信息安全数学基础

1 原根与指标

1.1 原根

定义 1.1 (指数)**.** 设 $m \in \mathbb{Z}, m > 1, a \perp m$, 称使得

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

的最小正整数 e 为 a 模 m 的**指数** (阶), 记为 $\mathrm{ord}_m(a)$

定义 1.2 (原根)**.** 若 $\mathrm{ord}_m(a) = \varphi(m)$, 则 a 称为 m 的**原根**.

定理 1.1. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 整数 d 满足 $a^d \equiv 1 \pmod m \iff \mathrm{ord}_m(a) \mid d$.

根据这个定理, 指数一定是 $\varphi(m)$ 的因子, 只需要在这些数里面找就行了.

定理 1.2. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 如果 $n \mid m$, 则 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

定理 1.3. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 如果 $a \equiv b \pmod m$, 则 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

定理 1.4. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 如果 $ab \equiv 1 \pmod m$, 则 $\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.

定理 1.5. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. 则

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

模 m 互不同余.

如果恰好 $\mathrm{ord}_m(a) = \varphi(m)$, 则 $a^0, a^1, \cdots, a^{\mathrm{ord}_m(a)-1}$ 构成一个简化剩余系.

定理 1.6. 设 $m \in \mathbb{Z}(m > 1), a \perp m$. $a^k \equiv a^l \pmod m \iff k \equiv l \pmod{\mathrm{ord}_m(a)}$.

定理 1.7. 设 $m \in \mathbb{Z}(m > 1), a \perp m$, k 是非负整数. 则,

$$\mathrm{ord}_m(a^k) = \frac{\mathrm{ord}_m(a)}{\gcd(\mathrm{ord}_m(a), k)}$$

定理 1.8. 设 $m \in \mathbb{Z}(m > 1), k \in \mathbb{Z}^+$. a 是 m 的原根 $\iff \gcd(k, \varphi(m)) = 1$.

定理 1.9. 设 $m \in \mathbb{Z}(m > 1)$. 如果 m 有原根, 则原根个数是 $\varphi(\varphi(m))$.

定理 1.10. 设 $m \in \mathbb{Z}(m > 1), a \perp m, b \perp m$. 则,

$$\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b) \iff a \perp b.$$

定理 1.11. 设 $m \in \mathbb{Z}(m > 1), a \perp m, b \perp m$. 则 $\exists c$ 使得

$$\mathrm{ord}_m(c) = \mathrm{lcm}(\mathrm{ord}_m(a), \mathrm{ord}_m(b)).$$

更一般地, $\exists g$ 使得 $\mathrm{ord}_m(g) = \mathrm{lcm}(\mathrm{ord}_m(a_1), \cdots, \mathrm{ord}_m(a_k)), \quad 2 \le k \le \varphi(m)$.

定理 1.12. 设 $m, n \in \mathbb{Z}(m > 1), a, m, n$ 两两互素. 则

$$\mathrm{ord}_{mn}(a) = \mathrm{lcm}(\mathrm{ord}_m(a), \mathrm{ord}_n(a)).$$

定理 1.13. 设 $m, n \in \mathbb{Z}(m > 1, n > 1, m \perp n), a_1 \perp mn, a_2 \perp mn$ 两两互素. 则 $\exists a:$

$$\mathrm{ord}_{mn}(a) = \mathrm{lcm}(\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)).$$

其中 a 是同余方程组 $x \equiv a_1 \pmod m, x \equiv a_2 \pmod n$ 的解.

定理 1.14. p 是素数 $\implies$ p 有原根.

定理 1.15 (原根判定)**.** 设 p 是奇素数, $q_i (1 \le i \le s)$ 都是 $p-1$ 的不同的素因数. 则 g 是模 p 原根 iff

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod p, \quad 1 \le i \le s.$$

定理 1.16. 设 a, m, n 两两互素,

定理 1.17. 模 m 存在原根当且仅当 $m = 1 \quad$ 或 $\quad 2 \quad$ 或 $\quad 4 \quad$ 或 $\quad p^\alpha \quad$ 或 $\quad 2p^\alpha$. 其中 α 是奇素数.

定理 1.18. g 是模 $p^{\alpha+1}$ 的原根 $\implies$ g 是模 p^α 的原根. p 是奇素数.

定理 1.19. 如果 g 是 p^α 的原根, 则 $\mathrm{ord}_{p^{\alpha+1}}(g) = \varphi(p^\alpha) \quad$ 或 $\quad \mathrm{ord}_{p^{\alpha+1}}(g) = \varphi(p^{\alpha+1})$

定理 1.20. 设 g 是模奇素数 p 的原根, 且 g 满足 $g^{p-1} = 1 + rp$ 且 $p \nmid r$, 则 g 是模 p^α 的原根.

定理 1.21. 如果 g' 是模奇素数 p 的原根, 则 $g = g' + kp$ 都是 p 的原根.

通过原根找原根:

- p 为奇素数, 则模 p 的素数必然存在, 如 g.
- 可以构造一个模 p 的原根 $\tilde{g}$

1.2 指标

定义 1.3 (指标)**.** 对于整数 r 满足 $0 < r \le \varphi(m)$, 如果

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

则称 r 为**以 g 为底的 a 模 m 的指标**. 记为 $\mathrm{ind}_g a$. 也可以称为**离散对数**, 记为 $\log_g a$.

定理 1.22 (指数-对数互换)**.** 设 m 是大于 1 的整数, g 是模 m 的原根. 如果 $g^s \equiv a \pmod m$, 则

$$s \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$$

定理 1.23.

$$\mathrm{ind}_g(a_1 \cdots a_n) = \mathrm{ind}_g a_1 + \cdots + \mathrm{ind}_g a_n$$

定理 1.24. 设 g 是模 m 的原根. 在模 m 的简化剩余系中, 指数为 e 的整数个数为 $\varphi(e)$.

特别地: $(\mathbb{Z}/m\mathbb{Z})^*$ 的原根个数为 $\varphi(\varphi(m))$

定理 1.25 (n 次同余方程)**.**

2 环

定理 2.1. 设 R 是有单位元的交换环, M 是 R 中极大理想的充要条件是: R/M 是域.

群 $(\mathbb{Z}_n, +_n)$ 的幂零元是什么?

$n = \prod p_i^{\alpha_i}$, 那么幂零元素就是

$$x = \prod p_i^w \quad \text{if} \quad w \neq 0$$

3 多项式环

定义 3.1 (多项式环)**.** 整数环、有理数域、实数域上的全体多项式构成的**多项式环**:

$$\mathbb{Z}[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{Z}, n \geq 0\}$$
$$\mathbb{Q}[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{Q}, n \geq 0\}$$
$$\mathbb{R}[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in \mathbb{R}, n \geq 0\}$$

定义 3.2. 设 R 是一个整环. 系数取自 R 的全体多项式构成的集合:

$$R[x] = \{\sum_{i=0}^{n} a_i x^i | a_i \in R, n \geq 0\}$$

则称 $R[x]$ 是**多项式整环**.

定义 3.3. 设 $f(x), g(x)$ 是多项式整环 $R[x]$ 中的任意两个多项式, 其中 $g(x) \neq 0$. 如果存在多项式 $q(x)$ 使得等式

$$f(x) = q(x) \cdot g(x)$$

成立, 就称 $g(x)$ **整除** $f(x)$, 记为 $g(x) \mid f(x)$.

定义 3.4 (不可约多项式)**.** 设 $f(x)$ 是整环 R 上的非常数多项式. 如果除了平凡因式 $f(x)$ 以外, $f(x)$ 没有其他非常数多项式, 那么, $f(x)$ 就称为 **不可约多项式**; 否则称为可约多项式.

例子: $4x^2 + 4$ 是一个不可约多项式.

定理 3.1. 设 $f(x)$ 是域 K 上的次数为 n 的可约多项式, $p(x)$ 是 $f(x)$ 的次数最小的非常数因式. 则 $p(x)$ 一定是不可约多项式, 且

$$\deg p < \frac{1}{2} \deg f$$

定理 3.2. 设 $f(x)$ 是域 K 上的多项式, 如果 $\forall p(x)$ 满足 $\deg p < \frac{1}{2} \deg f$ 且 $p(x)$ 不可约, 都有: $p(x) \nmid f(x)$, 则 $f(x)$ 一定是不可约多项式.

例 3.1. *$f(x) = x^8 + x^4 + x^3 + x + 1$ 是 $\mathbb{F}_2[x]$ 中的不可约多项式.*

定义 3.5 (多项式的 Euclid 除法). 给定整环上的多项式 $f(x), g(x)(\deg f \geq \deg g)$, 那么可以找到两个多项式 $q(x), r(x)$ 使得

$$f(x) = q(x) \cdot g(x) + r(x)$$

且 $\deg r < \deg g$.

定义 3.6 (最大公因式, 最小公倍式). 设 $f(x), g(x), d(x)$ 是整环 R 上的多项式. 称 $d(x)$ 是 $f(x), g(x)$ 的 **最大公因式**, 如果

$$d(x) \mid f(x), \quad d(x) \mid g(x)$$

并且 $\forall h(x) : h(x) \mid f(x), h(x) \mid g(x)$ 都有 $h(x) \mid d(x)$.

称 $m(x)$ 是 $f(x), g(x)$ 的 **最小公倍式**, 如果

$$f(x) \mid m(x), \quad g(x) \mid m(x)$$

并且 $\forall h(x) : f(x) \mid h(x), g(x) \mid h(x)$ 都有 $m(x) \mid h(x)$.

$d(x), m(x)$ 都可以记为 $\gcd(f(x), g(x)), \operatorname{lcm}(f(x), g(x))$.

定义 3.7 (多项式互素). 设 $f(x), g(x), d(x)$ 是整环 R 上的多项式. 若 $\gcd(f(x), g(x)) = 1$, 则称 $f(x)$ 与 $g(x)$ 互素. 记为 $f(x) \perp g(x)$

定理 3.3 (多项式广义 Euclid 除法). 设 $f(x), g(x), d(x)$ 是域 K 上的多项式. $\exists s_k(x), t_k(x)$ 使得

$$s_k(x)f(x) + t_k(x)g(x) = \gcd(f(x), g(x))$$

对于 $i = 0, 1, 2, \cdots, k$. $s_i(x), t_i(x)$ 归纳定义为:

$$\begin{cases} r_{-2}(x) = f(x), \quad r_{-1}(x) = g(x), \quad r_i = r_{i-2} \bmod r_{i-1} \\ q_i = \lfloor \frac{r_{i-2}}{r_{i-1}} \rfloor \\ s_{-2}(x) = 1, \quad s_{-1}(x) = 0, \quad s_i(x) = -q_i(x)s_{i-1} + s_{i-2} \\ t_{-2}(x) = 0, \quad s_{-1}(x) = 1, \quad t_i(x) = -q_i(x)t_{i-1} + t_{i-2} \end{cases}$$

还可以在域 K 上的多项式环 $K[x]$ 上完美复刻第二章关于同余的知识点.

定义 3.8 (多项式环的商环). 设 $p(x)$ 是域 K 上的多项式环 $K[x]$ 中的一个多项式

定理 3.4. 设 $p(x)$ 是域 K 上的多项式环 $K[x]$ 的一个不可约多项式, 则 $K[x]$ 关于理想 $(p(x))$ 的商环 $K[x]/(p(x))$ 关于多项式模 $p(x)$ 加法以及模 $p(x)$ 乘法构成一个域.

定理 3.5. 设素数 p. $p(x)$ 是多项式环 $\mathbb{F}_p[x]$ 中的一个代数次数为 n 的不可约多项式, 则 $\mathbb{F}_p[x]$ 关于理想 $(p(x))$ 的商环 $\mathbb{F}_p[x]/(p(x))$ 满足:

$$\mathbb{F}_p[x]/(p(x)) = \{a_{n-1}x^{n-1} + \cdots + a_1x + a_0 | a_i \in \mathbb{F}_p\}$$

一般记 $\mathbb{F}_p[x]/(p(x)) = \mathbb{F}_{p^n}$.

定义 3.9 (本原多项式). 设素数 p. 设 $f(x)$ 是有限域 $\mathbb{F}_p$ 上的多项式环 $\mathbb{F}_p[x]$ 中的一个 n 次多项式. 使得

$$x^e \equiv 1 \pmod{f(x)}$$

成立的最小正整数 e 叫做 $f(x)$ 在有限域 $\mathbb{F}_p$ 上的指数. 记为 $\operatorname{ord}_p(f(x))$.

特别地, 如果 $\operatorname{ord}_p(f(x)) = p^n - 1$, 则称 $f(x)$ 为 $\mathbb{F}_p$ 上的本原多项式

例 3.2. 对于计算机最喜欢的 $\mathbb{F}_2 = (\{0,1\}, +_2, (\cdot)_2)$, 有一个本原多项式 $x^8+x^4+x^3+x^2+x$, 令

$$\mathbb{F}_{2^8} = \mathbb{F}_2[x]/(x^8+x^4+x^3+x^2+x)$$