初等数论

张昕渊

September 22, 2023

预备知识

- 模n下的基本算数运算：
  - $((i \mod n) \circ (j \mod n)) = (i \circ j) \mod n$，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

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

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$a^{-1} \in \{1, 2, \ldots, p-1\}$满足$a^{-1}a = 1$。此时$b/a$在模$p$下被定义为$b \cdot a^{-1} \mod p$.
  - 逆元的求解

Theorem (费马小定理)

当a, p互素时，$a^{p-1} \equiv 1 \mod p$。

Proof.

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

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

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

第一小节的内容大纲

- $\{1, 2, ..., p-1\}$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。

$\{1, 2, \ldots, p-1\}$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$a \in \{1, 2, \ldots, p-1\}$，哪一些指数$x$满足如下同余方程?

$$a^x \equiv 1 \mod p$$

$\{1, 2, \ldots, p-1\}$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

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

□

Corollary

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

$\{1, 2, \ldots, p-1\}$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。

$\{1, 2, \ldots, p-1\}$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

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

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

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

$\{1,2,\ldots,p-1\}$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

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

Proof.

令g为p对应的原根，则

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

□

$\{1,2,\ldots,p-1\}$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$\{1,2,\ldots,m\}$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$g^{i_x}\equiv x \mod p$。
- 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$g^{\frac{p-1}{q}} \neq 1 \mod p$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$1 \le a < p$，找到一组下列同余方程的解：

$$a^x \equiv x \mod p.$$

- $p \le 10^9$。

例题：同余方程

- 由费马小定理：当$x \equiv 0 \mod p-1$时，$a^x \equiv 1 \mod p$。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$1 \le x, y < p$，判断方程$x^a \equiv y \mod p$是否有解。
- $p \le 10^{18}$。
- 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$x \equiv g^{i_x} \mod p$，$y \equiv g^{i_y} \mod p$。
- 因此原问题转换为
  - 是否存在$a \in \{0, 1, 2, \ldots, p-2\}$满足$i_x a \equiv i_y \mod (p-1)$。
- 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，$S \subseteq \{0, 1, \ldots, p-1\}$为一集合。对于任意的$c \in \{0, 1, \ldots, p-1\}$，令$S_c = \{(c \cdot x) \mod p \mid x \in S\}$。求$\max_{c \in \{0,1,\ldots,p-1\}} mex(S_c)$，其中$mex(S)$为最小未出现在$S$中的非负整数。
- $1 \le |S| \le p \le 2 \cdot 10^5$。
- 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$c \in \{1, 2, \ldots, p-1\}$，使得$1, 2, \ldots, L$均在$S_c$中。
- 考虑任意的原根g，对于任意的集合S，令$T_S = \{i \in \{0, 1, \ldots, p-2\} \mid \exists j \in S, g^i \equiv j \mod p\}$。则问题转化为
  - 是否存在$c \in \{0, 1, \ldots, p-2\}$，使得

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

  - 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$1 \le a, b < p$，求下述方程的一个解或判定该方程无解:

$$a^x \equiv b \mod p.$$

- 我们下面将给出一个时间复杂度为$\widetilde{O}(\sqrt{p})$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$0 \le x < p-1$的解。
- 令$B = \lceil \sqrt{p} \rceil + 1$，则一定存在$0 \le L, R \le B$使得$x = L \cdot B - R$。
- 此时，方程将转变为求解$0 \le L, R < B$满足

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

- 此步转化用到了$a \not\equiv 0 \mod p$！
- 预处理出$S = \{(a^B)^L \mod p \mid 0 \le L < B\}$的值，对于每个$0 \le R < B$计算出$ba^R \mod p$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$x^a \equiv y \mod p$。
- $p \leq 10^9$。

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$g^{i_x} \equiv x \mod p$，$g^{i_y} \equiv y \mod p$。
- 问题即求解$i_x \cdot a \equiv i_y \mod p$，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$g^{i_x} \equiv x \mod p$，$g^{i_y} \equiv y \mod p$。
- 问题即求解$i_x \cdot a \equiv i_y \mod p$，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，$0 \le A, B, S, G < p$为整数。考虑如下线性递推

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

  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，$p \le 10^9$。
- 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$X_n + C = A(X_{n-1} + C) \mod p$，解得$C = (A-1)^{-1} \cdot B \mod p$;
  - 令$Y_n = (X_n + C) \mod p$，此时$Y_n = A^n \cdot Y_0 \mod p$，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

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

其中$\binom{x}{y} = 0$若$x < y$。

Lucas定理

Theorem (Lucas定理)

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

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$(1+x)^p \equiv 1+x^p \mod p$，因此

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

对比系数即得结果。 $\square$

Lucas定理

Theorem (Lucas定理)

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

- 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$\binom{n}{m} \mod p$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.

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

例题：Number of Binomial Coefficients

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

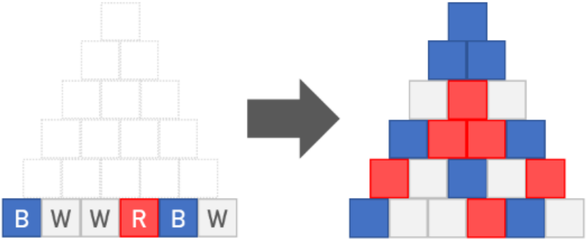
例题：Number of Binomial Coefficients

- 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$\alpha$次，即$n-k$借位至少$\alpha$次。
- 令A在p进制下的展开为$x_1, x_2, \ldots, x_k$，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$-(x+y) \mod 3$。
- 令$x_0, x_1, \ldots, x_N$为底层颜色，则最顶层颜色为$(-1)^N \sum_{i=0}^{N} \binom{N}{i} x_i \mod 3$；
- 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$a = [a_0, a_1, \ldots, a_{n-1}]$，我们可以采用下述操作更新序列：
  - 令$b = [b_0, b_1, \ldots, b_{n-1}]$，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$\bigoplus_{j=0}^{k}\left(\binom{k}{j} \mod 2\right) a_{(i+j) \bmod n}$。
- $k = n$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$\bigoplus_{j \text{ and } k=j} a_{(i+j) \bmod n}$。
- 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。
- $c_i = b_i \oplus b_{(i+2^d) \bmod n}$。

第一小节内容总结

- $\{1, 2, \ldots, p-1\}$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：$a \cdot b \equiv a \cdot \left(b \mod \frac{m}{\gcd(a,m)}\right) \mod m$。
- $a \mid b$且$a \mid c$ 当且仅当$a \mid \gcd(b, c)$；
- $a \mid c$且$b \mid c$当且仅当$\mathrm{lcm}(a, b) \mid c$。

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

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

- 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$\{ax \mod b \mid 0 \le x < b\} = \{0, 1, \ldots, b-1\}$即可，这等价于证明不存在$0 \le x_1 < x_2 < b$满足$ax_1 \equiv ax_2 \mod b$。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。 □

- 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$b \mod a \leq \frac{b}{2}$。
- 拓展欧几里得算法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$[g, x, y] = \mathrm{exgcd}(b \bmod a, a)$，则我们有

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

  - 由$b \mod a = b - \left\lfloor \frac{b}{a} \right\rfloor a$，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exgcd(a,b)（返回gcd(a,b)和x,y，方程$ax+by=\gcd(x,y)$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$ax\equiv c \mod b$的最小非负整数解?
  - 有解当且仅当$\gcd(a,b)\mid c$。
  - x,y为exgcd返回值，则$x_0=\frac{c}{\gcd(a,b)}x, y_0=\frac{c}{\gcd(a,b)}y$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

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

- 考虑$i\to(i+a) \mod b$的有向图，上述其实表明了这一个有向图由$\gcd(a,b)$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$a_1, a_2, \ldots, a_n$的整线性组合的取值集合。即

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

- 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$x_1, x_2, \ldots, x_n$。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$k \in S$。
- $-10^{18} \le k, x_i \le 10^{18}$，$n \le 10^5$。
- 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$\gcd(x_2, x_3, \ldots, x_n)$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$10^{10^{100}}$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;
- 我们首先先考虑所有图G中所有的简单圈$C_1, C_2, \ldots, C_s$，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$\gcd(C_1, C_2, \ldots, C_s) \mid 10^{10^{100}}$。
- 求解$\gcd(C_1, C_2, \ldots, C_s)$:
    - 找一颗任意节点为根的BFS树;
    - 对于所有的非树边$u \to v$，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。
- $|V|,|E|\le 100$，$w_i\le 10^4$，$t\le 10^{18}$.

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$0 \le t_i < m_i$，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。
- $|V|,|E|,q \le 10^5, m_i \le 10^9$。
- 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，

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

其中$\phi(m)$为$1 \le x \le m$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

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

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

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

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 mod 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

```
初始化数组p = []，以及长度为n + 1值全为0的vis数组和φ数组;
for i = 2 to n do
    if vis[i] == 0 then
        p数组末尾加入i;
        φ[i] = i − 1;
    for j = 0 to p.size() - 1 do
        if i ∗ p[j] > n then
            break;
        vis[i ∗ p[j]] = 1;
        if i mod p[j] == 0 then
            φ[i ∗ p[j]] = p[j] ∗ φ[i];
        else
            φ[i ∗ p[j]] = (p[j] − 1) ∗ φ[i];
        if i mod p[j] == 0 then
            break;
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

初始化数组$p = []$，以及长度为$n+1$值全为0的vis数组和μ数组;
for $i = 2$ **to** n **do**
    if $vis[i] == 0$ **then**
        p数组末尾加入i;
        $\mu[i] = -1$;
    for $j = 0$ **to** $p.size()$ - 1 **do**
        if $i * p[j] > n$ **then**
            break;
        $vis[i * p[j]] = 1$;
        if $i \bmod p[j] == 0$ **then**
            $\mu[i * p[j]] = 0$;
        else
            $\mu[i * p[j]] = -\mu[i]$;
        if $i \bmod p[j] == 0$ **then**
            break;
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，$a^x \mod m$需要如何计算?

Theorem

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

Proof.

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

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

由欧拉定理，$a^{x-L} \equiv a^{(x-L) \bmod \phi(m/g)} \mod \frac{m}{g}$。
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$i \to ai \mod m$。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$a = [a_1, a_2, \ldots, a_k]$，令$w(a) = a_1^{a_2^{a_3^{\cdot^{\cdot^{\cdot^{a_k}}}}}} \mod m$。给定序列$b = [b_1, b_2, \ldots, b_n]$，回答$q$个询问$w(b[l:r])$。
- $n, q \le 10^5$，$m \le 10^9$。

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

$$x \equiv x_i \mod m_i,$$

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

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

□

一般模数到素数幂次模数：中国剩余定理

- 令$\phi : [M] \to [m_1] \times [m_2] \times \ldots \times [m_n]$如下

$$\phi(x) = (x \mod m_1, x \mod m_2, \ldots, x \mod m_n),$$

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

例题：Koxia and Number Theory

- 若存在质数p满足对于任意的$0 \le k < p$ 都有$\sum_{i=1}^{n}[a_i \mod p = k] \ge 2$成立，则不存在；否则存在。
- 存在性简单证明：对于每个素数$p \le 10^{18}$，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。
  - $1 \le a, b \le p(p-1)$；
  - $a^b \equiv b^a \mod p$。
- $p \le 10^9$.

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$g^u \equiv a \mod p$, $g^v \equiv b \mod p$，则由费马小定理，方程转化为

$$av \equiv bu \mod p-1.$$

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

$$a \equiv a_0 \mod p-1$$
$$a \equiv g^u \mod p.$$

  由中国剩余定理，存在唯一正整数$1 \le a \le p(p-1)$满足条件。
- 因此，我们只需求出满足$av \equiv bu \mod m$的四元组(a, u, b, v)个数，其中$0 \le a, u, b, v < m$，$m = p-1$

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$av \equiv bu \mod q^k$的四元组(a, u, b, v)的个数，其中$1 \le a, u, b, v \le q^k$。

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：

$$
\begin{aligned}
x &\equiv x_1 \mod m_1 \\
x &\equiv x_2 \mod m_2
\end{aligned}
$$

- 令$g = \gcd(m_1, m_2)$，当$x_1 \not\equiv x_2 \mod g$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

$$
\begin{aligned}
y &\equiv 0 \mod m_1/g \\
y &\equiv (x_2 - x_1)/g \mod m_2/g
\end{aligned}
$$

  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$a^x \equiv x \mod m$。
- $a, m \leq 10^9$。

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。

$$x \equiv a^{x_0} \mod m$$
$$x \equiv x_0 \mod \phi(m)$$

此时，该同余方程组有解当且仅当x_0满足

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

- 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：

$$a^x \equiv b \mod m.$$

- 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$a^{LB-R} \equiv b \mod m$不再等价于$a^{LB} \equiv ba^R \mod m$.
- 解决办法：只考虑$x > C = \log_2 m$的情形。此时同余方程将变为

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

  - 当$g = \gcd(a^C, m) \nmid b$时无解；
  - 否则，同余方程将变为$a^{x-C} a^C / g \equiv b/g \mod m/g$。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$g^x \not\equiv 1 \mod m$.
- 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$5^s * (-1)^t \mod m$, $0 \leq s < 2^{n-2}, t \in \{0, 1\}$.

*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：
  1. 交换律：$f * g = g * f$；
  2. 分配律：$f * (g + h) = f * g + f * h$;
  3. 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: $(1, 0, 0, 0, \ldots)$;
- 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:
  1. 交换律：$f * g = g * f$;
  2. 分配律：$f * (g + h) = f * g + f * h$;
  3. 结合律：$f * (g * h) = (f * g) * h$。
- 单位元: $e = (1, 0, 0, 0, \ldots)$（$e * f = f$）;
- 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$\{1, 2, \ldots, n\}$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$\mathbf{1} * \mu = e$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$g(n) = \sum_{n|m} \mu(\frac{m}{n}) f(m)$；
  - 证明这个结论，我们需要还是需要利用$\mathbf{1} * \mu = e$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$g(1), g(2), \ldots, g(N)$。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，$f(i)=\left\lfloor \frac{n}{i} \right\rfloor$，否则为0；
- 由莫比乌斯反演，有$g(1)=\sum_{d}\mu(d)f(d)=\sum_{d|m}\mu(d)\left\lfloor \frac{n}{d} \right\rfloor$
- 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$a = [a_1, a_2, \ldots, a_n]$的个数:
  1. $a_i \in [l_i, r_i]$;
  2. $\sum_{i=1}^{n} a_i \leq m$;
  3. $\gcd(a_1, a_2, \ldots, a_n) = 1$。
- $n \leq 50$，$m \leq 10^5$。

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$x_1, x_2, \ldots, x_n$，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$x_1, x_2, \ldots, x_n$中等于i的个数。则

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

- $O(m \log m)$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$1 \le i \le B$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$j \le \frac{n}{i} < j+1$，即$\frac{n}{j+1} < i \le \frac{n}{j}$，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$a_1, a_2, \ldots, a_n$，$b_1, b_2, \ldots, b_n$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$B = \sqrt{L}$，

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

- 只需统计$a_i \mod m + b_j \mod m >= m$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$\{\gcd(x, y) | l \le x < y \le r\}$的大小。
- $1 \le l < r \le 10^{18}$, $l \le 10^9$，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：
  - $1 * \mu = id = (1, 0, 0, 0, \ldots)$;
  - $1 * \phi = (1, 2, 3, \ldots)$.

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$x^2 \equiv i \mod p$。
- 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: