2021年8月8日 15:06

代数数论

回顾代数知识

$\mathbb{Z}/n\mathbb{Z}$

$a \equiv a' \mod n$, $b \equiv b' \mod n$ $\Rightarrow$ $ab \equiv a'b' \mod n$, $a+b \equiv a'+b' \mod n$

交换环

$\mathbb{Z}$ PID UFD

Th $\forall n \in \mathbb{Z}$ 有唯一分解 $n = \pm 1 \, p_1^{\alpha_1} \cdots p_n^{\alpha_n}$

p_i 素数. $\alpha_i \in \mathbb{N}$ $\alpha_i > 0$

$\mathbb{Z}^\times = \{\pm 1\}$

$a = \pm p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ $\alpha_i \geq 0$

$b = \pm p_1^{\beta_1} \cdots p_n^{\beta_n}$ $\beta_i \geq 0$

最大公因子 $\gcd(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_n^{\min(\alpha_n,\beta_n)}$

最小公倍数 $\operatorname{lcm}(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_n^{\max(\alpha_n,\beta_n)}$

Th (Bézout) Euclid 辗转相除法

$\forall a,b \in \mathbb{Z}$ $\exists \alpha, \beta \in \mathbb{Z}$ $\gcd(a,b) = \alpha a + \beta b$

例 $a = 37$ $b = 13$

$37 = \underset{a}{} \quad \underset{b}{} \quad 13 \times 2 + \boxed{11}$

$13 = 11 \times 1 + (2)$

$11 = 2 \times 5 + (1)$ gcd

$2= 1 \times 2 + 0$ 停

$1 = 11 - (2) \times 5$

$= 11 - (13 - 11 \times 1) \times 5$

$= 11 - 13 \times 5 + 11 \times 5$

$= \boxed{11} \times 6 - 13 \times 5$

$= (37 - 13 \times 2) \times 6 - 13 \times 5$

$= 37 \times 6 - 13 \times 12 - 13 \times 5$

$= 37 \times 6 - 13 \times 17$

$= 37\times 6 - 13\times 12 - 13\times 5$

$= 37\times 6 - 13\times 17$

$a \quad \alpha \qquad b \quad \beta$

一般证明: $\forall a, b \in \mathbb{N}$

$a = bq_0 + r \qquad 0 \le r < b$

$b = rq_1 + r_2 \cdots \qquad r \ge 0 \quad r \downarrow$ 有限步后 $r = 0$. #

$\mathbb{Z}$ PID: $(a, b) = (\gcd(a, b))$

Prop $n \in \mathbb{Z} \qquad \bar{n} \in \mathbb{Z}/n\mathbb{Z}$ 以下等价

(1) $\bar{n}$ 生成 $\mathbb{Z}/n\mathbb{Z}$ (作为加群)

(2) $\gcd(n, n) = 1$

(3) $\bar{n} \in (\mathbb{Z}/n\mathbb{Z})^\times$ (可逆元)

Def $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$ Euler 函数

例 1. 素数. $n = p$ $\qquad \varphi(p^r) = p^r - p^{r-1} = p(p^{r-1} - 1)$

$\mathbb{Z}/p^r\mathbb{Z}$

$\forall n \in \mathbb{N}$ 计算 $\varphi(n)$?

Th (中国剩余定理)

$m, n \in \mathbb{Z}$ 互素 $\gcd(m, n) = 1$ 则有环同构 $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Cor m, n 互素, 则有 Abel 群同构 $(\mathbb{Z}/mn\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/n\mathbb{Z})^\times$

即 $\varphi(mn) = \varphi(m)\varphi(n)$

$n = p_1^{\alpha_1} \cdots p_m^{\alpha_m} \qquad \varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_m^{\alpha_m} - p_m^{\alpha_m - 1})$

$= n \cdot \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right)$

Pf of Th: $f: \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

Pf of Th: $f: \mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$x \longmapsto x \bmod m,\ x \bmod n$

$\ker(f) = mn\mathbb{Z}$ $\quad \mathbb{Z}/mn\mathbb{Z} \hookrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ 单射同态

左右大小相等, $\Rightarrow$ 同构 #

域 多个含量

有限域的特征

$\mathbb{F}$ 域 $|\mathbb{F}|$ 有

$\varphi: \mathbb{Z} \longrightarrow \mathbb{F}$

$1 \longmapsto 1_{\mathbb{F}}$

$\ker\varphi = p\mathbb{Z}$ $\quad \mathbb{F}_p = \mathbb{Z}/\ker\varphi \hookrightarrow \mathbb{F}$

$\mathrm{char}\,\mathbb{F} = p$ $\quad \mathbb{F}_p \subset \mathbb{F}$

$\mathbb{F}$: 有限维 $\mathbb{F}_p$-向量空间

Th p 素, $f \geq 1$ 同构意义下 存在唯一一个 $q = p^f$ 元的有限域 $\mathbb{F}_q = \mathbb{F}_{p^f}$

$\overline{\mathbb{F}}_p = \mathbb{F}_p$ 的代数闭包 $\quad q = p^f$

$\mathbb{F}_{p^f} = \{ \alpha \in \overline{\mathbb{F}}_p \mid \alpha$ 是 $X^q - X$ 的根 $\}$ 在 $\overline{\mathbb{F}}_p$ 有限可分扩张

$\mathbb{F}_q = \mathbb{F}_p(\alpha) = \mathbb{F}_p[x]/(p)$

$p \in \mathbb{F}_p[x]$ 为 α 在 $\mathbb{F}_p$ 上的极小多项式.

例 $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$ 余 $\mathbb{Z}/4\mathbb{Z}$

$\mathbb{F}_8 = \mathbb{F}_2[x]/(x^3+x+1)$

$\mathbb{F}_{11} = \mathbb{F}_2[x]/(x^4+x^3+x^2+x+1)$

$$\mathbb{F}_{16} = \mathbb{F}_2[X] / (X^4+X^3+X^2+X+1)$$

Th K 域，则 K^* 的有限子群总是循环群

($\Leftrightarrow$ $\mathbb{F}_q^*$ 循环群)

Pf $G \subset K^*$ 有限子群　　$g \in G$　$\mathrm{ord}(g) \mid d \Leftrightarrow g^d = 1$

即 $g \in K^*$ 是 $X^d - 1 = 0$ 的根（至多有 d 个根）

从而 G 中阶整除 d 的元素个数至多 d 个

$\Rightarrow$ G 是循环子群　　#

Cor $\left[\mathbb{F}_p^* : \mathbb{F}_p^{*2}\right] = 2$　（即 $\mathbb{F}_p^*$ 一半是平方，一半非平方）

$(\pm 1)^2$　$(\pm 2)^2$, $\cdots$ $(\pm(p-1))^2$

Pf $G = \mathbb{F}_p^* \cong \mathbb{Z}/n\mathbb{Z}$　　$|H| \mid |G|$　　$m = dn$

$H = \mathbb{F}_p^{*2} \cong \mathbb{Z}/m\mathbb{Z}$　　$2(G/H) = 0 \Rightarrow d = 1, 2$

$\Rightarrow [G:H] = 2$　　#

Motivation　数论 $\longleftrightarrow$ 整 $\mathbb{Q}$ 上解方程

Legendre 符号

Def　$p \neq 2$　　$a \in \mathbb{Z}$

$$\left(\frac{a}{p}\right) := \begin{cases} 0 & p \mid a \\ 1 & p \nmid a \quad \bar{a} \in \mathbb{F}_p^{*2} \\ -1 & p \nmid a \quad \bar{a} \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2} \end{cases}$$

$x^2 \equiv a \bmod p$ 是否有解

Th p 是奇素数.

(1) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(2) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$

$\frac{p-1}{2}$ 个 $-1 \bmod p$ 平方 $\Leftrightarrow p \equiv 1 \ (4)$

(4) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p$

(3) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ $\begin{cases} -1 \bmod p \text{ 平方} \Leftrightarrow p \equiv 1 \ (4) \\ 2 \bmod p \text{ 平方} \Leftrightarrow p \equiv \pm 1 \ (8) \end{cases}$

(4)(Gauss二次互反律) $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

pf (1) 若 $p \mid ab$ 则证=0

设 $p \nmid a$, $p \nmid b$ $\quad \mathbb{F}_p^{*2} \lhd \mathbb{F}_p^*$ 指标 $\quad \bar{a}, \bar{b}$ 平方 $\Rightarrow \bar{a}\bar{b}$ 平方

$\bar{a}$ 平方, $\bar{b}$ 不平方 $\Rightarrow \bar{a}\bar{b}$ 不平方

还要验证 $\bar{a}$, $\bar{b}$ 不平方 $\quad \mathbb{F}_p^*/\mathbb{F}_p^{*2} \cong \mathbb{Z}/2\mathbb{Z}$

$\bar{a}_1 \longrightarrow 1 \qquad |+1| = 0$

平方 $\bar{a}\bar{b}$ $\quad \bar{b}_1 \longrightarrow 1$

(2) $\boxed{a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p}$ $\quad p \mid a$ ✓ $\quad p \nmid a$

$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \overset{\text{Fermat}}{\equiv} 1 \ (p) \Rightarrow a^{\frac{p-1}{2}} = \pm 1 \in \mathbb{F}_p^*$

$H := \{ g \in \mathbb{F}_p^* \mid \operatorname{ord}(g) \mid \frac{p-1}{2} \} < \mathbb{F}_p^*$

$|H| = \frac{p-1}{2}$ $\quad$ 又知 $\left|\mathbb{F}_p^{*2}\right| = \frac{p-1}{2}$

$\mathbb{F}_p^{*2} \subset H$: $\forall\, a \in \mathbb{F}_p^{*2}$ $\quad a = b^2$ $\quad a^{\frac{p-1}{2}} = b^{2\cdot\frac{p-1}{2}} = b^{p-1} = 1 \in \mathbb{F}_p$

$\Rightarrow a \in H$

从而 $H = \mathbb{F}_p^{*2}$

即 $a \in \mathbb{F}_p^{*2} \Leftrightarrow a^{\frac{p-1}{2}} = 1 \in \mathbb{F}_1$

$a \notin \mathbb{F}_p^{*2} \Leftrightarrow a^{\frac{p-1}{2}} = -1 \in \mathbb{F}_p$

(3) $\boxed{\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}}$

(2)中取 $a = -1$ $\quad (-1)^{\frac{p-1}{2}} \equiv \left(\frac{-1}{p}\right) \bmod p$

$\{\pm 1\}$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

$\{\pm 1\}$ (1)

$\alpha \in \overline{\mathbb{F}_p}$ 是 $X^4+1=0$ 的根

$\alpha^4 = -1 \neq 1$ $\alpha^8 = 1$

8次 非平凡根

$\alpha^2 = -\alpha^{-2}$

取 $\beta = \alpha + \alpha^{-1}$, $\beta^2 = \alpha^2 + \alpha^{-2} + 2 = 0 + 2 = 2 \in \mathbb{F}_p^*$

即 $2 \in \mathbb{F}_p^{*2} \iff \beta \in \mathbb{F}_p \iff \beta^p - \beta = 0$

$\beta^p = (\alpha+\alpha^{-1})^p = \alpha^p + \alpha^{-p}$ $\alpha^8 = 1$

$p \equiv \pm 1 (8) \Rightarrow \beta^p = \alpha^p + \alpha^{-p} = \alpha + \alpha^{-1} = \beta \iff 2 \in \mathbb{F}_p^{*2}$

$p \equiv \pm 3 (8) \Rightarrow \beta^p = \alpha^p + \alpha^{-p} = \alpha^3 + \alpha^{-3} = -(\alpha+\alpha^{-1}) = -\beta \neq \beta$

$\alpha^4 = -1$

$\beta^p \neq \beta$

β 不是 $X^p - X = 0$ 的根

$\iff 2 \notin \mathbb{F}_p^{*2}$ #

应用例子

例 $p = 1087$ 是. $X^2 = 6 \bmod 1087$

$6 \in \mathbb{F}_p^{*2}$?

$$\left(\frac{6}{1087}\right) = \left(\frac{2}{1087}\right)\left(\frac{3}{1087}\right) = (-1)^{\frac{1087^2-1}{8}} \cdot \left(\frac{3}{1087}\right)$$

$1087 \equiv -1 (8)$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p+1}{2}\frac{q-1}{2}}$$

$$= \left(\frac{1087}{3}\right)(-1)^{\frac{1087-1}{2}\cdot\frac{3-1}{2}} = -\left(\frac{1087}{3}\right) = -\left(\frac{1}{3}\right) = -1$$

-1

$1087 \equiv 1 (3)$

6 不是 mod 1087 的平方数.

例 求证 $\forall p \neq 2$ $(x^2-5)(x^2-7)(x^2-35)=0$ 在 $\mathbb{F}_p$ 中总有解

证: $p \neq 2,5,7$. 若 $\left(\frac{5}{p}\right)=1$ $x^2-5=0$ $\mathbb{F}_p$ 中有解

若 $\left(\frac{7}{p}\right)=1$ $x^2-7=0$ ✓

若 $\left(\frac{5}{p}\right)=\left(\frac{7}{p}\right)=-1 \Rightarrow \left(\frac{35}{p}\right)=1$ $x^2-35=0$ ✓

RH 二次互反律 $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

关于2个素数的定理，而今不用你的局部

一个整体的定理

$p \neq q$ 奇素 $\alpha \in \overline{\mathbb{F}_q}$ p次单位根

$$\alpha^p-1=0 \quad \alpha \neq 1$$
$$\alpha^{p-1}+\alpha^{p-2}+\cdots+\alpha+1=0$$

定义 (Gauss和) $\tau=\sum_{x \in \mathbb{F}_p}\left(\frac{x}{p}\right)\cdot\alpha^x \in \mathbb{F}_q(\alpha) \subset \overline{\mathbb{F}_q}$

lem (1) $\tau^2=\left(\frac{-1}{p}\right)\cdot p \in \mathbb{F}_q$ ($\Rightarrow \tau \neq 0$)

(2) $\tau^{q-1}=\left(\frac{q}{p}\right) \in \mathbb{F}_q(\alpha) \subset \overline{\mathbb{F}_q}$

Pf (1) $\tau^2=\sum_{x,y \in \mathbb{F}_p}\left(\frac{xy}{p}\right)\alpha^{x+y}=\sum_{u \in \mathbb{F}_p} S(u)\alpha^u$

其中 $S(u)=\sum_{\substack{x+y=u \\ x \in \mathbb{F}_p^* \\ y \in \mathbb{F}_p^*}}\left(\frac{xy}{p}\right)=\sum_{x \in \mathbb{F}_p}\left(\frac{x(u-x)}{p}\right)$

case1 $u=0$ $S(0)=\sum\left(\frac{-x^2}{p}\right)=\sum\left(\frac{-1}{p}\right)\left(\frac{x^2}{p}\right)=(p-1)\left(\frac{-1}{p}\right)$

Case 1 $u=0$ $\quad S(0)=\sum_{x\in\mathbb{F}_p^*}\left(\frac{-x^2}{p}\right)=\sum_{x\in\mathbb{F}_p^*}\left(\frac{-1}{p}\right)\left(\frac{x^2}{p}\right)=(p-1)\left(\frac{-1}{p}\right)$

Case 2 $u\in\mathbb{F}_p^*$ $\quad S(u)=\sum_{x\in\mathbb{F}_p^*}\left(\frac{x(u-x)}{p}\right)=\sum_{x\in\mathbb{F}_p^*}\left(\frac{-x^2(1-ux^{-1})}{p}\right)=\left(\frac{-1}{p}\right)\sum_{x\in\mathbb{F}_p^*}\left(\frac{1-ux^{-1}}{p}\right)$

$x\rightsquigarrow\mathbb{F}_p^*$ $\quad y=1-ux^{-1}$ 取遍 $\mathbb{F}_p\setminus\{1\}$

$$\sum_{y\in\mathbb{F}_p}\left(\frac{y}{p}\right)=0$$

$$=-\left(\frac{-1}{p}\right)$$

case 1+2 $\Rightarrow$

$$\tau^2=\left(\frac{-1}{p}\right)\cdot\left(p-1-\sum_{u=1}^{p-1}\alpha^u\right)=\left(\frac{-1}{p}\right)\cdot p$$

(2) $\tau^{q-1}=\cdots\cdots\in\mathbb{F}_q$

$$\tau^q=\sum_{x\in\mathbb{F}_p}\left(\frac{x}{p}\right)^q\alpha^{qx}=\sum_{x\in\mathbb{F}_p}\left(\frac{x}{p}\right)\alpha^{qx}=\left(\frac{q}{p}\right)\underbrace{\sum_{x\in\mathbb{F}_p}\left(\frac{qx}{p}\right)\alpha^{qx}}_{\tau}$$

$$=\left(\frac{q}{p}\right)\cdot\tau$$

(1)代入 $\Rightarrow\quad \tau^{q-1}=\left(\frac{q}{p}\right)$ #

二次互反律证明：$q\neq a$

$$a^{\frac{q-1}{2}}\equiv\left(\frac{a}{q}\right)\bmod q \qquad \text{取 } a=p$$

$\mathbb{F}_q(\alpha)$ 中

$$\left(\frac{p}{q}\right)\equiv p^{\frac{q-1}{2}}\overset{\text{Lem(1)}}{=}\left(\left(\frac{-1}{p}\right)\tau^2\right)^{\frac{q-1}{2}}=\left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\tau^{q-1}\overset{\text{Lem(2)}}{=}\left(\frac{-1}{p}\right)^{\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right)$$

$$=\left((-1)^{\frac{p-1}{2}}\right)^{\frac{q-1}{2}}\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{q}{p}\right)$$

$$= \left((-1)^{\frac{p-1}{2}}\right)^2 \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right)$$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \in \overline{\mathbb{F}_q} \quad (q \neq 2)$$

$$\in \mathbb{Z}$$

---

p-adic 数

Motivation 在 $\mathbb{Q}$ 之中解方程

$x^2 + y^2 = a$ $\quad a = -1$ 有解吗?

$\mathbb{Q} \subset \mathbb{R}$ $\quad$ $\mathbb{R}$ 中无解 $\Rightarrow$ $\mathbb{Q}$ 中无解.

⇑

几何意义

$\mathbb{Q} \rightsquigarrow \mathbb{R}$: 加入 $\mathbb{Q}$ 中所