数论

罗进

December 29, 2017

Outline

一些记号

- $gcd(x, y)$ 为 x, y 的最大公约数，$lcm(x, y)$ 为 x, y 的最小公倍数.
- $[\ some\_condition\ ]$ 当 $some\_condition$ 为真时等于 1，为假时等于 0.
- $\varphi(n)$ 为欧拉函数，$\mu(n)$ 为默比乌斯函数.
- $\sigma(n)$ 为 n 的约数之和.
- $\sigma_k(n)$ 为 n 的约束的 k 次方之和.
- 如果 $N = k \cdot a$，我们就称 a 整除 N，记作 $a \mid N$.

定义及性质

定义

- 素数指在大于 1 的自然数中，除了 1 与自身外，无法被其他自然数整除的数.

性质

- 有无穷多个素数.

素数密度

- $\pi(x) \sim \frac{x}{\ln x}$

筛法

- 求出 $1 \sim N$ 中所有的素数.

Eratosthenes 筛法

- 记录一个 vis 数组代表数字有没有被标记，从 2 到 n 枚举，如果当前数没有被标记，那么它就是一个素数，否则它是一个合数．如果是一个素数，就把当前数的倍数全都标记．复杂度为 $O(NlogN)$

筛法

- 求出 $1 \sim N$ 中所有的素数.

Eratosthenes 筛法

- 记录一个 vis 数组代表数字有没有被标记，从 2 到 n 枚举，如果当前数没有被标记，那么它就是一个素数，否则它是一个合数. 如果是一个素数，就把当前数的倍数全都标记. 复杂度为 $O(NlogN)$

Euler 筛法

- 同样记录一个 vis 数组，但是要保证每个数只会被标记 1 次. 从 2 到 n 枚举，如果当前数没有被标记，那它就是一个素数. 然后枚举小于等于当前数最小质因子的素数 p，并把 $p \times i$ 标记. 显然每个数有当 p 为它最小质因子时会被标记一遍，所以复杂度为 $O(N)$.
- 利用 Euler 筛法的性质能够求出某个积性函数在 1 到 n 的值.

素数测试

素数测试

暴力判定

- N 要么是一个素数，要么就会存在一个不超过 $\sqrt{N}$ 的约数. 因此，我们只需要枚举 $1 \to \sqrt{N}$ 的数，判断它能否整除 N，复杂度 $O(\sqrt{N})$.

素数测试

暴力判定

- N 要么是一个素数，要么就会存在一个不超过 $\sqrt{N}$ 的约数. 因此，我们只需要枚举 $1 \to \sqrt{N}$ 的数，判断它能否整除 N，复杂度 $O(\sqrt{N})$.
- 但是 N 很大怎么办呢?

素数测试

暴力判定

- N 要么是一个素数, 要么就会存在一个不超过 $\sqrt{N}$ 的约数. 因此, 我们只需要枚举 $1 \to \sqrt{N}$ 的数, 判断它能否整除 N, 复杂度 $O(\sqrt{N})$.
- 但是 N 很大怎么办呢?

费马小定理

- 如果 p 为质数, 那么 $a^{p-1} \equiv 1 \pmod p, (0 < a < p)$.

素数测试

暴力判定

- N 要么是一个素数，要么就会存在一个不超过 $\sqrt{N}$ 的约数. 因此，我们只需要枚举 $1 \rightarrow \sqrt{N}$ 的数，判断它能否整除 N，复杂度 $O(\sqrt{N})$.
- 但是 N 很大怎么办呢?

费马小定理

- 如果 p 为质数，那么 $a^{p-1} \equiv 1 \pmod p, (0 < a < p)$.

证明

- 如果 $x \neq y, (0 < x, y < p)$，则对于 $0 < a < p$, $x \cdot a \not\equiv y \cdot a \pmod p$.
- $1 \cdot 2 \cdot 3 \cdots (p-1) \equiv (1 \cdot a) \cdot (2 \cdot a) \cdot (3 \cdot a) \cdots ((p-1) \cdot a) \pmod p$.
  即 $W \equiv W \cdot a^{p-1} \pmod p \Rightarrow a^{p-1} \equiv 1 \pmod p$.

素数测试

伪素数测试

- 如果存在 $0 < a < p$ 使得 $a^{p-1} \not\equiv 1 \pmod{p}$，那么就能够说明 p 不是素数.
- 随机 a，然后进行判断. ~~感觉挺靠谱~~ .
- 但是对于有些合数并不能找到这样的 a.
- 比如说 561, 1105 等，这些数被称为 Carmichael 数.

Miller-Rabin 素数测试

定理

如果 $x^2 \equiv 1 \pmod{p}$ 且 p 为素数，那么 $x \equiv \pm 1 \pmod{p}$.

判定方法

- 结合上面的定理与费马小定理.
- 设 $n-1=2^t u$, 每次随机一个 a, 先求出 a^u ，然后倍增到 $a^{2^t u}$. 倍增的同时利用上面的定理判断，最后再判断 $a^{2^t u}$ 模 n 的值.

性质

- carmichael 数存在能证明它是合数的证据.
- 如果 n 是一个奇合数，则 n 为合数的证据数目至少为 $\frac{n-1}{2}$.
- 随机 k 次，出错的概率为 $\frac{1}{2^k}$.

定义及性质

定义

$$\mu(n) = \begin{cases} (-1)^k & n = p_1 p_2 \cdots p_k \\ 0 & p_k^2 \mid n \\ 1 & n = 1 \end{cases}$$

性质

- $\mu(n)$ 是积性函数.
- $\sum_{d|n} \mu(d) = [n = 1]$

默比乌斯反演

公式

- $g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$
- $g(n) = \sum_{n|d} f(d) \iff f(n) = \sum_{n|d} \mu(d) g(\frac{d}{n})$

默比乌斯反演

公式

- $g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) g(\frac{n}{d})$
- $g(n) = \sum_{n|d} f(d) \iff f(n) = \sum_{n|d} \mu(d) g(\frac{d}{n})$

证明

- $\sum_{d|n} \mu(d) g(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{x|\frac{n}{d}} f(x) = \sum_{x|n} f(x) \sum_{d|\frac{n}{x}} \mu(d) = \sum_{x|n} f(x) [\frac{n}{x} = 1] = f(n)$
- 第二个式子同理.

BZOJ 2301

- T 次询问, 给出 n, m, k, 求 $1 \le a \le n, 1 \le b \le m$ 中有多少对 (a, b) 满足 $gcd(a, b) = k$.
- $T, n, n \le 5 \times 10^4$.

Solution

$$
\begin{aligned}
\sum_{i=1}^{n}\sum_{j=1}^{m}[gcd(i,j)=k] &= \sum_{i=1}^{\lfloor\frac{n}{k}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{k}\rfloor}[gcd(i,j)=1] \\
&= \sum_{i=1}^{\lfloor\frac{n}{k}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{k}\rfloor}\sum_{d|gcd(i,j)}\mu(d) \\
&= \sum_{d=1}^{min(\lfloor\frac{n}{k}\rfloor,\lfloor\frac{m}{k}\rfloor)}\mu(d)\sum_{d|i,i\le n}\sum_{d|j,j\le m}1 \\
&= \sum_{d=1}^{min(\lfloor\frac{n}{k}\rfloor,\lfloor\frac{m}{k}\rfloor)}\mu(d)\times\lfloor\frac{n}{kd}\rfloor\times\lfloor\frac{m}{kd}\rfloor
\end{aligned}
$$

- $\lfloor\frac{n}{d}\rfloor$ 至多只有 $2\sqrt{n}$ 个取值，所以预处理出 $\mu(d)$ ，然后每次询问可以 $O(\sqrt{n})$ 回答.

定义及性质

定义

- $\varphi(n)$ 为不超过 n 且与 n 互质的数的个数.
- 当 $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ 时.
- $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1) = n \times \prod_{i=1}^{k}(1 - \frac{1}{p_i})$

定义及性质

定义

- $\varphi(n)$ 为不超过 n 且与 n 互质的数的个数.
- 当 $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ 时.
- $\varphi(n) = \prod_{i=1}^{k} p_i^{a_i-1}(p_i - 1) = n \times \prod_{i=1}^{k}(1 - \frac{1}{p_i})$

性质

- $\varphi(n)$ 为积性函数.
- $\sum_{d|n} \varphi(n) = n$
- 1 到 n 中与 n 互质的数的和为 $n \times \frac{\varphi(n)}{2}(n > 1)$.

DZY Loves Math V [BZOJ 3560]

- 求 $\sum_{i_1|a_1}\sum_{i_2|a_2}\cdots\sum_{i_n|a_n}\varphi(i_1 i_2\cdots i_n)$.
- $1\le n\le 10^5, 1\le a_i\le 10^7$.

Solution

- 显然对于每个质数可以独立计算然后再乘起来.
- $\varphi(p^e) = p^e \times \frac{p-1}{p}(e > 0)$.
- $\sum_{i|p^e} \varphi(i) = \frac{p-1}{p} \times ((\sum_{i=0}^{e} p^i) - 1) + 1$.
- 对于素数 p, 它对答案的贡献为 $(\prod_{i=1}^{n} \frac{p^{e_i+1}-1}{p-1} - 1) \times \frac{p-1}{p} + 1$.

逆元

定义

- 对于两个整数 a, M, 如果存在一个 $0 < x < M$ 使得 $a \cdot x \equiv 1 \pmod{M}$, 我们称 x 为 a 在模 M 意义下的逆元.

性质

- 如果 $gcd(a, M) \neq 1$, 那么不存在 a 在模 M 意义下的逆元.
- 如果 a 存在逆元, 那么逆元唯一.

求逆元

线性求逆元

- 设 $inv[i]$ 为 i 的逆元，$M = k \cdot i + r, r < i, 1 < i$.
- $k \cdot i + r \equiv 0 \pmod{M} \Rightarrow k \cdot inv[i] + inv[r] \equiv 0 \pmod{M}$.
- $inv[i] \equiv -k \cdot inv[r] \pmod{M} \Rightarrow inv[i] \equiv -\lfloor \frac{M}{i} \rfloor \cdot inv[M\%i]$.

欧拉定理

- 如果 $gcd(a, M) = 1$, $a^{\varphi}(M) \equiv 1 \pmod{M} \Rightarrow a \cdot a^{\varphi(M)-1} \equiv 1 \pmod{M}$.
- 即 a 的逆元为 $a^{\varphi(M)-1}$.

拓展欧几里得求算法逆元

- 求出 $a \cdot x - M \cdot y = 1$ 的一组解.
- 用拓展欧几里得算法即可.

离散对数

问题

- 给出 a, b, M, 求出一个 $0 < x < M$, 使得 $a^x \equiv b \pmod{M}$.
- 这里只考虑 M 为质数的情况.

Shank's Baby-Step-Giant-Step

- 预处理 $a^0, a^1, a^2 \cdots, a^{\sqrt{M}}$ 的值.
- 设 $x = k \cdot \sqrt{M} + r$.
- 枚举 k , 然后找是否存在一个 r 满足 $a^r \equiv b \cdot a^{-k \cdot \sqrt{M}} \pmod{M}$.
- 用 map 或者哈希表实现, 复杂度 $O(\sqrt{M} \log M)$ 或 $O(\sqrt{M})$.

杜教筛

- 求 $\sum_{i=1}^{n} \mu(i)$ 和 $\sum_{i=1}^{n} \varphi(i)$.
- $1 \le N \le 10^{10}$.

Solution

- 讲怎么求 $S(n)=\sum_{i=1}^{n}\mu(i)$, $\varphi(n)$ 的前缀和同理.

Solution

- 讲怎么求 $S(n) = \sum_{i=1}^{n} \mu(i)$, $\varphi(n)$ 的前缀和同理.
- 我们有 $\sum_{d|i} \mu(d) = [i = 1] \Rightarrow \sum_{i=1}^{n} \sum_{d|i} \mu(d) = 1$.

Solution

- 讲怎么求 $S(n)=\sum_{i=1}^{n}\mu(i)$, $\varphi(n)$ 的前缀和同理.
- 我们有 $\sum_{d|i}\mu(d)=[i=1]\Rightarrow\sum_{i=1}^{n}\sum_{d|i}\mu(d)=1$.

$$
\begin{aligned}
S(n) &= \sum_{i=1}^{n}\sum_{d|i}\mu(d)-\sum_{i=1}^{n}\sum_{d|i,d\neq i}\mu(d) \\
&= 1-\sum_{i=1}^{n}\sum_{d|i,d\neq 1}\mu(\frac{i}{d}) \\
&= 1-\sum_{d=1}^{n}\sum_{i=1}^{\lfloor\frac{n}{d}\rfloor}\mu(i) \\
&= 1-\sum_{d=1}^{n}S(\lfloor\frac{n}{d}\rfloor)
\end{aligned}
$$

- $\varphi(n)$ 的前缀和只要用 $\sum_{d|i}\varphi(d)=i$ 就可以了.

复杂度

- 一共只会访问 $O(\sqrt{N})$ 个状态, 因为 $\lfloor \frac{N}{k} \rfloor$ 只有 $O(\sqrt{N})$ 个取值.
- 状态 $S(x)$ 的转移复杂度为 $O(\sqrt{x})$.

复杂度

- 一共只会访问 $O(\sqrt{N})$ 个状态，因为 $\lfloor \frac{N}{k} \rfloor$ 只有 $O(\sqrt{N})$ 个取值.
- 状态 $S(x)$ 的转移复杂度为 $O(\sqrt{x})$.
- 转移总数为 $\sum_{i=1}^{\sqrt{N}} \sqrt{i} + \sum_{i=1}^{\sqrt{N}} \sqrt{\lfloor \frac{N}{i} \rfloor}$.
- 后半部分显然大于前半部分，可以忽略前半部分.
- 用积分近似可以求出复杂度为 $O(N^{\frac{3}{4}})$.

复杂度

- 一共只会访问 $O(\sqrt{N})$ 个状态，因为 $\lfloor \frac{N}{k} \rfloor$ 只有 $O(\sqrt{N})$ 个取值.
- 状态 $S(x)$ 的转移复杂度为 $O(\sqrt{x})$.
- 转移总数为 $\sum_{i=1}^{\sqrt{N}} \sqrt{i} + \sum_{i=1}^{\sqrt{N}} \sqrt{\lfloor \frac{N}{i} \rfloor}$.
- 后半部分显然大于前半部分，可以忽略前半部分.
- 用积分近似可以求出复杂度为 $O(N^{\frac{3}{4}})$.
- 如果可以将 $N \leq K$ 的预处理出来，那么复杂度转移数就是 $\sum_{i=1}^{\lfloor \frac{N}{K} \rfloor} \sqrt{\lfloor \frac{N}{i} \rfloor}$.
- 如果预处理复杂度为 $O(K)$，那么取 $K = N^{\frac{2}{3}}$ 时，就能够将复杂度降至 $O(N^{\frac{2}{3}})$.
- 这种优化复杂度的思想很多时候都能用.

题目

Project Euler 439

- 求 $S(n) = \sum_{i=1}^{n} \sum_{j=1}^{n} \sigma(i \cdot j)$ 模 $10^9 + 7$.
- $n \leq 10^{10}$.

Solution

从 $\sigma(i \times j)$ 入手, $\sigma(i \times j) = \sum_{x|i} \sum_{y|j} x \cdot \frac{j}{y}[gcd(x, y) = 1]$.

Solution

从 $\sigma(i \times j)$ 入手，$\sigma(i \times j) = \sum_{x|i} \sum_{y|j} x \cdot \frac{j}{y}[gcd(x,y)=1]$.

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{n}\sum_{x|i}\sum_{y|j} x \cdot \frac{j}{y}[gcd(x,y)=1] &= \sum_{x=1}^{n}\sum_{y=1}^{n}[gcd(x,y)=1]\lfloor\frac{n}{x}\rfloor S(\lfloor\frac{n}{y}\rfloor) \\ &= \sum_{x=1}^{n}\sum_{y=1}^{n}\sum_{d|gcd(x,y)}\mu(d)\lfloor\frac{n}{x}\rfloor S(\lfloor\frac{n}{y}\rfloor) \\ &= \sum_{d=1}^{n}\mu(d)\sum_{x=1}^{\lfloor\frac{n}{d}\rfloor}\lfloor\frac{n}{d \cdot x}\rfloor\sum_{y=1}^{\lfloor\frac{n}{d}\rfloor}S(\lfloor\frac{n}{d \cdot y}\rfloor)\end{aligned}$$

- $S(m)$ 等于 $\frac{(m+1)\cdot m}{2}$.

Solution

从 $\sigma(i \times j)$ 入手, $\sigma(i \times j) = \sum_{x|i} \sum_{y|j} x \cdot \frac{j}{y} [gcd(x, y) = 1]$.

$$\begin{aligned} \sum_{i=1}^{n} \sum_{j=1}^{n} \sum_{x|i} \sum_{y|j} x \cdot \frac{j}{y} [gcd(x, y) = 1] &= \sum_{x=1}^{n} \sum_{y=1}^{n} [gcd(x, y) = 1] \lfloor \frac{n}{x} \rfloor S(\lfloor \frac{n}{y} \rfloor) \\ &= \sum_{x=1}^{n} \sum_{y=1}^{n} \sum_{d|gcd(x,y)} \mu(d) \lfloor \frac{n}{x} \rfloor S(\lfloor \frac{n}{y} \rfloor) \\ &= \sum_{d=1}^{n} \mu(d) \sum_{x=1}^{\lfloor \frac{n}{d} \rfloor} \lfloor \frac{n}{d \cdot x} \rfloor \sum_{y=1}^{\lfloor \frac{n}{d} \rfloor} S(\lfloor \frac{n}{d \cdot y} \rfloor) \end{aligned}$$

- $S(m)$ 等于 $\frac{(m+1) \cdot m}{2}$.
- 对于 $\sum_{i=1}^{m} \lfloor \frac{m}{i} \rfloor$, 可以预处理 m 不超过 $n^{\frac{2}{3}}$ 的和, 然后大于 $n^{\frac{2}{3}}$ 的 $O(\sqrt{m})$ 计算.
- $\sum_{i=1}^{m} S(\lfloor \frac{m}{i} \rfloor)$ 同理.
- $\mu(n)$ 的前缀和用杜教筛.
- 总复杂度为 $O(n^{\frac{2}{3}})$

题目

BZOJ 3884

T 组数据, 每次给出 P, 求 $2^{2^{2^{\cdots}}}$ 对 P 取模后的值.

Solution

扩展欧拉定理

- 如果 $gcd(a, M) \neq 1$, 那么 $a^b \equiv a^{b\%\varphi(M)+\varphi(M)} \pmod M (b > \varphi(M))$.

做法

- 设 $f = 2^{2^{2^{\cdots}}}$, 则 $f \equiv 2^{f\%\varphi(M)+\varphi(M)} \pmod M$.
- 递归处理, 如果 M 为奇数 $\varphi(M)$ 则为偶数, 否则 $\varphi(M) \leq \frac{M}{2}$, 最多递归 log 层.