ACM 中的数学问题

北京大学ACM 竞赛队队员

林舒

引言

. 在ACM 竞赛中, 经常可以看到数学问题的身影

. 可以是纯数学问题, 也可以是需要利用数学上

的一些公式, 定理, 算法来辅助解决的问题

. 会者不难, 而不会的人在赛场上一般很难推出

公式或进行证明

. 往往想起来费劲, 写起来却很轻松

常见的数学问题

. 数论

. 组合数学

. 博弈论

. 线性代数

. 高等数学

. 线性规划

. 概率论

....

本讲内容

. 简单数论

.Polya 定理

.SG 函数

. 与矩阵有关的问题

本讲内容

. 基本上是最基础的, 同时也是ACM 竞赛中

最常用的数学算法

. 一些数学定理, 公式的简略证明或推导, 从

而加深对它们的理解和认识, 也方便记忆

. 往届ACM 竞赛中的数学问题

数论

. 简而言之, 数论是研究整数的理论

. 在ACM 竞赛中, 经常用到数论的相关知识

. 纯数论的题目不多, 大部分是和其他类型

的问题结合起来的

. 约数, 倍数, 模线性方程, 欧拉定理, 素数

整除的性质

. 性质1:a|b,b|c => a|c

. 性质2:a|b => a|bc

. 性质3:a|b,a|c => a|kb±lc

. 性质4:a|b,b|a <=> a=±b

. 性质5:a=kb±c <=> a,b的公因数与b,c 的

公因数完全相同(利用性质3)

最大公约数

最小公倍数

. 欧几里德算法(辗转相除法, 短除法)

. 原理:若a ≡r(mod b),则gcd(a,b)=gcd(b,r)(利

用性质5证明)

. 算法步骤(递归实现):

. 整数a,b, 假设|a|>|b|

. 若b=0,则gcd(a,b)=|a|;否则gcd(a,b)=gcd(b,a%b)

. 最小公倍数:lcm(a,b)=a\*b/gcd(a,b)

解二元模线性方程

. 二元模线性方程(二元一次不定方程):形

如ax ≡c(mod b)或ax+by=c

. 扩展欧几里德算法

. 原理:

. 令d=gcd(a,b),原方程有整数解当且仅当d|c

.bx+(a%b)y=1 <=> ay+b(x-[a/b]\*y)=1

解二元模线性方程

. 算法步骤:

. 整数a,b,c, 设d=gcd(a,b)

. 在用欧几里德算法求gcd(a,b)的过程中求方程

ax+by=d的一组整数解:

. 若b=0,则x=1,y=0;

. 否则, 递归调用gcd(b,a%b),可以得到bx'+(a%b)y'=d的解

x',y', 令x=y',y=x-[a/b]y'即满足ax+by=d

. 若d|c,设c=kd,则有a(kx)+b(ky)=c;否则原方程无整

数解

中国剩余定理

. 孙子定理, 韩信点兵, 隔墙算, 鬼谷算, 大衍求一

术...

." 物不知数" 问题:"今有物不知其数, 三三数之剩

二, 五五数之剩三, 七七数之剩二, 问物几何? 答

曰:'二十三.' 术曰:三三数之剩二, 置一百四十,

五五数之剩三, 置六十三, 七七数之剩二, 置三十,

并之, 得二百三十三, 以二百一十减之, 即得. 凡三

三数之剩一, 则置七十, 五五数之剩一, 则置二十

一, 七七数之剩一, 则置十五, 即得." --孙子算经

中国剩余定理

. 一般性问题:给定两两互质的正整数n1,n2,...,nk,

要求找到最小的正整数a, 满足a ≡ai(mod ni)

. 算法步骤:

. 令n=n1n2...nk,mi=n/ni

. 显然gcd(mi,ni)=1,利用扩展欧几里德算法计算出xi

满足mixi ≡1(mod ni)

.a ≡a1x1m1+a2x2m2+...+akxkmk(mod n)

筛法

. 目标:求出n 以内的所有质数

. 算法步骤:

. 初始时容器内为2到n 的所有数

. 取出最小的数p,p 一定是质数, 删去p 的所有倍数(注:

只需从p2开始删除即可)

. 重复上述步骤直到容器为空

. 用bool 数组实现即可

. 缺陷:一个数可能被重复删去多次, 影响效率

筛法

. 改进:

. 初始时容器内为2到n 的所有数

. 取出最小的数p,p 一定是质数

. 删去所有的pi, 令q 为第一个未被删除的数, 保留q, 删

去所有的piq, 再令q 为下一个未被删除的数, 删去所

有的piq... 直到q 遍历所有未被删除的数为止(这一步

骤可以把最小质因数为p 的所有数删去)

. 重复上面两个步骤直到容器为空

. 用bool 数组+双向链表实现

. 小优化:初始时只加入奇数

算术基本定理

. 任何一个大于1的自然数n, 都可以唯一分

解成有限个质数的乘积

.n=p1r1p2r2...pkrk

.p1<p2<...<pk均为质数,r1,r2,...rk 均为正整

数

欧拉函数

. 记φ(x)为与x 互质且小于x 的正整数个数

. 设x=p1r1p2r2...pkrk

. φ(x)=x\*(1-1/p1)\*(1-1/p2)\*...\*(1-1/pk)或

φ(x)=p1(r1-1)(p1-1)p2(r2-1)(p2-1)...pk(rk-1)(pk-1)

. 递推式:质数p 满足p|x,若p2|x,则

φ(x)=φ(x/p)\*p,否则φ(x)=φ(x/p)\*(p-1)

欧拉函数

. 证明:

. 若p 为质数, 则φ(p)=p-1

. φ(pr)=pr(1-1/p)=p(r-1)(p-1)

. 若a,b 互质, 则φ(ab)=φ(a)φ(b)

. 扩展:n的所有因子之和

(p10+...+p1r1)(p20+...+p2r2)...(pk0+...+pkrk)

欧拉定理

. 若a 和m 互质, 则a φ(m)≡1(mod m)

. 证明:

. 设φ(m)个正整数r1,r2,...,r φ(m)满足:ri与m 互质, 对于

任意i ≠j,ri ≠rj(mod m)

. 利用反证法可以简单证明ar1,ar2,...,ar φ(m)依然满足

上述条件

.(ar1)(ar2)...(arφ(m) )≡a φ(m)r1r2...rφ(m)(mod m)

. 两边同时约去r1r2...r φ(m)即得到欧拉定理

素数测试

. 费马小定理:若p 为素数, 则对于任意小于

p 的正整数a, 有a(p-1)≡1(mod p)

. 证明:用欧拉定理直接得出

. 二次探测定理:若p 为素数,a2≡1(mod p)

小于p 的正整数解只有1和p-1

. 满足费马小定理和二次探测定理的数可

以确定是素数

素数测试

.Miller-Rabin 算法

. 算法步骤:

. 判定n 是否为素数

. 令n-1=m\*2j,m为奇数

. 随机在2到(n-1)之间取一个整数b

. 令v=bm,之后每次对v 平方, 当v=1时, 若上一次的v 既

不是1也不是(n-1),由二次探测定理,n 不是素数, 退出;

不断循环直到计算出b(n-1)

.v=1,满足费马小定理, 通过测试; 否则n 一定不是素数

. 选取几个不同的b 多次测试

素数测试

.Miller-Rabin 只能算一种测试, 因为通过

测试的数不一定是素数, 非素数通过测试

的概率是1/4

. 虽然一次测试的结果不一定令人满意, 但

五六次随机测试基本可以保证正确率超

过99.9%

大整数分解

. 至今仍是世界难题

. 在密码学中起着至关重要的作用

. 试除法,Fermat 方法,Pollard 方法

.Pollard rho方法

Pollard rho方法

. 原理:用某种方法生成两个整数a 和b, 计算p=gcd(a-b,n),

直到p 不为1或a,b 出现循环为止, 若p=n,则n 为质数, 否则

p 为n 的一个约数

. 算法步骤:

. 选取一个小的随机数x1

. 迭代生成xi=x(i-1)

2+k,一般取k=1,若序列出现循环则退出

. 计算p=gcd(x(i-1)-xi,n),若p=1,返回上一步; 直到p>1为止

. 若p=n,则n 为素数, 否则p 为n 的一个约数并递归分解p 和n/p

数论小结

. 前面的这些都是一些初等数论的知识

. 可以看出, 数论所研究的内容, 很大一部分

都是和素数紧密联系的. 因此, 数论是名副

其实的" 素论"

. 这些算法代码量都不大, 但如果没有准备

好模版的话, 往往会忽略一些细节

Polya 定理

. 组合数学理论中最重要的定理之一

. 在组合计数问题中有重要作用

. 涉及的概念和定理比较多, 证明较复杂, 本

讲只是粗略地介绍

一个经典的例子

. 用两种颜色去染排成一个圈的6个棋子,

如果能够通过旋转得到只算作一种, 问有

多少种染色状态

. 下面将通过这个例子来形象地介绍Polya

定理的内容和解决这类问题的方法

. 置换:用矩阵形式表示的顶点的变换

. 例子中, 将棋子从某个点顺时针标上1到6,

则将所有棋子顺时针旋转一个位置的置

换可表示为:

1 2 3 4 5 66 1 2 3 4 5

置换

置换群

. 以置换为元素的群

. 置换群G={a1,a2,...,a|G|}

. 例子中G 内共有6个置换

123456 123456 123456123456 612345 561234123456 123456 123456456123 345612 234561

循环

. 在一个置换下,x1->x2,x2->x3,...,xn->x1,这

样x1,x2,...,xn 就构成了一个循环

. 定义ck 为在置换ak 下的循环总数

. 例子中:

c1=6,c2=1,c3=2,c4=3,c5=2,c6=1

Polya 定理

. 设G={a1,a2,...,a|G|}是N={1,2,...,N}上的置

换群, 现用m 种颜色对这N 个点染色, 则不

同的染色方案数为

S=(mc1+mc2+...+mc|G|)/|G|

. 证明比较复杂, 略

利用Polya 定理

解决组合计数问题的步骤

. 写出置换群

123456 123456 123456123456 612345 561234123456 123456 123456456123 345612 234561 . 求出每个置换的循环数

c1=6,c2=1,c3=2,c4=3,c5=2,c6=1

. 计算染色方案

S=(26+21+22+23+22+21)/6=14

常见置换的循环数

. 计算置换的循环数, 是这一算法的瓶颈. 如果能 够快速计算出各置换的循环数, 就可以大大提 高程序的运行效率

. 旋转:n个点顺时针(或逆时针) 旋转i 个位置的置 换, 循环数为gcd(n,i)

. 翻转:

.n 为偶数时,

. 对称轴不过顶点:循环数为n/2

. 对称轴过顶点:循环数为n/2+1

.n 为奇数时, 循环数为(n+1)/2

Polya 定理小结

. 前面所讲的内容, 仅适用于置换数目较少, 着色 没有其他限制的情况, 是最简单的一类Polya 定 理的问题

. 复杂的Polya 定理的问题还需要用到数论知识 来加快速度, 用排列组合或动态规划来辅助计 数

. 不过, 对于ACM 竞赛来说, 掌握简单的Polya 定理 就能够解决很多问题了

从博弈说起

. 一门古老的游戏; 棋牌, 彩票...

. 博弈论是二人或多人在平等的对局中各 自利用对方的策略变换自己的对抗策略， 达到取胜目标的理论

. 合作博弈/非合作博弈

. 静态博弈/动态博弈

. 完全信息博弈/非完全信息博弈

公平组合博弈

. 二人博弈

. 非合作博弈:博弈双方利益完全对立

. 动态博弈:两人轮流行动, 后手知道先手的 动作

. 完全信息博弈:双方都了解当前格局 . 非偶然性:无随机事件

公平组合博弈

. 游戏局面的状态数有限

. 对于同一局面, 两个游戏者可操作的集合 完全相同

. 无法进行任何操作时游戏结束, 不能操作 的一方为负

. 游戏总可以在有限步之内结束

. 假定:两个人都" 足够聪明"

先手必胜/后手必胜

. 由于公平组合博弈必在有限步结束, 且不 会有随机事件, 因此, 在双方都采用最佳策 略的前提下, 任一局面不是先手必胜就是 后手必胜

. 规定:先手胜为N(Next)局面, 后手胜为 P(Pre)局面

先手必胜/后手必胜

. 最终局面都是P 局面

. 对于一个局面, 若至少有一种操作使它变 为P 局面, 则它是N 局面

. 对于一个局面, 无论如何操作都使它变为 N 局面, 则它是P 局面

抽象模型

. 所有的公平组合博弈都可以抽象成下列 模型:

. 有向无环图, 某个点上有一枚棋子, 双方轮流 将棋子沿某条有向边移动, 无法移动者为负 . 其中, 一个点表示一个局面, 而一条有向边则 表示一种可行操作

公平组合博弈问题解法

. 往往可以从终局面出发, 逆向递推, 求出任 意局面是P 局面还是N 局面

. 但如果游戏是一系列子游戏的组合时, 局 面的数量非常庞大, 上述方法就会变得十 分低效

. 下面将引入SG 函数来解决这一类问题

本文档下载自360文档中心，www.360docs.net更多营销,职业规划,工作简历,入党,工作报告,总结,学习资料,学习总结,PPT模板下载,范文等文档下载；转载请保留出处:http://www.360docs.net/doc/info-df037f28cfc789eb172dc803.html