円上の格子点

志甫　淳*

2022年10月9日

目 次

1　円上の格子点：問題

円は最も基本的な幾何学的図形の一つであり，何千年も前から数学的考察の対象であったとされる．円は数学のあらゆる分野 (代数，幾何，解析，応用) に現れるが，この話では，代数的な観点から円に関するある問題を考えてみたい．

座標平面内で，原点Oを中心とする円を考える．平面に座標を入れる，ということは，平面に縦横の直線たちを碁盤の目のように引くことを意味する．それらの直線たちと曲線である円との交わりの様子は少し不思議である．

座標平面において，x座標，y座標がともに整数であるような点を格子点とよぶことにし，次の問題を考えてみよう．

問題 1. 原点Oを中心とする円上に格子点はいくつあるか？

*東京大学大学院数理科学研究科．令和４年度群馬県高校生数学キャンプ「円の数学」における講演 (講演者：志甫　淳，岩木耕平)．

もちろん，この問題の答えは円の半径に依存する．点 (x, y) の原点 O からの距離は $\sqrt{x^2+y^2}$ であるから，正の実数 r に対して，原点 O を中心とする半径 r の円の方程式は

$$x^2 + y^2 = r^2$$

である．従って，上の問は $x^2+y^2=r^2$ を満たす整数の組 (x, y) の個数を問う問題である．もしこのような整数の組 (x, y) が存在すれば r^2 は正の整数になるから，そのような場合だけを考えればよい．従って，問題は次のようになる．

問題 2. n を正の整数とするとき，$x^2+y^2=n$ を満たす整数の組 (x, y) の個数 $S(n)$ はいくつか？

2 観察

問題 2 について考えるため，小さな n に対して，$x^2+y^2=n$ を満たす整数の組 (x, y) とその個数 $S(n)$ を求めてみよう．

n	(x, y)	$S(n)$
1	$(\pm1, 0), (0, \pm1)$	4
2	$(\pm1, \pm1)$	4
3		0
4	$(\pm2, 0), (0, \pm2)$	4
5	$(\pm2, \pm1), (\pm1, \pm2)$	8
6		0
7		0
8	$(\pm2, \pm2)$	4
9	$(\pm3, 0), (0, \pm3)$	4
10	$(\pm3, \pm1), (\pm1, \pm3)$	8

但し，上の表における符号 $\pm$ はどのような組み合わせをとってもよい (複号任意)．

演習問題 1. $11 \leq n \leq 100$ を満たす整数 n に対して，$x^2+y^2=n$ を満たす整数の組 (x, y) とその個数 $S(n)$ を求めよ．

演習問題 2. $x^2+y^2=1000$ を満たす整数の組 (x, y) とその個数 $S(1000)$ を求めよ．

$S(n)$ はどのような性質を満たすだろうか．まず，2 つの性質を示す．

命題 1. $S(n)$ は常に 4 の倍数である．

証明. 座標平面から原点を除いた領域を次のように 4 つに分ける．

A_0 : 第 1 象限に y 軸の正の部分を付け加えた領域,

A_1 : 第 2 象限に x 軸の負の部分を付け加えた領域,

A_2 : 第 3 象限に y 軸の負の部分を付け加えた領域,

A_3 : 第 4 象限に x 軸の正の部分を付け加えた領域.

このとき，円 $x^2+y^2=n$ 上の格子点のうち領域 A_j 内にあるものは領域 A_0 内にあるこの円上の格子点を原点の周りに $(90\times j)$ 度回転させることにより得られる．従って

$$S(n)=4\times(A_0\text{ 内にある円上の格子点の個数})$$

となるので，$S(n)$ は 4 の倍数である． □

注 2. A_0, A_1, A_2, A_3 を原点の周りに -45 度回転させて得られる領域を B_0, B_1, B_2, B_3 とおくとき，上の議論は A_j を B_j におきかえてもそのまま成り立つ．特に

$$S(n)=4\times(B_0\text{ 内にある円上の格子点の個数})$$

である．

命題 3. n が 4 で割って 3 余るとき，$S(n)=0$ である．

証明. $S(n)>0$ であるときに，n を 4 で割った余りが 3 でないことを示せばよい．$S(n)>0$ より，$x^2+y^2=n$ を満たす整数 x, y がある．

一般に整数 z に対して，z が偶数ならば $z=2z'$ (z' は整数) と書けるので $z^2=(2z')^2=4z'^2$ は 4 で割り切れ，また，z が奇数ならば $z=2z'+1$ (z' は整数) と書けるので，$z^2=(2z'+1)^2=4(z'^2+z')+1$ は 4 で割って 1 余る整数となる．

このことから，x, y がともに偶数のときは n は 4 で割り切れ，x, y の一方が奇数，他方が偶数のときは n は 4 で割って 1 余り，x, y が共に奇数のときは n は 4 で割って 2 余ることがわかる．以上で題意が証明された． □

なお，n を 4 で割った余りが $0, 1, 2$ のときは，$S(n)=0$ になることも $S(n)>0$ になることもある．

3 素数のとき

n が素数 p であるときに $S(p)$ がどうなるかを考える．

演習問題 3. $2\le p\le 100$ を満たす素数 p に対する $S(p)$ の表を作れ．

$S(2)=4$ であり，また，命題 3 より p が 4 で割って 3 余る素数のとき $S(p)=0$ である．ここでは次の定理を示す．

定理 4 (フェルマーの二平方和定理)**.** p が 4 で割って 1 余る素数のとき，$x^2+y^2=p$ を満たす整数の組 (x, y) が存在する．従って $S(p)>0$ である．

証明. この定理の短い証明として有名な Zagier の一文証明 [1] を紹介する．原文は次の通りである：

The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 \mid x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & (\text{if } x < y - z) \\ (2y - x, y, x - y + z) & (\text{if } y - z < x < 2y) \\ (x - 2y, x - y + z, y) & (\text{if } x > 2y) \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point.

以下，この証明をもう少し詳しく述べる．

$$S = \{(x, y, z) \mid x, y, z \text{ は正の整数}, x^2 + 4yz = p\}$$

とおく．これは座標空間内の有限個の点からなる．S の点 (x, y, z) に対して，S の点 $f(x, y, z)$ を

$$f(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) & (\text{if } x < y - z) \\ (2y - x, y, x - y + z) & (\text{if } y - z < x < 2y) \\ (x - 2y, x - y + z, y) & (\text{if } x > 2y) \end{cases}$$

と定義する．(右辺の場合分けが全ての場合をつくしていること，右辺が実際に S に入っていることを確かめる必要がある．) このとき，f を 2 回ほどこすと元の点に戻ることが確かめられる．そして，$f(x, y, z) = (x, y, z)$ を満たす点 (x, y, z) は $(1, 1, \frac{p-1}{4})$ のみである．すると，S は奇数個の点からなることがわかる．一方，S の点 (x, y, z) に対して，S の点 $g(x, y, z)$ を $g(x, y, z) = (x, z, y)$ と定義する．(この右辺が S に入っていることはすぐにわかる.) g を 2 回ほどこすとやはり元の点に戻る．よって，もし $g(x, y, z) = (x, y, z)$ を満たす点がないとすると，S は偶数個の点からなることになり，これは矛盾である．従って，$g(x, y, z) = (x, y, z)$，つまり $y = z$ を満たす S の点がある．このとき $x^2 + (2y)^2 = p$ となる． □

演習問題 4. 上の証明における細かな議論を埋めて，詳細を書いてみよ．

上の定理は $S(p)$ に関する重要な結果であるが，まだ $S(n)$ を求めるには不充分である．次節以降で，ガウス整数を考えることにより，問題 2 の解答を与える．

4 複素数平面とガウス整数

$a^2 = -1$ となる実数 a は存在しない．そこで，$i^2 = -1$ を満たす「数」i を導入し，$\alpha = a + bi$ $(a, b$ は実数$)$ という形の新しい「数」を考える．これを複素数という．a を α の実部，b を α の虚部という．実数 a は $a + 0i$ と考えることにより，複素数であるとみなせる．つまり，複素数は，実数を真に含む数の体系をなす.

複素数 $\alpha = a + bi, \beta = c + di$ に対して，その和，差，積を

$$\alpha \pm \beta = (a \pm c) + (b \pm d)i,$$

$$\alpha\beta = (a+bi)(c+di) = (ac-bd)+(ad+bc)i,$$

と定め，$\beta \neq 0$(つまり $(c,d) \neq (0,0)$) のときに商を

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i$$

と定める．

複素数 $\alpha = a+bi$ の複素共役を $\overline{\alpha} = a-bi$ と定める．このとき，

$$\overline{\alpha \pm \beta} = \overline{\alpha} \pm \overline{\beta}, \quad \overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}, \quad \overline{\left(\frac{\alpha}{\beta}\right)} = \frac{\overline{\alpha}}{\overline{\beta}}, \quad \overline{\overline{\alpha}} = \alpha$$

となることが確かめられる．

また，複素数 $\alpha = a+bi$ のノルムを

$$\mathrm{N}(\alpha) = \alpha\overline{\alpha} = a^2+b^2$$

と定める．このとき，複素数 α, β に対して

$$\mathrm{N}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = \mathrm{N}(\alpha)\mathrm{N}(\beta), \quad \mathrm{N}(\overline{\alpha}) = \overline{\alpha}\,\overline{\overline{\alpha}} = \overline{\alpha}\alpha = \mathrm{N}(\alpha)$$

が成り立つ．

座標平面内の点 (x,y) に対して複素数 $x+yi$ を対応させることにより，座標平面内の点全体を複素数全体と同一視することができる．このように，複素数を用いて表した平面のことを複素数平面という．複素数平面においては，複素数 α, β に対して，$\mathrm{N}(\alpha-\beta)$ は α と β の距離の 2 乗になる．特に，円 $x^2+y^2=n$ は $N(z)=n$ (但し $z=x+iy$) と書ける．また，複素数 $x+yi$ に対して $i(x+yi) = -y+xi$ であり，点 $(-y,x)$ は点 (x,y) を原点の周りに 90 度回転させることにより得られる点なので，複素数を i 倍することは，複素数平面において原点の周りに 90 度回転させることに対応することがわかる．同様に，-1 倍，$-i$ 倍することは，原点の周りの 180 度回転，270 度回転に対応する．

整数 a, b により $\alpha = a+bi$ の形に書ける複素数のことをガウス整数という．整数 a は $a+0i$ と考えることによりガウス整数であると見なせるので，ガウス整数は整数を真に含む数の体系をなす．整数のときと同じように，ガウス整数は和，差，積で閉じているが，商では閉じていない．また，0 でないガウス整数 $\alpha = a+bi$ に対して，$\mathrm{N}(\alpha) = a^2+b^2$ は正の整数となる．

複素数平面においては，ガウス整数は格子点に対応する．従って，問題 2 は次のように言い換えることができる．

問題 3. n を正の整数とするとき，$N(\alpha) = n$ を満たすガウス整数 α の個数 $S(n)$ はいくつか？

5　ガウス整数の整数論

まず，通常の整数の性質について復習する．

定義 5. 単数とは，0 でない整数 a で，$\dfrac{1}{a}$ も整数であるようなもののこと．

つまり，単数とは ± 1 のことである．任意の 0 でない整数は，適当に単数をかけることにより正の整数にできる．

定義 6. 素数とは，単数でない正の整数 p で，$p = ab\,(a, b$ は整数$)$ と書けるならば a または b が単数になる，という性質を満たすもののこと．

例えば，$2, 3, 5, \ldots$ は素数である．このとき，次が成り立つ．

定理 7 (素因数分解とその一意性)**.** 任意の 0 でない整数 n は

$$n = \epsilon p_1 p_2 \ldots p_m \quad (\epsilon \text{ は単数}，p_1, \ldots, p_m \text{ は素数})$$

の形に書ける (素因数分解)．また，この書き方は，$p_1, \ldots, p_m$ の並べかえを除いて一意的である．

以上の性質のガウス整数における類似を考える．以下，ガウス整数における性質は「ガウス〜」と呼ぶことにする．

定義 8. ガウス単数とは，0 でないガウス整数 α で，$\dfrac{1}{\alpha}$ もガウス整数であるようなもののこと．

命題 9. ガウス整数 α に対して，α がガウス単数 $\iff \mathrm{N}(\alpha) = 1 \iff \alpha = \pm 1, \pm i.$

証明. α がガウス単数ならば $\mathrm{N}(\alpha)\mathrm{N}(\frac{1}{\alpha}) = \mathrm{N}(1) = 1$ で，また $\mathrm{N}(\alpha), \mathrm{N}(\frac{1}{\alpha})$ は正の整数なので $\mathrm{N}(\alpha) = 1$ となる．これが成り立つとき，$\alpha = a + bi$ とおくと a, b は整数で $a^2 + b^2 = 1$ なので，$(a, b) = (\pm 1, 0), (0, \pm 1)$，つまり $\alpha = \pm 1, \pm i$ となる．最後に，$\pm 1, \pm i$ がガウス単数であることは容易にわかる．　□

複素数平面において $B_0 := \{z = x + iy \,|\, x > 0, -x < y \leq x\}$ とおく．これは注 2 における領域 B_0 を複素数平面で表したものに他ならない．$i, -1, -i$ をかけることが原点の周りの 90 度，180 度，270 度の回転であったことを思い出すと，次がわかる：任意の 0 でないガウス整数は，適当にガウス単数をかけることにより，B_0 内の点に移すことができる．そこで次の定義をする．

定義 10. ガウス素数とは，ガウス単数でない B_0 内のガウス整数 σ で，$\sigma = \alpha\beta\,(\alpha, \beta$ はガウス整数$)$ と書けるならば α または β がガウス単数になる，という性質を満たすもののこと．

注 11. 多くの本などでは「B_0 内の」という条件をつけずに定義しているが，ここでは，整数のときの話と平行に進めるため，この条件をつけた．

ガウス整数においても，素因数分解とその一意性が次の形で成り立つ：

定理 12 (ガウス素因数分解とその一意性)**.** 任意の 0 でないガウス整数 α は

$$\alpha = \epsilon\sigma_1\sigma_2\dots\sigma_m \quad (\epsilon \text{ はガウス単数，} \sigma_1,\dots,\sigma_m \text{ はガウス素数})$$

の形に書ける (ガウス素因数分解)．また，この書き方は，$\sigma_1,\dots,\sigma_m$ の並べかえを除いて一意的である．

定理 12 の証明は難しいので，最後に付録で述べる．後でゆっくり読んでほしい．
ガウス素数にはどのようなものがあるだろうか？

定理 13. 素数 p のガウス素因数分解は次の通りである．
(1) $p = 2$ のとき，$2 = (-i)(1+i)^2$.
(2) p が 4 で割って 1 余る素数のとき，あるガウス素数 $\sigma = a + bi\,(a > b > 0)$ で $p = \sigma\overline{\sigma}$ となるものがあり，これがガウス素因数分解となる．
(3) p が 4 で割って 3 余る素数のとき，p 自身がガウス素数となる．
また，任意のガウス素数は，上の (1), (2), (3) のガウス素因数分解に現れるもののいずれかになる．

証明. 一般に，$\mathrm{N}(\alpha)$ が素数であるガウス整数 α はガウス素数であることに注意する：実際，$\alpha = \beta\gamma$ とガウス整数の積で書けたとすると，$\mathrm{N}(\alpha) = \mathrm{N}(\beta)\mathrm{N}(\gamma)$ で $\mathrm{N}(\beta), \mathrm{N}(\gamma)$ は正の整数なので $\mathrm{N}(\beta), \mathrm{N}(\gamma)$ のいずれかは 1 であり，従って β, γ のいずれかはガウス単数になる．

定理の証明を始める．(1) の等式は容易に確かめられる．また，$\mathrm{N}(1+i) = 2$ なので $1+i$ はガウス素数であるから，(1) の等式は 2 のガウス素因数分解を与える．

次に，p を 4 で割って 1 余る素数とするとき，定理 4 より $a^2 + b^2 = p, a > b > 0$ となる整数の組 (a, b) がある．$\sigma = a + bi$ とおくと $\mathrm{N}(\sigma) = \mathrm{N}(\overline{\sigma}) = \sigma\overline{\sigma} = p$ となる．よって $\sigma, \overline{\sigma}$ はガウス素数であり，(2) の等式が p のガウス素因数分解を与えることがわかる．

また，p を 4 で割って 3 余る素数とするとき，命題 3 より $a^2 + b^2 = p$ となる整数の組 (a, b) は存在しない．よって $\mathrm{N}(\alpha) = p$ となるガウス整数 α はない．p が $p = \alpha\beta$ とガウス整数の積で書けたとすると，$p^2 = \mathrm{N}(\alpha)\mathrm{N}(\beta)$ と書けるが，$\mathrm{N}(\alpha)$ は p^2 の約数で p ではないので 1 または p^2 であり，$\mathrm{N}(\alpha) = p^2$ ならば $\mathrm{N}(\beta) = 1$ となる．よって $\mathrm{N}(\alpha), \mathrm{N}(\beta)$ のいずれかは 1 であり，従って α, β のいずれかはガウス単数になる．従って p はガウス素数である．

次に，ガウス素数が (1), (2), (3) のガウス素因数分解に現れるもののみであることを示す．σ をガウス素数とし，

$$\sigma\overline{\sigma} = \mathrm{N}(\sigma) = \epsilon p_1 p_2 \cdots p_m$$

と書く．但し，右辺は整数 $\mathrm{N}(\sigma)$ の素因数分解である．各 p_i のガウス素因数分解たちの積 (但しガウス単数の積は 1 つにまとめたもの) が $\mathrm{N}(\sigma)$ のガウス素因数分解となるので，ガウス素因数分解の一意性より，σ はある素数 p_i のガウス素因数分解に現れる．それは (1), (2), (3) のガウス素因数分解のいずれかに現れるものとなる． □

6　円上の格子点：解答

問題 3 の解答を与える．

定理 14. $\mathrm{N}(\alpha)=n$ となるガウス整数 α の個数 $S(n)$ は以下の通りである：

$$n=2^d p_1^{e_1}\cdots p_k^{e_k} q_1^{f_1}\cdots q_l^{f_l}$$

(d は 0 以上の整数, e_j, f_j は 1 以上の整数，p_j は 4 で割って 1 余る素数，q_j は 4 で割って 3 余る素数) を n の素因数分解とするとき，$f_1,\ldots,f_l$ のうちのいずれかが奇数であれば $S(n)=0$ である．$f_1,\ldots,f_l$ が全て偶数であれば $S(n)=4(e_1+1)\cdots(e_k+1)$ である．

証明. ガウス素数のノルムは，定理 13 の場合分けに対応して
(1)　2,
(2)　4 で割って 1 余る素数,
(3)　4 で割って 3 余る素数の 2 乗
いずれかであり，α のノルムはそのガウス素因数分解に現れるガウス素数のノルムの積なので，α のノルムは上の (1), (2), (3) に現れる整数の積となる．それが n となるような α を求める．

$f_1,\ldots,f_l$ のうちのいずれかが奇数のときは，上の (1), (2), (3) に現れる整数の積が n にならないので，$\mathrm{N}(\alpha)=n$ となるガウス整数 α は存在しない．

$f_1,\ldots,f_l$ が全て偶数のときは，$\mathrm{N}(\sigma_j)=p_j$ となるガウス素数 $\sigma_j=a_j+b_j i\,(a_j>b_j>0)$ をとると，$\mathrm{N}(\alpha)=n$ となるガウス整数 α は

$$\alpha=\epsilon(1+i)^d\sigma_1^{e_{11}}\overline{\sigma_1}^{e_{12}}\cdots\sigma_k^{e_{k1}}\overline{\sigma_k}^{e_{k2}}q_1^{f_1/2}\cdots q_l^{f_l/2}$$

(但し ϵ はガウス単数，e_{j1}, e_{j2} は $e_{j1}+e_{j2}=e_j$ を満たす 0 以上の整数) という形になる．ϵ の取りかたは 4 通り，(e_{j1}, e_{j2}) の取りかたは (e_j+1) 通りあるので，求める α の個数は $4(e_1+1)\cdots(e_k+1)$ となる．　□

例 15. $n=1000=2^3 5^3$ のとき，$S(n)=4(3+1)=16$ となる．$5=(2+i)(2-i)$ なので，$\mathrm{N}(\alpha)=1000$ となるガウス整数 α は

$$\alpha=\epsilon(1+i)^3(2+i)^{e_1}(2-i)^{e_2}$$

(ϵ はガウス単数，e_1, e_2 は $e_1+e_2=3$ を満たす 0 以上の整数) という形をしている．$\epsilon=1, (e_1,e_2)=(3,0)$ のとき

$$\alpha=(1+i)^3(2+i)^3=(1+3i-3-i)(8+12i-6-i)=(-2+2i)(2+11i)=-26-18i,$$

$\epsilon=1, (e_1,e_2)=(2,1)$ のとき

$$\alpha=(1+i)^3(2+i)^2(2-i)=(-2+2i)(2+i)5=(-6+2i)5=-30+10i$$

である．他の 14 通りは上の 2 つから実部と虚部の入れかえや実部または虚部の符号の変更を適宜繰り返すことにより得られる．つまり，$\mathrm{N}(\alpha)=1000$ となるガウス整数 α は

$$\pm 26\pm 18i,\quad \pm 18\pm 26i,\quad \pm 30\pm 10i,\quad \pm 10\pm 30i$$

となる．

7　付録：ガウス素因数分解とその一意性

この節では定理 12 を証明する．

命題 16. α をガウス整数，β を 0 でないガウス整数とするとき，$\alpha = \beta\gamma + \delta$, $\mathrm{N}(\delta) < \mathrm{N}(\beta)$ を満たすガウス整数 γ, δ が存在する．

証明. 複素数 $\dfrac{\alpha}{\beta}$ に最も近いガウス整数 (の 1 つ) を γ とすると，$\dfrac{\alpha}{\beta}$ と γ の距離は $\dfrac{1}{\sqrt{2}}$ 以下なので，$\mathrm{N}\left(\dfrac{\alpha}{\beta} - \gamma\right) \leq \dfrac{1}{2} < 1$ である．従って $\mathrm{N}(\alpha - \beta\gamma) = \mathrm{N}\left(\dfrac{\alpha}{\beta} - \gamma\right)\mathrm{N}(\beta) < \mathrm{N}(\beta)$. よって $\delta = \alpha - \beta\gamma$ とおけばよい. □

ガウス整数 α, β に対して $\alpha = \beta\gamma$ を満たすガウス整数 γ が存在するとき，α は β の倍数，β は α の約数であるという．

命題 17. ガウス整数 α, β に対して $\gamma = \alpha'\alpha + \beta'\beta$　(α', β' はガウス整数) の形のガウス整数 γ で，α, β の両方の約数となるものがある．

証明. $\alpha'\alpha + \beta'\beta$ (α', β' はガウス整数) の形の 0 でないガウス整数 γ を，ノルムが最小になるようにとる．$\alpha = \gamma\gamma' + \delta, \mathrm{N}(\delta) < \mathrm{N}(\gamma)$ を満たすガウス整数 γ', δ をとると，

$$\delta = \alpha - \gamma\gamma' = \alpha - (\alpha'\alpha + \beta'\beta)\gamma' = (1 - \gamma'\alpha')\alpha - \gamma'\beta'\beta$$

となる．よって，γ の取りかた (ノルムの最小性) より $\delta = 0$ となる．すると $\alpha = \gamma\gamma'$ となるので，γ は α の約数となる．同様にして，γ が β の約数になることも言える． □

命題 18. σ をガウス素数, α, β がガウス整数で σ が $\alpha\beta$ の約数であるとき，σ は α, β の少なくとも一方の約数となる．

証明. $\epsilon = \gamma\alpha + \delta\sigma$ (γ, δ はガウス整数) を 0 でないガウス整数で α, σ 両方の約数となるものとする．すると，$\sigma = \epsilon\epsilon'$ という形に書け，σ はガウス素数なので ϵ, ϵ' のいずれかはガウス単数である．

ϵ がガウス単数のとき

$$\epsilon\beta = \gamma\alpha\beta + \delta\beta\sigma$$

となり，σ が $\alpha\beta$ の約数であることから右辺は σ を約数とする．従って，$\beta = \epsilon^{-1}\epsilon\beta$ も σ を約数とする．

ϵ' がガウス単数のとき，$\epsilon = \epsilon'^{-1}\sigma$ で ϵ が α の約数なので，σ は α の約数となる． □

定理 12 の証明. 0 でないガウス整数 α がガウス素因数分解できることを $\mathrm{N}(\alpha)$ に関する数学的帰納法で示す．$\mathrm{N}(\alpha) = 1$ のときは α はガウス単数なので，ガウス素因数分解できる．(現れるガウス素数の個数は 0 個である.) $\mathrm{N}(\alpha) > 1$ の場合，もし $\alpha = \beta\gamma$ で，β, γ がガウス単数でないように書けないならば，α は (ガウス単数) × (ガウス素数) の形になるので，ガウス素因数分解できる．$\alpha = \beta\gamma$ で，β, γ がガウス単数でないように書けるなら

ば，$\mathrm{N}(\beta), \mathrm{N}(\gamma) < \mathrm{N}(\alpha)$ となるので，数学的帰納法の仮定より，β, γ はガウス素因数分解できる．よって，その積である α もガウス素因数分解できることがわかる．

次に，0 でないガウス整数 α が

$$\alpha = \epsilon\sigma_1 \cdots \sigma_m = \epsilon'\sigma'_1 \cdots \sigma'_{m'}$$

と 2 通りのガウス素因数分解を持つとする．$m \leq m'$ だとしてよい．このとき，現れるガウス素数の並べ替えを除いて両者が一致することを m に関する数学的帰納法で示す．$m = 0$ のときは，α はガウス単数なので $\mathrm{N}(\alpha) = 1$ であり，よって $m' = 0$, $\alpha = \epsilon = \epsilon'$ となるので題意は成り立つ．$m > 0$ のとき，σ_1 は ${\epsilon'}^{-1}\alpha = \sigma'_1 \cdots \sigma'_{m'}$ の約数である．命題 18 を繰り返し使うことにより，σ_1 はある σ'_i の約数になることがわかる．$\sigma'_1, \ldots, \sigma'_{m'}$ を並べ替えることにより，σ_1 は σ'_1 の約数であるとしてよい．このとき $\sigma'_1 = \sigma_1\beta$ の形に書けるが，σ'_1 はガウス素数で，σ_1 はガウス単数でないので，β はガウス単数，つまり $\pm 1, \pm i$ のいずれかになる．すると，σ_1, σ'_1 がともに B_0 内にあることから，$\beta = 1, \sigma_1 = \sigma'_1$ となることがわかる．従って，

$$\alpha/\sigma_1 = \epsilon\sigma_2 \cdots \sigma_m = \epsilon'\sigma'_2 \cdots \sigma'_{m'}$$

となる．この等式に数学的帰納法を用いることにより，α/σ_1 の 2 通りのガウス素因数分解が，現れるガウス素数の並べ替えを除いて一致することが言える．従って，α の 2 通りのガウス素因数分解についても同じことが言える． □

参考文献

[1] D. Zagier, A one-sentence proof that every prime $p \equiv 1(\mod 4)$ is a sum of two squares, The American Mathematical Monthly, Vol. 97, No. 2 (Feb., 1990), p. 144.