Factoring in number rings

Peter Koymans
Universiteit Leiden

Nederlands Mathematisch Congres

Veldhoven, Nederland, April 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.

In abstract algebra one learns about rings, where one can add, subtract and multiply.

Basic arithmetic

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

In abstract algebra one learns about rings, where one can add, subtract and multiply.

The integers form a prototypical example of a ring, and the fundamental theorem of arithmetic describes the multiplicative structure.

Basic arithmetic

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

In abstract algebra one learns about rings, where one can add, subtract and multiply.

The integers form a prototypical example of a ring, and the fundamental theorem of arithmetic describes the multiplicative structure.

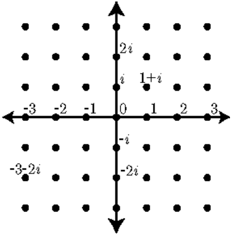
But what happens for other rings? Many applications ranging from abstract number theory and geometry to cryptography.

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

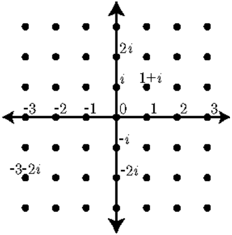
$$(1 + i) + (-3 - 2i) = -2 - i$$

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 $i^2 = -1$

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

Every Gaussian integer can uniquely be factored as a unit and Gaussian primes. The units of $\mathbb{Z}[i]$ are $\{\pm 1, \pm i\}$.

Primes and irreducibles

To study factorization in more general rings, we make a definition.

Definition 1

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

To study factorization in more general rings, we make a definition.

Definition 1

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

If R is an integral domain, then every prime element is irreducible. The converse also holds for $R = \mathbb{Z}$ and $R = \mathbb{Z}[i]$, but it does not hold in general.

Failure of unique factorization

In the ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It is not hard to see that 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible. The problem comes from the fact that 3 is irreducible but not prime.

Failure of unique factorization

In the ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It is not hard to see that 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible. The problem comes from the fact that 3 is irreducible but not prime.

We see that factorizations may no longer be unique! We say that a ring R is a number ring if it is a subring of a finite field extension of $\mathbb{Q}$.

Failure of unique factorization

In the ring $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$ we have

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

It is not hard to see that 2, 3, $1 + \sqrt{-5}$ and $1 - \sqrt{-5}$ are all irreducible. The problem comes from the fact that 3 is irreducible but not prime.

We see that factorizations may no longer be unique! We say that a ring R is a number ring if it is a subring of a finite field extension of $\mathbb{Q}$.

Theorem 1

If R is a a number ring, then every element of R can be factored into irreducible elements.

Kummer and ideals

Kummer realized around 1850 that the correct notion for factorization in number rings is that of ideals. Roughly speaking, every ideal can uniquely be factored into prime ideals.

Kummer and ideals

Kummer realized around 1850 that the correct notion for factorization in number rings is that of ideals. Roughly speaking, every ideal can uniquely be factored into prime ideals.

This led to the introduction of an abelian group called the class group, which measures the failure of unique factorization of elements.

Kummer and ideals

Kummer realized around 1850 that the correct notion for factorization in number rings is that of ideals. Roughly speaking, every ideal can uniquely be factored into prime ideals.

This led to the introduction of an abelian group called the class group, which measures the failure of unique factorization of elements.

Class groups are known to be finite, but still very mysterious. Cohen and Lenstra conjectured that class groups behave like random finite abelian groups in families of number fields.

Random finite abelian groups

How does one generate random finite abelian groups? Suppose that we want to generate a random finite abelian group A with 4 elements, say a, b, c and d.

Random finite abelian groups

How does one generate random finite abelian groups? Suppose that we want to generate a random finite abelian group A with 4 elements, say a, b, c and d.

A	a	b	c	d
a	$*$	$*$	$*$	$*$
b	$*$	$*$	$*$	$*$
c	$*$	$*$	$*$	$*$
d	$*$	$*$	$*$	$*$

Idea: generate a random addition table for A by picking a, b, c and d uniformly at random for each $*$ entry above. Discard those addition tables that do not give rise to an abelian group.

Random finite abelian groups

How does one generate random finite abelian groups? Suppose that we want to generate a random finite abelian group A with 4 elements, say a, b, c and d.

A	a	b	c	d
a	$*$	$*$	$*$	$*$
b	$*$	$*$	$*$	$*$
c	$*$	$*$	$*$	$*$
d	$*$	$*$	$*$	$*$

Idea: generate a random addition table for A by picking a, b, c and d uniformly at random for each $*$ entry above. Discard those addition tables that do not give rise to an abelian group.

Then we get the finite abelian groups of size 4 with probability proportional to $\frac{1}{|\mathrm{Aut}(A)|}$.

Current research: thin families

Only very few instances of the Cohen-Lenstra conjectures have been proven. Proving randomness of deterministic objects is extremely tricky. The following theorem builds on earlier joint work with Milovic.

Current research: thin families

Only very few instances of the Cohen-Lenstra conjectures have been proven. Proving randomness of deterministic objects is extremely tricky. The following theorem builds on earlier joint work with Milovic.

Theorem 2 (K., 2018)

The density of prime numbers p such that the class number of $\mathbb{Q}(\sqrt{-p})$ *is divisible by* 16 *is equal to* $\frac{1}{16}$.

Current research: wide families

Let l be an odd prime number. If K is a degree l cyclic field, then $\mathrm{Cl}(K)$ becomes a $\mathbb{Z}[\zeta_l]$-module in a natural way. The following theorem generalizes a result due to Smith.

Current research: wide families

Let l be an odd prime number. If K is a degree l cyclic field, then $\mathrm{Cl}(K)$ becomes a $\mathbb{Z}[\zeta_l]$-module in a natural way. The following theorem generalizes a result due to Smith.

Theorem 3 (K.-Pagano, 2018)

Assume GRH and let l be an odd prime number. Then the group $((1 - \zeta_l)\mathrm{Cl}(K))[l^\infty]$ has the distribution predicted by Cohen and Lenstra as K varies over degree l cyclic fields over $\mathbb{Q}$ ordered by discriminant.

Questions