裴蜀定理和扩展欧几里得算法

前置知识
讲解041 - 辗转相除法求最大公约数，代码中Code01_GcdAndLcm文件里有正确性的证明
讲解041 - 同余原理，加减乘的同余
讲解099 - 逆元和除法同余，逆元的意义，费马小定理求逆元的过程

本节课讲述
裴蜀定理及其证明，扩展欧几里得算法详解，常见题目解析

下节课讲述
扩展欧几里得算法和二元一次不定方程结合的内容，常见题目解析

左程云

裴蜀定理和扩展欧几里得算法

裴蜀定理
如果a和b是不全为0的整数，则有整数x、y，使得ax + by = gcd(a,b)
课上重点图解证明过程，证明很重要，可以帮助理解扩展欧几里得算法的过程

重要理解
a和b的最大公约数 = ax + by，随意给定整数x、y，能得到的最小正整数
a和b的最大公约数 = ax和by，随意给定整数x、y，能得到的最小正数差值

裴蜀定理推论
1，如果a和b是不全为0的整数，a和b互质，当且仅当存在整数x、y，使ax + by = 1
2，如果a和b是不全为0的整数，并且ax + by = c有解，那么c一定是gcd(a,b)的整数倍
3，a和b两项的裴蜀定理，可以推广到多项的情况

如果ax + by = c一旦有解，就意味着一定有无穷多组(x,y)，都可以使得式子成立

左程云

裴蜀定理和扩展欧几里得算法

扩展欧几里得算法
对于方程$ax + by = gcd(a,b)$，当a和b确定，那么$gcd(a,b)$也确定，要保证入参a和b没有负数
扩展欧几里得算法可以给出a和b的最大公约数d、以及其中一个特解x、y
课上重点图解，理解了裴蜀定理证明，也就理解了扩展欧几里得算法过程的正确性

时间复杂度
扩展欧几里得算法理论的时间复杂度$O(log\ min\{a,b\})$，但要注意%运算的代价比较高
所以实际的时间复杂度$O((log\ min\{a,b\})$的三次方)，证明略，知道极快即可

求逆元
费马小定理求逆元时，要求模的数字必须为质数
扩展欧几里得算法求逆元时，不要求模的数字必须为质数，但要求a和b互质

扩展欧几里得的更多内容会在下节课讲述，讲解140 - 扩展欧几里得和二元一次不定方程

左程云

裴蜀定理和扩展欧几里得算法

题目1
裴蜀定理模版题
给定长度为n的一组整数值[a1, a2, a3...]，你找到一组整数值[x1, x2, x3...]
要让a1*x1 + a2*x2 + a3*x3...得到的结果为最小正整数
返回能得到的最小正整数是多少
1 <= n <= 20
1 <= ai <= 10^5
测试链接：https://www.luogu.com.cn/problem/P4549

左程云

裴蜀定理和扩展欧几里得算法

题目2
修理宝塔
一共有编号1~n的宝塔，其中a号和b号宝塔已经修好了
Yuwgna和laka两个人轮流修塔，Yuwgna先手，laka后手，谁先修完所有的塔谁赢
每次可以选择j+k号或者j-k号塔进行修理，其中j和k是任意两个已经修好的塔
也就是输入n、a、b，如果先手赢打印"Yuwgna"，后手赢打印"laka"
2 <= n <= 2 * 10^4
测试链接：https://acm.hdu.edu.cn/showproblem.php?pid=5512
测试链接：https://vjudge.net/problem/HDU-5512

左程云

裴蜀定理和扩展欧几里得算法

题目3
均匀生成器
如果有两个数字step和mod，那么可以由以下方式生成很多数字
seed(1) = 0，seed(i+1) = (seed(i) + step) % mod
比如，step = 3、mod = 5
seed(1) = 0，seed(2) = 3，seed(3) = 1，seed(4) = 4，seed(5) = 2
如果能产生0 ~ mod-1所有数字，step和mod的组合叫 "Good Choice"
如果无法产生0 ~ mod-1所有数字，step和mod的组合叫 "Bad Choice"
根据step和mod，打印结果
1 <= step、mod <= 10^5
测试链接：http://poj.org/problem?id=1597

裴蜀定理和扩展欧几里得算法

题目4
同余方程
求关于x的同余方程 $ax \equiv 1 \pmod b$ 的最小正整数解
题目保证一定有解，也就是a和b互质
2 <= a、b <= 2 * 10^9
测试链接：https://www.luogu.com.cn/problem/P1082

左程云

裴蜀定理和扩展欧几里得算法

题目5
洗牌
一共有n张牌，n一定是偶数，每张牌的牌面从1到n，洗牌规则如下
比如n = 6，牌面最初排列为1 2 3 4 5 6
先分成左堆1 2 3，右堆4 5 6，然后按照右堆第i张在前，左堆第i张在后的方式依次放置
所以洗一次后，得到 4 1 5 2 6 3
如果再洗一次，得到 2 4 6 1 3 5
如果再洗一次，得到 1 2 3 4 5 6
想知道n张牌洗m次的之后，第l张牌，是什么牌面
1 <= n <= 10^10，n为偶数
0 <= m <= 10^10
测试链接：https://www.luogu.com.cn/problem/P2054

左程云