立方剰余

高校 1 年 1 組 22 番　清水元喜

1　はじめに

本日は数学研究部にお越しいただき、ありがとうございます。この記事では、「立方剰余」について研究していきます。立方剰余とは、大雑把に言えば、「方程式 $x^3 \equiv a \pmod{p}$ に解があるか？」ということです。

2　初等整数論

定義 2.1 (合同式)**.** $a, b, m \in \mathbb{Z}$ について、$a - b$ が m で割り切れるとき

$$a \equiv b \pmod{m}$$

と書き、a と b は m を法として合同であるという。

定義 2.2 ($\mathbb{Z}/m\mathbb{Z}$)**.**

$$\overline{a} = \{x \mid x \equiv a \pmod{m}\}$$

を a の属する剰余類という。すると $\mathbb{Z}$ は m 個の剰余類

$$\overline{0}, \overline{1} \ldots \overline{m-1}$$

に分割される。

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1} \ldots \overline{m-1}\}$$

とおき、

$$\overline{a} + \overline{b} = \overline{a+b}, \qquad \overline{a} \cdot \overline{b} = \overline{ab}$$

と定義することで、$\mathbb{Z}/m\mathbb{Z}$ に和・積が定められ、環になる。[1]

[1] 環とは、簡単に言うと足し算・引き算・掛け算ができる集合のことです。代表例は整数環 $\mathbb{Z}$ など。さらに割り算も出来るときには体と呼びます。こちらの代表例は有理数体 $\mathbb{Q}$ や実数体 $\mathbb{R}$、後に述べる $\mathbb{Z}/p\mathbb{Z}$ など。

定義 2.3 (剰余系)**.** 剰余類から一つずつ代表を選んでできる m 個の数の集合 $\{x_0, x_1, \ldots, x_{m-1}\}$ を $\mathrm{mod}m$ の剰余系という。

定理 2.4 (一次合同式)**.** $(a, m) = 1$ ならば、一次合同式 $ax \equiv b \pmod{m}$ は $\mathrm{mod}m$ で唯一の解を持つ。

証明略

定理 2.5. p が素数ならば、$\mathbb{Z}/p\mathbb{Z}$ は体である。

これは、任意の $a \not\equiv 0 \pmod{p}$ に対して $ax \equiv 1 \pmod{p}$ となるような x が存在することと同値であり、定理 2.4 から導かれます。

定理 2.6. p を素数とすると、

$$(a_1 + a_2 + \cdots + a_k)^p \equiv a_1^p + a_2^p \cdots + a_k^p \pmod{p}$$

証明. 左辺を展開したときの $a_1^p, a_2^p, \ldots, a_k^p$ 以外の項 $a_1^{n_1} a_2^{n_2} \ldots a_k^{n_k} (n_1 + n_2 + \cdots + n_k = p)$ の係数

$$\frac{p!}{n_1! n_2! \ldots n_k!}$$

は整数であり、分子は p で割り切れ、分母は p で割り切れないので $\equiv 0 \pmod{p}$ となる。 □

定理 2.7 (フェルマーの小定理)**.** p を素数とし、$(a, p) = 1$ とする。このとき

$$a^{p-1} \equiv 1 \pmod{p}$$

証明略

定理 2.8 (原始根の存在)**.** p を素数とすると、$p-1$ 乗して初めて 1 に合同になるような数 g が存在する。このとき、$(\mathbb{Z}/p\mathbb{Z})^{\times}$[2]は g を生成元とする巡回群[3]になる。すなわち $\{\overline{1}, \overline{2} \ldots, \overline{p-1}\} = \{\overline{g}, \overline{g^2}, \ldots \overline{g^{p-1}} = \overline{1}\}$ となる。

証明略

3 平方剰余の相互法則

3.1 平方剰余とは

$x^2 \equiv a \pmod{m}$ に解があるとき x は m の平方剰余であるといい、そうでないとき平方非剰余という。以下、基本的に m が素数の場合のみ考えていく。

[2] $\mathbb{Z}/p\mathbb{Z}$ から 0(正確には p と互いに素でない数) を除いた集合

[3] ある G の元 g があって、任意の G の元 x について、$x = g^n$(n は整数) と書けるような集合 G のこと。このとき g を生成元と呼ぶ。

3.2　ルジャンドル記号とその性質

定義 3.1. p を法とした a のルジャンドル記号は次のように定義される。

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & (a \text{ が } p \text{ の平方剰余であるとき}) \\ -1 & (a \text{ が } p \text{ の平方非剰余であるとき}) \end{cases}$$

但し、a が p の倍数であるときは $\left(\frac{a}{p}\right) = 0$ とする。[4]

定理 3.2. ルジャンドル記号について以下の性質が成り立つ。

(a) $\left(\frac{a}{p}\right) = \pm 1$ となる $1 \leq a \leq p-1$ はそれぞれ $(p-1)/2$ 個ずつである。

(b) $a \equiv g^l \pmod{p}$ (g は原始根) とすると $\left(\frac{a}{p}\right) = (-1)^l$

(c)

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

(d) （*Euler* の基準）

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

証明. **(a)** $a = 1^2, 2^2, \ldots (p-1)^2$ に対しては定義より $\left(\frac{a}{p}\right) = 1$。逆に $\left(\frac{a}{p}\right) = 1$ ならば a は $1^2, 2^2, \ldots (p-1)^2$ のどれかに mod$p$ で合同。ところで、$1^2 \equiv (p-1)^2, 2^2 \equiv (p-2)^2, \ldots, (\frac{p-1}{2})^2 \equiv (\frac{p+1}{2})^2 \pmod{p}$。また $a^2 \not\equiv b^2 (1 \leq a \not\equiv b \leq (p-1)/2)$ なので、$\left(\frac{a}{p}\right) = 1$ なる a は $1^2, 2^2, \ldots (\frac{p-1}{2})^2$ の $(p-1)/2$ 個。当然 $\left(\frac{a}{p}\right) = -1$ となる a は残りの $(p-1)/2$ 個。

(b) 略（簡単です）

(c) (b) より自明。

---

[4] $p \mid a$ の時には $\left(\frac{a}{p}\right)$ を定義しないというやり方もありますが、指標を F_p に拡張するときの方法 (定義 5.1) に従って上のような定義を取りました。

(d) (b)(c) を使って適当に場合わけすると示せます。

□

上の定理の (c) より、p, q が素数の場合に $\left(\frac{q}{p}\right)$ が計算できれば $\left(\frac{a}{p}\right)$ が計算できることがわかります。

定理 3.3 (平方剰余の相互法則)**.** p, q を相異なる奇素数とする。

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

第一補充則

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

第二補充則

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

証明は、後で導入するガウス和というものを使う方法が一番わかりやすい（主観的な意見ですが）し、立方剰余相互法則の証明との対比もしやすいので、ここでは与えません。

4 $\mathbb{Z}[\omega]$ について

定義 4.1. (a)

$$\mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}, \omega = e^{\frac{2\pi i}{3}}\}$$

(b) $\xi = a + b\omega$に対して、$\overline{\xi} = a + b\omega^2$を$\xi$の共役という。

(c) （整除性）

$\eta \mid \xi \Leftrightarrow$ ある$\zeta \in \mathbb{Z}[\omega]$ があって、$\xi = \eta\zeta$

(d)

$\epsilon \mid 1$ かつ $\epsilon \in \mathbb{Z}[\omega]$ のとき、ϵは単数であるという。

(e) $\xi = a + b\omega$に対して、

$$N(\xi) = \xi\overline{\xi} = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2$$

と定め、これを ξ のノルムと呼ぶ。

(f) $\eta = \epsilon\xi(\epsilon$は単数) となるとき ηはξに同伴するといい、$\eta \sim \xi$ と書く。

(g) $p \in \mathbb{Z}[\omega]$ が自身の同伴数と単数以外の約数を持たない時、p は（$\mathbb{Z}[\omega]$ における）素数であるという。[5]

定理 4.2 (性質)**. (a)** $N(\xi\eta) = N(\xi)N(\eta)$

(b) ϵ が単数 $\Leftrightarrow N(\epsilon) = 1$

(c) $\mathbb{Z}[\omega]$ の単数は、$\pm 1, \pm\omega, \pm\omega^2$ の *6* つである。

(d) $N(\xi)$ が有理素数ならば、ξ は素数である。

(e) 0 でも単数でもない任意の $\mathbb{Z}[\omega]$ の整数は素数の積で表せる。

(f) （割り算定理）任意の $\gamma, \gamma_1 \neq 0$ に対して、ある$\kappa \in \mathbb{Z}[\omega]$ があって、

$$\gamma = \kappa\gamma_1 + \gamma_2 \quad N(\gamma_2) < N(\gamma_1)$$

と書ける。

(g) （素因数分解の一意性）整数を素数の積として表す方法は、自明な差異[6]を除いて一意的である。

(h) π が素数のとき、$\pi \mid \beta\gamma \Rightarrow \pi \mid \beta$または$\pi \mid \gamma$

(i) （$\mathbb{Z}[\omega]$ の素数）$\mathbb{Z}[\omega]$ の素数は次の三種類である。

(i) $1 - \omega$ とその同伴数

(ii) $q \equiv 2 \pmod 3$ となる有理素数 q

(iii) $N(\pi) = \pi\overline{\pi} = p$ (p は有理素数) となる $\pi \in \mathbb{Z}[\omega]$

(iii) のとき、$p \equiv 1 \pmod 3$ となることが容易にわかる。**これから先の文中で注釈なしに p, q, π の文字を使うときは、それぞれ $\mathbf{mod\,3}$ で 1 に合同な有理素数、$\mathbf{mod\,3}$ で 2 に合同な有理素数、$\mathbb{Z}[\omega]$ の素数を指すものとする。**

---

[5]以下、単に素数といえばこの意味。これに対して $\mathbb{Z}$ における素数のことを「有理素数」と呼びます。

[6]素数の順序、同伴する素数の表れ方、単数の取り方

(j) πが素数ならば、$\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ は元の数 $N(\pi)$ の剰余体である。具体的には、

$$\begin{cases} \{a+b\omega \mid 0 \leq a < q, 0 \leq b < q\} & (\pi = q \text{ の場合}) \\ \{0, 1, \ldots p-1\} (\pi\overline{\pi} = p \text{ の場合}) \end{cases}$$

がそれぞれ $\mathrm{mod}\pi$ の剰余系である。

(k) πが素数で、$(\alpha, \pi) = 1$ ならば、

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$$

(l) πを法とする原始根が存在する。

証明. **(a)〜(h)** 自明だったり、結論が「いかにもなりたちそう」な割りに証明がめんどくさかったり[7]するので証明略。

(i) $1-\omega$ はノルムが 3 なので素数。

$\xi \mid q$ とすると、$N(\xi) \mid N(q) = q^2$。ところで

$$N(\xi) = a^2 - ab + b^2 \equiv 4a^2 - 4ab + b^2 = (2a-b)^2 \equiv 0 \text{ または } 1 \pmod{3}$$

なので、$N(\xi) = q$ となることはありえない。ゆえにξは単数または q の同伴数となる。即ち q は素数。次に $p \equiv 1 \pmod 3$ の場合を考えると、平方剰余の相互法則（定理 3.3）より、

$$\begin{aligned} \left(\frac{-3}{p}\right) &= \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) (-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}} \\ &= \left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1 \end{aligned}$$

だから、

$$p \mid a^2 + 3 = (a + \sqrt{-3})(a - \sqrt{-3}) = (a+1+2\omega)(a-1-2\omega)$$

となる $a \in \mathbb{Z}$ が存在する。p が素数なら、$p \mid (a+1+2\omega)$ または $p \mid (a-1-2\omega)$。ところが、$a \in \mathbb{Z}$ に対して、$\dfrac{a \pm 1}{p} \pm \dfrac{2}{p}\omega$は整数ではないからこれは誤り。よって、$p = \pi\gamma (\pi, \gamma$はいずれも単数ではない$)$ と書けて、$p^2 = N(\pi)N(\gamma)$ だから $N(\pi) = N(\gamma) = p$。したがって πはノルムが有理素数なので素数、また $p = N(\pi) = \pi\overline{\pi}$。なお、素因数分解の一意性より、$p = \pi\overline{\pi}$ と書き表す方法は一意的。

[7] 素因数分解の一意性とかその典型。でもほんとはこれが成り立つ代数体はむしろ例外的なんですが、そういうちゃんとした議論は代数的整数論の教科書に任せることにしましょう。

(j) 任意の $\mathbb{Z}[\omega]$ に属する数に対し、それと $\mathrm{mod}\pi$ で合同な数が S に含まれること、そして S に属する数は全て $\mathrm{mod}\pi$ で異なることをいえば、S が $\mathrm{mod}\pi$ の剰余系の一組であることは示されます。証明はそんなに難しくはないのですがめんどくさいので（笑)、省略します。

(k)

$$\prod t \equiv \prod at = a^{N(\pi-1)} \prod t \pmod{\pi}(t \text{ は } \mathrm{mod}\ \pi \text{の剰余系を動く})$$

$\prod t \not\equiv 0 \pmod{\pi}$ より、

$$a^{N(\pi)-1} \equiv 1 \pmod{\pi}$$

(l) 略（有理整数のときと同様）

□

これで、$\mathbb{Z}[\omega]$ が $\mathbb{Z}$ と似たような性質を持つことがわかってもらえたと思います。実は、立方剰余について考えるためにこの $\mathbb{Z}[\omega]$ という数学的対象は考え出されたのです。そしてやがて代数的整数論、類体論へと発展していくのです。

5　ガウス和とヤコビ和

定義　5.1 (指標)**.** 以下、剰余体 $\mathbb{Z}/p\mathbb{Z}$ のことを F_p と書く。[8]また、$F_p - \{0\}$ を $F_p^\times$、$\mathbb{C} - \{0\}$ を $\mathbb{C}^\times$ と書く。$\chi : F_p^\times \to \mathbb{C}^\times$が、任意の $a, b \in F_p^\times$ に対して$\chi(ab) = \chi(a)\chi(b)$ を満たすとき、χは指標であるという。εで、任意の $a \in F_p^\times$に対して$\varepsilon(a) = 1$ であるような指標をあらわすことにする。$\chi \neq \varepsilon$ に対しては$\chi(0) = 0$、εに対しては$\varepsilon(0) = 1$ と定めることで、指標を F_p上の関数に拡張できる。

定理 5.2 (指標の性質)**. (a)** $\chi(1) = 1$

(b) $a \neq 0$ のとき $(\chi(a))^{p-1} = 1$

(c) $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$

証明は指標の定義より簡単に出来ます。

定理 5.3. $\chi \neq \varepsilon$を F_pの指標とすると、

$$\sum_{t \in F_p} \chi(t) = 0$$

[8]この F は”finite field”の頭文字でしょうか ？

証明. $\chi \neq \varepsilon$ より、$\chi(a) \neq 1$ となる $a \in F_p^\times$ がある。よって、$S = \sum_{t \in F_p} \chi(t)$ とおくと、

$$\begin{aligned}\chi(a)S &= \sum_{t \in F_p} \chi(at) \\ &= \sum_{t \in F_p} \chi(t) = S(\because F_p^\times \text{は群})\end{aligned}$$

$\chi(a) \neq 1$ より、$S = 0$。 □

定義 5.4 (指標群)**.** $\hat{F_p} = \{\chi \mid \chi \text{は } F_p \text{の指標 }\}$ とする。指標の積を $\chi\lambda(a) = \chi(a)\lambda(a)$、逆元を $\chi^{-1}(a) = \chi(a)^{-1}$ と定義することで、 $\hat{F_p}$ は ε を単位元とする可換群となる。

定理 5.5. $\hat{F_p}$ は位数 $p-1$ の巡回群である。

証明. $F_p^\times$ の原始根を g とすると、$a \in F_p^\times$ について、$a = g^l$ (l は整数) と書ける。よって、

$$\chi(a) = \chi(g)^l$$

従って、χ は $\chi(g)$ の値によって一意的に定まる。$\chi(g)$ は 1 の $p-1$ 乗根だから、その取り方は高々 $p-1$ 通り。ここで

$$\lambda(g) = \zeta = e^{\frac{2\pi i}{p-1}}$$

とおくと、$\lambda^0 = \varepsilon, \lambda, \lambda^2, \ldots, \lambda^{p-2} \in \hat{F_p}$ かつこれらは全て異なる。即ち $\hat{F_p}$は λを生成元とする位数 $p-1$ の巡回群である。 □

定理 5.6. $a \neq 1$ のとき

$$\sum_{\chi \in \hat{F_p}} \chi(a) = 0$$

証明. λで 5.5 の証明で用いた指標と同じものをさすことにする。$\sum_\chi \chi(a) = S$ とおくと、

$$\begin{aligned}\lambda S &= \sum_\chi \lambda(a)\chi(a) \\ &= \sum_\chi \lambda\chi(a) \\ &= \sum_\chi \chi(a) = S(\because \hat{F_p}\text{は群})\end{aligned}$$

$\lambda(a) \neq 1$ より、$S = 0$。 □

定義 5.7 (ガウス和)**.** $\chi \in \hat{F_p}, a \in F_p$に対し、

$$g_a(\chi) = \sum_{t \in F_p} \chi(t)\zeta^{at}$$

をガウス和という。$g_1(\chi) = g(\chi)$ と略記する。但し ζ は 1 の原始 p 乗根（例えば $e^{\frac{2\pi i}{p}}$）とする。

定理 5.8. $a \neq 0, \chi \neq \varepsilon$のとき、$g_a(\chi) = \chi(a^{-1})g(\chi)$

証明.

$$\begin{aligned} g_a(\chi)\chi(a) &= \chi(a)\sum_t \chi(t)\zeta^{at} \\ &= \sum_t \chi(at)\zeta^{at} \\ &= \sum_t \chi(t)\zeta^t = g(\chi) \end{aligned}$$

□

定理 5.9. $\chi \neq \varepsilon$ならば、

$$|g(\chi)| = \sqrt{p},\ g(\chi)g(\overline{\chi}) = \chi(-1)p$$

証明. $\sum_{a \in F_p} g_a(\chi)\overline{g_a(\chi)}$ を二通りの方法で計算する。

$a \neq 0$ に対して、

$$\begin{aligned} g_a(\chi) &= \chi(a)g(\chi) \\ \overline{g_a(\chi)} &= \overline{\chi(a)g(\chi)} = \chi(a^{-1})\overline{g(\chi)} \\ g_a(\chi)\overline{g_a(\chi)} &= g(\chi)\overline{g(\chi)} = |g(\chi)|^2 \end{aligned}$$

$a = 0$ のとき、

$$g_0(\chi) = \sum_t \chi(t) = 0$$

よって、

$$\sum_{a \in F_p} g_a(\chi)\overline{g_a(\chi)} = (p-1)|g(\chi)|^2$$

一方、

$$\begin{aligned} g_a(\chi)\overline{g_a(\chi)} &= \sum_x \chi(x)\zeta^{ax}\sum_y \overline{\chi(y)\zeta^{ay}} \\ &= \sum_{x,y} \chi(x)\overline{\chi(y)}\zeta^{ax-ay} \end{aligned}$$

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_a \sum_{x,y} \chi(x)\overline{\chi(y)}\zeta^{ax-ay}$$
$$= \sum_{x,y} \chi(x)\overline{\chi(y)} \sum_a \zeta^{a(x-y)}$$

$\sum_t \zeta^{nt}$は $n=0$ のとき $p, n \neq 0$ のとき 0 だから、

$$= \sum_{x=y} \chi(x)\overline{\chi(y)}p$$
$$= \sum_x \chi(x)\overline{\chi(x)}p$$
$$= (p-1)p \quad (\chi(0)=0 \text{ に注意})$$

ゆえに、$|g(\chi)|^2 = p$。また、$\chi(-1) = \pm 1$ より $\overline{\chi(-1)} = \chi(-1)$ に注意すると、

$$\overline{g(\chi)} = \sum_t \overline{\chi(t)}\zeta^{-t}$$
$$= \chi(-1)\sum_t \overline{\chi(-t)}\zeta^{-t}$$
$$= \chi(-1)g(\overline{\chi})$$

従って、$g(\chi)\overline{g(\chi)} = p$ より、

$$g(\chi)g(\overline{\chi}) = \chi(-1)p$$

□

定義 5.10 (ヤコビ和)**.** $\chi, \lambda \in \hat{F_p}$のとき、

$$J(\chi,\lambda) = \sum_{\substack{a+b=1 \\ a,b\in F_p}} \chi(a)\lambda(b)$$

をヤコビ和と呼ぶ。

定理 5.11 (ヤコビ和の性質)**.** $\chi, \lambda \neq \varepsilon$とすると、

$$J(\chi,\chi^{-1}) = -\chi(-1)$$

$\chi\lambda \neq \varepsilon$ならば

$$J(\chi,\lambda) = \frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$
$$|J(\chi,\lambda)| = \sqrt{p}$$

証明.

$$J(\chi,\chi^{-1}) = \sum_{\substack{a+b=1\\ b\neq 0}} \chi(\frac{a}{b}) = \sum_{a\neq 1} \chi(\frac{a}{1-a})$$

さて、ここで $\frac{a}{1-a}$ がどのような値をとるか考えると、$\frac{a}{1-a} = \frac{a'}{1-a'}$ となるならば $a = a'$ となることがすぐにわかる。また $\frac{a}{1-a} = c$ とおくと、$c \neq -1$。ゆえに、a が $F_p^\times - \{1\}$ を動くとき、c は $F_p^\times - \{-1\}$ を動く。よって、

$$J(\chi,\chi^{-1}) = \sum_{c\neq -1} \chi(c) = \sum_{c} \chi(c) - \chi(-1) = -\chi(-1)$$

次に、

$$\begin{aligned} g(\chi)g(\lambda) &= (\sum_x \chi(x)\zeta^x)(\sum_y \lambda(y)\zeta^y) \\ &= \sum_{x,y} \chi(x)\lambda(y)\zeta^{x+y} \\ &= \sum_t \sum_{x+y=t} \chi(x)\lambda(y)\zeta^t \\ &= \sum_t \zeta^t \sum_{x+y=t} \chi(x)\lambda(y) \end{aligned}$$

$t = 0$ のとき

$$\begin{aligned} \sum_{x+y=0} \chi(x)\lambda(y) &= \sum_x \chi(x)\lambda(-x) \\ &= \lambda(-1)\sum_x \chi\lambda(x) \\ &= 0 \quad (\because \chi\lambda \neq \varepsilon) \end{aligned}$$

$t \neq 0$ のとき、$x = tx', y = ty'$ とおいて、

$$\begin{aligned} \sum_{x+y=t} \chi(x)\lambda(y) &= \chi\lambda(t) \sum_{x'+y'=1} \chi(x')\lambda(y') \\ &= \chi\lambda(t)J(\chi,\lambda) \end{aligned}$$

したがって、

$$\begin{aligned} g(\chi)g(\lambda) &= \sum_t \chi\lambda(t)\zeta^t J(\chi,\lambda) \\ &= g(\chi\lambda)J(\chi,\lambda) \end{aligned}$$

すなわち

$$J(\chi,\lambda)=\frac{g(\chi)g(\lambda)}{g(\chi\lambda)}$$

両辺の絶対値を取って $|g(\chi)|=\sqrt{p}$ を用いると、

$$|J(\chi,\lambda)|=\sqrt{p}$$

がわかる。 □

定理 5.12. $p\equiv 1 \pmod{n}, \chi\in\hat{F_p}$の位数[9]を n とすると、

$$g(\chi)^n=\chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\dots J(\chi,\chi^{n-2})$$

系 5.13. χの位数が 3 のとき、$p\equiv 1 \pmod{3}$ ならば

$$g(\chi)^3=pJ(\chi,\chi)$$

証明. 下の系のみ示します。(一般の場合も証明は全く同様です)。
定理 5.11 より、

$$\begin{aligned}
g(\chi)^2&=J(\chi,\chi)g(\chi^2)\\
g(\chi^2)&=g(\overline{\chi})(\because \chi\text{の位数は } 3)\\
g(\chi)^2&=J(\chi,\chi)g(\overline{\chi})\\
g(\chi)^3&=g(\chi)g(\overline{\chi})J(\chi,\chi)\\
&=\chi(-1)pJ(\chi,\chi)(\because \text{定理 } 5.9)\\
&=\chi^3(-1)pJ(\chi,\chi)=pJ(\chi,\chi)
\end{aligned}$$

□

6 立方剰余相互法則

さて、ようやく準備が終わりました。本題の立方剰余にとりかかりましょう。既に調べたガウス和、ヤコビ和の性質を使えば、立方剰余相互法則自体はかなり簡単に示すことができます。(補充則の証明はここでは与えません。)

[9] $\chi^l=\varepsilon$ を満たす最小の l

6.1 その前に

平方剰余の相互法則をまだ示していなかったのでここでガウス和を用いた証明を与えます。既に補充則（実際には第一補充則だけでよいが）は示されているものとします。$\left(\frac{a}{p}\right)$ は位数が 2 の指標とみなせるので、ガウス和 $\sum_t \left(\frac{t}{p}\right)\zeta^{at}$ を考えることが出来ます。以下、見やすくするために、$\left(\frac{a}{p}\right) = \chi_p(a)$ と書くことにします。また、

$$g_a = g_a(\chi_p) = \sum_t \left(\frac{t}{p}\right)\zeta^a t, \quad g = g_1$$

と書くことにします。$\chi_p(a) = \pm 1$ より、$\overline{\chi_p} = \chi_p$。定理 5.9 より、

$$g(\chi_p)g(\overline{\chi_p}) = g^2(\chi_p) = \chi_p(-1)\cdot p = (-1)^{\frac{p-1}{2}}p$$

$(-1)^{\frac{(p-1)}{2}}p = p^*$ とおくと、

$$\begin{aligned} g^{q-1} = (g^2)^{(q-1)/2} &\equiv \left(\frac{p^*}{q}\right) \pmod q \quad (\because \text{定理 } 3.2(d)) \\ g^q &\equiv g\cdot\left(\frac{p^*}{q}\right) \pmod q \\ g^q &= (\sum_t \left(\frac{t}{q}\right)\zeta^t)^q \\ &\equiv \sum_t \left(\frac{t}{q}\right)^q \zeta^{tq} \pmod q \quad (\because \text{定理 } 2.6) \end{aligned}$$

q は奇素数なので、

$$= \sum_t \left(\frac{t}{q}\right)\zeta^{tq} = g_q = \left(\frac{q^{-1}}{p}\right)\cdot g$$

したがって、

$$\left(\frac{q^{-1}}{p}\right)\cdot g \equiv \left(\frac{p^*}{q}\right)\cdot g \pmod q$$

両辺に g をかけて $g^2 = p^*$で割って、

$$\left(\frac{q^{-1}}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod q$$
$$\left(\frac{p^*}{q}\right)\left(\frac{q}{p}\right) \equiv 1 \pmod q$$

左辺は ± 1 をとり、q が奇素数かつ $q \geq 3$ だから、

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

$p^* = (-1)^{\frac{p-1}{2}}$ だったから、

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

6.2 3 次剰余指標の定義

定理 6.1. πが素数で $N(\pi) \neq 3$ の時、$1, \omega, \omega^2$ は $\bmod \pi$ で互いに合同でない。

証明略

定理 6.2. πは素数で $N(\pi) \neq 3$ とすると、$\pi \nmid \alpha \in \mathbb{Z}[\omega]$ に対し

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m \pmod{\pi}$$

となる $m = 0, 1, 2$ が一意に決まる。

証明.

$\alpha^{N(\pi)-1} - 1 = (\alpha^{\frac{N(\pi)-1}{3}} - 1)(\alpha^{\frac{N(\pi)-1}{3}} - \omega)(\alpha^{\frac{N(\pi)-1}{3}} - \omega^2) \equiv 0 \pmod{\pi}$(∵ 定理4.2($k$))

これと定理 4.2(h) より示される。 □

定義 6.3 (3 次剰余指標)**.** πは素数、$N(\pi) \neq 3$ の時ルジャンドル記号に対応する $\left(\frac{\alpha}{\pi}\right)_3$ を次のように定義する。$\alpha \in \mathbb{Z}[\omega]$。

$$\left(\frac{\alpha}{\pi}\right)_3 = \begin{cases} 0 & (\pi \mid \alpha) \\ \omega^m & (\pi \nmid \alpha) \text{ 但し、}\omega^m\text{は定理 6.2 におけるものと同じ。} \end{cases}$$

定理 6.4 ($\left(\frac{\alpha}{\pi}\right)_3$ の性質)**. (a)** $\left(\frac{\alpha}{\pi}\right)_3 = 1 \Leftrightarrow x^3 \equiv \alpha \pmod{\pi}$ に解がある。

(b)

$$\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$$

(c)

$$\alpha^{\frac{1}{3}(N(\pi)-1)} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}$$

(d) $\alpha \equiv \beta \pmod{\pi}$ ならば $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$

証明略

(c) が Euler の基準（定理 3.2(d)）の拡張になっています。

また、ちょっとした思惑があって[10]$\left(\frac{\alpha}{\pi}\right)_3$ を$\chi_\pi(\alpha)$ とも書くことにします。

定理 6.5.

$$\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$$

$$\overline{\chi_\pi(\alpha)} = \chi_{\overline{\pi}}(\overline{\alpha})$$

証明. 上のほうは明らか。

$$\alpha^{\frac{1}{3}(N(\pi)-1)} \equiv \chi_\pi(\alpha) \pmod{\pi}$$

の共役を取って

$$\overline{\alpha}^{\frac{1}{3}(N(\pi)-1)} \equiv \overline{\chi_\pi(\alpha)} \pmod{\overline{\pi}}$$

$N(\pi) = N(\overline{\pi})$ に注意すれば定義より $\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\chi_\pi(\alpha)}$ □

系 6.6. q が有理素数で $\mathbb{Z}[\omega]$ の素数の時

$$\chi_q(\overline{\alpha}) = \chi_q(\alpha^2)$$

$(n, q) = 1$ で n が有理整数ならば、

$$\chi_q(n) = 1$$

証明. $\overline{q} = q, \overline{n} = n$ に注目し定理 6.5 を使えば自明。 □

定義 6.7 (primary)**.** $\pi \in \mathbb{Z}[\omega]$ が $\pi \equiv 2 \pmod{3}$ を満たすとき、π は *primary* な数であるという。πが素数であるときにはπは*primary* であるという。[11]

π〜q（有理素数）の時には、$\pi = q$ が *primary* である。$\pi\overline{\pi} = p$ のときは、$\pi = a + b\omega (a \equiv 2, b \equiv 0 \pmod{3})$ が *primary* である。後者の場合はこれを満たすように π が一意的に取れることはそれほど自明ではないので、証明する。[12]

---

[10] 読んでいけばわかります

[11] このあたりの用語の使い方は標準的ではないかもしれません。

[12] なんでこんな定義をするのかは後々明かされるでしょう

表 1: mod3 の剰余系

$\boxed{0}$	1	2
ω	$1+\omega$	$\boxed{2+\omega}$
2ω	$\boxed{1+2\omega}$	$2+2\omega$

証明. mod3 の剰余系は上に示すような構造をしている。このうち、丸[13]で囲ったものは $1-\omega$ で割り切れるので、素数と合同にはならない。ここで例えば $\pi \equiv 2\omega \pmod 3$ とすると、

$$\pi \equiv 2\omega, -\pi \equiv \omega, \omega\pi \equiv 1+\omega, -\omega\pi \equiv 2+2\omega, \omega^2\pi \equiv 2, -\omega^2\pi \equiv 1 \pmod 3$$

となって、π の同伴数のうち primary であるものが唯一つ存在する。π が他の数に合同な場合でも同様の議論が明らかに成り立つ。よって π の同伴数のうち primary であるものが唯一つ存在する。 □

6.3 立方剰余相互法則

定理 6.8 (立方剰余相互法則)**.** π_1, π_2 は *primary* で $N(\pi_1) \neq N(\pi_2)$、$N(\pi_1), N(\pi_2) \neq 3$ とすると、

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$$

定理 6.9 (補充則)**.** πは素数で、$N(\pi) \neq 3$ とする。$\pi = q$ なら $q = 3m-1$、$\pi\overline{\pi} = p$ でπ が *primary* のときは $a = 3m-1$ と書ける。このとき

$$\chi_\pi(1-\omega) = \omega^{2m}$$

6.4 相互法則の証明

ようやくここまで辿り着きました。この証明を書くためにここまで頑張ってきたんです！

6.4.1 $\pi_1 = q_1, \pi_2 = q_2$ の場合

系 6.6 より、$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1) = 1$。

[13] 丸じゃなくて四角ではないか、とか突っ込まないで

6.4.2　π_1, π_2 のうち少なくとも一方が $\pi\overline{\pi} = p$ を満たす場合

まず、$\pi\overline{\pi} = p$ の時、$\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ の構造は $\mathbb{Z}/p\mathbb{Z} = F_p$ と同じなので、χ_π は F_p上の位数 3 の指標とみなせます。したがって、平方剰余の相互法則の証明からも類推できるように、$g(\chi_\pi)^3$ を計算するのが証明のミソです。そしてそれは系 5.13 より、$J(\chi_\pi, \chi_\pi)$ の値がわかれば求まります。ヤコビ和と χ_π の定義から、$J(\chi_\pi, \chi_\pi) \in \mathbb{Z}[\omega]$ です。

補題 6.10. $J(\chi_\pi, \chi_\pi) \sim \pi$または$\overline{\pi}$。

証明. $J(\chi_\pi, \chi_\pi) = x$ とおくと 定理 5.11 より、$|x|^2 = x\overline{x} = p$。$p = \pi\overline{\pi}$は p の素因数分解であり、$\mathbb{Z}[\omega]$ では素因数分解は一意的であるから、$x \sim \pi$または $x \sim \overline{\pi}$。 □

補題 6.11.

$$J(\chi_\pi, \chi_\pi) \equiv 2 \pmod 3$$

証明.

$$\begin{aligned} g(\chi_\pi)^3 &= (\sum_t \chi_\pi(t)\zeta^t)^3 \\ &\equiv \sum_t \chi_\pi(t)^3\zeta^{3t} \pmod 3 \quad (\because \text{定理 2.6}) \\ &= -1 \quad (\chi_\pi(0)^3 = 0, t \neq 0 \text{ ならば} \chi_\pi(t)^3 = 1 \text{ なので}) \end{aligned}$$

$g(\chi_\pi)^3 = pJ(\chi_\pi, \chi_\pi)$ で $p \equiv 1 \pmod 3$ より示された。 □

補題 6.12. $n \not\equiv 0 \pmod{N(\pi) - 1}$ ならば、$\sum_{a \in F_p} a^n \equiv 0 \pmod \pi$。

証明. $t \not\equiv 0 \pmod p$ に対し、

$$\begin{aligned} \sum_a a^n &\equiv \sum_a (ta)^n \pmod p \\ &= t^n \sum_a a^n \end{aligned}$$

$t \not\equiv 0 \pmod p$ より自明。 □

補題 6.13. $J(\chi_\pi, \chi_\pi) = \pi$

証明. 補題 6.10 と 6.11 から、π が primary で $\pi\overline{\pi} = p$ とすると、
$J(\chi_\pi, \chi_\pi) = \pi$ または$\overline{\pi}$。

$$\begin{aligned}
J(\chi_\pi, \chi_\pi) &= \sum_{a+b=1} \chi_\pi(a)\chi_\pi(b) \\
&= \sum_{a} \chi_\pi(a(1-a)) \\
&\equiv \sum_{a} (a - a^2)^{\frac{1}{3}(p-1)} \pmod{\pi} \\
&= \sum_{n=\frac{1}{3}(p-1)}^{\frac{2}{3}(p-1)} \sum_{a} k_n a^n \quad (k_n \text{は整数}) \\
&\equiv 0 \pmod{\pi} \quad (\because \text{補題 6.12})
\end{aligned}$$

従って、$J(\chi_\pi, \chi_\pi) \equiv 0 \pmod{\pi}$。$\overline{\pi} \not\equiv 0 \pmod{\pi}$ より、$J(\chi_\pi, \chi_\pi) = \pi$。 □

$\therefore \boldsymbol{g(\chi_\pi)^3 = p\pi}$

6.4.3 $\pi_1\overline{\pi_1} = p, \pi_2 = q$ の場合

証明.

$$\begin{aligned}
g(\chi_\pi)^3 &= p\pi \\
g^{q^2-1} &= (p\pi)^{\frac{1}{3}(q^2-1)} \equiv \chi_q(p\pi) \pmod{q} \\
g^{q^2} &\equiv \chi_q(p\pi)g \pmod{q}
\end{aligned}$$

一方、

$$\begin{aligned}
g^{q^2} &= (\sum_t \chi_\pi(t)\zeta^t)^{q^2} \\
&\equiv (\sum_t \chi_\pi(t)^q \zeta^{tq})^q \pmod{q} \quad (\because \text{定理 2.6}) \\
&\equiv \sum_t \chi_\pi(t) q^2 t^{tq^2} \pmod{q}
\end{aligned}$$

$q^2 \equiv 1 \pmod{3}$ より

$$\begin{aligned}
&= \sum_t \chi_\pi(t) t^{tq^2} = g_{q^2} \\
g_{q^2} &= \chi_\pi((q^2)^{-1})g \text{ だから、} \\
\chi_\pi((q^2)^{-1})g &\equiv \chi_q(p\pi)g \pmod{q}
\end{aligned}$$

$g(\overline{\chi_\pi})$ を両辺にかけて $g(\chi_\pi)g(\overline{\chi_\pi}) = \chi_\pi(-1)p$ で割って、

$$\chi_\pi((q^2)^{-1}) \equiv \chi_q(p\pi) \pmod{q}$$

系 6.6 より $\chi_q(p) = 1, \chi_\pi((q^2)^{-1}) = \chi_\pi(q), 1, \omega, \omega^2$は互いに $\bmod q$ で合同でないから、

$$\chi_\pi(q) = \chi_q(\pi)$$

□

6.4.4 $\pi_1\overline{\pi_1} = p_1, \pi_2\overline{\pi_2} = p_2$ の場合

証明. 6.4.3 節と同様にして、

$$\chi_{\pi_1}(p_2^2) = \chi_{\overline{\pi_2}}(\pi_1 p_1)$$
$$\chi_{\overline{\pi_2}}(p_1^2) = \chi_{\pi_1}(\overline{\pi_2} p_2)$$

を得る。両辺を掛け合わせて共通因数で割ると、[14]

$$\chi_{\pi_1}(\pi_2)\chi_{\overline{\pi_2}}(\overline{\pi_1}) = 1$$

$\chi_{\overline{\pi}}(\overline{\alpha}) = \overline{\chi_\pi(\alpha)}$ だったから、

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$$

□

6.5 補充則について

$\pi = q$ のときは簡単に証明できるのですが、$\pi\overline{\pi} = p$ のときがかなりやっかいです。$\left(\dfrac{\alpha}{\tau}\right)_3$ を τ が素数でないときにも拡張する必要があり、紙面や締切などの都合上割愛させていただきます。

6.6 あとがき

やっと終わりました。当初の予定より大幅に長くなってしまいました。その割には $\mathbb{Z}[\omega]$ の性質とかにページを割いたので内容が薄いかもしれません。この記事を読んで数論に興味を持ってくれる人がいると嬉しいです。

[14] ここの計算は端折りましたが、$p/\pi = \overline{\pi}$ に注意してください。

特にガウス和を使った証明は主観的には二つの素数が「ひっくり返る」ところが非常に面白いと思います。

下書き自体は比較的早く出来ていたのに、LaTeX を使って打ち込むのに予想以上に時間がかかってしまったのは今後の反省材料です。なお、この記事についての指摘、感想があれば s.genki0605@gmail.com までお寄せください。

最後までお読みくださってありがとうございました！

参考文献

[1] G. H. Hardy, E. M. Wright 「数論入門 I」（シュプリンガー数学クラシックス, 2001）

[2] J. H. Silverman 「はじめての数論」（ピアソンエデュケーション,2007）

[3] T. M. Apostol *Introduction to Analytic Number Theory* (Springer,1976)

[4] 倉田 令二朗「平方剰余の相互法則—ガウスの全証明」（日本評論社,1992）