdots + b_m x^m$

求 $h(x) = f(x) \times g(x)$

系数对 $p = k2^t + 1$ 取模 (p 是素数)

多项式卷积

$f(x) = a_0 + a_1x + \cdots + a_nx^n$
$g(x) = b_0 + b_1x + \cdots + b_mx^m$
求 $h(x) = f(x) \times g(x)$
系数对 $p = k2^t + 1$ 取模 (p 是素数)

hint

依然将 n 扩充为 2 的次幂
把原根 a 当作 ξ_n^1 即可 $\xi_n^k = a^{(p-1)\frac{k}{n}}$
n 次单位复根 $\Rightarrow F_p$ 上原 n 次单位根
然后跟 FFT 一毛一样 (注意除 n 时使用逆元)

若多项式系数不是很大，可以使用 NTT 代替 FFT

K 进制大整数乘法

给出两个 K 进制的大整数，求他们乘法后的 L 进制表示

K 进制大整数乘法

给出两个 K 进制的大整数，求他们乘法后的 L 进制表示

卷积式 DP 转移

$H_n = \sum F_i \times G_{n-1-i}$

构造生成函数 $f(x) = \sum F_i x^i$ 和 $g(x) = \sum G_i x^i$

类阶乘函数

求 $f(x) = \prod_{i=1}^{m}(x+i)$ 的系数表示

类阶乘函数

求 $f(x) = \prod_{i=1}^{m}(x+i)$ 的系数表示

hint

分治 FFT
$O(N\log^2 N)$

集合取数

给定整数集合 S，试问有多少中从 S 中取出 n 个数 (可重复) 的方案，使选出的数的积对 p 取模为 x，方案数对 1004535809 取模

$p < 8000, n < 10^9$

集合取数

给定整数集合 S，试问有多少中从 S 中取出 n 个数 (可重复) 的方案，使选出的数的积对 p 取模为 x，方案数对 1004535809 取模

$p < 8000, n < 10^9$

hint

$1004535809 = 479 \times 2^{21} + 1$

利用原根将乘法转化为加法

一些结论

$$\binom{n}{m} + \binom{n}{m-1} = \binom{n+1}{m} \tag{3}$$

$$\sum_{i=0}^{n} \binom{n}{i} = 2^n \tag{4}$$

$$\sum_{k=0}^{\lfloor n/2 \rfloor} \binom{n}{2k} = 2^{n-1} \tag{5}$$

$$m\binom{n}{m} = n\binom{n-1}{m-1} \tag{6}$$

计数

n 个人坐在 m 张凳子上
m 张凳子形成圆环
任意两个人的环上距离不小于 k，求方案数

PS: 循环翻转视为不同
$0 < n, m < 10^6, 0 < k < 100$, 多测

example

2 5 1
Ans=5

弱化问题

n 个人坐在 m 张凳子上
m 张凳子排成一列
任意两个人的距离不小于 k，求方案数

弱化问题

n 个人坐在 m 张凳子上
m 张凳子排成一列
任意两个人的距离不小于 k，求方案数

hint

考虑前 $n-1$ 个人, 并删去他后面的 k 张椅子
方案数即为

$$\binom{m-(n-1)k}{n}$$

hint

对于环的情况, 考虑破环成链
取长为 $k+1$ 的连续椅子
其中最多能放一个人
若放了一个人, 则问题转化为 $m-2k-1$ 的链上放 $n-1$ 个人
若未放人, 则问题转化为 $m-k-1$ 的链上放 n 个人

$$Ans = (k+1)\binom{m-2k-1-(n-2)k}{n-1} + \binom{m-k-1-(n-1)k}{n}$$

Trick: 一个人的时候 $Ans = m$

栈操作

有 n 个入栈操作和 m 个弹栈操作，求合法的操作序列方案数

Fibonacci 数列

$$A_n = \begin{cases} 0 & n = 0 \\ 1 & n = 1 \\ A_{n-1} + A_{n-2} & n > 1 \end{cases}$$

$$A_n = \frac{-\sqrt{5}}{5}\left(\frac{1-\sqrt{5}}{2}\right)^n + \frac{\sqrt{5}}{5}\left(\frac{1+\sqrt{5}}{2}\right)^n$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^n \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} A_n \\ A_{n+1} \end{bmatrix}$$

More Example

$$A_n = 5A_{n-1} - 6A_{n-2}$$
$$A_n + 2A_{n-1} + 3A_{n-2} = 7$$
$$A_n + 3A_{n-1} + 9A_{n-2} = 4^n$$
$$h_n = \sum_{i=0}^{n-1} h_i \times h_{n-1-i}$$

二项式展开

$$(x+a)^n = \sum_{k=0}^{n} \binom{n}{k} x^k a^{n-k} \tag{7}$$

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{8}$$

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k \tag{9}$$

$$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1) x^k \tag{10}$$

正 n 边形顶点连线, 连线仅在顶点处相交
划分为 $n-2$ 个三角形的方案数

n 个节点的有根二叉树形态数

长度为 n 的括号序列方案数

长度为 n 的括号序列方案数

hint

考虑 +-+–+ 与-+-+++ 的一一对应关系

$$Ans = \binom{n}{n/2} - \binom{n}{n/2+1}$$

从 $(0,0)$ 向右向上走到 (n,n)
不穿越对角线的方案数

从 $(0,0)$ 向右向上走到 (n,m)
不穿越 $y=x$ 的方案数

从 $(0,0)$ 向右向上走到 (n,m)
不穿越 $y=x$ 和 $y=x+m-n$ 的方案数

求满足以下要求带出 n 个物品的方案数

A,D:0 或 1	B:0 或 1 或 2
C:0 或 1 或 2 或 3	E: 奇数个
F: 偶数个	G:4 的倍数个
H:3 的倍数个	

Burnside 引理

$$S = \frac{1}{|G|}\sum_{i=1}^{|G|} c_1(\pi_i)$$

例

2*2 方格 01 染色问题，循环同构

Burnside 引理

$$S = \frac{1}{|G|}\sum_{i=1}^{|G|} c_1(\pi_i)$$

例

2*2 方格 01 染色问题，循环同构
2*2 方格 01 染色问题，循环翻折同构

Polya 计数

为解决染色问题中，Burnside 运算量过大的问题，改进提出 Polya 计数原理

$$S = \frac{1}{|G'|}\sum_{i=1}^{|G'|} M^{c(\pi_i)}$$

例

2*2 方格 01 染色问题，循环同构
2*2 方格 01 染色问题，循环翻折同构

简单题-

n 元环 m 染色，循环翻折同构，求方案数

$n < 1000, m < 10^5$

简单题-

n 元环 m 染色，循环翻折同构，求方案数

$n < 1000, m < 10^5$

简单题

n 元环 m 染色，循环翻折同构，求方案数

$n < 10^{12}, m < 10^5$

简单题 +

n 元环 m 染色，循环翻折同构
同时给出 k 组限制 a_i, b_i，要求不能有相邻的颜色为 a_i, b_i，求方案数

$n < 10^{12}, m < 100$

康托展开

求排列 $a_n, a_{n-1}, \cdots, a_1$ 的排名 T

$T = \sum rank(a_i) \times (i-1)!$

$rank(a_i)$ 表示 $a_1 \sim a_i$ 中 a_i 的排名 (从 0 开始)

康托展开

求排列 $a_n, a_{n-1}, \cdots, a_1$ 的排名 T

$T = \sum rank(a_i) \times (i-1)!$

$rank(a_i)$ 表示 $a_1 \sim a_i$ 中 a_i 的排名 (从 0 开始)

例

4，2，1，3 $\Rightarrow 3*3!+1*2!+0+0=20$

至于这个有什么用，大约可能会有那种求第 k 字典序大的题，然后可以和数据结构结合起来，用来二分 or 快速统计

Section 5

博弈论

Nim 游戏

经典组合游戏，n 堆石头，两个玩家轮流行动，每次选择某一堆石头，拿走数量大于 0 的石子，不能操作者输
问先手是否必胜

SG 函数

定义一个局面 X 经过一步操作后的所有后继局面集合为 S，
则 $SG(X) = mex\{SG(Y_i)\}, Y_i \in S$，即第一个不在 S 中的自然数
若 X 由若干个独立的子游戏 $X_1, \cdots, X_n$ 组成，则

$$SG(X) = \bigoplus_{k=1}^{n} SG(X_k)$$

SG 函数

定义一个局面 X 经过一步操作后的所有后继局面集合为 S，则 $SG(X) = mex\{SG(Y_i)\}, Y_i \in S$，即第一个不在 S 中的自然数
若 X 由若干个独立的子游戏 $X_1, \cdots, X_n$ 组成，则

$$SG(X) = \bigoplus_{k=1}^{n} SG(X_k)$$

解释

在 Nim 游戏中，单独一堆大小为 x 的石堆的局面为 x，$SG(x) = x$，整个局面的 SG 值为所有石堆大小的异或和计算出每个局面的 SG 值后，游戏便等效于 Nim 取石子游戏

SG 函数的性质

- SG(X) 非 0 时，存在一个后继局面 Y，使得 $SG(Y) = 0$ 分析：对 X 的某一个子游戏进行操作后 SG(X) 的改变，等效于异或上该子游戏 SG 值和小于该子游戏 SG 值的一个值。一定存在一个子游戏，SG 值二进制下最高位和 SG(X) 相同，异或之后剩下的值，可以补一个一模一样的数字直接将它消去。于是我们找到了一个后继局面 $SG(Y) = 0$
- SG(X) 为 0 时，对于所有后继局面 Y，都有 $SG(Y) \neq 0$ 分析：任意一个子游戏操作后，相当于 SG(x) 异或了两个不同的值。由于 $SG(x) = 0$, 那么一定有 $SG(Y) \neq 0$

重要推论

必胜态：存在一步操作，变成必败态
必败态：对于任意操作，变成必胜态
而由 SG 函数的这两个性质，我们可以得出，SG(X) 非 0 为必胜态，SG(X) 为 0 时为必败态

Crosses and Crosses

$1 \times n$ 的棋盘上，两人轮流行动，每次选择一个空格子画 X。若某人操作后，出现了连续 3 个 X，则他获得胜利
问先手是否必胜

$2 < n < 2000$

N 阶 NIM 和

从 m 堆石子中，每次选定不超过 n 堆，每堆至少取 1 个石子，不能取的人输
问先手是否必胜?

hint

每堆石子的 SG 函数依然是石子数量。
由于每次可以取 n 堆，此时一个局面的 SG 函数不再是简单的异或和。简单异或是每次只能取不超过 1 堆时的特殊情况。
设二进制位最高位为第 k 位。石堆 $x_i = SG(x_i) = \sum b_{ij} 2^j$，则对于局面 X

$$SG(X) = \sum_{j=0}^{k}((\sum_{i=0}^{m} b_{ij}) \mod (n+1)) \times 2^j$$

也即在二进制下，每一位求和后对 (n+1) 取模

Section 6

一些习题

一道奇怪的题

给出 x，试求出一个 y，使得

$$\phi(x+y)=\phi(y)$$

$x < 10^{18}$

一道奇怪的题

给出 x，试求出一个 y，使得

$$\phi(x+y) = \phi(y)$$

$x < 10^{18}$
$x < 10^{1000}$

轮状病毒

一个圆环上有 N 个点，每个点通过圆环与相邻的两个点直接相连，而且每个点与圆心有一条连边，试求生成树个数

$N < 10^{18}$

轮状病毒

一个圆环上有 N 个点，每个点通过圆环与相邻的两个点直接相连，而且每个点与圆心有一条连边，试求生成树个数

$N < 10^{18}$

hint

$F_i = 3F_{i-1} - F_{i-2} + 2$
不找规律怎么求行列式递推?
看我表演 TAT(挂黑板的话... 你们理解意思就行了

巨额奖金

给出一个带权无向图，求最小生成树的个数

$N < 100, M < 1000$
同权值边至多 10 条

巨额奖金

给出一个带权无向图，求最小生成树的个数

$N < 100, M < 1000$
同权值边至多 10 条

巨额奖金 +

给出一个带权无向图，求最小生成树的个数

$N < 500, M < 100000$

开门

N 个房间，M 把钥匙分散在不同房间，只要用了一下钥匙，就能被传送到那把钥匙对应的房间，但是钥匙一旦使用就会消失。现在你在 1 号房间，而任务是把所有的钥匙都用完，并且最后回到 1 号房间。你想知道完成这个任务有多少种方式
两种完成任务的方式算作不同当且仅当使用钥匙的顺序不同
(所有钥匙都是互不相同的)
答案对 1000003 取模

$N < 100, M < 200000$

开门

N 个房间，M 把钥匙分散在不同房间，只要用了一下钥匙，就能被传送到那把钥匙对应的房间，但是钥匙一旦使用就会消失。现在你在 1 号房间，而任务是把所有的钥匙都用完，并且最后回到 1 号房间。你想知道完成这个任务有多少种方式
两种完成任务的方式算作不同当且仅当使用钥匙的顺序不同
(所有钥匙都是互不相同的)
答案对 1000003 取模

$N < 100, M < 200000$

hint

有向图的欧拉回路个数

BEST 定理

有向图 G 的欧拉回路个数为

$$t(G,i)\times\prod_{j\in G}(r_j-1)!$$

其中，如果 $t(G,i)$ 是内向树的个数，那么 r_j 是 j 的出度；如果 $t(G,i)$ 是外向树的个数，那么 r_j 是 j 的入度

proof

每个内向树决定了除了根节点以外其余节点的第一次出边，之后所有的出边可以任意选择
对于根节点，可以强行选择某个方向作为第一次出边 (不然会重复计某一个欧拉环路，只是起点不同而已)
由乘法原理得到结论成立。

一道不知道放在哪里的题

$$b_i = \sum_{j=1}^{n} a_i \& a_j$$

$$c_i = \sum_{j=1}^{n} a_i | a_j$$

给出 $\{b_n\}$ 和 $\{c_n\}$, 试构造 $\{a_n\}$ 或判断无解

Example

b: 6 8 4 4
c: 16 22 10 10
a: 3 5 1 1

取模序列

给出序列 $\{A_n\}$
每次询问 L 至 R

$$F(L,R) = \begin{cases} A_i & L = R \\ F(L,R-1) \mod A_R & L < R \end{cases}$$

$n < 10^5, q < 10^5$

取模序列

给出序列 $\{A_n\}$
每次询问 L 至 R

$$F(L,R)=\begin{cases} A_i & L=R \\ F(L,R-1) \mod A_R & L<R \end{cases}$$

$n<10^5, q<10^5$

hint

$$\forall n \geqslant m,\ n\%m \leqslant \left\lfloor \frac{n}{2} \right\rfloor$$

dzy loves math

$$\sum_{i=1}^{a}\sum_{j=1}^{b} f(gcd(i,j))$$

$$f(n) = \max\{k, p^k | n\}$$

又是一个圆桌问题

n 对夫妇围坐在有 2n 个座位的圆桌旁，要求每个丈夫不能与自己的妻子或其他丈夫相对而坐，求方案数 (旋转同构)
每个人的标号不同

又是一个圆桌问题

n 对夫妇围坐在有 2n 个座位的圆桌旁，要求每个丈夫不能与自己的妻子或其他丈夫相对而坐，求方案数 (旋转同构)
每个人的标号不同

hint

n 个丈夫固定后，剩余的即是一个错排
$2^{n-1} \cdot (n-1)! \cdot n! \cdot (\sum_{k=2}^{n} (-1)^k \frac{1}{k!})$

我也不知道起什么名字

求 $(\frac{\sqrt{5}+1}{2})^n$ 的整数部分对 M 取模的结果

我也不知道起什么名字

求 $(\frac{\sqrt{5}+1}{2})^n$ 的整数部分对 M 取模的结果

hint

构造数列使特征值为 $\phi, \frac{1}{\phi}$

$A_{n+1} + A_{n-1}$ 来消除乘法因子的影响

我还是不知道起什么名字

圆桌边有 n 个座位，一种坐人的方案合法当且仅当没有人的左右手边坐着人，求方案数 (循环同构视为相同)

$n < 10^{12}$

A Funny Stone Game

游戏中，有 n 堆石子，被编号为 0 到 n-1。两名玩家轮流取石子。每一轮游戏，每名玩家选取 3 堆石子 i，j，k ($i < j, j \leqslant k$，且至少有一枚石子在第 i 堆石子中)，从 i 中取出一枚石子，并向 j，k 中各放入一枚石子 (如果 $j = k$ 则向 k 中放入 2 颗石子)。最先不能取石子的人输

石子堆的个数不会超过 23，每一堆石子不超过 1000 个

hint

每一堆的每个石子之间都是相互独立的
将第 i 位每一个石子看做一个子游戏，每一步操作都是删除该石子并在 j，k 位置各增加一个石子
这样分解后，在 n^3 计算每个子游戏的 SG 值
然后再在 $O(\sum a_i)$ 时间内计算整个 SG 值

这是一道真正的反演题

解出 x_i

$$\forall i, \sum_{j=1}^{n} gcd(i,j)^c lcm(i,j)^d x_j \equiv b_i \mod p$$

Thanks!