

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

中国剩余定理及其扩展

中国剩余定理

给出 n 个同余方程， m_1 、 m_2 、.. m_n 一定两两互质，求满足同余方程的最小正数解 x

$$x \equiv r_1 (\% m_1) \quad x \equiv r_2 (\% m_2) \quad x \equiv r_3 (\% m_3) \dots x \equiv r_n (\% m_n)$$

求解的原理： $x = c_1 + c_2 + c_3 + \dots + c_n$ ，如果 $i \neq j$ ， $c_i \% m_i = r_i$ ， $c_i \% m_j = 0$ ，则 x 达标

当 m_1 、 m_2 、.. m_n 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 $m_1 * m_2 \dots * m_n$ 的结果，因为 m_1 、 m_2 、.. m_n 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：

$$a_i = lcm / m_i \quad a_i \text{逆元} = a_i \text{在 \% } m_i \text{ 意义下的逆元} \quad c_i = (r_i * a_i * a_i \text{逆元}) \% lcm$$

3，最小正数解 $x =$ 每一项 c_i 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

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， $x \equiv r_i (\% m_i)$

$1 \leq n \leq 10$

$0 \leq r_i, m_i \leq 10^5$

所有 m_i 一定互质

所有 m_i 整体乘积 $\leq 10^{18}$

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 (x_0, y_0)

那么通解可以表示为： $x = x_0 + (b/d) * n$ $y = y_0 - (a/d) * n$ 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 (x_0', y_0')

其中， $x_0' = x_0 * (c / d)$ ， $y_0' = y_0 * (c / d)$

那么通解可以表示为： $x = x_0' + (b/d) * n$ $y = y_0' - (a/d) * n$ 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 $x = x_0' + (b/d) * n$ ，如何得到最小非负特解？利用如下公式

最小非负特解 = $x_0' \% (b / d)$ ，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 M_i 之间可能并不互质

$$x \equiv R_1 \pmod{M_1} \quad x \equiv R_2 \pmod{M_2} \quad x \equiv R_3 \pmod{M_3} \dots x \equiv R_n \pmod{M_n}$$

求解过程，课上重点图解

- 1, 补充初始模数 $m_0 = 1$, $lcm = 1$, $tail = 0$, 那么, $ans = lcm * x + tail$, 这必然成立
- 2, 当前来到模数 m_i , 余数 r_i , 新的方程, $ans = m_i * y + r_i$, 两个方程相减得到新表达式
- 3, $lcm * x + m_i * y = r_i - tail$, 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 x_0
- 5, 通解 $x = x_0 + (b/d) * n$, 带入 $ans = lcm * x + tail$
- 6, 得到 $ans = lcm * (b/d) * n + (lcm * x_0 + tail)$
- 7, 令 $lcm * (b/d)$ 记为 lcm' , 令 $(lcm * x_0 + tail) \% lcm'$ 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， $x \equiv r_i (\% m_i)$

$1 \leq n \leq 10^5$

$0 \leq r_i, m_i \leq 10^{12}$

所有 m_i 不一定互质

所有 m_i 的最小公倍数 $\leq 10^{18}$

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 $r_1, r_2, r_3 \dots$ ，另一组为 $m_1, m_2, m_3 \dots$

其中第二组数字两两互质，求最小正数解 x

要求 x 满足， $m_i \mid (x - r_i)$ ，即 $(x - r_i)$ 是 m_i 的整数倍

$1 \leq n \leq 10$

$-10^9 \leq r_i \leq +10^9$

$1 \leq m_i \leq 6 * 10^3$

所有 m_i 的乘积 $\leq 10^{18}$

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 $1 \sim n$ 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 $b_i * ans \equiv r_i (\% m_i)$ 方程组 + 特殊处理