§5. 单位群 $(\mathbb{Z}/m\mathbb{Z})^\times$ 的结构

本节基本问题 1) $(\mathbb{Z}/m\mathbb{Z})^\times$ 何时为循环群

2) 判定 $a \bmod p$ 是否为 $\mathbb{F}_p^\times$ 中平方元.

(判定 $x^2 \equiv a \bmod p$ 是否有解.)

§5.1. 原根.

例: 1) $(\mathbb{Z}/8\mathbb{Z})^\times = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ $\bar{3}^2 = \bar{5}^2 = \bar{7}^2 = 1$ ✗

2) $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$. ✓

3) $(\mathbb{Z}/9\mathbb{Z})^\times$: $1 \to \underline{\underline{5}} \to 7 \to 8 \to 4 \to \underline{\underline{2}} \to 1$ ✓

4) $(\mathbb{Z}/18\mathbb{Z})^\times$: $1 \to \underline{\underline{5}} \to 7 \to 17 \to 13 \to \underline{\underline{11}} \to 1$ ✓

5) $(\mathbb{Z}/15\mathbb{Z})^\times$: $\bar{2}^4 = \bar{4}^2 = \bar{7}^4 = \bar{8}^4 = \bar{11}^2 = \bar{13}^4 = \bar{14}^2 = \bar{1}$ ✗

何时为循环群?

定理: $(\mathbb{Z}/m\mathbb{Z})^\times$ 为循环群 $\Leftrightarrow m = 2, 4, p^\alpha$ 或 $2p^\alpha$.

设 $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$. 则由中国剩余定理 有

$$\boxed{\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^\times &\cong (\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z})^\times \times (\mathbb{Z}/p_2^{\alpha_2}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z})^\times \\ r \bmod m &\longmapsto (r \bmod p_1^{\alpha_1}, r \bmod p_2^{\alpha_2}, \cdots, r \bmod p_s^{\alpha_s}) \end{aligned}}$$

引理: 设 $G = H_1 \times H_2 \times \cdots \times H_n$ 为有限群. 则

$$G \text{ 循环} \Leftrightarrow \begin{cases} H_1, \cdots, H_n = \text{循环} \\ \gcd(\#H_i, \#H_j) = 1 \quad \forall i \neq j \end{cases}$$

Pf: ⇐): 记 $m_i := \#H_i$, $m = \prod_{i=1}^{n} m_i$. 则 m_i 两两互素 因此

$$G = H_1 \times \cdots \times H_n \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z} \times \cdots \times \mathbb{Z}/m_n\mathbb{Z} \overset{CRT}{\cong} \mathbb{Z}/m\mathbb{Z}$$

为循环群. 循环群的结构定理.

⇒): 设 $g = (h_1, h_2, \cdots, h_n)$ 为 $G = H_1 \times \cdots \times H_n$ 的生成元.

则 $H_1 \times \cdots \times H_n$ 中任意元素都可表示为 $g^k = (h_1^k, \cdots, h_n^k)$ 的形式. 特别地, H_i 可由 h_i 生成. 因此 H_i 循环.

设 $m' = \mathrm{lcm}(m_1, m_2, \cdots, m_n)$. 则

$$(h_1, \cdots, h_n)^{m'} = (h_1^{m'}, \cdots, h_n^{m'}) = (1, \cdots, 1) = 1_G$$

$$\Rightarrow \#G = \mathrm{ord}(h_1, \cdots, h_n) \mid m' = \mathrm{lcm}(m_1, \cdots, m_n) \mid \#G.$$

$$\Rightarrow \mathrm{lcm}(m_1, \cdots, m_n) = \#G = m_1 m_2 \cdots m_n$$

⇒ $m_1, \cdots, m_n$ 两两互素.

定理: $(\mathbb{Z}/m\mathbb{Z})^\times$ 循环 ⇒ $m = 2, 4, p^\alpha, 2p^\alpha$

Pf: 若 p 为素数, $\alpha \in \mathbb{Z}_{>0}$ s.t. $p^\alpha \geq 3$, 则 $2 \mid \#(\mathbb{Z}/p^\alpha\mathbb{Z})^\times = \varphi(p^\alpha) = p^{\alpha-1}(p-1)$.

由引理知 ⇒ $\begin{cases} 1)\ m \text{ 不含两不同的奇素因子} \\ 2)\ 4 \mid m \Rightarrow m \text{ 不含奇素因子} \end{cases}$

$$\Rightarrow m = 2^\beta\ (\beta \geq 1) \text{ 或 } 2^\beta p^\alpha\ (\beta \leq 1, \alpha \geq 1)$$

下面仅需证明: $(\mathbb{Z}/2^\beta\mathbb{Z})^\times\ (\beta \geq 3)$ 不为循环群.

$$(\mathbb{Z}/2^\beta\mathbb{Z})^\times \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^\times \qquad r \bmod 2^\beta \mapsto r \bmod 8$$

由例题知 $(\mathbb{Z}/8\mathbb{Z})^\times$ 不为循环群. 因此 $(\mathbb{Z}/2^\beta\mathbb{Z})^\times$ 不为循环群. 否则若 $r \bmod 2^\beta$ 为 $(\mathbb{Z}/2^\beta\mathbb{Z})^\times$ 的生成元, 则 $r \bmod 8$ 为 $(\mathbb{Z}/8\mathbb{Z})^\times$ 生成元也.

下面仅需证明 $(\mathbb{Z}/p^{\alpha}\mathbb{Z})^{\times}$ 为循环群 ($\forall p =$ 奇素数).

定理: $\mathbb{F}_p^{\times}$ 为 $p-1$ 阶循环群.

Pf: $S_d := \#\{a \in \mathbb{F}_p^{\times} \mid \mathrm{ord}(a) = d\} = \begin{cases} \varphi(d) & \exists\, d \text{ 阶元} \\ 0 & \nexists\, d \text{ 阶元} \end{cases}$

(设 a 为 d 阶元, 则 $1, a, \cdots, a^{d-1}$ 为 $x^d=1$ 的全部的根.
所有 d 阶元均为 $x^d=1$ 的根, 且恰有 $\varphi(d)$ 个根为 d 阶元)

$$p-1 = \sum_{d \mid p-1} S(d) \leq \sum_{d \mid p-1} \varphi(d) = p-1$$

$\Rightarrow S(p-1) = \varphi(p-1) \neq 0 \Rightarrow \exists\, p-1$ 阶元 $\Rightarrow$ ✓ $\square$

定理: p 为奇素数. $k \geq 2$. 则 $(\mathbb{Z}/p^k\mathbb{Z})^{\times}$ 为循环群.

Pf: $k=1$ ✓ 设 $g \bmod p$ 为 $\mathbb{F}_p^{\times}$ 的生成元.

$k=2$. $\forall a \in \mathbb{Z}$ & $\gcd(a,p)=1$. 记 $d = \mathrm{ord}(a \bmod p^2)$

$\Rightarrow a^d \equiv 1 \bmod p^2 \Rightarrow a^d \equiv 1 \bmod p \Rightarrow \mathrm{ord}(a \bmod p) \mid d$

$\Rightarrow \mathrm{ord}(a \bmod p) \mid \mathrm{ord}(a \bmod p^2)$.

$a = g$ 或 $g+p$

$\Rightarrow p-1 \mid \mathrm{ord}(g \bmod p^2)$ & $p-1 \mid \mathrm{ord}(g+p \bmod p^2)$

$\xRightarrow{\#(\mathbb{Z}/p^2\mathbb{Z})^{\times} = p(p-1)} \mathrm{ord}(g \bmod p^2), \mathrm{ord}(g+p \bmod p^2) = p-1$ 或 $p(p-1)$

又因为 $g^{p-1} \equiv 1 (p^2)$ 与 $(g+p)^{p-1} \equiv 1 (p^2)$ 不同时成立.

(这是由于: $(g+p)^{p-1} - g^{p-1} = \sum_{k \geq 1} \binom{p-1}{k} g^{p-1-k} p^k \equiv p(p-1) g^{p-2} \not\equiv 0 (p^2)$)

$\Rightarrow \mathrm{ord}(g \bmod p^2) = p(p-1)$ 或 $\mathrm{ord}(g+p \bmod p^2) = p(p-1)$

$\Rightarrow (\mathbb{Z}/p^2\mathbb{Z})^{\times} =$ 循环.

$k\geq 3$. 设 $g \bmod p^2$ 为 $(\mathbb{Z}/p^2\mathbb{Z})^\times$ 的一个生成元. 则 $g^{p-1}\not\equiv 1 \bmod p^2$.

断言: $p^m \,\|\, g^{\varphi(p^m)}-1 \quad (\forall\, m\geq 1)$ $\left(\text{i.e. } p^m \mid g^{\varphi(p^m)-1} \;\&\; p^{m+1}\nmid g^{\varphi(p^m)-1}\right)$

对 m 归纳: $m=1$ ✓ (g 为 $(\mathbb{Z}/p^2\mathbb{Z})^\times$ 生成元 $\Rightarrow g^{p-1}\not\equiv 1 \bmod p^2$)

假若 $p^m \,\|\, g^{\varphi(p^m)}-1$, 下证 $p^{m+1}\,\|\, g^{\varphi(p^{m+1})}-1$

$$g^{\varphi(p^{m+1})}-1=\left(\left(g^{\varphi(p^m)}-1\right)+1\right)^p-1 \overset{p\neq 2}{\equiv} p\left(g^{\varphi(p^m)}-1\right) \bmod p^{2m+1}$$

$$\Rightarrow p^{m+1}\,\|\, g^{\varphi(p^{m+1})}-1$$

断言 $\Rightarrow g^{\varphi(p^k)}\equiv 1 \bmod p^k \;\&\; g^{\varphi(p^{k-1})}\not\equiv 1 \bmod p^k$

$$\Rightarrow \operatorname{ord}(g \bmod p^k)\mid \varphi(p^k) \;\&\; \operatorname{ord}(g \bmod p^k)\nmid \varphi(p^{k-1})$$

$$\overset{p-1\mid \operatorname{ord}(g \bmod p^k)}{\Longrightarrow} \operatorname{ord}(g \bmod p^k)=\varphi(p^k) \Rightarrow \checkmark.$$

推论: $(\mathbb{Z}/2p^k\mathbb{Z})^\times$ 为循环群.

Pf: $(\mathbb{Z}/2p^k\mathbb{Z})^\times \xrightarrow[\text{CRT}]{\sim} (\mathbb{Z}/2\mathbb{Z})^\times\times(\mathbb{Z}/p^k\mathbb{Z})^\times \cong (\mathbb{Z}/p^k\mathbb{Z})^\times$.

命题 $(\mathbb{Z}/2\mathbb{Z})^\times=\{\bar{1}\}$ $\quad(\mathbb{Z}/4\mathbb{Z})^\times=\{\bar{1},\bar{3}\}$

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2^{k-2}\mathbb{Z}\times \mathbb{Z}/2\mathbb{Z} \quad \forall\, k\geq 3.$$

Pf: $\forall$ 奇数 $a \Rightarrow a^2\equiv 1 \bmod 8 \Rightarrow a^{2^{k-2}}\equiv 1 \bmod 2^k \Rightarrow \operatorname{ord}(a \bmod 2^k)\leq 2^{k-2}$

$$2^2\,\|\, 5^{2^0}-1 \Rightarrow 2^k \,\|\, 5^{2^{k-2}}-1 \quad (k\geq 2).$$

$$\Rightarrow \operatorname{ord}(5 \bmod 2^k)=2^{k-2}$$

$$5^k\equiv 1,5 \bmod 8 \Rightarrow -1 \bmod 2^k \notin \langle 5 \bmod 2^k\rangle$$

$$\Rightarrow \langle 5 \bmod 2^k\rangle\times\langle -1 \bmod 2^k\rangle \hookrightarrow (\mathbb{Z}/2^k\mathbb{Z})^\times \Rightarrow \checkmark$$

例：方程 $x^2=1$ 在 $\mathbb{Z}/m\mathbb{Z}$ 上有多少解？

$m=2^{\alpha}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ $\alpha\geq 0,\ \alpha_1,\cdots,\alpha_s>0.$

1° $\alpha=0,1$ $\Rightarrow$ 2^s 个解

2° $\alpha=2$ $\Rightarrow$ 2^{s+1} 个解

3° $\alpha\geq 3$ $\Rightarrow$ 2^{s+2} 个解

对应初等数论中的概念：设 $\gcd(a,m)=1$.

a 模 m 的阶 $:=$ 为 $a+m\mathbb{Z}$ 在 $(\mathbb{Z}/m\mathbb{Z})^\times$ 中的阶.

g 为模 m 的原根 $\Leftrightarrow$ $g+m\mathbb{Z}$ 生成整个群 $(\mathbb{Z}/m\mathbb{Z})^\times$

模 m 有原根 $\Leftrightarrow$ $(\mathbb{Z}/m\mathbb{Z})^\times$ 为循环群

初等数论　　群论

例. 模2原根 $=1$，模4原根 $=3$. 5为模6的原根. 模8没有原根.

定理：模 m 有原根 $\Leftrightarrow$ $m=2,4,p^\alpha$ 或 $2p^\alpha$ 其中 p 为奇素数，$\alpha\geq 1$.

问题：如何找到原根？　$m=p^k$ or $2p^k$

算法：1) 概率法求模 p 的原根 g

随机选取 $a\in[2,p-1]$ 为原根的概率为 $\frac{\varphi(p-1)}{p-2}$

2) $g^{p-1}\not\equiv 1 \bmod p^2$ $\Rightarrow$ g 为模 p^k 的原根

$g^{p-1}\equiv 1 \bmod p^2$ $\Rightarrow$ $g+p$ 为模 p^k 的原根.

3). 设 g 为模 p^k 的原根

$2\nmid g$ $\Rightarrow$ g 为模 $2p^k$ 的原根

$2\mid g$ $\Rightarrow$ $g+p^k$ 为模 $2p^k$ 的原根.

习题：$f: G \to H$ 群同态. $\forall g \in G$. 则

$$\operatorname{ord}(f(g)) \mid \operatorname{ord}(g).$$

Pf $\quad g^{\operatorname{ord}(g)} = 1 \Rightarrow f(g)^{\operatorname{ord}(g)} = 1 \Rightarrow \operatorname{ord}(f(g)) \mid \operatorname{ord}(g).$ $\square$

习题：p 为奇素数 $\forall p^n \geq 3$, $\forall a, b \in \mathbb{Z}$ s.t. $p \nmid ab$, 则

$$p^n \parallel a-b \xRightarrow{p^n \geq 3} p^{n+k} \parallel a^{p^k} - b^{p^k}$$

Pf：仅需证明 $k=1$ 情形.

$p^n \parallel a-b \Rightarrow a = b + p^n \delta \quad (p \nmid \delta,\ p^n \geq 3)$

$$\Rightarrow a^p = (b+p^n\delta)^p = b^p + \binom{p}{1} b^{p-1} \cdot p^n \delta + \cdots + \binom{p}{p-1} b (p^n\delta)^{p-1} + \binom{p}{p} (p^n \delta)^p$$

$$\equiv b^p + \binom{p}{1} b^{p-1} \cdot p^n \delta + \binom{p}{2} b^{p-2} p^{2n} \delta^2 \mod p^{3n}$$

$$\equiv \begin{cases} b^p + p^{n+1} b^{p-1} \delta + p^{2n} \delta^2 \pmod{p^{3n}} & p=2 \\ b^p + p^{n+1} b^{p-1} \delta + p^{2n+1} b^{p-2} \delta^2 \pmod{p^{3n}} & p \geq 3 \end{cases}$$

$$\equiv b^p + p^{n+1} b^{p-1} \delta \pmod{p^{n+2}}$$ $\square$

§ $\mathbb{F}_p^\times$ 中的平方元与二次剩余.

p = 奇素数　g = 模 p 原根. 则

$$(\mathbb{F}_p^\times)^2 := \{a^2 \mid a \in \mathbb{F}_p^\times\} = \{1, g^2, g^4, \cdots, g^{p-3}\}$$

平方元组成的子集 构成 $\mathbb{F}_p^\times$ 的 $\frac{p-1}{2}$ 阶子群.

定义: 称 $\mathbb{F}_p^\times$ 中的平方元为二次剩余 (quadratic residue)

反之, 则称为二次非剩余 (quadratic nonresidue)

注: 1) 各占一半 (陪集分解)

2) g^k 为二次剩余 $\Leftrightarrow 2 \mid k$.

定义: · $\forall\, a \in \mathbb{F}_p$.

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ 为二次剩余} \\ 0 & a = 0 \\ -1 & a \text{ 为二次非剩余.} \end{cases}$$

勒让德符号

Legendre symbol.

· $\forall\, a \in \mathbb{Z}$　$\left(\frac{a}{p}\right) := \left(\frac{a \bmod p}{p}\right)$

命题: $\left(\frac{\cdot}{p}\right) : \mathbb{F}_p^\times \to \{\pm 1\}$ 为群同态.　$\mathrm{Ker}\left(\frac{\cdot}{p}\right)$ 为二次剩余组成的子群.

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

Pf: $\left(\frac{g^k}{p}\right)\left(\frac{g^l}{p}\right) = (-1)^k \cdot (-1)^l = (-1)^{k+l} = \left(\frac{g^{k+l}}{p}\right)$　□

命题: $a \in \mathbb{F}_p^\times$. 则

$$\left(\frac{a}{p}\right)=1 \Leftrightarrow x^2=a \text{ 在 } \mathbb{F}_p^\times \text{ 中有解} \Leftrightarrow x^2-a \text{ 在 } \mathbb{F}_p[x] \text{ 中可约}$$

命题: $x^2\equiv a \bmod p$ 的解数为 $\left(\frac{a}{p}\right)+1$.

Legendre Symbol 的计算:

$$\forall\ a = (-1)^{\varepsilon} 2^{\alpha} p_1^{\alpha_1}\cdots p_s^{\alpha_s} \quad (\varepsilon, \alpha, \alpha_i \in \mathbb{N})$$

$$\Rightarrow \left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^{\varepsilon}\left(\frac{2}{p}\right)^{\alpha}\left(\frac{p_1}{p}\right)^{\alpha_1}\cdots\left(\frac{p_s}{p}\right)^{\alpha_s}$$

仅需计算: $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$.

命题(欧拉判别法): $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$

Pf: $p\mid a \Rightarrow \checkmark$.

设 $a\equiv g^k \pmod p$. $\Rightarrow \left(\frac{a}{p}\right)=(-1)^k$

$$a^{\frac{p-1}{2}} \equiv g^{k\frac{p-1}{2}} \equiv \begin{cases} (g^{p-1})^{\frac{k}{2}} \equiv 1 \bmod p & (2\mid k) \\ (g^{p-1})^{\frac{k-1}{2}}\cdot g^{\frac{p-1}{2}} \equiv -1 \bmod p & 2\nmid k \end{cases}$$

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

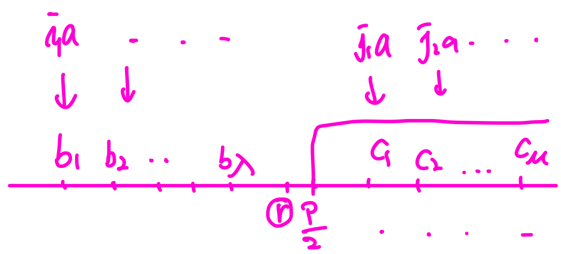
推论 $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

高斯引理: $p=$ 奇素数, $(a,p)=1$, $r=\frac{p-1}{2}$,

$$\mu := \#\left\{ ia \;\middle|\; \begin{array}{l} 1\le i\le r \\ ia \text{ 模} p \text{余数} > \frac{p}{2} \end{array} \right\}$$

则 $\left(\frac{a}{p}\right) = (-1)^{\mu}$

Pf:



$(\lambda+\mu=r)$

$$\{b_1,b_2,\cdots,b_r,\ p-c_1,\ p-c_2,\cdots,\ p-c_\mu\} = \{1,2,\cdots,r\}$$

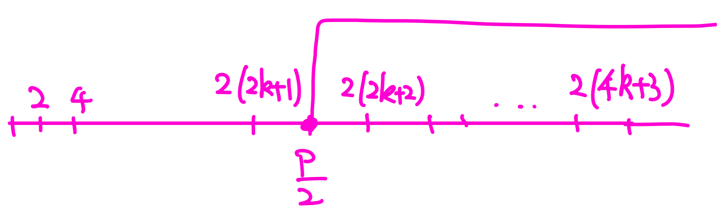
$$\left(p\nmid b_i+c_j \Rightarrow b_i\neq p-c_j\right)$$

$$\Rightarrow r! \equiv b_1b_2\cdots b_r(-c_1)\cdots(-c_\mu) \equiv r!\cdot a^r\cdot(-1)^\mu \mod p$$

$$\Rightarrow \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^\mu \mod p.$$

推论: $$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p\equiv\pm1\,(8) \\ -1 & p\equiv\pm3\,(8). \end{cases}$$

Pf: case: $p=8k+7$



$\Rightarrow \mu=2k+2 \Rightarrow \left(\frac{2}{p}\right)=1$

其它情况, 类似可得

□. -5-9-

定理（二次互反律, quadratic reciprocity law） p,q 奇素数，则

高斯 → 现代数论的开始

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

例: $x^2\equiv 219\ (383)$ 是否有解？

解: $\left(\frac{219}{383}\right)=\left(\frac{73}{383}\right)\cdot\left(\frac{3}{383}\right)=\left(\frac{383}{73}\right)\cdot\left(-\left(\frac{383}{3}\right)\right)$

$= -\left(\frac{18}{73}\right)\left(\frac{2}{3}\right) = -\left(\frac{2}{73}\right)(-1) = \left(\frac{2}{73}\right) = 1$

$\Rightarrow$ 有解.

例: 求 p s.t. $x^2+2x+7\in \mathbb{F}_p[x]$ 不可约.

解: $\Rightarrow p\neq 2,3$

$\left(\frac{-3}{p}\right)=\left(\frac{p}{3}\right)$

不可约 $\Leftrightarrow \left(\frac{-6}{p}\right)=-1 \Leftrightarrow \left(\frac{2}{p}\right)=-\left(\frac{p}{3}\right)$

$\Leftrightarrow \begin{cases} p\equiv 1,7\ (8) \\ p\equiv -1\ (3)\end{cases}$ 或 $\begin{cases} p\equiv 3,5\ (8) \\ p\equiv 1\ (3)\end{cases}$

$\Leftrightarrow p\equiv 17,23,13,19\ (24)$.

问题: 固定 a, $\left(\frac{a}{p}\right)$ 如何随着 p 变化？

现代数论指导

例: $a=-2$, $\Rightarrow \left(\frac{-2}{p}\right)=\begin{cases} 1 & p\equiv 1,3\ (8) \\ -1 & p\equiv 5,7\ (8)\end{cases}$

-5-10- $\left(\frac{-2}{p}\right)=1 \Leftrightarrow p = x^2+2y^2$ 有整数解 $\rightsquigarrow \mathbb{Z}[\sqrt{-2}]=\mathrm{PID}$.

二次互反律的证明

Pf: $(a, 2p)=1$. $r=\frac{p-1}{2}$

$$ia = p\left[\frac{ia}{p}\right] + r_i \qquad 0 \le r_i < p \qquad i=1,\cdots,r.$$

$$\{r_1, r_2, \cdots, r_r\} = \{b_1, \cdots, b_\lambda\} \sqcup \{c_1, \cdots, c_\mu\}$$

$$\Rightarrow \frac{p^2-1}{8} a = p \underbrace{\sum_{i=1}^{r}\left[\frac{ia}{p}\right]}_{A} + \underbrace{\sum_{j=1}^{\lambda} b_j}_{B} + \underbrace{\sum_{k=1}^{\mu} c_k}_{C}$$

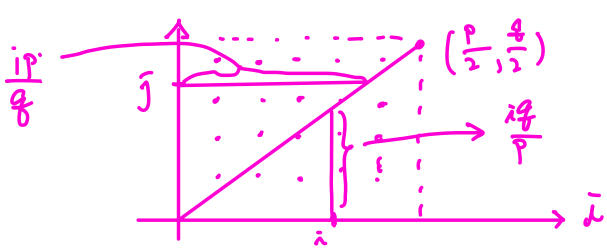
$$\{b_1, \cdots, b_\lambda\} \sqcup \{p-c_1, \cdots, p-c_\mu\} = \{1, 2, \cdots, r\} \Rightarrow B + \mu p - C = \frac{r(r+1)}{2} = \frac{p^2-1}{8}$$

$$\Rightarrow \frac{p^2-1}{8}(a-1) = (A-\mu)p + 2C$$

$$\Rightarrow A \text{与} \mu \text{ 同奇偶} \Rightarrow \left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]}$$

同理: $\left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right]}$

仅需证明 $\displaystyle\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}$



$$\left(\mathbb{Z}/m\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/2^{\alpha}\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/p_1^{\alpha_1}\mathbb{Z}\right)^\times \times \cdots \times \left(\mathbb{Z}/p_s^{\alpha_s}\mathbb{Z}\right)^\times$$

?? ✓ ✓

命题 $\left(\mathbb{Z}/2\mathbb{Z}\right)^\times = \{\bar{1}\}$ $\quad\left(\mathbb{Z}/4\mathbb{Z}\right)^\times = \{\bar{1},\bar{3}\}$

$$\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \cong \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \quad \forall k\geq 3.$$

Pf: $\forall$ 奇数 $a \Rightarrow a^2\equiv 1 \bmod 8 \Rightarrow a^{2^{k-2}} \equiv 1 \bmod 2^k \Rightarrow \operatorname{ord}(a \bmod 2^k) \leq 2^{k-2}$

$2^2 \,\|\, 5^{2^0}-1 \Rightarrow 2^k \,\|\, 5^{2^{k-2}}-1 \quad (k\geq 2).$

$\Rightarrow \operatorname{ord}(5 \bmod 2^k) = 2^{k-2}$

$5^k \equiv 1,5 \bmod 8 \Rightarrow -1 \bmod 2^k \notin \langle 5 \bmod 2^k\rangle$

$\Rightarrow \langle 5 \bmod 2^k\rangle \times \langle -1 \bmod 2^k \rangle \hookrightarrow \left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times \Rightarrow$ ✓

例: 方程 $x^2=1$ 在 $\mathbb{Z}/m\mathbb{Z}$ 上有多少解？

$m = 2^{\alpha} p_1^{\alpha_1}\cdots p_s^{\alpha_s}$ $\quad \alpha\geq 0,\ \alpha_1,\cdots,\alpha_s>0.$

1° $\alpha=0,1 \Rightarrow 2^s$ 个解

2° $\alpha=2 \Rightarrow 2^{s+1}$ 个解

3° $\alpha\geq 3 \Rightarrow 2^{s+2}$ 个解

二次剩余

原根

$\mathbb{F}_p^\times = \langle g\rangle = \{1, g, g^2, \cdots, g^{p-2}\}$

$\Rightarrow (\mathbb{F}_p^\times)^2 = \{1, g^2, g^4, \cdots, g^{p-3}\} \leq \mathbb{F}_p^\times$ 指数为2的子群.

$a\in\mathbb{F}_p^\times.$ $\quad a\in(\mathbb{F}_p^\times)^2 \Leftrightarrow \left(\frac{a}{p}\right)=1$

$\left(\frac{\cdot}{p}\right): \mathbb{F}_p^\times \to \pm 1$ 为群同态. 仅需会计算

$\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$ ← 二次互反律.

欧拉判别法 高斯引理

命题（欧拉判别法）： $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p$

$\forall i = 1, 2, \cdots, r. \Rightarrow ia = \left[\frac{ia}{p}\right] \cdot p + \left\{\frac{ia}{p}\right\} \cdot p$

将 $\left\{\frac{a}{p}\right\} \cdot p\ \left\{\frac{2a}{p}\right\} \cdot p, \cdots, \left\{\frac{ra}{p}\right\} \cdot p$ 从小到大排序，并记为

$$b_1, b_2, \cdots, b_\lambda, c_1, c_2, \cdots, c_\mu$$

其中 $b_1 < b_2 < \cdots < b_\lambda < \frac{p}{2} < c_1 < c_2 < \cdots < c_\mu$ ， $\lambda + \mu = r$.

例 $p = 11$, $a = 3 \Rightarrow \{1, 2, 3, 4, 5\} \rightsquigarrow \{1, 3, 4, 6, 9\}$

$a = 7 \Rightarrow \{1, 2, 3, 4, 5\} \longrightarrow \{2, 3, 6, 7, 10\}$

高斯引理： $p =$ 奇素数， $(a, p) = 1$， $r = \frac{p-1}{2}$，记

$$\mu := \#\left\{ i \in \{1, 2, \cdots, r\} \,\middle|\, ia \text{ 除}p\text{余数} > \frac{p}{2} \right\}$$

则 $\left(\frac{a}{p}\right) = (-1)^\mu$.

例 $\left(\frac{3}{11}\right) = (-1)^2 = 1 \quad \left(\frac{7}{11}\right) = (-1)^3 = -1$

Pf: $\forall i, j. \Rightarrow p \nmid b_i + c_j \Rightarrow b_i \not\equiv p - c_j \bmod p \quad \forall i, j.$

$\Rightarrow \{b_1, b_2, \cdots, b_\lambda, p - c_1, p - c_2, \cdots, p - c_\mu\}$ 为 $\{1, 2, \cdots, r\}$ 的一个重排.

$\Rightarrow r! \equiv b_1 b_2 \cdots b_r (-c_1) \cdots (-c_\mu) \equiv r! \cdot a^r \cdot (-1)^\mu \bmod p$

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

定理（二次互反律，quadratic reciprocity law） p, q 奇素数，则

高斯

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

现代数论的开始

Pf: • $ia = \left[\frac{ia}{p}\right]\cdot p + \left\{\frac{ia}{p}\right\}\cdot p$

$$\Rightarrow \sum_{i=1}^{r} ia = \Bigg(\overbrace{\sum_{i=1}^{r}\left[\frac{ia}{p}\right]}^{A}\Bigg)\cdot p + \overbrace{\sum_{i=1}^{\lambda} b_i}^{B} + \overbrace{\sum_{j=1}^{\mu} c_j}^{C}$$

$$\Rightarrow \frac{p^2-1}{8}\, a = pA+B+C \qquad \cdots\cdots ①$$

• $\{b_1, b_2, \cdots, b_\lambda, p-c_1, p-c_2, \cdots, p-c_\mu\}$ 为 $\{1,2,\cdots,r\}$ 的一个重排.

$$\Rightarrow \frac{p^2-1}{8} = B + p\mu - C \qquad \cdots\cdots ②$$

$$①② \Rightarrow \frac{p^2-1}{8}(a-1) = p(A-\mu)+2C$$

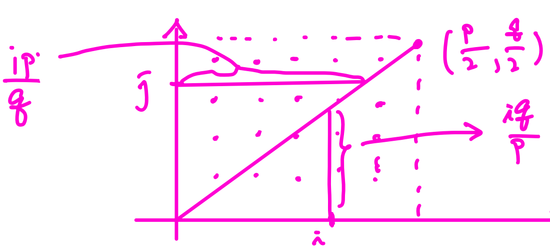
$\Rightarrow$ 若 $2\nmid a$, 则 $A \equiv \mu \bmod 2$

$\Rightarrow$ 若 $2\nmid a$, 则 $\left(\frac{a}{p}\right) = (-1)^A = (-1)^{\sum_{i=1}^{r}\left[\frac{ia}{p}\right]}$

8

$$\Rightarrow \begin{cases} \left(\frac{q}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right]} \\ \left(\frac{p}{q}\right) = (-1)^{\sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right]} \end{cases}$$

仅需证明 $\displaystyle\sum_{i=1}^{\frac{p-1}{2}}\left[\frac{iq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}}\left[\frac{jp}{q}\right] = \frac{p-1}{2}\cdot\frac{q-1}{2}$



例： $x^2\equiv 219\ (383)$ 是否有解？

解： $\left(\frac{219}{383}\right)=\left(\frac{73}{383}\right)\cdot\left(\frac{3}{383}\right)=\left(\frac{383}{73}\right)\cdot\left(-\left(\frac{383}{3}\right)\right)=-\left(\frac{18}{73}\right)\left(\frac{2}{3}\right)=-\left(\frac{2}{73}\right)(-1)=\left(\frac{2}{73}\right)=1 \Rightarrow$ 有解.

例： 求 p s.t. $x^2+2x+7\in\mathbb{F}_p[x]$ 不可约.

解： $\Rightarrow p\neq 2,3$

$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)$

不可约 $\Leftrightarrow \left(\frac{-6}{p}\right)=-1 \Leftrightarrow \left(\frac{2}{p}\right)=-\left(\frac{p}{3}\right) \Leftrightarrow \begin{cases} p\equiv 1,7\ (8) \\ p\equiv -1\ (3)\end{cases}$ 或 $\begin{cases} p\equiv 3,5\ (8) \\ p\equiv 1\ (3)\end{cases} \Leftrightarrow p\equiv 17,23,13,19\ (24)$.

问题： 固定 a, $\left(\frac{a}{p}\right)$ 如何随着 p 变化？

现代数论
推广

例： $a=-2$. $\Rightarrow \left(\frac{-2}{p}\right)=\begin{cases} 1 & p\equiv 1,3\ (8) \\ -1 & p\equiv 5,7\ (8)\end{cases}$

$\left(\frac{-2}{p}\right)=1 \Leftrightarrow p=x^2+2y^2$ 有整数解 $\rightsquigarrow \mathbb{Z}[\sqrt{-2}]=\text{PID}$.

习题： $\left(\frac{m}{p}\right)=1 \Leftrightarrow \exists\ \alpha\geq 1$ s.t. $p^\alpha=x^2-my^2$ 有非平凡解 $\rightarrow$ i.e. $p\nmid x$ & $p\nmid y$,

$\left(\frac{m}{p}\right.$