x^2+xy+y^2　（x, y は自然数）で表される素数ついて

2022 年 10 月
片山　喜美

はじめに

課題研究の中で、生徒が次の事実を予想した。

> x^2+xy+y^2 の x, y に自然数を代入して現れる数の中で素数となるものは、$3, 7, 13, 19, \quad \cdots$ であり、3 を除いてすべて $6n+1$ 型のものである。逆に、$6n+1$ 型の素数はすべて x^2+xy+y^2 で表すことができる。

興味深いことに気づいたものだと感心した。そこで、少し考えてみることにした。

関連したことでは、「x^2+y^2 で表される数の中で素数となるものは、2 を除いてすべて $4n+1$ 型のものである。また、$4n+1$ 型の素数はすべて x^2+y^2 で表すことができる」という事実がよく知られている。この場合は以下のような手順で示すのであった。（詳しくは、参考文献 [1] を参照）

- 虚数単位を i として、Gauss 整数 $\mathbb{Z}[i]=\{x+yi \mid x, y \in \mathbb{Z}\}$ を用いて考える。
- p を素数とするとき、$1, 2, \quad \cdots \quad , p-1$ の $p-1$ 個の数の中に、$a, a^2, \quad \cdots \quad , a^{p-1}$ が $mod\ p$ ですべて異なるような数 a がある。それを「p を法とする原始根」という。このとき、$a, a^2, \quad \cdots \quad , a^{p-1}$ は、$mod\ p$ で $1, 2, \quad \cdots \quad , p-1$ を並び変えたものになる。また、 $a^{p-1} \equiv 1 \pmod{p}$ となる。

  例えば、$p=13$ のときは、

  $2,\ 2^2=4,\ 2^3=8,\ 2^4 \equiv 3,\ 2^5 \equiv 6,\ 2^6 \equiv 12,\ 2^7 \equiv 11,\ 2^8 \equiv 9,\ 2^9 \equiv 5,\ 2^{10} \equiv 10$

  $2^{11} \equiv 7,\ 2^{12} \equiv 1$
- $p=4n+1$ のとき、$b=a^n$ とする。$b^2=a^{2n}$ は $\bmod p$ で 1 ではなく、 $(b^2)^2=a^{4n}=a^{p-1} \equiv 1$ であるから、$b^2 \equiv -1$ である。

  $p=13$ のときは、$b=2^3 \equiv 8$ として、$8^2 \equiv -1 \pmod{13}$ である。
- Gauss 整数の中で、$(b-i)(b+i)=b^2+1 \equiv 0$ となる。この b について、Gauss 整数における最大公約数 $gcd(b-i,\ p)=r=x+yi$ を考えると、そのノルム $N(r)=x^2+y^2$ が p となる。

x^2+xy+y^2 の場合には、少し異なった複素整数で考える。このとき、素数 $p=6n+1$ について、$p-1=6n$ であることに着目する。

- i の代わりに 1 の 6 乗根の 1 つ $\omega_6=\dfrac{1+\sqrt{3}i}{2}$ を使う。Gauss 整数の代わりになるのは $\mathbb{Z}[\omega_6]=\{x+y\,\omega_6 \mid x, y \in \mathbb{Z}\}$ である。

- ノルムは $N(x+y\,\omega_6)=|x+y\,\omega_6|^2=\left|x+y\cdot\dfrac{1+\sqrt{3}i}{2}\right|^2=\left(x+\dfrac{1}{2}y\right)^2+\left(\dfrac{\sqrt{3}}{2}y\right)^2$
  $=x^2+xy+y^2$ とする。

- p を法とする原始根、すなわち、$1\leqq a\leqq p-1$ で $a,\,a^2,\quad\cdots\quad,a^{p-1}$ が p を法としてすべて異なるものが存在する。このとき、 $a^{p-1}\equiv 1\pmod p$ となる。

  $p=6n+1$ であるから、 $b=a^n$ とすると、 $b^6=a^{6n}=a^{p-1}\equiv 1$ が成り立ち、$b^3\equiv -1$ となる。さらに、$b^3+1=(b+1)(b-\omega_6)(b-\overline{\omega_6})\equiv 0$ で、 $b+1\not\equiv 0$ であるから、 $(b-\omega_6)(b-\overline{\omega_6})\equiv 0$

  例として $p=13$ の場合は、先に述べたように 2 が原始根である。

  そこで、$b=2^2=4$ とすると、 $4^3\equiv -1\pmod{13}$ となる。

- $gcd(b-\omega_6,\,p)=r$ を考えて、 $N(r)=N(x+y\,\omega_6)=x^2+xy+y^2=p$ となることが示される。ただし、$x,\,y$ として正の整数をとれるかどうかに注意が必要である。

  例えば $p=13$ の場合は、 $b=4$ であるから $gcd(4-\omega_6,\,13)$ を考える。
  $\dfrac{13}{4-\omega_6}=\dfrac{13(4-\overline{\omega_6})}{(4-\omega_6)(4-\overline{\omega_6})}=\dfrac{13\{4-(1-\omega_6)\}}{4^2-4+1}=3+\omega_6$ となるので、$13=(4-\omega_6)(3+\omega_6)$ とわかる。このことから、13 は $4-\omega_6$ の複素整数倍であり、

  $gcd(4-\omega_6,\,13)=4-\omega_6$ となる。

  $x=4,\,y=-1$ とすると、 $x^2+xy+y^2=13$ を満たす。ただし、 $y<0$ となる。

  これについては、$4-\omega_6$ と同伴な数 $\omega_6(4-\omega_6)=4\omega_6-\omega_6^2=4\omega_6-(\omega_6-1)=1+3\omega_6$ を感が手、 $x=1,\,y=3$ が $x^2+xy+y^2=13$ を満たす。一般の素数 $p=6n+1$ についても、同伴数の中に $x,\,y>0$ を満たすものを見つけることができる。

上記に従って、x^2+xy+y^2 で表される素数について、以下にまとめてみる。なお、参考文献 [1] で $x^2+y^2=p$ を扱った時と重なっている部分が多いが、そのまま記載しておいた。

目 次

1　複素整数　$\mathbb{Z}[\omega_6] = \{x + y\,\omega_6 \,|\, x,\, y \in \mathbb{Z}\}$ について

1.1　関連事項の定義

1の6乗根を考える。$x^6 = 1$ とすると、$x^6 - 1 = (x^3 - 1)(x^3 + 1) = 0$ である。$x^3 - 1 = 0$ の解は1の3乗根であるから。 $x^3 + 1 = 0$ を考える。$(x+1)(x^2 - x + 1) = 0$。虚数解は $x = \dfrac{1 \pm \sqrt{3}i}{2}$。 $\omega_6 = \dfrac{1 + \sqrt{3}i}{2}$ とおくと、 ω_6 は6乗して初めて1となる虚数であることがわかる。

定義 1.1　（1 の 6 乗根に関わる複素整数）

$x,\, y \in \mathbb{Z}$ とするとき、 $a = x + y\,\omega_6$ と表される複素整数を考える。それらの集合を $\mathbb{Z}[\omega_6] = \{x + y\,\omega_6 \,|\, x,\, y \in \mathbb{Z}\}$ と表す。

定義 1.2　（ノルム）

複素数 $a = x + y\,\omega_6 \quad (a,\, b \in \mathbb{R})$ に対して $N(a) = x^2 + xy + y^2$ を a のノルムという。

$a = x + \dfrac{1 + y\sqrt{3}i}{2} = \left(x + \dfrac{1}{2}y\right) + \dfrac{\sqrt{3}}{2}y\,i$ なので、通常の絶対値は

$|a| = \sqrt{\left(x + \dfrac{1}{2}y\right)^2 + \left(\dfrac{\sqrt{3}}{2}y\right)^2} = \sqrt{x^2 + xy + y^2}$ となるので、

$N(a) = |a|^2 = x^2 + xy + y^2$ と定義するのである。

補題 1.3　$N(ab) = N(a)N(b)$ が成り立つ。

証明）複素数の絶対値で $|ab| = |a| \cdot |b|$ が成り立つので、 $|ab|^2 = |a|^2 \cdot |b|^2$ となる。従って、 $N(ab) = N(a)N(b)$ が成り立つ。　　(証明終)

定義 1.4　（単数）

$N(a) = 1$ を満たす複素整数 a を「単数（$unit$)」 と言う。

複素整数 $x + y\,\omega_6$ が単数であるとする。

$x^2 + xy + y^2 = 1$ であるから、 $\left(x + \dfrac{1}{2}y\right)^2 + \dfrac{3}{4}y^2 = 1$

$(2x + y)^2 + 3y^2 = 4$　　よって、 $3y^2 \leqq 4$ となるので、 $y = 0,\, \pm 1$

$(x,\, y) = \pm(1, 0),\, \pm(0, 1),\, \pm(1, -1)$ 。

従って、**複素整数 $\mathbb{Z}[\omega_6]$ の単数は $\pm 1,\, \pm\omega_6,\, \pm(1 - \omega_6)$ の 6 つである。**

注意

$1 - \omega_6 = \dfrac{1 - \sqrt{3}i}{2} = \overline{\omega_6}$ であるから、単数は $\pm 1,\, \pm\omega_6,\, \pm\overline{\omega_6}$ である。

定義 1.5　（同伴数）

複素整数 $a,\, b$ が $a = \epsilon b$　(ϵ は単数) となるとき、 a と b は同伴数であるという。

定義 1.6　$a,\, b \in \mathbb{Z}[\omega_6]$ を複素整数とする。$c \in \mathbb{Z}[\omega_6]$ が存在して、 $a = bc$ となるとき、 a は b の倍数であるという。また、 b は a の約数であるという。

このとき、 $b|a$ と表す。

$a,\, b$ どちらともの倍数となっている複素整数を $a,\, b$ の公倍数という。

$a,\, b$ どちらともの約数となっている複素整数を $a,\, b$ の公約数という。

$a = bc$ のとき、単数 ϵ に対して、$\epsilon\overline{\epsilon} = 1$ であるから、$a = (\epsilon b)\cdot(\overline{\epsilon}c)$ が成り立つので、 b の同伴数 ϵb も a の約数である。従って、約数を考えるときは、同伴数全体を同一視して、代表として 1 つの数を取り上げるといった扱いをすることもある。例えば、$(1+2\omega_6)(1+2\overline{\omega_6}) = 1^2+1\cdot 2+2^2 = 7$ なので、$1+2\omega_6$ は 7 の約数であるが、その同伴数を考えると、$\pm(1+2\omega_6)$, $\pm\omega_6(1+2\omega_6)$, $\pm\overline{\omega_6}(1+2\omega_6)$ が約数である。それらを代表して、「$1+2\omega_6$ が約数である」ということもある。

ここで、ω_6, $\overline{\omega_6}$ は 2 次方程式 $x^2-x+1=0$ の 2 つの解であるから、

$\omega_6+\overline{\omega_6} = 1$, $\omega_6\cdot\overline{\omega_6} = 1$ である。また、$\omega_6^2 = \omega_6 - 1 = -\overline{\omega_6}$ が成り立つ。

$\omega_6(1+2\omega_6) = \omega_6+2\omega_6^2 = \omega_6+2(\omega_6-1) = -2+3\omega_6$

$\overline{\omega_6}(1+2\omega_6) = \overline{\omega_6}+2\overline{\omega_6}\omega_6 = 1-\omega_6+2 = 3-\omega_6$

従って、「$1+2\omega_6$ が 7 の約数である」が意味することは、

「 $\pm(1+2\omega_6)$, $\pm(-2+3\omega_6)$, $\pm(3-\omega_6)$」が 7 の約数である」ということである。

$1+2\overline{\omega_6} = 1+2(1-\omega_6) = 2-\omega_6$ であり、これは上記の 6 つの複素整数に含まれない。すなわち、$1+2\omega_6$ と $1+2\overline{\omega_6}$ は同伴ではない。従って、7 は異なる 2 つの因数（同伴数にならない 2 つの因数）を持つといえる。

それに比べて、$3 = (1+\omega_6)(1+\overline{\omega_6})$ については、$\omega_6(1+\overline{\omega_6}) = \omega_6+\omega_6\overline{\omega_6} = \omega_6+1$ であるから、$1+\omega_6$ と $1+\overline{\omega_6}$ は同伴数である。従って、 3 は平方数（と同伴な数）であるといえる。

1.2 ユークリッドのアルゴリズム

整数 $\mathbb{Z}$ で公約数を求めるときには、ユークリッドの互除法が有効な手段であった。ユークリッドの互除法は Gauss 整数 $\mathbb{Z}[i]$ でも使用することができたのであった。そして、複素整数 $\mathbb{Z}[\omega_6]$ にも適用できるのである。

定理 1.7 $a, b \in \mathbb{Z}[\omega_6]$ $b \neq 0$ のとき、 $q, r \in \mathbb{Z}[\omega_6]$ で $a = bq+r$ $0 \leqq N(r) < N(b)$ を満たすものがある。

証明）$a = x+y\,\omega_6$, $b = z+w\,\omega_6$ $(x,\, y,\, z,\, w \in \mathbb{Z})$ とする。

$$\frac{a}{b} = \frac{x+y\,\omega_6}{z+w\,\omega_6} = \frac{(x+y\,\omega_6)(z+w\,\overline{\omega_6})}{z^2+zw+w^2} = \frac{xz+xw\overline{\omega_6}+yz\omega_6+yw\omega_6\overline{\omega_6}}{z^2+zw+w^2}$$

$$= \frac{xz+xw(1-\omega_6)+yz\omega_6+yw\cdot 1}{z^2+zw+w^2} = \frac{(xz+xw+yw)+(-xw+yz)\omega_6}{z^2+zw+w^2}$$

ここで、$\left|\dfrac{xz+xw+yw}{z^2+zw+w^2}-u\right| \leqq \dfrac{1}{2}$, $\left|\dfrac{-xw+yz}{z^2+zw+w^2}-v\right| \leqq \dfrac{1}{2}$ を満たす整数 u, v が存在する。

ただし、 $u, v \in \mathbb{Z}$ の取り方は一意的とは限らない。

$q = u+v\,\omega_6$ とすると、

$$N\left(\frac{a}{b}-q\right) = N\left(\left(\frac{xz+xw+yw}{z^2+zw+w^2}-u\right)+\left(\frac{-xw+yz}{z^2+zw+w^2}-v\right)\omega_6\right)$$

$$\leqq \left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2 < 1$$

補題 1.3 より、 $N(a-bq) = N\left(\frac{a}{b} - q\right) N(b) < 1 \cdot N(b)$
$r = a - bq$ とおくと、 $a = bq + r \quad 0 \leqq N(r) < N(b)$ （証明終）

複素整数 $\mathbb{Z}[\omega_6]$ におけるユークリッドのアルゴリズムを以下のとおり定める。
$a, b \in \mathbb{Z}[\omega_6] \quad b \neq 0$ のとき、

- $r_0 = a$, $r_1 = b$ と定める。
- $k \in \mathbb{N}$ について、 $r_k \neq 0$ ならば、定理 1.7 により、
  $r_{k-1} = r_k q_k + r_{k+1} \quad 0 \leqq N(r_{k+1}) < N(r_k)$ を満たす複素整数 q_k, r_{k+1} が存在する。
  これにより、新たな r_{k+1} を定める。
- $r_k = 0$ ならば、この作業を終了する。

命題 1.8 ある自然数 n があり、 $N(r_n) > 0$ かつ $N(r_{n+1}) = 0$ となる。すなわち、ユークリッドのアルゴリズムは、必ずストップする。

証明） $N(r_1) > N(r_2) > \quad \cdots$ は、減少する非負整数の列であるから、$N(r_n) > 0$ かつ $r_{n+1} = 0$ となる自然数 n が必ずある。 （証明終）

補題 1.9 a, b の公倍数でノルムが最小のものの 1 つを l とする。このとき、 a, b の任意の公倍数 m は、 l の倍数である。

証明）$m = lq + r \quad (0 \leqq N(r) < N(l)$ を満たす $q, r \in \mathbb{Z}[\omega_6]$ が存在する。
$r = m - lq$ であり、 m, l がともに a, b の公倍数であるから、 r も a, b の公倍数である。
このとき、 $0 < N(r) < N(b)$ であるとすると、l が最小公倍数であることに反する。従って、 $N(r) = 0$ であり、 $m = lq$ となる。すなわち、 m は l の倍数である。（証明終）

補題 1.10 l_1, l_2 がいずれも a, b の公倍数で、ノルムが最小のものであるとする。このとき、 $l_2 = \epsilon l_1 \quad (\epsilon$ は単数$)$ となる。

証明）補題 1.9 より、$l_2 = l_1 c, \quad c \in \mathbb{Z}[\omega_6]$ とできる。
l_1, l_2 のノルムの最小性より、 $N(l_1) = N(l_2)$ である。従って、 $N(c) = 1$ 。すなわち、c は単数である。$c = \epsilon$ と書き換えて、$l_2 = \epsilon l_1 \quad (\epsilon$ は単数$)$ となる。 （証明終）

この補題により、a, b の公倍数でノルムが最小のものの 1 つを l とすると、

- $\epsilon l \quad (\epsilon$ は単数 $)$ はすべて a, b の公倍数でノルムが最小のものである。
- a, b の公倍数でノルムが最小であるものは、$\epsilon l \quad (\epsilon$ は単数 $)$ のいずれかである。

以上を踏まえて、以下のように定義する。

定義 1.11 （最小公倍数）
$a, b \in \mathbb{Z}[\omega_6]\quad a, b \neq 0$ について、l が a, b の公倍数でノルムが最小のものであるとき、「l は a, b の最小公倍数である」といい、 $l = lcm(a, b)$ で表す。ただし、このとき ϵ を単数とするとき、 ϵl も a, b の最小公倍数であり、 $\epsilon l = lcm(a, b)$ となる。
逆の書き方にすると、 $lcm(a, b)$ はϵl （ϵ は単数) のどれかであり、どれにしてもよいこととする。

補題 1.12 g を a, b の公約数でノルムが最大のものの 1 つとする。このとき、a, b の任意の公約数 d は g の約数である。

証明） $l = lcm(g, d)$ とする。l は g の倍数であるから $N(l) \geqq N(g)$
a は g, d の公倍数であるから、補題 1.9 より a は l の倍数である。同様に、 b も l の倍数である。従って、l は a, b の公約数である。g は a, b の公約数の中でノルムが最も大きいものであると仮定しているので、 $N(l) \leqq N(g)$
以上より、 $N(l) = N(g)$ となり、 $\epsilon l = g$ （ϵ は単数) となる。
$l = lcm(g, d)$ なので、 l は d の倍数である。したがって、 $g = \epsilon l$ より g も d の倍数となる。 （証明終）

補題 1.13 g_1, g_2 を a, b の公約数でノルムが最大のものとすると、$g_2 = \epsilon g_1$ （ϵ は単数) となる。

証明）補題 1.13 より、$g_2 = \epsilon g_1$ （$\epsilon \in \mathbb{Z}[\omega_6]$) とできる。$g_1, g_2$ のノルムの最大性より、$N(g_1) = N(g_2)$ である。従って、 $N(\epsilon) = 1$ となる。よって、 ϵ は単数である。

定義 1.14 $a, b \in \mathbb{Z}[\omega_6]\quad a, b \neq 0$ について、g が a, b の公約数でノルムが最大のものであるとき、 g を「a, b の最大公約数」といい、 $g = gcd(a, b)$ と表す。このとき、a, b の最大公約数となるのは、 ϵg （ϵ は単数) である。逆に書くと、$gcd(a, b) = \epsilon g$ （ϵ は単数) となる。

命題 1.15 $\mathbb{Z}[\omega_6]$ の 2 つの複素整数 $a, b \neq 0$ からユークリッドのアルゴリズムで数列

$$r_0, r_1, r_2, \quad \cdots \quad r_n, r_{n+1} \qquad (N(r_n) > 0, r_{n+1} = 0)$$

が得られたとする。このとき、 次が成り立つ。

- $gcd(r_{k-1}, r_k) = gcd(r_k, r_{k+1})$ である。
- ユークリッドのアルゴリズムによって得られた数列の最後が $N(r_n) > 0, r_{n+1} = 0$ であるとき、 $gcd(a, b) = r_n$ である。

証明） $g_k = gcd(r_{k-1}, r_k), \quad g_{k+1} = gcd(r_k, r_{k+1})$ とする。

- $r_{k+1} = r_{k-1} - r_k q_k$ で、$g_k \,|\, r_{k-1}$ かつ 、$g_k \,|\, r_k$ であるから、 $g_k \,|\, r_{k+1}$ 。従って、 g_k は r_k, r_{k+1} の公約数である。これにより、 $N(g_k) \leqq N(gcd(r_k, r_{k+1})) = N(g_{k+1})$
  $r_{k-1} = r_k q_k + r_{k+1}$ で、$g_{k+1} \,|\, r_k$ かつ 、$g_{k+1} \,|\, r_{k+1}$ であるから、 $g_{k+1} \,|\, r_{k-1}$ 。従って、g_{k+1} は r_{k-1}, r_k の公約数である。これにより、$N(g_{k+1}) \leqq N(gcd(r_{k-1}, r_k)) = N(g_k)$
  以上により、 $N(g_k) = N(g_{k+1})$ である。従って、（単数の積を除いて） $g_k = g_{k+1}$ が成り立つ。 (証明終)

- 上で示したことより、 $gcd(a,\, b) = g_1 = g_2 = \quad \cdots \quad = g_{n+1} = gcd(r_n,\, 0) = r_n$ となる。 (証明終)

定理 1.16 $a,\, b \in \mathbb{Z}[\omega_6] \quad a,\, b \neq 0, \quad g = gcd(a,\, b)$ のとき、$a\mu + b\nu = g$ を満たす $\mu,\, \nu \in \mathbb{Z}[\omega_6]$ が存在する。

証明) ユークリッドのアルゴリズムで $r_0 = a,\, r_1 = b,\, r_2, \quad \cdots \quad r_n = g,\, r_{n+1} = 0$ が得られたとする。このとき、$r_{n-2} = r_{n-1}q_{n-1} + r_n$ である。$r_n = g$ であり、$r_{n-2} - r_{n-1}q_{n-1} = g$ となる。 $\mu_{n-2} = 1,\, \nu_{n-1} = -q_{n-1}$ とおくと、

$$r_{n-2}\mu_{n-2} + r_{n-1}\nu_{n-1} = g \quad (\mu_{n-2},\, \nu_{n-1} \in \mathbb{Z}[\omega_6])$$

もし、ある $k \in \mathbb{N}$ について、

$$r_{k-1}\mu_{k-1} + r_k\nu_k = g \quad (\mu_{k-1},\, \nu_k \in \mathbb{Z}[\omega_6])$$

が成り立つとすると、$r_k = r_{k-2} - r_{k-1}q_{k-1}$ であるから

$$r_{k-1}\mu_{k-1} + (r_{k-2} - r_{k-1}q_{k-1})\nu_k = g, \quad r_{k-2}\nu_k + r_{k-1}(\mu_{k-1} - q_{k-1}\nu_k) = g$$

ここで、$\mu_{k-2} = \nu_k, \quad \nu_{k-1} = \mu_{k-1} - q_{k-1}\nu_k$ とおくと

$$r_{k-2}\mu_{k-2} + r_{k-1}\nu_{k-1} = g \quad (\mu_{k-2},\, \nu_{k-1} \in \mathbb{Z}[\omega_6])$$

とできる。

この操作を繰り返していくと、

$$r_0\mu_0 + r_1\nu_1 = g \quad (\mu_0,\, \nu_1 \in \mathbb{Z}[\omega_6])$$

$\mu_0 = \mu,\, \nu_1 = \nu$ とすると、$r_0 = a,\, r_1 = b$ であるから

$$a\mu + b\nu = g \quad (\mu,\, \nu \in \mathbb{Z}[\omega_6]))$$

とできる。 (証明終)

2 複素整数 $\mathbb{Z}[\omega_6]$ における素数について

定義 2.1 $a \in \mathbb{Z}[\omega_6]$ が複素整数における素数であるとは、

a の約数が単数もしくは、 a の同伴数、すなわち $\epsilon a \quad (\epsilon$ は単数) に限るときであるとする。

補題 2.2 $N(a) = p \quad (p$ は有理整数 $\mathbb{N}$ における整数)

$\Longrightarrow \qquad a$ は $\mathbb{Z}[\omega_6]$ における素数である。

証明) $a = bc \quad (b,\, c \in \mathbb{Z}[\omega_6])$ とする。 $N(a) = N(b)N(c)$ より、 $p = N(b)N(c)$ となる。

$N(b),\, N(c) \in \mathbb{N}, \quad p$ は素数であるから、 $N(b) = 1$ もしくは $N(b) = p$ のいずれかである。従って、 b は単数であるか、もしくは、 $\epsilon p \quad (\epsilon$ は単数) のいずれかである。 (証明終)

命題 2.3 $gcd(a,\,b)=1$ かつ $a\,|\,bc \quad \Longrightarrow a\,|\,c$

証明）定理 1.16 により、 $a\mu+b\nu=1$ を満たす $\mu,\,\nu\in\mathbb{Z}[\omega_6]$ が存在する。両辺に c を掛けて、$ac\mu+bc\nu=c$ 。ここで、 $a\,|\,bc$ より、この式の左辺は a の倍数である。 よって、 $a\,|\,c$ となる。 (証明終)

命題 2.4 $a\in\mathbb{Z}[\omega_6]$ が 0 でも単数でも無いとき、 $\mathbb{Z}[\omega_6]$ の素数で a を割り切るものが存在する。

証明） a が素数の時は、a 自身が a を割り切る素数となり、命題の主張は正しい。

a が素数で無いときは、 $a=a_1b_1 \quad (a_1,\,b_1\in\mathbb{Z}[\omega_6] \quad N(a_1),\,N(b_1)>1)$ と積の形で表すことができる。$N(a)=N(a_1)N(b_1)$ であるから、 $1<N(a_1)<N(a)$ が成り立つ。ここで、 a_1 が素数であれば命題の主張が成立する。a_1 が素数で無いときは、 $a_1=a_2b_2$ と積に表すことができ、 $a,\,a_1$ のところで述べたことと同じ状況が生じる。 素数で無いものが続く間は、 $N(a)>N(a_1)>N(a_2)>\quad\cdots\quad>1$ という数列を作っていくことになるが、これを無限に続けることは不可能である。よって、どこかで、 a_j が素数となる。従って、 a はその素数で割りきれることになり、命題が正しいと言える。 (証明終)

命題 2.5 $a\in\mathbb{Z}[\omega_6],\quad q\neq0$ とするとき、単数 ϵ および $\mathbb{Z}[\omega_6]$ の相異なる素数 $p_1,\,p_2,\quad\cdots\quad,p_k$ があって、 $a=\epsilon p_1^{n_1}p_2^{n_2}\cdot\quad\cdots\quad\cdot p_k^{n_k}\quad n_1,\,n_2,\quad\cdots\quad,n_k\geqq1$ と表すことができる。また、この表し方は、単数 ϵ の取り方、及び $p_1,\,p_2,\quad\cdots\quad,p_k$ をそれぞれ同伴な $\mathbb{Z}[\omega_6]$ の素数に取り替えることを除けば一意的である。

証明）a が単数の時は命題が正しいことは自明である。

a が単数で無いとき、先の命題より、 a はある素数で割りきれる。a が素数 p_1 で割り切れるものとし、 $p_1^{n_1}$ で割り切れるが、$p_1^{n_1+1}$ では割り切れないとすると、$a=p_1^{n_1}a_1 \quad (a_1\in\mathbb{Z}[\omega_6])$ とできる。このとき、a_1 が単数ならば、 $a=p_1^{n_1}\epsilon \quad \epsilon$は単数 とできるので、命題が正しいことが示される。もし、 a_1 が単数で無いならば、 a_1 に対して、a について考えたことと同じことを考える。この操作を繰り返すと、 $a=\epsilon p_1^{n_1}p_2^{n_2}\cdot\quad\cdots\quad\cdot p_k^{n_k}$ と表すことができる。

一意性について

$a=\epsilon`q_1^{m_1}q_2^{m_2}\quad\cdots\quad q_l^{m_l}\quad q_1,\,q_2,\quad\cdots\quad,q_l$ は相異なる素数、 $m_1,\,m_2,\quad\cdots\quad,m_l\geqq1$ とも表されたとする。$p_1\neq q_1$ と仮定すると、 $gcd(p_1,\,q_1^{m_1})=1 \quad p_1\,|\,q_1^{m_1}\cdot\epsilon`q_2^{m_2}\quad\cdots\quad q_l^{m_l}$ より、$p_1\,|\,\epsilon q_2^{m_2}\quad\cdots\quad q_l^{m_l}$ 。もし、$p_1\neq q_2$ ならば、同様な考察により、$p_1\,|\,\epsilon q_3^{m_3}\quad\cdots\quad q_l^{m_l}$ 。p_1 が $q_1,\quad\cdots\quad,q_l$ のいずれとも異なるとすると、考察を繰り返して、 $p_1\,|\,\epsilon'$ となる。これは不可能である。従って、 p_1 は $q_1,\quad\cdots\quad,q_l$ のいずれかと等しくなる。必要なら番号を付け替えて、 $p_1=q_1$ としてよい。また、割り算について考察して、指数について、 $n_1=m_1$ であることがわかる。

さらに、 $k=l \quad p_2=q_2,\quad\cdots\quad,p_k\;q_k,\quad n_2=m_2,\quad\cdots\quad,n_k=m_k$ がわかる。 （証明終）

3 素数 p を $x^2+xy+y^2=p \quad (x,\,y$ は自然数$)$ と表すことについて

$2^2+2\cdot1+1^2=7,\quad 1^2+1\cdot3+3^2=13,\quad 2^2+2\cdot3+3^2=19$ などについて考える。そのために、もう少し準備が必要である。

補題 3.1 p を奇素数、 k を p と互いに素な整数とする。このとき、 $kl \equiv 1 \pmod{p}$ を満たす整数 l が存在する。

証明）ユークリッドのアルゴリズムにより、$kl + pm = 1$ を満たす整数 l, m を求めることができる。このとき、 $kl \equiv 1 \pmod{p}$ が成り立つ。 （証明終）

3.1 $b^3 \equiv -1 \pmod{p}$ を満たす整数 b が存在するかどうかについて

結論から言うと、奇素数 p について、$p \equiv 1 \pmod{6}$ ならば、$b^3 \equiv -1 \pmod{p}$ を満たす整数 b が存在する。 $p \equiv 5 \pmod{6}$ ならば、$b^3 \equiv -1 \pmod{p}$ を満たす整数 b は存在しない。

定理 3.2 p を素数とする。このとき、 $1 \leqq a \leqq p-1$ で、$a, a^2, \quad \cdots \quad , a^{p-1}$ が p を法としてすべて異なるものがある。

この定理の証明は、このレポートでは省略する。整数関係の教科書で証明を調べることができる。なお、自分も学習したメモとして「$\mathbb{F}_p^{\times}$ が巡回群であることについて」というレポートを書いておいた。 （http://ja9nfo.web.fc2.com/math/20200716junkaigun.pdf 参照）

なお、上記のような a を「**p を法とする原始根**」と呼ぶ。

奇数は 6 を法として考えると、1 または 5 に等しい。次の定理が成り立つ。

定理 3.3 素数 p が $p \equiv 1 \pmod{6}$ を満たすとき、 $b^3 \equiv -1 \pmod{p}$ を満たす整数 $1 \leqq b \leqq p-1$ が存在する。

証明）$p = 6n+1$ とおく。定理 3.2 の原始根 a を考えると、$a^{p-1} = a^{6n} \equiv 1$ が成り立つ。 $(a^{3n})^2 = 1$ かつ a^{3n} は 1 に合同ではないから、 $a^{3n} \equiv -1$ である。$b = a^n$ とすると、$b^3 = a^{3n} \equiv -1$ となる。ここで、 b を法 p で合同なものにとりかえても同じ式がなりたつので、 $1 \leqq b \leqq p-1$ としてよい。 （証明終わり）

3.2 $p = 6n+1$ のタイプの素数の二次式による表現について

上の定理により、$p = 6n+1$ のとき、 $1 \leqq b \leqq p-1$ で $b^3 \equiv -1 \pmod{p}$ を満たすものが存在する。$b^3 + 1 \equiv 0 \pmod{p}$ となるので、 $(b+1)(b-\omega_6)(b-\overline{\omega_6}) \equiv 0 \pmod{p}$ である。$b+1 \not\equiv 0$ なので、 $(b-\omega_6)(b-\overline{\omega_6}) = cp \quad (c \in \mathbb{Z}[\omega_6])$ とおける。このとき、複素整数 $\mathbb{Z}[\omega_6]$ における $b-\omega_6$ と p の最大公約数を $r = gcd(b-\omega_6, p)$ とおく。$N(r)$ は $N(p) = p^2$ の約数であるから $N(r) = 1, p, p^2$ のいずれかである。

- $N(r) = 1$ のとき

  $(b-\omega_6)(b-\overline{\omega_6}) = cp$ (c は複素整数) なので、 $p \,|\, (b-\omega_6)(b-\overline{\omega_6})$ である。$N(r) = 1$ より $gcd(b-\omega_6, p) = 1$ であるから、命題 2.3 より、$p | b-\overline{\omega_6}$ が成り立たなければいけない。したがって、$b - \overline{\omega_6} = dp \quad (d \in \mathbb{Z}[\omega_6])$ とできる。このとき、 複素共役をとって、$b - \omega_6 = \overline{d}p$。これは、$r$ が p の倍数であることを意味するので、$N(r) = 1$ であることに矛盾する。

  よって、$N(r) = 1$ となることはありえない。

- $N(r) = p^2$ のとき

  ノルムを考えると p は r の単数倍であるから、逆に r は p の単数倍であるといえる。よって、 $b - \omega_6$ が p の単数倍とならなければいけないが、ω_6 の係数が 1 であることからありえない。

以上より、 $N(r) = p$ である。
残る問題は、自然数 x, y で $x^2 + xy + y^2 = p$ とできるかどうかである。$x, y \in \mathbb{N}$ とする。

- $r = x + y\,\omega_6$ や $r = -x - y\,\omega_6$ のときは、 $x^2 + xy + y^2 = p$ となる。

- $r = x - y\,\omega_6$ のとき

  r に単数をかけてもノルムの値は変わらないことを利用する。

  $\omega_6 r = x\omega_6 - y\omega_6^2 = x\omega_6 - y(\omega_6 - 1) = y + (x - y)\omega_6$

  $-\overline{\omega_6} r = -x\overline{\omega_6} + y\omega_6\overline{\omega_6} = -x(1 - \omega_6) + y \cdot 1 = (y - x) + x\omega_6$

  上記２つのうちいずれかは、２つの自然数を係数にする表現になるので、条件を満たす。

- $r = -x + y\,\omega_6$ のとき

  $-r = x - y\,\omega_6$ なので先の場合に帰着できる。

以上のことから自然数 x, y で $x^2 + xy + y^2 = p$ とできる。　　（証明終）

3.3　$p = 6n + 5$ のタイプの素数について

$x, y \in \mathbb{N}$ のとき、$x, y \equiv 0, 1, 2 \pmod 3$ である。
$x^2 + xy + y^2$ を 3 を法とした剰余類で考えてみる。表では、縦を x、横を y とする。

5

	0	1	2
0	0	1	1
1	1	0	1
2	1	1	0

表による計算により、$x^2 + xy + y^2 \equiv 0, 1 \pmod 3$ となる。しかるに、$p = 6n + 5$ のときは、 $p \equiv 2 \pmod 3$ であるから、 $x^2 + xy + y^2$ と合同となることはない。
なお、$x^2 + xy + y^2 = p \equiv 0 \pmod 3$ は $p = 3$ に対応している。

以上のことから、$6n + 1$ のタイプの素数　p については、必ず $x^2 + xy + y^2 = p$ を満たす自然数 x, y が存在し、また、 $6n + 5$ のタイプの素数については $x^2 + xy + y^2 = p$ を満たす自然数 x, y が存在しないことがわかった。

参考文献

[1] 片山　喜美「$x^2+y^2=p$　(p は素数) について」
（http://ja9nfo.web.fc2.com/math/202203FactorizationOfp.pdf 参照）

[2] 片山　喜美「$\mathbb{F}_p^{\times}$ が巡回群であることについて」
（http://ja9nfo.web.fc2.com/math/20200716junkaigun.pdf 参照）