OI数学基础

Shinetism

YALI

July 21, 2019

OI数学基础

- 今天的主题是数学
- 信息学竞赛的数学主要是离散数学
- 主要包括数论和排列组合
- 在信息学竞赛中，两者互相融合，有时甚至难以区分
- 信息学竞赛中的数学和数学竞赛中不同
- 它更多地注重利用数学降低时间复杂度
- 所以它的变化也比单纯的数学题要复杂

目录

- 欧几里得算法
- 扩展欧几里得算法
- 素数
- 乘法逆元
- 排列组合
- 容斥

欧几里得算法

公约数！

欧几里得算法

- 欧几里得算法又叫辗转相除法，用于求解两个数的最大公约数。
- 利用了如下结论：
  - $\gcd(a,b)=\gcd(b, a \bmod b)$
- 证明如下：
  - 设$d|a$，$d|b$
  - $a \bmod b = a - \left\lfloor \frac{a}{b} \right\rfloor \times b$，因为 $d|a, d|b$， 所以 $d|(a \bmod b)$。
  - 原命题得证。
- 时间复杂度为 $O(\log b)$，证明相对复杂，证明不断取模的序列反转后不小于斐波那契数列，这里略去不讲。

欧几里得算法

- 然后我们讲讲最小公倍数。
- 有如下结论：
  - $lcm(a,b)=\frac{ab}{\gcd(a,b)}$
- 证明很简单：
  - 设 $a=a_0\times g, b=b_0\times g$, 其中 $\gcd(a_0,b_0)=1$
  - 那么 $lcm(a,b)=a_0\times b_0\times g=\frac{ab}{\gcd(a,b)}$
- 注意一点，有些题目会坑在 $a\times b$ 爆 int，所以我们先除再乘。

一个小思考

- 如何求两个 10^{10000} 以内的数字的最大公约数？
- 高精度取模？
- 不不不，那个太难写。
- 我们用更相减损术+高精度减法。

扩展欧几里得算法

解不定方程！

扩展欧几里得算法

- 我们先讲讲裴蜀定理：
  - $\forall x, y \in Z, \gcd(a, b) \mid (ax + by)$, 且 $\exists x, y \in Z, ax + by = \gcd(a, b)$.
- 这个定理很容易证明，而且证明也不是很重要，大家记住就可以。
- 而扩展欧几里得算法就是用来求解方程 $ax + by = \gcd(a, b)$ 的一组解

扩展欧几里得算法

- 我们现在需要求解 $ax + by = \gcd(a, b)$
- 我们先求解 $bx_0 + (a \bmod b)y_0 = \gcd(b, a \bmod b)$
- $\Rightarrow ay_0 - \left\lfloor \frac{a}{b} \right\rfloor by_0 + bx_0 = \gcd(b, a \bmod b)$
- $\Rightarrow ay_0 + b\left(x_0 - \left\lfloor \frac{a}{b} \right\rfloor y_0\right) = \gcd(a, b)$
- 所以我们有$\begin{cases} x = y_0 \\ y = x_0 - \left\lfloor \frac{a}{b} \right\rfloor y_0 \end{cases}$，递归求解。

T1「BZOJ1477」青蛙的约会

- Description:
  - 两只青蛙分别在一个长度为 l 的环上的 x, y 两个位置，两只青蛙向同一个方向跳跃，每次分别跳 m 和 n 个单位。现在它们同时开始跳跃，问至少几次跳跃后处于同一位置。
- Restraints:
  - $x \neq y < 2e9, 0 < m, n < 2e9, 0 < l < 2.1e9$

T1「BZOJ1477」青蛙的约会

- 题意即是求方程 $(x+ms)-(y+ns)=kl$ 的最小的解 s_0。
- 移项，得到 $(n-m)s+lk=x-y$。那么我们就是要探寻 $ax+by=n$ 的所有解中，x 最小的解。
- 如果 $\gcd(\mathrm{a},\mathrm{b}) \nmid \mathrm{n}$，那么无解
- 如果 $\gcd(a,b) \mid n$，设 $g=\gcd(a,b)$, $a=a_0\times g, b=b_0\times g, n=n_0\times g$
  - 先得到 $a_0x+b_0y=1$ 的一组解 x'', y''
  - 然后 $a_0x+b_0y=n_0$ 的所有解可以表示为 $\begin{cases} x'=n_0x''+b_0t \\ y'=n_0y''-a_0t \end{cases}$
  - 该解同时也是 $ax+by=n$ 的所有解，调整到最小正整数即可。

素数

素数

- 素数是个大工程，我们接下来要讲这么几个内容：
  - 素数筛法
  - Miller-Rabin 算法
  - Pollard-Rho 算法

素数筛法

- 我们实现一下线性筛法。

Miller-Rabin 算法

- Miller-Rabin 是一种快速判断素数的不确定性算法
- 首先有一个引理：
  - 若 p 为素数且 $x^2 \equiv 1(mod\, p)$，则 $x = 1$ 或者 $x = p - 1$。
- 想一想它的逆否命题：
  - 若 $x \neq 1$ 且 $x \neq p - 1$，则 $x^2 \not\equiv 1(mod\, p)$ 或 p 不为素数。
  - 即若 $x \neq 1$ 且 $x \neq p - 1$ 且 $x^2 \equiv 1(mod\, p)$，则 p 不为素数。
- 所以，我们可以用它来尝试排除合数。

Pollard-Rho 算法

- 我们现在需要对大数 n 进行质因数分解。
- 我们直接随机找到 n 的质因数的概率是很小的；
- 随机两个数 a,b ，使得 $|a-b|\mid n$的概率就要大些；
- 随机两个数 a,b ，使得 $\gcd(n,|a-b|)\neq 1$ 的概率更大。
- 至于为什么要随机两个数，是因为这样可以大大提高概率（生日悖论）
- 我们构造一个数列 $\{a_n\}$ 满足 $a_n=(a_{n-1}^2+c)\,mod\,n$ ，且 a_1 为随机值，c 为任意常数。
- 我们每次拿该数列中两个相邻的数求差再找是否存在公共质因数，然后递归分解。
- Time Complexity: $O(n^{\frac{1}{4}})$

一些说明

- 关于素数，NOIP中很少考到
- 与这些算法相关的题目一般都涉及到了积性函数（一大堆∑的典型省选题）
- 所以我没有找到NOIP范围内这方面的例题
- 下面讲一道有点超纲的题目

T2「BZOJ4802」欧拉函数

- Description:
  - 已知 n，求 $\varphi(n)$。（$\varphi(n)$ 表示小于 n 的与 n 互质的数的个数）
- Restraints:
  - $n \leq 1e18$

T2「BZOJ4802」欧拉函数

- 首先，$\varphi(n)$ 是一个积性函数，即：
  - $if\ \gcd(a,b)=1,\ \varphi(ab)=\varphi(a)\varphi(b)$
- 很容易证明。
- 所以我们将 n 进行质因数分解，然后只需要求 $\varphi(p^k)$。
- 可以得到 $\varphi\left(p^k\right)=p^k-p^{k-1}=p^{k-1}(p-1)$ 。
- 时间复杂度 $O(n^{\frac{1}{4}})$

乘法逆元

等效替代！

乘法逆元

- 乘法逆元体现了一种等效替代思想。
- 它实质上是一个数在模意义下的倒数。
- 记 a 的乘法逆元为 a^{-1}，它满足下面的条件：
  - $\frac{b}{a} \equiv b \times a^{-1} (mod\ M)$
- 我们只考虑 M 为质数的情况。

乘法逆元

- 如何求一个数的乘法逆元?
- 我们先来理解费马小定理：
  - 对于任意质数 p，任意正整数 $a < p$，有 $a^{p-1} \equiv 1(mod\ p)$.

- 所以我们可以令 $a^{-1} = a^{p-2}$.（注意：逆元是唯一的）
- 乘法逆元是一个简单应用，不会成为主要考点，但是几乎所有的计数题都会用到它。
- 所以等会再讲题目。

排列组合

计数！变换！

排列组合

- 基本的排列组合大家都学过了，这里再强调两种基本套路：
- 打桩法：
  - 譬如：九个停车位要停入三辆不同的汽车，要求两两不相邻，求方案数？
  - 先把六个空位作为“桩”固定（无区别，不计数），然后插入三个带车停车位。
  - 答案是 $\binom{7}{3} \times 3!$
- 这是一种信息竞赛生常常忘记的套路，往往看到就往容斥方面想（虽然也做得出来）

排列组合

- 基本的排列组合大家都学过了，这里再强调两种基本套路：
- 隔板法：
  - 譬如：将九张无区别的门票分给三个不同的人（可以有人没有票）。
  - 也就是九张门票插两个板（剪两刀），变为十一个元素中选出两个板。
  - 答案是$\binom{11}{2}$。
- 这个不是高考范围，但是竞赛中常用。

T3「BZOJ3907」网格

- Description:
  - 从坐标原点出发走到 (n,m) 点，每次只能向上或者向右走，且路线不经过直线 $y = x$ 左上方的点。求方案数（对998244353取模）。
- Restraints:
  - $n \leq 1e6, \mathrm{m} \leq 1e6$

T3「BZOJ3907」网格

- 这道题需要画图讲解
- 最后就是求 $\binom{n+m}{n} - \binom{n+m}{n+1}$。
- 预处理阶乘，以及阶乘逆元，直接计算。

容斥

理解力的高峰！

容斥

- 容斥是一个难点
- NOIP 不怎么考容斥，而要系统的学习容斥需要花很多的时间且难度很大
- 所以这里直接讲一个题目，大家细细体会，以后简单的容斥题就能做出来了。

T4「BZOJ2839」集合计数

- Description:
  - 一个有 n 个元素的集合有 2^n 个不同子集（包含空集），现在要在这 2^n 个集合中取出若干集合（至少一个），使得它们的交集的元素个数为 K，求取法的方案数，答案模1000000007。
- Restraints:
  - $n \leq 1e6, \mathrm{K} \leq n$

T4「BZOJ2839」集合计数

- 首先很容易想到一个错误的式子：

$$b_i=\binom{n}{i}\sum_{j=1}^{2^{n-i}}\binom{2^{n-i}}{j}=\binom{n}{i}(2^{2^{n-i}}-1)$$

- 我们先想想 $K=0$ 怎么做。

$$a_0=\sum_{i=0}^{n}(-1)^i\binom{n}{i}(2^{2^{n-i}}-1)$$

- 对于 $K\neq 0$，先把 $n -= K$，得到答案后乘上 $\binom{n}{K}$。

完结撒花~