数论题目选讲

张一钊

IIS, Tsinghua University

2022 年 10 月 2 日

P2312 解方程

已知多项式方程：

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = 0$$

求这个方程在 $[1, m]$ 内的整数解（n 和 m 均为正整数）。

$0 < n \leq 100, |a_i| \leq 10^{10000}, a_n \neq 0, m \leq 10^6$。

P2312 解方程

令多项式为 $f(x)$。令 p 是一个出题人不知道的素数。若 $f(x) \equiv 0 \pmod{p}$ 则很有可能有 $f(x) = 0$。

计算 $f(x) \bmod p$ 只需要 $a_i \bmod p$，可以在读入 a_i 的时候顺便计算。

P2312 解方程

我们考虑 k 个素数 $p_1, \ldots, p_k$。我们认为 $f(x) = 0$ 当且仅当对于每个 i，$f(x) \equiv 0 \pmod{p_i}$。

注意到 $f(x) \equiv f(x \bmod p_i) \pmod{p_i}$。对于每个 p_i，对于 $0 \leq x < p_i$ 计算 $f(x) \bmod p_i$。对于每个 $x \in [0, m]$，如果 $f(x \bmod p_i) \bmod p_i$ 均为 0，我们认为 $f(x) = 0$。复杂度 $O\left(n \sum p_i + mk\right)$。

CF757B Bash's Big Day

给出 $\{a_1, a_2, \ldots, a_n\}$。求一个集合 $I = \{i_1, i_2, \ldots, i_k\}$，满足

$$\gcd(a_{i_1}, a_{i_2}, \ldots, a_{i_k}) > 1$$

且 k 尽量大。

$n, a_i \le 10^5$。

CF757B Bash's Big Day

如果 $\gcd(a_{i_1}, a_{i_2}, \ldots, a_{i_k}) = d$，则 $a_{i_1}, a_{i_2}, \ldots, a_{i_k}$ 都是 d 的倍数。

设 $V = \max a_i$。预先数一下每个数有多少个。对于每个 $2 \le d \le V$，枚举 d 的倍数，统计有多少个。

复杂度是什么？

$$\sum_{d \ge 2} \left\lfloor \frac{V}{d} \right\rfloor$$

CF757B Bash's Big Day

$$\sum_{i=1}^{n} \frac{1}{i} \sim \ln n$$

因此复杂度是 $O(n + V \ln V)$。

如果只枚举素数的倍数，复杂度是 $O(n + V \ln \ln V)$。

P1445 [Violet] 樱花

给定 n，求有多少组正整数 (x, y) 满足

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n!}$$

答案对 $10^9 + 7$ 取模。

$n \le 10^6$。

P1445 [Violet] 樱花

$$\frac{1}{x}+\frac{1}{y}=\frac{1}{n!} \iff (x-n!)(y-n!)=(n!)^2$$

令 $\sigma_0(n)$ 表示 n 的因子个数。设 $n={p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_s}^{\alpha_s}$ 是 n 的标准分解，则

$$\sigma_0(n)=(\alpha_1+1)(\alpha_2+1)\dots(\alpha_s+1)$$

因此问题变为如何求 $(n!)^2$ 的标准分解，可以先求 $n!$ 的标准分解。

P1445 [Violet] 樱花

$n!$ 中素因子 p 的幂次为

$$\left\lfloor\frac{n}{p}\right\rfloor+\left\lfloor\frac{n}{p^2}\right\rfloor+\left\lfloor\frac{n}{p^3}\right\rfloor+\cdots$$

枚举不超过 n 的素数 p，计算出 $n!$ 中 p 的幂次，那么即可计算出 $\sigma_0((n!)^2)$。

P3601 签到题

我们定义一个函数：qiandao(x)为小于等于x的数中与x**不互质**的数的个数。

这题作为签到题，给出l和r，要求求$\sum_{i=l}^{r} qiandao(i) \ mod \ 666623333$。

$1 \le l \le r \le 10^{12}, r - l \le 10^6$。

Euler 函数

Euler 函数 $\varphi(n)$ 表示小于等于 n 且与 n 互质的正整数的个数。

设 $n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\cdots{p_s}^{\alpha_s}$ 是 n 的标准分解，则

$$\varphi(n) = n \cdot \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right)$$

P3601 签到题

注意到 n 最多有一个大于 $\sqrt{n}$ 的素因子。

对于每个小于 $\sqrt{r}$ 的素数 p，枚举 p 在 l 与 r 之间的倍数，把 p 从里面除尽。这之后，每个数最多只剩下一个素因子。这样对于 l 到 r 中的每个 n，我们可以计算出每个素因子对 $\varphi(n)$ 的贡献，就可以计算出 $\varphi(n)$。

答案就是 $\sum_{n=l}^{r}(n-\varphi(n))$。

P2568 GCD

给定正整数 n，求 $1 \le x, y \le n$ 且 $\gcd(x, y)$ 为素数的数对 (x, y) 有多少对。

$n \le 10^7$。

P2568 GCD

设 $\gcd(x, y) = p$。令 $x = x'p, y = y'p$，则 $x', y' \le \lfloor n/p \rfloor$ 且 $\gcd(x', y') = 1$。枚举素数 $p \le n$，问题转化为求 $1 \le x, y \le k$，且 $\gcd(x, y) = 1$ 的组数（特别的，要求的是 $k = \lfloor n/p \rfloor$ 的情况）。

P2568 GCD

$$\begin{aligned}\sum_{i=1}^{k}\sum_{j=1}^{k}[\gcd(i,j)=1] &= 2\sum_{i=1}^{k}\sum_{j=1}^{i}[\gcd(i,j)=1]-\sum_{i=1}^{k}[\gcd(i,i)=1]\\ &= 2\sum_{i=1}^{k}\varphi(i)-1\end{aligned}$$

P2568 GCD

因此答案就是

$$\sum_{\substack{p\leq n \\ p \text{ is prime}}} \left(2\sum_{i=1}^{\lfloor n/p\rfloor} \varphi(i) - 1\right)$$

线性筛求出 $\varphi(i)$，前缀和以后枚举 p 就能算出答案。

P4139 上帝与集合的正确用法

有 T 个询问，每个询问给出 m，求

$$2^{2^{2^{\cdot^{\cdot^{\cdot}}}}} \bmod m$$

$T \le 1000, m \le 10^7$。

欧拉定理

正整数 a, n 满足 $\gcd(a, n) = 1$，则

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

P4139 上帝与集合的正确用法

设 $m = 2^r \cdot q$，其中 q 是奇数，则

$$2^{2^{2^{\cdot^{\cdot^{\cdot}}}}} = 2^r \times 2^{2^{2^{\cdot^{\cdot^{\cdot}}}} - r} \equiv 2^r \times 2^{\left(2^{2^{\cdot^{\cdot^{\cdot}}}} - r\right) \bmod \varphi(q)} \pmod q$$

$\left(2^{2^{2^{\cdot^{\cdot^{\cdot}}}}} - r\right) \bmod \varphi(q)$ 可以递归的算。
$O(\log m)$ 次以后将有 $q \leq 2$，递归终止。

一个结论

如果 a 与 n 不一定互质，则如果 $k \geq \varphi(n)$，则有

$$a^k \equiv a^{k \bmod \varphi(n) + \varphi(n)} \pmod{n}$$

P3868 [TJOI2009] 猜数字

现有两组数字，每组 k 个。

第一组中的数字分别用 $a_1, a_2, \cdots, a_k$ 表示，第二组中的数字分别用 $b_1, b_2, \cdots, b_k$ 表示。

其中第二组中的数字是两两互素的。求最小的 $n \in \mathbb{N}$，满足对于 $\forall i \in [1, k]$，有 $b_i | (n - a_i)$。

$1 \le k \le 10, |a_i| \le 10^9, 1 \le b_i \le 6 \times 10^3, \prod_{i=1}^{k} b_i \le 10^{18}$。

P3868 [TJOI2009] 猜数字

$b_i \mid (n - a_i) \iff n \equiv a_i \pmod{b_i}$。

令 $M = \prod_{i=1}^{k} b_i$。由中国剩余定理，可以唯一确定一个 $0 \le n_0 < M$，使得 $n \equiv n_0 \pmod{M}$。

中国剩余定理

设 $M_i = M/b_i$。则 $\gcd(M_i, b_i) = 1$；而对于 $j \neq i$，有 $b_i \mid M_j$。那么存在 r_i 满足 $r_i M_i \equiv 1 \pmod{b_i}$。令 $n = \sum_{i=1}^{k} a_i M_i r_i$。则

$$n \equiv a_i M_i r_i \equiv a_i \pmod{b_i}$$

可令 $n_0 = n \bmod M$。

二元一次不定方程

形如 $ax+by=c$ 的方程称为二元一次不定方程, 其中 x,y 为未知数。特别的，我们研究 a,b,c 均为整数的方程的整数解。

Bézout 定理说明了，方程 $ax+by=c$ 有整数解当且仅当 $\gcd(a,b)\mid c$。

容易看出，若一个二元一次不定方程有整数解，则其必有无穷多组解。

扩展 Euclid 算法

记 $\gcd(a,b)=d$，考虑方程 $ax+by=d$。

由于 $\gcd(a,b)=\gcd(b,a \bmod b)=d$，那么方程

$bx+(a \bmod b)y=d$ 也有解。

扩展 Euclid 算法

设有 x_0, y_0 满足 $bx_0 + (a \bmod b)y_0 = d$。

那么可以证明，

$$\begin{cases} x = y_0 \\ y = x_0 - \left[\dfrac{a}{b}\right] y_0 \end{cases}$$

满足 $ax + by = d$。

扩展 Euclid 算法

当 $b = 0$ 时，显然 $x = 1, y = 0$ 是一个合法的解。

当 $b \neq 0$ 时，我们递归的求解方程 $bx + (a \bmod b)y = d$，利用得到的解推出原方程的解。

这个算法称为扩展 Euclid 算法。

逆元

对于整数 a，如果存在一个 x，使得 $ax \equiv 1 \pmod{m}$，则称 x 为 a 模 m 的逆，记作 $a^{-1} \pmod{m}$。

注意到

$$
\begin{aligned}
ax &\equiv 1 \pmod{m} \\
\Leftrightarrow ax + my &= 1
\end{aligned}
$$

因此 $a^{-1} \pmod{m}$ 存在当且仅当 $\gcd(a, m) = 1$。

可以使用扩展 Euclid 算法求逆元。

P4495 [HAOI2018] 奇怪的背包

小 C 非常擅长背包问题，他有一个奇怪的背包，这个背包有一个参数 P ，当他向这个背包内放入若干个物品后，背包的重量是物品总体积对 P 取模后的结果。

现在小 C 有 n 种体积不同的物品，第 i 种占用体积为 V_i ，每种物品都有无限个。他会进行 q 次询问，每次询问给出重量 w_i ，你需要回答有多少种放入物品的方案，能将一个初始为空的背包的重量变为 w_i。注意，两种方案被认为是不同的，当且仅当放入物品的种类不同，而与每种物品放入的个数无关．不难发现总的方案数为 2^n。

由于答案可能很大，你只需要输出答案对 10^9+7 取模的结果。

$n, q \leq 10^6, P \leq 10^9$。

观察

设 $S = \{V_1, V_2, \ldots, V_k\}$ 是一些物品的集合。

那么 S 能凑出 w，即意味着

$$x_1V_1 + x_2V_2 + \cdots + x_kV_k \equiv w \pmod P$$

有解，也等价于

$$x_1V_1 + x_2V_2 + \cdots + x_kV_k + yP = w$$

有解。

观察

由 Bézout 定理，这个方程有解当且仅当

$$\gcd(V_1, V_2, \ldots, V_k, P) \mid w$$

另外，可以观察到：

$$\gcd(V_1, V_2, \ldots, V_k, P) = \gcd(\gcd(V_1, P), \ldots, \gcd(V_k, P))$$

观察

以及：已知 $d \mid P$。那么 $d \mid w \iff d \mid \gcd(P, w)$。

因此，方程有解当且仅当

$$\gcd(\gcd(V_1, P), \ldots, \gcd(V_k, P)) \mid \gcd(w, P)$$

观察

问题被转化为：设 $S = \{V_1, \dots, V_n\}$ 为物品的集合。每次给出 w，求有多少个 S 的子集 $T = \{V_{i_1}, \dots, V_{i_k}\}$ 满足

$$\gcd(\gcd(V_{i_1}, P), \dots, \gcd(V_{i_k}, P)) \mid \gcd(w, P)$$

进一步，我们可以先考虑有多少子集 T 满足

$$\gcd(\gcd(V_{i_1}, P), \dots, \gcd(V_{i_k}, P)) = d$$

显然 $\gcd(V_i, P)$ 相同的 V_i 要一起考虑。a_k 就是满足 $\gcd(V_i, P) = d_k$ 的 V_i 的个数。

P4495 [HAOI2018] 奇怪的背包

体积为 V_i 的物品相当于体积为 $\gcd(P, V_i)$ 的物品。

根据 Bézout 定理，存在正整数 k 使得 $kV_i + \ell P = \gcd(P, V_i)$，即 $kV_i \bmod P = \gcd(P, V_i)$，即 k 个体积为 V_i 的物品可以视为一个体积为 $\gcd(P, V_i)$ 的物品。

假设 P 共有 σ 个因子，令 d_k 表示 P 的第 k 大的因子。问题描述相当于告诉你体积为 d_k 的物品有 a_k 个。

P4495 [HAOI2018] 奇怪的背包

集合 S 中的物品能凑出 w 当且仅当 $\gcd S \mid w$，也等价于 $\gcd S \mid \gcd(P, w)$。

也是 Bézout 定理。

P4495 [HAOI2018] 奇怪的背包

令 $f(i, d_j)$ 表示前考虑 P 的前 i 个因子，gcd 恰好为 d_j 的集合有多少个。这时候只有 $j \le i$ 有意义。
一开始 $f(i, d_j) \leftarrow f(i-1, d_j)$。枚举 $1 \le j < i$，如果加入至少一个 d_i，对 $f(i, \gcd(d_i, d_j))$ 产生 $(2^{a_i} - 1)f(i-1, d_j)$ 的贡献。
另外，$f(i, d_i) = 2^{a_i} - 1$。

P4495 [HAOI2018] 奇怪的背包

再计算 $g(d)=\sum_{k|d}f(\sigma,k)$，那么 w_i 的答案就是 $g(\gcd(w_i,P))$。