中国剩余定理及其扩展

前置知识
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，除法同余
讲解139 - 裴蜀定理和扩展欧几里得算法，扩展欧几里得算法详解，扩展欧几里得算法求逆元
讲解140 - 扩展欧几里得和二元一次不定方程，分析解如何变化的数学工具

中国剩余定理

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?

--《孙子算经》、韩信点兵的故事

左程云

中国剩余定理及其扩展

中国剩余定理
给出n个同余方程，m1、m2、..一定两两互质，求满足同余方程的最小正数解x
x ≡ r1 (% m1) x ≡ r2 (% m2) x ≡ r3 (% m3) .. x ≡ rn (% mn)

求解的原理：x = c1 + c2 + c3 + .. + cn，如果i!=j，ci % mi = ri，ci % mj = 0，则x达标
当m1、m2、..一定两两互质，必存在这样的x，根据如下过程就可以求出这样的x，并且是最小正数解

求解过程
1，计算m1 * m2 .. * mn的结果，因为m1、m2、.. mn一定两两互质，所以结果为最小公倍数lcm
2，对每一个同余方程计算：
   ai = lcm / mi   ai逆元 = ai在%mi意义下的逆元   ci = (ri * ai * ai逆元) % lcm
3，最小正数解x = 每一项ci的累加和 % lcm，因为，通解x = ? * lcm + 最小正数解x

课上重点图解，同时说明过程的正确性，以及为什么要求模数两两互质

左程云

中国剩余定理及其扩展

题目1
中国剩余定理模版
给出n个同余方程，求满足同余方程的最小正数解x
一共n个同余方程，x ≡ ri(% mi)
1 <= n <= 10
0 <= ri、mi <= 10^5
所有mi一定互质
所有mi整体乘积 <= 10^18
测试链接 ： https://www.luogu.com.cn/problem/P1495

中国剩余定理及其扩展

讲解扩展中国剩余定理之前，先介绍一个关于扩展欧几里得算法的小结论

如果ax + by = d，d为gcd(a,b)，其中一个特解是(x0, y0)
那么通解可以表示为： x = x0 + (b/d) * n　　y = y0 - (a/d) * n　　n为任意整数

如果ax + by = c，c为d的整数倍，根据上面的特解，可以得到该等式的一个特解(x0', y0')
其中，x0' = x0 * (c / d)，y0' = y0 * (c / d)
那么通解可以表示为： x = x0' + (b/d) * n　　y = y0' - (a/d) * n　　n为任意整数

以上都是，讲解140 - 扩展欧几里得和二元一次不定方程，讲的内容

其中通解x = x0' + (b/d) * n，如何得到最小非负特解？利用如下公式

最小非负特解 = x0' % (b / d)，取非负余数

中国剩余定理及其扩展

扩展中国剩余定理
给出n个同余方程，求满足同余方程的最小正数解x，所有Mi之间可能并不互质
x ≡ R1 (% M1) x ≡ R2 (% M2) x ≡ R3 (% M3) .. x ≡ Rn (% Mn)

求解过程，课上重点图解
1，补充初始模数m0 = 1，lcm = 1，tail = 0，那么，ans = lcm * x + tail，这必然成立
2，当前来到模数mi，余数ri，新的方程，ans = mi * y + ri，两个方程相减得到新表达式
3，lcm * x + mi * y = ri - tail，记为 ax + by = c，扩展欧几里得算法求解
4，如果不存在解，过程结束，说明不存在这样的ans。如果存在解，得到最小非负特解x0
5，通解x = x0 + (b/d) * n，带入ans = lcm * x + tail
6，得到ans = lcm * (b/d) * n + (lcm * x0 + tail)
7，令 lcm * (b/d) 记为 lcm’，令 (lcm * x0 + tail) % lcm’ 记为 tail’
8，表达式又是，ans = lcm’ * x + tail’，去往下一组方程，继续迭代ans
9，直到所有方程计算完毕，最终返回tail就是答案

中国剩余定理及其扩展

题目2
扩展中国剩余定理模版
给出n个同余方程，求满足同余方程的最小正数解x
一共n个同余方程，x ≡ ri(% mi)
1 <= n <= 10^5
0 <= ri、mi <= 10^12
所有mi不一定互质
所有mi的最小公倍数 <= 10^18
测试链接 ： https://www.luogu.com.cn/problem/P4777
测试链接 ： https://www.luogu.com.cn/problem/P1495

中国剩余定理及其扩展

题目3
猜数字
给定两个长度为n数组，一组为r1，r2，r3...，另一组为m1，m2，m3...
其中第二组数字两两互质，求最小正数解x
要求x满足，mi | (x - ri)，即(x - ri)是mi的整数倍
1 <= n <= 10
-10^9 <= ri <= +10^9
1 <= mi <= 6 * 10^3
所有mi的乘积 <= 10^18
测试链接 ： https://www.luogu.com.cn/problem/P3868

中国剩余定理及其扩展

题目4
屠龙勇士
一共n只巨龙，每只巨龙都有初始血量hp[i]，每只巨龙都有恢复能力recovery[i]
每只巨龙都会在攻击结束后开始恢复，初始一共m把剑，每把剑攻击力init[i]
每只巨龙只有当血量恰好为0时，才能被杀死。面对某只具体的龙，只能用固定的剑来攻击，规定如下：
攻击力不高于当前巨龙的血量，并且攻击力最大的一把剑，如果没有这样的剑，就选择攻击力最低的一把剑
需要按1~n的顺序依次讨伐巨龙，i号巨龙被杀后，那把攻击的剑会消失，同时奖励攻击力reward[i]的剑
勇士制定的策略如下，不管面对什么巨龙，攻击过程只打击ans下，让当前巨龙的血量<=0
然后在当前巨龙恢复的过程中，如果血量恰好为0，那么当前巨龙被杀死，勇士继续讨伐下一只
你的任务是算出最小的ans，让勇士可以在该策略下杀死所有巨龙
如果在固定打击次数的策略下，就是无法杀死所有巨龙，返回-1
查看数据范围可以打开测试链接 ： https://www.luogu.com.cn/problem/P4774

有序表的使用 + 转化为bi * ans ≡ ri(% mi) 方程组 + 特殊处理

左程云