# 第五章 原根与指标

2024年12月12日 星期四 17:09

定义 5.1.1

设 $m>1$, $m\in\mathbb{Z}$, $a$ 是与 $m$ 互素的正整数

则使 $a^e\equiv 1 \pmod m$ 成立的最小正整数 $e$ 叫做 $a$ 对模 $m$ 的指数，记作 $\operatorname{ord}_m(a)$

$\operatorname{ord}_m(a)=e$ (类比 $a^x=m$, $x=\log_m a$)

如果 $a$ 对 $m$ 的指数是 $\varphi(m)$，则 $a$ 叫作模 $m$ 的原根

$\operatorname{ord}_m(a)=\varphi(m)$ $a$ 为原根

定理 5.1.1

设 $m>1$ 是整数，$a$ 是与 $m$ 互素的整数，则整数 $d$ 使

$a^d\equiv 1 \pmod m$ 的充要条件是 $\operatorname{ord}_m(a)\mid d$

证明: $\Leftarrow$: 若 $\operatorname{ord}_m(a)\mid d$ 成立

则 $\exists q$ 使 $d=q\cdot\operatorname{ord}_m(a)$

$\therefore a^d=[a^{\operatorname{ord}_m(a)}]^q\equiv 1 \pmod m$

$\Rightarrow$: 若 $a^d\equiv 1 \pmod m$ 且 $\operatorname{ord}_m(a)\mid d$ 不成立

则 $d=q\cdot\operatorname{ord}_m(a)+r$ $(0<r<\operatorname{ord}_m(a))$

$a^r=[a^{\operatorname{ord}_m(a)}]^q\cdot a^r=a^d\equiv 1 \pmod m$

与 $\operatorname{ord}_m(a)$ 的最小性矛盾

推论 1. 设 $m>1$, $m\in\mathbb{Z}$, $a$ 与 $m$ 互素，则

$\operatorname{ord}_m(a)\mid\varphi(m)$

推论 2. 设 $p$ 是奇素数，$\frac{p-1}{2}$ 也是素数，若 $a$ 模 $p$ 不为 0, 1, -1,

则 $\operatorname{ord}_p(a)=\frac{p-1}{2}$ 或 $p-1$

性质 5.1.1

设 $m>1$, $m\in\mathbb{Z}$, $a$ 与 $m$ 互素

(1) 若 $b\equiv a \pmod m$，则 $\operatorname{ord}_m(b)=\operatorname{ord}_m(a)$

(2) 设 $a^{-1}$ 使 $a^{-1}\cdot a\equiv 1 \pmod m$，则 $\operatorname{ord}_m(a^{-1})=\operatorname{ord}_m(a)$

定理 5.1.2

设 $m>1$, $m\in\mathbb{Z}$, $a$ 与 $m$ 互素，则

$1=a^0, a, \cdots a^{\operatorname{ord}_m(a)-1}$

模 $m$ 两两不同余.

当 $a$ 是模 $m$ 的原根，即 $\operatorname{ord}_m(a)=\varphi(m)$ 时，这 $\varphi(m)$ 个数

$1=a^0, a, \cdots, a^{\operatorname{ord}_m(a)-1}$ 组成模 $m$ 的简化剩余系