複素整数の素数

1　複素数

定義 1（**共役・ノルム・絶対値・シュプール**）

$\alpha = a + bi (a, b \in \mathbb{R})$ を複素数とするとき，次のように定義する．

α の共役 (conjugate)	$\overline{\alpha} = a - bi$
α の絶対値 (absolute value)	$\lvert\alpha\rvert = \sqrt{a^2 + b^2}$
α のノルム (norm)	$N(\alpha) = a^2 + b^2 = \alpha\overline{\alpha} = \lvert\alpha\rvert^2$
α のシュプール (spure) あるいはトレース (trace)	$S(\alpha) = \alpha + \overline{\alpha} = 2a$

定理 1（**複素数の性質**）

1. $a \in \mathbb{R}$ ならば $\overline{a\alpha} = a\overline{\alpha}$
2. $\overline{\overline{\alpha}} = \alpha$
3. $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$
4. $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$
5. $\beta \neq 0$ ならば $\overline{\left(\dfrac{\alpha}{\beta}\right)} = \dfrac{\overline{\alpha}}{\overline{\beta}}$
6. $\lvert\alpha\rvert = \lvert\overline{\alpha}\rvert$
7. $\lvert\alpha\rvert - \lvert\beta\rvert \leq \lvert\alpha + \beta\rvert \leq \lvert\alpha\rvert + \lvert\beta\rvert$（**三角不等式**）
8. $\lvert\alpha\beta\rvert = \lvert\alpha\rvert\lvert\beta\rvert$
9. $\left\lvert\dfrac{\alpha}{\beta}\right\rvert = \dfrac{\lvert\alpha\rvert}{\lvert\beta\rvert} \quad (\beta \neq 0)$
10. $N(\alpha) = N(\overline{\alpha})$
11. $N(\alpha\beta) = N(\alpha)N(\beta)$
12. $N\left(\dfrac{\alpha}{\beta}\right) = \dfrac{N(\alpha)}{N(\beta)} \quad (\beta \neq 0)$
13. $S(\alpha + \beta) = S(\alpha) + S(\beta)$

[証明略]

2　複素整数（ガウス整数）

定義 2 複素数 $\alpha = a + bi$ において a, b ともに整数である複素数を**複素整数**あるいは**ガウス整数**とよび，複素整数全体の集合を $\mathbb{Z}[i]$ と表す．つまり

$$\mathbb{Z}[i] = \{\alpha | \alpha = a + bi, a, b \in \mathbb{Z}\}$$

である．

$\mathbb{Z}[i]$ は環である（**ガウスの整数環**）．通常の整数を複素整数と区別する場合**有理整数**とよぶ場合もある．また単に**整数**と言った場合，複素整数の方を指す場合もある．以下，特にことわりのない限りアルファベットは有理整数，ギリシャ文字は複素整数を表すものとする．ただし i は虚数単位である．

3　複素整数の除法

定理 2　［**複素整数の除法**］複素整数 α, β に対して

$$\alpha = \beta\kappa + \rho, \qquad N(\rho) \leq \frac{N(\beta)}{2} \tag{1}$$

となる複素整数 κ, ρ が存在する．

[証明]

$$\xi = \frac{\alpha}{\beta} = x + yi$$

と置く．

$$\kappa = \left[x + \frac{1}{2}\right] + \left[y + \frac{1}{2}\right] i \tag{2}$$

とすると，

$$|\xi - \kappa| \leq \frac{1}{\sqrt{2}}$$

$$\left|\frac{\alpha}{\beta} - \kappa\right| \leq \frac{1}{\sqrt{2}}$$

$$|\alpha - \beta\kappa| \leq \frac{|\beta|}{\sqrt{2}}$$

$$N(\alpha - \beta\kappa) \leq \frac{N(\beta)}{2}$$

$\rho = \alpha - \beta\kappa$ と置くと (1) を満たす．　[証明おわり]

(1) の条件だけでは除法は一意的には決まらないこともあるが，(2) と定めることによって一意的に決まる．

問題 1　ガウスの整数環における除法を行い，

$$13 + 5i = (7 - 2i)\kappa + \rho$$

となる κ, ρ を求めよ．

［解］

$$\frac{13 + 5i}{7 - 2i} = \frac{(13 + 5i)(7 + 2i)}{53} = \frac{81 + 61i}{53}$$

$$\kappa = \left[\frac{81}{53} + \frac{1}{2}\right] + \left[\frac{61}{53} + \frac{1}{2}\right] i = 2 + i$$

$$\rho = 13 + 5i - (7 - 2i)(2 + i) = 13 + 5i - (16 + 3i) = -3 + 2i$$

$$\therefore 13 + 5i = (7 - 2i)(2 + i) + (-3 + 2i)$$

これが一応正解ではあるが，定理 2 の条件だけでは一意的に定まらないことを示すと，

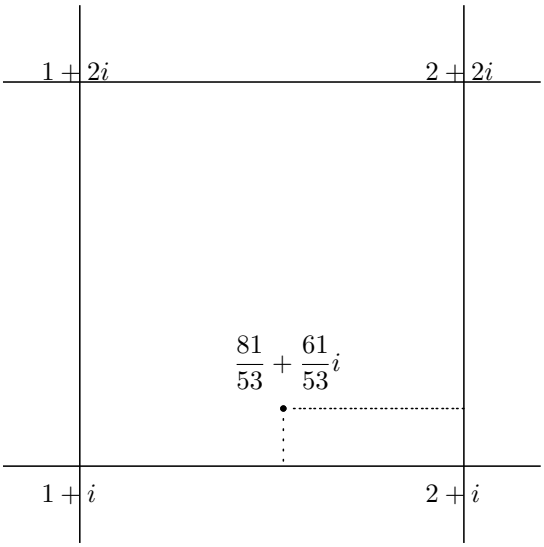
$$\kappa = 1 + i$$

とすると,

$$\rho = 13 + 5i - (7 - 2i)(1 + i) = 13 + 5i - (9 + 4i) = 4$$

となり,

$$N(\rho) = 16 < \frac{53}{2}$$



で条件を満たす．ちなみに，次で定める「割り切れる」ような場合は定理 1 の条件だけでも除法は一意的に定まる．

4　約数・倍数・単数・同伴数

定義 3 定理 1 において $\rho = 0$ のときつまり $\alpha = \beta\kappa$ のとき，α は β で**割り切れる**といい,

$$\beta \mid \alpha$$

と表す．α を β の**倍数**，β を α の**約数** (**因数**) とよぶ．$\rho \neq 0$ のときつまり $\alpha \neq \beta\kappa$ のとき，α は β で**割り切れない**といい,

$$\beta \nmid \alpha$$

と表す．**公約数**，**公倍数**の定義は $\mathbb{Z}$ の場合と同様である．

定義 4 公約数の中で ノルムが最大のもの を**最大公約数**とよぶ．公倍数の中で 0 を除き ノルムが最小のもの を**最小公倍数**とよぶ．α, β の 最大公約数を (α, β) と表す．α, β の最小公倍数を $\{\alpha, \beta\}$ と表す（$[\alpha, \beta]$ と表す流儀もある）．

定理 3 $\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n$ が β の倍数ならば,

$$\alpha_1\gamma_1 + \alpha_2 + \gamma_2 + \alpha_3\gamma_3 + \cdots + \alpha_n\gamma_n$$

は β の倍数である．

［証明］

$$\frac{\alpha_1\gamma_1+\alpha_2+\gamma_2+\alpha_3\gamma_3+\cdots+\alpha_n\gamma_n}{\beta}=\frac{\alpha_1}{\beta}\gamma_1+\frac{\alpha_2}{\beta}+\gamma_2+\frac{\alpha_3}{\beta}\gamma_3+\cdots+\frac{\alpha_n}{\beta}\gamma_n$$

であるから右辺は整数である．　[証明おわり]

定理 4 二つ以上の整数の公倍数は最小公倍数の倍数である．

［証明］$\alpha,\beta,\gamma,\cdots$ の最小公倍数を λ とし，μ を任意の公倍数とする．μ を λ で割り

$$\mu=\kappa\lambda+\rho,\qquad N(\rho)\leq\frac{N(\lambda)}{2}$$

とすれば,

$$\rho=\mu-\kappa\lambda$$

定理 3 より ρ もやはり $\alpha,\beta,\gamma,\cdots$ の公倍数である．しかしながら 0 を除きノルムが最小の公倍数が λ であるから,

$$N(\rho)\leq\frac{N(\lambda)}{2}$$

を満たすのは

$$\rho=0$$

以外にない．すなわち

$$\mu=\kappa\lambda$$

つまり $\alpha,\beta,\gamma,\cdots$ の公倍数は最小公倍数の倍数である．　[証明おわり]

定理 5 二つ以上の整数の公約数は最大公約数の約数である．

［証明］$\alpha,\beta,\gamma,\cdots$ の最大公約数を μ とし，δ を任意の公約数とする．μ と δ の最小公倍数を λ とする．α は μ の倍数であり，また δ の倍数でもある．よって α は μ,δ の公倍数である．よって α は λ の倍数である．同様に $\beta,\gamma,\cdots$ は λ の倍数である．よって λ は $\alpha,\beta,\gamma,\cdots$ の公約数である．よって

$$N(\lambda)\leq N(\mu)$$

また λ は μ の倍数でもあり，0 ではないから

$$N(\lambda)\geq N(\mu)$$

$$\therefore\lambda=\mu$$

よって δ は μ の約数である．　[証明おわり]

定義 5 全ての整数の約数である整数を**単数** (unit,Einheit) とよぶ．

定理 6 $\mathbb{Z}[i]$ の単数は

$$\pm1,\pm i$$

の 4 個である．

[証明] 全ての整数の約数なので 1 の約数でもある．単数を $\epsilon = a + bi$ とすると，

$$\frac{1}{\epsilon} = \epsilon'$$

とおくことができ，ϵ' は整数である．（実際は ϵ' も単数になるのだが，この時点では一応ただの整数とする．）

$$\epsilon\epsilon' = 1$$

ノルムの性質により

$$N(\epsilon\epsilon') = N(\epsilon)N(\epsilon') = 1$$

$$\therefore N(\epsilon) = 1$$

$$\therefore a^2 + b^2 = 1$$

$$\therefore (a, b) = (\pm 1, 0), (0, \pm 1)$$

つまり，

$$\epsilon = \pm 1, \pm i$$

である．逆に $\epsilon = \pm 1, \pm i$ であるとき，明らかに ϵ は全ての複素整数の約数となる．よって単数は $\pm 1, \pm i$ の 4 個である．　[証明おわり]

定義 6（同伴数） $\dfrac{\alpha}{\beta}$ が単数であるとき，α と β は**同伴** (associate) であるという．α の同伴数は $\alpha, -\alpha, i\alpha, -i\alpha$ の 4 個である．また同伴数のうち，第一象限にあるものを**正規型**と呼ぶことがある．

定理 7 α, β の最小公倍数を λ，最大公約数を μ とすれば，

$$\alpha\beta = \epsilon\lambda\mu$$

（ただし ϵ は単数とする．）

［証明］λ は α, β の公倍数であるから

$$\lambda = \alpha\beta' = \beta\alpha' \tag{3}$$

とおける．さて $\alpha\beta$ はもちろん α, β の公倍数であるから，$\alpha\beta$ は λ の倍数である．よって

$$\alpha\beta = \delta\lambda \tag{4}$$

とおける．(3) を (4) に代入して，

$$\alpha\beta = \delta\alpha\beta' = \delta\beta\alpha'$$

つまり

$$\alpha = \delta\alpha', \qquad \beta = \delta\beta'$$

を得る．ゆえに δ は α, β の公約数である．よって

$$\mu = \delta\kappa \tag{5}$$

とする．α, β は μ の倍数であるから

$$\delta\alpha' = \alpha''\delta\kappa, \qquad \delta\beta' = \beta''\delta\kappa$$

とおけ，さらには

$$\alpha' = \alpha''\kappa, \qquad \beta' = \beta''\kappa \tag{6}$$

を得る．(6) を (3) に代入して，

$$\lambda = \alpha\beta''\kappa = \beta\alpha''\kappa$$

さらに

$$\frac{\lambda}{\kappa} = \alpha\beta'' = \beta\alpha''$$

つまり $\dfrac{\lambda}{\kappa}$ は α, β の公倍数である．$N(\kappa) > 1$ とすると $N\left(\dfrac{\lambda}{\kappa}\right) < N(\lambda)$ となり λ が最小公倍数であることと矛盾する．

$$\therefore \kappa = \epsilon$$

(5) より

$$\mu = \delta\epsilon$$

$$\therefore \delta = \epsilon\mu \tag{7}$$

(7) を (4) に代入して，

$$\alpha\beta = \epsilon\lambda\mu$$

[証明おわり]

二つの整数 α, β が単数以外の公約数を有しないときには，α, β を**互いに素**といい，$(\alpha, \beta) = 1$ と表す．

定理 8 $(\alpha, \beta) = 1$ で，かつ $\alpha \mid \beta\gamma$ ならば，$\alpha \mid \gamma$

［証明］$(\alpha, \beta) = 1$ であるから α, β の最小公倍数は $\alpha\beta$ である．しかるに仮定により $\beta\gamma$ は α の倍数である．よって $\beta\gamma$ は α, β の公倍数である．よって $\beta\gamma$ は $\alpha\beta$ の倍数である．

故に

$$\frac{\beta\gamma}{\alpha\beta} = \frac{\gamma}{\alpha}$$

は整数である．すなわち，γ は α で割り切れる．　[証明おわり]

5　素数

定義 7（**素数**）複素整数 α について，α 自身と単数は**自明（トリビアル）な約数**といい，それ以外の約数を**真の約数**と呼ぶ．0 と単数を除く α が真の約数をもたないとき α は**素数**と呼ぶ．0，単数，素数以外を**合成数**と呼ぶ．有理整数の素数を特に区別して**有理素数**と呼ぶことがある．

定理 9 複素整数 α のノルム $N(\alpha)$ が有理素数ならば，α は素数である．逆は成り立たない．

[証明]　α が合成数とすると，単数以外の β, γ を用いて

$$\alpha = \beta\gamma$$

と表せる．

$$N(\alpha) = N(\beta)N(\gamma)$$

これが有理素数であるから，β, γ のどちらかが単数である．よって合成数であるという仮定と矛盾する．よって α は素数である．　[証明おわり]

有理素数が $\mathbb{Z}[i]$ の素数であることもあるし，合成数であることもある．

問題 2 有理素数 2 が $\mathbb{Z}[i]$ の合成数であることを示せ．

[解]　2 が合成数であるとすると，単数以外の β, γ を用いて

$$2 = \beta\gamma$$

と表せる．

$$N(2) = N(\beta)N(\gamma)$$

$$N(\beta)N(\gamma) = 4$$

$$\therefore N(\beta) = N(\gamma) = 2$$

$$\therefore \beta = 1 \pm i, -1 \pm i, \gamma = 1 \pm i, -1 \pm i$$

このなかで，例えば，

$$(1+i)(1-i)$$

などが 2 の素因数分解を与える．よって，たしかに 2 は合成数である．　[証明おわり]

問題 3 $1+i$ が素数であることを示せ．

[解]　$1+i$ が合成数であると仮定すると，単数以外の β, γ を用いて

$$1 + i = \beta\gamma$$

と表せる．

$$N(1+i) = N(\beta)N(\gamma)$$

$$N(\beta)N(\gamma) = 2$$

$$\therefore N(\beta) = 1 \ or \ N(\gamma) = 1$$

これは β, γ が単数以外の数であることと矛盾する．よって $1+i$ は素数である．　[証明おわり]

問題 4 3,5,7,11,13 が素数か合成数かを判定せよ．

[解]　3 が合成数であると仮定すると，単数以外の β, γ を用いて

$$3 = \beta\gamma$$

と表せる．

$$N(3) = N(\beta)N(\gamma)$$

$$N(\beta)N(\gamma) = 9$$

$$\therefore N(\beta) = N(\gamma) = 3$$

このような β, γ は存在しないので 3 は素数である．

5 が合成数であると仮定すると，単数以外の β, γ を用いて

$$5 = \beta\gamma$$

と表せる．

$$N(\beta)N(\gamma) = 25$$

$$\therefore N(\beta) = N(\gamma) = 5$$

$\beta = 1 + 2i, \gamma = 1 - 2i$ などがこれを満たすので 5 は合成数である．

7 が合成数であると仮定すると，単数以外の β, γ を用いて

$$7 = \beta\gamma$$

と表せる．

$$N(\beta) = N(\gamma) = 7$$

このような β, γ は存在しないので 7 は素数である．

11 が合成数であると仮定すると，単数以外の β, γ を用いて

$$11 = \beta\gamma$$

と表せる．

$$N(\beta) = N(\gamma) = 11$$

このような β, γ は存在しないので 11 は素数である．

13 が合成数であると仮定すると，単数以外の β, γ を用いて

$$13 = \beta\gamma$$

と表せる．

$$N(\beta) = N(\gamma) = 13$$

$\beta = 3 + 2i, \gamma = 3 - 2i$ などがこれを満たすので 13 は合成数である．

定理 10 $4m + 3$ 型の有理素数は素数である．

［証明］有理素数 $p = 4m + 3$ が合成数であると仮定すると，単数以外の β, γ を用いて

$$p = \beta\gamma$$

と表せる．

$$N(\beta) = N(\gamma) = p$$

$\beta = a + bi$ とおく．p は奇数なので $a^2 + b^2$ も奇数．つまり a, b ともに偶数であることはなく，両方とも奇数であることもない．つまりどちらかが奇数でどちらかが偶数である．今 $a = 2k, b = 2l + 1$ とすると，$a^2 + b^2 = 4k^2 + 4l^2 + 4l + 1$ となり $4m + 3$ とはなりえない．a の方が奇数でも同様である．よってこのような a, b の組は存在せず，p は素数である．［証明おわり］

定理 11 ρ を素数とするとき，$\rho \mid \alpha\beta$ ならば $\rho \mid \alpha$ または $\rho \mid \beta$ である．

［証明］$(\rho,\alpha)\neq 1$ のときつまり α が ρ の倍数であるとき，明らかに $\rho\mid\alpha$．$(\rho,\alpha)=1$ のとき定理 8 より $\rho\mid\beta$.　［証明おわり］

定理 12 $4m+1$ 型の有理素数は合成数である．

［証明］$p=4m+1$ とおく．平方剰余の第一補充法則より

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

つまり

$$a^2+1=bp$$

となる a,b が存在する．つまり

$$(a+i)(a-i)=bp$$

が成り立つ．定理 11 より，p が素数ならば $p\mid a+i$ または $p\mid a-i$ つまり $p(c+di)=a+i$ または $p(c+di)=a-i$ であるが，このようなことはあり得ない（$pd=\pm 1$ になることはない）ので p は素数ではない.　［証明おわり］

定理 13 $4m+1$ 型の有理素数は二つの互いに共役である素数の積 $\pi\overline{\pi}$ で表せる．この二つの素数は同伴数ではない.

［証明］$p=4m+1$ とおく．前定理より p は合成数であることがわかった．よって単数でない π_1,π_2 を用いて次のように表せる.

$$p=\pi_1\pi_2$$

$$N(p)=p^2$$

より

$$N(\pi_1)=N(\pi_2)=p$$

定理 9 より π_1,π_2 は素数であることがわかった．$\pi_1=x_1+y_1i,\pi_2=x_2+y_2i$ とおくと，

$${x_1}^2+{y_1}^2={x_2}^2+{y_2}^2=p \tag{8}$$

$$x_1x_2-y_1y_2+(x_1y_2+x_2y_1)i=p$$

つまり

$$x_1x_2-y_1y_2=p \tag{9}$$

$$x_1y_2+x_2y_1=0 \tag{10}$$

(8),(9) より

$$(x_1-x_2)^2+(y_1+y_2)^2=0$$

$$\therefore x_1=x_2,\quad y_1=-y_2$$

$$\therefore \pi_1=\overline{\pi_2}$$

また π_1, π_2 が同伴数であると仮定すると．

$$\frac{\pi_1}{\pi_2} = \frac{{x_1}^2 - {y_1}^2 + 2x_1y_1i}{{x_1}^2 + {y_1}^2}$$

が単数にならなければいけないが，(8) より $x_1 = 0$ または $y_1 = 0$ となることもないし，${x_1}^2 = {y_1}^2$ となることもないので，同伴数ではない．［証明おわり］

問題 5 π_1 を素数とする．$\pi_1\pi_2$ が有理整数となるとき $\pi_2 = a\overline{\pi_1}$ であることを証明せよ．

［解］$\pi_1 = x_1 + y_1i, \pi_2 = x_2 + y_2i$ とおくと，

$$\pi_1\pi_2 = x_1x_2 - y_1y_2 + (x_1y_2 + x_2y_1)i$$

つまり

$$x_1y_2 = -x_2y_1 \tag{11}$$

π_1 が素数なので，有理整数の範囲において，x_1, y_1 は互いに素である．つまり

$$x_2 = ax_1, \quad y_2 = by_1$$

とおける．(11) より

$$bx_1y_1 = -ax_1y_1$$

つまり

$$a = -b$$

であるので

$$\pi_2 = a\overline{\pi_1}$$

［証明おわり］

素数にある整数をかけて有理整数になるのは共役複素整数あるいはその有理整数倍に限ることがわかった．言い換えると素数の倍数である有理整数のなかで，最小のもの（もちろん 0 を除いた正の有理整数のなかで）は共役な素数同士の積であることがわかった．

定理 14 π を素数とすると，$\pi\overline{\pi}$ は有理素数である．

［証明］$p = \pi\overline{\pi}$ とする．p は π で割り切れる自然数の中で，最小のものである．π は単数でないから，$p \neq 1$．もしも p が有理整数の合成数なら

$$p = ab$$

とおける．もちろん

$$p > a > 1, \quad p > b > 1$$

である．π は素数だから，$\pi \mid a$ または，$\pi \mid b$ となり，p がこのような自然数の中で最小のものであるという仮定と矛盾する．よって p は有理素数である．［証明おわり］

これまでのことから複素整数の素数の全貌がおおよそ明らかになった．まとめると

$\mathbb{Z}[i]$ の素数 π は次のいずれかである.

1. $1+i$ とその同伴数.
2. $4m+3$ 型の有理素数とその同伴数.
3. $N(\pi)$ が $4m+1$ 型の有理素数である整数.

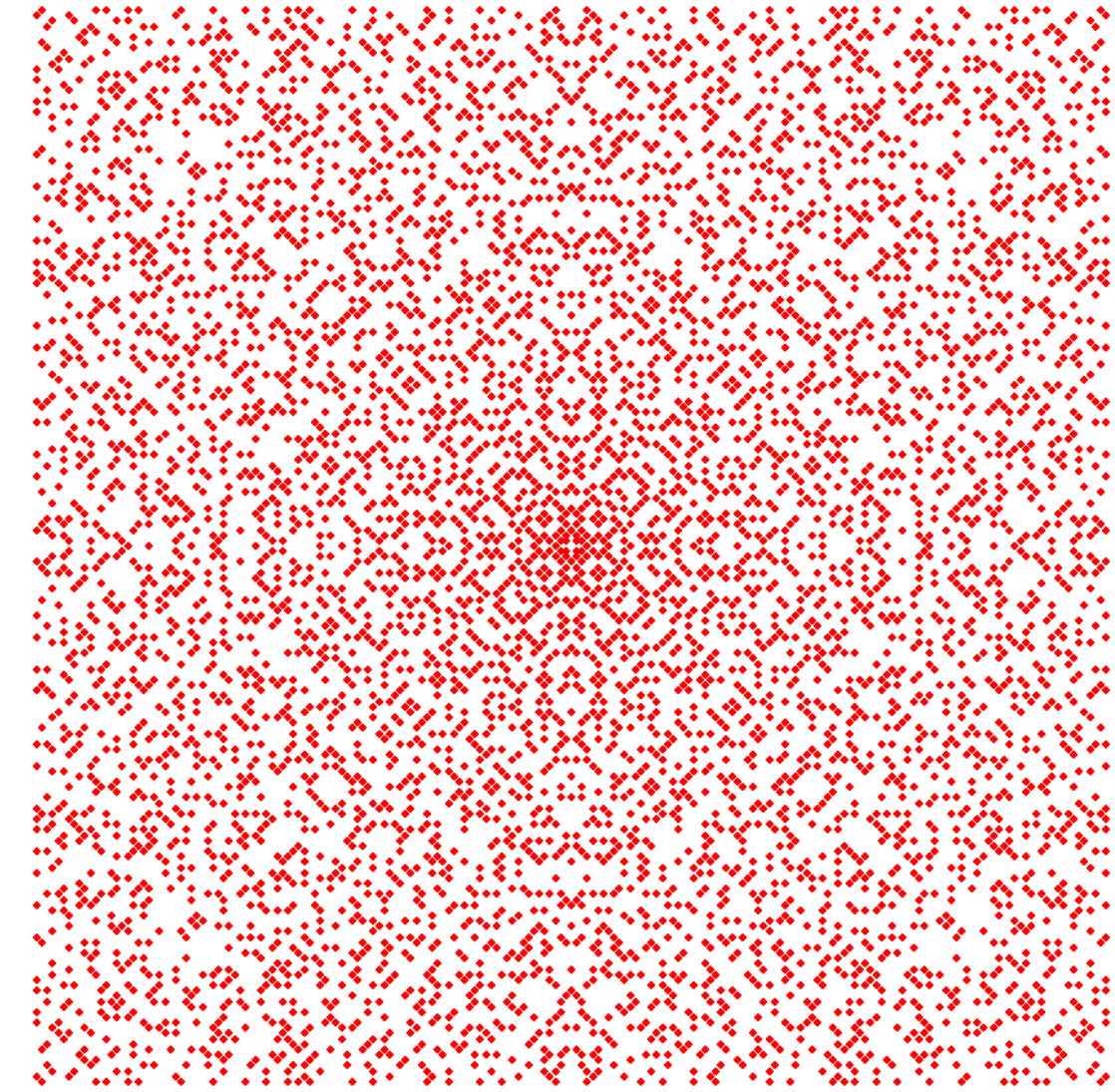


図 1　ガウス整数の素数分布

6　ガウスの整数環の基本定理

定理 15 全ての整数 θ は，単数因子の違いを除き，ただ一通りの方法で，素数の積に分解できる．

［証明］θ が素数ならば，それで証明は終わる．もしも θ が素数でなければ有限個の約数をもつ．もし有限でないとすると，同じノルムをもつ素数は有限個であるから，それらノルムを順番に並べると，

$$N_1 < N_2 < N_3 < \cdots$$

となり，θ 自身が有限であることと矛盾する．

θ の約数のうちでノルムが最小のものを α_1 とすると，α_1 は素数である．

$$\theta = \alpha_1 \alpha$$

α が素数ならこれで証明は終わる．素数でなければこれを繰り返すことにより，θ は有限個の素数の積に分解できることが証明できる．

また，θ が次のように二通りに素因数分解されたとする．

$$\theta = \alpha_1\alpha_2\alpha_3 = \beta_1\beta_2\beta_3\beta_4$$

$\alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3, \beta_4$ は全て素数で等しいものがあってもよい．

$$\alpha_1 \mid \theta$$

より，$\beta_1\beta_2\beta_3\beta_4$ の中でどれかは α_1 に等しい．これを β_1 とし θ を $\alpha_1 = \beta_1$ で割ると，

$$\alpha_2\alpha_3 = \beta_2\beta_3\beta_4$$

同様に続けていけば，最後に残った $\beta_4 = 1$．結局

$$\theta = \alpha_1\alpha_2\alpha_3 = \beta_1\beta_2\beta_3$$

で，

$$\alpha_1 = \beta_1, \alpha_2 = \beta_2, \alpha_3 = \beta_3$$

なので全く同じ素因数分解となる．　［証明おわり］

問題 6 素因数分解せよ．

1. $2 + 9i$
2. $5 + 7i$
3. $11 - 10i$
4. $-22 + 16i$
5. $33 + 61i$

［解］

1.

$$N(2 + 9i) = 4 + 81 = 85 = 5 \times 17$$

$$(1 + 2i)(4 + i) = 2 + 9i$$

2.

$$N(5+7i) = 25+49 = 74 = 2\times 37$$

$$(1+i)(6+i) = 5+7i$$

3.

$$N(11-10i) = 221 = 13\times 17$$

つまり $2+3i$ またはその共役の同伴数を因数とする.

$$\frac{11-10i}{2+3i} = \frac{-8-53i}{13}, \frac{11-10i}{2-3i} = \frac{52+13i}{13} = 4+i$$

より,

$$11-10i = (2-3i)(4+i)$$

4.

$$-22+16i = 2(-11+8i) = (1+i)(1-i)(-11+8i)$$

$$N(-11+8i) = 121+64 = 185 = 5\times 37$$

よって $1+2i$ またはその共役を因数にもつ.

$$\frac{-11+8i}{1+2i} = \frac{5+30i}{5} = 1+6i$$

$$\therefore -22+16i = (1+i)(1-i)(1+2i)(1+6i)$$

5.

$$N(33+61i) = 1089+3721 = 4810 = 2\times 5\times 13\times 37$$

ノルムの小さいほうから順に求めていくと,

$$\frac{33+61i}{1+i} = \frac{94+28i}{2} = 47+14i$$

$$\frac{47+14i}{1+2i} = \frac{75-80i}{5} = 15+16i$$

$$\frac{15+16i}{2+3i} = \frac{78-13i}{13} = 6-i$$

$$\therefore 33+61i = (1+i)(1+2i)(2+3i)(6-i)$$

定理 16 有理奇素数 p が二つの有理整数の平方和で表せる必要十分条件は p が $4m+1$ 型の素数であることである.

［証明］p が二つの有理整数の平方和で表せたとすると,

$$p = a^2+b^2$$

とかける．p は奇数なので，a, b のどちらかが奇数で，他方が偶数である.

$$a = 2l+1, \quad b = 2n$$

とすると，

$$p = 4(l^2 + l + n^2) + 1$$

となり p は $4m+1$ 型である．逆に，p が $4m+1$ 型の素数であるとき，定理 13 より, 単数でない π により

$$p = \pi\overline{\pi}$$

と素因数分解できる．

$$\pi = a + bi$$

とすると

$$p = a^2 + b^2$$

［証明おわり］

7　無限降下法

素数 p は $4m+1$ 型とする．平方剰余の第一補充法則により

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

つまり

$$x^2 + 1 \equiv 0 \pmod{p}$$

となるような $x(1 < x < p)$ がある．このとき

$$(p-x)^2 + 1 = x^2 - 2px + p^2 + 1 \equiv 0 \pmod{p}$$

でもあるからそのような x のうち小さいほうを選べば

$$x^2 + 1 \equiv 0 \pmod{p}, \quad 1 < x < \frac{p}{2}$$

とすることができる．つまり

$$x^2 + 1 = kp, \quad 1 < x < \frac{p}{2}$$

$$k < \frac{p}{2}$$

である．今，便宜上

$$x^2 + y^2 = kp \tag{12}$$

とする．k を法として

$$u \equiv x \pmod{k}, \quad -\frac{k}{2} < u \leq \frac{k}{2}$$

$$v \equiv y \pmod{k}, \quad -\frac{k}{2} < v \leq \frac{k}{2}$$

となるような u, v を選べば,

$$u^2 + v^2 \equiv 0 \pmod{k}$$

となり，

$$u^2+v^2=tk,\quad (t\leq\frac{k}{2}) \tag{13}$$

と表すことができる．(12) と (13) を辺々かければ，

$$(x^2+y^2)(u^2+v^2)=pk^2t$$

左辺を変形して

$$(xv-yu)^2+(xu+yv)^2=pk^2t \tag{14}$$

ここで

$$u\equiv x,\quad v\equiv y\pmod{k}$$

なので

$$xv-yu\equiv xy-xy\equiv 0\pmod{k}$$
$$xu+yv\equiv x^2+y^2\equiv 0\pmod{k}$$

つまり，(14) は両辺を k^2 で割ることができ，さらに

$$kz=xv-yu,\ kw=xu+yv$$

とすることにより

$$z^2+w^2=pt, t\leq\frac{k}{2}$$

を得る．z,x,t を x,y,k に置き換えて (12) に戻り，$t=1$ となるまで繰り返す．そしてついには

$$a^2+b^2=p$$

を得る．このような方法を**無限降下法**と呼ぶ.

問題 7 無限降下法により次の奇素数を二つの平方和に分解せよ.

1. $p=13$
2. $p=97$

［解］

1. 平方剰余の第一補充法則により

$$\left(\frac{-1}{13}\right)=1$$

つまり

$$x^2+1\equiv 0\pmod{13}$$

となる x がある．たかだか 13 なので順に探すと

$$5^2+1^2=13\cdot 2$$

を得る．$u=1,v=1$ とすると

$$5-1=4,5+1=6$$
$$4^2+6^2=2^2\times 13$$

の両辺を 4 で割って

$$2^2+3^2=13$$

2.

$$22^2+1=97\times 5$$

$u=2,v=1$ とすると

$$(22-2)^2+(44+1)^2=5^2\cdot 4^2+5^2\cdot 9^2=5^2\cdot 97$$

より

$$4^2+9^2=97$$

8　一般の有理整数の二平方和分解

定理 17 全ての素因数が $4m+1$ 型の素数であるような正の有理整数は二平方和に分解できる.

［証明］これまでのことと，恒等式

$$(a^2+b^2)(c^2+d^2)=(ad-bc)^2+(ac+bd)^2 \tag{15}$$

より明らか.　［証明おわり］

定理 18 有理整数 $n\neq 1$ が，互いに素である有理整数 x,y により

$$n=x^2+y^2$$

と平方和に分解できるならば，n の全ての約数も有理整数の二平方和に分解できる.

［証明］

$$n=(x+yi)(x-yi)=\alpha\overline{\alpha}$$

とし，$\alpha=x+yi$ を素因数分解する.

$$\alpha=\pi_1\pi_2\pi_3\cdots\pi_k$$

$\pi_1,\pi_2,\pi_3,\cdots,\pi_k$ の中に有理素数 p があれば

$$p\mid\alpha,\ p\mid x,\ p\mid y$$

で，$(x,y)=1$ に反するから，$\pi_1,\pi_2,\pi_3,\cdots,\pi_k$ は全て有理整数でない素数で,

$$n=N(\alpha)=N(\pi_1)N(\pi_2)N(\pi_3)\cdots N(\pi_k)=p_1p_2p_3\cdots p_k$$

ここで $p_1,p_2,p_3,\cdots,p_k$ は 2 または $4m+1$ 型の有理素数である．これらはいずれも 2 平方和分解ができる．n の約数はこれらの積で表せるので，恒等式 (15) より n の任意の約数は有理整数の二平方和で表せる.

［証明おわり］

参考文献

[1] 高木貞治『初等整数論講義第 2 版』（共立出版社，1997 年）
[2] 芹沢正三『数論入門』（講談社ブルーバックス，2008 年）