史 上 最 难 的 数 论 ppt
基 础 章 节

by kqp

1、 数学相关

1.1、容斥原理

- 普通容斥：形如$n-\frac{n}{p1}-\frac{n}{p2}-\frac{n}{p3}+\frac{n}{p1?p2}+\frac{n}{p1?p3}+\frac{n}{p2?p3}-\frac{n}{p1?p2?p3}\cdots\cdots$奇正偶负或者奇负偶正，?表示某种二元运算。
- 线性容斥：若每个p互质，则可以写成$n(1-\frac{1}{p1})(1-\frac{1}{p2})(1-\frac{1}{p3})\cdots\cdots$
- 正难则反：这也是容斥的重要体现

HAOI2008 硬币购物

【题目描述】

一共有4种硬币。面值分别为c1,c2,c3,c4。某人去商店买东西，去了tot次。每次带di枚ci硬币，买si的价值的东西。请问每次有多少种付款方法。

【数据范围】

di, si <= 10^5

tot <= 1000

HAOI2008 硬币购物

- $fo(k,1,4)\ f[i] += f[i-c[k]]$，感觉加些条件就能做？
- 这个dp式是不管硬币数量限制的，而硬币种类只有4，这是允许容斥的关键。
- 总的$f[s]$，减去第一个硬币超过的，减去第二个硬币超过的……加上前两个硬币超过的……减去前三个硬币超过的……
- 如何计算第一个硬币超过的方案数？（其他类推）
- $f[s-(d[1]+1)c[1]]$

JZOJ4695 佐助的难题

【题目描述】

求在1到n!范围内，与m!互质的数的数量。

【数据范围】

$m <= n <= 10^7$

$T<=10000$

JZOJ4695 佐助的难题

- ⇒求n!以内不含≤m的质因子的数的个数
- 由于m比较小我们可以把这些质数全部筛出来
- 不含某些质因子这种题，就是容斥的经典模型，但是这里质数数量很大，普通容斥是不行的，我们要用线性容斥。
- 假设m以内的质数是$p1$、$p2$、…、pk
- $ans = n!\left(1-\frac{1}{p1}\right)\left(1-\frac{1}{p2}\right)\dots\left(1-\frac{1}{pk}\right)$

1.2、分数运算

- 1.2.1裂项
- 1.2.2调和级数
- 1.2.3连分数
- 1.2.4

1.2.1、裂项

- $\frac{1}{1\times2}+\frac{1}{2\times3}+\frac{1}{3\times4}+\cdots+\frac{1}{(n-1)\times n}$
  $=1-\frac{1}{2}+\frac{1}{2}-\frac{1}{3}+\frac{1}{3}-\frac{1}{4}+\cdots-\frac{1}{n}=1-\frac{1}{n}$
- 类似地，
- $\frac{1}{1\times3}+\frac{1}{3\times5}+\cdots+\frac{1}{(2n-1)\times(2n+1)}=\frac{1}{2}(1-\frac{1}{2n+1})$
- $\frac{1}{n(n+1)(n+2)}=\frac{1}{2}\left(\frac{1}{n(n+1)}-\frac{1}{(n+1)(n+2)}\right)$
- 详情参考必修五第二章及其相关练习

JZOJ(junior)1867 裂项相消

【题目描述】

计算 $1+\frac{1}{1+2}+\frac{1}{1+2+3}+\frac{1}{1+2+3+4}+\cdots+\frac{1}{1+2+3+\cdots+n}$

输出最简分数的形式。

【数据范围】

n <= 10^7

JZOJ(junior)1867 裂项相消

- $\frac{1}{1+2+3+\cdots+n}=\frac{1}{\frac{n(n+1)}{2}}=\frac{2}{n(n+1)}$
- 原式$=2(\frac{1}{1\times2}+\frac{1}{2\times3}+\frac{1}{3\times4}+\cdots+\frac{1}{n(n+1)})$
- $=2(1-\frac{1}{n+1})$
- $=\frac{2n}{n+1}$
- 出题人也承认这是纯数学题，那就当给大家活跃下气氛吧。。

1.2.2、调和级数

- 全不为0的等差数列的倒数数列叫调和数列。
- 通常我们研究$1,\frac{1}{2},\frac{1}{3},\dots,\frac{1}{n}$
- 它的前缀和叫调和级数。这个数列是发散的，即调和级数是无穷大的。
- $1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}=\ln(n)+C$，其中$C$是欧拉常数，约等于0.57722
- 所以放在OI上，肯定是考别的东西，比如：

GDKOI2016 小学生数学题

【题目描述】

计算 $\sum_{i=1}^{n}\frac{1}{i} \bmod m$

其中$m = p^k$， p是个奇素数。

题目给出p、 k和n，保证答案的分母有逆元。

【数据范围】

p <= 10^5

n*p^k <= 10^18

1.2.3、连分数

- 欢迎张俊逸

1.3、高斯消元

- 1.3.1加减高斯消元
- 1.3.2异或高斯消元

1.3.1、加减高斯消元

- 用来求解线性方程组。

1.3.1、加减高斯消元

用高斯消去法解方程组：

$$\begin{cases} 2x+3y+11z+5w=2 \\ x+y+5z+2w=1 \\ 2x+y+3z+2w=-3 \\ x+y+3z+3w=-3 \end{cases}$$

把四个方程编好序号：

$$\begin{cases} 2x+3y+11z+5w=2 & (1) \\ x+y+5z+2w=1 & (2) \\ 2x+y+3z+2w=-3 & (3) \\ x+y+3z+3w=-3 & (4) \end{cases}$$

$$\begin{pmatrix} 2 & 3 & 11 & 5 & 2 \\ 1 & 1 & 5 & 2 & 1 \\ 2 & 1 & 3 & 2 & -3 \\ 1 & 1 & 3 & 4 & -3 \end{pmatrix} \xrightarrow{\frac{1}{2}\times(1)} \begin{pmatrix} 1 & \frac{3}{2} & \frac{11}{2} & \frac{5}{2} & 1 \\ 1 & 1 & 5 & 2 & 1 \\ 2 & 1 & 3 & 2 & -3 \\ 1 & 1 & 3 & 4 & -3 \end{pmatrix}$$

$$\xrightarrow[-1\times(1)+(4)]{\substack{-1\times(1)+(2) \\ -2\times(1)+(3)}} \begin{pmatrix} 1 & \frac{3}{2} & \frac{11}{2} & \frac{5}{2} & 1 \\ 0 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & -2 & -8 & -3 & -5 \\ 0 & -\frac{1}{2} & -\frac{5}{2} & \frac{3}{2} & -4 \end{pmatrix}$$

Baidu经验 jingyan.baidu.com

1.3.1、加减高斯消元

$$\xrightarrow{-2\times(2)}\begin{pmatrix}1 & \frac{3}{2} & \frac{11}{2} & \frac{5}{2} & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & -2 & -8 & -3 & -5\\ 0 & -\frac{1}{2} & -\frac{5}{2} & \frac{3}{2} & -4\end{pmatrix}$$

$$\xrightarrow[\frac{1}{2}\times(2)+(4)]{2\times(2)+(3)}\begin{pmatrix}1 & \frac{3}{2} & \frac{11}{2} & \frac{5}{2} & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & 0 & -6 & -1 & -5\\ 0 & 0 & -2 & 2 & -4\end{pmatrix}\xrightarrow{-\frac{1}{6}\times(3)}\begin{pmatrix}1 & \frac{3}{2} & \frac{11}{2} & \frac{5}{2} & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & 0 & 1 & \frac{1}{6} & \frac{5}{6}\\ 0 & 0 & -2 & 2 & -4\end{pmatrix}$$

$$\xrightarrow{2\times(3)+(4)}\begin{pmatrix}1 & \frac{3}{2} & \frac{11}{2} & \frac{5}{2} & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & 0 & 1 & \frac{1}{6} & \frac{5}{6}\\ 0 & 0 & 0 & \frac{7}{3} & -\frac{7}{3}\end{pmatrix}$$

$$\xrightarrow{\frac{3}{7}\times(4)}\begin{pmatrix}1 & \frac{3}{2} & \frac{11}{2} & \frac{5}{2} & 1\\ 0 & 1 & 1 & 1 & 0\\ 0 & 0 & 1 & \frac{1}{6} & \frac{5}{6}\\ 0 & 0 & 0 & 1 & -1\end{pmatrix}$$

1.3.1、加减高斯消元

（以下是回代过程）

$$\xrightarrow[-\frac{5}{2}\times(4)+(1)]{-\frac{1}{6}\times(4)+(3) \quad -1\times(4)+(2)} \begin{pmatrix} 1 & \frac{3}{2} & \frac{11}{2} & 0 & \frac{7}{2} \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\xrightarrow[-\frac{11}{2}\times(3)+(1)]{-1\times(3)+(2)} \begin{pmatrix} 1 & \frac{3}{2} & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\xrightarrow{-\frac{3}{2}\times(2)+(1)} \begin{pmatrix} 1 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

所以方程组的解为：

$$\begin{cases} x=-2 \\ y=0 \\ z=1 \\ w=-1 \end{cases}$$

这种高斯消去法也叫做有回代过程的高斯消去法

1.3.2、异或高斯消元

- 把加减改成异或，一样的。

未知来源题

【题目描述】

给你n个long long范围内的整数，你可以选取1个或多个数进行异或操作，使得结果最大。求最大的结果

【数据范围】

1 <= n <= 10^5

CF451E Devu and Flowers

【题目描述】

有n个花坛，要选s支花，每个花坛有f[i]支花，同一个花坛的花颜色相同，不同花坛的花颜色不同，问说可以有多少种组合。

【数据范围】

1 <= n <= 20

0 <= s <= 10^14

0 <= f[i] <= 10^12

2、欧几里得相关

2.1、gcd

- 2.1.1最大公约数
- 2.1.2实现方法
- 2.1.3正确性证明
- 2.1.4时间复杂度证明

2.1.1、最大公约数

- 去小学课本找定义

2.1.2、实现方法

- 更相减损术（必修3第一章）
- “可半者半之，不可半者，副置分母、子之数，以少减多，更像减损，求其等也。以等数约之。”
- 意思是：以2去约这两个数，约完之后以较大的数减较小的数，接着把所得的差与较小的数比较，并以大数减小数。继续这个操作，直到所得的减数和差相等为止。
- 则第一步中约掉的若干个2与第二步中等数的乘积就是所求的最大公约数。

2.1.2、实现方法

- 辗转相除法
- gcd=(b) ?gcd(b,a%b) :a
- 其实就是更相减损术的优化版
- 递归与非递归都要会啊

2.1.3、正确性证明

下面简要说明一下这个算法的正确性，对于任意两个数x和y，令$x = y \times a + b$，则对于任意$d \mid x$且$d \mid y$，有$x'd = y'd \times a + b$，$b = (x' - y' \times a) \times d$。所以$d \mid (x \bmod y)$，这说明了最后的结果$ans$一定是$x$和$y$的公约数。类似的对于任何$x$和$y$的公约数$d$，都有$d \mid ans$，这表明了$ans$为最大公约数。

2.1.4、时间证明

- 考虑这样的运算：a=a mod b
- 经过一次运算，a至少减少一半。
- 考虑gcd(a,b)=gcd(b,a%b)=gcd(a%b,···)，发现两次运算之后两个值都至少减少一半，所以你可以理解成log*2。

UR#3 核聚变反应强度

【题目描述】

共有n个原子，每个原子特征值为$a[i]$。

特征值为x的原子和特征值为y的原子反应，强度为$sgcd(x,y)$，表示x和y的次大公约数。

给出这n个原子的特征值，求$\text{sgcd}(a[1],a[1])$、$\text{sgcd}(a[1],a[2])$、 $\text{sgcd}(a[1],a[3])$、……、$\text{sgcd}(a[1],a[n])$

【数据范围】

n <= 10^5

a[i] <= 10^9

UR#3 核聚变反应强度

- 两个数的次大公约数实际上是最大公约数的最大约数。
- $O(n\sqrt{a})$：随便搞搞最大约数
- $O(\sqrt{a[1]} + n\log a)$：我们要找的最大约数也是$a[1]$的约数，于是我们把$a[1]$分解质因数之后，扫一扫就好了。

经典例题

【题目描述】

操场是由n个格子围成的圆形，从1到n编号。

有m个同学，每个同学步长a[i]，从1开始跑。求每个同学不会经过的格子数。

【数据范围】

m <= 10^5

n, a[i] <= 10^9

2.2、扩展gcd

- 2.2.1目标
- 2.2.2有解判断
- 2.2.3解法

2.2.1、目标

- 求解方程 $ax + by = c$

2.2.2、有解判断

- 设$d = \gcd(a, b)$
- 则方程可表示为 $a'dx + b'dy = c$
- 因此必须 $d|c$，满足这个条件则一定有解，否则一定无解。
- （在整数情况下）

2.2.3、解法

- 考虑$ax+by=\gcd(a,b)=d$ ……①
- $=>\ bx'+(a\%b)y'=d$ ……②
- 当递归到$a\%b=0$时，会有$b=d$，此时必有解 $x=1$，$y=0$
- 考虑回溯，即联立①②。
- $d=ax+by\ \ =bx'+\left(a-\left\lfloor\frac{a}{b}\right\rfloor\times b\right)y'$
- $\ \ =ay'+b(x'-\left\lfloor\frac{a}{b}\right\rfloor y')$
- $\therefore x=y'$，$y=x'-\left\lfloor\frac{a}{b}\right\rfloor y'$

2.2.3、解法

- 按照上述步骤我们可以得到方程的一组解，用时等于辗转相除法

- 由于$ax+by=d$，所以$\begin{cases} X=x+\frac{b}{d}k \\ Y=y-\frac{a}{d}k \end{cases}(k\in Z)$也是解，

  同样$\begin{cases} X=x-\frac{b}{d}k \\ Y=y+\frac{a}{d}k \end{cases}(k\in Z)$也是解。这就是通解。

- 回到原始方程$ax+by=c$，此时$c=d*c'$，则我们把所求得的解全部乘个c'就行了。

NOIP2012 同余方程

【题目描述】

求关于x的同余方程 $ax \equiv 1 \pmod{b}$ 的最小正整数解。

【数据范围】

对于40%的数据，$2 \le b \le 1000$

对于60%的数据，$2 \le b \le 5*10^7$

对于100%的数据，$2 \le a, b \le 2*10^9$

NOIP2012 同余方程

- $ax \equiv 1\ (mod\ b)$
- $=>\ ax - by = 1$
- 第一步：若a、b不互质则无解。（虽然原题保证有解）
- 第二步：扩展gcd解出一组解。
- 第三步：若$x < 0$，则给它加b加到大于0为止。

2.3、gcd的应用

- 2.3.1线性方程
- 2.3.2 多项式的最大公约式

2.3.1、线性方程

- 求解$a_1x_1+a_2x_2+\cdots+a_nx_n=b$
- $\because a_1x_1+a_2x_2=k\times\gcd(a_1,a_2)$
- $\therefore k\times\gcd(a_1,a_2)+a_3x_3+\cdots+a_nx_n=b$
- 于是把 k 看作新变量递归下去，就变成扩展gcd啦！

2.3.2、多项式的最大公约式

- 我们要先定义多项式带余除法
- 多项式除以多项式，商和余数都是多项式
- 形如下面的竖式运算：

2.3.2、多项式的最大公约式

$$
\begin{array}{r|l}
 & x^2 + x + 1 \\
\hline
x-1 & x^3 + \square + \square - 1 \\
 & \underline{x^3 - x^2} \\
 & x^2 + \square \\
 & \underline{x^2 - x} \\
 & x - 1 \\
 & \underline{x - 1} \\
 & 0
\end{array}
$$

$$
\begin{array}{r|l}
 & s \quad - 4 \\
\hline
s^2 + 5s + 6 & s^3 + s^2 + 7s + 9 \\
 & \underline{s^3 + 5s^2 + 6s} \\
 & -4s^2 + s + 9 \\
 & \underline{-4s^2 - 20s - 24} \\
 & 21s + 33
\end{array}
$$

2.3.2、多项式的最大公约式

$$
\begin{array}{r@{}l}
 & \frac{1}{3}x-\frac{7}{9}\cdots\cdots q(x) \\
g(x)\cdots\cdots 3x^2-2x+1 & \overline{\big)\,x^3-3x^2-x-1}\cdots\cdots f(x) \\
 & \underline{x^3-\frac{2}{3}x^2+\frac{1}{3}x} \\
 & -\frac{7}{3}x^2-\frac{4}{3}x-1 \\
 & \underline{-\frac{7}{3}x^2+\frac{14}{9}x-\frac{7}{9}} \\
 & -\frac{26}{9}x-\frac{2}{9}\cdots\cdots r(x)
\end{array}
$$

2.3.2、多项式的最大公约式

- 那么两个多项式就可以做模运算了
- 因此也就可以辗转相除法了。
- 所以就可以类似地求出最大公因式。

2.4、类欧几里得算法

- 2.4.1一般形式
- 2.4.2扩展

2.4.1、一般形式

- 设$f(a,b,c,n)=\sum_{i=0}^{n}\left\lfloor\frac{ai+b}{c}\right\rfloor$
- 给定a,b,c,n，求f。

2.4.1、一般形式

- $f(a,b,c,n)=\sum_{i=0}^{n}\left\lfloor\frac{ai+b}{c}\right\rfloor$
- 当$a \geq c$或$b \geq c$时：
- $f(a,b,c,n)=\sum_{i=0}^{n}\left(\left\lfloor\frac{(a\%c)i+(b\%c)}{c}\right\rfloor+\left\lfloor\frac{a}{c}\right\rfloor i+\left\lfloor\frac{b}{c}\right\rfloor\right)$
- $=f(a\%c,b\%c,c,n)+\left\lfloor\frac{a}{c}\right\rfloor\frac{n(n+1)}{2}+(n+1)\left\lfloor\frac{b}{c}\right\rfloor$

2.4.1、一般形式

- $f(a,b,c,n)=\sum_{i=0}^{n}\left\lfloor\frac{ai+b}{c}\right\rfloor$
- 当$a<c$且$b<c$时：
- 设$m=\left\lfloor\frac{an+b}{c}\right\rfloor$
- $f(a,b,c,n)=\sum_{i=0}^{n}\sum_{j=1}^{m}\left[j\le\left\lfloor\frac{ai+b}{c}\right\rfloor\right]$
- $=\sum_{i=0}^{n}\sum_{j=0}^{m-1}\left[j<\left\lfloor\frac{ai+b}{c}\right\rfloor\right]$
- $=\sum_{j=0}^{m-1}\sum_{i=0}^{n}\left[i>\frac{cj-b+c-1}{a}\right]$

2.4.1、一般形式

- $= \sum_{j=0}^{m-1}\left(n - \left\lfloor \frac{cj-b+c-1}{a} \right\rfloor\right)$
- $= mn - \sum_{j=0}^{m-1}\left\lfloor \frac{cj-b+c-1}{a} \right\rfloor$
- $= mn - f(c, c-b-1, a, m-1)$
- 观察第一、第三个系数，我们发现它们从(a, c)变成了$(c, a\%c)$，这就是该算法时间复杂度的关键，也因此它叫类欧几里得。
- 也可以从几何角度来理解这个算法。

2.4.2、扩展

- $f(a,b,c,n)=\sum_{i=0}^{n}\left\lfloor\frac{ai+b}{c}\right\rfloor$
- 设$g(a,b,c,n)=\sum_{i=0}^{n}i\left\lfloor\frac{ai+b}{c}\right\rfloor$
- 设$h(a,b,c,n)=\sum_{i=0}^{n}\left(\left\lfloor\frac{ai+b}{c}\right\rfloor\right)^2$

2.4.2、扩展

当$a \ge c$或$b \ge c$时：

- $g(a,b,c,n) = g(a\%c, b\%c, c, n) + \frac{n(n+1)(2n+1)}{6} \cdot \left\lfloor \frac{a}{c} \right\rfloor + \frac{n(n+1)}{2} \cdot \left\lfloor \frac{b}{c} \right\rfloor$
- $h(a,b,c,n) = h(a\%c, b\%c, c, n) + \frac{n(n+1)(2n+1)}{6} \cdot \left\lfloor \frac{a}{c} \right\rfloor^2 + (n+1)\left\lfloor \frac{b}{c} \right\rfloor^2 + 2\left\lfloor \frac{a}{c} \right\rfloor g(a\%c, b\%c, c, n) + 2\left\lfloor \frac{b}{c} \right\rfloor f(a\%c, b\%c, c, n) + n(n+1)\left\lfloor \frac{a}{c} \right\rfloor \left\lfloor \frac{b}{c} \right\rfloor$

2.4.2、扩展

当$a < c$且$b < c$时：

- $g(a,b,c,n) = \frac{(n+1)nm-h(c,c-b-1,a,m-1)-f(c,c-b-1,a,m-1)}{2}$
- $h(a,b,c,n) = nm(m+1) - 2g(c,c-b-1,a,m-1) - f(a,b,c,n) - 2f(c,c-b-1,a,m-1)$

2.4.2、扩展

- 注意我们总是从(a,b,c,n)到$(a\%c,b\%c,c,n)$到$(c,c-b+1,a,m-1)$，所以具体实现的时候，可以按照参数来分层递归。

bzoj2852 vijos1504 强大的区间

【题目描述】

给出两个实数 a、b，我们要求一个最小的正整数 k，使得区间［ak，bk］是一个包含至少一个整数的区间。

比如 a=1.2，b=1.3，当 k=4 时，区间为［4.8，5.2］，包含了整数 5。

【数据范围】

a、b 的整数部分不超过maxlongint，小数部分不超过300位。

bzoj2852 vijos1504 强大的区间

- 题解请访问我的博客
- http://blog.csdn.net/rzO_KQP_Orz/article/details/52497951

JZOJ3327 陶陶的难题

【题目描述】

陶陶给Crash出了一个大难题，他要求Crash计算出下面式子的值：

$$\sum_{x=L}^{R} x\left\lfloor\frac{Ax+C}{B}\right\rfloor$$

其中A,B,C,L,R均为给定正整数。由于答案可能会很大，你只需要输出答案mod 1,000,000,007后的值。

【数据范围】

A, B, C, L, R <= 10^9

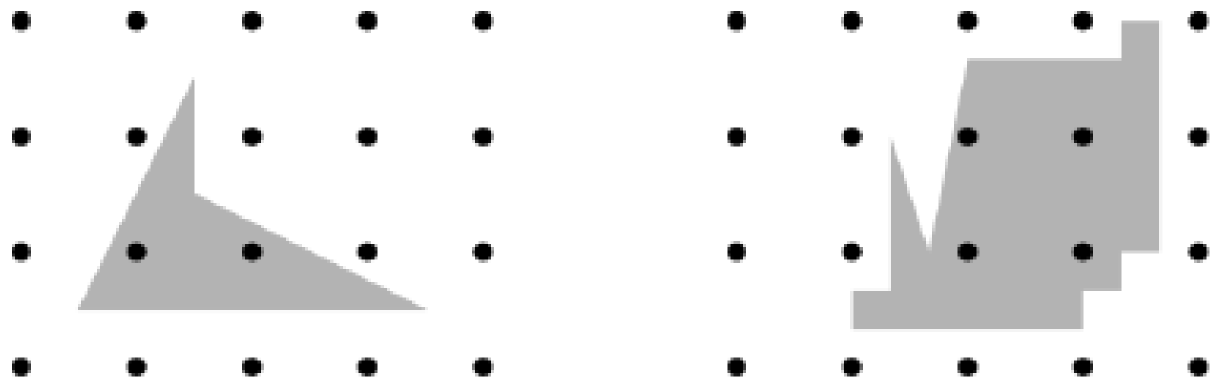
JZOJ3327 陶陶的难题

- 求$g(a,b,c,n)$的模板题，给大家练手。

经典例题

【题目描述】

在整数格点的平面上有一个简单多边形（顶点坐标均为有理数），问其内部有多少格点。（题目保证不会有格点出现在边界上）



【数据范围】

顶点数n<=100

坐标<=10^9

经典例题

- 梯形剖分：把每个出现了顶点的纵坐标描黑，可以把原图划分成若干个梯形（或退化的梯形）
- 先梯形剖分，任务变成求某条线段下方的整点数。
- 这就是$\sum\left\lfloor\frac{ax+b}{c}\right\rfloor$的形式了。

3、质数相关

3.1、质数的判定

- 3.1.1根号法
- 3.1.2Wilson定理
- 3.1.3Miller_Rabin

3.1.1、根号法

```
for i:=2 to sqrt(n) do
    if n mod i=0 then exit(false);
exit(true);
```

- 原理：若能分，必有小于sqrt(n)的约数
- 应用范围：单个质数的判定

3.1.2、Wilson定理

- 正整数$n>1$，则n是素数当且仅当$(n-1)!\equiv -1(mod\, n)$
- 证明：（写不下，自己百度）
- 应用范围：预处理了阶乘之后，或用后面会讲的快速求阶乘法。

3.1.3、Miller_Rabin

- 费马小定理：若p是质数，$p \nmid a$，则
$$a^{p-1} \equiv 1(mod\, p)$$
- 猜想Ⅰ：若$p \nmid a$，且$a^{p-1} \equiv 1(mod\, p)$，则$p$是质数
- 显然不一定成立，但是试多几个a，好像就挺准的？

3.1.3、Miller_Rabin

- 于是我们得出了伪Miller_Rabin算法：
- 对于$a = 2, 3, 5, 7, 11, 13, 17, 19, 23$，若都满足$a = p$或$a^{p-1} \equiv 1 (mod\, p)$，且$p \neq 1$，则$p$是质数。
- 实测证明，这种算法在10^18内卡不掉（论文里说会出错的事实上都对了）

3.1.3、Miller_Rabin

- 但是严谨的我们并不能满足于此，如何优化？
- 二次探测定理：若$a^2 \equiv 1(mod\, p)(a \neq 1, a \neq p-1)$时，$p$一定是合数。
- 我们可以在计算a^{p-1}的过程中顺便验证这条式子

3.1.3、Miller_Rabin

- 于是我们得出了专业Miller_Rabin算法：
- a取2，3，5，7，11，13，17，19，23
- 设$p-1=2^s d$，我们先计算a^d，然后给它平方s次。
- 若$a^d=1$，则该a无法验证（视为通过）；

  若平方过程中$=1$，则不通过；

  若平方过程中=-1，则该a无法验证（视为通过）；

  把最后a^{p-1}的判断也视作上面的过程，则程序最后return 不通过。

3.2、分解质因数

- 3.2.1根号法
- 3.2.2素数表
- 3.2.3n个数分解
- 3.2.4Pollard_ ρ

3.2.1、根号法

- 就不讲了好不好。。。

3.2.2、素数表

- 筛个表出来分解
- 就不讲了好不好。。。

3.1.3、n个数分解

- n个数的序列a[1..n]，每个数都分解，a[i]<=10^7
- 线筛预处理10^7以内每个数的最小质因子。当要分解某个a[i]的时候，一路除下去就好了。

3.1.4、Pollard_ρ

- 主要思想：对于我们要分解的N，快速地找到它的一个约数d，然后递归分解$\frac{N}{d}$和d。
- 我们用随机大法来快速找d。

3.1.4、Pollard_ρ

- 最坏情况：$N = pq$，其中p和q都是质数，我们假设要随机出p。
- 随机大法1：random(N)，则概率为$\frac{1}{N}$；
- 随机大法2：随机两个数x_1和x_2，则$p = x_2 - x_1$的概率约为$\frac{2}{N}$；
- 随机大法3：随机三个数，则任意两个的差为p的概率约为$\frac{6}{N}$；
- ……

3.1.4、Pollard_ ρ

- 随机大法n：根据birthday trick，当随机$\sqrt{N}$个数时，成功率约为一半。
- 随机大法n+1：随机k个数$x_1 \dots x_k$，查找是否有$\gcd(x_i - x_j, N) > 1$，这样概率又大了许多，这时候k只需要$n^{\frac{1}{4}}$（别问我为什么）

3.1.4、Pollard_ρ

- 但是我们随机生成k个数很浪费空间
- 使用伪随机函数$f(x) = x^2 + c$，每次生成两个数，并求出差值与N的gcd。
- 这个函数是会循环的，怎么办？
- 假设两个随机数是x和y，则x每次走一步，y每次走两步，若某一天重合，则y走了一圈。

3.1.4、Pollard_ρ

- 于是我们得出了快速找到N的一个约数的方法：
- 设随机函数$f(x)=x^2+c$，我们一开始随机出c、x_1和x_2，并判断$\gcd(|x_1-x_2|,N)$是否大于1，若是，则返回该gcd；否则$x_1=f(x_1)$，$x_2=f\big(f(x_2)\big)$。若此时$x_1=x_2$，则重新随机c、x_1和x_2。

POJ2429 GCD&LCM

【题目描述】

给出两个数gcd和lcm，找出两个数a和b，使它们的最大公约数为gcd，最小公倍数为lcm，如果存在多个，则输出a+b最小的那个。

【数据范围】

gcd,lcm<=2^63

hdu4344 Mark the Rope

【题目描述】

给一个数n，求由n的约数（不含1和n）组成的最大的集合，使得在这个集合中元素两两互素，求最大的元素个数，并求出在此基础上元素和的最大值。

【数据范围】

n<=2^63

NJUST1722 所有的平方差

给定一个数 n，有如下条件

$$n = a_1^2 - b_1^2 = a_2^2 - b_2^2 = \dots = a_m^2 - b_m^2$$

其中对任意的 $1 \le k_1, k_2 \le m$，都有 $a_{k_1} \ne a_{k_2}$，$b_{k_1} \ne b_{k_2}$ 和 $a_{k_1}, a_{k_2}, b_{k_1}, b_{k_2} \ge 0$，求表达式

$n^{a_1^2+b_1^2+a_2^2+b_2^2+\dots+a_m^2+b_m^2} \, mod \; 10000000019$ 的值。

【数据范围】

n<=2^63

6、 群论

6.2、置换群相关

- 6.2.1概念
- 6.2.2burnside引理
- 6.2.3polya定理

经典例题

【题目描述】

共有m种颜色的珠子，每种珠子有无数个。你要用这些珠子拼成大小为n的环。

若一个环经过旋转可以和另一个环相同，则它们本质相同。

求本质不同的环的个数 $mod\ (10^9+7)$。

【数据范围】

n <= 10^5

m <= 10^9

经典例题

【题目描述】

共有m种颜色的珠子，每种珠子有无数个。你要用这些珠子拼成大小为n的环。

若一个环经过旋转或翻转可以和另一个环相同，则它们本质相同。

求本质不同的环的个数 $mod\ (10^9+7)$。

【数据范围】

n <= 10^5

m <= 10^9

经典例题

【题目描述】

共有m种颜色的珠子，每种珠子有无数个。你要用这些珠子拼成大小为n的环。

要求相邻的两个珠子异色。

若一个环经过旋转可以和另一个环相同，则它们本质相同。

求本质不同的环的个数 $mod\ (10^9+7)$。

【数据范围】

n <= 10^5

m <= 10^9

经典例题

【题目描述】

共有m种颜色的珠子，每种珠子有无数个。你要用这些珠子拼成大小为n的环。

要求相邻的两个珠子异色。

若一个环经过旋转可以和另一个环相同，则它们本质相同。

求本质不同的环的个数 $mod\ (10^9+7)$。

T组询问。

【数据范围】

T <= 1000

n <= 1000

m <= 10^9

经典例题

【题目描述】

共有m种颜色的珠子，每种珠子有无数个。你要用这些珠子拼成大小为n的环。

要求每种颜色至少用一次。

若一个环经过旋转可以和另一个环相同，则它们本质相同。

求本质不同的环的个数 $mod\ (10^9+7)$。

【数据范围】

n <= 1000

m <= 1000

JZOJ4423 正十二面体

【题目描述】

正十二面体有12个面，20个点，30条边。

现在你有30个木棒，给出每个木棒的颜色。你要拼出一个正十二面体。两种拼法不同当且仅当它们不能通过空间旋转重合。

求本质不同的正十二面体的个数。

SGU 282 Isomorphism

【题目描述】

用m种颜色对一个n阶完全图染色（染边），若一张图的节点经过重排后变成另一张图则称两张图同构，问一共有多少种不同构的染色方案，结果模p。

【数据范围】

$n <= 53$

$m <= 1000$

7、模意义下的高级运算

7.0、模意义下的等式性质

- 以下不特指则在$\bmod m$意义下，整数意义下
- 传递性：若$a \equiv b$，$b \equiv c$，则$a \equiv c$
- 加减：若$a \equiv b$，则$a \pm c \equiv b \pm c$
- 乘幂：若$a \equiv b$，则$a^k c \equiv b^k c$，其中$k > 0$
- 除：若$ac \equiv bc (\bmod m)$，则$\mathrm{a} \equiv b(\bmod \frac{m}{(c,m)})$

即，若c,m互质，则可以直接约。

7.1、逆元

- 7.1.0啥是逆元
- 7.1.1费马小定理求逆元
- 7.1.2欧拉定理求逆元
- 7.1.3扩展gcd求逆元
- 7.1.4线性求逆元
- 7.1.5逆元总结

7.1.0、啥是逆元

- 对于一种可逆二元运算$a \oplus b$，设其逆运算为$\ominus$，那么使$a \oplus b = a \ominus c$的这个c，就是b的逆元，记作$b^{-1} = c$。
- 例如$3 \div 7 = 3 \times \frac{1}{7}$，那么$\frac{1}{7}$就是7的乘法逆元
- 我们知道模意义下不能直接做除法，所以我们要乘上除数的模意义乘法逆元。
- 例如$3 \div 7 (mod\ 11) \Rightarrow 3 \times 8 (mod\ 11)$

7.1.1、费马小定理求逆元

- 费马小定理：若p是质数，$p \nmid a$，则
$$a^{p-1} \equiv 1(mod\, p)$$
- 求逆元：若满足模数p是质数，$p \nmid a$，则a的逆元
$$x \equiv \frac{1}{a} \equiv a^{p-2}(mod\, p)$$
- 这是最简单、用得最多的方法，但条件比较苛刻。

7.1.2、欧拉定理求逆元

- 欧拉定理：若a与p互质，则

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

- 求逆元：若a与p互质，则a的逆元

$$x \equiv \frac{1}{a} \equiv a^{\varphi(p)-1}(mod\, p)$$

- 比费马小定理的条件放松了些

7.1.3、扩展gcd求逆元

- a的逆元x满足$ax \equiv 1(mod\, p)$
- $\Rightarrow ax - bp = 1$
- $\Rightarrow ax + bp = 1$
- 用扩展gcd解出x的最小正整数解就是逆元。
- 不用求φ好像更简单通用了呢^_^

7.1.4、线性求逆元

- 求1到$p-1$每个数的逆元$(mod\,p)$。
- 当$i=1$时，$i^{-1}=1$；
- 当$i>1$时，设$p=k\times i+r$，$r<i$
- $\Rightarrow k\times i+r\equiv 0(mod\,p)$
- 两边同时乘$i^{-1}\times r^{-1}$，得
$$k\times r^{-1}+i^{-1}\equiv 0(mod\,p)$$
- $\therefore i^{-1}\equiv -k\times r^{-1}\equiv -\left\lfloor\frac{p}{i}\right\rfloor\times(p\,mod\,i)^{-1}$
- 这就成了线性递推，负数的话加模数加到正。

7.1.5、逆元总结

- 一个数有逆元的充要条件是与模数互质。（扩展gcd法可证）
- 若有逆元，则逆元唯一。
- 选好求逆元的方法。对于单个数或对于多个数？模数是否是质数？
- 注意有时需要预处理逆元。

7.2、中国剩余定理

- 7.2.1基本形式
- 7.2.2m互质
- 7.2.3m不互质

7.2.1、基本形式

- 给出n条形如$x \equiv a_i(\bmod m_i)$的方程，求解这个x。
- 如果x带系数？
- $kx \equiv a_i(\bmod m_i)$，设$d = \gcd(k, m_i)$，则$\frac{k}{d}x \equiv \frac{a_i}{d}\left(\bmod \frac{m_i}{d}\right)$。
- 此时系数与模数互质，可以逆元除掉。若$d \nmid a_i$则方程无解

7.2.2、m互质

- $x \equiv a_i (\bmod m_i)$，若各方程的m互质：
- 考虑如果$x = \sum_{i=1}^{n} F(i)$，且保证
  $F(i) \bmod m_i = a_i$，$F(i) \bmod m_{j\,(j \neq i)} = 0$
  那么这就出解了。
- 那么显然，记$M = \prod m_i$，则

$$F(i) = \frac{M}{m_i} \times \left(\left(\frac{M}{m_i}\right)^{-1} \bmod m_i \right) \times a_i$$

7.2.3、m不互质

- $x \equiv a_i (\bmod m_i)$，若各方程的m不互质：
- 考虑合并方程。
- 对于 $x \equiv a_1 (\bmod m_1)$ 和 $x \equiv a_2 (\bmod m_2)$，则$x = a_1 + m_1 k_1 = a_2 + m_2 k_2$
- $\therefore m_1 k_1 = m_2 k_2 + (a_2 - a_1)$
- $\therefore m_1 k_1 \equiv a_2 - a_1 (\bmod m_2)$
- 有解判断：$\gcd(m_1, m_2) | (a_2 - a_1)$

7.2.3、m不互质

- 设$d = \gcd(m_1, m_2)$，$c = a_2 - a_1$
- 则$\frac{m_1}{d} k_1 \equiv \frac{c}{d} \left(mod \frac{m_2}{d} \right)$
- $\therefore k_1 = y \frac{m_2}{d} + \frac{c}{d} \left(\frac{m_1}{d} \right)^{-1}$
- 代入$x = a_1 + m_1 k_1$得：$x = a_1 + m_1 \left(y \frac{m_2}{d} + \frac{c}{d} \left(\frac{m_1}{d} \right)^{-1} \right)$
- $x = a_1 + m_1 \frac{c}{d} \left(\frac{m_1}{d} \right)^{-1} + y \frac{m_1 m_2}{d}$
- $\Rightarrow x \equiv a_1 + m_1 \frac{c}{d} \left(\frac{m_1}{d} \right)^{-1} \left(mod \frac{m_1 m_2}{d} \right)$，这就合并好了。

7.3、组合数取模

- 7.3.1Lucas定理
- 7.3.2中国剩余定理

7.3.0、目标

- 计算$C_n^m \bmod p$有什么方法？
- 当$n,m \le 1000$时，杨辉三角形预处理
- 当$n,m \le 10^6$时，预处理阶乘和逆元
- 当n,m很大很大时，就要高级算法了

7.3.1、Lucas定理

- 计算$C_n^m \bmod p$，其中p是质数，$p \le 10^5$
- $C_n^m \equiv C_{n\%p}^{m\%p} \times C_{\lfloor \frac{n}{p} \rfloor}^{\lfloor \frac{m}{p} \rfloor} \pmod p$

7.3.2、中国剩余定理

- 计算$C_n^m \bmod p$，现在p不是质数了。
- 设$p = p_1^{c_1} p_2^{c_2} \dots p_k^{c_k}$，考虑对每一个$p_i^{c_i}$都求出$x_i \equiv C_n^m (\bmod p_i^{c_i})$，最后用中国剩余定理合并。

7.3.2、中国剩余定理

- 现在要求$C_n^m \bmod p_i^{c_i}$
- $C_n^m = \frac{n!}{m!(n-m)!}$
- 考虑把上下所有的p_i因子提取出来，然后剩下的东西就有逆元了。
- 计算：$num(n)$表示$n!$的因子p_i的数量；$sum(n)$表示不含因子p_i的$n!$
- 这俩玩意儿分治搞定。

7.4、二次剩余

- 7.4.1形式1
- 7.4.2形式2
- 7.4.3形式3
- 7.4.4形式4

7.4.1、形式1

- $x^2 \equiv n (\bmod p)$，p是奇质数，求解x
- 这也是二次同余方程的基本形式

7.4.1、形式1

$x^2 \equiv n(\bmod p)$，p是奇质数

- 首先看两个东西：
- 1、n满足什么条件有解；
- 2、有解的话，有几个解。

7.4.1、形式1

$x^2 \equiv n(\bmod p)$， p是奇质数

- 定义有解的n叫做模p的二次剩余，无解的n叫做模p的二次非剩余（或非二次剩余）
- 欧拉判定法：n是模p的二次剩余，当且仅当$n^{\frac{p-1}{2}} \equiv 1(\bmod p)$
- 证明略

7.4.1、形式1

$x^2 \equiv n(\mathrm{mod}\, p)$， p是奇质数

- 若n是模p的二次剩余，则必有两解，即模意义下的$x = \pm x_0$

7.4.1、形式1

$x^2 \equiv n(\bmod p)$，p是奇质数

- 设$1 \le a < p$，若$\omega = a^2 - n$是二次非剩余，则其中一个解为$x = (a + \sqrt{\omega})^{\frac{p+1}{2}}$
- 证明：把这个x^2展开一下，就明白了。

7.4.2、形式2

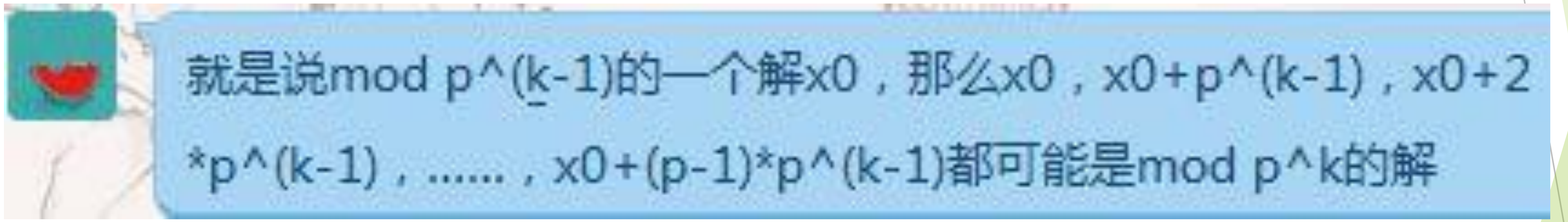
- $ax^2+bx\equiv c(\bmod p)$，p是奇质数，求解x
- 通过配方可得$(2ax+b)^2\equiv b^2-4ac(\bmod p)$
- 然后就那样解方程，解出$2ax+b$
- 然后就扩展gcd什么的搞出x
- 思考：a没逆元怎么办？

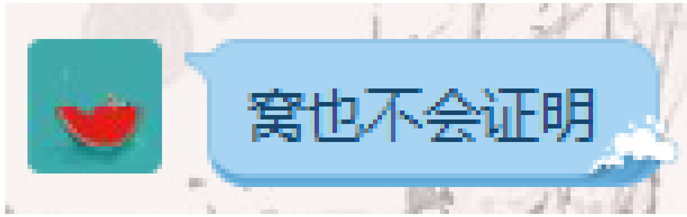
7.4.3、形式3

- $x^2 \equiv n(\mathrm{mod}\ p_1p_2\dots p_k)$，$p_i$是奇质数，求解$x$
- 对于每个p_i单独求解，最后中国剩余定理合并

7.4.4、形式4

- $x^2 \equiv n(\bmod p^m)$，p是奇质数，求解x





7.5、原根与离散对数

- 7.5.1BSGS
- 7.5.2指数与原根
- 7.5.3离散对数

7.5.1、BSGS

- 求解$a^x \equiv b(mod\, p)$， $p \leq 10^9 + 7$
- 提示：分三种情况考虑：p为质数、p非质数但与a互质、p任意。

7.5.1、BSGS

- p为质数：
- 考虑费马小定理，$x \le p-1$，因为大于就跟小于的循环了。
- 设$x = A\sqrt{p} + B$，则原式$\Rightarrow a^{A\sqrt{p}+B} \equiv b(mod\, p)$
- $\Rightarrow a^{A\sqrt{p}} \equiv b \times (a^{B})^{-1}\,(mod\, p)$
- 枚举A，再用hash判断最小的B是啥。
- 相当于要预处理右边那一坨东西，放进hash表里。
- 时间$O(\sqrt{p})$

7.5.1、BSGS

- 小优化：设$x = A\sqrt{p} - B$，这样就不用求逆元了。

7.5.1、BSGS

- p非质数但$(m,a)=1$：
- 考虑欧拉定理，$x\le\varphi(p)-1$，因为大于就跟小于的循环了。
- 所以仍可以设$x=A\sqrt{p}-B$，然后跟之前一样做。

7.5.1、BSGS

- p非质数：
- 考虑如何转换成前两种形式：
- 设$d=\gcd(a,p)$，原式$\Rightarrow \frac{a}{d}a^{x-1}\equiv\frac{b}{d}(mod\,\frac{p}{d})$
- 然后a的系数就有逆元了，除过去以后就跟之前一样了。
- 注意因为这样除一次以后左边底数仍为a，所以可能要除多次，但最多log次，因为模数每次至少除以2。
- 优化：若某时刻$b=1$，则已经出解了。

7.5.2、指数与原根

- 若$p>1$且$(a,p)=1$，则使$a^d\equiv 1(mod\ p)$成立的最小的正整数d，称为a对模p的指数（或叫a对模p的阶），记作$ord_p(a)$
- 若$ord_p(g)=\varphi(p)$，则称g为模p的一个原根

7.5.2、指数与原根

- 指数与原根常用性质：
- 若$\gcd(a,p)=1$且$a^d\equiv 1(mod\ p)$，则$d|\varphi(p)$
- 若g为模p的原根，则对于$x\in[1,p-1]$，g^x可以表示整个模p剩余系（除去0）。

7.5.2、指数与原根

- 原根存在性：一个数有原根当且仅当这个数形如：$1,2,4,p,2p,p^n$，其中p是奇质数。
- 求原根的方法：
- 1、枚举
- 2、枚举并科学地验证
- (设$p-1=p_1^{c_1}*p_2^{c_2}*p_3^{c_3}\ldots$，我们枚举的是$a$，那么只要判断$a^{\frac{p-1}{p_1}}$、$a^{\frac{p-1}{p_2}}$、$a^{\frac{p-1}{p_3}}\ldots$是否都不为1即可)

7.5.3、离散对数

- 设g是模p的一个原根，对于任一整数a，$(a,p)=1$，都有$a \equiv g^y$，$0 \leq y \leq \varphi(p)$，我们把y称为以g为底的a对模p的离散对数，记为$ind_g a$

7.5.3、离散对数

- 求解$x^A \equiv B(\bmod p)$，其中p是奇素数
- 设g为p的原根
- $B = g^b$，$x = g^y$
- 则原式$\Rightarrow g^{Ay} \equiv g^b$
- $\Rightarrow Ay \equiv b(\bmod p-1)$
- 就可以随便解了。

完