「学习总结」整数模 n 乘法群

Jiayi Su (ShuYuMo)

2021-02-18 08:29:14

对于 任意 一个正整数 n ，$1 \sim n$ 中与 n 互质的 $\varphi(n)$ 个数字组成的集合记作 $\mathbb{Z}_n^*$。

事实上，由 $\mathbb{Z}_n^*$ 和模 n 意义下的乘法组成的代数系统 $(\mathbb{Z}_n^*, \times)$ 是一个群。

从这一点出发理解原根和阶往往有很多奇妙的感受…

几点补充

欧拉函数

$n = \prod p_i^{e_i}$

$$\varphi(n) = \prod p_i^{e_i - 1}(p_i - 1)$$

欧拉函数是一个经典的积性函数。

群的直积

又名 笛卡尔（**Descartes**）积，其定义如下：

设 $(G_1, *) \times (G_2, \cdot) = (G, \oplus)$

其中

- $\times$ 为两个群的笛卡尔积。
- $G = \{(a, b) \mid a \in G_1, b \in G_2\}$
- $\oplus$ 定义为 $(a_1, b_1) \oplus (a_2, b_2) = (a_1 * a_2, b_1 \cdot b_2)$

原根

若 g 为 n 的原根，等价于 $g \perp n, g^0 \sim g^{\varphi(n)-1} \mod n$ 互不相同，等价于 $g \perp n,\ \forall i \in [1, \varphi(n) - 1], g^i \neq 1.$ （$x \perp y$ 表示 x, y 互质）

一个数 n 有原根当且仅当 $n = 2, 4, p^k, 2p^k$ 其中 p 为奇素数。

小结论：若一个正整数 n 有原根，则其原根数量恰好为 $\varphi(\varphi(n))$ 。

阶

若 $a \perp n$，则使 $a^k \equiv 1 \pmod n$ 成立的 最小 正整数 k，称为 a 模 n 意义下的阶，记作 $\mathrm{ord}_n(a)$。可以发现若 g 为模 n 意义下原根，那么 $\mathrm{ord}_n(g) = \varphi(n)$。

整数模 n 乘法群

定义

对于 任意 一个正整数 n ，$1\sim n$ 中与 n 互质的 $\varphi(n)$ 个数字组成的集合记作 $\mathbb{Z}_n^*$。

事实上，由 $\mathbb{Z}_n^*$ 和模 n 意义下的乘法组成的代数系统 $(\mathbb{Z}_n^*,\times)$ 是一个群。

这一点可以考虑 $\mathbb{Z}_n^*$ 中元素所包含的质因子，可以发现是显然的。

因为任意一个处于 n 的剩余系中且不与 n 互质的元素 x ，都可以除掉 $\gcd(x,n)$ 放到 $\frac{n}{\gcd(n,x)}$ 的剩余系内考虑，所以这里只讨论 n 的剩余系中与 n 互质的元素组成的集合，即 $\mathbb{Z}_n^*$ （称其为 n 的简化剩余系），当然也因为 ~~我不会~~ $\mathbb{Z}_n^*$ 的性质实在是太美了。

离散对数

若 n 存在原根，取任意一个 n 的原根 g ，则对于 $\mathbb{Z}_n^*$ 中的一个每个元素 x ，都存在唯一的 $k\in[0,\varphi(n)-1]$ ，使得 $g^k=x$ 。

可以得出 $[0,\varphi(n)-1]\cap\mathbb{Z}$ 中的元素与 $\mathbb{Z}_n^*$ 中的元素之间一一对应。

可以建立函数 $f(x)$ 表示 $\mathbb{Z}_n^*$ 向 $[0,\varphi(n)-1]\cap\mathbb{Z}$ 的映射。可以形象的称 $f(x)$ 为 离散对数。这里满足很多实数定义下对数的性质。需要注意离散对数间的运算是定义在 $\mod\varphi(n)$ 意义下的。

原根不存在的剩余系下离散对数的定义

离散对数的取值依赖于原根的选取，所以只有 n 存在原根时，$\mathbb{Z}_n^*$ 中的元素才存在 直接的 的离散对数。

可以利用类似于中国剩余定理的一般思想，将 n 分解为质数幂的形式，分别求出 x 在每个 p_i^k 剩余系下的离散对数 a_i ，则可以用 $(a_0,a_1,a_2,\cdots)$ 这样的“坐标”来类似地定义 x 在 n 剩余系下的“离散对数”。根据中国剩余定理，可以发现这样的“坐标”是能够实现和原数一一对应的。

可以先考虑原根存在的 $\mathbb{Z}_n^*$ ，对 $\mathbb{Z}_n^*$ 中的每一个元素取离散对数（不妨设这里的原根取最小的原根）放入一个集合 G ，然后重新定义群 乘法运算为模 $\varphi(n)$ 意义下的 加法，这样 $(G,\times)$ 也能够形成一个群。不妨用 G_n 来表示这个群。

类似地定义原根不存在的 $\mathbb{Z}_m^*$，设 $m=\prod\limits_{i=1}^{s}P_i^{e_i}$ 。

他们的“离散对数”形成的群可以表示为 $G_{P_1^{e_1}}\times G_{P_2^{e_2}}\times G_{P_3^{e_3}}\times\cdots\times G_{P_s^{e_s}}$ ，其中 $\times$ 为定义在群上的直积。

值得一提的是：可以发现，两个群做直积，得到的群的阶为之前两个群的阶的乘积，可以发现，这和欧拉函数的积性是相符的。

这好像没有什么用，只是可以帮助理解或者得到一些小结论吧。

模 $2^k(k>2)$ 意义下的离散对数

注意到，$2^k(k>2)$ 也是没有原根的。

定义 $2^k(k>2)$ 意义下的“离散对数”需要如下两个结论

$$\mathrm{ord}_{2^k}(5)=2^{k-2}$$

而且对于任意一个 2^k 的简化剩余系下能表示成形如 5^α 的元素 x，$-x$ 一定不能表示成形如 5^α 的元素。

一个栗子

当 $k=4$ 时，即 $16=2^4$。

$\mathbb{Z}_{16}^*=\{1,3,5,7,9,11,13,15\}$

$5^0 = 1, 5^1 = 5, 5^2 = 9, 5^3 = 13, 5^4 = 1$

$\mathrm{ord}_{16}(5) = 4 = 2^{k-2} = 2^2$

且 $-1 \equiv 15, -5 \equiv 11, -9 \equiv 7, -15 \equiv 2$ 这些数字都没有在上面出现过。

简单来说就是 2^k 的简化剩余系下（大小为 2^{k-1}），有恰好一半的数字可以表示成 $5^\alpha \mod 2^k$，恰好一半不可以，这两部分元素一一对应，互为剩余系下的相反数。

所以，可以把模 $2^k (k > 2)$ 意义下的循环群看成是两个原根为 5 和 -1 的乘法群的直积。

其中的元素 x 的离散对数形如 (a, b) 表示 $5^a \times (-1)^b$ 。

从乘法群的角度考虑原根和阶

对于任意正整数 n ，n 的简化剩余系中的取任意一个数字 x 。

设 $S_x = \{x^0, x^1, x^2, \cdots\}$ ，可以发现如果定义集合 S 的乘法运算为模 n 意义下的乘法，那么这东西就是 $(\mathbb{Z}_n^*, \times)$ 的一个子群…这里 $|S_x|$ （群 $(S_x, \times)$ 的阶）就可以称为 x 在模 n 意义下的阶。

把剩余系的环和群的环结合着理解一下，可以发现这个定义和原先的定义是等价的。

根据这个东西，不难发现：

$$|S_x| = \frac{\varphi(n)}{\gcd(f(x), \varphi(n))}$$

这里的 $f(x)$ 为 x 在任意原根意义下的离散对数。

存在一个显然的事实：一个常数 x 的所有倍数模 m 能够取到所有形如 $k \cdot \gcd(x, m)$ 的数（$k \in \mathbb{Z}^*$ ）。

从 n 的某个原根意义下离散对数的角度考虑，S_x 可以看作“所有离散对数为 $\gcd(f(x), \varphi(n))$ 的倍数的元素”组成的集合，这样的数字显然有 $\frac{\varphi(n)}{\gcd(f(x), \varphi(n))}$ 个，也就是循环子群的阶数。

之后的问题中，如果不好考虑某个引理，可以转化为选取一个原根后，对每个元素，求其离散对数，然后扔到一个剩余系环上考虑。即使是关于原根本身的引理，也可以用这样的方法证明。

可以发现，我们想要的原根 x，满足 x 的循环子群能够取遍原来群中所有元素，即 $f(x) \perp \varphi(n)$ 。

考虑一下原根的数量，对于任意一个正整数 n ，其简化剩余系阶为 $\varphi(n)$ ，每个数字取离散对数，指数和 $\varphi(n)$ 互质的即可成为原根，这样的数字有 $\varphi(\varphi(n))$ 个。事实上，这是原根数量的精确值。

对于 任意 一个正整数 n ，若其剩余系存在原根，则原根数恰好为 $\varphi(\varphi(n))$.

实现上的相关问题

什么求原根、求阶和求离散对数之类的人间烟火，可以查看 「学习总结」数论

相关栗题

debris

给定素数 P，求满足 $1 \le n, m \le P(P-1)$ 且 $n^m \equiv m^n \pmod P$ 的数对 (n, m) 个数。

答案对素数 M 取模。数据组数 $T \le 100, P \le 10^{12}, M \le 10^9$

如果 n, m 一个为 P 的倍数，另一个不是，那么显然这些方案都不合法。

分两种情况：

如果 n, m 都是 P 的倍数，那么这一部分的贡献是平凡的，就是 $(P-1)^2$。

如果 n, m 都不是 P 的倍数，可以取其离散对数：

$$
\begin{aligned}
& n^m \equiv m^n \pmod P \\
\Rightarrow\ & g^{am} \equiv g^{bn} \pmod P \\
\Rightarrow\ & am \equiv bn \pmod{\varphi(P)} \\
\Rightarrow\ & ad \equiv bc \pmod{P-1}
\end{aligned}
$$

定义 $n=(a,c), m=(b,d)$。任何一个数字 n,m 都可以用形如 (x,y) 的数对表示。

同时 $\forall x,y\in[0,P-2]$ (x,y) 的数对都唯一的对应一个在 $[1,P(P-1)]$ 的数字。

原式化简：

$$
\begin{aligned}
& n^m \equiv m^n \pmod P \\
\Rightarrow\ & g^{am} \equiv g^{bn} \pmod P \\
\Rightarrow\ & am \equiv bn \pmod{\varphi(P)} \\
\Rightarrow\ & ad \equiv bc \pmod{P-1}
\end{aligned}
$$

问题转化为：

若 a,b,c,d 可以在 $[0,P-1)$ 内任取，方程 $ad\equiv bc \pmod{P-1}$ 的解 (a,b,c,d) 的数量。

根据乘法群的理论，把 $(\mathbb{Z}^*_{P-1},\times)$ 拆分成多个 p^k 的群的直积。“坐标”每一维行为独立。

分别求出每一个 $ad\equiv bc \pmod{p^k}$ 的解数量相乘即可。

考虑如何求出形如 $ab\equiv bc \pmod{p^k}$ 的方程解数量。

仍然可以分两种情况：

- 方程两边都与 p 互质，这样答案也是平凡的可以考虑其中三个数字任取，然后最后一个数字算逆元即可，答案就是 $\varphi(p^k)^3$ 。
- 方程两边与 p 不互质，可以考虑方程一边的取值个数，考虑枚举 a,b 中 p 的次数，同时除去这个值，转化为互质的情况。需要注意如果其次数和大于 p^k 两边 p 的幂次没必要相等。

子

求 $x^k \bmod m$ (x 为非负整数) 的不同值个数，答案对 10^9+7 取模。

$m=\prod\limits_{i=1}^{m_s} p_i^{a_i}$

$k=\prod\limits_{i=1}^{k_s} q_i^{b_i}$

$m_s,k_s\le 2\times 10^5, p_i,q_i\le 10^7, 1\le a_i,b_i\le 10^9$

下辈子再学。

小 **A** 与两位神仙

给定一个奇质数次幂 m。

n 组询问，每组给定 (x,y) 满足 $x\perp m, y\perp m$

判定是否存在 $x^a\equiv y \pmod m$

$n\le 2\times 10^4, m\le 10^{18}$

显然求离散对数非常舒服，直接算倍数即可。只可惜 m 有亿点点大。

但是可以通过离散对数考虑，设 u, v 分别为 x, y 的离散对数。

显然我们希望：

$$t \in \mathbb{Z} \quad \text{s.t.} \quad ut = v \pmod{\varphi(m)}$$

即：

$$\gcd(u, \varphi(m)) | v$$

其等价于：

$$\gcd(u, \varphi(m)) | \gcd(v, \varphi(m))$$

由上面乘法群的推论：

$$|S_x| = \frac{\varphi(m)}{\gcd(\varphi(m), f(x))}$$

于是可以转化为：

$$\frac{\varphi(m)}{|S_x|} \mid \frac{\varphi(m)}{|S_y|}$$

即：

$$|S_y| \quad | \quad |S_x|$$

所以只需要对原数 x, y 分别求阶，然后判断 $\text{ord}_m(y) | \text{ord}_m(x)$ 即可。