数学第二讲
离散对数、元根、反演

丁尧尧

上海交通大学

August 13, 2017

目录

对于以下问题：

Definition (离散对数)

给定 a,b,m，其中 a 与 m 互素，求最小的非负（正）整数 x，使得：

$$a^x \equiv b \pmod m$$

我们称 x 为在模 m 意义下，以 a 为底的 b 的离散对数，记作 $ind_a b$。

对于以下问题：

Definition (离散对数)

给定 a,b,m，其中 a 与 m 互素，求最小的非负（正）整数 x，使得：

$$a^x \equiv b \pmod m$$

我们称 x 为在模 m 意义下，以 a 为底的 b 的离散对数，记作 $ind_a b$。

给出 a, b, m，（我们假设 a 与 m 互素）我们如何求 x 呢？

有一个叫做大步小步的算法（Baby Step Giant Step）。我们假设 $x = ic + j$ 是一个答案（其中 c 是我们自己选定的一个在 $2, m-1$ 之间的数）。我们先计算出：

$$a^0, a^1, a^2, a^3, \cdots, a^{c-1}$$

如果发现其中某个值是 b，那么我们就找到答案了。

有一个叫做大步小步的算法（Baby Step Giant Step）。我们假设 $x = ic + j$ 是一个答案（其中 c 是我们自己选定的一个在 $2, m-1$ 之间的数）。我们先计算出：

$$a^0, a^1, a^2, a^3, \cdots, a^{c-1}$$

如果发现其中某个值是 b，那么我们就找到答案了。
否则，我们将这些数放在一个数据结构中（平衡二叉树，哈希表都可以），要求可以通过 a^i 的值快速得到 i。那么我们再依次算出：

$$ba^{-c}, ba^{-2c}, \cdots, ba^{-kc}$$

有一个叫做大步小步的算法（Baby Step Giant Step）。我们假设 $x = ic + j$ 是一个答案（其中 c 是我们自己选定的一个在 $2, m-1$ 之间的数）。我们先计算出：

$$a^0, a^1, a^2, a^3, \cdots, a^{c-1}$$

如果发现其中某个值是 b，那么我们就找到答案了。
否则，我们将这些数放在一个数据结构中（平衡二叉树，哈希表都可以），要求可以通过 a^i 的值快速得到 i。那么我们再依次算出：

$$ba^{-c}, ba^{-2c}, \cdots, ba^{-kc}$$

每算完一个 ba^{-ic}，我们就看上面的数据结构中是否有一个值 a^j 等于它，如果有，那么它们满足：

$$a^j \equiv ba^{-ic} \pmod m$$

即：

$$a^{ic+j} \equiv b \pmod m$$

分析复杂度，如果我们上面用哈希表存，那么可以 $O(1)$ 判断某个值是否存在。
那么我们总共需要计算的数的个数是 $O(b+\frac{m}{b})$，我们取 $b=\sqrt{m}$，
可以得到 $O(\sqrt{m})$ 的复杂度.

分析复杂度，如果我们上面用哈希表存，那么可以 $O(1)$ 判断某个值是否存在。
那么我们总共需要计算的数的个数是 $O(b+\frac{m}{b})$，我们取 $b=\sqrt{m}$，可以得到 $O(\sqrt{m})$ 的复杂度.
上面的方法，a 不限于整数，还可以是矩阵，但都有同一个要求，即 a 存在乘法逆元.（有方法可以避免求逆元，但是还是要求逆元存在。）

我们先介绍一些概念.

Definition (剩余系)

对于给定模数 $m(m>0)$, 如果有一组数 $\{a_i\}$:

$$a_1, a_2, a_3, \ldots, a_m$$

对于任何数 a, 存在唯一数 a_i 满足:

$$a \equiv a_i \pmod m$$

那么我们将 $\{a_i\}$ 称作模 m 的一组完全剩余系.

类似的有:

Definition (既约剩余系)

对于给定模数 $m(m > 0)$, 如果有一组数 $\{a_i\}$:

$$a_1, a_2, a_3, \ldots, a_k$$

满足:

$$gcd(a_i, m) = 1$$

且对于任何和 m 互质的数 a, 有唯一的 a_i 满足:

$$a \equiv a_i \pmod{m}$$

那么我们将 $\{a_i\}$ 称作模 m 的一组既约剩余系.

类似的有:

Definition (既约剩余系)

对于给定模数 $m(m>0)$, 如果有一组数 $\{a_i\}$:

$$a_1, a_2, a_3, \dots, a_k$$

满足:

$$gcd(a_i, m) = 1$$

且对于任何和 m 互质的数 a, 有唯一的 a_i 满足:

$$a \equiv a_i \pmod m$$

那么我们将 $\{a_i\}$ 称作模 m 的一组既约剩余系.

模 m 的既约剩余系的个数记作 $\varphi(m)$.

Definition (阶)

给定一个与 $m(1 \leq m)$ 互素的 a，则最小的一个满足:

$$a^r \equiv 1 \pmod{m}$$

的正整数 r 叫做 a 模 m 的阶，一般记作 $r = \delta_m(a)$

Definition (阶)

给定一个与 $m(1 \leq m)$ 互素的 a，则最小的一个满足:

$$a^r \equiv 1 \pmod m$$

的正整数 r 叫做 a 模 m 的阶，一般记作 $r = \delta_m(a)$

Definition (元根)

对于模数 m，如果存在一个数 g，满足:

$$\delta_m(g) = \varphi(m)$$

我们则称 g 为模 m 的一个元根

我们知道，如果 a 与 m 互素，那么:

$$a^1, a^2, a^3, \ldots, a^i, \ldots$$

都与 m 互素，即它们都是缩系的元素.

我们知道，如果 a 与 m 互素，那么:

$$a^1, a^2, a^3, \ldots, a^i, \ldots$$

都与 m 互素，即它们都是缩系的元素.
元根的意义在于，将缩系中的每一个元素，都与一个 g^i 这种形式对应起来.
假如我们找到了一个模 m 的元根 g，想求其缩系中的一个元素 a 对应的指数是什么，我们就可以用离散对数找到满足:

$$g^i \equiv a \pmod{m}$$

的 i.

并不是所有数都有元根.

Theorem

只有形如:

$$1, 2, 4, p^\alpha, 2p^\alpha$$

的数存在元根 (其中 $\alpha \geq 1$ 且 p 是奇素数).

并不是所有数都有元根.

Theorem

只有形如:

$$1, 2, 4, p^\alpha, 2p^\alpha$$

的数存在元根 (其中 $\alpha \geq 1$ 且 p 是奇素数).

那么我们怎样找元根呢?

并不是所有数都有元根.

Theorem

只有形如:

$$1, 2, 4, p^{\alpha}, 2p^{\alpha}$$

的数存在元根 (其中 $\alpha \geq 1$ 且 p 是奇素数).

那么我们怎样找元根呢?

Theorem

如果存在正数 a, b, m, 且 $gcd(a, m) = 1$, 满足

$$a^{b} \equiv 1 \pmod{m}$$

那么有:

$$\delta_m(a) \mid b$$

通过上面这个定理可以证明:

Theorem

对于给定的与 $m \geq 2$ 互素的一个数 g, g 是 m 的一个元根当且仅当对于 $\varphi(m)$ 的所有素因子 p_i, 有:

$$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod m$$

通过上面这个定理可以证明:

Theorem

对于给定的与 $m \geq 2$ 互素的一个数 g, g 是 m 的一个元根当且仅当对于 $\varphi(m)$ 的所有素因子 p_i, 有:

$$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod m$$

因为在 10^9 范围内的所有素数的最小的元根都很小 (最大的不过一百多), 所以我们可以暴力从小到大 check.

我们来道例题看看:

例题 1

给你 a, b, m, 都是正整数, 其中 m 是素数, 求:

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

其中:$2 \leq m \leq 2 \times 10^9$,$1 \leq a, b < m$

我们来道例题看看:

例题 1

给你 a, b, m, 都是正整数, 其中 m 是素数, 求:

$$a^x \equiv b \pmod m$$

其中:$2 \leq m \leq 2 \times 10^9$,$1 \leq a, b < m$

很容易离散对数就可以秒了对不对.

例题 2

给你 a_1, b_1, a_2, b_2, m，都是正整数，其中 m 是素数，求满足下面条件的 x:

$$a_i^x \equiv b_i \pmod m \quad (i = 1, 2)$$

其中:$2 \leq m \leq 2 \times 10^9$ 且 $1 \leq a_i, b_i < m$.

先找到 m 的一个元根, 然后找到 a_i 和 b_i 的离散对数:

$$g^{c_i} \equiv a_i \quad (mod\ m)$$

$$g^{d_i} \equiv b_i \quad (mod\ m)$$

先找到 m 的一个元根，然后找到 a_i 和 b_i 的离散对数:

$$g^{c_i} \equiv a_i \pmod{m}$$

$$g^{d_i} \equiv b_i \pmod{m}$$

然后就把问题化简成了:

$$g^{xc_i} \equiv g^{d_i} \pmod{m}$$

因为 g 是模 m 的元根，所以上面的方程等价于:

$$xc_i \equiv d_i \pmod{m-1}$$

先找到 m 的一个元根, 然后找到 a_i 和 b_i 的离散对数:

$$g^{c_i} \equiv a_i \pmod{m}$$

$$g^{d_i} \equiv b_i \pmod{m}$$

然后就把问题化简成了:

$$g^{xc_i} \equiv g^{d_i} \pmod{m}$$

因为 g 是模 m 的元根, 所以上面的方程等价于:

$$xc_i \equiv d_i \pmod{m-1}$$

从而把问题转化为解一元一次同余方程组的问题.

例题 3

给你三个正整数 a, b, m, 其中 m 是质数, 求 x 满足:

$$x^a \equiv b \pmod m$$

其中:$1 \leq x, b < m$

例题 3

给你三个正整数 a, b, m, 其中 m 是质数, 求 x 满足:

$$x^a \equiv b \pmod m$$

其中:$1 \leq x, b < m$

同样先求离散对数, 然后解一次方程, 得到 $ind_g(x)$, 最后快速幂一下就行了.

元根，离散对数，主要的作用是把一些和指数有关的问题转化成一般的一次同余方程，类似于正实数上的开 log 运算.
只是在模意义下，我们的底需要精细地选取.

Definition (数论函数)

定义域是正整数，值域为复数域的函数是数论函数。

有这样一个问题：

问题

存在一个数论函数 $f(n)$，由它可以产生一个数论函数：

$$F(n) = \sum_{d|n} f(d)$$

假如我们知道 $F(n)$，怎样求得 $f(n)$ 呢？

请大家先自行解决这个问题 (提示：容斥原理)

因为我们要的是一个普适的规律，所以我们把 $f(i)$ 看成一个个独立的元素，而把 $F(n)$ 看成某些 $f(i)$ 构成的集合。（比如： $F(9)=\{f(1),f(3),f(9)\}$）。我们发现， $F(n)$ 中包含了 $f(n)$，所以我们可以尝试用把 $F(n)$ 中多加的元素去掉，来得到 $f(n)$。

因为我们要的是一个普适的规律，所以我们把 $f(i)$ 看成一个个独立的元素，而把 $F(n)$ 看成某些 $f(i)$ 构成的集合。(比如：$F(9)=\{f(1),f(3),f(9)\}$)。
我们发现，$F(n)$ 中包含了 $f(n)$，所以我们可以尝试用把 $F(n)$ 中多加的元素去掉，来得到 $f(n)$。
我们来看看 $F(n)$ 包含了哪些元素。
设 $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$，那么 $F(n)$ 包含的元素就是

$$F(n)=\{f(d)\mid d=p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k},0\le b_i\le a_i\}$$

因为我们要的是一个普适的规律，所以我们把 $f(i)$ 看成一个个独立的元素，而把 $F(n)$ 看成某些 $f(i)$ 构成的集合。（比如： $F(9)=\{f(1),f(3),f(9)\}$）。
我们发现，$F(n)$ 中包含了 $f(n)$，所以我们可以尝试用把 $F(n)$ 中多加的元素去掉，来得到 $f(n)$。
我们来看看 $F(n)$ 包含了哪些元素。
设 $n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$，那么 $F(n)$ 包含的元素就是

$$F(n)=\{f(d)\mid d=p_1^{b_1}p_2^{b_2}\cdots p_k^{b_k},0\le b_i\le a_i\}$$

我们的目标是得到 $\{f(n)\}$（不妨用 $f(n)$ 来表示这个集合）。

考虑用容斥原理来解决这个问题。思考后我们发现，有：

$$f(n) = F(n) - \bigcup_{p_i|n} F(\frac{n}{p_i})$$

考虑用容斥原理来解决这个问题。思考后我们发现，有:

$$f(n) = F(n) - \bigcup_{p_i|n} F(\frac{n}{p_i})$$

用容斥原理，我们可以把后面那个求并打开（注意，下面我们把集合理解成可重集，运算 $+$ 就是把两个集合的元素放在一起，不去重，运算 $-$ 指去掉后面那个集合的元素，后面有几个去几个，交和并还是要去重）:

$$f(n) = F(n) - F(\frac{n}{p_1}) - F(\frac{n}{p_2}) - \cdots + F(\frac{n}{p_1}) \cap F(\frac{n}{p_2}) \cdots - \cdots$$

考虑用容斥原理来解决这个问题。思考后我们发现，有:

$$f(n) = F(n) - \bigcup_{p_i|n} F(\frac{n}{p_i})$$

用容斥原理，我们可以把后面那个求并打开（注意，下面我们把集合理解成可重集，运算 $+$ 就是把两个集合的元素放在一起，不去重，运算 $-$ 指去掉后面那个集合的元素，后面有几个去几个，交和并还是要去重）:

$$f(n) = F(n) - F(\frac{n}{p_1}) - F(\frac{n}{p_2}) - \cdots + F(\frac{n}{p_1}) \cap F(\frac{n}{p_2}) \cdots - \cdots$$

我们有:

$$F(\frac{n}{p_1}) \cap F(\frac{n}{p_2}) = F(\frac{n}{p_1 p_2})$$

替换后，我们两边求个和（下面就是代表的数值而不是集合了）:

$$f(n) = F(n) - F(\frac{n}{p_1}) - \cdots + F(\frac{n}{p_1 p_2}) + \cdots - F(\frac{n}{p_1 p_2 p_3}) - \cdots$$

我们发现，$f(n)$ 可以用一些 $F(d)$ 来表示，且 $d \mid n$。
如果 $\frac{n}{d}$ 不是一些素数单个乘起来，那么 $F(d)$ 就不出现在我们的结果里。
否则，$\frac{n}{d}$ 的素因子个数决定了 $F(d)$ 前的系数，奇数个为负，偶数个为正。

我们发现，$f(n)$ 可以用一些 $F(d)$ 来表示，且 $d \mid n$。
如果 $\frac{n}{d}$ 不是一些素数单个乘起来，那么 $F(d)$ 就不出现在我们的结果里。
否则，$\frac{n}{d}$ 的素因子个数决定了 $F(d)$ 前的系数，奇数个为负，偶数个为正。
举个例子：$f(12) = F(12) - F(6) - F(4) + F(2)$。

莫比乌斯函数

Definition (莫比乌斯函数)

假如正整数有如下质因数分解： $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$，那么有：

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & a_i = 1 \\ 0 & \text{某个 } a_i > 1 \end{cases}$$

莫比乌斯函数

Definition (莫比乌斯函数)

假如正整数有如下质因数分解：$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$，那么有：

$$\mu(n) = \begin{cases} 1 & n = 1 \\ (-1)^k & a_i = 1 \\ 0 & \text{某个 } a_i > 1 \end{cases}$$

我们发现，这个函数就是我们上面所说的系数。通过这个函数，我们就可以把我们上面得到的结果表示成：

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

由上面的讨论，我们发现莫比乌斯函数本质就是处理关于" 质因子" 容斥时的系数，所以它的用处不光用于反演。

由上面的讨论，我们发现莫比乌斯函数本质就是处理关于" 质因子" 容斥时的系数，所以它的用处不光用于反演。

思考

现在有一些范围在 $[1, n]$ 中的整数，已知他们中是 d 的倍数的数有 $F(d)$ 个，求 $f(d)$，表示等于 d 的个数。
给你 $F(1), F(2), \cdots, F(n)$，
需要你求 $f(1), f(2), \cdots, f(n)$。（假如你有能力 $O(n)$ 求出 $\mu(1), \mu(2), \cdots, \mu(n)$）。

由上面的讨论，我们发现莫比乌斯函数本质就是处理关于" 质因子" 容斥时的系数，所以它的用处不光用于反演。

思考

现在有一些范围在 $[1, n]$ 中的整数，已知他们中是 d 的倍数的数有 $F(d)$ 个，求 $f(d)$，表示等于 d 的个数。
给你 $F(1), F(2), \cdots, F(n)$，
需要你求 $f(1), f(2), \cdots, f(n)$。(假如你有能力 $O(n)$ 求出 $\mu(1), \mu(2), \cdots, \mu(n)$)。

有 $O(nlogn)$ 做法吗？

由上面的讨论，我们发现莫比乌斯函数本质就是处理关于" 质因子" 容斥时的系数，所以它的用处不光用于反演。

思考

现在有一些范围在 $[1, n]$ 中的整数，已知他们中是 d 的倍数的数有 $F(d)$ 个，求 $f(d)$，表示等于 d 的个数。
给你 $F(1), F(2), \cdots, F(n)$，
需要你求 $f(1), f(2), \cdots, f(n)$。(假如你有能力 $O(n)$ 求出 $\mu(1), \mu(2), \cdots, \mu(n)$)。

有 $O(nlogn)$ 做法吗？
有 $O(n)$ 做法吗？

莫比乌斯函数有一个很重要的性质：

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

其中 $[n == 1]$ 是一个关于 n 的函数，n 为 1 时它是 1，否则它为 0。

莫比乌斯函数有一个很重要的性质：

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

其中 $[n == 1]$ 是一个关于 n 的函数，n 为 1 时它是 1，否则它为 0。证明很简单，大家思考一下。

莫比乌斯函数有一个很重要的性质:

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

其中 $[n == 1]$ 是一个关于 n 的函数，n 为 1 时它是 1，否则它为 0。
证明很简单，大家思考一下。
这个公式是我们推反演的时候经常使用的。

我们进入正题。

Theorem (莫比乌斯反演公式)

设 $f(n)$ 为一个数论函数，我们定义:

$$F(n) = \sum_{d|n} f(d)$$

那么有:

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

这个公式我们上面已经证明过了。但运用上面那个莫比乌斯函数的性质有个更简洁的证明：

$$\sum_{d|n}\mu(d)F(\frac{n}{d}) = \sum_{d|n}\mu(d)\sum_{c|\frac{n}{d}}f(c) \tag{1}$$

$$= \sum_{c|n}f(c)\sum_{d|\frac{n}{c}}\mu(d) \tag{2}$$

$$= \sum_{c|n}f(c)[n == c] \tag{3}$$

$$= f(n) \tag{4}$$

证毕。

这个公式我们上面已经证明过了。但运用上面那个莫比乌斯函数的性质有个更简洁的证明：

$$\sum_{d|n}\mu(d)F(\frac{n}{d}) = \sum_{d|n}\mu(d)\sum_{c|\frac{n}{d}}f(c) \tag{1}$$

$$= \sum_{c|n}f(c)\sum_{d|\frac{n}{c}}\mu(d) \tag{2}$$

$$= \sum_{c|n}f(c)[n == c] \tag{3}$$

$$= f(n) \tag{4}$$

证毕。
注意，上面那两个公式本质是可以互推的，上推下已经完成，请自己下来推一推下推上。

另一种形式

莫比乌斯反演还有一种形式:

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

另一种形式

莫比乌斯反演还有一种形式：

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

证明和上面类似，请自己下来推一推。

积性函数

Definition (积性函数)

一个数论函数 $f(n)$ 是积性的，当且仅当：

$$f(ab) = f(a)f(b) \quad (\text{当 } gcd(a,b) = 1 \text{ 时})$$

如果连互质都不需要，那么我们就叫它完全积性函数。

积性函数

Definition (积性函数)

一个数论函数 $f(n)$ 是积性的，当且仅当：

$$f(ab) = f(a)f(b) \quad (\text{当 } gcd(a,b) = 1 \text{ 时})$$

如果连互质都不需要，那么我们就叫它完全积性函数。

常见的完全积性函数：

$$f(n) = n^a (a \geq 1) \tag{5}$$

$$f(n) = 1 \tag{6}$$

积性函数

Definition (积性函数)

一个数论函数 $f(n)$ 是积性的，当且仅当：

$$f(ab) = f(a)f(b) \quad (\text{当 } gcd(a,b) = 1 \text{ 时})$$

如果连互质都不需要，那么我们就叫它完全积性函数。

常见的完全积性函数：

$$f(n) = n^a (a \geq 1) \tag{5}$$
$$f(n) = 1 \tag{6}$$

常见的积性函数：

$$\mu(n), \eta(n)((\text{约数个数})), \sigma(n)(\text{约数和}), \varphi(n)$$

积性函数有些"生成规则":
如果 $f(n)$ 和 $g(n)$ 是积性的，那么:

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

都是积性的。

积性函数有些" 生成规则" :
如果 $f(n)$ 和 $g(n)$ 是积性的，那么 :

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

都是积性的。
大家应该会线性筛求积性函数吧。

我们来做题吧

例一

求欧拉函数：$\varphi(n)$ 的值（$n \le 10^7$）

例二

给你 $n, m(n, m \leq 10^7)$，求在 $[1, m]$ 中与 n 互质的数的个数。

例三

给你 $n, m(n, m \leq 10^7)$，求在 $[1, m]$ 中与 n 互质的数的和，模 10^9+7。

例三

给你 $n, m(n, m \leq 10^7)$，求在 $[1, m]$ 中与 n 互质的数的和，模 $10^9 + 7$。

改成 k 次方的和呢？$(0 \leq k \leq 1000)$

例四

给你 $n, m(n, m \leq 10^7)$，求在 $[1, m]$ 中的每个数与 n 的最大公约数的和。

例五

给你 $n, m(n, m \leq 10^7)$，求满足 $1 \leq i \leq n, 1 \leq j \leq m, gcd(i, j) = 1$ 的二元组 (i, j) 的对数。

例六

给你 $n, m(n, m \leq 10^7)$，所有满足 $1 \leq i \leq n, 1 \leq j \leq m, gcd(i, j) = 1$ 的二元组 (i, j) 对答案的贡献为 ij，求最终答案（模 $10^9 + 7$）。

例七

给你 $n, m(n, m \leq 10^7)$，所有满足 $1 \leq i \leq n, 1 \leq j \leq m$ 的二元组 (i, j) 对答案的贡献为 $gcd(i, j)$，求最终答案（模 $10^9 + 7$）。

例八

给你 $n, m(n, m \le 10^7)$，所有满足 $1 \le i \le n, 1 \le j \le m$ 的二元组 (i, j) 对答案的贡献为 $\sigma(gcd(i, j))$，求最终答案（模 $10^9 + 7$）。

例九

给你 $n, m(n, m \le 10^7)$，所有满足 $1 \le i \le n, 1 \le j \le m$ 的二元组 (i, j) 对答案的贡献为 $lcm(i, j)$，求最终答案（模 $10^9 + 7$）。