

初等数论

张昕渊

September 29, 2023

预备知识

- 模 n 下的基本算数运算:
 - $((i \bmod n) \circ (j \bmod n)) = (i \circ j) \bmod n$, 其中 \circ 可以表示加法、减法和乘法。
 - 求解仅包含加法、减法和乘法的表达式模 n 的值, 我们可以在计算过程中的任意时刻对任意计算结果模 n , 最终结果模 n 的值不会改变。
- 示例: 计算斐波那契数列 f_n 模 $P = 10^9 + 7$ 的值。
- 利用

$$\begin{aligned}f_n \bmod P &= (f_{n-1} + f_{n-2}) \bmod P \\&= (f_{n-1} \bmod P + f_{n-2} \bmod P) \bmod P\end{aligned}$$

进行计算, 此时不会出现整数溢出的情形。

预备知识

- 模素数 p 下的基本算数运算:
 - 对于任意不为 p 倍数的元素 a , 我们可以找到唯一的元素 $a^{-1} \in \{1, 2, \dots, p-1\}$ 满足 $a^{-1}a = 1$ 。此时 b/a 在模 p 下被定义为 $b \cdot a^{-1} \bmod p$ 。
 - 逆元的求解

Theorem (费马小定理)

当 a, p 互素时, $a^{p-1} \equiv 1 \bmod p$ 。

Proof.

注意到 $\{a, 2a, \dots, (p-1)a\} = \{1, 2, \dots, p-1\}$ 。因此,

$$\prod_{i=1}^{p-1} (ai) = a^{p-1} \prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} i \bmod p.$$

两边乘以 $\prod_{i=1}^{p-1} i$ 在 p 下的逆元即得证。



第一小节的内容大纲

- $\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构;
- 原根与离散对数问题;
- Lucas定理、*Kummer定理。

$\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构

- 从现在开始，我们讨论的模数 p 为一给定素数。
- 我们现在考虑如下问题：

Problem

对于给定的素数 p 以及 $a \in \{1, 2, \dots, p-1\}$ ，哪一些指数 x 满足如下同余方程？

$$a^x \equiv 1 \pmod{p}$$

$\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构

Fact

若 x, y 均为上述方程的解，则 $\gcd(x, y)$ 也是方程的解。

Proof.

由裴蜀定理，存在整数 u, v 满足 $ux + vy = \gcd(x, y)$ 。因此

$$a^{\gcd(x, y)} = a^{ux+vy} = (a^x)^u \cdot (a^y)^v \equiv 1 \pmod{p}.$$



Corollary

令 $\delta_p(a)$ 为方程 $a^x \equiv 1 \pmod{p}$ 的最小正整数解，则方程的解均为 $\delta_p(a)$ 的倍数。特别地， $\delta_p(a) \mid p-1$ 。

$\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构

Definition (原根)

给定素数 p ，若整数 g 满足以下条件，则我们称之为原根。

- $(g, p) = 1$;
- $\delta_p(g) = p - 1$ 。

Theorem (原根的存在性)

任意给定的素数 p 都存在对应的原根 g 。

- 证明较为复杂，感兴趣的同学可以参考oi-wiki中的内容。

$\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构

Theorem (原根的存在性)

任意给定的素数 p 都存在对应的原根 g 。

Corollary

$$\{g^0, g^1, \dots, g^{p-2}\} = \{1, 2, \dots, p-1\}$$

- 这一推论非常重要！它隐含着 $\{1, 2, \dots, p-1\}$ 模 p 意义下乘法运算与 $\{0, 1, \dots, p-2\}$ 模 $p-1$ 意义下加法运算的等价性！
 1. 对于任意的 $a \in \{1, 2, \dots, p-1\}$ ，我们可以找到唯一的元素 i_a 满足 $a \equiv g^{i_a} \pmod{p}$ ；
 2. 对于任意的 $a, b \in \{1, 2, \dots, p-1\}$ ，我们可以通过考虑 i_a, i_b （离散对数）将乘法转为加法：

$$a \cdot b \equiv g^{i_a} \cdot g^{i_b} = g^{(i_a+i_b) \pmod{p-1}} \pmod{p}.$$

$\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构

- 很多时候将乘法运算转为加法运算可以极大的简化问题。

Theorem (威尔逊定理)

对于任意的素数 p ，我们有

$$\prod_{i=1}^{p-1} i \equiv -1 \pmod{p}.$$

Proof.

令 g 为 p 对应的原根，则

$$\prod_{i=1}^{p-1} i \equiv \prod_{i=1}^{p-1} g^i = g^{p(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \pmod{p}.$$



$\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构

- 很多时候将乘法运算转为加法运算可以极大的简化问题。

Theorem

对于任意的素数 p ，原根的个数为 $\phi(p-1)$ ，其中 $\phi(m)$ 为 $\{1, 2, \dots, m\}$ 中与 m 互素的数的个数。

Proof.

选定任意的原根 g ，则 g^i 为原根当且仅当 $\gcd(i, p-1) = 1$ 。 □

- 更一般的， $\delta_p(x) = \frac{p-1}{\gcd(i_x, p-1)}$ ，其中 i_x 满足 $g^{i_x} \equiv x \pmod{p}$ 。
- 一个自然的推论是 $\delta_p(x) \mid p-1$ ，因此当给定 $p-1$ 的分解时，我们可以在 $O(\log^2 p)$ 的时间内求解 $\delta_p(x)$ 。
- 一个值得指出的点是该结论与原根的选取无关。

$\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构

- 对于算法竞赛而言，很多时候我们不仅仅需要知道原根的存在性，我们更需要找出一个原根用以计算。
- 首先我们考虑一个更简单的问题：

Problem

对于一个元素 $g \in \{1, 2, \dots, p-1\}$ ，判定 g 是否为原根。

- 由于 $\delta_p(g) \mid p-1$ ，因此我们只需要对于所有 $p-1$ 的素因子 q 验证 $\delta_p(g) \nmid \frac{p-1}{q}$ 即可。
- 上述等价于验证 $g^{\frac{p-1}{q}} \not\equiv 1 \pmod p$ 是否成立。
- 对于原问题，我们只需要重复随机选取 $g \in \{1, 2, \dots, p-1\}$ 进行验证，直至 g 为原根即可。
- 原根个数为 $\phi(p-1)$ ，因此当 $p \leq 10^{18}$ 时，随机到一个原根的概率至少为 $\phi(p-1)/(p-1) \geq 0.1$ ，因此期望10次随机可以找到一个原根。

例题：同余方程

- 给定素数 p 以及正整数 $1 \leq a < p$ ，找到一组下列同余方程的解：

$$a^x \equiv x \pmod{p}.$$

- $p \leq 10^9$ 。

例题：同余方程

- 由费马小定理：当 $x \equiv 0 \pmod{p-1}$ 时， $a^x \equiv 1 \pmod{p}$ 。因此 $x = (p-1)^2$ 就是一组合法解。

例题：小A 与两位神仙（简化版本）

- 给定素数 p 以及正整数 $1 \leq x, y < p$ ，判断方程 $x^a \equiv y \pmod p$ 是否有解。
- $p \leq 10^{18}$ 。
- Luogu 5605

例题：小A 与两位神仙（简化版本）

- 令 g 为原根，则存在 i_x, i_y 满足 $x \equiv g^{i_x} \pmod{p}$, $y \equiv g^{i_y} \pmod{p}$ 。
- 因此原问题转换为
 - 是否存在 $a \in \{0, 1, 2, \dots, p-2\}$ 满足 $i_x a \equiv i_y \pmod{p-1}$ 。
- 上述为经典问题，当 $\gcd(i_x, p-1) \mid \gcd(i_y, p-1)$ 时有解（我们将在下一节课会详细讲述此类问题的求解）。

例题： Classic: Classical Problem

- 令 p 为素数， $S \subseteq \{0, 1, \dots, p-1\}$ 为一集合。对于任意的 $c \in \{0, 1, \dots, p-1\}$ ，令 $S_c = \{(c \cdot x) \bmod p \mid x \in S\}$ 。求 $\max_{c \in \{0, 1, \dots, p-1\}} \text{mex}(S_c)$ ，其中 $\text{mex}(S)$ 为最小未出现在 S 中的非负整数。
- $1 \leq |S| \leq p \leq 2 \cdot 10^5$ 。
- 来源： The 1st Universal Cup Stage 15: Hangzhou, F

例题: Classic: Classical Problem

- 若 $0 \notin S$, 则选取 $c = 0$ 时取得最大值 1。
- 否则, 我们考虑二分答案。问题转化为
 - 是否存在 $c \in \{1, 2, \dots, p-1\}$, 使得 $1, 2, \dots, L$ 均在 S_c 中。
- 考虑任意的原根 g , 对于任意的集合 S , 令 $T_S = \{i \in \{0, 1, \dots, p-2\} \mid \exists j \in S, g^i \equiv j \pmod{p}\}$ 。则问题转化为
 - 是否存在 $c \in \{0, 1, \dots, p-2\}$, 使得

$$T_{\{1, 2, \dots, L\}} \subseteq (T_S + c) \pmod{p-1}.$$

- 该问题为经典问题, 可用FFT解决。

离散对数问题与大步小步(BSGS)算法

- 我们考虑下述离散对数问题:

Problem

给定素数 p 以及整数 $1 \leq a, b < p$, 求下述方程的一个解或判定该方程无解:

$$a^x \equiv b \pmod{p}.$$

- 我们下面将给出一个时间复杂度为 $\tilde{O}(\sqrt{p})$ 的算法。该算法基于meet-in-the-middle思想（相遇）。

离散对数问题与大步小步(BSGS)算法

- 首先观察到如果方程存在解 x ，则存在一个介于 $0 \leq x < p-1$ 的解。
- 令 $B = \lceil \sqrt{p} \rceil + 1$ ，则一定存在 $0 \leq L, R \leq B$ 使得 $x = L \cdot B - R$ 。
- 此时，方程将转变为求解 $0 \leq L, R < B$ 满足

$$a^{LB} \equiv ba^R \pmod{p}$$

- 此步转化用到了 $a \not\equiv 0 \pmod{p}$!
- 预处理出 $S = \{(a^B)^L \pmod{p} \mid 0 \leq L < B\}$ 的值，对于每个 $0 \leq R < B$ 计算出 $ba^R \pmod{p}$ 是否在 S 中即可。
- 思考：解集是什么？

例题：小A与两位神仙（变种）

- 给定素数 p 以及 $1 \leq x, y < p$ ，求解 $x^a \equiv y \pmod{p}$ 。
- $p \leq 10^9$ 。

例题：同余方程II

- 令 g 为原根，则我们通过BSGS算法求得 i_x, i_y 满足 $g^{i_x} \equiv x \pmod{p}$, $g^{i_y} \equiv y \pmod{p}$ 。
- 问题即求解 $i_x \cdot a \equiv i_y \pmod{p}$ ，这是一个经典问题，我们将在之后讲述该方程的求解。

例题：同余方程II

- 令 g 为原根，则我们通过BSGS算法求得 i_x, i_y 满足 $g^{i_x} \equiv x \pmod{p}$, $g^{i_y} \equiv y \pmod{p}$ 。
- 问题即求解 $i_x \cdot a \equiv i_y \pmod{p}$ ，这是一个经典问题，我们将在之后讲述该方程的求解。

例题: Sequence in mod P

- 令 p 为一质数, $0 \leq A, B, S, G < p$ 为整数。考虑如下线性递推

$$X_n = \begin{cases} S & n = 0 \\ (AX_{n-1} + B) \bmod p & n \geq 1 \end{cases}$$

求解是否存在 i 使得 $X_i = G$ 。若存在, 找到最小的正整数解。

- 100组询问, $p \leq 10^9$ 。
- ABC270 G

例题：Sequence in mod P

- 不妨假设 $A \geq 2$ 。
- 我们可以通过常见的数列技巧将 X_n 转为等比序列：
 - 待定系数 C 有 $X_n + C = A(X_{n-1} + C) \pmod p$ ，解得 $C = (A - 1)^{-1} \cdot B \pmod p$ ；
 - 令 $Y_n = (X_n + C) \pmod p$ ，此时 $Y_n = A^n \cdot Y_0 \pmod p$ ，问题已经被转换为离散对数问题，可以用BSGS解决。

Lucas定理

- 关于素数模数，我们最后再来介绍一下Lucas定理。

Theorem (Lucas定理)

令 p 为素数，我们有

$$\binom{n}{m} \equiv \binom{n \bmod p}{m \bmod p} \binom{\lfloor \frac{n}{p} \rfloor}{\lfloor \frac{m}{p} \rfloor} \pmod{p},$$

其中 $\binom{x}{y} = 0$ 若 $x < y$ 。

Lucas定理

Theorem (Lucas定理)

$$\binom{n}{m} \equiv \binom{n \bmod p}{m \bmod p} \binom{\lfloor \frac{n}{p} \rfloor}{\lfloor \frac{m}{p} \rfloor} \pmod{p}.$$

Proof.

一方面, $\binom{n}{m}$ 为多项式 $(1+x)^n$ 中 x^m 次项的系数。
另一方面, 由于 $(1+x)^p \equiv 1+x^p \pmod{p}$, 因此

$$\begin{aligned}(1+x)^n &= (1+x)^{n \bmod p + \lfloor \frac{n}{p} \rfloor p} \\ &\equiv (1+x)^{n \bmod p} \cdot (1+x^p)^{\lfloor \frac{n}{p} \rfloor} \pmod{p}\end{aligned}$$

对比系数即得结果。



Lucas定理

Theorem (Lucas定理)

$$\binom{n}{m} \equiv \binom{n \bmod p}{m \bmod p} \binom{\lfloor \frac{n}{p} \rfloor}{\lfloor \frac{m}{p} \rfloor} \pmod{p}.$$

- 给定一个素数 p 以及 n, m ，我们可以通过 $O(p + \log n)$ 的时间求解 $\binom{n}{m} \bmod p$ 的值。
- 进一步的，我们有如下推论：
 1. $\binom{n+m}{m}$ 不是 p 的倍数当且仅当 $n + m$ 在 p 进制下加法不产生进位。
 2. 当 $p = 2$ 时，上述等价于 n and $m = 0$ 。

*Kummer定理

- 如何求解最大的正整数 $\alpha = \nu_p \left(\binom{n+m}{n} \right)$ 使得 $p^\alpha \mid \binom{n+m}{n}$?

Theorem (Kummer定理)

$$\nu_p \left(\binom{n+m}{n} \right) = \frac{S_p(n) + S_p(m) - S_p(n+m)}{p-1},$$

其中 $S_p(x)$ 为 x 的数位和。

特别地， $\nu_p \left(\binom{n+m}{n} \right)$ 恰为 $n+m$ 在 p 进制下加法产生进位的次数。

Proof.

$$S_p(n) = \sum_{k=0}^{+\infty} \left(\left\lfloor \frac{n}{p^k} \right\rfloor - p \left\lfloor \frac{n}{p^{k+1}} \right\rfloor \right) = n - (p-1) \sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor. \quad \square$$

例题： Number of Binominal Coefficients

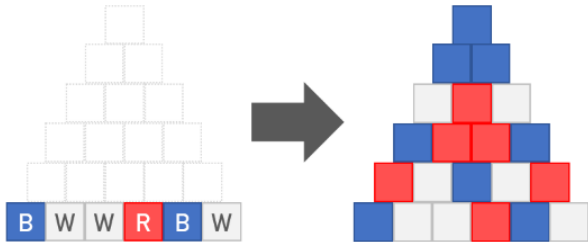
- 给定素数 p ，整数 α, A ，求整数对 $0 \leq k \leq n \leq A$ 满足 $p^\alpha \mid \binom{n}{k}$ 。
答案对 $10^9 + 7$ 取模。
- $\alpha, p \leq 10^9, A \leq 10^{1000}$ 。

例题： Number of Binominal Coefficients

- 由Kummer定理, $p^\alpha \mid \binom{n}{k}$ 等价于 $(n - k) + k$ 在 p 进制下至少进位 α 次, 即 $n - k$ 借位至少 α 次。
- 令 A 在 p 进制下的展开为 x_1, x_2, \dots, x_k , 我们考虑标准的数位 dp , 即从高位向低位 dp , 维护前缀有 k 次借位的方案数:
 - 令 dp_{i,j,f_1,f_2} 为前 i 位中已产生 j 次借位的方案数, 其中 f_1 为 n 是否可能达到或超过上界的指示变量, f_2 为第 i 位是否产生借位的指示变量。
- 时间复杂度为 $O(|A|^2)$ (尽管常数相当大)。

例题：Tricolor Pyramid

- 有一个由三种颜色 R, G, B 构成的金字塔。现给定底层的颜色，其余格子的颜色由下述规则生成：
 - 令该格子下一层临接格子颜色分别为 x, y ，若 $x = y$ 则该格子颜色为 x ；否则颜色为三者中剩余颜色。
- 求最顶层颜色。
- 底层大小 $N \leq 4 \cdot 10^5$ 。
- ARC117 C



例题：Tricolor Pyramid

- 令 R, G, P 分别为 $0, 1, 2$ ，则上述规则转化为 $-(x + y) \bmod 3$ 。
- 令 x_0, x_1, \dots, x_N 为底层颜色，则最顶层颜色为 $(-1)^N \sum_{i=0}^N \binom{N}{i} x_i \bmod 3$ ；
- 这可由 Lucas 定理 / Kummer 定理解决。

例题: Vika and Wiki

- 给定正整数 k 以及长度为 $n = 2^k$ 的序列 $a = [a_0, a_1, \dots, a_{n-1}]$, 我们可以采用下述操作更新序列:
 - 令 $b = [b_0, b_1, \dots, b_{n-1}]$, 其中 $b_i = a_i \oplus a_{(i+1) \bmod n}$;
 - 将 a 更新为 b 。
- 求最少操作次数使得序列 a 变为全0, 或判定不可能通过上述操作变为全0。
- $k \leq 20$ 。

例题: Vika and Wiki

- 类似上题, 我们发现经过 k 次更新后, 序列 a 的第 i 位的值为 $\bigoplus_{j=0}^k \left(\binom{k}{j} \bmod 2 \right) a_{(i+j) \bmod n} \circ$
- $k = n$ 时, 序列一定为全0, 因此答案小于等于 n 。
- 在模2下, 我们可以替换为 $\bigoplus_{j \text{ and } k=j} a_{(i+j) \bmod n} \circ$
- 从高位到低位枚举答案, 假设我们现在知道 a 经过 $\sum_{i=d+1}^k c_i 2^i$ 次操作后的序列为 b , 我们现在需要判断 b 再经过 2^d 次操作后的序列 c 。
- $c_i = b_i \oplus b_{(i+2^d) \bmod n} \circ$

第一小节内容总结

- $\{1, 2, \dots, p-1\}$ 在模 p 乘法运算下的结构:
 - 乘法通过原根转化为加法。
 - 素数意义下的带有指数的同余方程常常可以考虑原根。
- 原根与离散对数问题。
- Lucas定理、*Kummer定理。
 - 重要推论: $p=2$ 时组合数 $\binom{n}{m}$ 为奇数的等价条件。

- 第一小节内容结束，我们休息5-10分钟后继续下半节的内容；
- 有疑问的同学可以在课间或者课后咨询。

第二节的内容大纲

- 一般模数下乘法运算与加法运算的结构;
- *一般模数下的原根、离散对数问题;
- *一般模数下的Lucas定理。

预备知识

- $a \mid b \cdot c$ 当且仅当 $\frac{a}{\gcd(a,b)} \mid c$ 。
- 推论: $a \cdot b \equiv a \cdot \left(b \bmod \frac{m}{\gcd(a,m)} \right) \pmod{m}$ 。
- $a \mid b$ 且 $a \mid c$ 当且仅当 $a \mid \gcd(b, c)$;
- $a \mid c$ 且 $b \mid c$ 当且仅当 $\text{lcm}(a, b) \mid c$ 。

一般模数下的逆元

- 类似于素数模数，我们可以定义一般模数下的逆元。

Definition

给定正整数 m, a ，我们称 a^{-1} 为 a 在模 m 下的逆元，若

$$a^{-1} \cdot a \equiv 1 \pmod{m}.$$

- 当 $\gcd(a, m) > 1$ 时， $\gcd(a, m) \mid ax + bm$ ，因此不存在逆元；
- 当 $\gcd(a, m) = 1$ 时，裴蜀定理保证了逆元的存在性：

Theorem (裴蜀定理)

令 a, b 为整数。存在整数 x, y 使得

$$ax + by = \gcd(a, b).$$

一般模数下的逆元

Theorem (裴蜀定理)

令 a, b 为整数。存在整数 x, y 使得

$$ax + by = \gcd(a, b).$$

Proof.

我们只需要证明 $\{ax \bmod b \mid 0 \leq x < b\} = \{0, 1, \dots, b-1\}$ 即可，这等价于证明不存在 $0 \leq x_1 < x_2 < b$ 满足 $ax_1 \equiv ax_2 \pmod{b}$ 。若不然，则 $b \mid a(x_1 - x_2)$ 。由 $\gcd(a, b) = 1$ 可知 $b \mid x_1 - x_2$ ，矛盾。 \square

- 裴蜀定理只告诉了解的存在性，如何得到解？

一般模数下的逆元

- 欧几里得算法 $\gcd(a, b)$:
 - 若 $a = 0$, 则返回 b ;
 - 否则返回 $\gcd(b \bmod a, a)$ 。
- 算法复杂度 $O(\log \max(a, b))$: 若 $b \geq a$ 则 $b \bmod a \leq \frac{b}{2}$ 。
- 拓展欧几里得算法 $\text{exgcd}(a, b)$ (返回 $\gcd(a, b)$ 和 x, y , 方程 $ax + by = \gcd(a, b)$ 的一组解)。
 - 若 $a = 0$, 则返回 $[b, 0, 1]$;
 - 否则, 令 $[g, x, y] = \text{exgcd}(b \bmod a, a)$, 则我们有

$$(b \bmod a)x + ay = \gcd(a, b).$$

- 由 $b \bmod a = b - \lfloor \frac{b}{a} \rfloor a$, 我们令

$$x' = y - \left\lfloor \frac{b}{a} \right\rfloor x \text{ and } y' = x,$$

并返回 $[g, x', y']$.

一般模数下的逆元

- 拓展欧几里得算法 $\text{exgcd}(a, b)$ （返回 $\text{gcd}(a, b)$ 和 x, y ，方程 $ax + by = \text{gcd}(a, b)$ 的一组解）。
- 当 $a, b \neq 0$ 时，算法返回解 x, y 满足 $|x|, |y| \leq a + b$ （因此我们不需要担心溢出的问题）。
- 如何求解 $ax \equiv c \pmod b$ 的最小非负整数解？
 - 有解当且仅当 $\text{gcd}(a, b) \mid c$ 。
 - x, y 为 exgcd 返回值，则 $x_0 = \frac{c}{\text{gcd}(a, b)}x, y_0 = \frac{c}{\text{gcd}(a, b)}y$ 为可行解。
 - 令 x_0, y_0 为方程 $ax + by = c$ 的一组整数解。所有整数解为

$$\forall k \in \mathbb{Z}, \quad x = x_0 + \frac{b}{\text{gcd}(a, b)}k \text{ and } y = y_0 - \frac{a}{\text{gcd}(a, b)}k.$$

- 考虑 $i \rightarrow (i + a) \pmod b$ 的有向图，上述其实表明了这一个有向图由 $\text{gcd}(a, b)$ 个大小一致的圈组成，其中第 i 个圈中包含 i 。

一般模数下的逆元

- 裴蜀定理并不仅仅说明了解的存在性，裴蜀定理更说明了 a_1, a_2, \dots, a_n 的整线性组合的取值集合。即

$$\left\{ \sum_{i=1}^n a_i x_i \mid x_i \in \mathbb{Z} \right\} = \{ k \gcd(a_1, a_2, \dots, a_n) \mid k \in \mathbb{Z} \}.$$

- 我们将通过下面的几个例题来理解整线性组合与gcd之间的密切联系。

例题: Nezzar and Board

- 集合 S 中有 n 个整数 x_1, x_2, \dots, x_n 。我们一次操作可以选择 $x, y \in S$, 将 $2x - y$ 加入 S 中。问是否可以通过若干次操作使得 $k \in S$ 。
- $-10^{18} \leq k, x_i \leq 10^{18}, n \leq 10^5$ 。
- CF 1477A

例题: Nezzar and Board

- 若 $x_1 = 0$, 我们可以通过上述操作进行组合得到下面的基础操作:
 1. $x, y \in S$, 则可以有 $x + y \in S$;
 2. $x \in S, k \in F$, 则可以有 $kx \in S$ 。
- 因此生成 S 的集合为 $\gcd(x_2, x_3, \dots, x_n)$ 的倍数。
- 当 $x_1 \neq 0$ 时, 所有数减去 x_1 即可。

例题：Return to 1

- 给一个有向图 $G = (V, E)$ ，求是否可以从顶点1走 10^{100} 步恰好走到顶点1。
- $|V|, |E| \leq 2 \cdot 10^5$ 。
- ABC306 G

例题：Return to 1

- 不妨假设图是强连通的；
- 我们首先考虑所有图 G 中所有的简单圈 C_1, C_2, \dots, C_s ，则对于任意的 $t \in T$ ，我们都可在 t 时间内返回1，其中

$$T = \left\{ \sum_{i=1}^s k_i |C_i| : k_i \in \mathbb{N}_{\geq 2} \right\},$$

- $10^{10^{100}}$ 充分大，因此条件等价于 $\gcd(C_1, C_2, \dots, C_s) \mid 10^{10^{100}}$ 。
- 求解 $\gcd(C_1, C_2, \dots, C_s)$:
 - 找一颗任意节点为根的BFS树；
 - 对于所有的非树边 $u \rightarrow v$ ，令 $g \leftarrow \gcd(g, |d_v - d_u - 1|)$ 。

例题：Return to s

- 给一个带权无向图 $G = (V, E, w)$ ，是否可以从顶点1花费 t 恰好走到顶点 s 。
- $|V|, |E| \leq 100$, $w_i \leq 10^4$, $t \leq 10^{18}$.

例题：Return to s

- 不妨假设1到 s 连通。
- 令 e 为邻接 s 的边，若我们可以花费 x 到顶点 s ，则我们可以通过花费 $2w_e + x$ 到顶点；
- 因此我们考虑模 $2w_e$ 下的最小花费：对每个顶点 u 拆点 $(u, i)_{i=0}^{2w_e-1}$ ，表示到顶点 u 花费模 $2w_e$ 为 i 的状态。我们在新图上跑最短路即可。

例题：Phoenix and Odometers

- 给一个带权有向图 $G = (V, E, w)$ ， q 个询问，每个询问给定顶点 s_i 以及值 $0 \leq t_i < m_i$ ，问是否存在一个从顶点 s_i 回到本身的游走，游走总权值和模 m_i 为 t_i 。
- $|V|, |E|, q \leq 10^5, m_i \leq 10^9$ 。
- CF1515 G

例题： Phoenix and Odometers

- 做法基本和Return to 1一致，我们这里不再赘述。

欧拉定理与欧拉函数

- 对于一般模数，我们也有类似于费马小定理的结论。

Theorem (欧拉定理)

当 $\gcd(a, m) = 1$ 时,

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

其中 $\phi(m)$ 为 $1 \leq x \leq m$ 中满足 $\gcd(x, m) = 1$ 的个数。

Proof.

证明与费马小定理的证明类似，令 $A = \{x \mid \gcd(x, a) = 1\}$ 。则

$$a^{\phi(m)} \cdot \prod_{i \in A} i = \prod_{i \in A} (a \cdot i) \equiv \prod_{i \in A} i \pmod{m}.$$

两边乘以 $(\prod_{i \in A} i)^{-1}$ 可得结论。 □

- 当 a, m 互素，计算 $a^n \pmod{m}$: $a^n \equiv a^{n \bmod \phi(m)} \pmod{m}$ 。

欧拉定理与欧拉函数

- 欧拉函数 $\phi(m)$ 的计算:
 - 令 $m = \prod_{i=1}^d p_i^{\alpha_i}$ 。则 $\phi(m) = m \prod_{i=1}^d \left(1 - \frac{1}{p_i}\right)$ 。（容斥原理）
- 欧拉函数的性质:
 - $\sum_{d|n} \phi(d) = n$: 在 $n \log n$ 时间内求解1到 n 内欧拉函数的值。
 - 积性函数: 若 x, y 互素, 则 $\phi(xy) = \phi(x)\phi(y)$;
 - 莫比乌斯函数 $\mu(x) = \begin{cases} 1 & x = 1 \\ 0 & p^2 \mid x \\ (-1)^k & x = \prod_{i=1}^k p_i \end{cases}$ 、因子个数、因子和都为积性函数。
- 如何线性时间求解1到 n 内积性函数的值?

线性筛与积性函数

Algorithm 1: 线性筛

Input: 正整数 n

Output: 1到 n 中的所有质数

```
1 初始化数组 $p = []$ 以及长度为 $n + 1$ 值全为0的 $vis$ 数组;  
2  for  $i = 2$  to  $n$  do  
3     if  $vis[i] == 0$  then  
4          $p$ 数组末尾加入 $i$ ;  
5     for  $j = 0$  to  $p.size() - 1$  do  
6         if  $i * p[j] > n$  then  
7             break;  
8          $vis[i * p[j]] = 1$ ;  
9         if  $i \bmod p[j] == 0$  then  
10            break;  
11 return  $p$ ;
```

- 每个合数 x 只会在Line 6被标记一次。且被标记时 $p[j]$ 为 x 的最小素因子。因此上述算法可以记录每个数的最小素因子。

线性筛与积性函数

- 我们可以通过简单的修改用于计算1到 n 内欧拉函数的值。

Algorithm 2: 欧拉函数的算法

Input: 正整数 n

Output: 1到 n 欧拉函数的值

```
1 初始化数组 $p = []$ ，以及长度为 $n + 1$ 值全为0的 $vis$ 数组和 $\phi$ 数组；
2  for  $i = 2$  to  $n$  do
3     if  $vis[i] == 0$  then
4          $p$ 数组末尾加入 $i$ ；
5          $\phi[i] = i - 1$ ；
6     for  $j = 0$  to  $p.size() - 1$  do
7         if  $i * p[j] > n$  then
8             break；
9          $vis[i * p[j]] = 1$ ；
10        if  $i \bmod p[j] == 0$  then
11             $\phi[i * p[j]] = p[j] * \phi[i]$ ；
12        else
13             $\phi[i * p[j]] = (p[j] - 1) * \phi[i]$ ；
14        if  $i \bmod p[j] == 0$  then
15            break；
16 return  $p$ ；
```

线性筛与积性函数

- 同样的，我们可以用于计算1到 n 内莫比乌斯函数的值。

Algorithm 3: 欧拉函数的算法

Input: 正整数 n

Output: 1到 n 欧拉函数的值

```
1 初始化数组 $p = []$ ，以及长度为 $n + 1$ 值全为0的 $vis$ 数组和 $\mu$ 数组；
2  for  $i = 2$  to  $n$  do
3     if  $vis[i] == 0$  then
4          $p$ 数组末尾加入 $i$ ；
5          $\mu[i] = -1$ ；
6     for  $j = 0$  to  $p.size() - 1$  do
7         if  $i * p[j] > n$  then
8             break；
9          $vis[i * p[j]] = 1$ ；
10        if  $i \bmod p[j] == 0$  then
11             $\mu[i * p[j]] = 0$ ；
12        else
13             $\mu[i * p[j]] = -\mu[i]$ ；
14        if  $i \bmod p[j] == 0$  then
15            break；
16 return  $p$ ；
```

线性筛与积性函数

- 对于一般的积性函数都可通过线性筛求得1到 n 内函数值。留给同学们课下思考。

欧拉定理与欧拉函数

- 当 a, m 不互素时, $a^x \bmod m$ 需要如何计算?

Theorem

当 $x \geq L = \lceil \log_2 m \rceil$ 时, $a^x \equiv a^{\phi(m)+x \bmod \phi(m)} \bmod m$ 。

Proof.

令 $g = \gcd(a^L, m)$, 此时 $\gcd(a, \frac{m}{g}) = 1$ 。因此,

$$a^x = a^L \cdot a^{x-L} \equiv \frac{a^L}{g} \cdot g \cdot a^{x-L} \equiv \frac{a^L}{g} \cdot g \cdot (a^{x-L} \bmod \frac{m}{g}) \bmod m.$$

由欧拉定理, $a^{x-L} \equiv a^{(x-L) \bmod \phi(m/g)} \bmod \frac{m}{g}$ 。

由于 $\phi(m/g) \mid \phi(m)$ 以及 $\phi(m) \geq \lceil \log_2 m \rceil = K$, 结论得证。 □

- 考虑有向图 $i \rightarrow ai \bmod m$ 。该图为基环内向树, 圈的长度被 $\phi(m)$ 整除, 从任何顶点出发 $\log_2 m$ 步内将走到环内。

例题: Power Tower

- 对于序列 $a = [a_1, a_2, \dots, a_k]$, 令 $w(a) = a_1^{a_2^{a_3 \dots a_k}} \bmod m$ 。给定序列 $b = [b_1, b_2, \dots, b_n]$, 回答 q 个询问 $w(b[l : r])$ 。
- $n, q \leq 10^5, m \leq 10^9$ 。

例题：Power Tower

- 重复利用欧拉定理的示例；
- m 通过 $O(\log_2 m)$ 次欧拉函数操作将变为1：若 m 为奇数，则 $\phi(m)$ 为偶数。

一般模数到素数幂次模数：中国剩余定理

Theorem (中国剩余定理)

令 m_1, m_2, \dots, m_n 为两两互素的正整数，则对于任意的 x_1, x_2, \dots, x_n ，都存在正整数 $0 \leq x < M$ 满足

$$x \equiv x_i \pmod{m_i},$$

其中 $M = \prod_{i=1}^n m_i$ 。

Proof.

令 q_i 为 $\frac{M}{m_i}$ 在模 m_i 下的逆元， $x = \sum_{i=1}^n \frac{M}{m_i} \cdot x_i q_i$ ，则有

$$\sum_{i=1}^n \frac{M}{m_i} \cdot x_i q_i \equiv \frac{M}{m_k} \cdot x_k q_k \equiv x_k \pmod{m_k}.$$



一般模数到素数幂次模数：中国剩余定理

- 令 $\phi : [M] \rightarrow [m_1] \times [m_2] \times \dots \times [m_n]$ 如下

$$\phi(x) = (x \bmod m_1, x \bmod m_2, \dots, x \bmod m_n),$$

中国剩余定理表明上述映射是一个双射。进一步的， $\phi(ax + by) = \phi(a)\phi(x) + \phi(b)\phi(y)$ 。

- 因此，对于很多模 $M = \prod_{i=1}^n p_i^{\alpha_i}$ 的问题，我们令 $m_i = p_i^{\alpha_i}$ ，我们可将问题拆解到更容易解决的素数模数上。

例题: Koxia and Number Theory

- 给定 n 个两两不同的数 a_1, a_2, \dots, a_n , 判定是否存在正整数 x 满足对于任意的 $1 \leq i < j \leq n$ 都有 $\gcd(a_i + x, a_j + x) = 1$ 。
- $1 \leq n \leq 100, a_i \leq 10^{18}$ 。
- CF1770 C

例题：Koxia and Number Theory

- 若存在质数 p 满足对于任意的 $0 \leq k < p$ 都有 $\sum_{i=1}^n [a_i \bmod p = k] \geq 2$ 成立，则不存在；否则存在。
- 存在性简单证明：对于每个素数 $p \leq 10^{18}$ ，我们都可以找到一个好的“偏移量” x_0 。

例题：同余方程

- 给定素数 p ，求解满足下列条件的二元组 (a, b) 的个数。
 - $1 \leq a, b \leq p(p-1)$;
 - $a^b \equiv b^a \pmod{p}$ 。
- $p \leq 10^9$.

例题：同余方程

- 我们下面只考虑 a, b 均非 p 倍数的情形。
- 令 g 为原根，我们考虑 $g^u \equiv a \pmod{p}$, $g^v \equiv b \pmod{p}$ ，则由费马小定理，方程转化为

$$av \equiv bu \pmod{p-1}.$$

- 注意到如果我们给定 $a \pmod{p-1}$ 的值 a_0 ， $u \pmod{p-1}$ 的值，则我们得到了下述同余方程组

$$a \equiv a_0 \pmod{p-1}$$

$$a \equiv g^u \pmod{p}.$$

由中国剩余定理，存在唯一正整数 $1 \leq a \leq p(p-1)$ 满足条件。

- 因此，我们只需求出满足 $av \equiv bu \pmod{m}$ 的四元组 (a, u, b, v) 个数，其中 $0 \leq a, u, b, v < m$ ， $m = p-1$

例题：同余方程

- 再由中国剩余定理，我们只需要将 $m = p - 1$ 进行分解，分别求解模每个质数的素数幂次的答案即可。即求满足 $av \equiv bu \pmod{q^k}$ 的四元组 (a, u, b, v) 的个数，其中 $1 \leq a, u, b, v \leq q^k$ 。

中国剩余定理：非互质版本

- 当 m_1, m_2 不互质时，考虑同余方程组：

$$x \equiv x_1 \pmod{m_1}$$

$$x \equiv x_2 \pmod{m_2}$$

- 令 $g = \gcd(m_1, m_2)$ ，当 $x_1 \not\equiv x_2 \pmod{g}$ 时，上述一定无解。
- 否则，令 $x = gy + x_1$ ，则上述同余方程组将转换为

$$y \equiv 0 \pmod{m_1/g}$$

$$y \equiv (x_2 - x_1)/g \pmod{m_2/g}$$

这转化为互质版本。

- 若同余方程组包含多个方程，两两合并即可。
- 进一步解读：每一个同余方程可以写成若干个模素数或素数幂次的方程组。我们只需要检查每一个素数或者素数幂次是否存在“冲突”即可。

例题：同余方程

- 求解 $a^x \equiv x \pmod{m}$ 。
- $a, m \leq 10^9$ 。

例题：同余方程

- 假设我们有解 $x_0 > 100$ ，则 x_0 是以下同余方程组的一个解。

$$x \equiv a^{x_0} \pmod{m}$$

$$x \equiv x_0 \pmod{\phi(m)}$$

此时，该同余方程组有解当且仅当 x_0 满足

$$a^{x_0} \equiv x_0 \pmod{\gcd(m, \phi(m))}.$$

- 因此，我们只需递归求解 $m' = \gcd(m, \phi(m))$ 即可。

一般模数下的大步小步算法

- 回顾离散对数问题:

Problem

给定 a, b, m , 给出下列同余方程的解:

$$a^x \equiv b \pmod{m}.$$

- 当 $\gcd(a, m) = 1$ 时, 之前素数模数下的大步小步算法仍然适用, 但不互质时不再适用!
 - 这是因为 $a^{LB-R} \equiv b \pmod{m}$ 不再等价于 $a^{LB} \equiv ba^R \pmod{m}$.
- 解决办法: 只考虑 $x > C = \log_2 m$ 的情形。此时同余方程将变为

$$a^{x-C} a^C \equiv b \pmod{m}$$

- 当 $g = \gcd(a^C, m) \nmid b$ 时无解;
- 否则, 同余方程将变为 $a^{x-C} a^C / g \equiv b/g \pmod{m/g}$ 。此时 $(a, m/g) = 1$, 可以直接使用BSGS算法。

*一般模数下的原根

- 这部分内容在算法竞赛中考察非常少，仅做了解。
- 给定正整数 $m \geq 2$ ， g 称为原根若对于任意的 $1 \leq x < \phi(m)$ 都有 $g^x \not\equiv 1 \pmod m$.
- m 有原根当且仅当 $m = 2, 4, p^\alpha, 2p^\alpha$ ，其中 p 为奇素数。
- $m = 2^n$ 是什么情况？任何奇数 $1 \leq x < m$ 可以表示成 $5^s * (-1)^t \pmod m$, $0 \leq s < 2^{n-2}, t \in \{0, 1\}$.

*一般模数下的Lucas定理

- 这部分内容在算法竞赛中考察非常少，仅做了解，可以参考oi-wiki的内容。

狄利克雷 (Dirichlet) 卷积

- 对于定义域在正整数集合上的函数 f, g ，我们考虑Dirichlet卷积如下：

Definition (Dirichlet卷积)

$$(f * g)(n) = \sum_{x|n} f(x)g\left(\frac{n}{x}\right).$$

- 卷积可以看作是函数上的乘法运算：
 - 交换律: $f * g = g * f$;
 - 分配律: $f * (g + h) = f * g + f * h$;
 - 结合律: $f * (g * h) = (f * g) * h$ 。
- 积性函数的卷积还是积性函数。
- 单位元: $(1, 0, 0, 0, \dots)$;
- 全一函数的逆元: 莫比乌斯函数。
- 若 f, g 定义在 $[n]$ 上，卷积可在 $O(n \log n)$ 的时间内求解。

狄利克雷 (Dirichlet) 卷积

- 对于定义域在正整数集合上的函数 f, g ，我们考虑Dirichlet卷积如下：

Definition (Dirichlet卷积)

$$(f * g)(n) = \sum_{x|n} f(x)g\left(\frac{n}{x}\right).$$

- 卷积可以看作是函数上的乘法运算：
 - 交换律: $f * g = g * f$;
 - 分配律: $f * (g + h) = f * g + f * h$;
 - 结合律: $f * (g * h) = (f * g) * h$ 。
- 单位元: $e = (1, 0, 0, 0, \dots)$ ($e * f = f$) ;
- 全一函数 $\mathbf{1}$ 的逆元: 莫比乌斯函数 (即 $\mathbf{1} * \mu = e$) 。
- 若 f, g 定义在 $\{1, 2, \dots, n\}$ 上, 并且只需要求卷积的前 n 项, 可在 $O(n \log n)$ 的时间内求解。

莫比乌斯反演

- 莫比乌斯反演本质上就是 $\mathbf{1} * \mu = \mathbf{e}$ 的应用:
 - 对于数论函数 f, g 满足 $f = \mathbf{1} * g$ 等价于 $g = \mu * f$ 。
 - $(\mathbf{1} * g)(n) = \sum_{m|n} g(m)$, $(\mu * f)(n) = \sum_{m|n} \mu(m)f\left(\frac{n}{m}\right)$ 。
 - 这个定理本质上是告诉你已知所有因子的函数和，如何求解函数本身的值。（你可以看成是某种“容斥”）
- 有没有上述定理对倍数和而非因子和的版本？
 - 假设 g 仅在有限个位置非零，则 $f(n) = \sum_{n|m} g(m)$ 等价于 $g(n) = \sum_{n|m} \mu\left(\frac{m}{n}\right)f(m)$ ；
 - 证明这个结论，我们需要还是需要利用 $\mathbf{1} * \mu = \mathbf{e}$ 的性质（ M 充分大），这个恒等式非常关键，可能在很多地方都有涉及！

$$\begin{aligned} g(n) &= \sum_{k=1}^M [k=1]g(kn) = \sum_{k=1}^M \sum_{d|k} \mu(d)g(kn) \\ &= \sum_{d=1}^M \mu(d) \sum_{d|k} g(kn) = \sum_{d=1}^M \mu(d)f(dn). \end{aligned}$$

莫比乌斯反演

- 已知所有 $f(n) = \sum_{d|n} g(d)$ ，需要求解 $g(1), g(2), \dots, g(N)$ 。我们可以通过下列简单的算法来求解问题（时间复杂度为 $O(n \log n)$ ）：
 - t 从 1 到 N 循环，当前序列 $f(t)$ 的值即为真实值，将所有 $i \geq 2$ 中 $f(i * t)$ 的值减去 $f(t)$ 即可。
- 对于倍数版本，我们也有类似的做法，这里不再赘述。

例题： $[1, n]$ 中与 m 互素的数的个数

- 求 $[1, n]$ 中与 m 互素的数的个数；
- 100组询问， $m \leq 10^9$ ， $n \leq 10^{18}$ 。

例题： $[1, n]$ 中与 m 互素的数的个数

- 令 $g(i)$ 为 1 到 n 中 $\gcd(x, m) = i$ 的个数，
则 $f(i) = \sum_{i|d} g(d)$ 为 $\gcd(x, m)$ 是 i 的倍数的个数。
- 当 i 是 m 的因子时， $f(i) = \lfloor \frac{n}{i} \rfloor$ ，否则为 0；
- 由莫比乌斯反演，有 $g(1) = \sum_d \mu(d) f(d) = \sum_{d|m} \mu(d) \lfloor \frac{n}{d} \rfloor$
- 可以解读为容斥系数为 $\mu(d)$ 的容斥原理。

例题: Mocha and stars

- 求满足下列条件的正整数序列 $a = [a_1, a_2, \dots, a_n]$ 的个数:
 1. $a_i \in [l_i, r_i]$;
 2. $\sum_{i=1}^n a_i \leq m$;
 3. $\gcd(a_1, a_2, \dots, a_n) = 1$ 。
- $n \leq 50, m \leq 10^5$ 。

例题：Mocha and stars

- 令 $g(i)$ 是gcd为 i 的方案数，则 $f(i) = \sum_{i|d} g(d)$ 为gcd是 i 的倍数的方案数。
- 我们可以在 $O(nm/i)$ 的时间内求解 $f(i)$ 。
- 利用莫比乌斯变换，我们可以在 $O(nm \log m)$ 的时间内求解。

例题：互素对数

- 给定 n 个正整数 x_1, x_2, \dots, x_n ，求有序对 (i, j) 满足 x_i 与 x_j 互素的个数。
- $n \leq 5 \cdot 10^5, 1 \leq x_i \leq 10^6$ 。

例题：互素对数

- 令 c_i 为 x_1, x_2, \dots, x_n 中等于 i 的个数。则

$$\begin{aligned}\sum_{i=1}^m \sum_{j=1}^m c_i c_j [\gcd(i, j) = 1] &= \sum_{1 \leq i, j \leq m} \sum_{d | \gcd(i, j)} \mu(d) c_i c_j \\ &= \sum_d \mu(d) \sum_{i, j} c_{di} c_{dj} \\ &= \sum_d \mu(d) \left(\sum_i c_{di} \right)^2.\end{aligned}$$

- $O(m \log m)$ 的复杂度。

杂谈：数论分块

- 现在考虑求解下列问题：

Problem

$$\sum_{i=1}^n \left\lfloor \frac{n}{i} \right\rfloor.$$

- 数论分块在 $O(\sqrt{n})$ 的时间内来求解上述问题。
 - 令 $B = \sqrt{n}$;
 - 当 $1 \leq i \leq B$ 时，我们暴力求解；
 - 当 $i > B$ 时， $\lfloor \frac{n}{i} \rfloor$ 的取值不超过 B 个。
 - $\lfloor \frac{n}{i} \rfloor = j$ 当且仅当 $j \leq \frac{n}{i} < j+1$ ，即 $\frac{n}{j+1} < i \leq \frac{n}{j}$ ，在此区间段的正整数 i 将贡献 j 的权重。

例题：数论分块

- 给定 $2n$ 个正整数 $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n$ 以及 $L = 2 \cdot 10^9$, 求

$$\sum_{i=1}^n \sum_{j=1}^n f(L, a_i + b_j),$$

其中 $f(L, x) = \sum_{i=1}^L \lfloor \frac{x}{i} \rfloor$.

- $a_i, b_i \leq 10^9, n \leq 1000, 10s$.

例题：数论分块

- 由数论分块可知，给定 $B = \sqrt{L}$,

$$f(L, x) = \sum_{i=1}^B \left\lfloor \frac{x}{i} \right\rfloor + \sum_{i=1}^B \max\left(\left\lfloor \frac{x}{i} \right\rfloor - B, 0\right).$$

- 只需统计 $a_i \bmod m + b_j \bmod m \geq m$ 的对数即可，这可以用数状数组解决。

例题: Josuke and Complete Graph

- 给定 l, r , 求 $\{\gcd(x, y) \mid l \leq x < y \leq r\}$ 的大小。
- $1 \leq l < r \leq 10^{18}$, $l \leq 10^9$, 100组测试。

例题：Josuke and Complete Graph

- gcd分两类考虑：
 1. $g \geq l$ 。此时只需 $2g \leq r$ 即可。
 2. $g < l$ ，此时我们考虑数论分块：
 - $g \leq \sqrt{l}$ ：暴力求解。
 - $g > \sqrt{l}$ ： $\lceil \frac{l}{g} \rceil$ 只有 \sqrt{l} 个可能取值，枚举 $\lceil \frac{l}{g} \rceil$ 取值即可。

杂谈：*亚线性筛

- 这里我们介绍杜教筛。
- 杜教筛的主要思想是利用狄利克雷卷积，将求解函数 f 前缀和的问题变为求解更简单函数前缀和的问题。
- $f * g = h: \sum_{n=1}^N h(n) = \sum_{n=1}^N \sum_{d|n} f(d)g(n/d)$ 。
- $S_h(N) = \sum_{n=1}^N h(n) = \sum_{n=1}^N g(n)S_f(\lfloor \frac{N}{n} \rfloor)$ 。
- 结合整数分块，假设 g 的前缀和易于求解，我们可以在 $\tilde{O}(n^{2/3})$ 的时间内解决。
- 一些简单的积性函数可以通过杜教筛处理：
 - $1 * \mu = id = (1, 0, 0, 0, \dots)$;
 - $1 * \phi = (1, 2, 3, \dots)$ 。

杂谈：*二次剩余

- 给定素数 p ， $1 \leq i < p$ 称为二次剩余，若存在 x 使得 $x^2 \equiv i \pmod{p}$ 。
- 当 $p > 2$ 时，恰有一半的数为二次剩余。
- 你可以将二次剩余的元素 i 所对应的 x 当成 i 在模 p 下开根号的值。

例题： DZY Loves Fibonacci Numbers

- 给一个序列 a_1, a_2, \dots, a_n ，做如下操作：
 1. 区间加斐波那契数列；
 2. 区间求和模 $10^9 + 9$ 。
- $n, q \leq 2 \cdot 10^5$ 。

例题： DZY Loves Fibonacci Numbers

- 斐波那契数列有通项公式 $f_n = C(A^n + B^n)$ ，其中 A, B 中有 $\sqrt{5}$ 这一项难以处理。
- 注意到5是模 $10^9 + 7$ 下的二次剩余，因此我们可以直接找到 $x^2 \equiv 5 \pmod{P}$ 替代 $\sqrt{5}$ 即可。
- 问题转化为区间加定公比的等比数列，可以用线段树解决。