

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

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

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 $O((\log \min\{a, b\})^3)$, 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

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 $[a_1, a_2, a_3 \dots]$ ，你找到一组整数值 $[x_1, x_2, x_3 \dots]$

要让 $a_1 * x_1 + a_2 * x_2 + a_3 * x_3 \dots$ 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

$1 \leq n \leq 20$

$1 \leq a_i \leq 10^5$

测试链接：<https://www.luogu.com.cn/problem/P4549>

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Iaka两个人轮流修塔，Yuwgna先手，Iaka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"Iaka"

$2 \leq n \leq 2 * 10^4$

测试链接： <https://acm.hdu.edu.cn/showproblem.php?pid=5512>

测试链接： <https://vjudge.net/problem/HDU-5512>

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

$\text{seed}(1) = 0, \text{seed}(i+1) = (\text{seed}(i) + \text{step}) \% \text{mod}$

比如, $\text{step} = 3, \text{mod} = 5$

$\text{seed}(1) = 0, \text{seed}(2) = 3, \text{seed}(3) = 1, \text{seed}(4) = 4, \text{seed}(5) = 2$

如果能产生 $0 \sim \text{mod}-1$ 所有数字, step和mod的组合叫 "Good Choice"

如果无法产生 $0 \sim \text{mod}-1$ 所有数字, step和mod的组合叫 "Bad Choice"

根据step和mod, 打印结果

$1 \leq \text{step}, \text{mod} \leq 10^5$

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 $ax \equiv 1(\text{mod } b)$ 的最小正整数解

题目保证一定有解，也就是a和b互质

$2 \leq a, b \leq 2 * 10^9$

测试链接：<https://www.luogu.com.cn/problem/P1082>

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

$1 \leq n \leq 10^{10}$ ， n 为偶数

$0 \leq m \leq 10^{10}$

测试链接：<https://www.luogu.com.cn/problem/P2054>