JASB
JOURNAL OF THE ASB SOCIETY

Solving Diophantine Equations by Factoring in Number Fields

Pezlar, Zdeněk[1]*

1 *Gymnázium Brno, třída Kapitána Jaroše 14, příspěvková organizace*

About the author

Zdeněk Pezlar is a student at the třída Kaptiána Jaroše grammar school, Brno. At the moment he is mostly interested in olympiad mathematics and next to that in number theoretic properties of elliptic curves. He has so far written two projects which have both competed in the Student Professional Activities - SPA (Středoškolská odborná činnost - SOC) competition. The first one won first place in the competition, an award from the Learned Society of the Czech Republic and a special prize at the international competition EUCYS. The second project placed third at the competition and won the "České hlavičky" award. Apart from SOČ, Zdeněk has represented the Czech Republic in olympiad mathematics - he has won a bronze and a silver medal at the Middle European olympiad MEMO. In the time he does not spend with mathematics, he often plays the piano and also plays frisbee

Explanation for general audience

The article focuses on a branch of mathematics called 'algebraic number theory' and in particular its applications in elementary number theory - solving hard diophnatine equations. Let's back up a bit.

When working with integers, we often make use of either modular arithmetic or their unique factorisation into primes. The crown jewels of modular arithmetic are quadratic residues, which allow for more advanced discussions concerning divisibility over the integers. Theorems such as Euler's criterion then allow us to quickly decide when a given diophantine equation has no integer solutions - simply find a modulus under which no solutions exist. These basic methods can, however, get us only so far. Take an equation such as $x^2 + 13 = y^3$ for an example. It has an integral solution for $x = 70$, so a solution modulo every integer, and no obvious way to factor presents itself. So how do we proceed? Well, it is not entirely true, that no easy factorisation exists, over the complex numbers one is immediate: $x^2 + 13 = (x + \sqrt{(}-13))(x - \sqrt{(}-13))$. What use could that be to us, though?

Questions such as that puzzled the old masters. When attempting to solve the famous Fermat's Last Theorem - i.e showing that the equation $x^n + y^n = z^n$ has no non-trivial integral solutions for $n > 2$ - mathematicians such as Carl Friedrich Gauss, Ernst Kummer and Peter Gustav Dirichlet pioneered the field of algebraic number theory and paved the way for mathematicians in centuries to come. In particular they tried considering number theoretic of complex roots of polynomials over the integers, or rather extensions of $\mathbb{Q}$ containing these numbers. It turns out that studying the ideals in certain subrings of these number fields is the way to proceed. Indeed, it is true, that ideals uniquely decompose into prime ideals, much like ordinary integers do. This is in stark contrast with the rings themselves, which mostly do not admit unique factorisation. In what is a beautiful connection of those two concepts, we introduce the ideal class group, which neatly connects both concepts and provides the final piece of the puzzle allowing us to solve equations by factoring in fields containing, say, the square-root of -13.

JASB
JOURNAL OF THE ASB SOCIETY

Solving Diophantine Equations by Factoring in Number Fields

Pezlar, Zdeněk[1]*

1 *Gymnázium Brno, třída Kapitána Jaroše 14, příspěvková organizace*
* *Corresponding author: zdendapezlar@seznam.cz*

In this text we provide an introduction to algebraic number theory and show its applications in solving certain difficult diophantine equations. We begin with a quick summary of the theory of quadratic residues, before diving into a select few areas of algebraic number theory. Our article is accompanied by a couple of worked problems and exercises for the reader to tackle on their own.

Key words: diophantine equation, quadratic residue, number field, ideal class group, unique factorisation .
(Submitted: 15 April 2021, Accepted: 26 November 2021, Published: 27 December 2021)

1 Introduction

Finding solutions to an equation over the integers in two or more variables, commonly referred to as *diophantine equations*, has been the focus of number theory over the past two millennia. Some of the most studied problems include finding Pythagorean triples or solving the equation $x^n + y^n = z^n$ for $n \geqslant 3$ featured in Fermat's Last Theorem.

We may go on about solving equations in one of several ways. We can attempt to restrict the solution set by the means of inequalities, factorisation or modular arithmetic. One of the more advanced areas of modular arithmetic are the so-called *quadratic residues*, which will help us work with integer squares.

2 Quadratic residues

Definition 2.1. We call an integer d coprime with n a *quadratic residue* modulo n, if there exists $x \in \mathbb{Z}$ such that $x^2 \equiv d \pmod{n}$, and a *quadratic nonresidue* modulo n otherwise.

Finding the set of quadratic residues in $\mathbb{Z}_n$, the ring of residues modulo n, is rather difficult without knowing the factorisation of n, however the case with n being a prime power is easier. To do this, we define the Legendre symbol for odd primes p:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue modulo} p, \\ 0, & \text{if } p \mid a, \\ -1, & \text{otherwise.} \end{cases}$$

The Legendre symbol can be computed as

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Indeed, the case $p \mid a$ is vacuous. Fermat's Little Theorem states for all the other a:

$$0 \equiv a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} + 1\right)\left(a^{\frac{p-1}{2}} - 1\right) \pmod{p},$$

or $a^{\frac{p-1}{2}} \in \{\pm 1\} \pmod{p}$. If a is a non-zero square in $\mathbb{Z}_p$, then we have $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$ for some x. It can be shown that a polynomial of degree n has at most n roots in $\mathbb{Z}_p$, so the congruence $x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ has no more than $\frac{p-1}{2}$ incongruent solutions. Every element of $\mathbb{Z}_p$ has at most two square roots, since $x^2 \equiv y^2$ has two solutions, namely $\pm y$. There are precisely $\frac{p-1}{2}$ non-zero squares in $\mathbb{Z}_p$, all of which are roots of $x^{\frac{p-1}{2}} - 1$, so all the non-residues must satisfy $x^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Quadratic residues of prime powers can be quite easily found using the knowledge of quadratic residues modulo a prime, and reconstructed for arbitrary positive integers using the Chinese remainder theorem.

There are many important and interesting properties of quadratic residues, for example the Law of Quadratic Reciprocity and its supplements. For a more comprehensive overview of the theory of quadratic residues, we direct the reader to [1, 2]. We demonstrate the power of quadratic residues on a couple "victims" in the chapter Associated content.

Nevertheless, not all equations are solvable using only modular arithmetic. Take, for instance, the equation:

$$x^2 + 13 = y^3.$$

This equation has an integral solution $(70, 17)$ and therefore a solution modulo every positive integer. Furthermore, there are equations with solutions differing in size, for example the equation $x^2 + 26 = y^3$ with a solution for $x = 1$ and $x = 207$. There is no easy way to bound variables in an equation with coprime powers, as can be seen in prevalence of problems such as *Catalan's conjecture*, which was only recently confirmed in the affirmative. We then have to find a new course of action in, say, factoring one of the sides.

Recall the formula for the difference of squares $a^2 - b^2 = (a - b)(a + b)$, which can be extended to $a^2 + b^2 = (a + bi)(a - bi)$ by using complex numbers. Likewise, we get $x^2 + 13 = \left(x + \sqrt{-13}\right)\left(x - \sqrt{-13}\right)$, which contains both imaginary and irrational numbers, certainly not ideal from an elementary viewpoint. In the rest of our article, we will be exploring the necessary theoretical background, which allows us to solve equations using similar unorthodox factorisations.

3 Number fields

The idea of using imaginary and irrational numbers in solving equations over the integers goes all the way back to Carl Friedrich Gauss, who was also one of the founders of modern modular arithmetic. First breakthroughs in this *algebraic number theory* were done in hopes of solving Fermat's Last Theorem, and even though the first correct proof came via elliptic curves, the algebraic view gave the problem valuable insight.

We will be studying complex roots of polynomials over the integers, called *algebraic numbers*, and be paying especially close attention to *algebraic integers*, i.e. algebraic numbers, which are roots of monic polynomials over the integers. The *minimal polynomial* of an algebraic number α is the integer polynomial f with the smallest possible degree such that $f(\alpha) = 0$.

Definition 3.1. A field K containing $\mathbb{Q}$ is said to be an *algebraic number field*, if it contains only algebraic numbers and there exist $x_1, \dots, x_n \in K$, such that $K = \{c_1x_1 + \cdots + c_nx_n | c_i \in \mathbb{Q}\}$.

We will often simply call these sets number fields.

Definition 3.2. Let $\alpha_1, \dots, \alpha_n$ be irrational numbers linearly independent over $\mathbb{Q}$. We shall denote the smallest (with respect to inclusion) number field containing these numbers as $\mathbb{Q}(\alpha_1, \dots, \alpha_n)$.

The set of algebraic integers in a number field K, denoted by $\mathcal{O}_K$, forms a ring. As a result, we will also be referring to this set as the *ring of integers of* K. Before studying the properties of $\mathcal{O}_K$, we would first want to know what it looks like.

We will mainly be concerned with extensions of the rationals by a number whose minimal polynomial over $\mathbb{Z}$ is quadratic, i.e. fields of the form $\mathbb{Q}\left(\sqrt{m}\right)$ for $m \in \mathbb{Z}$, such extensions are called *quadratic fields*.

The ring of integers of the field $\mathbb{Q}(i)$ is the ring of the Gaussian integers $\mathbb{Z}[i]$. We could conclude that the ring of integers of the field $\mathbb{Q}\left(\sqrt{m}\right)$ is simply $\mathbb{Z}\left[\sqrt{m}\right]$, unfortunately this is not always the case. It only takes a bit of casework to arrive at the following characterisation:

Theorem 3.1. *Let $m \neq 0, 1$ be square-free and $K = \mathbb{Q}(\sqrt{m})$ a number field. Then:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}\left[\sqrt{m}\right] & = \left\{a + b\sqrt{m} | a, b \in \mathbb{Z}\right\}, \text{ if } \quad m \equiv 2, 3 \pmod 4, \\ \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right] & = \left\{a + b\frac{1+\sqrt{m}}{2} \middle| a, b \in \mathbb{Z}\right\}, \text{ if } \quad m \equiv 1 \pmod 4. \end{cases}$$

The proof follows from the form roots of quadratic polynomials take and it can be found in [3]. We will now further explore the theory surrounding these rings. Let us begin with divisibility.

The only integers having a multiplicative inverse are clearly ± 1. Similarly, we define *units* as elements of $\mathcal{O}_K$ with a multiplicative inverse. Plus and minus 1 are units in $\mathcal{O}_K$ for any K, often times, though, they are not alone. Take the Gaussian integers $\mathbb{Z}[i]$ with additional units $\pm i$ for an example. A similar generalisation can be made from primes to *irreducible elements* of $\mathcal{O}_K$, as numbers which cannot be written as a product of two elements of $\mathcal{O}_K$ both non-units. This time not all integer primes are irreducible, for instance we may write $5 = (2+i)(2-i)$ in $\mathbb{Z}[i]$ as a product of two non-units, yet the number 7 is indeed irreducible, as we will soon see.

In fact, even unique factorisation into irreducible elements does not always hold, and we mainly want to work with objects which uniquely factor into irreducibles. In some rings, this condition is satisfied by *ideals*.

Ideals can be thought of as generalisations of multiples of whole numbers in rings. Formally:

Definition 3.3. An *ideal* is a non-empty subset $\mathcal{I}$ of a ring R, such that for any (not necessarily distinct) elements a, b of $\mathcal{I}$ and $r \in R$, we have $a + b \in \mathcal{I}, r \cdot a \in \mathcal{I}$.

In this article, we will only be concerned with rings whose ideals are generated by a finite set, which is satisfied by $\mathcal{O}_K$. We will therefore think of an ideal $\mathcal{I}$ of a ring R as a set $\{r_1a_1 + \cdots + r_na_n | a_i \in R\}$ for some $n \in \mathbb{N}$ and $r_1, \dots, r_n \in R$. We say r_i *generate* $\mathcal{I}$ and denote this ideal $(r_1, \dots, r_n)$. An ideal generated by a single element, i.e. (a) for some a, is called *principal*.

If we were to define the product of two ideals, we would want it to be generated by the pairwise products of the

respective generators, and so the following definition comes naturally:

$$\mathcal{I}\cdot\mathcal{J}=\left\{\sum_{i=1}^{n}a_ib_i\middle|\,a_i\in\mathcal{I},b_i\in\mathcal{J},n\in\mathbb{N}\right\}.$$

Indeed, if $\mathcal{I}$ and $\mathcal{J}$ are generated by the sets $\{a_1,\dots,a_k\}$ and $\{b_1,\dots,b_\ell\}$, respectively, their product has the generating set $\{a_1b_1,a_1b_2\dots,a_2b_1,\dots,a_kb_\ell\}$ and is an ideal itself.

Beyond this, few obvious properties arise. For one, ideal product is associative:

$$(\mathcal{I}\cdot\mathcal{J})\cdot\mathcal{K}=\left\{\sum_{i=1}^{n}a_ib_ic_i\middle|\,a_i\in\mathcal{I},b_i\in\mathcal{J},c_i\in\mathcal{K},n\in\mathbb{N}\right\}=\mathcal{I}\cdot(\mathcal{J}\cdot\mathcal{K}).$$

We also define the k-th power of an ideal like so:

$$\mathcal{I}^k=\underbrace{\mathcal{I}\cdot\mathcal{I}\cdots\mathcal{I}}_{k}.$$

Multiplication of principal ideals is exceptionally nice. Not only is the product of two principal ideals principal, we can form the following stronger result:

Theorem 3.2. *If $a,b\in R$, then:*

$$(a)(b)=(ab).$$

Proof. Clearly $ab\in(a)(b)$ and since ab is contained in $(a)(b)$, so are all its multiples in R, therefore $(ab)\subseteq(a)(b)$. Also, every finite sum $\sum_{i=1}^{n}a_ib_i$ with $a_i\in(a),b_i\in(b),n\in\mathbb{N}$ has every summand divisible by ab, so $(a)(b)\subseteq(ab)$. □

Ideal divisibility can be defined in the evident way, i.e. $\mathcal{I}\mid\mathcal{J}$ if and only if an ideal $\mathcal{K}$ such that $\mathcal{J}=\mathcal{I}\cdot\mathcal{K}$ exists. The principal case is once again simple.

Corollary 3.1. *The equivalence:*

$$(a)\mid(b)\Leftrightarrow b\in(a)$$

holds for non-zero $a,b\in R$.

Proof. If $b\in(a)$, b is a multiple of a, so $b=ak$ for some $k\in R$, hence from the previous theorem we have $(a)\mid(a)(k)=(ak)=(b)$. On the other hand if $(a)\mid(b)$ holds, $(b)=(a)\cdot\mathcal{I}$ for a non-zero ideal $\mathcal{I}\subseteq R$. From the definition of ideal product, every element of $(a)\cdot\mathcal{I}$ is represented by a finite sum of products of two elements, one belonging in (a) and the other in $\mathcal{I}$. Every such summand is divisible by a, therefore $b\in(b)=(a)\cdot\mathcal{I}\subseteq(a)$ as desired. □

Let us now take a look at divisibility in the ring $\mathcal{O}_K$ itself. To help us through, we will invoke several familiar terms used when describing complex numbers.

4 Norms and prime ideals

For a complex number $z=a+bi$, we define its conjugate $\overline{z}=a-bi$ and absolute value a non-negative real number satisfying $|z|^2=z\overline{z}=a^2+b^2$, so $|z|=\sqrt{a^2+b^2}$.

We will define conjugates over a quadratic field slightly differently:

$$\overline{\left(a+b\sqrt{m}\right)}=a-b\sqrt{m},$$
$$\overline{\left(a+b\frac{1+\sqrt{m}}{2}\right)}=a+b\frac{1-\sqrt{m}}{2}.$$

We then easily get $\overline{\alpha}=\alpha$ for rational α and furthermore a number and its conjugate always share their minimal polynomial. Indeed, these numbers have a minimal polynomial of degree at most 2 and non-rational numbers $a+b\sqrt{m}$, $a+b\frac{1+\sqrt{m}}{2}$ have minimal polynomials $(x-a)^2-b^2m$ and $(x-a)^2-bx+ab+b^2\frac{1-m}{4}$, respectively. For $m=-1$ the definition of a conjugate number corresponds with the classical definition of a complex conjugate.

Rather than extending the definition of the absolute value, we instead define the *norm* of a number as $N(z)=z\overline{z}$. The norm of a number is roughly the constant term of its minimal polynomial:

Theorem 4.1. *Let $m\neq0,1$ be a square-free integer. The norm of $a+b\sqrt{m}\in\mathbb{Q}\left(\sqrt{m}\right)$ is:*

- $N\left(a+b\sqrt{m}\right)=a^2-mb^2$, *if* $m\not\equiv1\pmod4$,
- $N\left(a+b\frac{1+\sqrt{m}}{2}\right)=a^2+ab+\frac{1-m}{4}b^2$, *if* $m\equiv1\pmod4$.

Taking norms helps in studying divisibility in $\mathcal{O}_K$. Indeed, an element of K has an integral norm iff it lies in $\mathcal{O}_K$. The norm is a multiplicative function, namely for $a+b\sqrt{m},c+d\sqrt{m}\in\mathbb{Z}\left[\sqrt{m}\right]$:

$$\begin{aligned}&\left(a+b\sqrt{m}\right)N\left(c+d\sqrt{m}\right)=(a^2-mb^2)(c^2-md^2)\\&=a^2c^2+m^2b^2d^2-m\left(a^2d^2+b^2c^2\right)\\&=a^2c^2+2acmbd+m^2b^2d^2-m\left(a^2d^2+b^2c^2\right)-2acmbd\\&=(ac+mbd)^2-m(ad+bc)^2=N\left(ac+mbd+\sqrt{m}(ad+bc)\right)\\&=N\left(\left(a+b\sqrt{m}\right)\left(c+d\sqrt{m}\right)\right).\end{aligned}$$

An analogous computation can be carried through for elements of the rings $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. If a number a divides b in $\mathcal{O}_K$ in the sense that $b=ac$ for some $c\in\mathcal{O}_K$, then $N(b)=N(a)N(c)$ and so $N(a)\mid N(b)$. The converse does not always hold, take the numbers $2+i$ and $1+2i$ in $\mathbb{Z}[i]$ for an example, having the same norm and quotient $\frac{2+i}{1+2i}=\frac{(2+i)(1-2i)}{5}=\frac{4-3i}{5}$, which is not a Gaussian integer. To properly study divisibility in $\mathcal{O}_K$, we will first check up with units.

Let $\alpha\in\mathcal{O}_K$ be a unit, then $\alpha\cdot\beta=1$ for some $\beta\in\mathcal{O}_K$. From the multiplicativity of norms it follows:

$$N(\alpha)N(\beta)=N(\alpha\cdot\beta)=N(1)=1.$$

Because the norm of an element of $\mathcal{O}_K$ is an integer, we have $N(\alpha)=\pm1=N(\beta)$, so units of $\mathcal{O}_K$ have norms equal to ±1. Furthermore, from the definition of the norm as a product of conjugates, every element of the ring $\mathcal{O}_K$ with

norm equal to ± 1 is a unit. The units of the rings $\mathbb{Z}\left[\sqrt{m}\right]$, where $m \not\equiv 1 \pmod 4$, are given by:

$$\pm 1 = N\left(a + b\sqrt{m}\right) = a^2 - mb^2,$$

and are solutions to the extended Pell's equation. The case $m < 0$ gives only finitely many solutions, units of the ring $\mathbb{Z}[i]$ are $\pm 1, \pm i$ and the rest of the rings in question have units only ± 1. In the case of a positive m the units form an infinite multiplicative group. Similarly, for $0 > m \equiv 1 \pmod 4$ we only have a finitely many solutions, for $m > 0$ the set of units forms an infinite cyclic group. The units in quadratic fields are therefore mostly easily characterised.

Units help us work with principal ideals, namely to decide whether two principal ideals coincide. To do so, however, we will have to briefly stop by zero divisors in rings.

If a ring contains no zero divisors, meaning the product of two non-zero elements is itself nonzero, we call it an *integral domain*. The ring of integers modulo 6 is not an integral domain, since the product of 2 and 3 is 0. By contrast, the ring of integers $\mathcal{O}_K$ of a number field K is clearly always an integral domain. We can then state the following:

Theorem 4.2. *Let $a, b \in \mathcal{O}_K$. Then the equality $(a) = (b)$ holds iff there exists a unit $u \in \mathcal{O}_K$ satisfying $a = ub$.*

Proof. If $(a) \mid (b)$, then $b \in (a)$, so by corollary 3.1: $b = ax$ for some $x \in \mathcal{O}_K$. By the same token: $a \in (b)$, so $a = by, y \in \mathcal{O}_K$. Then $a = axy$, so $a(1 - xy) = 0$, and since $\mathcal{O}_K$ is an integral domain, at least one of the two factors is 0. The case $a = 0$ is trivial, so let $xy = 1$, then the numbers x, y are units. On the other hand if $a = ub$ for a unit $u \in \mathcal{O}_K$: $a = ub \in (b)$, so $(a) \subseteq (b)$. Similarly $b = \frac{1}{u}a \in (a)$, or $(b) \subseteq (a)$. Consequently $(a) = (b)$. □

Having looked at units and norms, it is time to combine the two together. That is because norms finally offer a justification for the irreducibility of, say, 7 in $\mathbb{Z}[i]$, as if it were a product of two non-units, both of then would have norm 7, since $N(7) = 49$. However, the equation $7 = a^2 + b^2 = N(a + bi)$ has no integer solutions, because squares only leave residues 0 and 1 when divided by 4. In some cases, quadratic residues can even help us proving irreducibility of a prime (note composite numbers are reducible by default), for example 2 and 7 in the ring $\mathbb{Z}\left[\sqrt{11}\right]$.

We want to work with divisibility in the realm of ideals of $\mathcal{O}_K$ and to do so, we define the ideal norm. The norm of an ideal is defined as the cardinality of a certain set, which is not at all important to our exposition, the precise definition can be found in [4]. Regardless of our imprecise definition, it is key that we can easily determine the norm of a principal ideals of $\mathcal{O}_K$:

Theorem 4.3. *Any $m \in \mathcal{O}_K$ satisfies:*

$$N((m)) = |N(m)|.$$

Despite the elegance of this statement, the proof is quite involved and can be found in [5]. Note the appearance of an absolute value, since the norm of an element can be negative, but the ideal norm is always non-negative. From the multiplicative property of the norm we see the ideal norm is multiplicative on principal ideals. The norm is multiplicative on any two nonzero ideals $\mathcal{I}, \mathcal{J} \subseteq \mathcal{O}_K$:

$$N(\mathcal{I})N(\mathcal{J}) = N(\mathcal{I} \cdot \mathcal{J}),$$

The proof once again uses more advanced number theory tools. It can be found in [6, Theorem 22].

Now let us look at prime ideals, which are to ideals of $\mathcal{O}_K$ what primes are to integers.

Definition 4.1. Suppose $\mathcal{P} \subset \mathcal{O}_K$ is an ideal such that for any $a, b \in \mathcal{O}_K$ satisfying $ab \in \mathcal{P}$, it follows that $a \in \mathcal{P}$ or $b \in \mathcal{P}$. We call such an ideal *prime*.

We know an element of $\mathcal{O}_K$ has a prime norm only if it's irreducible. Prime ideal norms work in much the same way.

Theorem 4.4. *Let $\mathcal{P}$ be a prime ideal. Then there are a prime p and a $j \in \mathbb{N}$ such that $N(\mathcal{P}) = p^j$ and $p \in \mathcal{P}$.*

The existence of such a prime can be recovered from the precise definition of the ideal norm, the proof can be found in [6]. Prime ideals have norms equal to prime powers and conversely, an ideal with a prime norm is prime.

From our surface-level understanding of prime ideals so far, we can see they are intrinsically tied to primes, one of whose most important properties is uniqueness of prime factorisation. The main reason we defined ideals is because factorisation number rings is often not unique. Indeed, we can reduce the number 6 in the ring $\mathbb{Z}\left[\sqrt{-5}\right]$ as follows: $6 = 2 \cdot 3 = \left(1 + \sqrt{-5}\right)\left(1 - \sqrt{-5}\right)$. The numbers $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ are all irreducible in $\mathbb{Z}\left[\sqrt{-5}\right]$, since their norms are $4, 9, 6, 6$, respectively. The existence of an element with norm 2 or 3 contradicts the fact that $N\left(a + b\sqrt{-5}\right) = a^2 + 5b^2$ never leaves residues 2 or 3 when divided by 5, as they are both quadratic nonresidues modulo 5.

In general, unique factorisation into prime ideals in a ring does not necessarily hold and when it does, we call the ring a *Dedekind domain*. In particular, it can be shown the ring $\mathcal{O}_K$ is a Dedekind domain. Any two ideals share a unique greatest common divisor and we may thus call them *coprime* if it is the ideal (1).

The ideal (6) possesses unique factorisation $(6) = \left(2, 1 + \sqrt{-5}\right)^2 \left(3, 1 + \sqrt{-5}\right)\left(3, 1 - \sqrt{-5}\right)$, with the two sets of factors of 6 generating ideals, which can be factored as follows:

- $(2) = \left(2, 1 + \sqrt{-5}\right)^2$,
- $(3) = \left(3, 1 + \sqrt{-5}\right)\left(3, 1 - \sqrt{-5}\right)$,
- $\left(1 + \sqrt{-5}\right) = \left(2, 1 + \sqrt{-5}\right)\left(3, 1 + \sqrt{-5}\right)$,

- $\left(1-\sqrt{-5}\right)=\left(2,1+\sqrt{-5}\right)\left(3,1-\sqrt{-5}\right)$.

We have already met the following statement in the case of principal ideals:

Theorem 4.5. *Let $\mathcal{A},\mathcal{B}$ be ideals $\mathcal{O}_K$. Then $\mathcal{B} \mid \mathcal{A}$ holds iff $\mathcal{A} \subseteq \mathcal{B}$.*

A proof using unique factorisation into prime ideals in $\mathcal{O}_K$ can be found in [5]. The next couple of theorems further explore the parallels between $\mathcal{O}_K$ and the set of integers:

Theorem 4.6. *Let $\mathcal{A},\mathcal{B},\mathcal{C}$ be non-zero ideals of the ring $\mathcal{O}_K$. If the equality $\mathcal{A}\cdot\mathcal{B}=\mathcal{C}^k$ holds for some $k\in\mathbb{N}$ and furthermore $\mathcal{A},\mathcal{B}$ are coprime, then there exist ideals $\mathcal{I},\mathcal{J}\subseteq\mathcal{O}_K$ such that:*

$$\mathcal{A}=\mathcal{I}^k, \qquad \mathcal{B}=\mathcal{J}^k.$$

Proof. Let $\mathcal{A}=\mathcal{P}_1^{a_1}\cdots\mathcal{P}_p^{a_p}, \mathcal{B}=\mathcal{Q}_1^{b_1}\cdots\mathcal{Q}_q^{b_q}$ be the respective factorisations of $\mathcal{A},\mathcal{B}$ into prime ideals. If $\mathcal{A},\mathcal{B}$ are coprime, the sequences of prime ideals $\mathcal{P}_i$ and $\mathcal{Q}_i$ are disjoint. Any prime ideal dividing $\mathcal{C}^k$ divides it in the k-th power (or a multiple of k), so since $\mathcal{A}$ and $\mathcal{B}$ are relatively prime, any prime ideal dividing their product divides exactly one them in a power of a multiple of k. Both ideals are thus k-th powers. □

The sum of two multiples of an integer d is once again divisible by d. We can state a similar property of ideals, but this time, we will hone in squarely on principal ideals.

Theorem 4.7. *If $a,b\in\mathcal{O}_K$ and in ideal $\mathcal{I}\subseteq\mathcal{O}_K$ satisfy $\mathcal{I}\mid(a),(b)$, then $\mathcal{I}\mid(a\pm b)$.*

Proof. If $\mathcal{I}\mid(a),(b)$, then according to the theorem 4.5, a,b belong to $\mathcal{I}$, so from the definition of an ideal we have $a\pm b\in\mathcal{I}$. The conclusion follows. □

Unique factorisation into prime ideals holds in Dedekind domains, particularly in $\mathcal{O}_K$, but the elements of $\mathbb{Z}$ and $\mathbb{Z}[i]$ also factor uniquely into irreducible elements. Carl Friedrich Gauss pondered, whether there are only a finite number of such rings among the rings of integers in imaginary quadratic fields, or $K=\mathbb{Q}\left(\sqrt{d}\right)$ for $d<0$. This conjecture was proven in the affirmative in the 20th century with the only such numbers being:

$$-1,-2,-3,-7,-11,-19,-43,-67,-163.$$

There is little to be said about the real case, to the extent that it is not even known if an infinite number of these fields have unique factorisation.

In general, we want to define a structure measuring to what extent unique factorisation fails in a ring. And that is precisely the purpose of the so-called *ideal class group*.

5 Class groups

Consider the set of all the ideals in the ring $\mathcal{O}_K$. We say two ideals $\mathcal{I},\mathcal{J}$ are *equivalent*, denoted as $\mathcal{I}\sim\mathcal{J}$, if $a,b\in\mathcal{O}_K$ such that $\mathcal{I}\cdot(a)=\mathcal{J}\cdot(b)$ exist. This relation partitions the set of ideals into equivalence classes, where two ideals lie in the same class if and only if $\mathcal{I}\sim\mathcal{J}$.

Multiplying an ideal by a principal one leaves its class invariant. The set of ideal classes then forms a multiplicative group, in which the class of principal ideals acts as the neutral element. Indeed, we have seen that ideal product is associative and any non-zero ideal of a Dedekind ring has an inverse, as shown in [5, Theorem 4.1.7.], which contains the proof for prime ideals. The existence of an inverse of any non-zero ideal in $\mathcal{O}_K$ then follows from unique factorisation into prime ideals.

The group described above is known as the *ideal class group* of the ring $\mathcal{O}_K$.

Theorem 5.1. *The ideal class group of the ring $\mathcal{O}_K$ is finite.*

A proof of this statement can be found in [5, Corollary 5.2.5.]. Note the ideal class group in an arbitrary ring is, in general, not finite, even if we restrict our efforts to Dedekind rings.

The number of ideal classes in $\mathcal{O}_K$ is called the *class number* of $\mathcal{O}_K$ and will be denoted by h_K. Ideal classes form a group and so it follows:

Theorem 5.2. *Let $\mathcal{I}$ be an ideal in $\mathcal{O}_K$. Then $\mathcal{I}^{h_K}$ is a principal ideal.*

This theorem lies at the core of our study of ideals in the ring $\mathcal{O}_K$. We will here on out be able to prove an ideal is principal by showing it is equal to a h_K-th power of an ideal.

We will now take a step back and dive into the ideas connecting unique factorisation in $\mathcal{O}_K$ and class groups. For one, the theorem above states that number fields with $h_K=1$ allow for any ideal to be principal. We can push this observation further:

Theorem 5.3. *If K is a number field with $h_K=1$, then $p\in\mathcal{O}_K$ is irreducible iff the ideal (p) is prime.*

Proof. Firstly, let (p) be a prime ideal and, say, $p=ab$ for some $a,b\in\mathcal{O}_K$. According to theorem 3.2 it follows that $(p)=(ab)=(a)(b)$, so unique factorisation dictates one of a,b be a unit and subsequently p irreducible. On the other side of the coin, let p be irreducible and (p) a product of two two ideals in $\mathcal{O}_K$. Since the theorem above states that every ideal of $\mathcal{O}_K$ is principal, or $(p)=(a)(b)$ for some $a,b\in\mathcal{O}_K$. The equality $(p)=(a)(b)=(ab)$ and theorem 4.2 imply $p=uab$ for a unit $u\in\mathcal{O}_K$. Since p is irreducible, at most one of a,b is not a unit, therefore one of $(a),(b)$ is the ring $\mathcal{O}_K$ itself and (p) is a prime ideal. □

Corollary 5.1. *Let K be a number field. If the class number of $\mathcal{O}_K$ is 1, then every element $\mathcal{O}_K$ can be uniquely written as a product of irreducible elements up to permutation and multiplication by a unit.*

Proof. First up, we will show that every non-unit element can be written as a product of irreducible elements. Suppose that there are elements, that cannot be written as

a product of irreducible elements and take $x \in \mathcal{O}_K$ one such element with the least value of $|N(x)|$. Clearly n is not irreducible, so let $n = ab$ with a, b both non-units. Then $N(x) = N(a)N(b)$, so $|N(a)|, |N(b)| < |N(x)|$, so by the assumption a and b can both be written as a product of irreducible elements. Since $x = ab$, this is the desired contradiction.

Now, let h_K be 1 and $n \in \mathcal{O}_K$ with two factorisations into irreducible elements $u_1 p_1 p_2 \cdots p_k = n = u_2 q_1 q_2 \cdots q_\ell$, where u_i are units. Theorem 3.2 implies the equality:

$$(p_1) \cdot (p_2) \cdots (p_k) = (p_1 p_2 \cdots p_k) = (q_1 q_2 \cdots q_\ell) = (q_1) \cdot (q_2) \cdots (q_\ell).$$

The ideals (p_i) and (q_i) are prime due to the theorem above. The decomposition of both sides into prime ideals necessarily coincides, so theorem 4.2 implies the sets of the corresponding irreducible generators are, up to multiplication by a unit, identical. □

It can be shown that unique factorisation in $\mathcal{O}_K$ implies $h_K = 1$. We direct an interested reader to [2, Chapters 4 a 5] for a more in-depth treatment of ideal and number decomposition in the ring $\mathcal{O}_K$.

We know the product of two principal ideals is also principal, so, naturally, we may notice:

Theorem 5.4. *Let $\mathcal{I}$ be an ideal in $\mathcal{O}_K$ and k an integer. If $\mathcal{I}^k$ is a principal ideal and k is relatively prime to h_K, then $\mathcal{I}$ is principal.*

Proof. If k and h_K are coprime, Bezout's lemma gives the existence of integers a, b with $ak + bh_K = 1$. Then $\mathcal{I} = \mathcal{I}^{ak+bh_K} = (\mathcal{I}^k)^a \cdot (\mathcal{I}^{h_K})^b$ is a product of two principal ideals, since the power of a principal ideal $(x)^y$ is by 3.2 the principal ideal (x^y). It follows that $\mathcal{I}$ is a principal ideal in $\mathcal{O}_K$. □

For example, there are two ideal classes in the ring $\mathbb{Z}\left[\sqrt{-5}\right]$, so if an odd power of $\mathcal{I}$ is a principal, $\mathcal{I}$ is principal as well. Unique factorisation obviously does not hold in this ring, as can be seen in the aforementioned decomposition of the number 6.

We have described how divisibility in $\mathcal{O}_K$ works in great detail and discussed various properties of the ideal class group. With that knowledge in mind, we can, at last, get to solving diophantine equations. We solve two equations in section "Problems" in Supporting information using the methods we presented. An additional equation is to be solved by an intrigued reader.

6 Conclusion

The study of number fields and ideal class groups helps us in solving certain equation, which would have been hardly solvable by elementary means. We have hopefully provided a small insight into the underlying theory, even though we had to omit numerous details. The methods mentioned in this article allow us to solve harder equations, as can the reader can read in [3] and my own thesis [4], where I ended up solving a general equation of the type *quadratic* $= y^3$. The methods as outlined in the text can be generalized further to take into acount other monomials, such as y^5. Pushing further quickly gets ugly and substantially harder, for an example see *Ramanujan Nagell's equation*, see[7].

Frankly, the study of algebraic number theory leads to many more important results than just solving a diophantine equation. Studying this area of mathematics allows for more thorough study of, for example, quadratic residues and proving the Law of Quadratic Reciprocity and extending it to the so-called *Artin's Reciprocity Law*. We can also among others study Dedekind zeta functions, which are the generalisations of the one of Riemann, and so are connected to the distribution of primes.

Acknowledgements

I would like to thank Tomáš Perutka for introducing me to algebraic number theory and overseeing the thesis, based on which this article was written.

References

(1) Beneš, P. Reciprocity laws, Final thesis, Masaryk university, 2010, pp 12–20, https://is.muni.cz/th/mkttq/.

(2) Perutka, T. Using decomposition group to prove the quadratic reciprocity law, High school thesis, Masaryk university, 2018, pp 6–10, 34–56.

(3) Hrnčiar, M. Solving diophantine equations by factorization in number fields, Final thesis, Charles university, 2015, pp 25–26, https://dspace.cuni.cz/handle/20.500.11956/77698.

(4) Pezlar, Z. Interesting Uses of Algebraic Number Theory, High school thesis, Masaryk University, 2020, p 16.

(5) Pupík, P. Application of the ideal class group for solving some Diophantine equations, Final thesis, Masaryk university, 2006, pp 29–30, 43, 51–53, https://is.muni.cz/th/v8xsj/?so=nx.

(6) Marcus, D. A., *Number fields*, 1991st ed.; Axler, S., Gehring, F. W., Halmos, P. R., Eds.; Springer-Verlag: Pomona, 1977, p 287, ISBN: 0-387-90279-1.

(7) De Chenne, S. *Eric Weisstein's World of Mathematics* **2013**, 1–9.