筛法

Min25 筛

求积性函数 f 的前缀和。

思想：找到**完全积性函数** g，使得 f, g 在质数处的取值一样，且 g 的前缀和很好算。于是：

1. 筛出所有 $G([n/i])$ 表示小于等于 $[n/i]$ 的质数对应的 g 的和。
2. 用这些值暴力搜索出 $F(n)$ 的值。

Min25 筛第一部分的复杂度被证明为 $O(\frac{n^{3/4}}{\log n})$，第二部分复杂度为 $O(n^{1-\epsilon})$，但是实际应用中很快。

第一部分

考虑不断地把某个质数筛掉，记 $f(i,j)$ 表示筛掉了前 i 个质数，剩下所有 $\leq j$ 的数字对应 g 的和。则有：

$$f(i,j)=f(i-1,j)-g(p_i)\left(f\left(i-1,\left\lfloor\frac{j}{p_i}\right\rfloor\right)-\sum_{k=1}^{i-1}g(p_j)\right)$$

注意到 i 最大级别为 $O(\frac{\sqrt{n}}{\log n})$，而 j 只需要存 $O(\sqrt{n})$ 个数值，并且转移过程只需要考虑 $j\geq p_i^2$ 的情况即可。因此总复杂度约为：

$$\frac{1}{\ln n}\left(\int_0^{\sqrt[4]{n}}2\sqrt{n}-x^2dx+\int_{\sqrt[4]{n}}^{\sqrt{n}}\frac{n}{x^2}dx\right)=O(\frac{n^{3/4}}{\log n})$$

第二部分

考虑如何算前缀和。质数的答案已经求出，我们只需枚举合数的最小质因子，及其次数。为了保证每次筛掉最小质因子，记 $F(i,j)$ 表示所有最小质因子大于等于 p_i 的数字 f 之和：

$$F(i,j)=G(j)-\sum_{k=1}^{i-1}f(p_k)+\sum_{p_i^2\le n}\sum_{p_k^{e+1}\le n}f(p_k^e)F(k+1,\frac{j}{p_k^e})+f(p_k^{e+1})$$

直接暴力 dfs 即可。最终答案即为 $F(1,n)$。

例题

求莫比乌斯函数、欧拉函数的前缀和。

LOJ6053 简单的函数

定义 $f(1)=1, f(p^c)=p \operatorname{xor} c$，且 f 是积性函数。求其前缀和。

Powerful Numbers

n 被称为 Powerful Numbers，当且仅当 n 的每个质因子次数都 ≥ 2。

$\leq n$ 的 Powerful Numbers 总共有 $O(\sqrt{n})$ 个。

PN 筛

构造一个容易求前缀和的函数 g，且 g, f 在质数处的取值一样。然后构造函数 $h = f/g$，这里 $/$ 表示迪利克雷除法（迪利克雷卷积的逆运算），即构造 $g * h = f$。

考虑 $f(p) = g(1)h(p) + h(1)g(p) = g(p) \Rightarrow h(p) = 0$，因此 h 只在 Powerful Numbers 处有值。因而显然可以 $O(\sqrt{n})$ 计算 f 的前缀和，只需算出 $h(p^c)$ 即可。

群论

代数系统

代数系统 S 是个定义了乘法运算（$*$）的集合，满足封闭性。

例如 $(N, +), (R, *)$ 都是代数系统。

半群

乘法运算（$*$）存在结合律的代数系统称为半群。

幺半群（幺群）

单位元： 若半群 G 中存在 e 使得 $\forall g \in G, eg = ge = e$，则 e 称为单位元。

存在单位元的**半群**称为幺半群或者幺群。

定理： 幺群中单位元唯一。

证明： 若存在两个单位元 e_1, e_2，则 $e_1 = e_1 e_2 = e_2$。

幺半群（幺群）

左逆和右逆： 对于 x，若存在 y 使得 $xy=1$，则 x 称为 y 的左逆，y 称为 x 的右逆。

逆元： 对于 x，若存在 y 使得 $xy=yx=1$，称 y 为 x 的逆元。

定理： 幺群中，若一个元素同时存在左逆和右逆，则其存在逆元。

证明： 不妨假设 $zx=xy=1$，则 $y=(zx)y=z(xy)=z$。

定理： 幺群中，若 x 存在逆元，则逆元唯一。证明同上。

群

若幺群中每个元素均存在逆元，则称为群。

阿贝尔群

若群中乘法满足交换律，则称为阿贝尔群。

循环群

若群 G 中存在一个元素 g，使得 $G=\{g^0,g^1,\cdots,g^k\}$，则 G 称为**循环群**，g 称为 G 的**生成元**。不难发现循环群一定是阿贝尔群。

定义： G 是有限群，设 $g\in G$，k 为最小的正整数使得 $g^k=1$，k 称为 g 的**阶**。因而 G 循环群当且仅当存在阶为 $|G|$ 的元素。

环

环是定义了两个运算 $+,*$ 的集合 S，满足 $(S,+)$ 是阿贝尔群，且乘法关于加法具有分配律，乘法具有结合律。

域

域是定义了两个运算 $+,*$ 的集合 S，满足 $(S,+)$ 和 $(S\setminus 0,*)$ 都是阿贝尔群，其中 0 是 $(S,+)$ 的单位元。

子群

设 G 为群，$S \subseteq G$，若 $x, y \in S$ 都有 $xy^{-1} \in S$，则称 S 为 G 的子群，记为 $S \leq G$。

置换群

设 A 是个非空集合，G 中每个元素 f 都是个 A 到 A 的**双射**。则 G 称为 A 上的置换群。

不妨设 $|A| = n$，S_n 表示**所有** A 到 A 双射构成的群（显然是群），则称 S_n 为 n 阶对称群（Symmetric Group）。显然所有 n 阶置换群都是 S_n 的子群。

群的陪集分解

陪集：对于群 G 和其子群 H，对任意 $a \in G$，定义 $aH = \{a * h | h \in H\}$ 为 H 的一个左陪集，$Ha = \{h * a | h \in H\}$ 为 H 的一个右陪集，且显然陪集大小均和 H 相同。

引理： $\forall a_1, a_2 \in G$，a_1H 和 a_2H 要么不交，要么相等。

定理（陪集分解定理）： 设 G 是有限群，则存在正整数 k，使得 $G = a_1H \cup a_2H \cup \cdots \cup a_kH$，且这 k 个陪集两两不交。

推论（Language 定理）： 任意有限群的子群大小一定是其大小的因数。

推论： 任意元素的阶一定是群大小的因数。因而若群大小是质数，则一定是循环群。

正规子群

设 H 为 G 的子群，若对于任意 $g \in G, h \in H$ 都存在 $h' \in H$ 使得 $gh = h'g$，则 H 称为 G 的**正规子群**，记为 $H \trianglelefteq G$。

等价定义 1：若 H 所有左陪集与右陪集相等，即 $aH = Ha$，则 H 是正规子群。

等价定义 2：若 $\forall g \in G, h \in H, ghg^{-1} \in H$（即 $gHg^{-1} = H$），则 H 是正规子群。

商群

设左陪集构成的集合为 $L=\{a_1H,\cdots,a_kH\}$，定义 L 上的乘法为 $a_1H*a_2H=(a_1*a_2)H$，单位元 $1H$，则 L 似乎可以成为一个群。

定理： 群 $(L,*)$ 良定义当且仅当 H 是正规子群。

证明： 充分性：若 H 是正规子群，则 $\forall h_1,h_2\in H$ 都有 $a_1h_1H*a_2h_2H=(a_1h_1a_2h_2)H=(a_1a_2h_1'h_2)H=(a_1a_2)H$。因此显然良定义。

必要性：$\forall g\in G,h_1,h_2\in H$，我们需要让 $(gh_1g^{-1}h_2)H=gh_1H*g^{-1}h_2H=gH*g^{-1}H=H$。因此必然有 $gh_1g^{-1}\in H$，这正是正规子群的定义。

定义： 若 $H\trianglelefteq G$，则 G/H 记为上述方法定义出来的群，即 G 除以 H 的商群。显然 $|H||G/H|=|G|$。

同态和同构

对于群 G, H，若存在映射 $f: G \to H$ 使得 $\forall g_1, g_2 \in G, f(g_1 g_2) = f(g_1)f(g_2)$，则称 G 和 H 同态（Homomorphic），f 称为 G 到 H 的同态映射（Homomorphism）。

此外，记 $\ker f$ 为 $\{f(g) = 1_H | g \in G\}$，这显然是一个群。

若 f 是双射，则称 G, H 同构（Isomorphic），称 f 为 G 和 H 的同构映射（Isomorphism），并且记为 $G \cong H$。

群的直积

两个群的直积定义为 $H = G_1 \times G_2 = \{(g_1, g_2) | g_1 \in G_1, g_2 \in G_2\}$，乘法定义为 $(g_1, g_2) * (g_1', g_2') = (g_1 *_{G_1} g_1', g_2 *_{G_2} g_2')$。

显然的，$|H| = |G_1||G_2|$，并且 $G_1' = \{(g_1, 1_{G_2}) | g_1 \in G_1\}$ 和 $G_2' = \{(1_{G_1}, g_2) | g_2 \in G_2\}$ 都是 H 的正规子群。

同构基本定理

设 $f: G \to H$ 为一个**同态满射**，则 $\ker f$ 是正规子群且 $\dfrac{G}{\ker f} \cong H$。

证明： 正规子群显然。令 $\varphi: \dfrac{G}{\ker f} \to H$ 定义为 $\varphi(g \ker f) = f(g)$，由 $\forall x \in \ker f, \varphi(gx \ker f) = f(gx) = f(g)$ 可知 φ 良定义。

同时 $\varphi(g_1 \ker f * g_2 \ker f) = \varphi(g_1 g_2 \ker f) = f(g_1 g_2) = f(g_1) f(g_2) = \varphi(g_1 \ker f) \varphi(g_2 \ker f)$，因此 φ 是同构映射。Q.E.D.

推论： 令 $H = G_1 \times G_2$，则 $H/G_1 \cong G_2$ 且 $H/G_2 \cong G_1$。

轨道-稳定集定理

设一个非空集合 S 以及它的一个置换群 G，定义：
$F_u = \{f(u)|f \in G\}$（u 的轨道），$P_u = \{f|f(u) = u\}$（u 的稳定集）
则有 $|F_u||P_u| = |G|$（轨道-稳定集定理）

证明： 考虑 G 在子群 P_u 下的陪集分解，显然每个陪集对应了轨道中唯一的元素。

推论（Burnside 引理）： 对于置换群 G 和作用集合 S，S 不同的轨道数等于每个置换不动点个数的平均值，即

$$\frac{1}{|G|}\sum_{g\in G}\sum_{s\in S}[g(s) = s]$$

证明： 每个轨道中的元素贡献 $1/$ 轨道大小，根据轨道-稳定集定理显然。

阿贝尔群

定理： 阿贝尔群的任意子群都是正规子群。

定理： 阿贝尔群的商群也是阿贝尔群。

定理（阿贝尔群基本定理）： 对于任意阿贝尔群 A，它一定能够唯一写成

$$A \cong \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_k} \times \mathbb{Z}^r$$

的形式，其中 $a_1 | a_2 | \cdots | a_k, a_1 > 1$，且若 A 是有限群，则 $r = 0$。

例题 1:

给定 n，求 n 阶阿贝尔群的个数。

由于 n 可能很大，会以质因数分解的形式给出，即给出

$$n = \sum_{i=1}^{m} p_i^{q_i}$$

$1 \le m \le 10^6$

定理： 若 $p \perp q$，则 $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$。

证明： 只需要证明 $\mathbb{Z}_p \times \mathbb{Z}_q$ 是循环群即可。显然 $(1,1)$ 是生成元。

推论： 有限阿贝尔群一定可以唯一写成如下形式：

$$\begin{gathered}\mathbb{Z}_{p_1^{a_{1,1}}} \times \mathbb{Z}_{p_1^{a_{1,2}}} \times \cdots \\ \times \mathbb{Z}_{p_2^{a_{2,1}}} \times \mathbb{Z}_{p_2^{a_{2,2}}} \times \cdots\end{gathered}$$

其中 $p_1, p_2, \cdots$ 为质数。

Lagrange 定理

域 F 上的任意 n 次多项式在 F 内至多有 n 个根。

推论： 域 F 的阿贝尔乘法群 $F^\times$ 的任意有限子群都是循环群。

证明： 设任意一个有限子群为 G，根据阿贝尔群基本定理可以将 G 做分解：

$$G \cong \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_k}$$

则 G 是循环群当且仅当 $k = 1$。若 $k > 1$，不妨设右侧 $(0, 0, \cdots, 0, 1)$ 对应的左侧元素为 g，则显然 $g^{a_1} = g^{a_2} = \cdots = g^{a_k} = 1_F$。因此多项式 $x^{a_k} - 1_F = 0_F$ 在域 F 上有至少 $a_1 a_2 \cdots a_k > a_k$ 个根，矛盾。

$\mathbb{Z}$ 上的乘法群

令 $\mathbb{Z}_n^*$ 为 $\bmod n$ 意义下的乘法群，显然 $|\mathbb{Z}_n^*| = \varphi(n)$。

定理（欧拉定理）： 若 $n \perp m$，则 $m^{\varphi(n)} \equiv 1 \pmod n$。

定理： 若 $p \perp q$，则 $\mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$。

证明： 定义映射 $f : \mathbb{Z}_{pq}^* \to \mathbb{Z}_p^* \times \mathbb{Z}_q^*$ 为 $f(i) = (i \bmod p, i \bmod q)$。由 CRT 可知这是双射。同时，$f$ 显然还是同态（即 $f(ij) = f(i)f(j)$），因而 f 是同构映射。

定理： $\mathbb{Z}_p^*$ 是循环群，其中 p 为质数。即，任意质数 p 存在原根。

定理： $\mathbb{Z}_{p^n}^* \cong \mathbb{Z}_{(p-1)p^{n-1}}$，其中 p 是奇质数。

设 p 的原根为 g，设 g 在 $\mathbb{Z}_{p^n}^*$ 中的阶为 d，则必然有 $p-1|d$，因此 $\mathbb{Z}_{p^n}^*$ 存在子群 $\mathbb{Z}_{p-1}$。同时，考察元素 $1+p$，我们有：

$$(1+p)^{p^{n-1}} \equiv \sum_{i=0}^{p^{n-1}} \binom{p^{n-1}}{i} p^i \equiv 1 \pmod{p^n}$$

这是因为 $i!$ 中 p 因子的个数一定小于 i： $i(p^{-1}+p^{-2}+\cdots) < i/(p-1) \leq i/2 < i$，以及

$$(1+p)^{p^{n-2}} \equiv \sum_{i=0}^{p^{n-2}} \binom{p^{n-2}}{i} p^i \equiv 1+p^{n-1} \pmod{p^n}$$

这是因为 $i>1$ 时 $i!$ 中 p 因子的个数一定小于 $i-1$： $i(p^{-1}+p^{-2}+\cdots) < i/2 \leq i-1$。因此 $1+p$ 的阶为 p^{n-1}，即 $Z_{p^n}^*$ 存在子群 $Z_{p^{a-1}}$。

综上，根据基本定理，一定有 $\mathbb{Z}_{p^n}^* \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{n-1}} \cong \mathbb{Z}_{(p-1)p^{n-1}}$。

推论： $\mathbb{Z}_{p^n}^*$ 是循环群，即 p^n 存在原根。

推论： $\mathbb{Z}_{2p^n}^*$ 是循环群，即 $2p^n$ 存在原根。

证明： 由之前定理，显然 $\mathbb{Z}_{2p^n}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_{p^n} \cong \mathbb{Z}_{p^n}$。

推论（原根存在性定理）： 正整数中仅 $1, 2, 4, p^a, 2p^a$ 具有原根。

证明： 充分性已经证明，接下来证明必要性，取 m 为 $1, 2, 4, p^a, 2p^a$ 以外的数。

若 $m = 2^n(n \geq 3)$，则考虑

$$(2k+1)^{2^{n-2}} \equiv \sum_{i=0}^{2^{n-2}} \binom{2^{n-2}}{i} 2^i k^i \equiv 1 + 2^{n-2}(2k) + \binom{2^{n-2}}{2}(2k)^2 \equiv 1 \pmod{2^n}$$

因此 m 一定不存在原根。

对于其他情况，m 一定可以写成 pq 的形式且满足 $p \perp q, \varphi(p), \varphi(q)$ 均为偶数。

由于 $\mathbb{Z}_m^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$，因此 $\forall g \in \mathbb{Z}_m$，考虑其对应元素 (a_1, a_2)，则 a_1 的阶至多为 $\varphi(p)$，a_2 的阶至多为 $\varphi(q)$。因此 m 的阶至多为

$$\operatorname{lcm}(\varphi(p), \varphi(q)) \leq \frac{1}{2}\varphi(m)$$

因而原根不可能存在。

威尔逊定理

1. 若 p 为质数，则 $(p-1)! \equiv -1 \pmod p$
2. 若 p 为质数，则 $(p^q)!_p \equiv -1 \pmod p$，其中 $(n!)_m$ 表示所有小于等于 n 且与 m 互质的正整数的乘积。

证明： 若 n 的原根存在（设为 g），则 $(n!)_n \equiv g^{\frac{\varphi(n)(\varphi(n)-1)}{2}} \pmod n$。因此若 $\varphi(n)$ 是偶数，则乘积为 -1，否则乘积为 1。而有原根的数字 φ 均为偶数，因此乘积均为 -1。

例题 2（HDU 2973）

求:

$$S_n = \sum_{k=1}^{n} \left[\frac{(3k+6)!+1}{3k+7} - \left[\frac{(3k+6)!}{3k+7} \right] \right]$$

$n \le 10^6$