$x^2+y^2=p$　（$x,\ y$ は整数、 p は素数）について

2022年6月
片山　喜美

はじめに

ある真実を証明することや、どうして成り立つのかを理解することが難しいときに、世界を広げるとうまくいくときがある。例えば、整数の問題を証明するときに、数の世界を複素数まで広げることが有効なことがある。その一つの例が $x^2+y^2=p$ と素数 p を2つの自然数の平方の和で表す問題である。自然数の範囲で考えていたのではなかなかうまくいかないのだが、 ガウス整数 $\mathbb{Z}[i]$ へ数の世界を広げることで解決の糸口がみつかる。なお、ガウス整数の世界でも、普通の整数と同様に、素数や素因数分解などを考えることができる。そして、普通の整数では扱うことができないこともある。そのことが、問題解決につながる。

自然数5は素数であり、5を割り切る自然数は、5自身と1の2つだけである。しかし、ガウス整数 $\mathbb{Z}[i]=\{x+iy\,|x,\,y\in\mathbb{Z}\}$ まで数の範囲を広げると、 $5=(2+i)(2-i)$ と2つの数の積に分解する。すなわち、5はガウス整数の世界では素数ではない。

では、3はどうであろうか。$3=(x+iy)(z+iw)$ とおいてみると、
$9=(x^2+y^2)(z^2+w^2)$。よって、$x^2+y^2=1,\,3,\,9$ のいずれかである。
$x^2+y^2=1$ のとき、$x+iy=\pm1,\,\pm i$ のいずれかである。 よって、$z+iw=\pm3,\,\mp3i$ のいずれかであり、ガウス整数で分解されたとは言い難い。$x^2+y^2=9$ のときも、 $z^2+w^2=1$ なので、同様の結果になる。残るのは、$x^2+y^2=3$ の場合であるが、そうなる整数 x,y は存在しない。従って、自然数3については、数の世界をガウス整数まで広げても新たな分解を得ることができない。すなわち、3はガウス整数の世界でも素数なのである。

自然数の素数でガウス整数を用いると分解できるものとできないものはどう違うのか？少し計算してみると、次のようなことがわかる。

- $2=(1+i)(1-i)$ と分解される。これは特別な素数だと考える。
  というのは、$(1+i)^2=2i$ となり、2は平方数とほぼ同じだとみなせるのである。
- $3,7,11,19,23,\cdots$ は分解できない。
- $5=(2+i)(2-i),\quad 13=(3+2i)(3-2i),\quad 17=(4+i)(4-i),\quad 29=(5+2i)(5-2i),\cdots$

特徴を考えてみると、分解できない素数は $p=4k+3$ のタイプで、分解できる奇素数は $p=4k+1$ のタイプである。この事実の証明について、整理してみる。

目 次

1　ガウス整数 $\mathbb{Z}[i] = \{x + yi \,|\, x,\, y \in \mathbb{Z}\}$ について

1.1　ガウス整数と関連事項の定義

定義 1.1（ガウス整数）
$x, y \in \mathbb{Z},\quad i$ を虚数単位とするとき、 $a = x + yi$ と表される数を「ガウス整数」という。また、それらの集合を $\mathbb{Z}[i] = \{x + yi \,|\, x, y \in \mathbb{Z}\}$ と表す。

定義 1.2（ノルム）
複素数 $a = x + yi \quad (a, b \in \mathbb{R})$ に対して $N(a) = x^2 + y^2$ を a のノルムという。
通常、 a の絶対値を $|a| = \sqrt{x^2 + y^2}$ と定義するので、 $N(a) = |a|^2$ の関係がある。ガウス整数を扱う場合には、ノルムにした方が、値が 0 以上の整数になるので扱いやすい面がある。

補題 1.3 $N(ab) = N(a)N(b)$ が成り立つ。

証明） $a = x + yi,\, b = u + vi$ とする。$ab = (x + yi)(u + vi) = (xu - yv) + (xv + yu)i$ 。
$N(ab) = (xu - yv)^2 + (xv + yu)^2 = (x^2u^2 - 2xuyv + y^2v^2) + (x^2v^2 + 2xvyu + y^2u^2)$
$= x^2u^2 + x^2v^2 + y^2v^2 + y^2u^2 = (x^2 + y^2)(u^2 + v^2) = N(a)N(b)$　　（証明終）

定義 1.4（単数）
$N(a) = 1$ を満たすガウス整数 a を「単数（$unit$)」 と言う。

ガウス整数 $x+yi$ が単数であるとする。$x^2+y^2 = 1$ であるから、$(x,\, y) = \pm(1, 0), \pm(0, 1)$ に限られる。従って、**ガウス整数の単数は $\pm 1, \pm i$ の 4 つである。**

定義 1.5（同伴数）
ガウス整数 a, b が $a = \epsilon b \quad (\epsilon$ は単数) のとき、 a と b は同伴数であるという。

定義 1.6 $a, b \in \mathbb{Z}[i]$ をガウス整数とする。$c \in \mathbb{Z}[i]$ 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ガウス整数を 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ガウス整数を a, b の公約数という。

$a = bc$ のとき、単数 ϵ に対して、$\epsilon\bar{\epsilon} = 1$ であるから、$a = (\epsilon b)\cdot(\bar{\epsilon}c)$ 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、$5 = (2+i)(2-i)$ なので、$2 + i$ は 5 の約数であるが、その同伴数を考えると、$\pm(2 + i), \pm i(2 + i)$ 、すなわち、$2+i,\, -2-i, -1+2i,\, 1-2i$ が約数である。それらを代表して、「$2 + i$ が約数である」ということもある。このとき、$2 - i$ は $2 + i$ の同伴数でははない。($\pm(2 + i), \pm i(2 + i)$ はいずれも $2 - i$ と一致しない）従って、5 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、$2 = (1 + i)(1 - i)$ については、$1 - i = -i(1 + i)$ であるから、$1 + i$ と $1 - i$ は同伴数である。従って、 2 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。
例えば、 $a = 62, b = 47$ のときには、
$62 = 47 \times 1 + 15, \qquad 47 = 15 \times 3 + 2, \qquad 15 = 7 \times 2 + 1, \qquad 2 = 1 \times 2 + 0$
従って、62 と 47 の最大公約数（自然数の公約数のうち、最も大きな数）は 1 である。
また、この計算を遡ることにより、一次不定方程式 $62x + 47y = 1$ の特殊解 $x = 22, y = -29$ を求めることができる。

【互除法の実施と不定方程式の特殊解の求め方の例】

	62	47			a	b	
	47		(1		b		(1
	15	47			$a-b$	b	
3)		45		3)		$3a-3b$	
	15	2			$a-b$	$-3a+4b$	
	14		(7		$-21a+28b$		(7
	1	2			$22a-29b$	$-3a+4b$	
2)		2		2)		$44a-58b$	
	1	0			$22a-29b$	$-47a+62b$	

この計算は、「$a, b \in \mathbb{Z}, \quad b \neq 0$ のとき、 $a = bq + r \quad (0 \leqq r < |b|)$ を満たす整数 q, r が存在する」ということを繰り返し使っている。
ガウス整数 $\mathbb{Z}[i]$ でも類似の計算ができることを示す。

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

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

$$\frac{a}{b} = \frac{x+yi}{z+wi} = \frac{(x+yi)(z-wi)}{z^2+w^2} = \frac{(xz+yw)+(-xw+yz)i}{z^2+w^2}$$

ここで、$\left|\dfrac{xz+yw}{z^2+w^2} - u\right| \leqq \dfrac{1}{2}, \left|\dfrac{-xw+yz}{z^2+w^2} - v\right| \leqq \dfrac{1}{2}$ 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。$\left(\frac{1}{2} + 2i \text{ に近いのは } 2i \text{ と } 1 + 2i \text{ の } 2 \text{ つ}\right)$
$q = u + vi$ とすると、

$$N\left(\frac{a}{b} - q\right) = N\left(\left(\frac{xz+yw}{z^2+w^2} - u\right) + \left(\frac{-xw+yz}{z^2+w^2} - v\right)i\right) \leqq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1$$

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

ガウス整数 $\mathbb{Z}[i]$ 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。
$a, b \in \mathbb{Z}[i] \quad b \neq 0$ 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、
  $r_{k-1} = r_k q_k + r_{k+1} \quad 0 \leqq N(r_{k+1}) < N(r_k)$ を満たすガウス整数 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） $N(r_1) > N(r_2) > \quad \cdots \quad$ 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）

例 1.9 $a = -21 + 23i$, $b = -2 + 11i$ のとき

- $r_0 = -21 + 23i$, $r_1 = -2 + 11$
- $\dfrac{r_0}{r_1} = \dfrac{-21+23i}{-2+11i} = \dfrac{(-21+23i)(-2-11i)}{4+121} = \dfrac{295+185i}{125} = \dfrac{59}{25} + \dfrac{37}{25}i$
  $\dfrac{59}{25}, \dfrac{37}{25}$ に最も近い整数は、それぞれ、2, 1 であるから、$q_1 = 2 + i$
  $r_2 = r_0 - r_1 q_1 = (-21 + 23i) - (-2 + 11i)(2 + i) = -6 + 3i$
- $\dfrac{r_1}{r_2} = \dfrac{-2+11i}{-6+3i} = \dfrac{(-2+11i)(-6-3i)}{36+9} = \dfrac{45-60i}{45} = 1 - \dfrac{4}{3}i$
  よって、$q_2 = 1 - i$
  $r_3 = r_1 - r_2 q_2 = (-2 + 11i) - (-6 + 3i)(1 - i) = 1 + 2i$
- $\dfrac{r_2}{r_3} = \dfrac{-6+3i}{1+2i} = \dfrac{(-6+3i)(1-2i)}{1+4} = \dfrac{0+15i}{5} = 3i$
  よって、$q_3 = 3i$
  $r_4 = r_2 - r_3 q_3 = (-6 + 3i) - (1 + 2i) \cdot 3i = 0$
  ここで、作業が終了する。

この例では、 $r_4 = 0$ の 1 つ手前の $r_3 = 1 + 2i$ で a, b を割ってみると、

$$\frac{-21+11i}{1+2i} = \frac{(-21+11i)(1-2i)}{1+4} = \frac{25+65i}{5} = 5 + 13i$$
$$\frac{-2+11i}{1+2i} = \frac{(-2+11i)(1-2i)}{1+4} = \frac{20+15i}{5} = 4 + 3i$$

従って、 r_4 は a, b の公約数である。実は、公約数の中でノルムが最も大きなものになっている。このようなことについて考えるため、いくつかの準備をする。

補題 1.10 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 $q, r \in \mathbb{Z}[i]$ 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 1.11 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 1.10 より、$l_2 = l_1 c, \quad c \in \mathbb{Z}[i]$ 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 1.12 （最小公倍数）

$a, b \in \mathbb{Z}[i] \quad a, b \neq 0$ 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$\epsilon l \quad (\epsilon$ は単数) のどれかとなる。

補題 1.13 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 1.10 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、 $l = \epsilon g \quad (\epsilon$ 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、 l の同伴数である g も d の倍数となる。　（証明終）

補題 1.14 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、$g_2 = \epsilon g_1 \quad (\epsilon$ は単数) となる。

証明）補題 1.14 より、$g_2 = \epsilon g_1 \quad (\epsilon \in \mathbb{Z}[i])$ とできる。g_1, g_2 のノルムの最大性より、$N(g_a) = N(g_2)$ である。従って、 $N(\epsilon) = 1$ となる。よって、 ϵ は単数である。

定義 1.15 $a, b \in \mathbb{Z}[i] \quad a, b \neq 0$ 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、 $\epsilon g \quad (\epsilon$ は単数) である。逆に書くと、$gcd(a, b) = \epsilon g \quad (\epsilon$ は単数) となる。

命題 1.16 *2*つのガウス整数 $a, b \neq 0$ 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_{+1k} 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 1.17 $a, b \in \mathbb{Z}[i] \quad a, b \neq 0, \quad g = gcd(a, b)$ のとき、$a\mu + b\nu = g$ を満たす $\mu, \nu \in \mathbb{Z}[i]$ 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、

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

もし、ある $k \in \mathbb{N}$ について、

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

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

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

とできる。

この操作を繰り返していくと、

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

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

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

とできる。 （証明終）

例 1.18 補題 *1.9* において $a = -21 + 23i,\ b = -2 + 11i$ を例とした計算で求めた値は以下のとおりであった。

n	r_n	q_n
0	$-21 + 23i$	
1	$-2 + 11i$	$2 + i$
2	$-6 + 3i$	$1 - i$
3	$1 + 2i$	$3i$
4	0	

これらの値から、以下のとおり順次計算する。
$\mu_1 = 1, \quad \nu_2 = -q_2 - 1 + i$
$\mu_0 = \nu_2 = -1 + i, \quad \nu_1 = \mu_1 - q_1\nu_2 = 1 - (2 + i)(-1 + i) = 4 - i$

従って、 $(-21 + 23i)(-1 + i) + (-2 + 11i)(4 - i) = 1 + 2i$

2 ガウス整数 $\mathbb{Z}[i]$ における素数について

定義 2.1 $a \in \mathbb{Z}[i]$ がガウス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 ϵa (ϵ は単数) に限るときであるとする。

補題 2.2 $N(a) = p$ (p は有理整数 $\mathbb{N}$ における整数)
$\Longrightarrow$ a は $\mathbb{Z}[i]$ における素数である。

証明） $a = bc \quad (b, c \in \mathbb{Z}[i])$ 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、 ϵp (ϵ 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 1.17 により、 $a\mu + b\nu = 1$ を満たす $\mu, \nu \in \mathbb{Z}[i]$ 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 $a \in \mathbb{Z}[i]$ が 0 でも単数でも無いとき、 $\mathbb{Z}[i]$ 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、 $a = a_1b_1 \quad (a_1, b_1 \in \mathbb{Z}[i] \quad N(a_1), N(b_1) > 1)$ 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 $a \in \mathbb{Z}[i], \quad q \neq 0$ とするとき、単数 ϵ および $\mathbb{Z}[i]$ の相異なる素数 $p_1, p_2, \quad \cdots \quad , p_k$ があって、 $a = \epsilon p_1^{n_1} p_2^{n_2} \cdot \quad \cdots \quad \cdot p_k^{n_k} \quad n_1, n_2, \quad \cdots \quad , n_k \geqq 1$ 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 $\mathbb{Z}[i]$ 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、$a = p_1^{n_1} a_1 \quad (a_1 \in \mathbb{Z}[i])$ 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、 $m_1, m_2, \quad \cdots \quad , m_l \geqq 1$ 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 $x^2 + y^2 = p \quad (x, y$ は自然数$)$ と表すことについて

「はじめに」で書いた、 $2^2 + 1^2 = 5, \quad 2^2 + 3^2 = 13, \quad 1^2 + 4^2 = 17$ 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 $a^2 \equiv -1 \pmod{p}$ を満たす整数 a 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、$p \equiv 1 \pmod{4}$ ならば、$a^2 \equiv -1 \pmod{p}$ を満たす整数 a が存在する。 $p \equiv 3 \pmod{4}$ ならば、$a^2 \equiv -1 \pmod{p}$ を満たす整数 a は存在しない。 (なお、 $p = 2$ については、 $1^2 \equiv -1 \pmod{2}$)

定義 3.2 （*Legendre* の記号）

p を奇素数とする。$gcd(a,p) = 1$ である a について、記号 $\left(\frac{a}{p}\right)$ を次のように定義する。

もし、$x^2 \equiv a \pmod{p}$ を満たす整数 x が存在すれば、$\left(\frac{a}{p}\right) = 1$ とする。そのような整数 x が存在しなければ $\left(\frac{a}{p}\right) = -1$ とする。

例 3.3

- $p = 5$ のとき、

x	1	2	3	4
$x^2 \pmod 5$	1	4	4	1

よって、$\left(\frac{1}{5}\right) = 1, \left(\frac{2}{5}\right) = -1, \left(\frac{3}{5}\right) = -1, \left(\frac{4}{5}\right) = 1$

- $p = 7$ のとき、

x	1	2	3	4	5	6
$x^2 \pmod 5$	1	4	2	2	4	1

よって、$\left(\frac{1}{7}\right) = 1, \left(\frac{2}{7}\right) = 1, \left(\frac{3}{7}\right) = -1, \left(\frac{4}{7}\right) = 1, \left(\frac{5}{7}\right) = -1, \left(\frac{6}{7}\right) = 1$

定理 3.4 （*Euler* の規準）

p を奇素数、a を p と互いに素な整数とする。このとき

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

が成り立つ。

証明）p と互いに素な整数 a をとる。$1 \leqq k \leqq p-1$ なる任意の整数 k に対して、補題 3.1 より、$kl \equiv 1 \pmod{p}$, $1 \leqq l \leqq p-1$ を満たす整数 l がただ一つ存在する。両辺に a をかけて、$k \cdot (al) \equiv a \pmod{p}$。$0 < k' \leqq p-1$, $al \equiv k' \pmod{p}$ を満たす k' がただ一つ存在して、$kk' \equiv a \pmod{p}$ を満たす。このことから、$1, 2, \cdots, p-1$ を $kk' \equiv a \pmod{p}$ $k \leqq k'$ を満たすペア (k, k') にする。ただし、$k = k'$ を満たすものがある場合と、$k < k'$ のペアのみの場合とがある。

- $\left(\frac{a}{p}\right) = 1$ のとき

  $x^2 \equiv a \pmod{p}$ を満たす x が存在する。その一つを $x = l$ $(1 \leqq l \leqq p-1)$ とすると、$(p-l)^2 = p^2 - 2pl + l^2 \equiv l^2 \equiv a \pmod{p}$ より $= p - l$ も解になる。このとき l と $p-l$ は異なる。もし $l = p - l$ ならば、$p = 2l$ 。p は奇素数であったからこれは不可能である。また、$m^2 \equiv a \pmod{p}$ とすると、$l^2 - m^2 \equiv 0 \pmod{p}$。$(l+m)(l-m) \equiv 0$ 。p は素数なので、これが成り立つのは $l - m \equiv 0 \pmod{p}$ もしくは、$l + m \equiv 0 \pmod{p}$ である。従って、$1 \leqq x \leqq p-1$ で $x^2 \equiv a \pmod{p}$ の解は、$x = l, p - l$ の 2 つだけである。

  先に述べたペアは、(l, l) と $(p-l, p-l)$ 以外は、$\frac{1}{2}\{(p-1)-2\} = \frac{1}{2}(p-3)$ 個のペア (k, k') （ただし、$k < k'$）となる。

これを利用して $(p-1)!$ を考えると、$kk' \equiv a$ となるペアが $\frac{1}{2}(p-3)$ 個と、あとは $l,\ p-l$ の積になる。 $l(p-l) \equiv -l^2 \equiv -a$ であるから、$(p-1)! \equiv a^{\frac{1}{2}(p-3)}(-a) \equiv -a^{\frac{1}{2}(p-1)}$

具体的な例で考えてみる。

例　$p=17,\ a=2$ のとき、 $6^2 = 36 \equiv 2 \pmod{17}$ より $\left(\frac{2}{17}\right) = 1$ である。

$(k,\ k')$　$k \leqq k'$ で $kk' \equiv 2 \pmod{17}$ を満たすペアをつくると、

$(1,\ 2),\ (3,\ 12),\ (4,\ 9),\ (5,\ 14),\ (6,\ 6),\ (7,\ 10),\ (8,\ 13),\ (11,\ 11),\ (15,\ 16)$

である。従って、

$$16! = (1\cdot 2)(3\cdot 12)(4\cdot 9)(5\cdot 14)(7\cdot 10)(8\cdot 13)(15\cdot 16)\times 6\cdot 11$$

$$\equiv 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot (-2) \equiv -2^{\frac{17-1}{2}}$$

- $\left(\frac{a}{p}\right) = -1$ のとき

$x^2 \equiv a \pmod{p}$ を満たす x が存在しない。 従って、 数 1 から $p-1$ は、$kk' \equiv a \pmod{p}$ を満たす $\frac{1}{2}\{(p-1)\} = \frac{1}{2}(p-3)$ 個のペア $(k,\ k')$　(ただし、$k < k'$) に分けられる。よって、 $(n-1)! \equiv a - \frac{1}{2}(p-1)$ となる。

例　$p=17,\ a=3$ のとき、 $a^2 \equiv 3 \pmod{17}$ を満たす a が存在しないので $\left(\frac{3}{17}\right) = -1$ である。

$(k,\ k')$　$k \leqq k'$ で $kk' \equiv 3 \pmod{17}$ を満たすペアをつくると、

$(1,\ 3),\ (2,\ 10),\ (4,\ 5),\ (6,\ 9),\ (7,\ 15),\ (8,\ 11),\ (12,\ 13),\ (14,\ 16)$

である。従って、

$$16! = (1\cdot 3)(2\cdot 10)(4\cdot 5)(6\cdot 9)(7\cdot 15)(8\cdot 11)(12\cdot 13)(14,\cdot 16)$$

$$\equiv 3\cdot 3\cdot 3\cdot 3\cdot 3\cdot 3\cdot 3\cdot 3 \equiv 3^{\frac{17-1}{2}}$$

上で次のことが示されている。

- $\left(\frac{a}{p}\right) = 1$ のとき $(p-1)! \equiv -a^{\frac{p-1}{2}}$
- $\left(\frac{a}{p}\right) = -1$ のとき $(p-1)! \equiv a^{\frac{p-1}{2}}$

ここで、次の定理が成り立つ。

Wilson の定理

p **が奇素数のとき、** $(p-1)! \equiv -1 \pmod{p}$

証明）明らかに $\left(\frac{1}{p}\right) = 1$ であるから、$(p-1)! \equiv -a^{\frac{1}{2}(p-1)}$ において、$a=1$ を代入することができる。

よって、$(p-1)! \equiv -1 \pmod{p}$ となる。（証明終わり）

これを上に代入すると、Euler の基準

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

が成り立つ。（証明終）

定理 3.5（平方剰余の相互法則　第一補充則）
p を奇素数するとき

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (p = 4k+1 \text{ のとき}) \\ -1 & (p = 4k+3 \text{ のとき}) \end{cases}$$

が成り立つ。

証明）Euler の基準により $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}}$ が成り立つ。$\left(\frac{-1}{p}\right)$ の値は ± 1 であるから、この合同式は等式になる。（証明終）

3.2　$p = 4k+1$ のタイプの素数について

上の定理により、$p = 4k+1$ のとき、$1 \leqq a \leqq p-1$ で $a^2 \equiv -1$ を満たすものが存在する。$a^2 + 1 \equiv 0 \pmod{p}$ となるので、$(a-i)(a+i) = bp \quad (b \in \mathbb{Z}[i])$ とおける。このとき、ガウス整数 整数) $\mathbb{Z}[i]$ における $a-i$ と p の最大公約数を $r = gcd(a-i, p)$ とおく。$N(r)$ は $N(p) = p^2$ の公約数であるから $N(r) = 1, p, p^2$ のいずれかである。

- $N(r) = 1$ のとき $(a-i)(a+i) = a^2 + 1 = kp \quad (k$ は整数$)$ なので、$p \,|\, (a-i)(a+i)$ である。$N(r) = 1$ より $gcd(a-i, p) = 1$ であるから、命題 2.3 より、$p|a+i$ が成り立たなければいけない。したがって、$gcd(a+i, p)$ は p の倍数である。しかし、$gcd(\overline{a+i}, p) = \overline{r}$ なので、$gcd(a+i, p)$ は単数である。これは $gcd(a+i, p)$ が p の倍数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、$a-i$ が p の単数倍とならなければいけないが、これはありえない。

以上より、$N(r) = p$ である。$r = x + iy \quad (x, y \in \mathbb{Z})$ とすると、$x^2 + y^2 = p$ となる。（証明終）

この証明によると、$a^2 \equiv -1 \pmod{p}$ の解を求め、$a-i$ と p との最大公約数を考えると $x^2 + y^2 = p$ を満たす x, y が求められることになる。なお、$p - k(a-i)$ の実部が小さくなるように自然数 k を設定するとよい。

- $p = 5$ のとき

  $2^2 \equiv -1 \pmod 5$ 。 $5 - 2(2 - i) = 1 + 2i.$ $1^2 + 2^2 = 5$

- $p = 13$ のとき

  $5^2 \equiv -1 \pmod{13}$ 。 $13 - 2(5 - i) = 3 + 2i.$ $3^2 + 2^2 = 13$

- $p = 17$ のとき

  $4^2 \equiv -1 \pmod{17}$ 。 $17 - 4(4 - i) = 1 + 4i.$ $1^2 + 4^2 = 17$

- $p = 29$ のとき

  $12^2 \equiv -1 \pmod{29}$ 。 $29 - 2(12 - i) = 5 + 2i.$ $5^2 + 2^2 = 29$

- $p = 37$ のとき

  $6^2 \equiv -1 \pmod{37}$ 。 $37 - 6(6 - i) = 1 + 6i.$ $1^2 + 6^2 = 37$

- $p = 41$ のとき $9^2 \equiv -1 \pmod 5$ 。 $41 - 4(9 - i) = 5 + 4i.$ $5^2 + 4^2 = 41$

順に調べていくと、このような計算で常に $x^2 + y^2 = p$ の解が求められるのかと思ってしまうが、そうとは限らない。

- $p = 89$ のとき

  $34^2 \equiv -1 \pmod{89}$ 。 $89 - 3(34 - i) = -13 + 3i.$ $13^2 + 3^2 = 178 = 2 \cdot 89$

- $p = 521$ のとき

  $235^2 \equiv -1 \pmod{521}$ 。 $521 - 2(235 - i) = 51 + 2i.$ $51^2 + 2^2 = 2605 = 5 \cdot 521$

89 の場合は、 $(34 - i) + 2(-13 + 3i) = 8 + 5i.$ $8^2 + 5^2 = 89$
521 の場合は、$(235 - i) - 5(51 + 2i) = -20 - 11i.$ $20^2 + 11^2 = 521$
いずれもユークリッドのアルゴリズムをもう一段増やしてやると、 $x^2 + y^2 = p$ の解が求められる。
※　$p = 4k + 1$ が大きな素数であるとき、 $x^2 + y^2 = p$ の解を $a^2 \equiv -1 \pmod p$ の解をもとに求めるのがいい方法なのかどうかは、よくわからない。

3.3　$p = 4k + 3$ のタイプの素数について

$x, y \in \mathbb{N}$ のとき、 $x^2, y^2 \equiv 0, 1 \pmod 4$　であるから、 $x^2 + y^2 \equiv 3 \pmod 4$ が成り立つことはない。したがって、 $p = 4k + 3$ のタイプの素数 p について、 $x^2 + y^2 = p$ を満たす自然数 x, y は存在しない。
以上により、$p = 4k + 1$ のタイプの素数については、必ず $x^2 + y^2 = p$ を満たす自然数 x, y が存在し、また、 $p = 4k + 3$ のタイプの素数については $x^2 + y^2 = p$ 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] 「An Introduction to the Theory of Numbers」 Oxford University Press （ネット上で閲覧できる）

[2] 高木貞治「初等整数論講義　第 2 版」　共立出版株式会社（ネット上で閲覧できる）