Factoring in number rings

Peter Koymans
Universiteit Leiden

This Week's Discoveries

Leiden, Nederland, May 2019

Basic arithmetic

The fundamental theorem of arithmetic, which dates back to Euclid, states that every positive integer can uniquely be factored into primes.

Basic arithmetic

The fundamental theorem of arithmetic, which dates back to Euclid, states that every positive integer can uniquely be factored into primes.

This talk we will consider factorization properties of more general mathematical structures that we call rings.

Basic arithmetic

The fundamental theorem of arithmetic, which dates back to Euclid, states that every positive integer can uniquely be factored into primes.

This talk we will consider factorization properties of more general mathematical structures that we call rings.

A ring is a set where one can add, subtract and multiply the elements.

Basic arithmetic

The fundamental theorem of arithmetic, which dates back to Euclid, states that every positive integer can uniquely be factored into primes.

This talk we will consider factorization properties of more general mathematical structures that we call rings.

A ring is a set where one can add, subtract and multiply the elements.

Some example of rings are: the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$ and

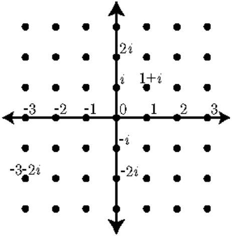
$$\left\{ \frac{a}{b} : a, b \in \mathbb{Z}, 2 \nmid b \right\}.$$

The Gaussian integers

In 1832 Gauss introduced the Gaussian integers
$\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.

The Gaussian integers

In 1832 Gauss introduced the Gaussian integers $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.



We can add Gaussian integers

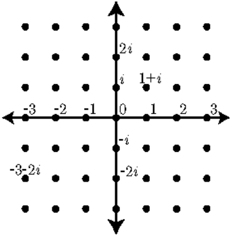
$$(1 + i) + (-3 - 2i) = -2 - i$$

and multiply Gaussian integers by expanding brackets and using the rule $i^2 = -1$

$$(2 + 5i) \cdot (3 - 4i) = 6 + 15i - 8i - 20i^2 = 26 + 7i.$$

The Gaussian integers

In 1832 Gauss introduced the Gaussian integers $\mathbb{Z}[i] := \{a + bi : a, b \in \mathbb{Z}\}$.



We can add Gaussian integers

$$(1 + i) + (-3 - 2i) = -2 - i$$

and multiply Gaussian integers by expanding brackets and using the rule $i^2 = -1$

$$(2 + 5i) \cdot (3 - 4i) = 6 + 15i - 8i - 20i^2 = 26 + 7i.$$

We will now study factorization properties of the Gaussian integers.

Units

Definition 1

If R is a ring, we say that $x \in R$ is a unit if there is $y \in R$ such that $xy = 1$.

Units

Definition 1

If R is a ring, we say that $x \in R$ is a unit if there is $y \in R$ such that $xy = 1$.

Example 1

The units of $\mathbb{Z}$ are ± 1, while the units of $\mathbb{Q}$ are $\mathbb{Q} \setminus \{0\}$.

Units

Definition 1

If R is a ring, we say that $x \in R$ is a unit if there is $y \in R$ such that $xy = 1$.

Example 1

The units of $\mathbb{Z}$ are ± 1, while the units of $\mathbb{Q}$ are $\mathbb{Q} \setminus \{0\}$.

To compute the units of $\mathbb{Z}[i]$, we define a function $N : \mathbb{Z}[i] \to \mathbb{Z}$ by

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

Units

Definition 1

If R is a ring, we say that $x \in R$ is a unit if there is $y \in R$ such that $xy = 1$.

Example 1

The units of $\mathbb{Z}$ are ± 1, while the units of $\mathbb{Q}$ are $\mathbb{Q} \setminus \{0\}$.

To compute the units of $\mathbb{Z}[i]$, we define a function $N : \mathbb{Z}[i] \to \mathbb{Z}$ by

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

If we view $\mathbb{Z}[i]$ as a subset of the complex numbers $\mathbb{C}$ we have

$$N(a + bi) = |a + bi|^2,$$

where $| \cdot |$ is the absolute value on $\mathbb{C}$. We have the fundamental property

$$N((a + bi) \cdot (c + di)) = N(a + bi) \cdot N(c + di).$$

Computing the unit group

Now suppose that $a + bi \in \mathbb{Z}[i]$ is a unit. Then, by definition, there is $c + di \in \mathbb{Z}[i]$ such that

$$(a + bi) \cdot (c + di) = 1,$$

which implies that $N(a + bi) \cdot N(c + di) = 1$.

Computing the unit group

Now suppose that $a + bi \in \mathbb{Z}[i]$ is a unit. Then, by definition, there is $c + di \in \mathbb{Z}[i]$ such that

$$(a + bi) \cdot (c + di) = 1,$$

which implies that $N(a + bi) \cdot N(c + di) = 1$.

Then we deduce $N(a + bi) = \pm 1$. But $N(a + bi) = a^2 + b^2$, so

$$a^2 + b^2 = 1 \Rightarrow (a, b) \in \{(1, 0), (0, 1), (-1, 0), (0, -1)\}.$$

Computing the unit group

Now suppose that $a + bi \in \mathbb{Z}[i]$ is a unit. Then, by definition, there is $c + di \in \mathbb{Z}[i]$ such that

$$(a + bi) \cdot (c + di) = 1,$$

which implies that $N(a + bi) \cdot N(c + di) = 1$.

Then we deduce $N(a + bi) = \pm 1$. But $N(a + bi) = a^2 + b^2$, so

$$a^2 + b^2 = 1 \Rightarrow (a, b) \in \{(1, 0), (0, 1), (-1, 0), (0, -1)\}.$$

We conclude that the units of $\mathbb{Z}[i]$ are $\{1, -1, i, -i\}$.

Primes and irreducibles

Definition 2

Let R be a ring. We say that $a \in R \setminus \{0\}$ is irreducible if it is not the product of two non-units.

Primes and irreducibles

Definition 2

Let R be a ring. We say that $a \in R \setminus \{0\}$ is irreducible if it is not the product of two non-units.

Definition 3

Let R be a ring. An element $a \in R$, that is non-zero and not a unit, is called prime if for all $b, c \in R$ we have $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Primes and irreducibles

Definition 2

Let R be a ring. We say that $a \in R \setminus \{0\}$ is irreducible if it is not the product of two non-units.

Definition 3

Let R be a ring. An element $a \in R$, that is non-zero and not a unit, is called prime if for all $b, c \in R$ we have $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Every prime element is irreducible. The converse does not hold in general.

Primes and irreducibles

Definition 2

Let R be a ring. We say that $a \in R \setminus \{0\}$ is irreducible if it is not the product of two non-units.

Definition 3

Let R be a ring. An element $a \in R$, that is non-zero and not a unit, is called prime if for all $b, c \in R$ we have $a \mid bc$ implies $a \mid b$ or $a \mid c$.

Every prime element is irreducible. The converse does not hold in general.

Example 2

For the integers, prime and irreducible are the same notion. The prime elements are exactly $\pm p$, where p is a prime number. This property is the key behind unique factorization!

Unique factorization again

If π is a prime in R and u is a unit, then $\pi \cdot u$ is prime.

Unique factorization again

If π is a prime in R and u is a unit, then $\pi \cdot u$ is prime.

Theorem 1 (Gauss)

Every non-zero Gaussian integer $a + bi$ can uniquely be factored into a unit and primes. This factorization is unique up to reordering the factors and multiplying primes by units.

Unique factorization again

If π is a prime in R and u is a unit, then $\pi \cdot u$ is prime.

Theorem 1 (Gauss)

Every non-zero Gaussian integer $a + bi$ can uniquely be factored into a unit and primes. This factorization is unique up to reordering the factors and multiplying primes by units.

Example 3

We have that

$$-3 + 9i = i \cdot 3 \cdot (1 + i) \cdot (2 - i) = 3i \cdot (-1 + i) \cdot (-1 - 2i),$$

where 3, $1 + i$ and $2 - i$ are all irreducible and prime. In fact: irreducible and prime are the same notion in $\mathbb{Z}[i]$.

Failure of unique factorization

In the ring $\mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ we have

$$6 = 2 \cdot 3 = -1 \cdot \sqrt{-6} \cdot \sqrt{-6}. \tag{1}$$

Failure of unique factorization

In the ring $\mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ we have

$$6 = 2 \cdot 3 = -1 \cdot \sqrt{-6} \cdot \sqrt{-6}. \tag{1}$$

Define $N : \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}$

$$N(a + b\sqrt{-6}) = a^2 + 6b^2.$$

Failure of unique factorization

In the ring $\mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ we have

$$6 = 2 \cdot 3 = -1 \cdot \sqrt{-6} \cdot \sqrt{-6}. \tag{1}$$

Define $N : \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}$

$$N(a + b\sqrt{-6}) = a^2 + 6b^2.$$

Once more we have the property

$$N((a + b\sqrt{-6}) \cdot (c + d\sqrt{-6})) = N(a + b\sqrt{-6}) \cdot N(c + d\sqrt{-6}).$$

Failure of unique factorization

In the ring $\mathbb{Z}[\sqrt{-6}] := \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ we have

$$6 = 2 \cdot 3 = -1 \cdot \sqrt{-6} \cdot \sqrt{-6}. \tag{1}$$

Define $N : \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z}$

$$N(a + b\sqrt{-6}) = a^2 + 6b^2.$$

Once more we have the property

$$N((a + b\sqrt{-6}) \cdot (c + d\sqrt{-6})) = N(a + b\sqrt{-6}) \cdot N(c + d\sqrt{-6}).$$

With a similar computation as for $\mathbb{Z}[i]$, it follows that the units of $\mathbb{Z}[\sqrt{-6}]$ are ± 1. We will show on the next slide that 2, 3, $\sqrt{-6}$ are irreducible. So we have two different factorizations of 6 in equation (1).

2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$

Suppose that we have

$$(a + b\sqrt{-6})(c + d\sqrt{-6}) = 2.$$

2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$

Suppose that we have

$$(a + b\sqrt{-6})(c + d\sqrt{-6}) = 2.$$

If we apply our function N we see that

$$(a^2 + 6b^2)(c^2 + 6d^2) = N(2) = 4.$$

and surely $b = d = 0$.

2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$

Suppose that we have

$$(a + b\sqrt{-6})(c + d\sqrt{-6}) = 2.$$

If we apply our function N we see that

$$(a^2 + 6b^2)(c^2 + 6d^2) = N(2) = 4.$$

and surely $b = d = 0$.

We conclude that $a^2c^2 = 4$, so $ac = \pm 2$. Then $a = \pm 1$ or $c = \pm 1$. If $a = \pm 1$, we get that $a + b\sqrt{-6} = \pm 1$ is a unit!

2 is irreducible in $\mathbb{Z}[\sqrt{-6}]$

Suppose that we have

$$(a + b\sqrt{-6})(c + d\sqrt{-6}) = 2.$$

If we apply our function N we see that

$$(a^2 + 6b^2)(c^2 + 6d^2) = N(2) = 4.$$

and surely $b = d = 0$.

We conclude that $a^2c^2 = 4$, so $ac = \pm 2$. Then $a = \pm 1$ or $c = \pm 1$. If $a = \pm 1$, we get that $a + b\sqrt{-6} = \pm 1$ is a unit!

This shows that 2 is irreducible, and similarly for 3 and $\sqrt{-6}$.

My work

For an integer d we define

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

My work

For an integer d we define

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

We have seen that unique factorization holds for $d = 1$ and $d = -1$, but not for $d = -6$.

My work

For an integer d we define

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

We have seen that unique factorization holds for $d = 1$ and $d = -1$, but not for $d = -6$.

Attached to an integer d, we can define an abelian group $\mathrm{Cl}(d)$ that measures the failure of unique factorization in $\mathbb{Z}[\sqrt{d}]$. We have

$$\mathrm{Cl}(d) = \{id\} \iff \overline{\mathbb{Z}[\sqrt{d}]} \text{ has unique factorization.}$$

My work

For an integer d we define

$$\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}.$$

We have seen that unique factorization holds for $d = 1$ and $d = -1$, but not for $d = -6$.

Attached to an integer d, we can define an abelian group $\mathrm{Cl}(d)$ that measures the failure of unique factorization in $\mathbb{Z}[\sqrt{d}]$. We have

$$\mathrm{Cl}(d) = \{id\} \iff \overline{\mathbb{Z}[\sqrt{d}]} \text{ has unique factorization.}$$

Given d there is an algorithm that computes $\mathrm{Cl}(d)$.

My work II

There are many open questions about the behavior of $\mathrm{Cl}(d)$ as d changes.

My work II

There are many open questions about the behavior of $\mathrm{Cl}(d)$ as d changes.

For example, a very famous problem going back to Gauss asks if there are infinitely many d with $\mathrm{Cl}(d) = \{id\}$, i.e. if there are infinitely many d such that $\overline{\mathbb{Z}[\sqrt{d}]}$ has unique factorization.

My work II

There are many open questions about the behavior of $\mathrm{Cl}(d)$ as d changes.

For example, a very famous problem going back to Gauss asks if there are infinitely many d with $\mathrm{Cl}(d) = \{id\}$, i.e. if there are infinitely many d such that $\overline{\mathbb{Z}[\sqrt{d}]}$ has unique factorization.

We have a solid heuristic framework to answer such questions, but we have been able to prove these only in very few instances.

My work II

There are many open questions about the behavior of $\mathrm{Cl}(d)$ as d changes.

For example, a very famous problem going back to Gauss asks if there are infinitely many d with $\mathrm{Cl}(d) = \{id\}$, i.e. if there are infinitely many d such that $\overline{\mathbb{Z}[\sqrt{d}]}$ has unique factorization.

We have a solid heuristic framework to answer such questions, but we have been able to prove these only in very few instances.

Together with Djordjo Milovic and Carlo Pagano I have been able to answer some of these questions.

Questions