Generalizations of the fundamental theorem of arithmetic

Vera Bulankina, Ivan Frolov, Timofei Zaitsev,
Aleksei Petukhov, Ruslan Salimov*

Introduction

The goal of this project is to generalize the fundamental theorem of arithmetic from integers to some more ”advanced” objects. For solving the problems of the project, it is possible to team up with other participants.

The fundamental theorem of arithmetic (Theorem 1 below, see also Theorems 4, 5, 7) is useful for finding integer solutions of various polynomial equations, i.e. Diophantine equations. For example they are useful in some proofs of Fermat's theorem on sum of two squares (Theorem 2) and Fermat's Last Theorem (Theorem 3) for $n = 3$. You can try to prove them right now, but most probably it is better to return to them after the relevant sections of the project. Also you will see that the uniqueness of the prime factorization does not always hold for analogs of integers.

In the second part of the project we consider the version of the fundamental theorem of arithmetic which works for numbers of the form $a + b\sqrt{d}$, where d is a fixed integer and a, b are any integer variables (to do this, we need a concept of ideal). This technique will be applied to Diophantine equations.

In the third part we will discuss a more general statement on arbitrary algebraic numbers.

Finally, there is an additional list of problems in which we will try to apply the general theory to Fermat's Last Theorem. We will discuss the so-called first case of the Fermat's Last Theorem for the regular prime numbers. Using similar ideas one can prove the second case of the Fermat's Last Theorem for any n, which is divisible by a regular prime number p. All prime number up to 37 are regular, see books of M. Postinkov or J. Milne or Wikipedia.

We would like to mention that Andrew Wiles general proof of the Fermat's Last Theorem is based on essentially different methods and ideas.

We have have used books of K. Ireland and M. Rosen, J. Milne, M. Postnikov, L. Washington, notes of K. Conrad and Wikipedia to prepare the project. We also added a few references [SS, Go, ZSS] that may be of interest to the reader who wants to learn more about this subject.

Theorem 1. The fundamental theorem of arithmetic.
Every integer $n > 1$ is a product $n = p_1 \cdot \ldots \cdot p_k$ of prime numbers $p_1, \ldots, p_k$. Moreover, this presentation is unique, up to an order of the factors.

Theorem 2. Fermat's theorem on sum of two squares.
An integer $n > 0$ can be expressed as a sum of two squares if and only if all prime numbers of the form $4k + 3$ participate the prime decomposition of n even number of times.

Theorem 3. Fermat's Last Theorem.
The equation $x^n + y^n = z^n$ has no solution in positive integers x, y and z for $n > 2$.

*We also wish to thank Mikhail Skopenkov, Ilya Bogdanov and Keith Conrad for a variety of useful comments on this project.

1 Gaussian integers

In this part of the project we want to discuss Gaussian integers. This is a generalization of integers which uses $\sqrt{-1}$. If you can't solve some of the problems from this section, then try to solve problems from other sections of the project and come back here later.

Definition. *Gaussian integers* is the set of complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$, $i = \sqrt{-1}$. We denote the set of Gaussian integers by $\mathbb{Z}[i]$.

Problem 1. Prove that the sum of any two Gaussian integers (and the product of any two Gaussian integers) is a Gaussian integer.

To proceed with the unique factorization for Gaussian integers we need a more exact formulation of the fundamental theorem of arithmetic. Strictly speaking, a straightforward analog of the statement of Theorem 1 is not literally correct even for integers: $2 \cdot 3 = 6 = (-2) \cdot (-3)$. For the new formulation we need few more definitions.

Definition. We say that an element $z \in \mathbb{Z}[i]$ is *invertible* if there is $b \in \mathbb{Z}[i]$ such that $ab = 1$. The invertible elements of $\mathbb{Z}$ are defined in the same way.

Exercise 1. Prove that the invertible elements in integers are 1 and -1. Prove that the invertible elements in Gaussian integers are 1, -1 and also $i, -i$.

Definition. A Gaussian integer is called *prime*, if for any it's factorization into two factors strictly one of these factors is an invertible element.

Definition. Two factorizations into prime numbers are *the same* if they have the same number of factors and if we can change the order of factors in such a way that the ratio of the corresponding prime factors is an invertible element. For example $7 \cdot 3, (-3) \cdot (-7)$ and $(-7i) \cdot (3i)$ are the same factorizations of 21 in Gaussian integers.

Our immediate goal is to prove and to discuss the following theorem.

Theorem 4. The fundamental theorem of arithmetic for the Gaussian integers.
Any two factorizations of a Gaussian integer into prime numbers are the same.

Problem 2.* Define a division-with-remainder for $\mathbb{Z}[i]$. Use it to prove Theorem 4.
Hint: use magnitude of complex numbers and graphical (Gaussian) interpretation of complex numbers.

Problem 3. Find all integer solutions of the equation $x^2 + 1 = y^n$.

Problem 4. a) Let $p \in \mathbb{Z}$ be prime. Prove that p is a prime Gaussian integer if and only if $p + 1$ is divisible by 4.

b) If $n, m \in \mathbb{Z}$ can be expressed as a sum of two squares, then mn can be expressed as a sum of two squares.

c) Prove Fermat's theorem on sum of two squares (Theorem 2).

Problem 5. Let n be an integer. Count the number of ways in which n can be decomposed into the sum of squares? Hint: try to use the prime factorization of n.

Eisenstein integers

The goal of this section is to solve of the following problem.

Problem 6*. Prove Theorem 3 for $n = 3$ using the following formula

$$x^3 + y^3 = (x + y)\left(x + \frac{-1 + \sqrt{-3}}{2}y\right)\left(x + \frac{-1 - \sqrt{-3}}{2}y\right).$$

Let's introduce several definitions and consider several ancillary problems to achieve this goal. Denote by ξ a cubic root of unity such that $\xi \neq 1$.

Exercise 2. Prove that $\xi = \frac{-1 \pm \sqrt{-3}}{2}$.

Put $\mathbb{Z}[\xi] := \{a + b\xi : \ a, b \in \mathbb{Z}\}$. Such numbers are called *Eisenstein integers.*

Definition. An Eisenstein integer $\alpha \in \mathbb{Z}[\xi]$ *is divisible* by $\beta \in \mathbb{Z}[\xi]$ if and only if there is $\gamma \in \mathbb{Z}[\xi]$ such that $\alpha = \beta\gamma$.

The invertible elements of $\mathbb{Z}[\xi]$ are defined similarly to the invertible elements of $\mathbb{Z}$ and of $\mathbb{Z}[i]$.

Definition. An Eisenstein integer $\alpha \in \mathbb{Z}[\xi]$ is *composite* if $\alpha = \beta\gamma$ where β and $\gamma \in \mathbb{Z}[\xi]$ aren't invertible. An nonzero Eisenstein integer $\alpha \in \mathbb{Z}[\xi]$ is *prime*, if α is neither composite nor invertible.

Problem 7. Find out all invertible elements of $\mathbb{Z}[\xi]$.

Problem 8. Define a division-with-remainder procedure for $\mathbb{Z}[\xi]$. Use it to formulate and to prove the fundamental theorem of arithmetic for $\mathbb{Z}[\xi]$.

Quadratic fields

In this section we consider quadratic fields. They generalise Gaussian integers and Eisenstein integers.

Definition. For complex numbers $a_1, \ldots, a_n$ let $\mathbb{Z}[a_1, \ldots, a_n]$ denote the smallest subset of $\mathbb{C}$ containing $\mathbb{Z}$ and $a_1, \ldots, a_n$ which is closed under addition, subtraction and multiplication.

Define $\mathbb{Q}[a_1, \ldots, a_n]$ similarly (replace $\mathbb{Z}$ by $\mathbb{Q}$). The sets $\mathbb{Z}[a_1, \ldots, a_n]$ play an analogous role in $\mathbb{Q}[a_1, \ldots, a_n]$ as the ordinary integers do in $\mathbb{Q}$. (Their elements can be added and multiplied).

Fix a square-free integer $d \neq 1$.

Remark. There are two main examples for d: $d = -3$ and $d = 2$. It can be useful to first check all problems of this section for these values of d, and then proceed to the general case.

Exercise 3. a) Prove that

$$\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\} \text{ and } \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}.$$

b) Prove that if $a, b \in \mathbb{Q}[\sqrt{d}]$ and $b \neq 0$, then $\frac{a}{b} \in \mathbb{Q}[\sqrt{d}]$.

Definition. *Integers in* $\mathbb{Q}[\sqrt{d}]$ are numbers $\alpha \in \mathbb{Q}[\sqrt{d}]$, satisfying $\alpha^2 + p\alpha + q = 0$ with $p, q \in \mathbb{Z}$.

Exercise 4. Is ξ an integer in $\mathbb{Q}[\sqrt{-3}]$? Is $\frac{1+i}{2}$ an integer in $\mathbb{Q}[i]$?

Set $\omega = \sqrt{d}$ when $d \equiv 2, 3 \bmod 4$, and $\omega = \frac{\sqrt{d}+1}{2}$ when $d \equiv 1 \bmod 4$.

The unique factorization into prime numbers can fail for $\mathbb{Z}[\omega]$, but there are several valid modifications of it. Further we will discuss one of them. For any $\alpha = a + b\sqrt{d}$, where $a, b \in \mathbb{Q}$, we define its conjugate $\overline{\alpha} = a - b\sqrt{d}$, its norm $N(\alpha) = \alpha\overline{\alpha}$ and its trace $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$.

Exercise 5. Prove that $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a}\overline{b}$.

Exercise 6. a) Prove that $\alpha \in \mathbb{Q}[\sqrt{d}]$ is a root of the polynomial $x^2 - \mathrm{Tr}(\alpha)x + N(\alpha)$.
b) Prove that $\alpha \in \mathbb{Q}[\sqrt{d}]$ is an integer in $\mathbb{Q}[\sqrt{d}]$ if and only if $N(\alpha) \in \mathbb{Z}$ and $\mathrm{Tr}(\alpha) \in \mathbb{Z}$.

Problem 9. Prove that the set of integers in $\mathbb{Q}[\sqrt{d}]$ coincides with $\mathbb{Z}[\omega]$.

The invertible elements of $\mathbb{Z}[\omega]$ are defined similarly to the invertible elements of $\mathbb{Z}$ and $\mathbb{Z}[i]$.

Exercise 7. Prove that $\gamma \in \mathbb{Z}[\omega]$ satisfies $N(\gamma) = \pm 1$ if and only if γ is invertible.

Definition. A number $\alpha \in \mathbb{Z}[\omega]$ *is divisible* by $\beta \in \mathbb{Z}[\omega]$ if there exists $\gamma \in \mathbb{Z}[\omega]$ such that $\alpha = \beta\gamma$.

Definition. A nonzero number $\alpha \in \mathbb{Z}[\omega]$ is *composite* if $\alpha = \beta\gamma$, where β and $\gamma \in \mathbb{Z}[\omega]$ are not invertible. A number $\alpha \in \mathbb{Z}[\omega]$ is *prime* if α is neither composite nor invertible.

Exercise 8. For $\gamma \in \mathbb{Z}[\omega]$ prove that if $|N(\gamma)| \in \mathbb{Z}$ is prime then γ is prime in $\mathbb{Z}[w]$. Show that the converse is false in $\mathbb{Z}[\sqrt{3}]$.

Exercise 9. Prove that if $\gamma \in \mathbb{Z}[\omega]$ is not invertible, then γ is a product of primes in $\mathbb{Z}[\omega]$.

Problem 10. Prove that all factors in the following decomposition of 15 in $\mathbb{Z}[\sqrt{-14}]$ are prime.

$$15 = 3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$$

Problem 11. Define a version of Euclidean algorithm for a) $\mathbb{Z}[\sqrt{-2}]$; b) $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Use it to prove the unique factorization in $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

Problem 12. Find all invertible elements of

$$\text{a) } \mathbb{Z}[\sqrt{-1}], \text{ b) } \mathbb{Z}[\sqrt{-d}] \text{ with } d \geq 2, \text{ c) } \mathbb{Z}[\tfrac{1+\sqrt{-3}}{2}], \text{ d*) } \mathbb{Z}[\sqrt{2}].$$

Problem 13. Does unique factorization hold in

$$\text{a) } \mathbb{Z}[\sqrt{2}], \text{ b) } \mathbb{Z}[\sqrt{-3}], \text{ c) } \mathbb{Z}[\sqrt{3}], \text{ d) } \mathbb{Z}[\sqrt{-5}], \text{ e) } \mathbb{Z}[\sqrt{5}], \text{ f) } \mathbb{Z}[\sqrt{10}], \text{ g) } \mathbb{Z}[\tfrac{1+\sqrt{5}}{2}],$$
$$\text{h) } \mathbb{Z}[\tfrac{1+\sqrt{-7}}{2}], \text{ i) } \mathbb{Z}[\tfrac{1+\sqrt{-11}}{2}], \text{ j*) } \mathbb{Z}[\tfrac{1+\sqrt{-19}}{2}] \text{ ?}$$

Problem 14. For which complex numbers ξ the sum and the product of any numbers of the form $a + b\xi$ with $a, b \in \mathbb{Z}$ have the same form?

Problem 15.* Find all positive integer solutions of
a) $3^n = k^2 + 2$ b) $2^n = k^2 + 7$.

Ideals

In the following sections we give an approach to the following problems.

Problem 16. Find all integer solutions of
a) $x^2+5=y^3$, b) $x^2+2x+7=y^3$ c) $5x^2+1=y^3$, d) $6x^2-12x+7=y^3$, e*) $x^2-6=y^3$.

Definition. A nonempty subset $I \in \mathbb{Z}$ is called an *ideal* if it is closed under addition, subtraction and multiplication by integers:

$$a, b \in I \implies a \pm b \in I, \quad a \in I, b \in \mathbb{Z} \implies ab \in I.$$

Remark. The notion of ideal was invented by Richard Dedekind as a replacement for the ideal numbers of Ernst Kummer (these numbers turn out to be useful to solve some cases Fermat's last theorem). One can check whether or not a given number is divisible by an ideal number even if this ideal number is not well defined. A similar idea is behind the definition of Dedekind cut of rational numbers.

Exercise 10. a) Prove that any ideal contains 0. b) Prove that $a \in I$ implies $-a \in I$. c) Prove that the set of all even integers form an ideal in $\mathbb{Z}$. d) Prove that the set $\{2018m : m \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$.

Exercise 11. Prove that the intersection of several ideals is an ideal.

We denote by $(a_1, \ldots, a_n)$ the smallest ideal (intersection of all ideals) containing $a_1, \ldots, a_n \in \mathbb{Z}$.

Problem 17. a) Let a, b be relatively prime numbers. Prove that $(a, b) = (1) = \mathbb{Z}$.

b) Prove that $(a, b) = (g)$, where $a, b \in \mathbb{Z}$ and g is the greatest common divisor of a, b.

c) Prove that every ideal $I \neq \{0\}$ in $\mathbb{Z}$ is (g) for some $g \in \mathbb{Z}$.

As in the previous section we set $\omega = \sqrt{d}$ when $d \equiv 2, 3 \mod 4$, and $\omega = \frac{\sqrt{d}+1}{2}$ when $d \equiv 1 \mod 4$. An ideal in $\mathbb{Z}[\omega]$ is defined similarly to $\mathbb{Z}$ ($\mathbb{Z}$ is replaced by $\mathbb{Z}[\omega]$). Similarly, numbers $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}[\omega]$ define an ideal $(\alpha_1, \ldots, \alpha_n)$ in $\mathbb{Z}[\omega]$. In particular, every element $\alpha \in \mathbb{Z}[\omega]$ defines the ideal (α).

Exercise 12. Prove that for nonzero α and β in $\mathbb{Z}[w]$ $(\alpha) = (\beta)$ if and only if $\alpha/\beta, \beta/\alpha \in \mathbb{Z}[\omega]$ (i.e. α/β is invertible in $\mathbb{Z}[\omega]$).

Exercise 13. Let $a, x, y \in \mathbb{Z}$. Prove that $x + y\omega \in (a)$ if and only if $a \mid x$ and $a \mid y$.

Definition. An ideal of the form (α) for some $\alpha \in \mathbb{Z}[\omega]$ is called *principal.* As we have seen in Problem 17, all ideals in $\mathbb{Z}$ are principal.

Problem 18. Show that $(2, \sqrt{-14})$ is not a principal ideal in $\mathbb{Z}[\sqrt{-14}]$.

Problem 19. Prove that, for each ideal I in $\mathbb{Z}[\omega]$, there exist $\alpha, \beta \in \mathbb{Z}[\omega]$ such that

$$I = \{x\alpha + y\beta : \quad x, y \in \mathbb{Z}\}.$$

Definition. For two ideals $I, J \in \mathbb{Z}[\omega]$ we set

$$I + J := \{i_1 + i_2 : i_1 \in I_1, i_2 \in J\}, \quad \overline{I} := \{\bar{i} : i \in I\},$$
$$IJ := \{i_1 j_1 + \cdots + i_k j_k : i_1, \ldots, i_k \in I, j_1, \ldots, j_k \in J\}.$$

Exercise 14. In $\mathbb{Z}[\sqrt{-14}]$ compute the product of ideals $I = (5 + \sqrt{-14}, 2 + \sqrt{-14})$ and $J = (4 + \sqrt{-14}, 2 - \sqrt{-14})$.

Exercise 15. Show that

$$(3) = p_1 p_2, \quad (5) = p_3 p_4, \quad (1 + \sqrt{-14}) = p_1 p_3, \quad (1 - \sqrt{-14}) = p_2 p_4,$$

where

$$p_1 = (3, 1 + \sqrt{-14}),\ p_2 = (3, 1 - \sqrt{-14})\ , p_3 = (5, 1 + \sqrt{-14}),\ p_4 = (5, 1 - \sqrt{-14}).$$

Exercise 16. Compute $(20)(18)$, $(20) + (18)$, $(20) \cap (18)$ in $\mathbb{Z}[\omega]$ for all d.

Exercise 17. Prove that $I + J, \overline{I}, IJ$ are ideals in $\mathbb{Z}[\omega]$ for all ideals $I, J \subset \mathbb{Z}[\omega]$.

2 Unique factorization: quadratic fields

In Problem 10 we saw that the straightforward version of the unique factorization fails for $\mathbb{Z}[\sqrt{-14}]$:

$$3 \cdot 5 = (1+\sqrt{-14})(1-\sqrt{-14}).$$

On the other hand, by Exercise 15,

$$(3) = p_1p_2, \quad (5) = p_3p_4, \quad (1+\sqrt{-14}) = p_1p_3, \quad (1-\sqrt{-14}) = p_2p_4,$$

where

$$p_1 = (3, 1+\sqrt{-14}), p_2 = (3, 1-\sqrt{-14}), p_3 = (5, 1+\sqrt{-14}), p_4 = (5, 1-\sqrt{-14}),$$

i.e. $(15) = p_1p_2p_3p_4$. The ideals p_1, p_2, p_3, p_4 are a replacement of prime numbers, see Problem 23, and the factorization $(15) = p_1p_2p_3p_4$ is unique up to the order of the factors, as the following theorem shows.

Theorem 5. Fundamental theorem of arithmetic for quadratic fields.
For every ideal $I \subset \mathbb{Z}[\omega]$ that is not (0) or (1) there exists a factorization of I as a product of prime ideals into prime ideals

$$I = p_1 \cdots p_s \subset \mathbb{Z}[\omega].$$

This factorization is unique up to an order of the factors.

Theorem 5 has two parts: existence of the factorization and its uniqueness. The former is proved in Problem 24 and the latter in Problem 27. As an example, this theorem can be used to solve Problem 16. See also the section on Fermat's Last Theorem.

Corollary. For every $m \in \mathbb{Z}[\omega]$ that is not 0 or invertible there exists a factorization of the ideal (m) into a product of prime ideals $p_1, \ldots, p_s \subset \mathbb{Z}[\omega]$, unique up to the order of the factors.

The proof is divided into the following problems.

Problem 20. For every $a_1, \ldots, a_n \in \mathbb{Z}[\omega]$ prove that

$$(a_1, \ldots, a_n)(\overline{a}_1, \ldots, \overline{a}_n) = (N(a_i), \mathrm{Tr}(a_i\overline{a_j}))_{1 \le i,j \le n}.$$

Hint: consider the case of an ideal generated by two elements.

Definition. We say that an ideal I *is divisible by* an ideal J if there exists an ideal H in $\mathbb{Z}[\omega]$ such that $I = JH$.

Problem 21. For any two ideals I, J in $\mathbb{Z}[\omega]$ prove that I is divisible by J if and only if I is contained in J.
Hint: use the previous problem.

Exercise 18. Use Problem 20 to prove that, for every nonzero ideal $I \subset \mathbb{Z}[\omega]$, there exists a positive integer $N(I)$ such that $I\overline{I} = (N(I))$.

Problem 22. Prove that an ideal H divides I and J if and only if it divides $I + J$.

Exercise 19. Prove that $N((a)) = |N(a)|$ for every nonzero $a \in \mathbb{Z}[\omega]$.

Exercise 20. Prove that $N(I)N(J) = N(IJ)$ for all nonzero ideals I, J in $\mathbb{Z}[w]$.

Exercise 21. Prove that if an ideal I divides an ideal J, than $N(I)$ divides $N(J)$.

Exercise 22. Prove that $N(I) = 1$ if and only if $I = (1)$.

An ideal I in $\mathbb{Z}[\omega]$ is called *prime* if it is not (1) and it is divisible by exactly two ideals: itself and (1).

Exercise 23. Prove that an ideal I is prime if and only if it is maximal, i.e. the only bigger ideal is (1).

Two ideals I, J are called *relatively prime* if $I + J = (1)$.

Exercise 24. Prove that any two distinct prime ideals are relatively prime.

Problem 23. Show that the following ideals are prime in $\mathbb{Z}[\sqrt{-14}]$:

$$p_1 = (3, 1 + \sqrt{-14}),\ p_2 = (3, 1 - \sqrt{-14}),\ p_3 = (5, 1 + \sqrt{-14}),\ p_4 = (5, 1 - \sqrt{-14}).$$

Problem 24. Prove that every nonzero ideal I in $\mathbb{Z}[\omega]$ besides (1) equals the product of several prime ideals.

Problem 25. Prove that if ideals I, J in $\mathbb{Z}[\omega]$ are relatively prime and I divides HJ for an ideal H, then I divides H.

Problem 26. a) Suppose that $a \in \mathbb{Z}[\omega]\backslash\{0\}$ and $(a)I = (a)J$ for ideals $I, J \subset \mathbb{Z}[\omega]$. Prove that $I = J$.
b) Suppose that ideals I, H, J satisfy $H \neq (0)$ and $HI = HJ$. Prove that $I = J$.

Problem 27. Prove that the factorization in Problem 24 is unique up to the order of the factors.

Prime ideals and prime numbers

Problem 28. a) Prove, that every ideal in $\mathbb{Z}[\sqrt{-5}]$ either is principal or equals $((1+\sqrt{-5})a, 2a)$ for some $a \in \mathbb{Q}[\sqrt{-5}]$.
b) Prove that every ideal in $\mathbb{Z}[\sqrt{-6}]$ either is principal or equals $(\sqrt{-6}a, 2a)$ for some $a \in \mathbb{Q}[\sqrt{-6}]$.

Problem 29. Prove that every nonzero ideal in $\mathbb{Z}[\omega]$ contains a positive integer.

Problem 30. Prove that every prime ideal I in $\mathbb{Z}[\omega]$ contains a unique prime number $p \in \mathbb{Z}, p > 0$.

Problem 31. Suppose I is a prime ideal. Prove that $N(I)$ equals either p or p^2 for some prime number $p \in \mathbb{Z}$.

Problem 32. Prove that prime numbers p in two previous problems coincide.

Problem 33. Prove that for any prime number $p \in \mathbb{Z}$ the ideal $(p) \subset \mathbb{Z}[\omega]$ either is prime or equals to a product of two (not nessesarily distinct) conjugate prime ideals.

Problem 34. Let $P_\omega(x)$ be monic quadratic polynomial with integer coefficients such that $P_\omega(\omega) = 0$. In assumptions of previous problem prove that former case takes place if and only if the equation $P_\omega(x) = 0$ do not have solutions modulo p.

Algebraic numbers

In this section we wish to discuss algebraic numbers together with techniques and problems arising from this notion.

The content of this section is present (as a general rule) in number theory courses of university level, but we believe that this content can be managed by advanced high school students as well.

Definition. A complex number $\alpha \in \mathbb{C}$ is called *algebraic* if it is a root of a nonzero polynomial with rational coefficients. An algebraic number $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients. We denote the set of algebraic numbers by $\overline{\mathbb{Q}}$. We denote the set of algebraic integers by $\overline{\mathbb{Z}}$.

Problem 35. Pick $a \in \mathbb{Q}$. Show that if $a \in \overline{\mathbb{Z}}$ then $a \in \mathbb{Z}$.

Problem 36.* Pick $\alpha, \beta \in \overline{\mathbb{Q}}$. Show that $\alpha \pm \beta \in \overline{\mathbb{Q}}$, $\alpha\beta \in \overline{\mathbb{Q}}$, $\alpha/\beta \in \overline{\mathbb{Q}}$ (in the latter case we assume that $b \neq 0$). Hint: use Vieta's formulas.

Problem 37.* Let β be a root of $\alpha_n x^n + \cdots + \alpha_0$ where $\alpha_0, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Show that $b \in \overline{\mathbb{Q}}$.

Problem 38. a) Define a division-with-remainder procedure for the set of polynomials (in one variable) with coefficients in real numbers, complex numbers and rational numbers.

b) Prove that the unique factorization property holds for the set of polynomials (in one variable) with rational coefficients.

Problem 39. Gauss's lemma for polynomials
Let c_g be the greatest common divisor of the coefficients of $g(x) \in \mathbb{Z}[x]$. Show that, for all nonzero $g_1(x), g_2(x) \in \mathbb{Z}[x]$, we have $c_{g_1 g_2} = c_{g_1} c_{g_2}$.

Problem 40. Can the constructions and the statements of Problem 38 be applied to the set of polynomials with integer coefficients? What about the set of polynomials in two variables with complex coefficients?

Problem 41. Pick an algebraic number α. Let $P_\alpha(x)$ be a monic irreducible polynomial of the least degree such that $P_\alpha(\alpha) = 0$. Prove that if $Q(\alpha) = 0$ for a polynomial $Q(x)$ then P_α divides Q.

Problem 42.* Pick $\alpha, \beta \in \overline{\mathbb{Z}}$. Show that $\alpha \pm \beta \in \overline{\mathbb{Z}}$, $\alpha\beta \in \overline{\mathbb{Z}}$. Hint: use Vieta's formulas.

Problem 43.* Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers. Show that if $\alpha, \beta \in \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ and $\beta \neq 0$ then $\frac{\alpha}{\beta} \in \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$.

Problem 44.* Pick an algebraic integer α. Let $Q(x)$ be a monic irreducible polynomial with rational coefficients of minimal degree such that $Q(\alpha) = 0$. Prove that the coeffecients of $Q(x)$ are integers.

Problem 45.* Let $f(x)$ be a monic polynomial with integer coefficients such that the absolute values of all roots of $f(x)$ in $\mathbb{C}$ are 1. Show that all roots of $f(x)$ are roots of unity.

3 Ideal classes

Definition. Let $\alpha_1, \ldots, \alpha_k$ be algebraic numbers. Set $\widetilde{\mathbb{Q}} := \mathbb{Q}[\alpha_1, \ldots, \alpha_k]$ and $\widetilde{\mathbb{Z}} := \overline{\mathbb{Z}} \cap \widetilde{\mathbb{Q}}$. Note that subsets of $\mathbb{C}$ which are closed under addition, subtraction and multiplication are called *rings*.

Definition. A nonempty subset I of $\widetilde{\mathbb{Z}}$ is called *ideal* if it is closed under addition, subtraction and multiplication by the elements of $\widetilde{\mathbb{Z}}$.

Definition. We say that two nonzero ideals $I, J \subseteq \widetilde{\mathbb{Z}}$ are *equivalent* ($I \sim J$) if there exist nonzero $\alpha, \beta \in \widetilde{\mathbb{Z}}$ such that $(\alpha)I = (\beta)J$.

Problem 46. Check that $\sim$ is an equivalence relation.

Definition. The equivalence classes of ideals are called *ideal classes* of $\widetilde{\mathbb{Z}}$.

Problem 47. Show that the number of ideal classes in $\widetilde{\mathbb{Z}}$ equals 1 if and only if all ideals in $\widetilde{\mathbb{Z}}$ are principal.

Problem 48. Let I_1, I_2, J_1, J_2 be nonzero ideals in $\widetilde{\mathbb{Z}}$ such that $I_1 \sim I_2$ and $J_1 \sim J_2$. Show that $I_1 J_1 \sim I_2 J_2$.

Problem 49. Describe the ideal classes of $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[\sqrt{-6}]$. Can you say anything about the multiplication of these classes?

Problem 50. Let I be a nonzero ideal in $\widetilde{\mathbb{Z}}$ and pick $\alpha \in \widetilde{\mathbb{Z}}$. If $I \subseteq (\alpha)$ then the set $(1/\alpha)I$ is an ideal of $\widetilde{\mathbb{Z}}$.

In the rest of this section we will discuss one the most fundamental statements of Algebraic Number Theory. This statement will play a key role in our proof of a version of the fundamental theorem of arithmetic. The latter proof will be discussed in the subsequent section under the assumption that Theorem 6 is already proven.

Theorem 6. The number of ideal classes in $\widetilde{\mathbb{Z}}$ is finite.

Definition. Consider $x_1, \ldots, x_n \in \widetilde{\mathbb{Q}}$. We say that $\{x_1, \ldots, x_n\}$ is a $\mathbb{Q}$-*basis* of $\widetilde{\mathbb{Q}}$ if every element $\alpha \in \widetilde{\mathbb{Q}}$ can be expressed uniqely in the form

$$m_1 x_1 + \cdots + m_n x_n$$

where $m_1, \ldots, m_n \in \mathbb{Q}$.

Problem 51. Pick an algebraic number α. Show that $\mathbb{Q}[\alpha]$ has a finite $\mathbb{Q}$-basis.

Problem 52. Show that $\widetilde{\mathbb{Q}}$ has a finite $\mathbb{Q}$-basis.

Problem 53. Pick an algebraic number α. Show that there exists a nonzero $n \in \mathbb{Z}$ such that $n\alpha$ is an algebraic integer.

Problem 54. Let $I \subset \widetilde{\mathbb{Z}}$ be a nonzero ideal. Show that there exists a finite set $\alpha_1, \ldots, \alpha_N \in I$ such that every $\alpha \in I$ equals $m_1\alpha_1 + m_2\alpha_2 + \ldots + m_N\alpha_N$ where $m_1, \ldots, m_N \in \mathbb{Z}$ (such $m_1, \ldots, m_N$ need not be unique).

Hint: show that, for a fixed $\mathbb{Q}$-basis of $\widetilde{\mathbb{Q}}$, the coefficients $\alpha \in I$ can't be too small.

Problem 55. Prove that there exists $\alpha_1, \ldots, \alpha_n \in I$ as in Problem 54 such that the respective representation is unique. Hint: use induction on the size of basis.

Definition. We say that $\{\alpha_1, \ldots, \alpha_n\} \subset I$ is an *integer basis* of I if they satisfy the conditions of Problem 55.

Problem 56. Prove that an integer $\mathbb{Q}$-basis of I is a $\mathbb{Q}$-basis of $\widetilde{\mathbb{Q}}$.

Definition. Denote by $\widetilde{\mathbb{Z}}/I$ the equivalence classes of the elements of $\widetilde{\mathbb{Z}}$ with respect to the equivalence relation

$$z_1 \equiv z_2 \mod I \iff z_1 - z_2 \in I.$$

The respective equivalence classes $\widetilde{\mathbb{Z}}/I$ are called *residue classes modulo I*.

Problem 57. Check that residue classes define equivalence classes and that if $\widetilde{\mathbb{Z}} = \mathbb{Z}$ the notion of residue class coincides with congruence classes in modular ariphmetic.

Problem 58. What is the number of elements of $\widetilde{\mathbb{Z}}/I$ for quadratic extensions?

Problem 59. Prove that every $I \neq \{0\}$ contains a nonzero integer.

Problem 60. Prove that the number of elements of $\widetilde{\mathbb{Z}}/I$ is finite.

Problem 61. Pick $\alpha \in \widetilde{\mathbb{Z}}\backslash\{0\}$. Prove that there are only finitely many ideals I such that $\alpha \in I$.

Fix an integer basis $\{\alpha_1, \ldots, \alpha_n$ of $(1) = \widetilde{\mathbb{Z}}\}$. We attach to every $\alpha \in \widetilde{\mathbb{Z}}$ the sequence of integers $(x_1, \ldots, x_n)$ such that $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$.

Definition. We say that such a sequence $(x_1, \ldots, x_n)$ is a *vector*. Set $||\alpha|| = |x_1| + |x_2| + \ldots + |x_n|$.

Problem 62. Prove that there exists $M_1 > 0$ such that, for every $\beta \in \widetilde{\mathbb{Z}}\backslash\{0\}$ there exists an integer basis $\{\beta_1, \ldots \beta_n$ of the ideal $(\beta)\}$ such that $||\beta_i|| < M_1||\beta||$ for all i.

Problem 63. Fix $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$. Show that there exists $c \in \widetilde{\mathbb{Z}}$ such that $||\alpha - c\beta|| < nM_1||\beta||$.

Problem 64. Fix $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$. Prove that there exists a positive integer $m \leq (2n^2M_1+1)^n+1 = M_2$ and a nonzero $c \in \widetilde{\mathbb{Z}}$ such that $||m\alpha - c\beta|| < ||\beta||$.

Problem 65. Pick a nonzero ideal $I \subset \widetilde{\mathbb{Z}}$. Show that there exists $\beta \in I$ such that $M_2!I \subseteq (\beta)$. In particular, $M_2! \in (1/\beta)M_2!I$.

Problem 66. Prove that the number of ideal classes in $\widetilde{\mathbb{Z}}$ is finite.

Fundamental Theorem of Arithmetic
The general case

Theorem 7. The Fundamental Theorem of Arithmetic for algebraic integers.
Let $a_1, \ldots, a_n$ be a collection of algebraic integers such that $\mathbb{Z}[a_1, \ldots, a_n]$ coincides with the integers of $\mathbb{Q}[a_1, \ldots, a_n]$. Then, for every nonzero ideal $I \subset \mathbb{Z}[a_1, \ldots, a_n]$, there exists a unique (up to a permutation of the factors) decomposition of I into the product of prime ideals

$$I = p_1 \cdots p_s \subset \mathbb{Z}[a_1, \ldots, a_n].$$

The proof of Theorem 7 splits into two parts: existence of a decomposition and uniqueness of the decomposition. The first part will be solved in Problem 71; the second part will be solved in Problem 76.

Problem 67. Consider $\alpha \in \widetilde{\mathbb{Q}}$ such that $\alpha I \subseteq I$. Show that $\alpha \in \widetilde{\mathbb{Z}}$.
Hint: use an integer basis of I to reformulate the conditions of the theorem. Then use Gauss's method of solving linear equations to construct a monic polynomial $f(x)$ with integer coefficients such that α is a root of $f(x)$.

Problem 68. Let $I, J \subset \widetilde{\mathbb{Z}}$ be nonzdero ideals such that $JI = I$. Show that $J = (1)$. Hint: use ideas of the proof of Problem 67.

Problem 69. a) Let $I \subset \widetilde{\mathbb{Z}}$ be a nonzero ideal. Show that there are positive integers $m > k$ such that $I^k \sim I^m$.

b) Prove that there exists $\alpha \in \widetilde{\mathbb{Z}}$ such that $I^{m-k} = (\alpha)$.

c) Show that for every nonzero ideal $I \subseteq \widetilde{\mathbb{Z}}$ there exist a nonzero ideal $J \subseteq \widetilde{\mathbb{Z}}$ and nonzero $\alpha \in \widetilde{\mathbb{Z}}$ such that $IJ = (\alpha)$.

Problem 70. Let $I, J \subset \widetilde{\mathbb{Z}}$ be nonzero ideals. Show that J divides I if and only if I is contained in J.

Problem 71. Show that every nonzero ideal $I \subseteq \widetilde{\mathbb{Z}}$ is a product of finitely many prime ideals in $\widetilde{\mathbb{Z}}$.

Problem 72. Let I, J, H be nonzero ideals in $\widetilde{\mathbb{Z}}$ such that I and J are relatively prime. Show that if $JH \subseteq I$ then $H \subseteq I$.

Problem 73. Let $p_1, p_2 \subset \widetilde{\mathbb{Z}}$ be prime ideals and $p_1 \neq p_2$. Show that p_1 and p_2 are relatively prime.

Problem 74. Let $I, J \subset \widetilde{\mathbb{Z}}$ such that I is prime. Show that if $I^m \subseteq J$ then $J = I^k$ for some $k \leq m$.

Problem 75. Show that any two powers of two relatively prime ideals are relatively prime.

Problem 76. Prove that the prime ideal factorisation of I in Problem 71 is unique up to a permutation of the factors.

Fundamental Theorem of Arithmetic and Fermat's Last Theorem

Fix $p > 2$ and denote by ζ_p a complex pth root of unity with $\zeta_p \neq 1$. The goal of this part of the project is to prove the following theorem.

Theorem 8. Assume nonzero integers x, y, z satisfy $x^p + y^p = z^p$ and the number of ideal classes of $\mathbb{Z}[\zeta_p]$ is not divisible by p. Then p divides xyz.

We hope that the participants of the project can prove Theorem 8 if they solve the following problems.

Exercise 25. Prove that $1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0$.

Problem 77. a) Provide a monic polynomial f of degree $p - 1$ with integer coefficients such that $1 - \zeta_p$ is a root of f.
b) Show that p divides all the coefficients of this polynomial (except the first one).
c) Prove that f is irreducible in $\mathbb{Q}[x]$.

Exercise 26. Consider rational numbers $a_0, \dots, a_{p-1}, b_0, \dots, b_{p-1}$. Show that

$$\Sigma_{i=0}^{p-1} a_i \zeta_p^i = \Sigma_{i=0}^{p-1} b_i \zeta_p^i$$

if and only if

$$a_0 - b_0 = a_1 - b_1 = \cdots = a_{p-1} - b_{p-1}.$$

We say that $\gamma \in \overline{\mathbb{Z}}$ is invertible if $\gamma, 1/\gamma \in \overline{\mathbb{Z}}$.

Problem 78. Prove that $\frac{1-\zeta_p^n}{1-\zeta_p}$ is invertible if $p \nmid n$.

Problem 79. Prove the following equalities of ideals $(1-\zeta_p)^p = (p)$.

Exercise 27. Consider $\alpha \in \mathbb{Z}[\zeta_p]$. Show that if $p \mid \alpha$ then $(1-\zeta_p) \mid \alpha$.

Let $\alpha_0, \dots, \alpha = \alpha_0 + \dots + \alpha_{p-1}\zeta_p^{p-1}$.

Problem 80. Prove that all coefficients of the following polynomial are rational:

$$P(a_0, \dots, a_{p-1}; x) := \Pi_{k=1}^{p-1}(x - \Sigma_{i=0}^{p-1} a_i \zeta_p^{ki}).$$

Recall that $P_\alpha(x)$ denotes the monic polynomial of minimal degree with coefficients in $\mathbb{R}$ such that $P_\alpha(\alpha) = 0$.

Problem 81.* Prove that $P(a_0, \dots, a_{p-1}; x) = P_a(x)^d$ for some positive integer d.

Problem 82. Assume $P_\alpha(x)$ has integer coefficients. Then for $1 \le k \le p-1$ and $l \in \mathbb{Z}$, the sum $\Sigma_{i=0}^{p-1} \alpha_i \zeta_p^{ki+l}$ is an algebraic integer.

Problem 83. Assume $P_\alpha(x)$ has integer coefficients. Prove that $p(a_i - a_j) \in \mathbb{Z}$ for all $0 \le i, j \le p-1$.

Problem 84. Show that $1/(1-\zeta_p)$ is not an algebraic integer.

Problem 85. Prove that $\mathbb{Z}[\zeta_p]$ coincides with the set of algebraic integers of $\mathbb{Q}[\zeta_p]$.
Hint: use Exercise 27.

Problem 86. Show that there exists $b \in \mathbb{Z}$ such that $p \mid (\alpha^p - b)$.

Problem 87. a) Prove that $\sqrt{-1} \notin \mathbb{Z}[\zeta_p]$.
b) Consider an odd prime $q \neq p$. Denote by ζ_q a qth root of unity with $q \neq 1$. Show that $\zeta_q \notin \mathbb{Z}[\zeta_p]$.
c) Denote by ζ_{p^2} a root of unity of degree p^2 with $\zeta_{p^2}^p \neq 1$. Show that $\zeta_{p^2} \notin \mathbb{Z}[\zeta_p]$.
d) Find all roots of unity in $\mathbb{Z}[\zeta_p]$.

Problem 88.* Prove that for every invertible element $u \in \mathbb{Z}[\zeta_p]$, there exist $i \in \mathbb{Z}$ and $v \in \mathbb{R}$ such that $u = \zeta_p^i v$.

Let x, y, z, p be as in Theorem 8.

Problem 89. Show that ideals $(x + \zeta_p^i y)$, for $0 \le i \le p-1$, are relatively prime to each other.

Problem 90. Prove Theorem 8.

References

[IR] K. Ireland, M. Rosen, *A classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **84**, Springer-Verlag.

[Mi] J. Milne, *Algebraic number theory*, http://jmilne.org/math/CourseNotes/ANT.pdf.

[C1] K. Conrad, *Factoring in quadratic fields*, http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/quadraticgrad.pdf.

[C2] K. Conrad, *Ideal factorization*, http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/idealfactor.pdf.

[Wa] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer-Verlag, 1996.

[Po] М. Постников, *Теорема Ферма*, Наука, 1978,.

[Go] А. Гончаров, *Арифметика гауссовых чисел*, Журнал "Квант" 12 (1985), http://kvant.mccme.ru/1985/12/.

[SS] В. Сендеров, А. Спивак, *Суммы квадратов и целые гауссовы числа*, Журнал "Квант" 3 (1993), см. также http://kvant.mccme.ru/pdf/1999/03/.

[ZSS] А. Заславский, А. Скопенков, М. Скопенков (редакторы), *Элементы математики в задачах - через олимпиады и кружки к профессии*, 2-ое изд., издательство МЦНМО, 2017.