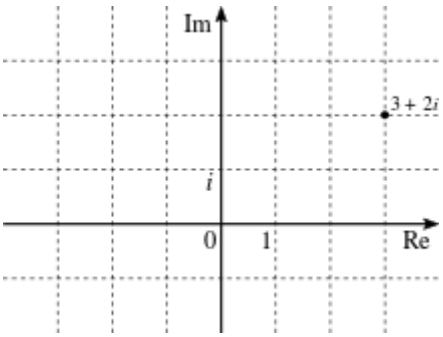
Gaussian integer

In number theory, a **Gaussian integer** is a complex number whose real and imaginary parts are both integers. The Gaussian integers, with ordinary addition and multiplication of complex numbers, form an integral domain, usually written as $\mathbf{Z}[i]$.[1] This integral domain is a particular case of a commutative ring of quadratic integers. It does not have a total ordering that respects arithmetic.

Contents

- **Basic definitions**
- **Euclidean division**
- **Principal ideals**
- **Gaussian primes**
- **Unique factorization**
- **Gaussian rationals**
- **Greatest common divisor**
- **Congruences and residue classes**
  - Examples
  - Describing residue classes
  - Residue class fields
- **Primitive residue class group and Euler's totient function**
- **Historical background**
- **Unsolved problems**
- **See also**
- **Notes**
- **References**
- **External links**



Gaussian integers as lattice points in the complex plane

Basic definitions

The Gaussian integers are the set[1]

$$\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}, \qquad \text{where } i^2 = -1.$$

In other words, a Gaussian integer is a complex number such that its real and imaginary parts are both integers. Since the Gaussian integers are closed under addition and multiplication, they form a commutative ring, which is a subring of the field of complex numbers. It is thus an integral domain.

When considered within the complex plane, the Gaussian integers constitute the 2-dimensional integer lattice.

The *conjugate* of a Gaussian integer $a + bi$ is the Gaussian integer $a - bi$.

The *norm* of a Gaussian integer is its product with its conjugate.

$$N(a+bi) = (a+bi)(a-bi) = a^2 + b^2.$$

The norm of a Gaussian integer is thus the square of its absolute value as a complex number. The norm of a Gaussian integer is a nonnegative integer, which is a sum of two squares. Thus a norm cannot be of the form $4k + 3$, with k integer.

The norm is multiplicative, that is, one has[2]

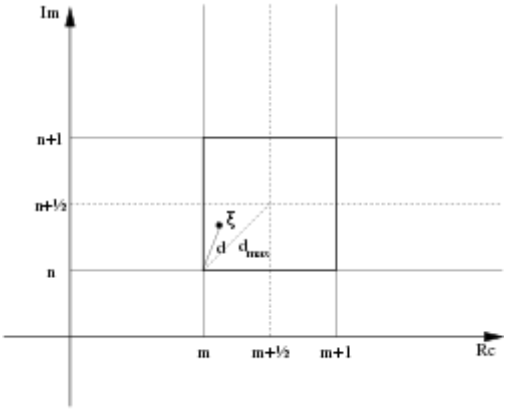
$$N(zw) = N(z)N(w),$$

for every pair of Gaussian integers z, w. This can be shown directly, or by using the multiplicative property of the modulus of complex numbers.

The units of the ring of Gaussian integers (that is the Gaussian integers whose multiplicative inverse is also a Gaussian integer) are precisely the Gaussian integers with norm 1, that is, 1, –1, i and $-i$.[3]

Euclidean division

Gaussian integers have a Euclidean division (division with remainder) similar to that of integers and polynomials. This makes the Gaussian integers a Euclidean domain, and implies that Gaussian integers share with integers and polynomials many important properties such as the existence of a Euclidean algorithm for computing greatest common divisors, Bézout's identity, the principal ideal property, Euclid's lemma, the unique factorization theorem, and the Chinese remainder theorem, all of which can be proved using only Euclidean division.



Visualization of maximal distance to some Gaussian integer

A Euclidean division algorithm takes, in the ring of Gaussian integers, a dividend a and divisor $b \neq 0$, and produces a quotient q and remainder r such that

$$a = bq + r \quad \text{and} \quad N(r) < N(b).$$

In fact, one may make the remainder smaller:

$$a = bq + r \quad \text{and} \quad N(r) \leq \frac{N(b)}{2}.$$

Even with this better inequality, the quotient and the remainder are not necessarily unique, but one may refine the choice to ensure uniqueness.

To prove this, one may consider the complex number quotient $x + iy = \frac{a}{b}$. There are unique integers m and n such that $-\frac{1}{2} < x - m \leq \frac{1}{2}$ and $-\frac{1}{2} < y - n \leq \frac{1}{2}$, and thus $N(x - m + i(y - n)) \leq \frac{1}{2}$. Taking $q = m + in$, one has

$$a = bq + r,$$

with

$$r = b\big(x - m + i(y - n)\big),$$

and

$$N(r) \leq \frac{N(b)}{2}.$$

The choice of $x - m$ and $y - n$ in a semi-open interval is required for uniqueness. This definition of Euclidean division may be interpreted geometrically in the complex plane (see the figure), by remarking that the distance from a complex number ξ to the closest Gaussian integer is at most $\frac{\sqrt{2}}{2}$.[4]

Principal ideals

Since the ring G of Gaussian integers is a Euclidean domain, G is a principal ideal domain, which means that every ideal of G is principal. Explicitly, an ideal I is a subset of a ring R such that every sum of elements of I and every product of an element of I by an element of R belong to I. An ideal is principal, if it consists of all multiples of a single element g, that is, it has the form

$$\{gx \mid x \in G\}.$$

In this case, one says that the ideal is *generated* by g or that g is a *generator* of the ideal.

Every ideal I in the ring of the Gaussian integers is principal, because, if one chooses in I a nonzero element g of minimal norm, for every element x of I, the remainder of Euclidean division of x by g belongs also to I and has a norm that is smaller than that of g; because of the choice of g, this norm is zero, and thus the remainder is also zero. That is, one has $x = qg$, where q is the quotient.

For any g, the ideal generated by g is also generated by any *associate* of g, that is, g, gi, $-g$, $-gi$; no other element generates the same ideal. As all the generators of an ideal have the same norm, the *norm of an ideal* is the norm of any of its generators.

In some circumstances, it is useful to choose, once for all, a generator for each ideal. There are two classical ways for doing that, both considering first the ideals of odd norm. If the $g = a + bi$ has an odd norm $a^2 + b^2$, then one of a and b is odd, and the other is even. Thus g has exactly one associate with a real part a that is odd and positive. In his original paper, Gauss made another choice, by choosing the unique associate such that the remainder of its division by $2 + 2i$ is one. In fact, as $N(2 + 2i) = 8$, the norm of the remainder is not greater than 4. As this norm is odd, and 3 is not the norm of a Gaussian integer, the norm of the remainder is one, that is, the remainder is a unit. Multiplying g by the inverse of this unit, one finds an associate that has one as a remainder, when divided by $2 + 2i$.

If the norm of g is even, then either $g = 2^k h$ or $g = 2^k h(1 + i)$, where k is a positive integer, and $N(h)$ is odd. Thus, one chooses the associate of g for getting a h which fits the choice of the associates for elements of odd norm.

Gaussian primes

As the Gaussian integers form a principal ideal domain they form also a unique factorization domain. This implies that a Gaussian integer is irreducible (that is, it is not the product of two non-units) if and only if it is prime (that is, it generates a prime ideal).

The prime elements of $\mathbf{Z}[i]$ are also known as **Gaussian primes**. An associate of a Gaussian prime is also a Gaussian prime. The conjugate of a Gaussian prime is also a Gaussian prime (this implies that Gaussian primes are symmetric about the real and imaginary axes).

A positive integer is a Gaussian prime if and only if it is a prime number that is congruent to 3 modulo 4 (that is, it may be written $4n + 3$, with n a nonnegative integer) (sequence A002145 in the OEIS). The other prime numbers are not Gaussian primes, but each is the product of two conjugate Gaussian primes.

A Gaussian integer $a + bi$ is a Gaussian prime if and only if either:

- one of a, b is zero and the absolute value of the other is a prime number of the form $4n + 3$ (with n a nonnegative integer), or
- both are nonzero and $a^2 + b^2$ is a prime number (which will *not* be of the form $4n + 3$).

In other words, a Gaussian integer is a Gaussian prime if and only if either its norm is a prime number, or it is the product of a unit ($\pm 1, \pm i$) and a prime number of the form $4n + 3$.

It follows that there are three cases for the factorization of a prime number p in the Gaussian integers:

- If p is congruent to 3 modulo 4, then it is a Gaussian prime; in the language of algebraic number theory, p is said to be inert in the Gaussian integers.
- If p is congruent to 1 modulo 4, then it is the product of a Gaussian prime by its conjugate, both of which are non-associated Gaussian primes (neither is the product of the other by a unit); p is said to be a decomposed prime in the Gaussian integers. For example, $5 = (2 + i)(2 - i)$ and $13 = (3 + 2i)(3 - 2i)$.
- If $p = 2$, we have $2 = (1 + i)(1 - i) = i(1 - i)^2$; that is, 2 is the product of the square of a Gaussian prime by a unit; it is the unique ramified prime in the Gaussian integers.

Unique factorization

As for every unique factorization domain, every Gaussian integer may be factored as a product of a unit and Gaussian primes, and this factorization is unique up to the order of the factors, and the replacement of any prime by any of its associates (together with a corresponding change of the unit factor).

If one chooses, once for all, a fixed Gaussian prime for each equivalence class of associated primes, and if one takes only these selected primes in the factorization, then one obtains a prime factorization which is unique up to the order of the factors. With the choices described above, the resulting unique factorization has the form

$$u(1+i)^{e_0} {p_1}^{e_1} \cdots {p_k}^{e_k},$$

where u is a unit (that is, $u \in \{1, -1, i, -i\}$), e_0 and k are nonnegative integers, $e_1, \ldots, e_k$ are positive integers, and $p_1, \ldots, p_k$ are distinct Gaussian primes such that, depending on the choice of selected associates,

- either $p_k = a_k + ib_k$ with a odd and positive, and b even,
- or the remainder of the Euclidean division of p_k by $2 + 2i$ equals 1 (this is Gauss's original choice[5]).

An advantage of the second choice is that the selected associates behave well under products for Gaussian integers of odd norm. On the other hand, the selected associate for the real Gaussian primes are negative integers. For example, the factorization of 231 in the integers, and with the first choice of associates is $3 \times 7 \times 11$, while it is $(-1) \times (-3) \times (-7) \times (-11)$ with the second choice.

Gaussian rationals

The field of Gaussian rationals is the field of fractions of the ring of Gaussian integers. It consists of the complex numbers whose real and imaginary part are both rational.

The ring of Gaussian integers is the integral closure of the integers in the Gaussian rationals.

This implies that Gaussian integers are quadratic integers and that a Gaussian rational is a Gaussian integer, if and only if it is a solution of an equation

$$x^2 + cx + d = 0,$$

with c and d integers. In fact $a + bi$ is solution of the equation

$$x^2 - 2ax + a^2 + b^2,$$

and this equation has integer coefficients if and only if a and b are both integers.

Greatest common divisor

As for any unique factorization domain, a *greatest common divisor (gcd)* of two Gaussian integers a, b is a Gaussian integer d that is a common divisor of a and b, which has all common divisors of a and b as divisor. That is (where $\mid$ denotes the divisibility relation),

- $d \mid a$ and $d \mid b$, and
- $c \mid a$ and $c \mid b$ implies $c \mid d$.

Thus, *greatest* is meant relatively to the divisibility relation, and not for an ordering of the ring (for integers, both meanings of *greatest* coincide).

More technically, a greatest common divisor of a and b is a generator of the ideal generated by a and b (this characterization is valid for principal ideal domains, but not, in general, for unique factorization domains).

The greatest common divisor of two Gaussian integers is not unique, but is defined up to the multiplication by a unit. That is, given a greatest common divisor d of a and b, the greatest common divisors of a and b are $d, -d, id$, and $-id$.

There are several ways for computing a greatest common divisor of two Gaussian integers a and b. When one knows the prime factorizations of a and b,

$$a = i^k \prod_m {p_m}^{\nu_m}, \quad b = i^n \prod_m {p_m}^{\mu_m},$$

where the primes p_m are pairwise non associated, and the exponents μ_m non-associated, a greatest common divisor is

$$\prod_m {p_m}^{\lambda_m},$$

with

$$\lambda_m = \min(\nu_m, \mu_m).$$

Unfortunately, except in simple cases, the prime factorization is difficult to compute, and Euclidean algorithm leads to a much easier (and faster) computation. This algorithm consists of replacing of the input (a, b) by (b, r), where r is the remainder of the Euclidean division of a by b, and repeating this operation until getting a zero remainder, that is a pair $(d, 0)$. This process terminates, because, at each step, the norm of the second Gaussian integer decreases. The resulting d is a greatest common divisor, because (at each step) b and $r = a - bq$ have the same divisors as a and b, and thus the same greatest common divisor.

This method of computation works always, but is not as simple as for integers because Euclidean division is more complicated. Therefore, a third method is often preferred for hand-written computations. It consists in remarking that the norm $N(d)$ of the greatest common divisor of a and b is a common divisor of $N(a)$, $N(b)$, and $N(a + b)$. When the greatest common divisor D of these three integers has few factors, then it is easy to test, for common divisor, all Gaussian integers with a norm dividing D.

For example, if $a = 5 + 3i$, and $b = 2 - 8i$, one has $N(a) = 34$, $N(b) = 68$, and $N(a + b) = 74$. As the greatest common divisor of the three norms is 2, the greatest common divisor of a and b has 1 or 2 as a norm. As a gaussian integer of norm 2 is necessary associated to $1 + i$, and as $1 + i$ divides a and b, then the greatest common divisor is $1 + i$.

If b is replaced by its conjugate $b = 2 + 8i$, then the greatest common divisor of the three norms is 34, the norm of a, thus one may guess that the greatest common divisor is a, that is, that $a \mid b$. In fact, one has $2 + 8i = (5 + 3i)(1 + i)$.

Congruences and residue classes

Given a Gaussian integer z_0, called a *modulus*, two Gaussian integers z_1,z_2 are *congruent modulo* z_0, if their difference is a multiple of z_0, that is if there exists a Gaussian integer q such that $z_1 - z_2 = qz_0$. In other words, two Gaussian integers are congruent modulo z_0, if their difference belongs to the ideal generated by z_0. This is denoted as $z_1 \equiv z_2 \pmod{z_0}$.

The congruence modulo z_0 is an equivalence relation (also called a congruence relation), which defines a partition of the Gaussian integers into equivalence classes, called here congruence classes or *residue classes*. The set of the residue classes is usually denoted $\mathbf{Z}[i]/z_0\mathbf{Z}[i]$, or $\mathbf{Z}[i]/\langle z_0 \rangle$, or simply $\mathbf{Z}[i]/z_0$.

The residue class of a Gaussian integer a is the set

$$\bar{a} := \{z \in \mathbf{Z}[i] \mid z \equiv a \pmod{z_0}\}$$

of all Gaussian integers that are congruent to a. It follows that $a = b$ if and only if $a \equiv b \pmod{z_0}$.

Addition and multiplication are compatible with congruences. This means that $a_1 \equiv b_1 \pmod{z_0}$ and $a_2 \equiv b_2 \pmod{z_0}$ imply $a_1 + a_2 \equiv b_1 + b_2 \pmod{z_0}$ and $a_1 a_2 \equiv b_1 b_2 \pmod{z_0}$. This defines well-defined operations (that is independent of the choice of representatives) on the residue classes:

$$\bar{a} + \bar{b} := \overline{a+b} \quad \text{and} \quad \bar{a} \cdot \bar{b} := \overline{ab}.$$

With these operations, the residue classes form a commutative ring, the quotient ring of the Gaussian integers by the ideal generated by z_0, which is also traditionally called the *residue class ring modulo* z_0 (for more details, see Quotient ring).

Examples

- There are exactly two residue classes for the modulus $1 + i$, namely $\underline{0} = \{0, \pm 2, \pm 4, \ldots, \pm 1 \pm i, \pm 3 \pm i, \ldots\}$ (all multiples of $1 + i$), and $1 = \{\pm 1, \pm 3, \pm 5, \ldots, \pm i, \pm 2 \pm i, \ldots\}$, which form a checkerboard pattern in the complex plane. These two classes form thus a ring with two elements, which is, in fact, a field, the unique (up to an isomorphism) field with two elements, and may thus be identified with the integers modulo 2. These two classes may be considered as a generalization of the partition of integers into even and odd integers. Thus one may speak of *even* and *odd* Gaussian integers (Gauss divided further even Gaussian integers into *even*, that is divisible by 2, and *half-even*).
- For the modulus 2 there are four residue classes, namely $\overline{0}, \overline{1}, \overline{i}, \overline{1+i}$. These form a ring with four elements, in which $x = -x$ for every x. Thus this ring is not isomorphic with the ring of integers modulo 4, another ring with four elements. One has $\overline{1 + i^2} = \overline{0}$, and thus this ring is not the finite field with four elements, nor the direct product of two copies of the ring of integers modulo 2.
- For the modulus $\underline{2} + 2\mathrm{i} = (i - 1)^3$ there are eight residue classes, namely $0, \pm 1, \pm i, 1 \pm i, 2$, whereof four contain only even Gaussian integers and four contain only odd Gaussian integers.

Describing residue classes

Given a modulus z_0, all elements of a residue class have the same remainder for the Euclidean division by z_0, provided one uses the division with unique quotient and remainder, which is described above. Thus enumerating the residue classes is equivalent with enumerating the possible remainders. This can be done geometrically in the following way.

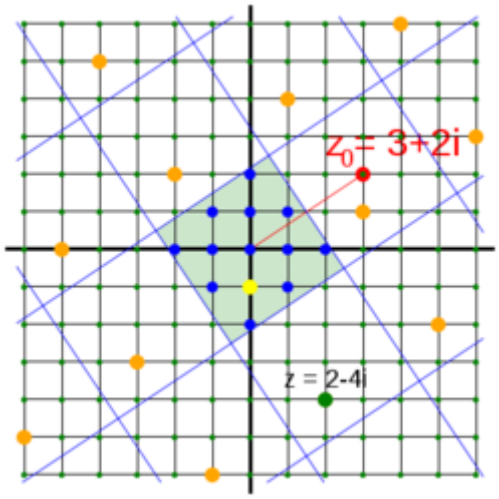
In the complex plane, one may consider a square grid, whose squares are delimited by the two lines

$$V_s = \left\{ z_0 \left(s - \tfrac{1}{2} + ix \right) \middle| \, x \in \mathbf{R} \right\} \quad \text{and}$$
$$H_t = \left\{ z_0 \left(x + i \left(t - \tfrac{1}{2} \right) \right) \middle| \, x \in \mathbf{R} \right\},$$

with s and t integers (blue lines in the figure). These divide the plane in semi-open squares (where m and n are integers)

$$Q_{mn} = \left\{ (s + it) z_0 \, \middle| \, s \in \left[m - \tfrac{1}{2}, m + \tfrac{1}{2} \right), t \in \left[n - \tfrac{1}{2}, n + \tfrac{1}{2} \right) \right\}.$$

The semi-open intervals that occur in the definition of Q_{mn} have been chosen in order that every complex number belong to exactly one square; that is, the squares Q_{mn} form a partition of the complex plane. One has



All 13 residue classes with their minimal residues (blue dots) in the square Q_{00} (light green background) for the modulus $z_0 = 3 + 2i$. One residue class with $z = 2 - 4i \equiv -i \pmod{z_0}$ is highlighted with yellow/orange dots.

$$Q_{mn} = (m + in)z_0 + Q_{00} = \{(m + in)z_0 + z \mid z \in Q_{00}\}.$$

This implies that every Gaussian integer is congruent modulo z_0 to a unique Gaussian integer in Q_{00} (the green square in the figure), which its remainder for the division by z_0. In other words, every residue class contains exactly one element in Q_{00}.

The Gaussian integers in Q_{00} (or in its boundary) are sometimes called *minimal residues* because their norm are not greater than the norm of any other Gaussian integer in the same residue class (Gauss called them *absolutely smallest residues*).

From this one can deduce by geometrical considerations, that the number of residue classes modulo a Gaussian integer $z_0 = a + bi$ equals its norm $N(z_0) = a^2 + b^2$ (see below for a proof; similarly, for integers, the number of residue classes modulo n is its absolute value $|n|$).

Proof

The relation $Q_{mn} = (m + in)z_0 + Q_{00}$ means that all Q_{mn} are obtained from Q_{00} by translating it by a Gaussian integer. This implies that all Q_{mn} have the same area $N = N(z_0)$, and contain the same number n_g of Gaussian integers.

Generally, the number of grid points (here the Gaussian integers) in an arbitrary square with the area A is $A + \Theta(\sqrt{A})$ (see Big theta for the notation). If one considers a big square consisting of $k \times k$ squares Q_{mn}, then it contains $k^2N + O(k\sqrt{N})$ grid points. It follows $k^2 n_g = k^2N + \Theta(k\sqrt{N})$, and thus $n_g = N + \Theta(\frac{\sqrt{N}}{k})$, after a division by k^2. Taking the limit when k tends to the infinity gives $n_g = N = N(z_0)$.

Residue class fields

The residue class ring modulo a Gaussian integer z_0 is a field if and only if z_0 is a Gaussian prime.

If z_0 is a decomposed prime or the ramified prime $1 + i$ (that is, if its norm $N(z_0)$ is a prime number, which is either 2 or a prime congruent to 1 modulo 4), then the residue class field has a prime number of elements (that is, $N(z_0)$). It is thus isomorphic to the field of the integers modulo $N(z_0)$.

If, on the other hand, z_0 is an inert prime (that is, $N(z_0) = p^2$ is the square of a prime number, which is congruent to 3 modulo 4), then the residue class field has p^2 elements, and it is an extension of degree 2 (unique, up to an isomorphism) of the prime field with p elements (the integers modulo p).

Primitive residue class group and Euler's totient function

Many theorems (and their proofs) for moduli of integers can be directly transferred to moduli of Gaussian integers, if one replaces the absolute value of the modulus by the norm. This holds especially for the *primitive residue class group* (also called multiplicative group of integers modulo n) and Euler's totient function. The primitive residue class group of a modulus z is defined as the subset of its residue classes, which contains all residue classes a that are coprime to z, i.e. $(a,z) = 1$. Obviously, this system builds a multiplicative group. The number of its elements shall be denoted by $\phi(z)$ (analogously to Euler's totient function $\varphi(n)$ for integers n).

For Gaussian primes it immediately follows that $\phi(p) = |p|^2 - 1$ and for arbitrary composite Gaussian integers

$$z = i^k \prod_m {p_m}^{\nu_m}$$

Euler's product formula can be derived as

$$\phi(z) = \prod_{m\,(\nu_m>0)} |{p_m}^{\nu_m}|^2 \left(1 - \frac{1}{|p_m|^2}\right) = |z|^2 \prod_{p_m|z} \left(1 - \frac{1}{|p_m|^2}\right)$$

where the product is to build over all prime divisors p_m of z (with $\nu_m > 0$). Also the important theorem of Euler can be directly transferred:

For all a with $(a,z) = 1$, it holds that $a^{\phi(z)} \equiv 1 \pmod{z}$.

Historical background

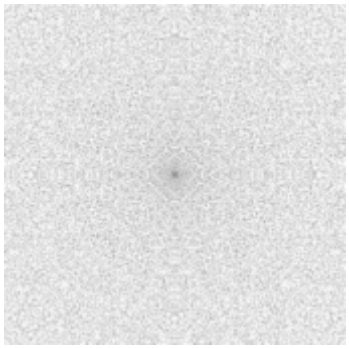
The ring of Gaussian integers was introduced by Carl Friedrich Gauss in his second monograph on quartic reciprocity (1832).[6] The theorem of quadratic reciprocity (which he had first succeeded in proving in 1796) relates the solvability of the congruence $x^2 \equiv q \pmod{p}$ to that of $x^2 \equiv p \pmod{q}$. Similarly, cubic reciprocity relates the solvability of $x^3 \equiv q \pmod{p}$ to that of $x^3 \equiv p \pmod{q}$, and biquadratic (or quartic) reciprocity is a relation between $x^4 \equiv q \pmod{p}$ and $x^4 \equiv p \pmod{q}$. Gauss discovered that the law of biquadratic reciprocity and its supplements were more easily stated and proved as statements about "whole complex numbers" (i.e. the Gaussian integers) than they are as statements about ordinary whole numbers (i.e. the integers).

In a footnote he notes that the Eisenstein integers are the natural domain for stating and proving results on cubic reciprocity and indicates that similar extensions of the integers are the appropriate domains for studying higher reciprocity laws.

This paper not only introduced the Gaussian integers and proved they are a unique factorization domain, it also introduced the terms norm, unit, primary, and associate, which are now standard in algebraic number theory.

Unsolved problems

Most of the unsolved problems are related to distribution of Gaussian primes in the plane.



The distribution of the small Gaussian primes in the complex plane

- Gauss's circle problem does not deal with the Gaussian integers per se, but instead asks for the number of lattice points inside a circle of a given radius centered at the origin. This is equivalent to determining the number of Gaussian integers with norm less than a given value.

There are also conjectures and unsolved problems about the Gaussian primes. Two of them are:

- The real and imaginary axes have the infinite set of Gaussian primes 3, 7, 11, 19, ... and their associates. Are there any other lines that have infinitely many Gaussian primes on them? In particular, are there infinitely many Gaussian primes of the form $1 + ki$?[7]
- Is it possible to walk to infinity using the Gaussian primes as stepping stones and taking steps of a uniformly bounded length? This is known as the Gaussian moat problem; it was posed in 1962 by Basil Gordon and remains unsolved.[8][9]

See also

- Algebraic integer
- Cyclotomic field
- Eisenstein integer
- Eisenstein prime
- Hurwitz quaternion
- Proofs of Fermat's theorem on sums of two squares
- Proofs of quadratic reciprocity
- Quadratic integer
- Splitting of prime ideals in Galois extensions describes the structure of prime ideals in the Gaussian integers
- Table of Gaussian integer factorizations

Notes

1. Fraleigh (1976, p. 286)
2. Fraleigh (1976, p. 289)
3. Fraleigh (1976, p. 288)

4. Fraleigh (1976, p. 287)
5. Carl Friedrich Gauss, Arithmetische Untersuchungen über höhere Arithmetik, Springer, Berlin 1889, p. 546 (in German) [1] (https://archive.org/details/carlfriedrichga00gausgoog)
6. http://www.ems-ph.org/journals/show_pdf.php?issn=0013-6018&vol=53&iss=1&rank=2
7. Ribenboim, Ch.III.4.D Ch. 6.II, Ch. 6.IV (Hardy & Littlewood's conjecture E and F)
8. Gethner, Ellen; Wagon, Stan; Wick, Brian (1998). "A stroll through the Gaussian primes". *The American Mathematical Monthly*. **105** (4): 327–337. doi:10.2307/2589708 (https://doi.org/10.2307%2F2589708). JSTOR 2589708 (https://www.jstor.org/stable/2589708). MR 1614871 (https://www.ams.org/mathscinet-getitem?mr=1614871). Zbl 0946.11002 (https://zbmath.org/?format=complete&q=an:0946.11002).
9. Guy, Richard K. (2004). *Unsolved problems in number theory* (3rd ed.). Springer-Verlag. pp. 55–57. ISBN 978-0-387-20860-2. Zbl 1058.11001 (https://zbmath.org/?format=complete&q=an:1058.11001).

References

- C. F. Gauss (1831) "Theoria residuorum biquadraticorum. Commentatio secunda." (https://babel.hathitrust.org/cgi/pt?id=mdp.39015073697180&view=1up&seq=285), *Comm. Soc. Reg. Sci. Göttingen* **7**: 89-148; reprinted in Werke, Georg Olms Verlag, Hildesheim, 1973, pp. 93–148. A German translation of this paper is available online in ″H. Maser (ed.): *Carl Friedrich Gauss' Arithmetische Untersuchungen über höhere Arithmetik. (https://archive.org/details/carlfriedrichga00gausgoog)* Springer, Berlin 1889, pp. 534″.
- Fraleigh, John B. (1976), *A First Course In Abstract Algebra* (2nd ed.), Reading: Addison-Wesley, ISBN 0-201-01984-1
- Kleiner, Israel (1998). "From Numbers to Rings: The Early History of Ring Theory" (http://www.ems-ph.org/journals/show_pdf.php?issn=0013-6018&vol=53&iss=1&rank=2). *Elem. Math*. **53** (1): 18–35. doi:10.1007/s000170050029 (https://doi.org/10.1007%2Fs000170050029). Zbl 0908.16001 (https://zbmath.org/?format=complete&q=an:0908.16001).
- Ribenboim, Paulo (1996). *The New Book of Prime Number Records* (3rd ed.). New York: Springer. ISBN 0-387-94457-5. Zbl 0856.11001 (https://zbmath.org/?format=complete&q=an:0856.11001).
- Henry G. Baker (1993). "Complex Gaussian Integers for "Gaussian Graphics" ". *ACM SIGPLAN Notices*. **28** (11): 22–27. doi:10.1145/165564.165571 (https://doi.org/10.1145%2F165564.165571). S2CID 8083226 (https://api.semanticscholar.org/CorpusID:8083226).

External links

- IMO Compendium (https://web.archive.org/web/20120306225505/http://www.imocompendium.com/index.php?options=mbb%7Ctekstkut&page=0&art=extensions_ddj%7Cf&ttn=Dushan%20D%3Bjukic1%7C%20Arithmetic%20in%20Quadratic%20Fields%7CN%2FA&knj=&p=3nbbw45001) text on quadratic extensions and Gaussian Integers in problem solving
- Keith Conrad, The Gaussian Integers (https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf).