初等数论选讲

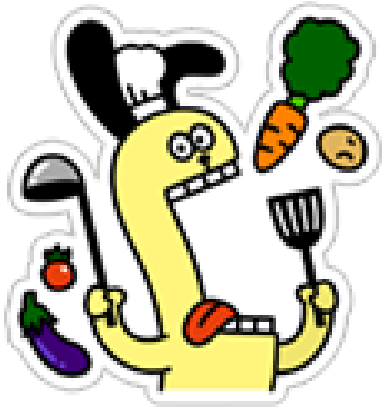
Tangjz

中国梦游协会

2019 年 1 月 21 日

写在前面

- 冬令营是交流的平台，~~欢迎打脸~~请各位不吝赐教



整体内容

- 整除理论
- 同余理论
- ~~不定方程~~
- ~~有理逼近~~
- ~~数论函数~~

整除理论

- 对于任意 $a, b \in \mathbb{Z},\ b \neq 0$，如果 $\exists_{q \in \mathbb{Z}}, a = bq$，那么 $b|a$，称 b 是 a 的约数（因数、因子），a 是 b 的倍数
- $c|b, b|a \Rightarrow c|a$
- $s, t \in \mathbb{Z}, c|a, c|b \Rightarrow c|sa + tb$
- $a|b, b|a \Rightarrow |a| = |b|$

整除理论

- 对于任意 $n \in \mathbb{Z}$，如果 $\exists_{k\in\mathbb{Z},|k|\neq 1,|k|\neq n} k|n$，则称 n 为合数，否则为质数（素数、不可约数）
- 若 $n \in \mathbb{Z}^+$ 为合数，则 $\min_{k|n} k \leq \sqrt{n}$
- 对于任意 $n \in \mathbb{Z}^+$，存在唯一的质数分解 $n = \prod_{i=1}^{k} {p_i}^{e_i}$，这里 p_i 互不相同
- 令 $\pi(n)$ 表示不超过 n 的质数个数，有 $\pi(n) = \Theta\left(\frac{n}{\ln n}\right)$

整除理论

- 对于 $x_1, x_2, \cdots, x_n \in \mathbb{Z}$，且 $\forall_{i=1,2,\cdots,n}, d|x_i$，则称 d 为它们的公约数
- 当 $x_1, x_2, \cdots, x_n$ 不全为零，存在最大的公约数，称为 $\gcd(x_1, x_2, \cdots, x_n)$
- 当 $\gcd(x_1, x_2, \cdots, x_n)$，称 $x_1, x_2, \cdots, x_n$ 互质（互素）
- $\gcd(a, b) = \gcd(a, b - a) = \gcd(a, b \bmod a)$
- 欧几里得算法：$r_1 = a, r_2 = b, r_3 = r_2 \bmod r_1, \cdots, r_{i+2} = r_i \bmod r_{i+1}, \cdots, r_{m-1} = \gcd(a, b), r_m = 0$，这里 $m = \mathcal{O}(\log a + \log b)$

整除理论

- 对于 $x_1, x_2, \cdots, x_n \in \mathbb{Z}$，且 $\forall_{i=1,2,\cdots,n}, x_i | d$，则称 d 为它们的公倍数
- 存在最小的正公倍数，称为 $\operatorname{lcm}(x_1, x_2, \cdots, x_n)$
- 对于质数 p 和 $x, y \in \mathbb{Z}$，有 $\gcd(p^x, p^y) = p^{\min(x,y)}$，$\operatorname{lcm}(p^x, p^y) = p^{\max(x,y)}$
- 对于 $a, b \in \mathbb{Z}^+$，有$a \cdot b = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$

试炼时间

整除理论

- **给定整数** a, b**，求** $\gcd(a, a+1, \cdots, b)$
- $1 \leq a \leq b \leq 10^{100}$
- **来源：** Codeforces Round #347 (Div. 2) – A. Complicated GCD

整除理论

- 给定整数 n，选出三个不超过 n 的正整数 x, y, z 使得 $\mathrm{lcm}(x, y, z)$ 最大
- $1 \leq n \leq 10^6$
- 来源：Codeforces Round #146 (Div. 1) – A. LCM Challenge

整除理论

- 给定 n 个正整数 $x_1, x_2, \cdots, x_n$，选出尽量多的数字 $x_{p_1}, x_{p_2}, \cdots, x_{p_m}$ $(1 \leq p_1 < p_2 < \cdots < p_m \leq n)$ 使得 $\gcd(x_1, x_2, \cdots, x_m) > 1$，或者确定解不存在
- $1 \leq n, x_i \leq 10^5$
- 来源：Codecraft-17 and Codeforces Round #391 – B. Bash's Big Day

整除理论

- 给定 n 个正整数 $x_1, x_2, \cdots, x_n$，删掉尽量少的数字使得所有数的 $\gcd$ 变大，或者确定解不存在
- $1 \leq n \leq 3 \times 10^5$, $1 \leq a_i \leq 1.5 \times 10^7$
- 来源：Codeforces Round #511 (Div. 1) – A. Enlarge GCD

整除理论

- 给定长度为 n 的序列 $a_1, a_2, \cdots, a_n$，有 q 个询问，每次询问给定 x，问有多少区间 (l, r) 满足 $\gcd(a_l, a_{l+1}, \cdots, a_r) = x$
- $1 \leq n \leq 10^5$, $1 \leq q \leq 3 \times 10^5$, $1 \leq a_i, x \leq 10^9$
- 来源：(Codeforces) Bayan 2015 Contest Warm Up – D. CGCDSSQ

整除理论

- 给定 m 个数 $a_1, a_2, \cdots, a_m$，定义 $n = \prod_{i=1}^{m} a_i$，求最大的整数 k 使得存在 $d|n$, $d^k|n$，并对这个最大的 k 计算有多少可能的正整数 d
- $1 \leq m \leq 600$, $2 \leq a_i \leq 10^{18}$
- 来源：Poland Olympiad Informatics 2010 – Divine divisor

整除理论

- 给定 n 个数 $a_1, a_2, \cdots, a_n$，定义 $a = \prod_{i=1}^{n} a_i$，求 a 的约数个数
- $1 \leq n \leq 500$, $1 \leq a_i \leq 10^{18}$, 保证 a_i 的约数个数在 3 到 5 之间
- 来源：(Codeforces) Lyft Level 5 Challenge 2018 - Elimination Round – D. Divisors

整除理论

- 给 n 个整数 $a_1, a_2, \cdots, a_n$ 和 m 个整数 $b_1, b_2, \cdots, b_m$，定义 $Q = \frac{a_1 \cdot a_2 \cdots a_n}{b_1 \cdot b_2 \cdots b_m} = \frac{A}{B}$，其中 A 与 B 互质。有 k 个询问，每个询问给出一个 M，求一个整数 C 满足 $0 \leq C < M$ 且 $A \equiv BC \pmod{M}$，或者确定解不存在
- $1 \leq n, m \leq 5000$, $1 \leq k \leq 50$, $2 \leq M \leq 10^{18}$, $1 \leq a_i, b_j \leq 10^{18}$
- 来源：Petrozavodsk Winter Camp 2016, SPb SU + SPb AU Contest – C. Fraction Factory

整除理论

- 对任意正整数 u，定义 $f(u)$ 是 u 的所有质因子组成的集合。如果正整数 u 和 v 满足 u 整除 v 且 $f(u) = f(v)$，那么认为 u 对 v 来说是友好的。给出两个正整数 k_1 和 k_2，分别求有多少个数对它们来说是友好的
- $1 \leq k_1, k_2 \leq 10^{24}$，保证 k_1 和 k_2 拥有相同的最大质因子，不同的次大质因子（如果存在）
- 来源：Asia Regional Changchun Online 2015 – K. Good Numbers

整除理论

- 有 n 种糖果，第 i 种糖果数量为 C_i，现在要用两种方式来包装它们。第一种方式要求每包只含一种糖果，第二种方式要求每包必须含所有种类糖果且每种数量均等。此外，要求每种包装方式至少使用一次，包装后每包糖果数量相等，严格大于 1，统计合法方案数。
- $2 \leq n \leq 10^5$, $1 \leq C_i \leq 10^9$
- 来源：Latin America Regional 2011 – C. Candy's Candy

整除理论

- 对于长度 A 宽度 B 的矩形，在其上沿着平行矩形边界的直线切若干刀，可以形成一系列小的矩形，给出每种小矩形的长 w 宽 h 和数量 c，求有多少种 A, B 能够切出这些小矩形
- $1 \leq n \leq 2 \times 10^5$, $1 \leq w, h, c \leq 10^{12}$
- 来源：Tinkoff Internship Warmup Round 2018 and Codeforces Round #475 (Div. 1) – C. Cutting Rectangle

整除理论

- 有 n 种卡片，第 i 种面值为 c_i，属性为 l_i，买进卡片 i 后可以在数轴上任意向左右移动 l_i 步任意次，花费最小的代价使得从 $x = 0$ 的位置可以到达所有 $x \in \mathbb{Z}$ 的位置，或者确定解不存在
- $1 \leq n \leq 300$, $1 \leq c_i \leq 10^5$, $1 \leq l_i \leq 10^9$
- 来源：Codeforces Round #290 (Div. 1) Rectangle – D. Fox And Jumping

整除理论

- 找出最小的 n 个正整数 z 使得 $z = \left\lfloor \frac{x}{2} \right\rfloor + x + xy$ 不存在 x 和 y 均为正整数的解，按照 z 升序输出每个 $(z \bmod (10^9 + 7))$
- $1 \leq n \leq 40$
- 来源：Codeforces Round #139 (Div. 1) – E. Unsolvable

Break Time

同余理论

- 对于正整数 m，若整数 a, b 满足 $m|a-b$，也即存在整数 k 使得 $a = b + km$，则称 a, b 在模 m 意义下同余，记作 $a \equiv b \pmod{m}$
- $a_1 \equiv b_1, a_2 \equiv b_2 \pmod{m} \Rightarrow a_1 \pm a_2 \equiv b_1 \pm b_2, a_1 a_2 \pmod{m}$
- 对于 $a \equiv b \pmod{m}$，若 $d|m$，则 $a \equiv b \pmod{d}$
- 对于 $a \equiv b \pmod{m}$，若 $d|a, d|b, d|m$，则 $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$
- 对于 $a \equiv b \pmod{m}$，有 $\gcd(a, m) = \gcd(b, m)$

同余理论

- 对于任意整数 a，存在整数 q, r 使得 $a = mq + r, 0 \leq r < m$，所有可能的 r 构成一个模 m 的剩余系，其定义了整数在模意义下的等价类 $\{a \bmod m | a \in \mathbb{Z}\}$
- 对于质数 m，若 $\gcd(a, m) = 1$，b 是任意整数，则 $\{(ax + b) \bmod m | x \in \mathbb{Z}\} = \{x \bmod m | x \in \mathbb{Z}\}$
- 对于质数 m_1 和 m_2，若 $\gcd(m_1, m_2) = 1$，则 $\{(m_2 x_1 + m_1 x_2) \bmod m_1 m_2 | x_1 \in \mathbb{Z}, x_2 \in \mathbb{Z}\} = \{x \bmod m_1 m_2 | x \in \mathbb{Z}\}$

同余理论

- 对于正整数 m，$\{a \bmod m | a \in \mathbb{Z}, \gcd(a, m) = 1\}$ 构成一个模 m 的简化剩余系，该集合的大小被定义为欧拉函数 $\varphi(m)$
- 对于正整数 m，若 $\gcd(a, m) = 1$，则 $\{ax \bmod m | x \in \mathbb{Z}, \gcd(x, m) = 1\} = \{x \bmod m | x \in \mathbb{Z}, \gcd(x, m) = 1\}$
- 对于正整数 m_1 和 m_2，若 $\gcd(m_1, m_2) = 1$，则 $\{(m_2 x_1 + m_1 x_2) \bmod m_1 m_2 | x_1 \in \mathbb{Z}, \gcd(x_1, m_1) = 1, x_2 \in \mathbb{Z}, \gcd(x_2, m_2) = 1\} = \{x \bmod m_1 m_2 | x \in \mathbb{Z}, \gcd(x, m_1 m_2) = 1\}$

同余理论

- 对于正整数 m，若 $\gcd(a,m)=1$，则存在 s 满足 $1\le s<m$，$sa\equiv 1 \pmod m$，也即存在整数 s,t 满足 $sa+tm=1$，记 s 为 a 在模 m 意义下的乘法逆元 a^{-1}
- 扩展欧几里得算法：寻找二元一次不定方程 $sx+ty=\gcd(x,y)$ 的一组整数解 (s,t)
  - $u_ix+v_iy=r_i$
  - $(u_1,v_1,r_1)=(1,0,x),(u_2,v_2,r_2)=(0,1,y)$
  - $q_{i+2}=\left\lfloor \frac{r_i}{r_{i+1}} \right\rfloor$
  - $(u_{i+2},v_{i+2},r_{i+2})=(u_i,v_i,r_i)-q_{i+2}\cdot(u_{i+1},v_{i+1},r_{i+1})$

同余理论

中国剩余定理：对于两两互质的 m_i，同余方程组

$$\begin{cases} x & \equiv r_1 \pmod{m_1} \\ x & \equiv r_2 \pmod{m_2} \\ \cdots & \\ x & \equiv r_k \pmod{m_k}, \end{cases}$$

的解为 $x \equiv \sum_{i=1}^{k} r_i M_i' M_i \pmod{M}$，其中 $M = \prod_{i=1}^{k} m_i$，

$M_i = \frac{M}{m_i}$，$M_i' \equiv {M_i}^{-1} \pmod{m_i}$

同余理论

- 费马小定理：若 p 是质数，则对于任意整数 a 有 $a^p \equiv a \pmod{p}$
- 欧拉定理：若 m 是正整数，$\gcd(a, m) = 1$，则有 $a^{\varphi(m)} \equiv 1 \pmod{m}$
- 威尔逊定理：若 p 是质数，则有 $(p-1)! \equiv -1 \pmod{p}$

试炼时间

同余理论

- 环上有 $4n$ 个点，按顺时针编号 1 到 $4n$，求集合

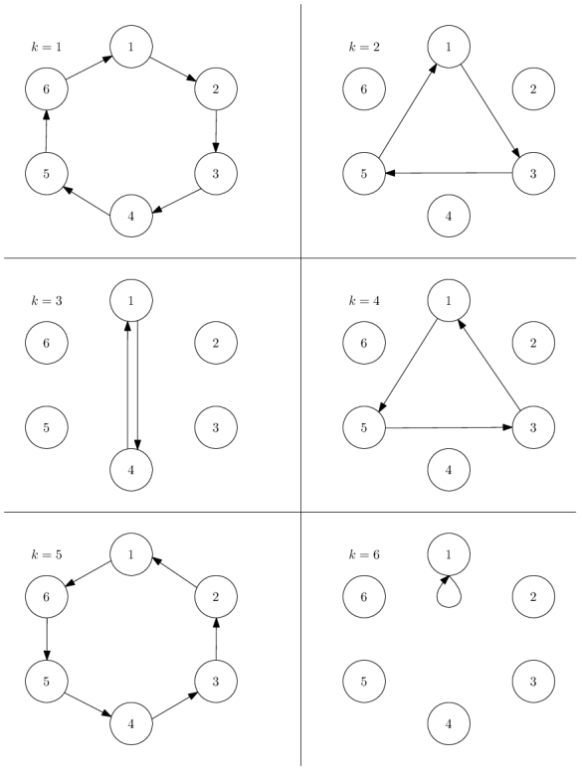
  $\{((n+1)x \bmod 4n)+1 | x \in \mathbb{N}\}$ 的元素个数

- $1 \leq n \leq 10^9$

- 来源：Codeforces Round #122 (Div. 2) – B. Square

同余理论

- 环上有 n 个点，按顺时针编号 1 到 n，对于整数 k，记集合 $\{(kx \bmod n) + 1 | x \in \mathbb{N}\}$ 的元素和为 f_k，求有多少种不同的 f_k，升序输出
- $2 \leq n \leq 10^9$
- 来源：(Codeforces) Good Bye 2018 – C. New Year and the Sphere Transmission



同余理论

- $n \times n$ 的矩阵（下标从 0 开始）里有 m 个特殊点，给定整数 dx, dy，请你选定一组整数 x, y 使得集合 $\{((x + kdx) \bmod n, (y + kdy) \bmod n) | k \in \mathbb{N}\}$ 中特殊点的数量最大
- $1 \leq n \leq 10^6$, $1 \leq m \leq 10^5$, $1 \leq dx, dy \leq n$, $\gcd(n, dx) = \gcd(n, dy) = 1$
- 来源：Codeforces Round #280 (Div. 2) – E. Vanya and Field

同余理论

- 给定一个周期为 n 的无穷序列中连续 n 项 $a_0, a_1, \cdots, a_{n-1}$，统计有多少整数对 (l, s) 满足 $0 \leq l < n$, $1 \leq s < n$ 且 $\forall_{k \in \mathbb{Z}}, a_k \geq a_{l+k}$
- $1 \leq n \leq 2 \times 10^5$, $1 \leq a_i \leq 10^6$
- 来源：Codeforces Round #323 (Div. 1) – C. Superior Periodic Subarrays

同余理论

- 构造三个 1 到 n 的置换 $a[1..n]$, $b[1..n]$, $c[1..n]$ 使得

  $\forall_{i=1,2,\cdots,n}, a_i + b_i \equiv c_i \pmod{n}$，或者确定解不存在

- $1 \leq n \leq 10^5$

- 来源：Codeforces Round #183 (Div. 1) – A. Lucky Permutation Triple

同余理论

- 构造一个 1 到 n 的置换 $a[1..n]$ 使得序列

  $\{a_1 \bmod n, a_1a_2 \bmod n, \cdots, \prod_{i=1}^{n} a_i \bmod n\}$ 为一个 0 到 $n-1$ 的置换，或者确定解不存在

- $1 \leq n \leq 10^5$

- 来源：Codeforces Round #278 (Div. 1) – C. Prefix Product Sequence

同余理论

- 给定 $a, b, c, x_1, x_2, y_1, y_2$，求 $ax + by + c = 0$ 满足 $x_1 \leq x \leq x_2$ 且 $y_1 \leq y \leq y_2$ 的整数解数量
- 所有数字绝对值不超过 10^8
- 来源：SGU 106 – The equation

同余理论

- 给定 $m, h_{i,0}, a_i, x_i, y_i$ $(i = 1, 2)$，定义

  $h_{i,j+1} = (x_i h_{i,j} + y_i) \bmod m$，求最小非负整数 k 使得 $h_{i,k} = a_i$

- $2 \le m \le 10^6$, $0 \le h_{i,0}, a_i, x_i, y_i < m$

- 来源：Codeforces Round #305 (Div. 1) – A. Mike and Frog

同余理论

- 有 n 个观察员，第一个观察员在 0 秒开始观察星空，随后第 i 个观察员会在第 $i-1$ 个观察员之后 a_i 秒观察，第一个观察员也会在第 n 个观察员之后 a_1 秒观察，有一颗星星每隔 T 秒闪烁一次，闪烁时一定是整数秒，问每个观察员有多少种可能成为第一个观察到这颗星星的人
- $1 \leq T \leq 10^9$, $2 \leq n \leq 2 \times 10^5$, $1 \leq a_i \leq 10^9$
- 来源：Codeforces Round #421 (Div. 1) – D. Mister B and Astronomers

同余理论

- 有 n 个带周期的无穷序列，第 i 个序列 a_i 的周期为 k_i，每个序列的第 1 项 $a_{i,1}$ 到第 k_i 项 a_{i,k_i} 给定。对于每种可能的元素取值 v，找到一个下标 j 使得 $j \leq 10^{100}$ 且序列 $\{a_{1,j}, a_{2,j}, \cdots, a_{n,j}\}$ 中连续的 v 组成的区间最长，只对每个 v 输出区间长度
- $1 \leq n, \max(v) \leq 10^5$, $1 \leq k_i \leq 40$, $\sum_{i=1}^{n} k_i \leq 2 \times 10^5$
- 来源：(Codeforces) Intel Code Challenge Elimination Round – F. Cyclic Cipher

同余理论

- 给定四个正整数 M, D, L, R，求最小非负整数 x 使得 $L \leq (Dx \bmod M) \leq R$，或者确定解不存在
- $1 \leq M, D, L, R \leq 2 \times 10^9$
- 来源：POJ Monthly, 2008.03.16 – D. A Modular Arithmetic Challenge

同余理论

- 给定两个十进制小数 a, b，求最小的正整数 k，使得存在整数 x 满足 $ak \leq x \leq bk$
- a, b 的有效数字小于 300 位
- 来源：Vijos 1504 – 强大的区间

同余理论

- 给出随机生成的不含前导零的正整数 p，找到最小的非负整数 k 使得 2^k 的十进制表示最高位与 p 完全相同
- $1 \leq p < 10^{50}$, 随机时首先随机 p 的十进制长度，然后随机每一位的值
- 来源：Petrozavodsk Summer Camp 2014, Petr Mitrichev Contest 12 – F. Recognize Power of Two

Thank you!