

6 $x^3 \equiv 2 \pmod{p}$ について

定理： $f(x) = x^3 - 2$ とする．素数 $p \geq 5$ について，以下が成り立つ．

- (A) $p \equiv 2 \pmod{3}$ ならば， $f(x)$ は 1 次式と 2 次式の積に既約分解する．
- (B) $p \equiv 1 \pmod{3}$ ならば，
 - (a) 条件 (Q) ならば， $f(x)$ は 3 つの 1 次式の積に既約分解する（注：このとき 1 次式はすべて異なる）．
 - (b) そうでなければ， $f(x)$ は既約である．

例： $p = 5$ とすると， $f(x) = (x - 3)(x^2 + 3x + 4)$ in $\mathbb{F}_5[x]$ ．

注意： 素数 $p \geq 5$ について， $p \equiv 1 \pmod{3} \Leftrightarrow \exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, x^2 + 3y^2 = p$ である．この書き方は符号を除いて一意的である．よって，条件 (Q) は $y \in 3\mathbb{Z}$ と同じである．

証明： $\Rightarrow$ は後のヤコビ和を用いた証明もあるが，ここでは初等的な証明を与える． $S = \{(i, j, k) \in \mathbb{Z}^2 \times \mathbb{Z}_{>0} \mid i^2 + 3j^2 = kp\}$ とする． $z \in \mathbb{Z}$ を $z^2 \equiv -3 \pmod{p}$ と取れる（平方剰余の相互法則）ことから， $S \neq \emptyset$ ． $(i, j, k) \in S$ で k が最小のものを取る． $k < p$ に注意する（何故なら $z \in (0, p/2)$ と取れるから $pk \leq (p/2)^2 + 3$ で， $k \leq 1 + p/4$ ）． $i^2 + 3j^2 = kp$ である． $k > 1$ として， $-k/2 < d, e \leq k/2$ をそれぞれ i, j を k で割った余りとすると， $d^2 + 3e^2 = kk_1$ と書ける（ここで $k_1 < k$ ．等号不成立が一見非自明だが， $d, e = k/2$ であれば p は偶数になってしまう）． $(A^2 + 3B^2)(C^2 + 3D^2) = (AC + 3BD)^2 + 3(BC - AD)^2$ より $(\frac{id+3je}{k})^2 + 3(\frac{jd-ie}{k})^2 = k_1p$ である．これを繰り返せばよい．

よくある別証明も書いておこう． $\mathbb{Z}[\zeta_3]$ は UFD である． $p|(z + \sqrt{-3})(z - \sqrt{-3})$ で $z + \sqrt{-3} = (z+1) + 2\zeta_3$ より， p は素元ではない．ノルムを考えると $p = \pi\bar{\pi}$ と素元分解することが分かる． $\pi = a + b\zeta_3$ のとき $p = N(\pi) = a^2 - ab + b^2$ である． $x = \frac{a+b}{2}, y = \frac{a-b}{2}$ なら $x^2 + 3y^2 = p$ なので， a と b の偶奇が同じであればよい． π の相伴元は $\pm(a + b\zeta_3), \pm(b + (b-a)\zeta_3), \pm((b-a) - a\zeta_3)$ なので，そのように取ることができる．

表示の一意性の証明は以下の通りである． $\mathbb{Z}[\zeta_3]$ は UFD である． $p = x^2 + 3y^2$ について $x + y\sqrt{-3} = (x+y) + 2y\zeta_3$ の相伴元は $\pm((x+y) + (2y)\zeta_3) = \pm(x + y\sqrt{-3}), \pm(2y + (2y - (x+y))\zeta_3) = \pm(\frac{x+3y}{2} - \frac{x-y}{2}\sqrt{-3}), \pm(((x+y) - 2y) + (x+y)\zeta_3) = \pm(\frac{x-3y}{2} + \frac{x+y}{2}\sqrt{-3})$ である．ここで x, y は偶奇が異なるから，このうち $\pm(x + y\sqrt{-3})$ だけが $\mathbb{Z}[\zeta_3]$ に属する．

定理 (A) の証明： $p-1$ と 3 が互いに素なので， $\mathbb{F}_p \rightarrow \mathbb{F}_p, x \mapsto x^3$ は全単射である．

定義（ガウス和）： 素数 p と指標 $\chi: \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$ について $G_\chi = \sum_{t=1}^{p-1} \chi(t)\zeta_p^t$, where $\zeta_p = \exp(2\pi\sqrt{-1}/p)$ ．

注意： $a \notin p\mathbb{Z}$ について， $G_{\chi;a} = \sum_{t=1}^{p-1} \chi(t)\zeta_p^{at}$ とすると $G_{\chi;a} = \chi(a^{-1})G_\chi$ ．

命題： $\chi \neq 1$ であれば， $\sum_{t \in \mathbb{F}_p^\times} \chi(t) = 0$ ．

証明： $\mathbb{F}_p^\times$ の生成元 g を取る． $\chi(g) = v$ とすると， $\chi \neq 1 \Leftrightarrow v \neq 1$ ． $v \neq 1$ ならば $\sum_{t \in \mathbb{F}_p^\times} \chi(t) = \frac{1-v^{p-1}}{1-v}$ ．

命題： $\chi \neq 1$ であれば， $G_\chi G_{\bar{\chi}} = \chi(-1)p$ （特に $|G_\chi| = \sqrt{p}$ ．何故なら $\overline{G_\chi} = \chi(-1)G_{\bar{\chi}}$ ．なお $\chi^2 = 1$ であれば， $G_\chi^2 = \chi(-1)p$ も得られたことになる）．

証明： $\sum_{s,t \in \mathbb{F}_p^\times} \chi(s)\overline{\chi(t)}\zeta_p^{s+t} = \sum_{s,t} \chi(s/t)\zeta_p^{s+t}$ だが， $k = s/t$ と変数変換すると， $\sum_{k,t} \chi(k)\zeta_p^{(k+1)t}$ と等しい．

$\sum_k \chi(k) = 0$ なので (ここに $\chi \neq 1$ を用いた), $\sum_{k,t} \chi(k) \zeta_p^{(k+1)t} = (p-1)\chi(-1) + \sum_{k \neq -1} -\chi(k) = p\chi(-1)$.

定義 (ヤコビ和) : p を素数とする. 指標 $\chi_1, \chi_2 : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$ について $J(\chi_1, \chi_2) = \sum_{t=0}^{p-1} \chi_1(t)\chi_2(1-t)$, where $\chi_1(0) = \chi_2(0) = 0$.

注意 : ガウス和とヤコビ和は, ガンマ関数 $\Gamma(s) = \int_0^\infty e^{-x} x^{s-1} dy$ とベータ関数 $B(p, q) = \int_0^1 x^{p-1}(1-x)^{q-1} dx = \Gamma(p)\Gamma(q)/\Gamma(p+q)$ の類似という説がある.

命題 : $\chi_1\chi_2 \neq 1$ であれば, $J(\chi_1, \chi_2) = G_{\chi_1}G_{\chi_2}/G_{\chi_1\chi_2}$.

証明 : $G_{\chi_1}G_{\chi_2} = \sum_{s,t} \chi_1(s)\chi_2(t)\zeta_p^{s+t} = \sum_u (\sum_{s+t=u} \chi_1(s)\chi_2(t))\zeta_p^u$ で, 以下より $G_{\chi_1\chi_2}J(\chi_1, \chi_2)$ と等しい.

- $u = 0$ のとき, $\sum_{s+t=0} \chi_1(s)\chi_2(t) = (\sum_t \chi_1\chi_2(t))\chi_2(-1) = 0$.
- $u \neq 0$ のとき, $\sum_{s+t=1} \chi_1(us)\chi_2(ut) = \chi_1\chi_2(u)J(\chi_1, \chi_2)$.

系 : $\chi : \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times$ が cubic 指標 (定義: $\chi^3 = 1, \chi \neq 1 \neq \chi^2$. すぐに分かることだが, $p \equiv 1 \pmod{3}$ でしか存在しない) ならば $G_\chi^3 = pJ(\chi, \chi)$.

証明 : $G_\chi^2 = J(\chi, \chi)G_{\chi^2}$ で, $\chi^2 = \bar{\chi}$ より, $G_\chi^3 = J(\chi, \chi)\chi(-1)p$.

系 : χ が cubic 指標のとき, $J(\chi, \chi) = a + b\zeta_3 (= (a-b) + (-b)\zeta_3^2)$ とすると (ここで $a, b \in \mathbb{Z}$) ならば $a \equiv 2 \pmod{3}, b \equiv 0 \pmod{3}$.

証明 : 適当な $A \in \mathbb{Z}$ を用いて, $G_\chi^3 = \sum_t \chi(t)^3 \zeta_p^{3t} + 3A = -1 + 3A$ と書ける. これは $pJ(\chi, \chi) = p(a + b\zeta_3)$ と等しい. これから $p(a + b\zeta_3^2) = -1 + 3\bar{A}$ でもある. よって $pb\sqrt{-3} \in 3\mathbb{Z}$. すなわち $-3p^2b^2 \in 9\mathbb{Z}$. これから $b \in 3\mathbb{Z}$ が分かる (何故なら $z \in \mathbb{Z}$ を $p^2b^2 = -3z$ とすると, $z \in \mathbb{Q} \cap \mathbb{Z} = \mathbb{Z}$). よって $pa + 1 \in 3\mathbb{Z}$ で, 同様に $pa + 1 \in 3\mathbb{Z}$ である. 最後に $p \equiv 1 \pmod{3}$ に注意する.

定義 : $N : \mathbb{Q}(\zeta_3) \rightarrow \mathbb{Q}, x = a + b\zeta_3 \mapsto (a + b\zeta_3)(a + b\zeta_3^2) = a^2 - ab + b^2$ は積を保つ.

命題 : $\mathbb{Z}[\zeta_3]^\times = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$.

証明 : $x \in \mathbb{Z}[\zeta_3]$ について, $x \in \mathbb{Z}[\zeta_3]^\times \Leftrightarrow N(x) = \pm 1$ (注: 実際には $\forall x \in \mathbb{Q}(\zeta_3), N(x) \geq 0$ に注意).

命題 : $\mathbb{Z}[\zeta_3]$ の素元は (同伴を除いて) 以下の合併である.

1. 素数 $p \equiv 2 \pmod{3}$ は $\mathbb{Z}[\zeta_3]$ で素元.
2. 素数 $p \equiv 1 \pmod{3}$ は $p = \pi\bar{\pi}$ と $\mathbb{Z}[\zeta_3]$ の素元を用いて書ける. π と $\bar{\pi}$ は同伴ではない.

証明 : $(1-\zeta_3)^2 = -3\zeta_3$ より 3 は素元ではない. 単元でない x, y について $p = xy$ とすると, $N(x) = p = N(y)$. $x = a + b\zeta_3$ のとき, $N(x) = a^2 - ab + b^2 = p$ とすると, $(2a-b)^2 + 3b^2 = 4p$. よって $4p$ は $(\text{mod } 3)$ の平方剰余でなければならない, $p \equiv 1 \pmod{3}$ でなければならない. 逆に $p \equiv 1 \pmod{3}$ なら $p = a^2 + 3b^2$ と書けるが, これから $p = (a+b)^2 - (a+b)(a-b) + (a-b)^2$ である (注: $|J(\chi, \chi)| = \sqrt{p}$ を用いてもよい).

π と $\bar{\pi}$ が同伴でないこと: $z^2 + 3 = pk$ と $z, k \in \mathbb{Z}$ が取れる. π は $z + \sqrt{-3}$ を $\mathbb{Z}[\zeta_3]$ で割るとしてよい. よって $\bar{\pi}$ は $\bar{z}$ を割る. 同伴性を仮定すると π は $2\sqrt{-3}$ を割る. よって $N(\pi) = p$ は 12 の約数となる.

命題 : $\gamma = a + b\zeta_3$ が $\mathbb{Z}[\zeta_3]$ の素元で, $N(\gamma) \equiv 1 \pmod{3}$ ならば, $\gamma' = a' + b'\zeta_3$ で $a \equiv 2 \pmod{3}, b \equiv 0 \pmod{3}$ となる同伴元がただ 1 つ存在する (これを primary な素元と呼ぶ).

証明 : γ の同伴元 $\pm\zeta_3^k\gamma$ は $\pm(a + b\zeta_3), \pm(b + (b-a)\zeta_3), \pm((a-b) + a\zeta_3)$ である. $\text{mod } 3$ で (a, b) は $a+b \neq 0$

(mod 3) であることから、主張が確認できる。

3 次剰余の定義： $p \equiv 1 \pmod{3}$ を素数とする。このとき $\mathbb{F}_p$ には 1 の原始 3 乗根が存在するが、1 つ固定し ω と書く。 $\varphi: \mathbb{Z}[\zeta_3] \rightarrow \mathbb{F}_p, \zeta_3 \mapsto \omega$ を modulo p 還元写像とする。 $a \in \mathbb{F}_p^\times$ について $a^{(p-1)/3} = \omega^k$ の形をしている。対応 $\chi: \mathbb{F}_p^\times \rightarrow \mathbb{C}^\times, a \mapsto \zeta_3^k$ は cubic 指標を定める。この定義では $\chi(a)$ の値は ω の取り方に依るが、 $\chi(a) = 1$ かどうかはそうではなく、また $\chi(a) = 1 \Leftrightarrow \exists z \in \mathbb{F}_p^\times, z^3 = a$ 。

例： $p = 7 = (3 + \zeta_3)(2 - \zeta_3)$ のとき、 $\omega = 4$ と取れる。 $\chi(1) = \zeta_3^0 = \chi(6), \chi(2) = \zeta_3 = \chi(5), \chi(3) = \zeta_3^2 = \chi(4)$ である。よってガウス和は $G = \zeta_3^0 \zeta_7 + \zeta_3 \zeta_7^2 + \zeta_3^2 \zeta_7^3 + \zeta_3^2 \zeta_7^4 + \zeta_3 \zeta_7^5 + \zeta_3^0 \zeta_7^6$ で与えられる。ちなみにこれを計算すると $(7 + 21\sqrt{-3})/2$ となる（注： $3 + \zeta_3$ と同伴な素元 $\omega := 2 + 3\zeta_3$ は primary である）。

命題： $p = \pi\bar{\pi}$ が $\varphi(\pi) = 0$ のとき、 φ は環同型 $\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3] \xrightarrow{\sim} \mathbb{F}_p$ を誘導する。また $\varphi(\bar{\pi}) \neq 0$ である。

証明： $\pi = a + b\zeta_3$ が $p = a^2 - ab + b^2$ である。 $b \notin p\mathbb{Z}$ なので、 $\mu = m + n\zeta_3$ について、 $bc \equiv n \pmod{p}$ となる $c \in \mathbb{Z}$ を取ると、 $\mu - c\pi \equiv m - ac \pmod{\pi}$ 。よって $\#(\mathbb{Z}[\zeta_3]/\pi\mathbb{Z}[\zeta_3]) \leq p$ 。 $\bar{\pi}$ は π と同伴でないから $\varphi(\bar{\pi}) \neq 0$ である。

補題： p を素数とする。 k が $p-1$ の倍数でなければ $1^k + 2^k + \cdots + (p-1)^k \in p\mathbb{Z}$

証明： $\mathbb{F}_p$ の生成元を取ればよい。

命題： $p = \pi\bar{\pi}$ が $\varphi(\pi) = 0$ で π が primary ならば、 $G^3 = p\pi$ 。

証明： $J(\chi, \chi)$ は $\pi, \bar{\pi}$ のどちらか一方とのみ同伴である。 $\varphi(J(\chi, \chi)) = \sum_{a=1}^{p-1} a^{(p-1)/3} (1-a)^{(p-1)/3} = 0$ 。

系： 1 の原始 $3p$ 乗根 $\theta \in L \supseteq \mathbb{F}_2$ と、modulo 2 還元写像 $Y: \mathbb{Z}[\zeta_{3p}] \rightarrow L$ を取る。 $Y(\pi) = Y(\chi(2))$ 。

証明： $Y(G)Y(p)Y(\pi) = Y(G^4) = \sum_{t=1}^{p-1} Y(\chi(t))^{4t} Y(\zeta_p)^{4t} = Y(\chi(2))Y(G)$ だが、 $Y(G) \neq 0$ in L 。

命題： $a, b \in \mathbb{Z}$ が $a^2 - ab + b^2 = p$ かつ $a \equiv 5, b \equiv 0 \pmod{6}$ ならば、 $\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2$ 。

証明： $p = (\frac{2a-b}{2})^2 + 27(\frac{b}{6})^2$ である。

命題： $\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2$ ならば、 $\exists a \in \mathbb{Z}, \exists b \in \mathbb{Z}, a^2 - ab + b^2 = p, a \equiv 5, b \equiv 0 \pmod{6}$ 。

証明： $a = \pm(x + 3y), b = \mp(6y)$ と取れる。 $a^2 \equiv p \pmod{6}$ よりどちらかは $a \equiv 1 \pmod{6}$ である。

定理 (B) の証明： $p \equiv 1 \pmod{3}$ より、 $\mathbb{F}_p$ に 1 の原始 3 乗根が存在しているので、 $\chi(2) = 1$ のとき、(P) が成立している。このとき $\pi = a + b\zeta_3$ は $Y(\pi) = Y(\chi(2)) = 1$ だから、命題が適用できて $\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2$ 。よって (B-b) (の対偶) が示された。(B-a) を示す。 $\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2$ なら、命題の a, b を用いて得られる $\pi' = a + b\zeta_3$ について (これは primary である)、 $p = \pi'\bar{\pi}'$ である。 $Y(\pi') = 1 = Y(\bar{\pi}')$ なので、 $Y(\chi(2)) = 1$ であり $\chi(2) = 1$ 。

定理： 素数 $p \geq 5$ について、以下は同値である。

(P) $\#\{z \in \mathbb{F}_p \mid z^3 = 2\} = 3$ 。

(Q) $\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2$ (注：このとき $p \equiv 1 \pmod{3}$ でもある)。

(R) $a_p = 2$, where $\sum_{\ell \geq 0} a_\ell q^\ell = q(q^6; q^6)_\infty (q^{18}; q^{18})_\infty$ 。

(R) と同値性の証明： $1 + a_p = \#\{z \in \mathbb{F}_p \mid z^3 = 2\}$ を言えばよく、そのためには以下を示せばよい。

1. $p \equiv 2 \pmod{3}$ ならば $a_p = 0$.

2. $p \equiv 1 \pmod{3}$ で $\exists x \in \mathbb{Z}, \exists y \in \mathbb{Z}, p = x^2 + 27y^2$ ならば $a_p = 2$. そうでなければ $a_p = -1$.

証明: $(q; q)_\infty = \sum_{\ell \in \mathbb{Z}} (-1)^\ell q^{\ell(3\ell+1)/2}$ (Euler 五角数定理) より,

$$a = \sum_{m,n \in \mathbb{Z}} (-1)^{m+n} q^{1 + \frac{6m(3m+1)}{2} + \frac{18n(3n+1)}{2}} = \sum_{m,n \in \mathbb{Z}} (-1)^{m+n} q^{\frac{(6m+1)^2}{4} + \frac{3(6n+1)^2}{4}}.$$

より $T_p = \{(m, n) \in \mathbb{Z}^2 \mid (6m+1)^2 + 3(6n+1)^2 = 4p\}$ を求めればよい.

以下の対応 $((m, n) \mapsto (6m+1, 6n+1))$ および $(s, t) \mapsto (\frac{s+3t}{4}, \frac{-s+t}{4})$ で, 最初の単射は全単射である.

$$\begin{aligned} & \{(m, n) \in \mathbb{Z}^2 \mid m+n \in 2\mathbb{Z}, 4p = (6m+1)^2 + 3(6n+1)^2\} \\ & \hookrightarrow \{(s, t) \in \mathbb{Z}^2 \mid s \equiv t \equiv 1 \pmod{3}, s \equiv t \pmod{4}, 4p = s^2 + 3t^2\} \\ & \hookrightarrow \{(x, y) \in \mathbb{Z}^2 \mid p = x^2 + 3y^2\} \end{aligned}$$

また下段の (x, y) が像の元である必要十分条件は $x \equiv 1, y \equiv 0 \pmod{3}$ で, このとき $(s, t) = (x-3y, x+y)$.

同様に以下の対応 $((m, n) \mapsto (6m+1, 6n+1))$ および $(s, t) \mapsto (\frac{s-3t}{4}, \frac{s+t}{4})$ で, 最初の単射は全単射である.

$$\begin{aligned} & \{(m, n) \in \mathbb{Z}^2 \mid m+n \notin 2\mathbb{Z}, 4p = (6m+1)^2 + 3(6n+1)^2\} \\ & \hookrightarrow \{(s, t) \in \mathbb{Z}^2 \mid s \equiv t \equiv 1 \pmod{3}, s \equiv -t \pmod{4}, 4p = s^2 + 3t^2\} \\ & \hookrightarrow \{(x, y) \in \mathbb{Z}^2 \mid p = x^2 + 3y^2\} \end{aligned}$$

また下段の (x, y) が像の元である必要十分条件は $x \equiv 1, y \equiv 2 \pmod{3}$ で, このとき $(s, t) = (x+3y, -x+y)$.

以上から $p \equiv 2 \pmod{3}$ ならば $a_p = 0$ である. $p = X^2 + 27Y^2$ と書けるとき, $\{(x, y) \in \mathbb{Z}^2 \mid p = x^2 + 3y^2\} = \{(\pm X, \pm 3Y)\}$ (4点集合) なので, このうち丁度2つが $x \equiv 1 \pmod{3}$ を満たす. よって $a_p = 2$ である. 書けないとき $p = u^2 + 3v^2$ とすると $v \notin 3\mathbb{Z}$ であり, $\{(x, y) \in \mathbb{Z}^2 \mid p = x^2 + 3y^2\} = \{(\pm u, \pm v)\}$ (4点集合) なので, このうち丁度1つが $x \equiv 1, y \equiv 2 \pmod{3}$ を満たす. よって $a_p = -1$ である.