算法基础——数学

邓丝雨

牛客竞赛
AC.NOWCODER.COM

算法竞赛中的数学

数论

数论是纯粹数学的分支之一，主要研究整数的性质。初等数论主要包括整除理论、同余理论、连分数理论。

组合数学

广义的组合数学就是离散数学，狭义的组合数学是离散数学除图论、代数结构、数理逻辑等的部分。合数学的主要内容有组合计数、组合设计、组合矩阵、组合优化（最佳组合）等。

线性代数

线性代数是数学的一个分支，它的研究对象是向量，向量空间（或称线性空间），线性变换和有限维的线性方程组。

概率与期望

概率论是研究随机现象数量规律的数学分支。事件的概率是衡量该事件发生的可能性的量度。数学期望是试验中每次可能结果的概率乘以其结果的总和，是最基本的数学特征之一。

博弈论

博弈论又被称为对策论（Game Theory），既是现代数学的一个新分支，也是运筹学的一个重要学科。博弈论考虑游戏中的个体的预测行为和实际行为，并研究它们的优化策略。

计算几何

计算几何是几何外形信息的计算机表示、分析和综合。

数论

牛客竞赛
AC.NOWCODER.COM

什么是质数?

- 质数（prime number）又称素数，一个大于1的自然数，除了1和它自身外，不能被其他自然数整除的数叫做质数；否则称为合数。
- 1既不是质数又不是合数。

质数的一些性质

- 1.在N>3时，在任何的N和N+1之中必然有一个数不是质数
- 2.质数有无穷多个
- 3.存在任意长的一段连续数，其中的所有数都是合数（相邻素数之间的间隔任意大）

质数的一些性质

- N以内的素数的个数随着N的增大趋近于log n
- 从不大于n的自然数随机选一个数，它是素数的概率大约是1/ln n （素数定理）
- 随着n的增大素数越来越稀疏。
- 在一个大于1的数*a*和它的2倍之间（即区间(a, 2a]中）必存在至少一个素数。

质数的一些猜想

- 孪生素数猜想：N和N+2都为素数的的情况有很多，这样的一对数素数叫做孪生素数（eg：3和5，5和7，11和13，1E9+7和1e9+9)
- 哥德巴赫猜想：任意大于2的正偶数都可以写成两个素数的和
- (一个充分大偶数必定可以写成一个素数加上一个最多由2个质因子所组成的合成数。简称为（1 + 2））

素数判定

- **枚举2到**$\sqrt[2]{n}$的所有的数，**看能否整除n**
- **时间复杂度O(**$\sqrt[2]{n}$**)**

素数筛法

- 埃氏筛法——由古希腊的数学家埃拉托塞尼提出
- “要得到不大于某个自然数N的所有素数，只要在2---N中将不大于$\sqrt[2]{N}$的素数的倍数全部划去即可”。

埃氏筛法

- 我们会发现，很多数会被重复筛，比如在筛掉6的时候，2和3分别标记了6一次。

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72

一个小优化：

- 对于每个合数我们都可以表示为a*b，其中a是一个质数，b可能是质数可能是合数
- 若a>b 那么a*b在用a筛掉其倍数之前就已经被b或者b的质因子筛掉了
- 所以，用a筛其倍数的时候，我们只需要从a*a开始枚举。
- 时间复杂度$O(\sum_{质数p\le N}\frac{N}{P}) = O(N \log \log N)$

线性筛

- 优化过的埃氏筛法还是会有重复的，如：12既会被2标记又会被3标记
- 我们希望一个合数只用一个素数来标记删掉
- 用最小的那个吧

- 我们用数组v记录每个数的最小质因子：
- 依次考虑2~N的每一个数I
- 如果V[i]=i那么i的质数，把它存下来，
- 扫描小于等于v[i]的所有质数，令v[i*p] = p,也就是在i上累积一个质因子。因为 p<=v[i]那么p是i*p的最小质因子，i*p是个合数。

```
for(int i <= 2; i <= n; i++)
{
    if(v[i] ==0 )  {v[i]= i; prime[++cnt]=i;}
    //如果没有筛过，记录素数
    for(int j = 1; j <= cnt; j++)
    {
        if(prime[j] > v[i] || i*prime[j] > n)  break;
        //i有比prime[j]小的因子，那>prime[j]的因子就没有意义了
        b[i*prime[j]] = prime[j];
        //筛去这个合数
    }
}
```

例1：

- 给你两个整数L,R求区间[L,R]中相邻的两个质数的差值最大是多少
- (L,R<=2^{31},R-L<=10^6)

- LR的范围导致素数表打不下……
- 但是R-L的范围不大
- 我们先把小于等于$\sqrt[2]{R}$的质数表打出来，然后用这些质数来筛L-R的质数。

算术基本定理

- 任何一个大于1的正整数都能唯一分解成为有限个质数的乘积，可以写作：
  - $\mathrm{N} = {p_1}^{c_1}{p_2}^{c_2}{p_3}^{c_3}{p_4}^{c_4} \dots {p_m}^{c_m}$
- 其中$p_1, p_2, p_3 \dots p_1$都是质数且递增， c_i都是正整数

分解质因数

- 试除法，把小于$\sqrt[2]{n}$的质数都试一遍

算术基本定理推论

- $\mathrm{N} = {p_1}^{c_1}{p_2}^{c_2}{p_3}^{c_3}{p_4}^{c_4} \ldots {p_m}^{c_m}$
- **那么N的正约数合集为**$\{{p_1}^{b_1}{p_2}^{b_2} \ldots {p_m}^{b_m}\}$**其中**$0 \le b_i \le c_i$
- **N的正约数个数为**$\prod_{\mathrm{i}=1}^{m}(c_i+1)$
- **N的所有正约数的和为**$(1 + p_1 + {p_1}^2 + \cdots + {p_1}^{c_1})$***...***$(1 + p_m + {p_m}^2 + \cdots + {p_m}^{c_m})$ **=** $\prod_{\mathrm{i}=1}^{m}(\sum_{j=0}^{ci}(p_m)^j)$

最大公约数和最小公倍数

- 最大公约数gcd(a,b)
- 欧几里得算法：(辗转相除法)
- gcd(a,b) = gcd(b,a mod b)
- gcd(a,b)记做(a,b)

- 最小公倍数
- gcd(a,b)*lcm(a,b) = a*b

求gcd的辗转相除法（又名欧几里得算法）

- LL gcd(LL a, LL b)
- {
-     return b ? gcd(b, a%b) : a;
- }

- （如果需要高精度——将除法改成减法）

欧拉函数

- **两个数gcd等于1，即两个数互质**
- **1到n中与n互质的数的个数称为欧拉函数记**$\emptyset(n)$
- 算术基本定理：$\mathrm{N}=p_1{}^{c_1}p_2{}^{c_2}p_3{}^{c_3}p_4{}^{c_4}\ldots p_m{}^{c_m}$
- $\emptyset(n)=N\times\frac{p^1-1}{p^1}\times\frac{p^2-1}{p^2}\times\cdots\times\frac{p^m-1}{p^m}$

欧拉函数

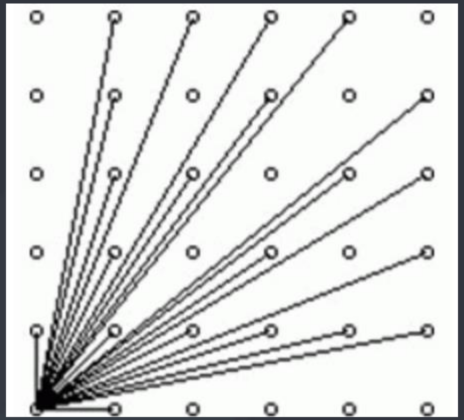
- $\emptyset(n) = N \times \prod_{质数\mathrm{p}|\mathrm{N}}(1 - \frac{1}{\mathrm{p}})$
- **证明：设p是N的质因子，1-N中p的倍数有p,2p,3p...共N/p个，若q也是N的质因子，1-N中q的倍数有N/q个，如果把他们都去掉，pq共同的倍数被算了两次要加回来，所以1-N中不与N有共同因子p或者q的数字个数为：**
- $N - N/p - N/q + N/pq = \mathrm{N}(1 - \frac{1}{p})(1 - \frac{1}{q})$

欧拉函数

- **性质：当a，b互质时**$\phi(a \times b) = \phi(a) \times \phi(b)$
- **——积性函数**

例1：[SDOI2008]仪仗队

- 仪仗队是由学生组成的N*N的方阵，为了保证队伍在行进中整齐划一，C君会跟在仪仗队的左后方，根据其视线所及的学生人数来判断队伍是否整齐(如下图)。希望你告诉他队伍整齐时能看到的学生人数。



同余的定义

- 若整数a和整数b除以正整数m的余数相等，则称为a,b模m余数相同，则称为a,b模m同余，记为$a \equiv b(mod\ m)$
- 同余满足反身性、对称性、传递性
- 即$a \equiv \mathrm{a}(mod\ m)$
- 若$a \equiv b(mod\ m)$则$b \equiv a(mod\ m)$
- 若$a \equiv b(mod\ m)$，$b \equiv c(mod\ m)$，则$a \equiv c(mod\ m)$

同余类与剩余系

- 对于$\forall a \in [0, m-1]$,集合$\{\mathrm{a} + \mathrm{km}\}(k \in Z)$的所有数模m同余，余数都是a，该集合是一个模m的同余类，记为$\overline{a}$
- 模m的同余类一共有m个，分别为$\overline{0}, \overline{1}, \overline{2}, \overline{3}, \dots \dots \overline{\mathrm{m}-1}$，它们构成m的完全剩余系

费马小定理

- **若p是质数，则对于任意不能被p整除的整数a，有**
- $a^{p-1} \equiv 1(mod\ p)$
- **若p是质数，则对于任意整数a，有**
- $a^{p} \equiv a(mod\ p)$

欧拉定理

- **如果正整数 n和整数a互质，那么就有**
- $a^{\emptyset(n)} \equiv 1(mod\ n)$
- **其中 $\emptyset(n)$是欧拉函数**

- **推论：**
- **如果正整数 n和整数a互质，那么就有**
- $a^{\mathrm{b}} \equiv a^{\mathrm{b\ mod}\ \emptyset(n)}(mod\ n)$
- **其中 $\emptyset(n)$是欧拉函数**

裴蜀定理

- 对任意两个不全为零的整数a，b，存在两个整数x，y，使得：
  - $ax+by = (a,b)$

怎么计算x和y?

- 刚刚的证明递归推回去即可
- 例题：
- $a = 288$, $b = 158$, 求一组x, y使得满足：
- $xa + yb = (a, b)$

扩展欧几里得算法

- Ps，求裴蜀定理中的x, y的方法又叫扩展欧几里得算法

```
typedef long long int64;
int64 gcd_ex(int64 a, int64 b,int64& x, int64& y)
{
    if (b == 0) { x = 1; y = 0; return a; }
    int64 d = gcd_ex(b, a % b, y, x);
    y = y - a / b * x;
    return d;
}
```

二元一次不定方程的通解

- 之前求出的x和y只是这个方程的一组解
- 如何求其通解?
- ax + by = c的通解为
- x = x0 – b1 * t
- y = y0 + a1 * t
- 其中，a = a1(a, b), b = b1(a, b)

什么情况下二元一次方程不定方程有解

- 二元一次不定方程$ax + by = c$有解的充要条件是
- $(a, b)|c$

牛客竞赛
AC.NOWCODER.COM

一元一次同余方程如何求解

- $ax=b \pmod m$ ($a \neq 0 \pmod m$)
- 如何判断这个方程是否有解？怎么求?
- 将这个等式化为二元一次方程不定方程即可
- $ax+km = b$
- 注意，这里的解，是一组解，不是单一的一个元，而是很多整数的一个集合。有时也把这个解叫做解空间。
- 但是我们算出来的还是一组解，那么其通解怎么表示？（大家自己先思考）

逆元

- 模运算没有除法。但是我们都知道，想要除以一个数，可以乘上它的逆。
- 所以模运算的除法，就是乘上逆。
- 不妨设a的逆元是x，那么有
- $ax \equiv 1 \pmod{m}$

中国剩余定理

- 南北朝时期《孙子算经》：有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二。问物几何?
- 宋朝数学家秦九韶于《数书九章》卷一、二《大衍类》做出了完整系统的解答。
- 明朝数学家程大位将解法编成易于上口的《孙子歌诀》：三人同行七十稀，五树梅花廿一支，七子团圆正半月，除百零五使得知。

中国剩余定理

- $\begin{cases} x \equiv 2(mod\ 3) \\ x \equiv 3(mod\ 5) \\ x \equiv 2(mod\ 7) \end{cases}$
- **找一个n1+n2+n3，使得：**
  - **n1除以3余2，且是5和7的公倍数。**
  - **n2除以5余3，且是3和7的公倍数。**
  - **n3除以7余2，且是3和5的公倍数。**

中国剩余定理

- $\begin{cases} x \equiv 2 (mod\ 3) \\ x \equiv 3 (mod\ 5) \\ x \equiv 2 (mod\ 7) \end{cases}$
- $2 \times 5 \times 7 \times 5^{-1} 7^{-1} (mod\ 3)$

牛客竞赛
AC.NOWCODER.COM

中国剩余定理

- $\begin{cases} x \equiv a_1 (mod\ m_1) \\ x \equiv a_2 (mod\ m_2) \\ \quad\quad \vdots \\ x \equiv a_n (mod\ m_n) \end{cases}$
- 令$M = m_1 m_2 m_3 \cdots m_n$，$M_i = \frac{M}{m_i}$，$M_i^{-1}$是$M_i$在模$m_i$下的逆元
- $\sum_{i=1}^{n} n_i = \sum_{i=1}^{n} a_i M_i M_i^{-1}$

组合数学

加法原理乘法原理

- 分类加法原理：做一件事情，完成它有n类方式，第一类方式有M1种方法，第二类方式有M2种方法，……，第n类方式有Mn种方法，那么完成这件事情共有M1+M2+……+Mn种方法。
- 分步乘法原理：做一件事，完成它需要分成n个步骤，做第一 步有m_1种不同的方法，做第二步有m_2种不同的方法，……，做第n步有m_n种不同的方法。那么完成这件事共有$N=m_1\times m_2\times m_3\times\ldots\times m_n$ 种不同的方法。

牛客竞赛
AC.NOWCODER.COM

排列组合

- **排列——从n个数的元素中取出m个数的元素进行排序（123和321不同）**
- $\mathrm{A}_{\mathrm{n}}^{\mathrm{m}}(P_{\mathrm{n}}^{\mathrm{m}}) = n \times (n-1) \times (n-2) \times \cdots \times (n-m+1) = \frac{n!}{(n-m)!}$
- **组合——从n元素中取出m个元素（123和321相同）**
- $C_{\mathrm{n}}^{\mathrm{m}} = \mathrm{A}_{\mathrm{n}}^{\mathrm{m}} / \mathrm{A}_{m}^{m} = \frac{n!}{m!(n-m)!}$

组合数的性质

- $C_{\mathrm{n}}^{\mathrm{m}} = C_{\mathrm{n}}^{\mathrm{n-m}}$
- $C_{\mathrm{n}}^{\mathrm{m}} = C_{\mathrm{n-1}}^{\mathrm{m}} + C_{\mathrm{n-1}}^{\mathrm{m-1}}$
- $C_{\mathrm{n}}^{0} + C_{\mathrm{n}}^{1} + \cdots + C_{\mathrm{n}}^{n} = 2^{n}$

二项式定理

- $(a+b)^n = \sum_{i=0}^{n} C_n^i \, a^{n-i} b^i$
- **杨辉三角：**
- 1
- 1 2 1
- 1 3 3 1
- 1 4 6 4 1

二项式定理

- 杨辉三角：
- 1
- 1 2 1
- 1 3 3 1
- 1 4 6 4 1

- 性质：
- 每个数等于上方两个数字的和
- $C_n^i = C_{n-1}^{i-1} + C_{n-1}^i$
- 第n行的数字和为2^{n}
- 第n行的第i个数和第n-i+1个数相等
- $C_n^i = C_n^{\mathrm{n}-i+1}$

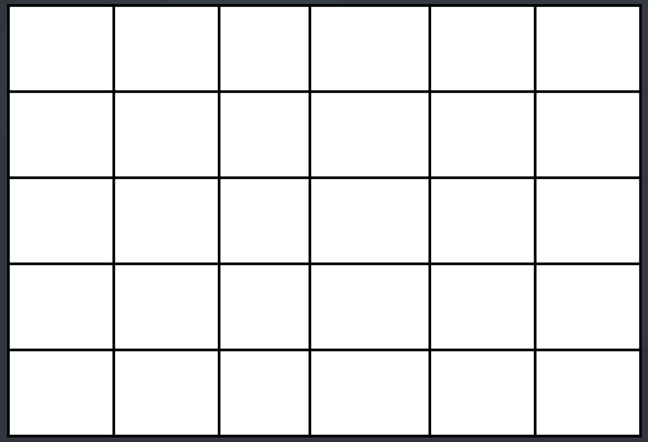
一些组合有关的问题

- 1.n*m的网格，从左上走到右下只能向下和向右走求方法数
- 2.从1,2,3...20中选3个不同的数组成的等差数列有多少种?
- 3.8个人排队

  甲乙两人一定要相邻

  甲乙两人一定不饿能相邻

  甲乙必须相邻且他俩与丙不能相邻



一些组合有关的问题

- 10个球放到八个盒子里每个盒子至少一个，有多少种方法?
- 20个相同的球放到三个不同的盒子里允许盒子为空，有多少种方法?

鸽巢原理

- N+1只鸽子飞回N个鸽巢至少有一个鸽巢有不少于两个鸽子

容斥原理

- 如果被计数的事物有A、B、C三类，那么，A类和B类和C类元素个数总和= A类元素个数+ B类元素个数+C类元素个数-既是A类又是B类的元素个数-既是A类又是C类的元素个数-既是B类又是C类的元素个数+既是A类又是B类而且是C类的元素个数。
- $A \cup B \cup C = A+B+C - A \cap B - B \cap C - C \cap A + A \cap B \cap C$

容斥原理

- 要计算几个集合并集的大小，我们要先将所有单个集合的大小计算出来，然后减去所有两个集合相交的部分，再加回所有三个集合相交的部分，再减去所有四个集合相交的部分………依此类推，一直计算到所有集合相交的部分。

例1:NC15079大水题

- 给出一个数n，求1到n中，有多少个数不是2 5 11 13的倍数。N<=10^18

例2：UVALive7243 青蛙

- 有m个石子围成一圈, 有n只青蛙从跳石子, 都从0号石子开始, 每只能越过xi个石子。问所有被至少踩过一次的石子的序号之和。
- N<=10^4, m<=10^5, xi <= 10^9

- 走的石头的编号就是步数跟石头数的最大共约数
- 直接容斥不行——n太大了
- 考虑枚举m中能到达的因子
- 对于每个因子的贡献做容斥
- 从小到大枚举因子
- 当计算了x的倍数和之后，将因子里是x的倍数的数计算次数减去刚刚x的计算次数

- V是m的因子表，cnt是表示的是当前这个因子需要计算的次数
- 初始：xi和m的gcd的倍数的cnt 值为1

```cpp
        for(int i = 0; i < v.size(); i++)
        {
            if(cnt[i])
            {
                ll num = m / v[i];
                ans += (0+(num-1) * v[i]) * num / 2 * cnt[i];
                for(int j = i + 1; j < v.size(); j++)
                    if(v[j] % v[i] == 0) cnt[j]-=cnt[i];
            }
        }
```

矩阵乘法及矩阵快速幂

牛客竞赛
AC.NOWCODER.COM

矩阵乘法

例：斐波拉契数列

- 求fib（n）% p的值
- n <= 10^18, p =10^9+7

$$\begin{pmatrix} F[1] \\ F[2] \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} F[2] \\ F[1] + F[2] \end{pmatrix} = \begin{pmatrix} F[2] \\ F[3] \end{pmatrix}$$

$$\begin{pmatrix} F[1] \\ F[2] \end{pmatrix} \times \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1} = \begin{pmatrix} F[\mathrm{n}] \\ F[\mathrm{n}+1] \end{pmatrix}$$

所以只需要求

$$\mathrm{res} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{n-1}$$

所求结果

$$F(n) = F[1] \times res[0][0] + F[2] \times res[0][1]$$

例:

- $F(n) = 5f(n-1) + 4f(n-2) + 1$
- $F(n) = 4f(n-1)+n +1$
- $F(n) = 3f(n-1) + 7f(n-2) +n^2 +3$

作业

- https://ac.nowcoder.com/acm/problem/collection/1261

- NC14399 素数判断
- NC14703 素数回文
- NC14731 逆序对
- NC201985 立方数
- NC16710 最大公约数(lcm)
- NC16563 同余方程
- NC18985 数字权重
- NC19872 [AHOI2005]SHUFFLE 洗牌
- NC20313 [SDOI2008]仪仗队
- NC23047 华华给月月出题
- NC23048 月月给华华出题
- NC16596 计算系数
- NC15077 造一造
- NC16525 转圈游戏

- NC15079 大水题
- NC16513 无关(relationship)
- NC20189 [JSOI2011]分特产
- NC200324 魔改森林
- UVALive7243 Frogs
- NC14607 递推
- NC15666 又见斐波那契
- NC200184 斐波那契
- NC17061 多彩的树
- NC17202 求幂
- NC18393 计数
- NC22599 Rinne Loves Sequence
- NC23616 小A的数学题