数论选讲

于孟宏

2024 年 7 月 25 日

山东省烟台第二中学

目录

数论入门

欧几里得算法

有以下性质:

- $\gcd(kn, km) = k\gcd(n, m)$ 以及 $lcm(kn, km) = k\ lcm(n, m)$
- 若 $a \perp b$, 则 $\gcd(a^m - b^m, a^n - b^n) = a^{\gcd(n,m)} - b^{\gcd(n,m)}$
- 如果 $n^a \equiv 1 \pmod m$ 且 $n^b \equiv 1 \pmod m$, 则 $n^{\gcd(a,b)} \equiv 1 \pmod m$

第二条的证明:

$\gcd(a^m - b^m, a^n - b^n) = \gcd(a^m - b^{m-n}a^n, a^n - b^n) = \gcd(a^n(a^{m-n} - b^{m-n}), a^n - b^n)$

第三条的证明:

$$\begin{aligned} n^a &\equiv 1 \pmod m \\ 0 \equiv n^a - n^{a-b}n^b &\equiv 1 - n^{a-b} \pmod m \\ n^{a-b} &\equiv 1 \pmod m \end{aligned}$$

[CF1656H]Equal LCM Subsets

有两个集合 A, B, 大小分别为 n, m, 你需要找两个非空子集 $S_A \subseteq A, S_B \subseteq B$, 使得 S_A 中元素的 lcm 和 S_B 中元素的 lcm 相等, 或判断无解.$n, m \leq 1000$, 值域为 4×10^{36}.

[CF1656H]Equal LCM Subsets

有两个集合 A, B, 大小分别为 n, m, 你需要找两个非空子集 $S_A \subseteq A, S_B \subseteq B$, 使得 S_A 中元素的 lcm 和 S_B 中元素的 lcm 相等, 或判断无解.$n, m \le 1000$, 值域为 4×10^{36}.

注意到插入可能有点小困难, 我们考虑从全集中删除: 注意到如果对于一个数字的某一个质因子, 如果它的指数大于了对方集合中相同质因子的最大指数, 那这个数一定不可能存在, 直接删掉. 不难发现删完后就是合法的了.

但是数据范围不允许我们判断质因子, 那么怎么做呢?

[CF1656H]Equal LCM Subsets

有两个集合 A, B, 大小分别为 n, m, 你需要找两个非空子集 $S_A \subseteq A, S_B \subseteq B$, 使得 S_A 中元素的 lcm 和 S_B 中元素的 lcm 相等, 或判断无解.$n, m \le 1000$, 值域为 4×10^{36}.

注意到插入可能有点小困难, 我们考虑从全集中删除: 注意到如果对于一个数字的某一个质因子, 如果它的指数大于了对方集合中相同质因子的最大指数, 那这个数一定不可能存在, 直接删掉. 不难发现删完后就是合法的了.

但是数据范围不允许我们判断质因子, 那么怎么做呢? 显然合法的条件等价于 $a_i | lcm(b), \forall 1 \le i \le n$(当然这个还要反过来再写一遍, 两个式子一起才是充要条件, 这里为了方便只写一个), 这个条件等价于 $\gcd_{j=1}^{n}(\frac{a_i}{\gcd(b_j, a_i)}) = 1$. 后者是方便做的.

然后上线段树处理一下, 好像先 random shuffle 一下再暴力删除也是对的.

基于值域预处理的快速 GCD

$O(n)$ 预处理,$O(1)$ 求任意两个小于等于 n 的数的 gcd.

引理: 对于任意整数 n, 存在一种划分方式 $n = abc$,a,b,c 三个数要么是质数, 要么 $\leq \sqrt{n}$.

证明:

如果 n 存在一个大于等于 $\sqrt{n}$ 的质因子, 显然成立.

否则, 使用数学归纳, 我们考虑 n 的最小质因子为 p, 设 $\frac{n}{p} = xyz$, 不妨设 $x \leq y \leq z$. 如果 $x = 1$, 显然成立. 不然有 $p \leq x \leq y \leq z$, 而 $pxyz = n$, 那么 $p^4 \leq n$,$p \leq n^{\frac{1}{4}}$. 现在我们想要证明不存在 $xp > \sqrt{n}$,$yp > \sqrt{n}$,$zp > \sqrt{n}$. 如果存在, 我们有:$xyzp^3 > n^{\frac{3}{2}}$

与我们前面的结论不符合. 因而引理成立.

基于值域预处理的快速 GCD

接下来，设 $m=\sqrt{n}$, 考虑使用 $O(n)$ 的时间求出每个小于等于 m 的数对的 gcd, 如果我们要求 $\gcd(x,y)$, 设 $x=abc$, 显然 $\gcd(x,y)=\gcd(a,y)\times\gcd(b,\frac{y}{\gcd(a,y)})\times\gcd(c,\frac{y}{\gcd(ab,y)})$.

如果 a 是质数，只需要判断 a 是否整除 y.

否则 $\gcd(a,y)=\gcd(y \mod a, a)$, 因为 $a\le\sqrt{n}$, 因而可以直接查表.

裴蜀定理

$\forall a, b, m \in \mathbb{Z}$, 则 $\exists x, y \in \mathbb{Z}$ 满足 $ax + by = m$, 当且仅当 $\gcd(a, b) | m$.

证明如下:

若 $a = 0$ 或 $b = 0$, 显然成立.

不然, 设集合 $A = \{xa + yb | x, y \in \mathbb{Z}\}$ 中的最小正元素 $d_0 = x_0 a + y_0 b$, 该集合中显然一定有正元素.

考虑取该集合中另一个正整数 $d_1 = x_1 a + y_1 b > d_0$, 注意到 $d_1 - d_0 = (x_1 - x_0)a + (y_1 - y_0)b \in A$, 所以 $\gcd(d_1, d_0) \in A$, 如果 $d_0 \nmid d_1$, 那么 $0 < \gcd(d_1, d_0) < d_0$, 与假设不符. 所以这个集合里的所有数一定都是 d_0 的倍数.

扩展欧几里得算法

考虑求方程 $ax + by = \gcd(a, b)$ 的一组解.

首先, 如果 $b = 0$, 那这组解显然就是 $\begin{cases} x = 1 \\ y = 0 \end{cases}$.

反之, 我们令 $c = a \mod b$, 考虑求方程 $cz + bw = \gcd(c, b)$ 的一组解.

接下来呢, 考虑带入 c, 则我们求出来的即方程

$(a - b\lfloor\frac{a}{b}\rfloor)z + bw = \gcd(a, b)$ 的一组解. 不难发现这也就是方程

$az + (w - \lfloor\frac{a}{b}\rfloor z)b = \gcd(a, b)$ 的一组解, 所以原本的方程的解也就是

$$\begin{cases} x = z \\ y = (w - \lfloor\frac{a}{b}\rfloor z) \end{cases}.$$

扩展欧几里得算法

另外, 这个算法也可以使用矩阵形式:

首先有 $\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} a \\ b \end{bmatrix}$, 令 $q = \lfloor \frac{a}{b} \rfloor$, 那么我们有

$$\begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \mod b \end{bmatrix}.$$

同样我们可以得到: $\begin{bmatrix} x_1 & y_1 \\ x_2 & y_2 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} \gcd(a,b) \\ 0 \end{bmatrix}$.

即 $ax_1 + by_1 = \gcd(a,b)$,(x_1, y_1) 就是一组特解.

vjudge Baekjoon-19523

$h \times w(h, w \leq 10^6)$ 的格子图, 只能往下往右走, 走到边界会循环, 问从 $(0, 0)$ 开始走遍历走一个哈密顿回路的方案数.

vjudge Baekjoon-19523

$h \times w(h, w \leq 10^6)$ 的格子图, 只能往下往右走, 走到边界会循环, 问从 $(0, 0)$ 开始走遍历走一个哈密顿回路的方案数.

这题最重要的地方其实在于观察到, 由于每个点只会被走到一次 (除了 $(0, 0)$, 它会被走到两次, 但只会由其它格子走来一次), 因此如果抽象成图, 每个格子只会有一个出边和一个入边. 这意味着每个格子上面的和左边的格子必定只有一个指向它, 进一步地, 这意味着这两个格子的状态必然相同.

vjudge Baekjoon-19523

$h\times w(h,w\le 10^6)$ 的格子图, 只能往下往右走, 走到边界会循环, 问从 $(0,0)$ 开始走遍历走一个哈密顿回路的方案数.

这题最重要的地方其实在于观察到, 由于每个点只会被走到一次 (除了 $(0,0)$, 它会被走到两次, 但只会由其它格子走来一次), 因此如果抽象成图, 每个格子只会有一个出边和一个入边. 这意味着每个格子上面的和左边的格子必定只有一个指向它, 进一步地, 这意味着这两个格子的状态必然相同.

由此我们发现, 每条副对角线 (取膜意义下) 的状态必然相同, 而取膜意义下的副对角线有多少条呢? 不难注意到是 $d=\frac{hw}{\text{lcm}(h,w)}=\gcd(h,w)$ 条. 也就是说, 我们只需要确定这 d 条对角线的值, 就可以确定整个矩阵的答案. 假设 R 表示向右走,D 表示向下走,a_i 表示第 i 条副对角线的状态, 最后的操作序列自然是 $a_0a_1\ldots a_{d-1}a_0a_1\ldots$.

vjudge Baekjoon-19523

那么我们接下来要做的就是给这 d 条副对角线定向, 并判断一个方案是否合法. 注意到一个方案不合法当且仅当出现了多于 1 个环. 意味着存在一个点, 它可以通过少于 hw 次走动走回自己. 另一件不难发现的事是, 第一个走回自己的点一定是 $(0,0)$. 并且走回自己的时候一定是经过了若干个周期:$a_0\,a_1 \ldots a_{d-1}\,a_0 \ldots a_{d-1}$, 因为每次向下或者向右走都会走到下一条副对角线, 而且最后要回到自己. 这就注意到每一个循环 $a_0\,a_1 \ldots a_{d-1}$ 内部具体什么情况是不在乎的, 只在乎经历过这个过程之后会发生什么样的变化.

vjudge Baekjoon-19523

那么我们接下来要做的就是给这 d 条副对角线定向, 并判断一个方案是否合法. 注意到一个方案不合法当且仅当出现了多于 1 个环. 意味着存在一个点, 它可以通过少于 hw 次走动走回自己. 另一件不难发现的事是, 第一个走回自己的点一定是 $(0,0)$. 并且走回自己的时候一定是经过了若干个周期:$a_0\,a_1\ldots a_{d-1}\,a_0\ldots a_{d-1}$, 因为每次向下或者向右走都会走到下一条副对角线, 而且最后要回到自己. 这就注意到每一个循环 $a_0\,a_1\ldots a_{d-1}$ 内部具体什么情况是不在乎的, 只在乎经历过这个过程之后会发生什么样的变化.

我们不妨假设序列 $\{a\}$ 中有 k 个 $R, d-k$ 个 D, 那会产生这种情况当且仅当 $\exists x \in \mathbb{N}_+, x < \frac{hw}{d}, \begin{cases} h \mid x(d-k) \\ w \mid xk \end{cases}$. 注意到这等价于寻找最小的 x, 判断其是否小于 $\frac{hw}{d}$, 于是条件等价于自然有 $x = lcm(\frac{h}{\gcd(d-k,h)}, \frac{w}{\gcd(w,k)})$, 枚举 k 并判断即可.

几个简单数论题

证明: 在 n 进制下, 若 $(11...1)_n$ 的 1 的个数不是质数则其一定不是质数.

几个简单数论题

证明: 在 n 进制下, 若 $(11...1)_n$ 的 1 的个数不是质数则其一定不是质数.

设 1 的个数为 m, 则 $(11...1)_n = \sum_{i=0}^{m-1} n^i$.

如果 $m \notin prime$, 不妨设 $m = cd, c, d \neq 1$.

$$\sum_{i=0}^{m-1} n^i$$

则

$$= \sum_{i=0}^{c-1} n^{di} \sum_{j=0}^{d-1} n^j$$

$$= (\sum_{i=0}^{c-1} n^{di})(\sum_{j=0}^{d-1} n^j)$$

显然不是质数.

几个简单数论题

定义费马数 $f_n = 2^{2^n} + 1.$

几个简单数论题

定义费马数 $f_n = 2^{2^n} + 1$.

求证: 如果 $m \neq n$, 则 $f_m \perp f_n$.

几个简单数论题

定义费马数 $f_n = 2^{2^n} + 1$.

求证: 如果 $m \neq n$, 则 $f_m \perp f_n$.

不难发现 $f_n = (f_{n-1} - 1)^2 + 1$.

不妨假设 $m < n$, 有:$\gcd(f_m, f_n) = \gcd(f_m, 2) = 1$.

求证: 若 $2^n + 1$ 是质数, 则 n 是 2 的整数幂.

几个简单数论题

定义费马数 $f_n = 2^{2^n} + 1$.

求证: 如果 $m \neq n$, 则 $f_m \perp f_n$.

不难发现 $f_n = (f_{n-1} - 1)^2 + 1$.

不妨假设 $m < n$, 有:$\gcd(f_m, f_n) = \gcd(f_m, 2) = 1$.

求证: 若 $2^n + 1$ 是质数, 则 n 是 2 的整数幂.

如果 $n = qm$ 且 q 是奇数, 我们
有:$2^n + 1 = (2^m + 1)(2^{n-m} - 2^{n-2m} + 2^{n-3m} \ldots - 2^m + 1)$.

同余

同余的基本性质

根据同余的定义, 若 $a, b, c, d, k \in \mathbb{Z}, n, m \in \mathbb{N}_+$, 我们有以下性质:

- $a \equiv b \pmod{m} \Leftrightarrow a - b = km.$
- $a \equiv b \pmod{m}$ 且 $c \equiv d \pmod{m} \Rightarrow a + c \equiv b + d \pmod{m}.$
- $a \equiv b \pmod{m}$ 且 $c \equiv d \pmod{m} \Rightarrow ac \equiv bd \pmod{m}.$
- $a \equiv b \pmod{m} \Rightarrow a^k \equiv b^k \pmod{m}.$
- $ad \equiv bd \pmod{m} \Leftrightarrow a \equiv b \pmod{m}, m \perp d.$
- $ad \equiv bd \pmod{md} \Leftrightarrow a \equiv b \pmod{m}, d \neq 0.$
- $ad \equiv bd \pmod{m} \Leftrightarrow a \equiv b \pmod{\frac{m}{\gcd(m, d)}}.$
- $a \equiv b \pmod{md} \Rightarrow a \equiv b \pmod{m}, d \neq 0.$
- $a \equiv b \pmod{m}$ 且 $a \equiv b \pmod{n} \Leftrightarrow a \equiv b \pmod{lcm(n, m)}.$

威尔逊定理

$$(p-1)! \equiv \begin{cases} -1(\mod p) & p \in prime \\ 2(\mod p) & p = 4 \\ 0(\mod p) & other \end{cases}$$

证明:

当 p 为质数时，考虑对于 a 和 $b = a^{-1}(\mod p)$, 若 $a = b$, 此时可证明 $a = 1$ 或 $a = p - 1$(需要用到下面独立剩余知识).

如果 $a \neq b$ 那么一定可以在 $[1, p-1]$ 找到一对数, 它们相乘为 1. 原因是若 $a_1 \neq a_2$, 那么 $a_1^{-1} \neq a_2^{-1}$.

若 p 不是质数, 则设 $p = ab$, 当 $a \neq b$ 时, 由于 $a, b \leq p$, 因此 $(p-1)!$ 一定是 p 的倍数.

若 $a = b$, 除非 $p = 4$, 不然一定能在 $[1, p-1]$ 里找到 a 和 $2a$, 此时 $(p-1)!$ 也是 p 的倍数.

费马小定理

$n^{p-1} \equiv 1(\mod p), n \perp p, p \in prime.$

我们有:

$\prod_{k=1}^{p-1} kn \equiv \prod_{k=1}^{p-1}(kn \mod p)(\mod p)$

$n^{p-1}(p-1)! \equiv (p-1)!(\mod p)$ 根据威尔逊定理, 显然可以推得费马小定理.

Miller-Rabin 算法

如果判断 n 是否是质数, 取 $a < n$, 设 $n - 1 = d \times 2^r$.

则要么 $a^d \equiv 1 \pmod n$.

要么 $\exists i$, 使得 $0 \le i < r, a^{d \times 2^i} \equiv -1 \pmod n$.

若一个都不满足, 则 n 一定不是质数, 不然可能是质数.

但是若取足够多的不同的 a(如果选 m 个), 那么 n 是质数的可能性更大.

此为 Miller-Rabin 算法, 复杂度 $O(m \times log_2 n)$. 不保证正确性.

其中 a 通常取质数, 原因不详.（事实上，如果 a 取前八个小质数，在 2^{64} 内是不会出错的）

中国剩余定理

对于方程组 $x \equiv a_i \pmod{m_i}$, 其中 m_i 两两互质, 求 x.

令 $m = \prod_{i=1}^{k} m_i$, 设 $M_i = \dfrac{m}{m_i}$,N_i 是 M_i 在 $\mod m_i$ 意义下逆元.

则 $x \equiv \sum_{i=1}^{k} M_i N_i a_i \pmod{m}$.

由于 x 在 $\mod m_i$ 意义下,$\sum$ 中枚举的所有不等于 i 的项都会成 0，等于 i 的项会成 a_i.

考虑每次合并两项，显然有:$a = a_1 + (a_2 - a_1) \times m_1 \times inv(m_1, m_2)$,$m = m_1 m_2$.

扩展中国剩余定理

对于方程组 $x \equiv a_i(\mod m_i)$, 若 m_i 两两不互质.

我们考虑每次合并两个方程:$\begin{cases} x \equiv a_1(\mod m_1) \\ x \equiv a_2(\mod m_2) \end{cases}$ 那这个方程组等价于:$\begin{cases} x = k_1 m_1 + a_1 \\ x = k_2 m_2 + a_2 \end{cases}$ 合并上下方程, 有:

$$k_1 m_1 + a_1 = k_2 m_2 + a_2$$
$$a_2 - a_1 = k_1 m_1 - k_2 m_2$$

设 $g = \gcd(m_1, m_2)$, 显然若 $g \nmid (a_2 - a_1)$, 方程无解.

扩展中国剩余定理

不然, 有:

$$\frac{a_2-a_1}{g}=k_1\frac{m_1}{g}-k_2\frac{m_2}{g}$$

$$k_1\frac{m_1}{g}=k_2\frac{m_2}{g}+\frac{a_2-a_1}{g}$$

$$k_1\frac{m_1}{g}\equiv\frac{a_2-a_1}{g}\pmod{\frac{m_2}{g}}$$

令 $inv(a,p)$ 表示 a 在 $\bmod p$ 意义下的逆元, 有:

$$k_1\equiv inv(\frac{m_1}{g},\frac{m_2}{g})\frac{a_2-a_1}{g}\pmod{\frac{m_2}{g}}$$

$$k_1=inv(\frac{m_1}{g},\frac{m_2}{g})\frac{a_2-a_1}{g}+k_3\frac{m_2}{g}$$

带回第一个方程:

$$x=m_1(inv(\frac{m_1}{g},\frac{m_2}{g})\frac{a_2-a_1}{g}+k_3\frac{m_2}{g})+a_1$$

$$x\equiv m_1 inv(\frac{m_1}{g},\frac{m_2}{g})\frac{a_2-a_1}{g}+a_1\pmod{\frac{m_1m_2}{g}}$$

[NOI2018] 屠龙勇士

扩展中国剩余定理的模板题.

欧拉函数

定义欧拉函数 $\varphi(m)$ 为所有满足 $1 \le n \le m, n \perp m$ 的 n 的个数.

令 $m = m_1 m_2$, 其中 $m_1 \perp m_2$. 由于若 $n \perp m_1, n \perp m_2$, 显然有 $(n \mod m_1) \perp m_1$ 且 $(n \mod m_2) \perp m_2$, 则根据中国剩余定理, 不难有 $\varphi(m) = \varphi(m_1)\varphi(m_2)$, 也即 $\varphi(x)$ 是积性函数.

若 $n = \prod_{i=1}^{k} p_i^{a_i}$, 则:

$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{a_i}) = \prod_{i=1}^{k} p_i^{a_i} - p_i^{a_i-1} = \prod_{i=1}^{k} p^{a_i-1}(p_i - 1)$.

考虑改变枚举方式, 因为 $n = \prod_{p|n} p^{a_p}$,

则:$\varphi(n) = \prod_{p|n} p^{a_p-1}(p-1) = \prod_{p|n} (p^{a_p} \times \dfrac{p-1}{p}) = n \times \prod_{p|n} \dfrac{p-1}{p}$.

欧拉定理

当 $a \perp m$ 时,$a^{\varphi(m)} \equiv 1 (\mod m)$.

证明考虑取出 $[1, m]$ 中所有和 m 互质的数, 设它们为 $b_1, b_2, \cdots, b_{\varphi(m)}$.
我们有:

$$\prod_{k=1}^{\varphi(m)} ab_k \equiv \prod_{k=1}^{\varphi(m)} (ab_k \bmod p) (\mod p)$$

$$a^{\varphi(m)} \prod_{k=1}^{\varphi(m)} b_k \equiv \prod_{k=1}^{\varphi(m)} b_k (\mod p)$$

欧拉定理可以用来求逆元:$a^{\varphi(p)} \equiv 1 (\mod p)$, 则有 $a^{-1} \equiv a^{\varphi(p)-1} (\mod p)$.

扩展欧拉定理

$$a^b \equiv a^c \pmod m, \text{其中 } c = \begin{cases} b \bmod \varphi(m) & a \perp m \\ b & b < \varphi(m) \\ (b \bmod \varphi(m)) + \varphi(m) & other \end{cases}$$

证明如下:

设 $m = \prod_{i=1}^{k} p_i^{e_i}$, 则要证 $a^b \equiv a^{(b \bmod \varphi(m))+\varphi(m)} \pmod m$, 即证 $\forall i$ 都有 $a^b \equiv a^{(b \bmod \varphi(m))+\varphi(m)} \pmod {p_i^{e_i}}$.

分情况讨论:

若 $p_i^{e_i} \perp a$, 则为普通欧拉定理情况, 即证明 $\varphi(p_i^{e_i})$ 是 $b-c$ 的因数. 由于 $\varphi(p_i^{e_i})$ 是 $\varphi(m)$ 的因数, 而 $\varphi(m)$ 是 $b-c$ 的因数, 显然得证.

不然, 发现 $e_i \le \varphi(p_i^{e_i}) \le \varphi(m) \le b$ 且 $\varphi(m) \le c$, 又发现 $p_i^{e_i} | a^{e_i}$, 所以 $p_i^{e_i} | a^b$,$p_i^{e_i} | a^c$, 左右两边均为 0, 得证.

CF906D Power Tower/[六省联考 2017] 相逢是问候

给定一个数列 w 和模数 p, 每次询问一个区间 $[l, r]$, 求 $w_l^{w_{l+1}^{w_{l+2}^{\cdots^{w_r}}}}$

CF906D Power Tower/[六省联考 2017] 相逢是问候

给定一个数列 w 和模数 p, 每次询问一个区间 $[l, r]$, 求 $w_l^{w_{l+1}^{w_{l+2}^{\cdots^{w_r}}}}$

考虑每次暴力做扩展欧拉定理, 注意到每次会把 p 变成 $\varphi(p)$, 如果 p 是奇数, 那它下一步会变为偶数, 如果 p 是偶数, 则下一步至少减半, 于是迭代次数是 $\log n$ 级别的.

原根和阶

阶: 找到一个最小的 k 使得 $a^k \equiv 1 \pmod p$, 则称 k 是 a 在膜 p 意义下的阶.

原根: 如果 a 在膜 p 意义下的阶是 $\varphi(p)$ 且 $a < p$, 则称 a 是 p 的一个原根.

若 m 有原根, 则 m 一定是 $2,4$ 或是 $p^a, 2p^a$, 其中 $p \in prime$ 且 $2 \nmid p$.

由于对于大部分 m 来说, 都存在一个很小的原根, 所以在实际应用中只需要暴力找就可以了.

根据阶的定义, 我们如果要判断一个 a 不是 p 的原根, 只需判断是否 $\exists i$ 使得 $a^i \equiv 1 \pmod p$. 而由于 $a^{\varphi(p)} \equiv 1 \pmod p$, 因此一定有 $i | \varphi(p)$, 因此只需判断 $\varphi(p)$ 的所有因数, 复杂度 $O(\sqrt{\varphi(p)})$.

事实上, 只需要判断对于 $\varphi(p)$ 的所有质因子 w, 是否有 $a^{\frac{\varphi(p)}{w}} \equiv 1 \pmod p$ 即可, 复杂度 $O(\omega(p))$.

原根和阶

给定 k,p,a, 求 $x^k \equiv a \pmod p$ 的所有解, 其中 $p \in prime, 1 \le k \le 10^5$.

原根和阶

给定 k,p,a, 求 $x^k \equiv a \pmod p$ 的所有解, 其中 $p \in prime, 1 \le k \le 10^5$.

考虑求出 p 的原根 g, 得到 $g^r \equiv a \pmod p$, 同时由于 $x \equiv g^y \pmod p$, 因此原方程变为:$g^{yk} \equiv g^r \pmod p$.

于是有:$yk \equiv r \pmod{p-1}$, 即可求解.

积性函数

积性函数

若函数 $f(x)$ 满足 $\forall n,m \in \mathbb{N}_+, n\perp m$, 有 $f(1)=1, f(nm)=f(n)f(m)$, 则称其为积性函数. 若 $\forall n,m \in \mathbb{N}_+$, 有 $f(1)=1, f(nm)=f(n)f(m)$, 则称其为完全积性函数.

定义两个函数的狄利克雷卷积为:$h=f*g$, 则 $h(n)=\sum_{d|n} f(d)g(\frac{n}{d})$.

若函数 $g(x)$ 是积性函数并且有 $g(m)=\sum_{d|m} f(d)$, 则 $f(x)$ 也是积性函数, 证明如下:

不妨考虑数学归纳, 首先 $g(1)=f(1)=1$.

令 $m=m_1m_2, m_1\perp m_2$, 则 $g(m)=\sum_{d|m} f(d)=\sum_{d_1|m_1}\sum_{d_2|m_2} f(d_1d_2)$. 由于归纳假设, 此时只有 $d_1=m_1$ 且 $d_2=m_2$ 的时候,$f(d_1d_2)$ 可能不等于 $f(d_1)f(d_2)$.

于是有

$$g(m)=\sum_{d_1|m_1}\sum_{d_2|m_2} f(d_1)f(d_2)-f(m_1)f(m_2)+f(m_1m_2)$$

狄利克雷卷积

不难证明狄利克雷卷积满足:

- 交换律:$f * g = g * f$.
- 结合律:$f * (g * h) = (f * g) * h$.
- 分配律:$f * (g + h) = f * g + f * h$.
- 若 f, g 是积性函数, 则 $f * g$ 也是积性函数.
- $\forall f, f(1) \neq 0, \exists f^{-1}, f * f^{-1} = \epsilon$.
- 积性函数的逆元也是积性函数.

狄利克雷卷积

考虑第四条的证明:

$$
\begin{aligned}
f * g(nm) &= \sum_{d|(nm)} f(d) g(\frac{n}{d}) \\
&= \sum_{c|n} \sum_{d|m} f(cd) g(\frac{nm}{cd}) \\
&= \sum_{c|n} \sum_{d|m} f(c) f(d) g(\frac{n}{c}) g(\frac{m}{d}) \\
&= (fg(n)) \times (fg(m))
\end{aligned}
$$

第五条的证明: 构造 $g(x)$ 满足 $f(1)g(x) = \epsilon(x) - \sum_{d|x, d\neq 1} f(d)g(\frac{x}{d})$ 显然就是满足条件的.

莫比乌斯函数

$$m=\prod_{i=1}^{k}p_i^{m_i},\mu(m)=\begin{cases}0 & m_i\ge 2\\(-1)^k & \forall m_i\le 1\end{cases}$$

.

狄利克雷前缀和

定义若 g 是 f 的狄利克雷前缀和, 则 $g(n)=\sum_{d|n}f(d)$, 也即 $g=f*I$.

下面证明 $\sum_{d|n}\varphi(d)=n$, 同理可证明 $\sum_{d|n}\mu(d)=[n=1]$.

我们考虑一个事实: 现在有 m 个不同的分数 $\frac{k}{m}, k\in[1,m]$, 这些分数进行约分后, 它们的分母即 m 的若干因数, 而它们的分子就是与这些因数互质的数, 同时这些数的个数总共是 m 个.

上面这个结论还有另一种证明方法: 由于 φ 是积性函数, 若 $n\neq 1$, 设 $n=\prod_{i=1}^{k}p_i^{q_i}$, 则 $\varphi(n)=\prod_{i=1}^{k}\varphi(p_i^{q_i})$, 则有:

$$\sum_{d|n}\varphi(d)=\sum_{w_1=0}^{q_1}\sum_{w_2=0}^{q_2}\ldots\ldots\sum_{w_k=0}^{q_k}\varphi(p_1^{w_1})\varphi(p_2^{w_2})\ldots\ldots\varphi(p_k^{w_k})$$

而 $\varphi(p^q)=p^q-p^{q-1}$, 于是有 $\sum_{i=1}^{q_i}(p_x^i-p_x^{i-1})=(p_x^{q_x}-1)$, 则有 $\sum_{i=0}^{q_x}\varphi(p_x^i)=p_x^{q_x}=n$.

则原式等于 $\prod_{i=1}^{k}p_i^{q_i}=n$.

莫比乌斯反演

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

证明:

$$g(n)=\sum_{m|n}[\frac{n}{m}=1]g(m)$$
$$=\sum_{m|n}\sum_{d|\frac{n}{m}}\mu(d)g(m)$$

注意到 $[d|\frac{n}{m}]=[md|n]=[m|\frac{n}{d}]$.

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

莫比乌斯反演

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

证明:

$$\begin{aligned}
g(n)&=\sum_{n|d}[\frac{d}{n}=1]g(d)\\
&=\sum_{n|d}\sum_{c|\frac{d}{n}}\mu(c)g(d)\\
&=\sum_{c|d}\sum_{nc|d}\mu(c)g(d)\\
&=\sum_{c}\mu(c)f(nc)\\
&=\sum_{n|d}\mu(\frac{d}{n})f(d)
\end{aligned}$$

莫比乌斯反演

求长度为 n 且仅包含小写英文字母且最小循环节长度恰为 n 的字符串个数.

莫比乌斯反演

求长度为 n 且仅包含小写英文字母且最小循环节长度恰为 n 的字符串个数.

不妨设 $f(n)$ 表示长度为 n 的字符串个数,$g(n)$ 表示长度为 n 且最小循环节长度恰为 n 的字符串个数.

有 $f(n) = \sum_{d|n} g(d)$, 根据莫比乌斯反演,$g(n) = \sum_{d|n} \mu(\frac{n}{d})f(d)$.

莫比乌斯反演

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[gcd(i,j)\in prime]$.

莫比乌斯反演

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[gcd(i,j) \in prime]$.

考虑增加枚举量, 则:

$$
\begin{aligned}
\sum_{i=1}^{n}\sum_{j=1}^{m}[gcd(i,j) \in prime] &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{p\in prime}[gcd(i,j)=p] \\
&= \sum_{p\in prime}\sum_{i=1}^{\lfloor\frac{n}{d}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{d}\rfloor}[gcd(pi,pj)=p] \\
&= \sum_{p\in prime}\sum_{i=1}^{\lfloor\frac{n}{p}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{p}\rfloor}[gcd(i,j)=1] \\
&= \sum_{p\in prime}\sum_{d=1}^{\min(\lfloor\frac{m}{p}\rfloor,\lfloor\frac{n}{p}\rfloor)}\mu(d)\lfloor\frac{n}{pd}\rfloor\lfloor\frac{m}{pd}\rfloor
\end{aligned}
$$

莫比乌斯反演

求 $\sum_{i=1}^{n}\sum_{j=1}^{m}[gcd(i,j)\in prime]$.

考虑增加枚举量, 则:

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{m}[gcd(i,j)\in prime] &= \sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{p\in prime}[gcd(i,j)=p] \\ &= \sum_{p\in prime}\sum_{i=1}^{\lfloor\frac{n}{d}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{d}\rfloor}[gcd(pi,pj)=p] \\ &= \sum_{p\in prime}\sum_{i=1}^{\lfloor\frac{n}{p}\rfloor}\sum_{j=1}^{\lfloor\frac{m}{p}\rfloor}[gcd(i,j)=1] \\ &= \sum_{p\in prime}\sum_{d=1}^{\min(\lfloor\frac{m}{p}\rfloor,\lfloor\frac{n}{p}\rfloor)}\mu(d)\lfloor\frac{n}{pd}\rfloor\lfloor\frac{m}{pd}\rfloor\end{aligned}$$

考虑设 $x=pd$, 则变为 $\sum_{x=1}^{\min(n,m)}\sum_{p\in prime,p|x}\mu(\frac{x}{p})\lfloor\frac{n}{x}\rfloor\lfloor\frac{m}{x}\rfloor$.

Thanks for listening!