Обобщение основной теоремы арифметики

Буланкина Вера, Зайцев Тимофей, Фролов Иван,
Петухов Алексей, Салимов Руслан*

Введение

Цель этого проекта — обобщить основную теорему арифметики с целых чисел на какие-то более "продвинутые" объекты. Для решения задач проекта можно (пожалуй, даже рекомендовано) объединяться в команды с другими участниками.

Основная теорема арифметики (Теорема 1 ниже, см. также её обобщения — Теоремы 4, 5, 7) полезна при решении различных уравнений в целых числах. Как мы увидим уже в первой части — примерами могут служить Рождественская теорема Ферма (Теорема 2) и Великая теорема Ферма (Теорема 3) для $n = 3$. Вы можете попробовать доказать их, не читая дальнейшего текста, но не тратьте на это много времени. Возвращайтесь к ним по мере чтения проекта. Также мы увидим, что однозначность разложения на простые множители не обязательно сохраняется для рассматриваемых нами аналогов целых чисел.

Во второй части проекта будет обсуждена версия основной теоремы арифметики, работающая для чисел вида $a + b\sqrt{d}$, где d — фиксированное целое число, a, b — любые целые (для этого нам потребуется понятие идеала). Эти знания мы применим к решению уравнений в целых числах.

В третьей части мы сформулируем более общее утверждение для произвольных алгебраических чисел.

Завершающая часть проекта будет посвящена связи общей теории с Великой теоремой Ферма. Вам предлагается доказать так называемый первый случай Великой теоремы Ферма для регулярных простых чисел. Используя похожие идеи можно доказать, что теорему Ферма и во втором случае для всех n, делящихся на регулярные простые числа p; все простые числа, меньшие 37 — регулярны, см. книги Дж. Милна и М. Постникова. Общее доказательство, придуманное Эндрю Вайлсом, использует существенно другие методы и идеи.

При подготовке проекта мы использовали книги К. Айэрланда и М. Роузена, Дж. Милна, М. Постникова, заметки К. Конрада и википедию. Мы также добавили несколько ссылок [SS, Go, ZSS], которые могут оказаться интересны читателю, желающему лучше познакомиться с этой темой.

Теорема 1. Основная теорема арифметики.
Каждое натуральное число $n > 1$ можно представить в виде $n = p_1 \cdot \ldots \cdot p_k$, где $p_1, \ldots, p_k$ — простые числа, причём такое представление единственно с точностью до порядка следования сомножителей.

Теорема 2. Рождественская теорема Ферма.
Натуральное число n представляется в виде суммы двух квадратов тогда и только тогда, когда все его простые делители вида $4k + 3$ входят в n в четной степени.

Теорема 3. Великая теорема Ферма.
Уравнение $x^n + y^n = z^n$ не имеет решений в натуральных числах при $n > 2$.

*Мы также хотим поблагодарить Михаила Скопенкова, Илью Богданова, Кейта Конрада за существенную помощь в подготовке проекта.

1 Гауссовы числа

Мы хотели обсудить в этой части проекта гауссовы числа — обобщение целых чисел, использующее $\sqrt{-1}$. Если у Вас не получится решить какие-то из задач про гауссовы числа, то попробуйте порешать задачи из других частей проекта и вернуться сюда позднее.

Определение. *Гауссовыми числами* называется множество комплексных чисел вида $a + bi$, где $a, b \in \mathbb{Z}$, $i = \sqrt{-1}$. Будем обозначать множество гауссовых чисел $\mathbb{Z}[i]$.

Задача 1. Докажите, что сумма и произведение любых двух гауссовых чисел — гауссово число.

Для решения следующей задачи потребуется дать более точную формулировку основной теоремы арифметики. Ведь, строго говоря, в старой формулировке она неверна уже для целых чисел: $2 \cdot 3 = 6 = (-2) \cdot (-3)$. Чтобы получить новую формулировку, нам потребуется новое понятие.

Определение. *Делители единицы в* $\mathbb{Z}[i]$ — такие гауссовы числа a, что существует гауссово число b такое, что $ab = 1$. Аналогично определяются делители единицы в $\mathbb{Z}$.

Упражнение 1. Докажите, что в целых числах делители единицы это 1 и -1, а в гауссовых добавляются еще i и $-i$.

Определение. Гауссово число называется *простым*, если в любом его разбиении на 2 множителя ровно один является делителем единицы.

Определение. Два разложения на простые множители называются *одинаковыми*, если в них одинаковое число множителей, и их можно так переставить, чтобы отношение соответствующих простых множителей было делителем единицы. Например, $7 \cdot 3, (-3) \cdot (-7)$ и $(-7i) \cdot (3i)$ — это одинаковые разложения числа 21 в гауссовых числах.

Наша ближайшая цель доказать и научиться применять идущую ниже теорему.

Теорема 4. Основная теорема арифметики для гауссовых чисел.
Любые два разложения гауссова числа на простые множители одинаковы.

Задача 2*. Определите деление с остатком для $\mathbb{Z}[i]$. Используя это, докажите Теорему 4. Подсказка: используйте модуль комплексного числа и графическую (гауссову) интерпретацию комплесных чисел.

Задача 3. Решите в целых числах уравнение $x^2 + 1 = y^n$.

Задача 4. а) Пусть $p \in \mathbb{Z}$ – простое число. Докажите, что число p является простым гауссовым числом тогда и только тогда, когда $p + 1$ делится на 4.

б) Если $n, m \in \mathbb{Z}$ представляются в виде $a^2 + b^2$, где a и $b \in \mathbb{Z}$, то mn представляется в виде суммы двух квадратов.

в) Докажите Рождественскую теорему Ферма (Теорему 2).

Задача 5. Как по разложению целого числа на (гауссовы) простые множители понять, сколькими способами оно раскладывается в сумму двух квадратов?

Числа Эйзенштейна

В этой главе мы постараемся помочь участникам решить следующую задачу.

Задача 6*. Докажите Теорему 3 для $n = 3$, используя формулу

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

Для этого мы введём несколько новых определений и рассмотрим несколько вспомогательных задач. Обозначим через ξ какой-то комплексный корень третьей степени из 1, не равный 1.

Упражнение 2. Докажите, что $\xi = \frac{-1\pm\sqrt{-3}}{2}$.

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

Определение. Число $a \in \mathbb{Z}[\xi]$ *делится* на $b \in \mathbb{Z}[\xi]$ тогда и только тогда, когда существует такое $c \in \mathbb{Z}[\xi]$, что $a = bc$.

Делители единицы в $\mathbb{Z}[\xi]$ определяются аналогично делителям единицы в $\mathbb{Z}$ и $\mathbb{Z}[i]$.

Определение. Число $\alpha \in \mathbb{Z}[\xi]$ *составное*, если $\alpha = \beta\gamma$, где β и $\gamma \in \mathbb{Z}[\xi]$ не являются делителями единицы. Число $\alpha \in \mathbb{Z}[\xi]$ называется *простым*, если α не составное и не делитель единицы.

Задача 7. Определите деление с остатком для $\mathbb{Z}[\xi]$. Используя его, сформулируйте и докажите, основную теорему арифметики для $\mathbb{Z}[\xi]$.

Задача 8. Найдите все делители единицы в $\mathbb{Z}[\xi]$.

Квадратичные расширения

В этой секции мы введём общие квадратичные расширения, как обобщения гауссовых чисел и чисел Эйзенштейна.

Определение. Для произвольного набора комплексных чисел $a_1, ..., a_n$ обозначим через $\mathbb{Z}[a_1, ..., a_n]$ множество всех комплексных чисел, получаемых из целых чисел ($\mathbb{Z}$), а также $a_1, ..., a_n$ сложением, вычитанием и умножением.

Аналогично определяется $\mathbb{Q}[a_1, ..., a_n]$. Мы рассматриваем такие множества $\mathbb{Z}[a_1, ..., a_n]$ как аналоги целых чисел (их элементы можно складывать, умножать и вычитать).

Фиксируем целое число $d \neq 1$, не делящееся на квадраты простых чисел.

Комментарий. Два важных примера: $d = -3$ и $d = 2$. Может оказаться полезным продумать и проанализировать все определения этой секции сначала для этих двух примеров, а потом для общего случая.

Упражнение 3. а) Докажите, что

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

б) Докажите, что если $a, b \in \mathbb{Q}[\sqrt{d}]$ и $b \neq 0$, то $\frac{a}{b} \in \mathbb{Q}[\sqrt{d}]$.

Определение. *Целыми числами в* $\mathbb{Q}[\sqrt{d}]$ называются $\alpha \in \mathbb{Q}[\sqrt{d}]$, которые являются корнями уравнений вида $x^2 + px + q$, где $p, q \in \mathbb{Z}$.

Упражнение 4. Является ли ξ целым в $\mathbb{Q}[\sqrt{-3}]$? Является ли $\frac{1+i}{2}$ целым в $\mathbb{Q}[i]$?

Положим $\omega = \sqrt{d}$ если $d \equiv 2, 3 \bmod 4$, и $\omega = \frac{\sqrt{d}+1}{2}$ если $d \equiv 1 \bmod 4$.

Для $\mathbb{Z}[\sqrt{d}]$ единственность разложения на простые множители не всегда имеет место, но, как мы надеемся, вы сможете доказать некоторую её модификацию. Для каждого числа $\alpha = a + b\sqrt{d}$, где $a, b \in \mathbb{Q}$, определим сопряженное число $\bar{\alpha} = a - b\sqrt{d}$, норму $N(\alpha) = \alpha\bar{\alpha}$ и след $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$.

Упражнение 5. Докажите, что $\overline{a+b} = \bar{a} + \bar{b}$ и $\overline{ab} = \bar{a}\bar{b}$.

Упражнение 6. а) Докажите, что $\alpha \in \mathbb{Q}[\sqrt{d}]$ — корень многочлена $x^2 - \mathrm{Tr}(\alpha)x + N(\alpha)$.

б) Докажите что $\alpha \in \mathbb{Q}[\sqrt{d}]$ цело тогда и только тогда когда $N(\alpha) \in \mathbb{Z}$ и $\mathrm{Tr}(\alpha) \in \mathbb{Z}$.

Задача 9. Докажите, что целые числа в $\mathbb{Q}[\sqrt{d}]$ совпадают с $\mathbb{Z}[\omega]$.

Делители единицы в $\mathbb{Z}[\xi]$ определяются аналогично делителям единицы в $\mathbb{Z}$ и $\mathbb{Z}[i]$.

Упражнение 7. Докажите, что для $\gamma \in \mathbb{Z}[\omega]$ выполнено $N(\gamma) = \pm 1$ тогда и только тогда, когда γ — делитель единицы.

Определение. Число $a \in \mathbb{Z}[\omega]$ *делится* на $b \in \mathbb{Z}[\omega]$ тогда и только тогда, когда существует такое $c \in \mathbb{Z}[\omega]$, что $a = bc$.

Определение. Число $\alpha \in \mathbb{Z}[\omega]$ *составное*, если $\alpha = \beta\gamma$, где β и $\gamma \in \mathbb{Z}[\omega]$ не являются делителями единицы. Число $\alpha \in \mathbb{Z}[\omega]$ называется *простым*, если α не составное и не делитель единицы.

Упражнение 8. Докажите, что если для числа $\gamma \in \mathbb{Z}[\omega]$ число $|N(\gamma)| \in \mathbb{Z}$ просто, то γ просто. Докажите что обратное утверждение неверно в $\mathbb{Z}[\sqrt{3}]$.

Упражнение 9. Докажите, что если $\gamma \in \mathbb{Z}[\omega]\backslash 0$ не делитель единицы, то γ равно произведению каких-то простых элементов $\mathbb{Z}[\omega]$.

Задача 10. Проверьте, что все множители в разложении

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

простые.

Задача 11. Определите деление с остатком для а) $\mathbb{Z}[\sqrt{-2}]$; б) $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Используя его, сформулируйте и докажите основную теорему арифметики для а) и б).

Задача 12. Найдите все делители единицы в

а) $\mathbb{Z}[\sqrt{-1}]$, б) $\mathbb{Z}[\sqrt{-d}]$, где $d \geq 1$, в) $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, г*) $\mathbb{Z}[\sqrt{2}]$.

Задача 13. Выполнена ли основная теорема арифметики для

а) $\mathbb{Z}[\sqrt{2}]$, б) $\mathbb{Z}[\sqrt{-3}]$, в) $\mathbb{Z}[\sqrt{3}]$, г) $\mathbb{Z}[\sqrt{-5}]$, д) $\mathbb{Z}[\sqrt{5}]$, е) $\mathbb{Z}[\sqrt{10}]$, ж) $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$,
з) $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, и) $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, к*) $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$?

Задача 14. При каких комплексных ξ сумма и произведение любых двух чисел вида $a + b\xi$, где a и $b \in \mathbb{Z}$, снова имеет такой же вид?

Задача 15*. Решите в целых числах уравнения
а) $3^n = k^2 + 2$ б) $2^n = k^2 + 7$.

Идеалы

В этой и последующих главах намечен подход к решению следующих трудных задач.

Задача 16. Решите в целых числах уравнения
а) $x^2+5=y^3$, б) $x^2+2x+7=y^3$ в) $5x^2+1=y^3$, г) $6x^2-12x+7=y^3$, д) $x^2-6=y^3$.

Определение. Непустое подмножество I множества целых чисел называется *идеалом*, если оно замкнуто относительно сложения, вычитания и умножения на целые числа:

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

Познавательная минутка. Идеалы были придуманы Юлиусом Дедекиндом как формализация "идеальных чисел", придуманных Э. Куммером, как считается, при размышлениях о Великой теоремы Ферма: можно говорить о том, делится или не делится данное число на "идеальное число" вне зависимости от того каков статус этого числа. Аналогичная идея стоит за определением дедекиндова сечения рациональных чисел.

Упражнение 10. а) Докажите, что всякий идеал содержит 0. б) Докажите, что если $a\in I$, то $-a\in I$. в) Докажите, что множество чётных чисел — идеал. г) Докажите, что множество чисел вида $2018m, m\in\mathbb{Z}$, — идеал.

Упражнение 11. Докажите, что пересечение идеалов — идеал.

Здесь и далее мы обозначаем через $(a_1,...,a_n)$ наименьший идеал, содержащий числа $a_1,...,a_n\in\mathbb{Z}$ (т.е. пересечение всех идеалов, содержащих числа $a_1,...,a_n\in\mathbb{Z}$).

Задача 17. а) Пусть a,b — это два взаимнопростых числа. Докажите, что $(a,b)=(1)=\mathbb{Z}$.
б) Докажите, что $(a,b)=(d)$, где $a,b\in\mathbb{Z}$, d есть наибольший общий делитель a,b.
в) Докажите, что любой идеал I в $\mathbb{Z}$ совпадает с (d) для какого-то числа $d\in\mathbb{Z}$.

Как в предудыщем разделе, считаем, что $\omega=\sqrt{d}$ если $d\equiv 2,3 \bmod 4$, и $\omega=\frac{\sqrt{d}+1}{2}$ если $d\equiv 1 \bmod 4$. Идеал в $\mathbb{Z}[\omega]$ определяется абсолютно точно так же, как и идеал в $\mathbb{Z}$ ($\mathbb{Z}$ заменяется на $\mathbb{Z}[\omega]$). Точно так же всякий набор $a_1,...,a_n\in\mathbb{Z}[\omega]$ определяет идеал $(a_1,...,a_n)$ в $\mathbb{Z}[\omega]$. В частности, любой элемент $a\in\mathbb{Z}[\omega]$ определяет идеал (a).

Упражнение 12. Докажите, что $(\alpha)=(\beta)$ тогда и только когда $\alpha/\beta\in\mathbb{Z}[\omega]$ и $\beta/\alpha\in\mathbb{Z}[\omega]$ (т.е. α/β — делитель единицы в $\mathbb{Z}[\omega]$).

Упражнение 13. Пусть $a,x,y\in\mathbb{Z}$. Докажите, что $x+y\omega\in(a)$ тогда и только тогда когда x и y делятся на a.

Определение. Идеал, имеющий вид (a) для какого-то $a\in\mathbb{Z}[\omega]$, называется *главным*. Как мы видели в Задаче 17, все идеалы в $\mathbb{Z}$ главные.

Задача 18. Докажите, что идеал $(2,\sqrt{-14})$ не является главным в $\mathbb{Z}[\sqrt{-14}]$.

Задача 19. Докажите, что для всякого идеала I в $\mathbb{Z}[\omega]$ существуют $\alpha,\beta\in\mathbb{Z}[\omega]$ такие, что

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

Определение. Для двух идеалов $I,J\in\mathbb{Z}[\omega]$ положим

$$I+J:=\{i_1+i_2: i_1\in I_1, i_2\in J\}, \quad \bar{I}:=\{\bar{i}: i\in I\},$$

$$IJ:=\{i_1j_1+...+i_kj_k: i_1,...,i_k\in I, j_1,...,j_k\in J\}.$$

Упражнение 14. Посчитайте в $\mathbb{Z}[\sqrt{-14}]$ произведение идеалов $I=(5+\sqrt{-14},2+\sqrt{-14})$ и $J=(4+\sqrt{-14},2-\sqrt{-14})$.

Упражнение 15. Проверьте равенства

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

где

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

Упражнение 16. Опишите $(20)(18)$, $(20) + (18)$, $(20) \cap (18)$ в $\mathbb{Z}[\omega]$ для всех допустимых значений d ($d \neq 1$, d не делится на квадраты простых чисел).

Упражнение 17. Докажите, что $I+J, \bar{I}, IJ$ являются идеалами в $\mathbb{Z}[\omega]$ для любых идеалов $I, J \subset \mathbb{Z}[\omega]$.

2 Основная теорема арифметики: квадратичный случай

Все рассматриваемые в этой главе идеалы, являются идеалами в $\mathbb{Z}[\omega]$ для подходящего d. В Задаче 10 мы убедились, что однозначность разложения на множители в самом очевидном смысле теряется для $\mathbb{Z}[\sqrt{-14}]$

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

С другой стороны, по Упражнению 15:

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

где

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

Т.е. $(15) = p_1 p_2 p_3 p_4$. Идеалы p_1, p_2, p_3, p_4 играют роль простых сомножителей, см. Задачу 23, а разложение $(15) = p_1 p_2 p_3 p_4$ единственно с точностью до перестановки множителей в соответствии со следующей теоремой.

Теорема 5. Основная теорема арифметики для квадратичных расширений.
Для каждого идеала $I \subset \mathbb{Z}[\omega]$ существует единственное с точностью до перестановки множителей разложение в произведение простых идеалов

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

(Определение простого идеала идёт ниже, Определение 2.)

В Теореме 5 есть две существенные части: существование такого разложения и его единственность. Первая доказывается в Задаче 24, вторая — в Задаче 27. В качестве примера задачи, которые можно решить, используя эту теорему, мы предлагаем Задачу 16, см. также завершающий листок про теорему Ферма.

Следствие. Для каждого $m \in \mathbb{Z}[\omega]$ существует единственное с точностью до перестановки множителей разложение идеала (m) в произведение простых идеалов $p_1, ..., p_s \subset \mathbb{Z}[\omega]$.

Доказательство можно разбить на цепочку утверждений, каждое из которых условно просто. В общем и целом схема доказательства похожа на схему доказательства основной теоремы арифметики для целых чисел.

Задача 20. Для всякого набора $a_1, ..., a_n \in \mathbb{Z}[\omega]$ докажите, что

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

Подсказка: разберите сначала случай идеала, порождённого 2 элементами.

Определение. Будем говорить что идеал I делится на идеал J, если $I = JH$, где H — какой-то идеал в $\mathbb{Z}[\omega]$.

Задача 21. Для любых двух идеалов I, J в $\mathbb{Z}[\omega]$, докажите, что I делится на J тогда и только тогда, когда I содержится в J.
Подсказка: воспользуйтесь предыдущей задачей.

Упражнение 18. Используя Задачу 20 докажите, что, для всякого идеала I в $\mathbb{Z}[\omega]$, существует неотрицательное целое число $N(I)$, такое что $I\bar{I} = (N(I))$.

Задача 22. Докажите, что идеал H делит I и J тогда и только тогда, когда он делит $I + J$.

Упражнение 19. Докажите что $N((a)) = |N(a)|$ для всех $a \in \mathbb{Z}[\omega]$.

Упражнение 20. Докажите что $N(I)N(J) = N(IJ)$ для любых двух идеалов I, J.

Упражнение 21. Докажите, что если идеал I делит идеал J, то $N(I)$ делит $N(J)$. Верно ли обратное?

Упражнение 22. Докажите, что $N(I) = 1$ тогда и только тогда, когда $I = (1)$.

Определение. Идеал I в $\mathbb{Z}[\omega]$ называется *простым*, если он делится ровно на два идеала: себя и (1).

Упражнение 23. Докажите, что идеал I прост тогда и только тогда, когда он максимален, т.е. когда единственный идеал больший его равен (1).

Два идеала называются *взаимнопростыми*, если $I + J = (1)$.

Упражнение 24. Докажите, что любые два различных простых идеала взаимнопросты.

Задача 23. Проверьте, что данные идеалы просты в $\mathbb{Z}[\sqrt{-14}]$:

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

Задача 24. Докажите, что любой ненулевой идеал I в $\mathbb{Z}[\omega]$ разлагается в произведение простых идеалов.

Задача 25. Докажите, что если два идеала I, J в $\mathbb{Z}[\omega]$ взаимнопросты и существует третий идеал H такой, что I делит HJ, то I делит H.

Задача 26. а) Пусть $a \in \mathbb{Z}[\omega]\backslash 0$ и $(a)I = (a)J$ для двух идеалов $I, J \subset \mathbb{Z}[\omega]$. Докажите, что тогда $I = J$.
б) Пусть для некоторых идеалов I, H, J верно что $H \neq (0)$ и $HI = HJ$. Докажите, что тогда $I = J$.

Задача 27. Докажите, что разложение на простые множители из Задачи 24 единственно с точностью до перестановки множителей.

Простые идеалы и простые числа

Задача 28. а) Докажите, что любой идеал в $\mathbb{Z}[\sqrt{-5}]$ либо главный, либо имеет вид $((1 + \sqrt{-5})a, 2a)$ для некоторого $a \in \mathbb{Q}[\sqrt{-5}]$.
б) Докажите, что любой идеал в $\mathbb{Z}[\sqrt{-6}]$ либо главный, либо имеет вид $(\sqrt{-6}a, 2a)$ для некоторого $a \in \mathbb{Q}[\sqrt{-6}]$.

Задача 29. Докажите, что любой ненулевой идеал в $\mathbb{Z}[\omega]$ содержит ненулевое целое число.

Задача 30. Докажите, что любой простой идеал I в $\mathbb{Z}[\omega]$ содержит единственное простое число $p \in \mathbb{Z}, p > 0$.

Задача 31. Докажите, что для всякого простого идеала I либо число $p = N(I)$ простое, либо оно квадрат простого числа $p > 0$.

Задача 32. Докажите, что простые числа p, определённые в двух предыдущих задачах, совпадают.

Задача 33. Докажите, что для всякого простого числа $p \in \mathbb{Z}$ или идеал $(p) \subset \mathbb{Z}[\omega]$ прост, или он равен произведению двух (не всегда различных) сопряжённых простых идеалов.

Задача 34. Пусть $P_\omega(x)$ — это приведённый квадратный трёхчлен с целыми коэффициентами, для которого $P_\omega(\omega) = 0$. Докажите, что в условиях предыдущей задачи первый случай имеет место тогда и только тогда, когда уравнение $P_\omega(x) = 0$ не имеет решений по модулю p.

Алгебраические числа

В этой части мы бы хотим обсудить понятие алгебраического числа, а также те задачи, которые при этом возникают. В общем и целом этот материал часто присутствует в университетских курсах по теории чисел, но может быть усвоен и в старших классах школы.

Определение. Комплексное число $\alpha \in \mathbb{C}$ называется *алгебраическим*, если оно является корнем ненулевого многочлена с рациональными коэффициентами. Алгебраическое число $\alpha \in \mathbb{C}$ называется *целым*, если оно является корнем приведённого многочлена с целыми коэффициентами. Множество алгебраических чисел обозначается $\bar{\mathbb{Q}}$. Множество целых алгебраических чисел обозначается $\bar{\mathbb{Z}}$.

Задача 35. Если для рационального числа a верно, что $a \in \bar{\mathbb{Z}}$, то $a \in \mathbb{Z}$.

Задача 36.* Докажите, что если $a, b \in \bar{\mathbb{Q}}$, то и $a \pm b \in \bar{\mathbb{Q}}$, $ab \in \bar{\mathbb{Q}}$, $a/b \in \bar{\mathbb{Q}}$ (в последнем случае считаем, что $b \neq 0$). Подсказка: попробуйте воспользоваться теоремой Виета.

Задача 37.* Пусть b — это корень уравнения $a_n x^n + ... + a_0$, где $a_0, ..., a_n \in \bar{\mathbb{Q}}$. Докажите, что $b \in \bar{\mathbb{Q}}$.

Задача 38. а) Определите деление с остатком в множестве многочленов от одной переменной с комплексными, вещественными и рациональными коэффициентами.

б) Докажите единственность разложения на простые множители в множестве многочленов с рациональными коэффициентами.

Задача 39. (Лемма Гаусса) Пусть c_g — наибольший общий делитель коэффициентов многочлена $g \in \mathbb{Z}[x]$. Тогда для любых $g_1(x), g_2(x) \in \mathbb{Z}[x]$ выполнено $c_{g_1 g_2} = c_{g_1} c_{g_2}$.

Задача 40. Какие из конструкций и утверждений Задачи 38 применимы к многочленам с целыми коэффициентами от одной переменной? К многочленам с рациональными коэффициентами от двух переменных?

Задача 41. Пусть a — алгебраическое число. Пусть $P_a(x)$ — приведённый ненулевой многочлен наименьшей степени с рациональными коэффициентами, для которого $P_a(a) = 0$. Докажите, что если $Q(a) = 0$ для какого-то многочлена $Q(x)$, то Q делится на P_a.

Задача 42.* Докажите, что если $a, b \in \bar{\mathbb{Z}}$, то и $a \pm b \in \bar{\mathbb{Z}}$, $ab \in \bar{\mathbb{Z}}$.
Подсказка: попробуйте воспользоваться теоремой Виета.

Задача 43.* Пусть $a_1, ...a_n$ — алгебраические числа. Докажите, что если $a, b \in \mathbb{Q}[a_1, ..., a_n]$ и $b \neq 0$, то $\frac{a}{b} \in \mathbb{Q}[a_1, ..., a_n]$.

Задача 44.* Пусть a — это целое алгебраическое число. Пусть $Q(x)$ — это приведённый многочлен наименьшей степени с рациональными коэффициентами, для которого $Q(a) = 0$. Докажите, что $Q(x)$ имеет целые коэффициенты.

Задача 45.* Пусть есть приведенный многочлен с целыми коэффициентами, такой что все его корни по модулю равны 1. Докажите, что тогда все его корни есть корни из 1.

3 Классы идеалов

Определение. Для алгебраических $\alpha_1, \ldots, \alpha_k$ положим $\widetilde{\mathbb{Q}} := \mathbb{Q}[a_1, ..., a_k]$ и $\widetilde{\mathbb{Z}} := \bar{\mathbb{Z}} \cap \widetilde{\mathbb{Q}}$. Отметим, что любое подмножество в $\mathbb{C}$, замкнутое относительно сложения, вычитания и умножения называется *кольцом*.

Определение. Непустое подмножество в $\widetilde{\mathbb{Z}}$ называется *идеалом*, если оно замкнуто относительно сложения, вычитания и умножения на элементы $\widetilde{\mathbb{Z}}$.

Определение. Назовем идеалы $I, J \subseteq \widetilde{\mathbb{Z}}$ *эквивалентными*, если существуют ненулевые $\alpha, \beta \in \widetilde{\mathbb{Z}}$, такие что $(\alpha)I = (\beta)J$. Эквивалентность идеалов будем обозначать $I \sim J$.

Задача 46. Проверьте, что $\sim$ является отношением эквивалентности.

Определение. Классы эквивалентности идеалов будем называть *классами идеалов*.

Задача 47. Докажите, что число классов идеалов равно 1 тогда и только тогда, когда все идеалы – главные.

Задача 48. Проверьте, что если $I_1 \sim I_2$ и $J_1 \sim J_2$, то $I_1 J_1 \sim I_2 J_2$.

Задача 49. Опишите классы идеалов в $\mathbb{Z}[\sqrt{-5}]$ и $\mathbb{Z}[\sqrt{-6}]$. Как в них устроено умножение идеалов?

Задача 50. Докажите, что если $I \subseteq (\alpha)$, то множество $(1/\alpha)I$ – идеал в $\widetilde{\mathbb{Z}}$.

В следующей серии задач обсуждается одно из фундаментальных утверждений алгебраической теории чисел. Это утверждение будет играть ключевую роль в доказательстве общего случая основной теоремы арифметики. Само доказательство обсуждается в следующей части проекта и может сдаваться в предположении что Теорема 6 уже доказана.

Теорема 6. Число классов идеалов конечно.

Определение. Назовем набор чисел $x_1, ..., x_n \in \widetilde{\mathbb{Q}}$ *базисом* над $\mathbb{Q}$, если любой элемент $a \in \widetilde{\mathbb{Q}}$ единственным образом представляется в виде $m_1 x_1 + ... + m_n x_n$, где $m_1, ..., m_n \in \mathbb{Q}$.

Задача 51. Если α — алгебраическое, то в $\mathbb{Q}[\alpha]$ существует конечный $\mathbb{Q}$-базис.

Задача 52. Докажите, что в $\widetilde{\mathbb{Q}}$ существует конечный базис над $\mathbb{Q}$.

Задача 53. Для любого алгебраического α существует такое ненулевое $n \in \mathbb{Z}$, что $n\alpha$ — целое алгебраическое число.

Задача 54. Пусть I – идеал в $\widetilde{\mathbb{Z}}$. Докажите, что существует конечный набор $\alpha_1, \ldots, \alpha_N \in I$, такой что любое $\alpha \in I$ представимо в виде $m_1\alpha_1 + m_2\alpha_2 + \ldots + m_N\alpha_N$ с целыми $m_1, \ldots, m_N$ (не обязательно единственным образом).

Подсказка: докажите, что для фиксированного базиса в $\widetilde{\mathbb{Q}}$ коэффициенты $\alpha \in I$ не могут быть слишком маленькими.

Задача 55. Докажите, что существует конечный набор $\alpha_1, \ldots, \alpha_n \in I$, для которого такое представление единственно.
Подсказка: индукция по размеру базиса.

Определение. Такие наборы будем называть *целым базисом* идеала I.

Задача 56. Докажите, что любой целый базис I является $\mathbb{Q}$-базисом $\widetilde{\mathbb{Q}}$.

Определение. Обозначим $\widetilde{\mathbb{Z}}/I$ – множество классов эквивалентности элементов $\widetilde{\mathbb{Z}}$ по отношению эквивалентности

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

Элементы $\widetilde{\mathbb{Z}}/I$ будем называть *вычетами по модулю* I.

Задача 57. Проверьте, что это действительно отношение эквивалентности, и при $\widetilde{\mathbb{Z}} = \mathbb{Z}$ – определение вычета совпадает со стандартным.

Задача 58. Чему равно количество элементов в $\widetilde{\mathbb{Z}}/I$ для квадратичных расширений?

Задача 59. Докажите, что I содержит ненулевое целое число.

Задача 60. Докажите, что число элементов в $\widetilde{\mathbb{Z}}/I$ конечно.

Задача 61. Докажите, что существует только конечное число идеалов, содержащих данное $\alpha \in \widetilde{\mathbb{Z}}$.

Зафиксируем целый базис $\alpha_1, \ldots, \alpha_n$ для идеала $(1) = \widetilde{\mathbb{Z}}$ и сопоставим каждому $\alpha \in \widetilde{\mathbb{Z}}$ набор целых чисел $(x_1, \ldots, x_n)$, таких что $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$. Положим

$$||\alpha|| = |x_1| + |x_2| + \ldots + |x_n|.$$

Задача 62. Пусть $\{\beta_1, ..., \beta_m\}$ — какой-то целый базиса идеала I. Докажите, что набор $\{\beta_1, ..., \beta_m\}$ является $\mathbb{Q}$-базисом в $\widetilde{\mathbb{Q}}$.

Задача 63. Докажите, что существует такое натуральное M_1, что для любого ненулевого $\beta \in \widetilde{\mathbb{Z}}$ можно выбрать целый базис $\beta_1, \ldots \beta_n$ идеала (β), такой что $||\beta_i|| < M_1||\beta||$ для всех i.

Задача 64. Докажите, что для любых $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$ существует $c \in \widetilde{\mathbb{Z}}$, такое что

$$||\alpha - c\beta|| < nM_1||\beta||.$$

Задача 65. Докажите, что для любых $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$ существуют натуральное

$$m \leq (2n^2M_1 + 1)^n + 1 = M_2$$

и $c \in \widetilde{\mathbb{Z}}$, такие что $||m\alpha - c\beta|| < ||\beta||$.

Задача 66. Докажите, что для любого идеала I существует $\beta \in I$, такое что $M_2!I \subseteq (\beta)$. В частности, $M_2! \in (1/\beta)M_2!I$.

Задача 67. Докажите, что число классов идеалов — конечно.

Основная теорема арифметики. Общий случай

Теорема 7. Основная теорема арифметики для целых алгебраических чисел.
Пусть $a_1, ..., a_n$ — набор целых алгебраических чисел, такой что $\mathbb{Z}[a_1, ..., a_n]$ совпадает с подмножеством целых алгебраических чисел в $\mathbb{Q}[a_1, ..., a_n]$. Тогда для каждого идеала $I \subset \mathbb{Z}[a_1, ..., a_n]$ существует и единственное с точностью до перестановки множителей разложение в произведение простых идеалов

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

В Теореме 7 есть две существенные части: существование такого разложения и его единственность. Первая рассматривается в Задаче 73, вторая — в Задаче 78.

Задача 68. Пусть для некоторого $\alpha \in \widetilde{\mathbb{Q}}$ выполнено $\alpha I \subseteq I$. Докажите, что $\alpha \in \widetilde{\mathbb{Z}}$.
Подсказка: в целом базисе I запишите условие того, что $\alpha I \subseteq I$, и, вспомнив метод Гаусса решения системы линейных уравнений, постройте приведенный многочлен с целыми коэффициентами, корнем которого является α.

Задача 69. Пусть для некоторых идеалов I, J выполнено $JI = I$. Докажите, что $J = (1)$. Подсказка: действуйте по аналогии с предыдущей задачей.

Задача 70. Докажите, что для любого идеала I существуют натуральные $m > k$, такие что $I^k \sim I^m$.

Задача 71. Докажите, что существует $\alpha \in \widetilde{\mathbb{Z}}$, такое что $I^{m-k} = (\alpha)$. В частности, для всякого идеала $I \subseteq \widetilde{\mathbb{Z}}$ существует идеал $J \subseteq \widetilde{\mathbb{Z}}$ и $\alpha \in \widetilde{\mathbb{Z}}$, такие что $IJ = (\alpha)$.

Задача 72. Докажите, что для любых двух идеалов I, J в $\widetilde{\mathbb{Z}}$ — идеал I делится на J тогда и только тогда, когда I содержится в J.

Задача 73. Докажите, что любой идеал $I \subseteq \widetilde{\mathbb{Z}}$ представим в виде произведения конечного набора простых идеалов.

Задача 74. Докажите, что если идеалы I, J взаимнопросты и $JH \subseteq I$, то $H \subseteq I$.

Задача 75. Докажите, что любые два различных простых идеала взаимно просты.

Задача 76. Докажите, что если I — простой идеал, и $I^m \subseteq J$, то $J = I^k$ для целого $k \leq m$.

Задача 77. Докажите, что степени двух различных простых идеалов взаимно просты.

Задача 78. Докажите однозначность разложения на множители в Задаче 73.

Основная теорема арифметики и Великая Теорема Ферма

Фиксируем простое число $p > 2$ и обозначим через ζ_p комплексный корень p-ой степени из 1. Цель данного раздела доказать следующую теорему.

Теорема 8. Пусть целые числа x, y, z таковы что $x^p + y^p = z^p$ и число классов $\mathbb{Z}[\zeta_p]$ не делится на p. Тогда xyz делится на p.

Мы надеемся, что участники проекта смогут доказать Теорему 8, после того, как прорешают идущие ниже задачи.

Упражнение 25. Докажите, что $1 + \zeta_p + \zeta_p^2 + .. + \zeta_p^{p-1} = 0$.

Задача 79. Найдите приведённый многочлен с целыми коэффициентами степени $p - 1$, корнем которого является $1 - \zeta_p$.

Задача 80. Докажите, что все коэффициенты этого многочлена (кроме первого) делятся на p и что этот многочлен неприводим.

Упражнение 26. Докажите, что $\Sigma_{i=0}^{p-1} a_i \zeta_p^i = \Sigma_{i=0}^{p-1} b_i \zeta_p^i$ для рациональных чисел

$$a_0, .., a_{p-1}, b_0, ..., b_{p-1}$$

если и только если

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

Напомним что число γ называется делителем единицы, если γ и $1/\gamma$ — целые алгебраические числа.

Задача 81. Докажите, что $\frac{1-\zeta_p^n}{1-\zeta_p}$ — делитель единицы, если n не делится на p.

Задача 82. Докажите, что $(1 - \zeta_p)^p = (p)$ (равенство идеалов).

Упражнение 27. Докажите, что если $a \in \mathbb{Z}[\zeta_p]$ делится на p, то оно делится на $1 - \zeta_p$.

Пусть числа $a_0, ..., a_{p-1}$ рациональны, $a = a_0 + .. + a_{p-1}\zeta_p^{p-1}$.

Задача 83. Докажите, что все коэффициенты многочлена

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

рассматриваемого как многочлен от x, также рациональны.

Напомним, что для всякого алгебраического числа a через $P_a(x)$ обозначается приведённый многочлен наименьшей степени, для которого $P_a(a) = 0$.

Задача 84.* Докажите, что $P(a_0, ..., a_{p-1}; x) = P_a(x)^d$, где d — целое положительное число.

Задача 85. Если многочлен $P_a(x)$ имеет целые коэффициенты, то для любых целых чисел $1 \leq k \leq p-1, l \in \mathbb{Z}$, число $\Sigma_{i=0}^{p-1} a_i \zeta_p^{ki+l}$ является целым алгебраическим.

Задача 86. Пусть многочлен $P_a(x)$ имеет целые коэффициенты. Докажите, что тогда $p(a_i - a_j) \in \mathbb{Z}$ для всех $0 \leq i, j \leq p-1$.

Задача 87. Докажите, что число $1/(1 - \zeta_p)$ не является целым алгебраическим.

Задача 88. Докажите что $\mathbb{Z}[\zeta_p]$ совпадает с множеством целых алгебраических чисел в $\mathbb{Q}[\zeta_p]$.
Подсказка: постарайтесь найти применение Упражнению 27.

Задача 89. Докажите, что для любого элемента $a \in \mathbb{Z}[\zeta_p]$ существует $b \in \mathbb{Z}$, такое что $a^p - b$ делится на p.

Задача 90. а) Докажите, что $\sqrt{-1} \notin \mathbb{Z}[\zeta_p]$.
б) Пусть $q \neq p, q \neq 2$ простое число, а ζ_q — комплексный корень q-ой степени из 1. Докажите, что $\zeta_q \notin \mathbb{Z}[\zeta_p]$.
в) Пусть ζ_{p^2} — корень p^2-ой степени из 1, не являющийся корнем p-ой степени из 1. Докажите, что $\zeta_{p^2} \notin \mathbb{Z}[\zeta_p]$.
г) Найдите все корни из 1 в $\mathbb{Z}[\zeta_p]$.

Задача 91.* Докажите, что любой делитель единицы в $u \in \mathbb{Z}[\zeta_p]$ представляется в виде $\zeta_p^i v$, где $i \in \mathbb{Z}$, $v \in \mathbb{R}$.

Пусть x, y, z, p как в теореме 8.

Задача 92. Докажите что идеалы $(x + \zeta_p^i y)$ попарно взаимно просты при $0 \leq i \leq p-1$.

Задача 93. Докажите Теорему 8.

Список литературы

[IR] К. Айерлэнд, М. Роузен, *Классическое введение в современную теорию чисел*, Мир, 1987.

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

[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.

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

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

[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.