МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ МГУ ИМЕНИ М.В. ЛОМОНОСОВА

ФОНД ВОЛЬНОЕ ДЕЛО

teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ

АЛГЕБРА. ЧАСТЬ I

ТИМАШЕВ
ДМИТРИЙ АНДРЕЕВИЧ

МЕХМАТ МГУ

КОНСПЕКТ ПОДГОТОВЛЕН СТУДЕНТАМИ, НЕ ПРОХОДИЛ ПРОФ. РЕДАКТУРУ И МОЖЕТ СОДЕРЖАТЬ ОШИБКИ. СЛЕДИТЕ ЗА ОБНОВЛЕНИЯМИ НА VK.COM/TEACHINMSU.

ЕСЛИ ВЫ ОБНАРУЖИЛИ ОШИБКИ ИЛИ ОПЕЧАТКИ, ТО СООБЩИТЕ ОБ ЭТОМ, НАПИСАВ СООБЩЕСТВУ VK.COM/TEACHINMSU.

БЛАГОДАРИМ ЗА ПОДГОТОВКУ КОНСПЕКТА
СТУДЕНТА МЕХАНИКО-МАТЕМАТИЧЕСКОГО ФАКУЛЬТЕТА МГУ
ЕФАНОВА АНТОНА АЛЕКСАНДРОВИЧА

Содержание

1. Трехдиагональные определители, рекуррентные уравнения 2-го порядка 5
1.1. Разбор домашнего задания . . . 5
1.2. Трехдиагональные определители . . . 8
1.3. Метод решения линейных однородных рекуррентных уравнений 2-го порядка . . . 10

2. Присоединенная матрица и ее свойства и вычисление обратной 14
2.1. Разбор домашнего задания . . . 14
2.2. Ранг произведения матриц . . . 18
2.3. Присоединенная матрица . . . 19

3. Теория вычетов. Малая теорема Ферма и теорема Эйлера. Символ Лежандра 23
3.1. Задачи на полями вычетов . . . 23
3.2. Диофантовы уравнения . . . 25
3.3. Малая теорема Ферма и теорема Эйлера . . . 26
3.4. Извлечение квадратного корня в поле вычетов . . . 28

4. Комплексные числа 30
4.1. Разбор домашнего задания . . . 30
4.2. Алгебраические операции над комплексными числами . . . 30
4.3. Геометрическая интерпретация комплексного числа . . . 31
4.4. Тригонометрическая запись комплексного числа . . . 33
4.5. Задачи тригонометрии . . . 34
4.6. Операция сопряжения . . . 35

5. Извлечение корней в поле комплексных чисел и вычисление сумм 37
5.1. Разбор домашнего задания . . . 37
5.2. Извлечение корней в поле комплексных чисел . . . 40
5.3. Свойства корней из 1 . . . 42
5.4. Вычисление сумм с помощью комплексных чисел . . . 44

6. Теорема Безу, схема Горнера, алгоритм Евклида для многочлена 45
6.1. Деление многочленов с остатком. Схема Горнера . . . 45
6.2. Разложение многочлена по степеням $x - x_0$ . . . 46
6.3. Понятие кратности корня . . . 48
6.4. НОД двух многочленов . . . 49

7. Неприводимые многочлены, редукция **53**
7.1. Неприводимые многочлены 53
7.2. Решето Эратосфена для многочленов над конечным полем 54
7.3. Разложение на неприводимые множители в $\mathbb{Q}[x]$ 56
7.4. Редукция 58

8. Признак Эйзенштейна, круговой многочлен. Поле рациональных дробей **61**
8.1. Разбор домашнего задания 61
8.2. Признак Эйзенштейна 63
8.3. Круговые многочлены 64
8.4. Поле рациональных дробей 64

9. Симметрические многочлены. Теорема Виета **68**
9.1. Разбор домашнего задания 68
9.2. Симметрические многочлены 69
9.3. Выражение степенных сумм через элементарные симметрические многочлены 72
9.4. Теорема Виета 73

1. Трехдиагональные определители, рекуррентные уравнения 2-го порядка

1.1. Разбор домашнего задания

Задача 16.19 а) *Найти определитель матрицы, элементы которой заданы условием:*

$$a_{ij} = \begin{cases} 1, & i|j \\ 0, & i \nmid j \end{cases}.$$

Понятно, что на главной диагонали будут стоять единицы, так как $i = j \Rightarrow i|j$. При $i > j$ получаем $i \nmid j \Rightarrow a_{ij} = 0$. Таким образом, данная матрица является верхнетреугольной с единицами на главной диагонали:

$$A = \begin{pmatrix} 1 & * & \dots & * \\ 0 & 1 & \dots & * \\ \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 0 & 1 \end{pmatrix},$$

где на месте $*$ могут стоять как нули, так и единицы, но это не влияет на ответ, так как определитель верхнетреугольной матрицы равен произведению элементов, стоящих на главной диагонали. Таким образом, $\det A = 1$.

Задача 16.19 б) *Найти определитель матрицы* (b_{ij}), *где* b_{ij} *равен количеству общих делителей* i *и* j.

Воспользуемся указанием к задаче: $B = A^T A$. Проверим это. Выпишем элемент матрицы $A^T A$:

$$a^T_{i1}a_{1j} + \dots + a^T_{ik}a_{kj} + \dots + a^T_{in}a_{nj} = a_{1i}a_{1j} + \dots + a_{ki}a_{kj} + \dots + a_{ni}a_{nj}.$$

Теперь вспомним определение элементов a_{ij}. В полученной сумме слагаемое не ноль тогда и только тогда, когда оба множителя равны 1, а это верно в том и только том случае, если k делит и i и j. Так как k пробегает от 1 до n и $i, j < n$, то количество ненулевых слагаемых совпадает с количеством общих делителей i и j. С учетом того, что каждое слагаемое может быть либо 0, либо 1, получаем, что эта сумма совпадает с количеством общих делителей i и j.

Остается воспользоваться свойством определителя произведения матриц и определителя транспонированной матрицы:

$$\det B = \det\left(A^T A\right) = \det A^T \det A = (\det A)^2 = 1.$$

Задача 12.3 и) *Вычислить определитель*

$$\Delta_n = \begin{vmatrix} a_0 & 1 & 0 & ... & 1 \\ 1 & a_1 & 0 & ... & 0 \\ 1 & 0 & a_2 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & ... & 0 & a_n \end{vmatrix}.$$

Разложим по последней строке:

$$\Delta_n = (-1)^{n+n} a_n \Delta_{n-1} + (-1)^{n+2} \begin{vmatrix} 1 & 1 & ... & 1 & 1 \\ a_1 & 0 & ... & 0 & 0 \\ 0 & a_2 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & ... & 0 & a_{n-1} & 0 \end{vmatrix}.$$

Последний определитель разложим по последнему столбцу:

$$\Delta_n = a_n \Delta_{n-1} + (-1)^{n+2} (-1)^{n+1} \begin{vmatrix} a_1 & 0 & ... & 0 & 0 \\ 0 & a_2 & ... & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & ... & 0 & 0 & a_{n-1} \end{vmatrix} = a_n \Delta_{n-1} - a_1 a_2 ... a_{n-1}.$$

Таким образом, получили рекуррентное соотношение:

$$\Delta_n = a_n \Delta_{n-1} - a_1 a_2 ... a_{n-1}.$$

Чтобы понять закономерность, распишем Δ_{n-1} и Δ_{n-2} :

$$\Delta_n = a_n \left(a_{n-1}\Delta_{n-2} - a_1 a_2 ... a_{n-2}\right) - a_1 a_2 ... a_{n-1} = a_n a_{n-1}\Delta_{n-2} - a_1 a_2 ... a_{n-2} a_n - a_1 a_2 ... a_{n-1} =$$

$$= a_n a_{n-1} \left(a_{n-2}\Delta_{n-3} - a_1 a_2 ... a_{n-3}\right) - a_1 a_2 ... a_{n-2} a_n - a_1 a_2 ... a_{n-1} =$$

$$= a_n a_{n-1} a_{n-2}\Delta_{n-3} - a_1 a_2 ... a_{n-3} a_{n-1} a_n - a_1 a_2 ... a_{n-2} a_n - a_1 a_2 ... a_{n-1} =$$

$$= a_0 a_1 ... a_{n-1} a_n - \sum_{i=1}^{n} \hat{a}_0 a_1 ... \hat{a}_i ... a_n,$$

где обозначение $\hat{a}_i$ обозначает отсутствие a_i. Формально нужно доказать через индукцию, но фактически мы сделали шаг индукции. Последнюю сумму можно переписать не используя обозначение $\hat{a}$ (при условии $a_i \neq 0 \ \forall i$):

$$\Delta_n = a_0 ... a_n - a_1 ... a_n \sum_{i=1}^{n} \frac{1}{a_i}.$$

Эта задача показывает, что определители можно представлять в виде рекуррентной зависимости, если сам определитель зависит от размера матрицы.

Задача 1* *Вычислить определитель*

$$\Delta_n = \begin{vmatrix} 1+x_1 & 1+x_2 & ... & 1+x_n \\ 1+x_1^2 & 1+x_2^2 & ... & 1+x_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ 1+x_1^n & 1+x_2^n & ... & 1+x_n^n \end{vmatrix}.$$

Этот определитель сильно напоминает определитель Вандермонда, мешают только единицы. Рассмотрим определитель другой матрицы, полученной из данной добавлением сверху единичной строки, а слева - столбец с одной единицей на первом месте и нулями на оставшихся:

$$\begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ 0 & 1+x_1 & 1+x_2 & ... & 1+x_n \\ 0 & 1+x_1^2 & 1+x_2^2 & ... & 1+x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 1+x_1^n & 1+x_2^n & ... & 1+x_n^n \end{vmatrix}.$$

Очевидно, что, разложив построенный определитель по первому столбцу, мы получим исходный. Теперь вычтем из всех строк первую:

$$\begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ -1 & x_1 & x_2 & ... & x_n \\ -1 & x_1^2 & x_2^2 & ... & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -1 & x_1^n & x_2^n & ... & x_n^n \end{vmatrix}.$$

Если бы на месте -1 стояли 1, то это был бы определитель Вандермонда от чисел $1, x_1, ..., x_n$. Но смена знака на этих местах равносильна смене знака единицы на месте $(1,1)$ (так как из первого столбца по свойствам определителя можно вытащить -1). Представим первую строку как сумму двух следующих строк:

$$(1, ..., 1) = (2, 0, ..., 0) + (-1, 1, ..., 1).$$

Теперь воспользуемся свойствам определителя (разложение в сумму):

$$\Delta_n = \underbrace{\begin{vmatrix} 2 & 0 & 0 & ... & 0 \\ -1 & x_1 & x_2 & ... & x_n \\ -1 & x_1^2 & x_2^2 & ... & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -1 & x_1^n & x_2^n & ... & x_n^n \end{vmatrix}}_{\text{раскладываем по первой строке}} + \underbrace{\begin{vmatrix} -1 & 1 & 1 & ... & 1 \\ -1 & x_1 & x_2 & ... & x_n \\ -1 & x_1^2 & x_2^2 & ... & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -1 & x_1^n & x_2^n & ... & x_n^n \end{vmatrix}}_{\text{выносим из первого столбца}-1} =$$

$$= 2\underbrace{\begin{vmatrix} x_1 & x_2 & ... & x_n \\ x_1^2 & x_2^2 & ... & x_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ x_1^n & x_2^n & ... & x_n^n \end{vmatrix}}_{\text{выносим из } i \text{ столбца } x_i} - \underbrace{\begin{vmatrix} 1 & 1 & 1 & ... & 1 \\ 1 & x_1 & x_2 & ... & x_n \\ 1 & x_1^2 & x_2^2 & ... & x_n^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_1^n & x_2^n & ... & x_n^n \end{vmatrix}}_{\text{определитель Вандермонда}} =$$

$$= 2x_1...x_nV(x_1, ..., x_n) - V(1, x_1, ..., x_n)$$

1.2. Трехдиагональные определители

Задача 14.1 а) *Вычислить определитель*

$$\Delta_n = \begin{vmatrix} 2 & 1 & 0 & 0 & ... & 0 \\ 1 & 2 & 1 & 0 & ... & 0 \\ 0 & 1 & 2 & 1 & ... & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & ... & 0 & 1 & 2 & 1 \\ 0 & ... & 0 & 0 & 1 & 2 \end{vmatrix}.$$

Разложим по первой строке:

$$\Delta_n = 2\Delta_{n-1} - \underbrace{\begin{vmatrix} 1 & 1 & 0 & 0 & ... & 0 \\ 0 & 2 & 1 & 0 & ... & 0 \\ 0 & 1 & 2 & 1 & ... & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & ... & 0 & 1 & 2 & 1 \\ 0 & ... & 0 & 0 & 1 & 2 \end{vmatrix}}_{\text{разложим по 1 стоблцу}} = 2\Delta_{n-1} - \Delta_{n-2}$$

Полученное рекуррентное соотношение определяет любой член последовательности определителей, зная первые два. Вычислим Δ_1 и Δ_2 :

$$\Delta_1 = |2| = 2, \quad \Delta_2 = \begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} = 3.$$

Вычислим по этой формуле несколько следующих членов последовательности:

$$\Delta_3 = 2 \cdot 3 - 2 = 4, \quad \Delta_4 = 2 \cdot 4 - 3 = 5, \quad \Delta = 2 \cdot 5 - 4 = 6.$$

Получаем гипотезу $\Delta_n = n + 1$. База индукции очевидна. Шаг:

$$\Delta_{n+1} = 2\Delta_n - \Delta_{n-1} = 2\,(n+1) - n = n + 2.$$

Таким образом, получаем ответ $\Delta_n = n + 1$.

Матрицы, у которых ненулевые элементы стоят только на главной диагонали и двух соседних, причем элементы каждой из диагоналей одинаковы, называются *трехдиагональными* и имеют вид:

$$\Delta_n = \begin{vmatrix} a & b & 0 & 0 & \dots & 0 \\ c & a & b & 0 & \dots & 0 \\ 0 & c & a & b & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & c & a & b \\ 0 & \dots & 0 & 0 & c & a \end{vmatrix}.$$

Получим явную формулу, действуя аналогично предыдущей задаче. Разложим по первой строке:

$$\Delta_n = a\Delta_{n-1} - b \underbrace{\begin{vmatrix} c & b & 0 & 0 & \dots & 0 \\ 0 & a & b & 0 & \dots & 0 \\ 0 & c & a & b & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & c & a & b \\ 0 & \dots & 0 & 0 & c & a \end{vmatrix}}_{\text{разложим по 1 столбцу}} = a\Delta_{n-1} - bc\Delta_{n-2}.$$

Рекуррентные соотношения такого вида называются *линейными однородными рекуррентными уравнениями 2-го порядка*, в общем виде записываемое так:

$$\delta_n = \alpha\delta_{n-1} + \beta\delta_{n-2}, \ \alpha, \beta \in \mathbb{R}, \ \beta \neq 0.$$

Последовательность полностью определяется первыми двумя членами последовательности.

1.3. Метод решения линейных однородных рекуррентных уравнений 2-го порядка

Определение 1. *Характеристическим уравнением для линейного однородного рекуррентного уравнения 2-го порядка называется уравнение вида:*

$$t^2 = \alpha t + \beta.$$

Решим это уравнение. Пусть t_1, t_2 - корни уравнения. Возможно две различные ситуации: когда корни различны и когда корни совпадают.

1. $t_1 \neq t_2$. Тогда выпишем две геометрические прогрессии:

   $$\delta'_n = t_1^n, \quad \delta''_n = t_2^n,$$

   которые называются *базисными*. Покажем, что каждая из последовательностей является решением рекуррентного уравнения, умножив равенство

   $$t_i^2 = \alpha t_i + \beta$$

   на t_i^{n-2}. Получим наше рекуррентное соотношение.

   Теперь воспользуемся тем фактом, что пространство всех решений рассматриваемого рекуррентного соотношения является векторным пространством, то есть сумма двух решений также решение и умножение на ненулевую константу - решение. То есть выражение вида

   $$C_1\delta'_n + C_2\delta'_n, \quad C_1, C_2 \in \mathbb{R}$$

   является решением.

   Утверждение 1. *Для любого решения рекуррентного уравнения существует единственная пара констант такая, что решение представимо в виде:*

   $$\delta_n = C_1 t_1^n + C_2 t_2^n.$$

   Доказательство: Пусть δ_n - решение, которое мы хотим представить в виде:

   $$\delta_n = C_1 t_1^n + C_2 t_2^n.$$

   В этом равенстве слева стоит рассматриваемое решение, справа тоже. Если мы покажем, что эти решения совпадают при $n = 1$ и $n = 2$, то они будут совпадать и для любых других значений n, так как рекуррентная последовательность определяется только первыми двумя членами.

Запишем равенства при $n = 1$ и $n = 2$:

$$\begin{cases} n = 1: & C_1 t_1 + C_2 t_2 = \delta_1 \\ n = 2: & C_1 t_1^2 + C_2 t_2^2 = \delta_2 \end{cases}$$

То есть мы получили систему на C_1 и C_2. То есть это квадратная система линейных уравнений. Определитель матрицы коэффициентов выглядит следующим образом:

$$\begin{vmatrix} t_1 & t_2 \\ t_1^2 & t_2^2 \end{vmatrix} = t_1 t_2 (t_2 - t_1).$$

Этот определитель не равен нулю, так как корни ненулевые ($\beta \neq 0$) и $t_1 \neq t_2$. А раз так, то система имеет единственное решение по теореме Крамера. ■

2. $t_1 = t_2$. В качестве базисных решений рассматриваем следующие последовательности:

$$\delta'_n = t_1^n, \quad \delta''_n = n t_1^n.$$

Проверим, что второе базисное решение действительно решение, подставив его в рекуррентное уравнение:

$$n t_1^n = \alpha (n-1) t_1^{n-1} + \beta (n-2) t_1^{n-2} = \alpha n t_1^{n-1} - \alpha t_1^{n-1} + \beta n t_1^{n-2} - 2\beta t_1^{n-2}.$$

Но мы знаем, что t_1^n является решением, поэтому слагаемые с множителем n можно убрать, после чего поделив на t_1^{n-2} (в силу $\beta \neq 0$):

$$0 = -\alpha t_1 - 2\beta.$$

В силу теоремы Виета для квадратного уравнения имеем $\alpha = 2t_1$, $\beta = -t_1^2$. Подставив эти значения в полученное уравнение, получим тождество.

Утверждение 2. *Для любого решения рекуррентного уравнения существует единственная пара констант такая, что решение представимо в виде:*

$$\delta_n = C_1 t_1^n + C_2 n t_1^n.$$

Доказательство: Пусть δ_n - решение, которое мы хотим представить в виде:

$$\delta_n = C_1 t_1^n + C_2 n t_1^n.$$

В этом равенстве слева стоит рассматриваемое решение, справа тоже. Если мы покажем, что эти решения совпадают при $n = 1$ и $n = 2$, то они будут совпадать

и для любых других значений n, так как рекуррентная последовательность определяется только первыми двумя членами.

Запишем равенства при $n = 1$ и $n = 2$:

$$\begin{cases} n = 1: & C_1 t_1 + C_2 t_1 = \delta_1 \\ n = 2: & C_1 t_1^2 + C_2 2t_1^2 = \delta_2 \end{cases}$$

То есть мы получили систему на C_1 и C_2. То есть это квадратная система линейных уравнений. Определитель матрицы коэффициентов выглядит следующим образом:

$$\begin{vmatrix} t_1 & t_1 \\ t_1^2 & 2t_1^2 \end{vmatrix} = t_1^3.$$

Этот определитель не равен нулю, так как $t_1 \neq 0$. А раз так, то система имеет единственное решение по теореме Крамера. ■

Рассмотрим примеры.

Задача 14.1 б) *Вычислить определитель*

$$\Delta_n = \begin{vmatrix} 3 & 2 & 0 & 0 & \dots & 0 \\ 1 & 3 & 2 & 0 & \dots & 0 \\ 0 & 1 & 3 & 2 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & 3 & 2 \\ 0 & \dots & 0 & 0 & 1 & 3 \end{vmatrix}.$$

Воспользуемся выведенной формулой для трехдиагональных определителей:

$$\Delta_n = 3\Delta_{n-1} - 2\Delta_{n-2}.$$

Составим характеристическое уравнение:

$$t^2 = 3t - 2 \Leftrightarrow t^2 - 3t + 2 = 0 \Rightarrow t_1 = 1, \quad t_2 = 2.$$

Согласно утверждению 1 общее решение имеет вид:

$$\Delta_n = C_1 2^n + C_2.$$

Вычислим константы C_1 и C_2 при $n = 1, 2$:

$$\begin{cases} n = 1: & C_1 2 + C_2 = 3 \\ n = 2: & C_1 4 + C_2 = 7 \end{cases}.$$

Вычитаем из второго уравнения первое:

$$2C_1 = 4 \Leftrightarrow C_1 = 2 \Rightarrow C_2 = -1 \Rightarrow \Delta_n = 2^{n+1} - 1.$$

Задача 14.1 б) *Вычислить определитель*

$$\Delta_n = \begin{vmatrix} 1 & 2 & 0 & 0 & 0 & \dots & 0 & 0 \\ 3 & 4 & 2 & 0 & 0 & \dots & 0 & 0 \\ 0 & 2 & 4 & 2 & 0 & \dots & 0 & 0 \\ 0 & 0 & 2 & 4 & 2 & \dots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & \dots & 0 & 0 & 2 & 4 & 2 & 0 \\ 0 & \dots & 0 & 0 & 0 & 2 & 4 & 2 \\ 0 & \dots & 0 & 0 & 0 & 0 & 2 & 4 \end{vmatrix}.$$

Разложим по последней строке:

$$\Delta_n = 4\Delta_{n-1} - 4\Delta_{n-2}.$$

Соответствующее характеристическое уравнение имеет вид:

$$t^2 = 4t - 4 \Rightarrow t_1 = t_2 = 2 \Rightarrow \Delta_n = C_1 2^n + C_2 n 2^n.$$

Вычислим константы C_1 и C_2 при $n = 1, 2$:

$$\begin{cases} n = 1: & C_1 2 + C_2 2 = 1 \\ n = 2: & C_1 4 + C_2 8 = -2 \end{cases} . \Rightarrow 4C_2 = -4 \Leftrightarrow C_2 = -1 \Rightarrow C_2 = \frac{3}{2}.$$

Решение принимает вид:

$$\Delta_n = \frac{3}{2} 2^n - n 2^n = 2^{n-1} (3 - 2n)$$

2. Присоединенная матрица и ее свойства и вычисление обратной

2.1. Разбор домашнего задания

Задача 11.10 е) *Вычислить определитель*

$$\Delta_n = \begin{vmatrix} 1+x_1y_1 & x_1y_2 & \dots & x_1y_n \\ x_2y_1 & 1+x_2y_2 & \dots & x_2y_n \\ \vdots & \vdots & \ddots & \vdots \\ x_ny_1 & x_ny_2 & \dots & 1+x_ny_n \end{vmatrix}.$$

Другими словами $a_{ij} = x_iy_j + \delta_{ij}$, где δ_{ij} - символ Кронекера. Представим последнюю строку следующим образом:

$$(x_ny_1, \dots, x_ny_{n-1}, 1+x_ny_n) = (0, \dots, 0, 1) + (x_ny_1, \dots, x_ny_{n-1}, x_ny_n).$$

Тогда по свойству определителя получаем:

$$\Delta_n = \underbrace{\begin{vmatrix} 1+x_1y_1 & x_1y_2 & \dots & x_1y_{n-1} & x_1y_n \\ x_2y_1 & 1+x_2y_2 & \dots & x_2y_{n-1} & x_2y_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n-1}y_1 & x_{n-1}y_2 & \dots & 1+x_{n-1}y_{n-1} & x_{n-1}y_n \\ 0 & 0 & \dots & 0 & 1 \end{vmatrix}}_{\text{раскладываем по последней строке}} +$$

$$+ \underbrace{\begin{vmatrix} 1+x_1y_1 & x_1y_2 & \dots & x_1y_{n-1} & x_1y_n \\ x_2y_1 & 1+x_2y_2 & \dots & x_2y_{n-1} & x_2y_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n-1}y_1 & x_{n-1}y_2 & \dots & 1+x_{n-1}y_{n-1} & x_{n-1}y_n \\ x_ny_1 & x_ny_2 & \dots & x_ny_{n-1} & x_ny_n \end{vmatrix}}_{\text{выносим из последней строки } x_n} =$$

$$= \Delta_{n-1} + x_n \begin{vmatrix} 1+x_1y_1 & x_1y_2 & \dots & x_1y_{n-1} & x_1y_n \\ x_2y_1 & 1+x_2y_2 & \dots & x_2y_{n-1} & x_2y_n \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ x_{n-1}y_1 & x_{n-1}y_2 & \dots & 1+x_{n-1}y_{n-1} & x_{n-1}y_n \\ y_1 & y_2 & \dots & y_{n-1} & y_n \end{vmatrix}.$$

В последнем определителе вычтем из i строки последнюю, умноженную на x_i :

$$\Delta_n = \Delta_{n-1} + x_n \underbrace{\begin{vmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ y_1 & y_2 & \ldots & y_{n-1} & y_n \end{vmatrix}}_{\text{нижнетреугольная матрица}} = \Delta_{n-1} + x_n y_n.$$

С учетом того, что $\Delta_1 = 1 + x_1 y_1$, получаем по индукции ответ:

$$\Delta_n = 1 + x_1 y_1 + x_2 y_2 + \ldots + x_n y_n.$$

Задача 14.11 о) *Вычислить определитель*

$$\Delta_n = \begin{vmatrix} a & x & \ldots & x & x \\ y & a & \ldots & x & x \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ y & y & \ldots & a & x \\ y & y & \ldots & y & a \end{vmatrix}.$$

Можно действовать по-разному. Вычтем из i столбца $i+1$, начиная с первого:

$$\Delta_n = \begin{vmatrix} a-x & 0 & 0 & \ldots & 0 & 0 & x \\ y-a & a-x & 0 & \ldots & 0 & 0 & x \\ 0 & y-a & a-x & \ldots & 0 & 0 & x \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a-x & 0 & x \\ 0 & 0 & 0 & \ldots & y-a & a-x & x \\ 0 & 0 & 0 & \ldots & 0 & y-a & a \end{vmatrix}. \tag{1}$$

Вычтем из i строки $i+1$, начиная с первой:

$$\Delta_n = \begin{vmatrix} 2a-x-y & x-a & 0 & \ldots & 0 & 0 & 0 \\ y-a & 2a-x-y & x-a & \ldots & 0 & 0 & 0 \\ 0 & y-a & 2a-x-y & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 2a-x-y & x-a & 0 \\ 0 & 0 & 0 & \ldots & y-a & 2a-x-y & x-a \\ 0 & 0 & 0 & \ldots & 0 & y-a & a \end{vmatrix}.$$

Теперь это трехдиагональный определитель и можно написать формулу, которая получена на предыдущем семинаре:

$$\Delta_n = (2a - x - y)\,\Delta_{n-1} - (x - a)\,(y - a)\,\Delta_{n-2}.$$

Записываем характеристическое уравнение:

$$t^2 = (2a - x - y)\,t - (x - a)\,(y - a) \Leftrightarrow t^2 - (a - x + a - y)\,t + (a - x)\,(a - y) = 0$$

По теореме Виета для квадратного уравнения получаем корни:

$$t_1 = (a - x)\,, \quad t_2 = (a - y)\,.$$

Будем считать, что числа a, x и y различны, тогда $t_1 \neq t_2$ и не равны нулю. В таком случае общее решение представимо в виде:

$$\Delta_n = C_1\,(a - x)^n + C_2\,(a - y)^n\,.$$

Найдем коэффициенты C_1 и C_2 при $n = 1, 2$:

$$\begin{cases} n = 1: \quad C_1\,(a - x) + C_2\,(a - y) = \Delta_1 = |a| = a \\ n = 2: \quad C_1\,(a - x)^2 + C_2\,(a - y)^2 = \Delta_2 = \begin{vmatrix} 2a - x - y & x - a \\ y - a & a \end{vmatrix} = a^2 - xy \end{cases}.$$

Решая эту линейную систему, получаем:

$$C_1 = \frac{-y}{x - y}, \quad C_2 = \frac{x}{x - y} \;\Rightarrow \Delta_n = \frac{x\,(a - y)^n - y\,(a - x)^n}{x - y}.$$

Понятно, что от знаменателя можно избавиться, так как определитель Δ_n является многочленом от a, x и y, но, красота данной формулы сильно уменьшится.

Отдельно следует рассмотреть случаи $x = y \neq a$ и $a = x \neq y$ (или $a = y \neq x$).

1. $a = x = y$. У матрицы есть две совпадающие строки, значит $\Delta_n = 0$.

2. $a = x \neq y$. Рассматриваемая матрица принимает вид нижнетругольной:

$$\Delta_n = \begin{vmatrix} x - y & 0 & 0 & \ldots & 0 & 0 & 0 \\ y - x & x - y & 0 & \ldots & 0 & 0 & 0 \\ 0 & y - x & x - y & \ldots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & x - y & 0 & 0 \\ 0 & 0 & 0 & \ldots & y - x & x - y & 0 \\ 0 & 0 & 0 & \ldots & 0 & y - x & x \end{vmatrix} = x\,(x - y)^{n-1}$$

3. $a = y \neq x$. Аналогично предыдущему (матрица принимает вид верхнетреугольной):
$$\Delta_n = y\,(y-x)^{n-1}$$

4. $x = y \neq a$. В этом случае $t_1 = t_2 = a - x$ и общее решение принимает вид:
$$\Delta_n = C_1\,(a-x)^n + C_2 n\,(a-x)^n\,.$$
Найдем коэффициенты C_1 и C_2 при $n = 1, 2$:
$$\begin{cases} n=1: & C_1\,(a-x) + C_2\,(a-x) = \Delta_1 = |a| = a \\ n=2: & C_1\,(a-x)^2 + 2C_2\,(a-x)^2 = \Delta_2 = a^2 - x^2 \end{cases}.$$
Из этой системы находим:
$$C_1 = 1,\quad C_2 = \frac{x}{a-x} \;\Rightarrow \Delta_n = (a-x)^{n-1}\,(a + (n-1)\,x)\,.$$
Этот случай можно было также получить, рассмотрев в основном случае следующий предел
$$\lim_{y\to x}\frac{x\,(a-y)^n - y\,(a-x)^n}{x-y} = \lim_{y\to x}\frac{-nx\,(a-y)^{n-1} - (a-x)^n}{-1} = \quad \text{(Правило Лопиталя)}$$
$$= nx\,(a-x)^{n-1} + (a-x)^n = (a-x)^{n-1}\,(a + (n-1)\,x)\,.$$

Рассмотрим второй способ решения. Разложим определитель (1) по первой строке:
$$\Delta_n = (a-x)\begin{vmatrix} a-x & 0 & \dots & 0 & 0 & x \\ y-a & a-x & \ddots & 0 & 0 & x \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & \ddots & a-x & 0 & x \\ 0 & 0 & \dots & y-a & a-x & x \\ 0 & 0 & \dots & 0 & y-a & a \end{vmatrix} +$$
$$+ (-1)^n\,x\begin{vmatrix} y-a & a-x & 0 & \dots & 0 & 0 \\ 0 & y-a & a-x & \ddots & 0 & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & a-x & 0 \\ 0 & 0 & 0 & \ddots & y-a & a-x \\ 0 & 0 & 0 & \dots & 0 & y-a \end{vmatrix} = (a-x)\,\Delta_{n-1} + (-1)^{n+1}\,x\,(y-a)^{n-1}\,.$$

Выпишем дополнительный шаг:

$$\Delta_n = (a-x)\left((a-x)\,\Delta_{n-2} + (-1)^n\,x\,(y-a)^{n-2}\right) + (-1)^{n+1}\,x\,(y-a)^{n-1} =$$

$$= (a-x)^2\,\Delta_{n-2} + (-1)^n\,x\,(a-x)\,(y-a)^{n-2} + (-1)^{n+1}\,x\,(y-a)^{n-1} = \ldots$$

$$\ldots = (a-x)\,\Delta_1 + x\sum_{i=1}^{n-1}(-1)^i\,(a-x)^{n-i-1}\,(y-a)^i =$$

$$= (a-x)\,a + x\sum_{i=1}^{n-1}(-1)^i\,(a-x)^{n-i-1}\,(y-a)^i\,.$$

2.2. Ранг произведения матриц

Известно, что ранг произведения матриц не превосходит рангов каждой из матриц $\mathrm{rk}AB \leqslant \mathrm{rk}A, \mathrm{rk}B$. Однако, в случае невырожденности, например, матрицы B неравенство превращается в равенство. Как доказать этот факт? Представим матрицу A в следующем виде (пользуясь ассоциативностью и существованием обратной матрицы к B в силу невырожденности):

$$A = ABB^{-1} = (AB)\,B^{-1} \Rightarrow \mathrm{rk}A \leqslant \mathrm{rk}\,(AB)\,,$$

но $\mathrm{rk}\,(AB) \leqslant \mathrm{rk}A \Rightarrow \mathrm{rk}\,(AB) = \mathrm{rk}A$.

Задача 1 *Пусть $A, B \in Mat_n$ и известны их ранги r и s соответственно. Найти ранг матрицы:*

$$M = \left(\begin{array}{c|c} A - A^2 & AB \\ \hline -A & B \end{array}\right) \in Mat_{2n}.$$

Попробуем привести эту матрицу к более простому виду с помощью элементарных преобразований. Забудем временно, что A и B матрицы, и будем воспринимать их как числа. Прибавим к первой строке вторую, умноженную на $-A$:

$$M \underset{1}{\longrightarrow} \left(\begin{array}{c|c} A & 0 \\ \hline -A & B \end{array}\right).$$

Теперь прибавим ко второй строке первую:

$$M \underset{2}{\longrightarrow} \left(\begin{array}{c|c} A & 0 \\ \hline 0 & B \end{array}\right).$$

Второе преобразование можно свести к элементарным преобразованиям: к $n+i$ строке прибавить i строку при $1 \leqslant i \leqslant n$. Поэтому при первом преобразовании ранг матрицы не меняется.

Если воспринимать первое преобразование как элементарное преобразование над числами, то его можно представить в виде умножения исходной матрицы на соответствующую матрицу слева:

$$\left(\begin{array}{c|c} A & 0 \\ \hline -A & B \end{array}\right) = \left(\begin{array}{c|c} 1 & -A \\ \hline 0 & 1 \end{array}\right) \left(\begin{array}{c|c} A - A^2 & AB \\ \hline -A & B \end{array}\right).$$

Теперь, если вернемся к матрицам, то нужно заменить 1 на единичную матрицу E. Этот результат сохранится в силу общего факта о перемножении матриц, разбитых на соответствующие блоки) - они перемножаются так, как будто блоки являются числами. Но матрица

$$\left(\begin{array}{c|c} E & -A \\ \hline 0 & E \end{array}\right)$$

является невырожденной, а умножение на невырожденную матрицу, как отмечалось ранее, сохраняет ранг. Первое преобразование можно также представить в виде умножения слева на "элементарную" матрицу:

$$\left(\begin{array}{c|c} E & 0 \\ \hline E & E \end{array}\right).$$

Таким образом, при преобразованиях 1 и 2 ранг матрицы M не меняется. Ранг матрицы, полученной при указанных преобразованиях, равен сумме рангов матриц A и B, то есть $r + s$. Это следует из метода Гаусса.

2.3. Присоединенная матрица

Пусть $A \in M_n$, тогда присоединенная матрицы определяется следующим образом:

$$\tilde{A} = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \vdots & \vdots & \vdots & \vdots \\ A_{1n} & A_{21} & \dots & A_{nn} \end{pmatrix} \Leftrightarrow \tilde{a}_{ij} = A_{ji}.$$

Основное свойство присоединенной матрицы, верное для любой квадратной матрицы:

$$A\tilde{A} = \tilde{A}A = \det A \cdot E.$$

Если матрица A невырождена, то $A^{-1} = \dfrac{\tilde{A}}{\det A}$.

Задача 2 *Пусть известен ранг матрицы A. Чему равен ранг присоединенной матрицы $\tilde{A}$?*

Рассмотрим случаи.

1. Если $\mathrm{rk}A = n$. В этом случае матрица A невырождена и, следовательно, $\det A \neq 0$. Из основного свойства присоединенной матрицы следует, что матрица $A\tilde{A}$ имеет ранг n. Но ранг произведения не превосходит ранга каждого из сомножителей, поэтому ранг присоединенной матрицы заведомо не меньше ранга произведения, то есть n. Но и больше n он быть не может в силу размера матрицы. Таким образом, ранг присоединенной матрицы в невырожденном случае совпадает с рангом исходной матрицы.

2. Если $\mathrm{rk}A \leqslant n-2$. По теореме о ранге матрицы ранг равен наибольшему порядку ненулевого минора матрицы. А раз ранг не превосходит $n-2$, то ненулевых миноров порядка $n-1$ нет. А элементы присоединенной матрицы являются минорами порядка $n-1$, то есть все они равны нулю, а значит и сама присоединенная матрица нулевая. Заключаем, что ранг присоединенной матрицы равен нулю.

3. Если $\mathrm{rk}A = n-1$. В этом случае $\det A = 0$ и основное свойство приобретает вид: $A\tilde{A} = \tilde{A}A = 0$. Рассмотрим присоединенную матрицу как матрицу неизвестных X, то имеем матричное уравнение $AX = 0$. Столбец произведения имеет вид AX^j и в силу матричное уравнения равен нулю. Это означает, что каждый столбец присоединенной матрицы является решением однородной системы линейных уравнений $Ax = 0$, размерность решений которой равна 1. Таким образом, все столбцы присоединенной матрицы пропорциональны. Нулевой присоединенная матрица быть не может, так как, если ранг исходной матрицы $n-1$, то существует ненулевой минор порядка $n-1$, а значит в присоединенной матрице точно есть ненулевой элемент. Таким образом, ранг равен 1.

Задача 3 *Найти определитель присоединенной матрицы.*
Рассмотрим случаи:

1. $\mathrm{rk}A \leqslant n-1$. В этом случае из задачи 2 получаем, что ранг присоединенной матрицы либо 0, либо 1. В обоих случаях определитель равен 0 (в случае $n = 1$ присоединенная матрица не определена, так как не определено алгебраическое дополнение к единственному элементу матрицы).

2. $\mathrm{rk}A = n$. В этом случае матрица невырождена и $\det A \neq 0$. Применим к основному свойству присоединенной матрицы свойства определителя произведения:

$$\det(\det A \cdot E) = \det\left(A\tilde{A}\right) \Leftrightarrow (\det A)^n \det E = \det A \det \tilde{A} \Leftrightarrow \det \tilde{A} = (\det A)^{n-1}$$

Можно заметить, что формула $\det \tilde{A} = (\det A)^{n-1}$ верна в любом случае.

Задача 16.3 *Пусть задан определитель матрицы $A = (a_{ij})$. Строим матрицу B следующему правилу: заменяем элемент a_{ij} на соответствующий минор M_{ij}. Найти определитель матрицы B. Найти определитель этой матрицы в случае замены не на минор, а на алгебраическое дополнение.*

Начнем со второго вопроса. Если мы заменяем на алгебраические дополнения, то получим транспонированную присоединенную матрицу. Но при транспонировании определитель не меняется. Тогда из задачи 3 получаем ответ $\det B = (\det A)^{n-1}$.

Первый вопрос. Умножим j столбец на $(-1)^j$, а i строчку на $(-1)^i$. В таком случае, M_{ij} умножится на $(-1)^{i+j}$, а это есть алгебраическое дополнение. Но определитель при умножении строчки или столбца на число, конечно, менятся. По столбцам выйдет компенсирующий множитель $(-1)^{1+2+\ldots+n}$ и по строкам такой же множитель, то есть в итоге получится просто 1. Таким образом, определитель матрицы, составленный из миноров, совпадает с определителем матрицы, составленной из алгебраических дополнений, и равен $(\det A)^{n-1}$.

Задача 18.8 в) *Найти обратную матрицу к матрице A по явной формуле, если*

$$A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}.$$

Выпишем явную формулу:

$$A^{-1} = \frac{\tilde{A}}{\det A}, \quad \tilde{A} = \begin{pmatrix} 5 & -2 \\ -3 & 1 \end{pmatrix}, \quad \det A = -1 \Rightarrow A^{-1} = \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix}.$$

В случае $n = 2$ удобно использовать явную формулу:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \Rightarrow A^{-1} = \frac{\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}}{ad - bc}$$

Задача 18.8 г) *Найти обратную матрицу к матрице A по явной формуле, если*

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 3 & 3 \end{pmatrix}.$$

Вычислим определитель, разложив по второй строке: $\det A = 1 \cdot 3 = 3$. Вычислим присоединенную матрицу:

$$A_{11} = \begin{vmatrix} 1 & 0 \\ 3 & 3 \end{vmatrix} = 3, \quad A_{12} = -\begin{vmatrix} 0 & 0 \\ 0 & 3 \end{vmatrix} = 0, \quad A_{13} = \begin{vmatrix} 0 & 1 \\ 0 & 3 \end{vmatrix} = 0,$$

$$A_{21} = -\begin{vmatrix} 1 & 0 \\ 3 & 3 \end{vmatrix} = -3, \quad A_{22} = \begin{vmatrix} 1 & 0 \\ 0 & 3 \end{vmatrix} = 3, \quad A_{23} = -\begin{vmatrix} 1 & 1 \\ 0 & 3 \end{vmatrix} = -3,$$

$$A_{31} = \begin{vmatrix} 1 & 0 \\ 1 & 0 \end{vmatrix} = 0, \quad A_{32} = -\begin{vmatrix} 1 & 0 \\ 0 & 0 \end{vmatrix} = 0, \quad A_{33} = \begin{vmatrix} 1 & 1 \\ 0 & 1 \end{vmatrix} = 1.$$

Выпишем обратную матрицу, поделив на определитель исходной матрицы сразу в присоединенной:

$$A^{-1} = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & -1 & 1/3 \end{pmatrix}$$

3. Теория вычетов. Малая теорема Ферма и теорема Эйлера. Символ Лежандра

3.1. Задачи на полями вычетов

Цель данного занятия показать, что с полями вычетов можно работать также, как, например, с полем действительных чисел.

Задача 66.19 *Решить систему линейных уравнений*

$$A = \begin{cases} x + \bar{2}z = \bar{1} \\ y + \bar{2}z = \bar{2} \\ \bar{2}x + z = \bar{1} \end{cases}$$

над полями а) $\mathbb{Z}_3$*, б)* $\mathbb{Z}_5$.

Будем решать методом Гаусса. Выпишем расширенную матрицу системы:

$$\left(\begin{array}{ccc|c} \bar{1} & \bar{0} & \bar{2} & \bar{1} \\ \bar{0} & \bar{1} & \bar{2} & \bar{2} \\ \bar{2} & \bar{0} & \bar{1} & \bar{1} \end{array}\right)$$

Вычтем из третьей строки первую, умноженную на $\overline{-2}$:

$$\left(\begin{array}{ccc|c} \overline{1} & \overline{0} & \overline{2} & \overline{1} \\ \overline{0} & \overline{1} & \overline{2} & \overline{2} \\ \overline{0} & \overline{0} & \overline{-3} & \overline{-1} \end{array}\right).$$

1. Над полем $\mathbb{Z}_3$ система принимает вид:

$$\left(\begin{array}{ccc|c} \overline{1} & \overline{0} & \overline{2} & \overline{1} \\ \overline{0} & \overline{1} & \overline{2} & \overline{2} \\ \overline{0} & \overline{0} & \overline{0} & \overline{-1} \end{array}\right).$$

   Из последней строки видно, что система решений не имеет.

2. Над полем $\mathbb{Z}_5$ система принимает вид:

$$\left(\begin{array}{ccc|c} \overline{1} & \overline{0} & \overline{2} & \overline{1} \\ \overline{0} & \overline{1} & \overline{2} & \overline{2} \\ \overline{0} & \overline{0} & \overline{2} & \overline{4} \end{array}\right).$$

Приведем систему каноническому виду: вычтем из первых двух строк третью, а затем поделим третью строку на $\overline{2}$:

$$\left(\begin{array}{ccc|c} \overline{1} & \overline{0} & \overline{0} & \overline{2} \\ \overline{0} & \overline{1} & \overline{0} & \overline{3} \\ \overline{0} & \overline{0} & \overline{1} & \overline{2} \end{array}\right).$$

Таким образом, система совместна и определена. Решение: $x = \overline{2}, y = \overline{3}, z = \overline{2}$.

Задача 66.24 а) *Решить квадратное уравнение*

$$x^2 + \overline{3}x + \overline{7} = 0$$

над полем $\mathbb{Z}_{11}$.

Найдем дискриминант $D = \overline{9} - \overline{28} = \overline{3}$. Чтобы понять, извлекается ли корень из $\overline{3}$, переберем квадраты всех элементов:

$$\overline{0}^2 = \overline{0},\ \overline{1}^2 = \overline{1},\ \overline{2}^2 = \overline{4},\ \overline{3}^2 = \overline{9},\ \overline{4}^2 = \overline{5},\ \overline{5}^2 = \overline{3} \Rightarrow \sqrt{D} = \pm\overline{5}.$$

Дальше перебирать не нужно, так как у квадратного уравнения может быть максимум только два корня, а соответствующие значения дискриминанта мы нашли. Таким образом, находим корни:

$$x = \frac{-\overline{3} \pm \overline{5}}{\overline{2}} = \overline{1}, \overline{7}.$$

Задача 66.24 б) *Решить квадратное уравнение*

$$x^2 + \overline{5}x + \overline{1} = 0$$

над полем $\mathbb{Z}_{11}$.

Найдем дискриминант $D = \overline{25} - \overline{4} = \overline{10}$. Чтобы понять, извлекается ли корень из $\overline{3}$, переберем квадраты всех элементов:

$$\overline{0}^2 = \overline{0},\ \overline{\pm 1}^2 = \overline{1},\ \overline{\pm 2}^2 = \overline{4},\ \overline{\pm 3}^2 = \overline{9},\ \overline{\pm 4}^2 = \overline{5},\ \overline{\pm 5}^2 = \overline{3}.$$

Из приведенного списка видно, что все элементы перебирать не нужно, так как, например, $\overline{9} = \overline{-2}$, а так как мы возводим в квадрат, то разницы никакой нет. Отсюда следует, что в поле $\mathbb{Z}_{11}$ корень из $\overline{10}$ не извлекается. Следовательно, решений над данным полем нет.

3.2. Диофантовы уравнения

Наша цель понять как теория вычетов помогает решать уравнения в целых числах.

Задача 1 *Решить уравнения*

1. $23x - 17y = 5$

2. $41x - 11y = 19$

3. $35x + 21y = 14$

4. $3x^2 + 2 = y^2$

5. $7x^2 + 2 = y^3$

6. $15x^2 - 7y^2 = 9$

1. Рассмотрим данное уравнение над полем $\mathbb{Z}_{17}$:

$$\overline{6}\overline{x} = \overline{5} \Rightarrow \overline{x} = \frac{\overline{5}}{\overline{6}} = \overline{5} \cdot \overline{6}^{-1} = \overline{5} \cdot \overline{3} = \overline{15} = \overline{-2}.$$

Если теперь вернуться к целым числам, то $x = -2 + 17k, k \in \mathbb{Z}$. Найдем y, подставив найденный x в исходное уравнение:

$$23\,(-2 + 17k) - 17y = 5 \Leftrightarrow -46 + 23 \cdot 17k - 17y = 5 \Leftrightarrow y = 23k - 3.$$

4. Рассмотрим данное уравнение на полем $\mathbb{Z}_3$:

$$\overline{2} = \overline{y}^2.$$

Корень из $\overline{2}$ над полем $\mathbb{Z}_3$ не извлекается, следовательно, решений в целых числах нет.

5. Рассмотрим данное уравнение на полем $\mathbb{Z}_7$:

$$\overline{2} = \overline{y}^3.$$

Переберем кубы всех элементов поля:

$$\overline{0}^3 = \overline{0},\ \overline{1}^3 = \overline{1},\ \overline{2}^3 = \overline{1},\ \overline{3}^3 = \overline{6},\ \overline{4}^3 = \overline{1},\ \overline{5}^3 = \overline{6},\ \overline{6}^3 = \overline{6}$$

Корень кубический из $\overline{2}$ над полем $\mathbb{Z}_7$ не извлекается, следовательно, решений в целых числах нет.

Нерешенные пункты остаются для самостоятельного решения.

3.3. Малая теорема Ферма и теорема Эйлера

Малая теорема Ферма на языке вычетов выглядит следующим образом:

Теорема 1 (Малая теорема Ферма)**.** *В поле вычетов $\mathbb{Z}_p$, где p - простое число, выполнено следующее тождество:*

$$a^p = a,\ \forall a \in \mathbb{Z}_p.$$

Для мультипликативной подгруппы можно написать:

$$a^{p-1} = 1,\ \forall a \in \mathbb{Z}_p^{\times}.$$

Задача 66.23 б) *Решить уравнение $x^7 = \overline{7}$ в $\mathbb{Z}_{11}$.*
Возведем обе части в третью степень:

$$x^{21} = \overline{7}^3 = \overline{7}^2\overline{7} = \overline{5} \cdot \overline{7} = \overline{35} = \overline{2};$$

с другой стороны, применив малую теорему Ферма, получим

$$x^{21} = x^{11}x^{10} = x \cdot 1 = x \Rightarrow x = \overline{2}.$$

Однако, возведение в куб обеих частей уравнения может оказаться неравносильным преобразованием, поэтому следует проверить полученный корень подстановкой:

$$\overline{2}^7 = \overline{128} = \overline{7}.$$

Рассмотрим теперь кольцо вычетов $\mathbb{Z}_m = \left\{\overline{0}, \overline{1}, ..., \overline{m-1}\right\}$. Элемемент $\overline{k} \in \mathbb{Z}_m^{\times}$ тогда и только тогда, когда НОД$(k, m) = 1$, то есть мультипликативная группа обратимых элементов состоит всех вычетов взаимнопростых с m. Если m простое, то все элементы мультипликативной группы обратимы. Количество обратимых элементов совпадает с количеством целых чисел от 1 до $m-1$ взаимнопростых с m. Последнее называется функцией Эйлера и обозначается $\varphi(m)$.

1. Если p - простое, то $\varphi(p) = p - 1$.
2. $\varphi(p^n) = p^n - p^{n-1}$.
3. Если разложить на простые $m = p_1^{k_1}...p_s^{k_s}$, то в силу мультипликативности функции Эйлера имеем:

$$\varphi(m) = \left(p_1^{k_1} - p_1^{k_1-1}\right) ... \left(p_s^{k_s} - p_s^{k_s-1}\right).$$

Малая теорема Ферма имеет обобщение в виде теоремы Эйлера.

Теорема 2 (Эйлера)**.** *В кольце вычетов $\mathbb{Z}_m$ верно равенство $a^{\varphi(m)} = 1\ \ \forall a \in \mathbb{Z}_m^{\times}$.*

Задача 2 *Пусть дана последовательности чисел:*

$$k_1 = 2, \quad k_2 = 2^2, \quad k_3 = 2^{2^2}, \ \ldots, k_{n+1} = 2^{k_n}, \ \ldots$$

Доказать, что $\exists N \in \mathbb{N}: \ \forall i, j \geqslant N \Rightarrow k_i = k_j$ *в* $\mathbb{Z}_7$.

Из теоремы Эйлера можно сделать следствие: если $k \equiv l \,(\mathrm{mod} \varphi(m))$, то $a^k \equiv a^l \,(\mathrm{mod}\ m)$. А у нас как раз так ситуация:

$$k_N \equiv k_{N+1} \equiv k_{N+2} \equiv \ldots \,(\mathrm{mod}\ 7) \Leftrightarrow 2^{k_{N-1}} \equiv 2^{k_N} \equiv 2^{k_{N+1}} \equiv \ldots \,(\mathrm{mod}\ 7)$$

То есть все эти сравнения будут следовать из того, что

$$k_{N-1} \equiv k_N \equiv k_{N+1} \equiv \ldots \,(\mathrm{mod}\ \varphi(7)).$$

С учетом того, что $\varphi(7) = 6$, применить теорему Эйлера напрямую к полученному условию нельзя, так как НОД$(2, 6) = 2 \neq 1$. Но сравнение по модулю 6 равносильно сравнению по модулю 2 и по модулю 3. Сравнение по модулю 2 очевидно в силу определения последовательности k_n (все члены последовательности являются степенью двойки):

$$2^{k_{N-2}} \equiv 2^{k_{N-1}} \equiv 2^{k_N} \equiv \ldots \,(\mathrm{mod}\ 6) \Leftrightarrow 2^{k_{N-2}} \equiv 2^{k_{N-1}} \equiv 2^{k_N} \equiv \ldots \,(\mathrm{mod}\ 3).$$

Понятно, что это верно при $N > 2$, так как k_{-1} и k_0 не определены. Последние сравнения будут верны, если

$$k_{N-2} \equiv k_{N-1} \equiv k_N \equiv \ldots \,(\mathrm{mod}\ \varphi(3)) \Leftrightarrow k_{N-2} \equiv k_{N-1} \equiv k_N \equiv \ldots \,(\mathrm{mod}\ 2).$$

Последнее условие также выполняется при любых $N \geqslant 3$. То есть получаем такую цепочку следствий:

$$k_{N-2} \equiv k_{N-1} \equiv k_N \equiv \ldots \,(\mathrm{mod}\ 2) \Rightarrow 2^{k_{N-2}} \equiv 2^{k_{N-1}} \equiv 2^{k_N} \equiv \ldots \,(\mathrm{mod}\ 3) \Rightarrow$$

$$\Rightarrow k_{N-1} \equiv k_N \equiv k_{N+1} \equiv \ldots \,(\mathrm{mod}\ 6) \Rightarrow 2^{k_{N-1}} \equiv 2^{k_N} \equiv 2^{k_{N+1}} \equiv \ldots \,(\mathrm{mod}\ 7) \Rightarrow$$

$$\Rightarrow k_N \equiv k_{N+1} \equiv k_{N+2} \equiv \ldots \,(\mathrm{mod}\ 7).$$

Аналогичная задача для самостоятельного решения:

Задача 2* *Пусть дана последовательность чисел:*

$$k_1 = k \in \mathbb{N}, \quad k_2 = k^k, \quad k_3 = k^{k^k}, \ \ldots, k_{n+1} = k^{k_n}, \ \ldots$$

Доказать, что $\forall m \in \mathbb{N}, \ \exists N \in \mathbb{N}: k_N \equiv k_{N+1} \equiv k_{N+2} \equiv \ldots \,(mod\ m)$.

3.4. Извлечение квадратного корня в поле вычетов

При решении квадратных уравнений нам приходилось извлекать корень с помощью перебора. Попытаемся понять, когда это можно сделать, а когда нет.

Определение 2. $a \in \mathbb{Z}_p^\times, p \neq 2$, *называется квадратичным вычетом, если он является полным квадратом, то есть* $\exists b \in \mathbb{Z}_p : b^2 = a$. *Если такого* b *не существует, то он называется квадратичным невычетом.*

Определение 3. *Символом Лежандра называется следующее число:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1, a - \textit{квадратичный вычет}, \\ -1, a - \textit{квадратичный невычет} \end{cases}.$$

То есть, чтобы выяснить извлекается ли квадратный корень из вычета все равно, что посчитать его символ Лежандра. Остается понять как его посчитать.

Выпишем свойства символа Лежандра:

1. Всего ненулевых элементов в поле $p-1$. Из них половина квадратичные вычеты, а другая - квадратичные невычеты, то есть их поровну $\frac{p-1}{2}$. Чтобы это понять, нужно рассмотреть отображение возведения в квадрат $\varphi : \mathbb{Z}_p^\times \to \mathbb{Z}_p^\times : b \mapsto b^2$. Ясно, что помимо b в b^2 переходит и $-b$, но у квадратного уравнения может максимум два корня, а значит других элементов, переходящих в b^2 нет. Если $b = -b$, то $2b = 0$, а так как поле имеют характеристику неравную 2, то на 2 можно сократить и получаем $b = 0$. Но ноль мы из рассмотрения исключили. Поэтому $-b \neq b$ и решений квадратного уравнения $x^2 = b^2$ ровно два.

   Теперь, если для $a \in \mathbb{Z}_p^\times$ существует $b \in \mathbb{Z}_p^\times$ такой, что $b^2 = a$, то существует и второй корень $-b$ и больше нет. Это означает, что не у всех элементов $\mathbb{Z}_p^\times$ есть прообраз, а точнее, он есть только у половины, так как на каждый образ приходится два прообраза. У второй половины решений уравнения $x^2 = a$ нет. Таким образом, число квадратных вычетов и невычетов поровну и равняется $\frac{p-1}{2}$.

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

   Во-первых, почему справа всегда будет либо 1, либо -1? Возведем правую часть в квадрат и применим малую теорему Ферма:

   $$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} = 1 \Leftrightarrow a^{\frac{p-1}{2}} = \pm 1.$$

   Во-вторых, нужно понять когда $+$, а когда $-$. Если a квадратичный вычет, то есть $a = b^2$, тогда

   $$\left(b^2\right)^{\frac{p-1}{2}} = b^{p-1} = 1.$$

Для квадратичного вычета всегда $+1$. Могут ли попасть в эту же категорию квадратичные невычеты? Количество корней уравнения $x^{\frac{p-1}{2}} = 1$ не более, чем $\frac{p-1}{2}$. Но квадратичных вычетов именно такое число и каждый является корнем. Значит других корней нет. Таким образом, для квадратичных невычетов остается единственная возможность -1.

3. Мультипликативное свойство:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Это свойство автоматически следует из пункта 2 и свойства степеней.

Итак, чтобы понять извлекается ли квадратный корень из вычета в соответствующем поле вычетов, нужно посчитать символ Лежандра этого вычета, а не перебирать все подряд.

4. Комплексные числа

4.1. Разбор домашнего задания

Задача 2* *Пусть дана последовательность чисел:*

$$k_1 = k \in \mathbb{N}, \quad k_2 = k^k, \quad k_3 = k^{k^k}, \ \ldots, k_{n+1} = k^{k_n}, \ \ldots$$

Доказать, что $\forall m \in \mathbb{N}, \ \exists N \in \mathbb{N} : k_N \equiv k_{N+1} \equiv k_{N+2} \equiv \ldots (mod\ m)$.

По определению $k_{n+1} = k^{k_n}$. Разложим на простые $m = p_1^{n_1} \cdot \ldots \cdot p_s^{n_s}$. Два числа при делении на m имеют одинаковые остатки тогда и только тогда, когда они имеют одинаковые остатки при делении на $p_i^{n_i}$ (так как разность должна делиться на m). Поэтому сравнимость по модулю m сводится к сравнимости по модулям $p_i^{n_i}$. Это позволяет применить индукцию по m.

Если $s > 1$ можно применить предположении индукции. А если $s = 1, m = p^n$ нужно разбирать два случая: либо НОД$(k, p) = 1$, либо НОД$(k, p) > 1$.

1. Если НОД$(k, p) > 1$, то НОД$(k, p) = p \Rightarrow k \vdots p$. В таком случае с ростом номера k_n степень p в его разложении будет неограниченно расти, а значит, в некоторый момент она станет больше, чем n. Тогда такие члены последовательности будут делиться нацело на p^n, а значит будут все сравнимы с $0\,(\mathrm{mod} m)$.

2. НОД$(k, p) = 1$. Отсюда следует, что НОД$(k, p^n) = 1$, значит, можно применить следствие теоремы Эйлера (точнее как достаточно условие):

$$\exists N \in \mathbb{N} : k_{N-1} \equiv k_N \equiv k_{N+1} \equiv \ldots (\mathrm{mod}\varphi(m)).$$

Но $\varphi(m) < m$, а значит, по предположению индукции утверждение доказано.

4.2. Алгебраические операции над комплексными числами

Всякое комплексное число записывается единственным образом в алгебраической форме:

$$\forall z \in \mathbb{C} \quad \exists x, y \in \mathbb{R} : z = x + iy; \quad x = \Re(z), y = \Im(z).$$

Задача 20.1 г) *Вычислить в алгебраической форме выражение*

$$\frac{(5+i)(7-6i)}{3+i}$$

Выполним умножение в числителе:

$$\frac{35 + 6 + 7i - 30i}{3+i} = \frac{41 - 23i}{3+i}.$$

Чтобы поделить на комплексное число, нужно домножить числитель и знаменатель на сопряженное комплексное число к знаменателю:

$$\frac{(41-23i)(3-i)}{(3+i)(3-i)} = \frac{123-41i-69i-23}{9+1} = \frac{100-110i}{10} = 10-11i.$$

4.3. Геометрическая интерпретация комплексного числа

Операции над векторами соответствуют операциям над комплексными числами. Поэтому, геометрически комплексное число можно интерпретировать как вектор.

1. Сложению комплексных чисел соответствует сумма векторов. (Рис.1).
2. Умножению на действительное число соответствует растяжение/сжатие вектора.
3. Сопряжению соответствует отражение вектора относительно действительно оси.
4. Модуль комплексного числа есть длина вектора.

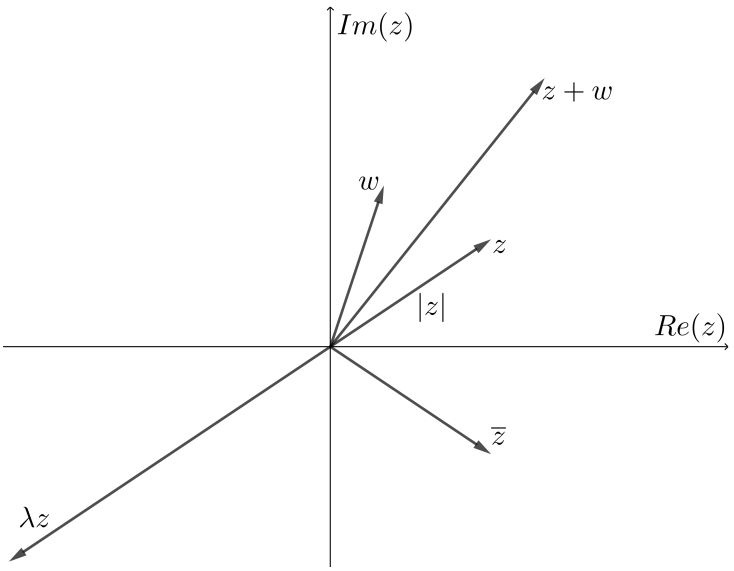


Рис. 1.

Посмотрим как геометрия помогает решить алгебраическую задачу.
Задача 1 *Решить в комплексных числах уравнение*

$$\left|\frac{z+1-i}{z-1+i}\right| = 1.$$

Модуль частного это частное модулей:

$$\left|\frac{z+1-i}{z-1+i}\right| = 1 \Leftrightarrow \frac{|z+1-i|}{|z-1+i|} = 1 \Leftrightarrow |z+1-i| = |z-1+i|\,.$$

Последнее преобразование равносильно в силу того, что, если обе части равенства равны нулю, то и каждый модуль равен нулю, а последнее равносильно равенству нулю самого комплексного числа. В таком случае z должно быть одновременно равно и $1-i$ и $-1+i$, что, естественно, невозможно.

Перепишем теперь последнее равенство следующим образом:

$$|z-(i-1)| = |z-(1-i)|\,.$$

Модуль разности двух вектор есть расстояние между концами этих векторов, то есть можно трактовать как расстояние между двумя точками. Таким образом, последнее равенство есть геометрическое место точек равноудаленных от двух заданных $i-1$ и $1-i$. Это ГМТ есть серединный перпендикуляр к отрезку с концами в указанных точках. (Рис.2)

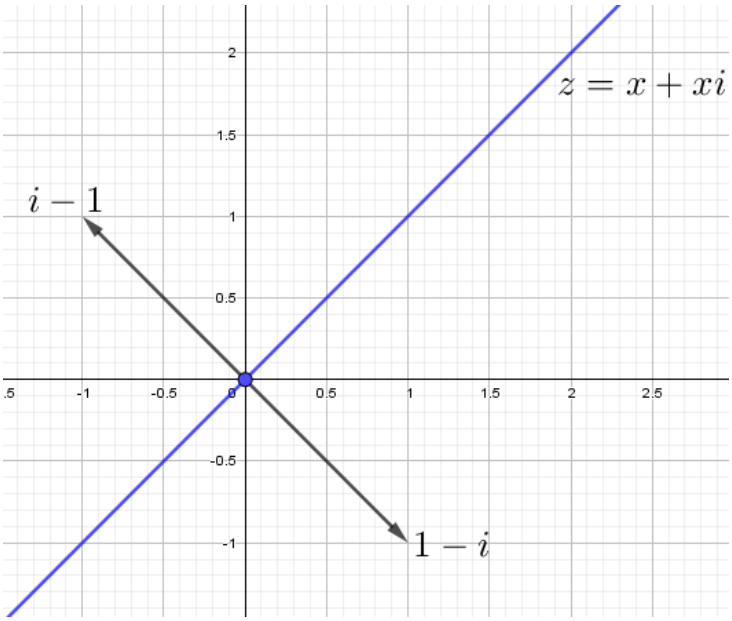


Рис. 2.

Как видно из рисунка 2, серединным перпендикуляром будет прямая $z = x + xi$.

Теперь рассмотрим другую ситуацию, когда алгебра помогает геометрии. Из школьной геометрии известен такой геометрический факт: сумма квадратов диагоналей параллелограмма равняется сумме квадратов всех сторон. Докажем этот факт с помощью алгебры комплексных чисел.

Задача 2 *Доказать, что сумма квадратов диагоналей параллелограмма равняется сумме квадратов всех сторон.*

На рисунке 3 обозначим вектор $\overrightarrow{AB}$ через z, а вектор $\overrightarrow{AD}$ через w. Тогда

$$\overrightarrow{BC} = w, \quad \overrightarrow{DC} = z, \quad \overrightarrow{AC} = z + w, \quad \overrightarrow{DB} = z - w.$$

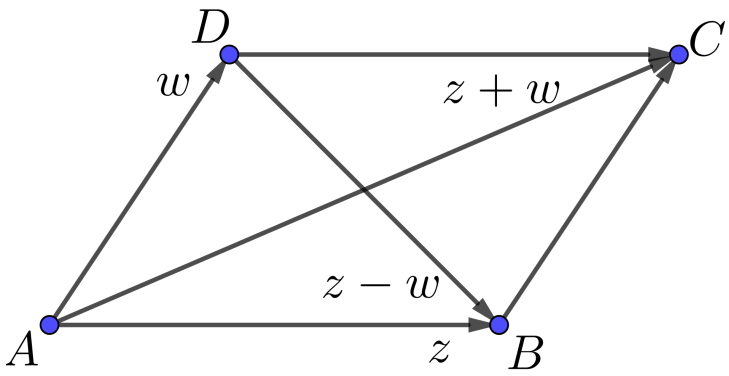


Рис. 3.

Преобразуем сумму квадратов диагоналей с помощью свойства модуля $|z|^2 = z\overline{z}$ и $\overline{z+w} = \overline{z} + \overline{w}$:

$$|z+w|^2 + |z-w|^2 = (z+w)(\overline{z}+\overline{w}) + (z-w)(\overline{z}-\overline{w}) =$$

$$= z\overline{z} + z\overline{w} + w\overline{z} + w\overline{w} + z\overline{z} - z\overline{w} - w\overline{z} + w\overline{w} = 2z\overline{z} + 2w\overline{w} = 2\left(|z|^2 + |w|^2\right).$$

4.4. Тригонометрическая запись комплексного числа

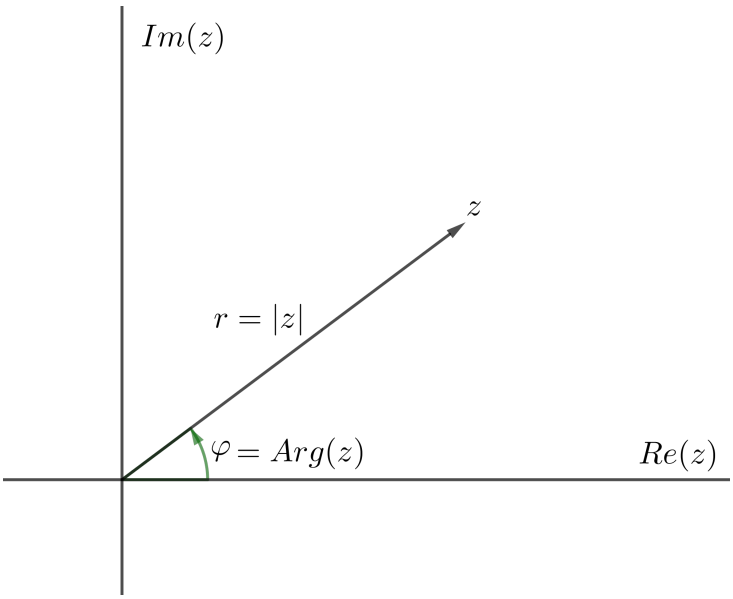


Рис. 4.

С помощью геометрической интерпретации можно ввести другую запись, которая носит название тригонометрической записи комплексного числа. Делается это с помощью рассмотрения прямоугольного треугольника, в котором известны угол между осью абсцисс и вектором φ и длина самого вектора r (Рис.4).

Тогда x и y являются катетами этого прямоугольного треугольника и выражаются через гипотенузу и тригонометрию угла φ :

$$z = r\left(\cos\varphi + i\sin\varphi\right).$$

Угол φ называется аргумент комплексного числа и обозначается $\mathrm{Arg}(z)$. Определен с точностью до $2\pi n, n \in \mathbb{Z}$.

Как известно, при умножении комплексных чисел аргументы складываются, а при делении - вычитаются. Поэтому скобку с тригонометрией можно воспринимать как показательную функцию. Вводится обозначение:

$$e^{i\varphi} := \cos\varphi + i\sin\varphi \Rightarrow z = |z|e^{i\mathrm{Arg}(z)} = re^{i\varphi}.$$

Задача 21.2 е) *Вычислить*

$$\left(\frac{1-i\sqrt{3}}{1+i}\right)^{12}.$$

Воспользуемся тригонометрической записью комплексного числа для числителя и знаменателя:

$$1-i\sqrt{3} = 2\left(\frac{1}{2} - i\frac{\sqrt{3}}{2}\right) = 2\left(\cos\left(-\frac{\pi}{3}\right) + i\sin\left(-\frac{\pi}{3}\right)\right) = 2e^{-i\frac{\pi}{3}};$$

$$1+i = \sqrt{2}\left(\frac{1}{\sqrt{2}} + i\frac{1}{\sqrt{2}}\right) = \sqrt{2}\left(\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)\right) = \sqrt{2}e^{i\frac{\pi}{4}}.$$

$$\left(\frac{1-i\sqrt{3}}{1+i}\right)^{12} = \left(\frac{2e^{-i\frac{\pi}{3}}}{\sqrt{2}e^{i\frac{\pi}{4}}}\right)^{12} = \left(\sqrt{2}e^{-i\frac{7\pi}{12}}\right)^{12} = 2^6 e^{-i7\pi} = 64\left(-1 + i\cdot 0\right) = -64.$$

Очевидно, что, действуя алгебраически, сил было бы затрачено намного больше, чем при использовании тригонометрически записи комплексного числа.

4.5. Задачи тригонометрии

Рассмотрим как комплексные числа помогают решать тригонометрические задачи.

Задача 21.11 в) *Выразить* $\sin(5\varphi)$ *и* $\cos(5\varphi)$ *через* $\sin(\varphi)$ *и* $\cos(\varphi)$.

Воспользуемся формулой Муавра:

$$(\cos\varphi + i\sin\varphi)^5 = \cos 5\varphi + i\sin 5\varphi.$$

То есть то, что нас просят найти, является действительной и мнимой комплексного числа, стоящего слева. Воспользуемся биномом Ньютона (коэффициенты через треугольник Паскаля) для 5 степени:

$$(\cos\varphi + i\sin\varphi)^5 =$$

$$= \cos^5\varphi + 5\cos^4\varphi i\sin\varphi + 10\cos^3\varphi i^2\sin^2\varphi + 10\cos^2\varphi i^3\sin^3\varphi + 5\cos\varphi i^4\sin^4\varphi + i^5\sin^5\varphi =$$

$$= \left(\cos^5\varphi - 10\cos^3\varphi\sin^2\varphi + 5\cos\varphi\sin^4\varphi\right) + i\left(5\cos^4\varphi\sin\varphi - 10\cos^2\varphi\sin^3\varphi + \sin^5\varphi\right) \Rightarrow$$

$$\Rightarrow \cos 5\varphi = \cos^5\varphi - 10\cos^3\varphi\sin^2\varphi + 5\cos\varphi\sin^4\varphi;$$

$$\Rightarrow \sin 5\varphi = 5\cos^4\varphi\sin\varphi - 10\cos^2\varphi\sin^3\varphi + \sin^5\varphi.$$

Задача 21.13 а) *Выразить* $\sin^4\varphi$ *через тригонометрию первой степени, но кратных углов, то есть через* $\sin n\varphi$ *и* $\cos n\varphi$ *для некоторых значений* n.

Воспользуемся экспоненциальной записью комплексного числа:

$$e^{i\varphi} = \cos\varphi + i\sin\varphi, \quad e^{-i\varphi} = \cos\varphi - i\sin\varphi, \quad \Rightarrow \sin\varphi = \frac{e^{i\varphi} - e^{-i\varphi}}{2i}.$$

Теперь воспользуемся биномом Ньютона:

$$\sin^4\varphi = \left(\frac{e^{i\varphi} - e^{-i\varphi}}{2i}\right)^4 = \frac{e^{i4\varphi} - 4e^{i2\varphi} + 6 - 4e^{-i2\varphi} + e^{-i4\varphi}}{16} =$$

$$= \frac{\cos 4\varphi + i\sin 4\varphi - 4\cos 2\varphi - 4i\sin 2\varphi + 6 - 4\cos 2\varphi + 4i\sin 2\varphi + \cos 4\varphi - i\sin 4\varphi}{16} =$$

$$= \frac{2\cos 4\varphi - 8\cos 2\varphi + 6}{16} = \frac{\cos 4\varphi - 4\cos 2\varphi + 3}{8}.$$

4.6. Операция сопряжения

Обозначим через σ отображение $\sigma : \mathbb{C} \to \mathbb{C} : z \mapsto \overline{z}$. Какими свойствами обладает данное отображение?

1. Линейность: $\sigma(z + w) = \sigma(z) + \sigma(w)$.
2. Мультипликативность: $\sigma(zw) = \sigma(z)\sigma(w)$.
3. σ является биекцией $\sigma^{-1} = \sigma$.
4. $\sigma(z) = z, \ \forall z \in \mathbb{R}$.

Первые три свойства говорят, что отображение σ является автоморфизмом. Более того, четвертое свойство говорит, что это автоморфизм поля $\mathbb{C}$ над полем $\mathbb{R}$. Все такие автоморфизмы образуют группу, их можно перемножать. Такая группа называется *группой Галуа*.

Определение 4. *Группой Галуа поля K над полем $L, L \subset K$ называется группа*

$$Gal\,(K/L) := \{\varphi : K \to K \mid \varphi - \textit{автоморфизм}, \varphi(x) = x,\ \forall x \in L\}\,.$$

Таким образом, в группе Галуа $Gal\,(\mathbb{C}/\mathbb{R})$ как минимум имеются два автоморфизма - тождественный id и сопряжение σ. Есть ли там что-то еще? Этот вопрос остается в качестве задачи к следующему семинару.

5. Извлечение корней в поле комплексных чисел и вычисление сумм

5.1. Разбор домашнего задания

Задача 21.12 *Выразить* $\sin nx$ *и* $\cos nx$ *через степени* $\sin x$ *и* $\cos x$.

Будем действовать также как в задаче 21.11 в) на прошлом семинаре. Воспользуемся формулой Муавра:

$$(\cos x + i \sin x)^n = \cos nx + i \sin nx.$$

То есть то, что нас просят найти, является действительной и мнимой комплексного числа, стоящего слева. Воспользуемся биномом Ньютона для 5 степени:

$$(\cos x + i \sin x)^n = \sum_{k=0}^{n} C_n^k \cos^{n-k} x i^k \sin^k x.$$

Теперь нужно выделить вещественную и мнимую части у слагаемого справа. В вещественную часть входят слагаемые при $k = 2l$, так как $i^k = (-1)^l$.

$$(\cos x + i \sin x)^n = \sum_{l=0}^{\left[\frac{n}{2}\right]} C_n^{2l} \cos^{n-2l} x \, (-1)^l \sin^{2l} x + i \sum_{l=0}^{\left[\frac{n-1}{2}\right]} C_n^{2l+1} \cos^{n-2l-1} x \, (-1)^l \sin^{2l+1} x \Rightarrow$$

$$\Rightarrow \cos nx = \sum_{l=0}^{\left[\frac{n}{2}\right]} C_n^{2l} \cos^{n-2l} x \, (-1)^l \sin^{2l} x; \quad \sin nx = \sum_{l=0}^{\left[\frac{n-1}{2}\right]} C_n^{2l+1} \cos^{n-2l-1} x \, (-1)^l \sin^{2l+1} x.$$

Задача 1 (теорема Птолемея) *Пусть в окружность вписан четырехугольник, тогда произведение длин диагоналей равно сумме произведений противоположных сторон.*

Все рассуждения будут строиться с использованием рисунка 5. Пусть мы имеем вписанный в окружность четырехугольник, длины сторон которого обозначим через a, b, c и d. Нам требуется доказаться следующее равенство:

$$ef = ac + bd. \tag{2}$$

Рассмотрим данную задачу на комплексной плоскости. Тогда каждая вершина четырехугольника может быть рассмотрена как комплексное число. Обозначим их, соответственно, через z_1, z_2, z_3 и z_4 как показано на рисунке 5. Тогда каждая сторона может восприниматься как вектор. Перепишем требуемое равенство в этих терминах:

$$|z_1 - z_3| \, |z_2 - z_4| = |z_2 - z_3| \, |z_1 - z_4| + |z_1 - z_2| \, |z_3 - z_4| \, . \tag{3}$$

Перепишем равенство (3) без модулей:

$$(z_1 - z_3)(z_2 - z_4) = (z_2 - z_3)(z_1 - z_4) + (z_1 - z_2)(z_3 - z_4). \tag{4}$$

Равенство (4), очевидно, выполняется для любых z_1, z_2, z_3 и z_4 (достаточно раскрыть скобки слева и справа). Введем обозначения:

$$\zeta_1 := (z_1 - z_3)(z_2 - z_4), \quad \zeta_2 := (z_2 - z_3)(z_1 - z_4), \quad \zeta_3 = (z_1 - z_2)(z_3 - z_4).$$

Тогда равенства (4) и (3) перепишутся в следующем виде:

$$\zeta_1 = \zeta_2 + \zeta_3, \quad |\zeta_1| = |\zeta_2| + |\zeta_3|.$$

Заменив в последнем ζ_1 через $\zeta_2 + \zeta_3$ получим равенство, которое требуется доказать:

$$|\zeta_2 + \zeta_3| = |\zeta_2| + |\zeta_3|. \tag{5}$$

Воспользуемся помощью геометрии. Если ζ_2 и ζ_3 вектора, составляющие две стороны треугольника, то $\zeta_2 + \zeta_3$ третья сторона треугольника. Но из курса школьной геометрии мы знаем, что для любого треугольника выполняется неравество треугольника, которое превращается в равенство тогда и только тогда, когда треугольник схлопывается в отрезок, причем вектора ζ_2 и ζ_3 коллинеарны и сонаправлены. В терминах комплексных чисел соноправленность равносильна совпадению аргументов $\operatorname{Arg}\zeta_2 = \operatorname{Arg}\zeta_3$.

Итак, нам нужно доказать, что $\operatorname{Arg}((z_2 - z_3)(z_1 - z_4)) = \operatorname{Arg}((z_1 - z_2)(z_3 - z_4))$.

Пользуясь свойством аргумента (произведение переходит в сумму), имеем:

$\operatorname{Arg}(z_2 - z_3) + \operatorname{Arg}(z_1 - z_4) = \operatorname{Arg}(z_1 - z_2) + \operatorname{Arg}(z_3 - z_4)$.

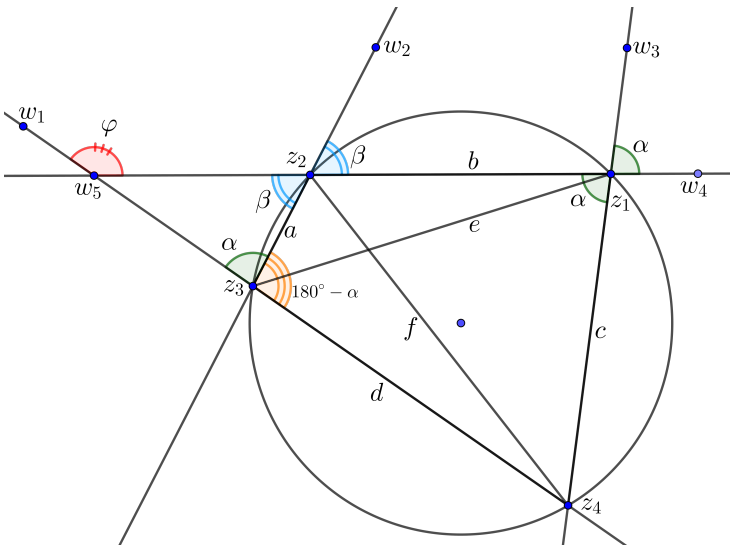


Рис. 5.

Так как аргумент отсчитывается от положительного направления оси абсцисс, то для удобства введем действительную ось вдоль прямой $(z_2 z_1)$ с положительным

направлением вдоль вектора $z_1 - z_2$. В этом случае $\operatorname{Arg}(z_1 - z_2) = 0$. Введем обозначения (см. рис.5):

$$\angle w_3 z_1 w_4 := \alpha = \operatorname{Arg}(z_1 - z_4), \quad \angle w_2 z_2 z_1 := \beta = \operatorname{Arg}(z_2 - z_3),$$

$$\angle w_1 w_5 z_2 := \varphi = \operatorname{Arg}(z_3 - z_4).$$

Угол $\angle z_2 z_1 z_4 = \angle w_3 z_1 w_4 = \alpha$ как вертикальные. Так как четырехугольник вписан в окружность, то сумма противоположных углов равна $180° \Rightarrow \angle z_2 z_3 z_4 = 180° - \angle z_2 z_1 z_4 = 180° - \alpha$. Углы $\angle w_5 z_3 z_2$ и $\angle z_2 z_3 z_4$ смежные, значит в сумме дают $180° \Rightarrow \angle w_5 z_3 z_2 = \alpha$. Углы $\angle w_5 z_2 z_3 = \angle w_2 z_2 z_1 = \beta$. Угол $\angle w_1 w_5 z_2$ является внешним для треугольника $\triangle w_5 z_2 z_3$, поэтому

$$\varphi = \angle w_1 w_5 z_2 = \angle w_5 z_2 z_3 + \angle w_5 z_3 z_2 = \alpha + \beta.$$

Задача 2 *Описать группу Галуа* $Gal(\mathbb{C}/\mathbb{R})$.

На прошлом семинаре было получено, что в рассматриваемой группе как минимум содержится тождественный автоморфизм и автоморфизм сопряжение. Есть ли там что-то еще? Для этого обсудим общие свойства автоморфизма. Будем рассматривать некоторый автоморфизм φ.

1. $\varphi(z + w) = \varphi(z) + \varphi(w)$.
2. $\varphi(zw) = \varphi(z)\varphi(w)$.
3. $\varphi(0) = \varphi(0 + 0) = \varphi(0) + \varphi(0) = 2\varphi(0) \Leftrightarrow \varphi(0) = 0$.
4. $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1)$, но φ биекция, поэтому $\varphi(1) \neq 0 \Rightarrow$ можно сократить и получим $\varphi(1) = 1$.
5. $0 = \varphi(0) = \varphi(z + (-z)) = \varphi(z) + \varphi(-z) \Leftrightarrow \varphi(-z) = -\varphi(z)$.
6. Пусть $z \neq 0$. Тогда $1 = \varphi(1) = \varphi(zz^{-1}) = \varphi(z)\varphi(z^{-1}) \Leftrightarrow \varphi(z^{-1}) = (\varphi(z))^{-1}$.

Рассмотренные свойства верны для любого автоморфизма без требования, чтобы он оставлял какое-то множество на месте. Теперь будем разбираться с тем, что будет, если добавить это требование. Пусть рассматриваем автоморфизм оставляет действительную ось на месте.

$$z = x + iy, \quad \varphi(z) = \varphi(x + iy) = \varphi(x) + \varphi(i)\varphi(y) = x + \varphi(i)y.$$

Остается выяснить чему равно $\varphi(i)$. Для этого воспользуемся основным определением $i^2 = -1 \Rightarrow$

$$\varphi(i^2) = \varphi(i \cdot i) = \varphi(i)\varphi(i) = \varphi(i)^2; \quad \varphi(-1) = -\varphi(1) = -1; \Rightarrow$$

$$\Rightarrow (\varphi(i))^2 = -1 \Leftrightarrow \varphi(i) = \pm i.$$

Если знак $+$, то $\varphi = id$. Если $-$, то $\varphi = \sigma$. Других случаев нет. Таким образом, $Gal(\mathbb{C}/\mathbb{R}) = \{id, \sigma\}$.

5.2. Извлечение корней в поле комплексных чисел

Рассмотрим ненулевое комплексное число z. Тогда его можно представить в тригонометрической форме $z = r(\cos\varphi + i\sin\varphi)$. Корнями степени n из числа z называются решения в комплексных числах уравнения $w^n = z$. Таких корней ровно n. Обозначим их через $w_0, w_1, ..., w_{n-1}$. Формула вычисления следующая:

$$w_k = \sqrt[n]{r}\left(\cos\left(\frac{\varphi + 2\pi k}{n}\right) + i\sin\left(\frac{\varphi + 2\pi k}{n}\right)\right), \quad k = 0, ..., n-1. \tag{6}$$

Геометрически корни изображаются вершинами правильного n-угольника (рис. 6), вписанного в окружность радиуса $\sqrt[n]{r}$.

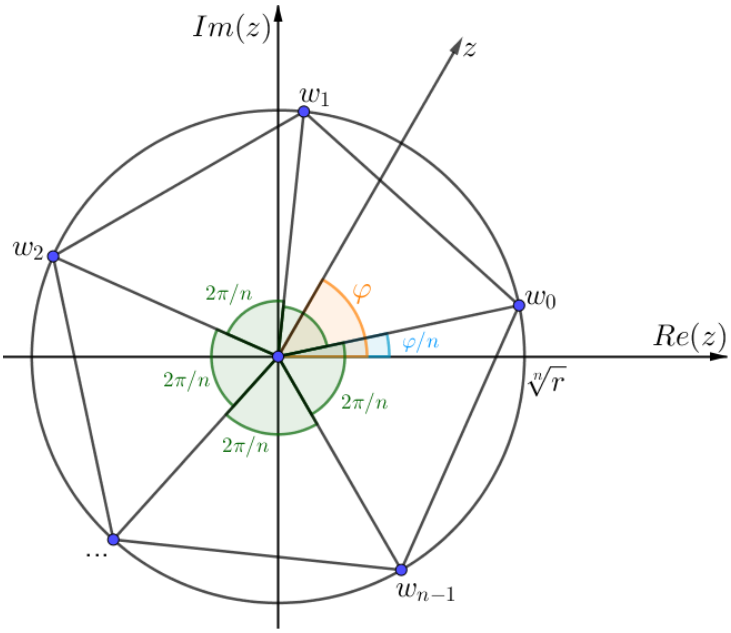


Рис. 6.

Отдельного внимания заслуживают корни из 1. Эти корни имеют специальное обозначение $\varepsilon_0, \varepsilon_1, ..., \varepsilon_{n-1}$ и вычисляются аналогично (частный случай формулы 6):

$$\varepsilon_k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right), \quad k = 0, ..., n-1.$$

Эти корни также образуют правильный n-угольник на комплексной плоскости, вписанный в единичную окружность, причем вершина ε_0 совпадает с точкой $1 + i0$.

Полезный факт заключается в том, что, если один из корней каким-то образом получен, то все остальные корни получаются умножением найденного на все корни из единицы. То есть, например, если угадан корень w_0, то $w_k = w_0\varepsilon_k$. Или общая формула: $w_{k+l} = w_k\varepsilon_l$.

Множество корней n степени из 1 обозначается через $\mathbb{U}_n$ и является группой относительно умножения. Разберемся как оно устроено при небольших значениях n.

1. $\mathbb{U}_1 = \{1\}$.
2. $\mathbb{U}_2 = \{-1, 1\}$.
3. $\mathbb{U}_3 = \left\{1, \frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right\}$. Рис. 7
4. $\mathbb{U}_4 = \{\pm 1, \pm i\}$. Рис. 7

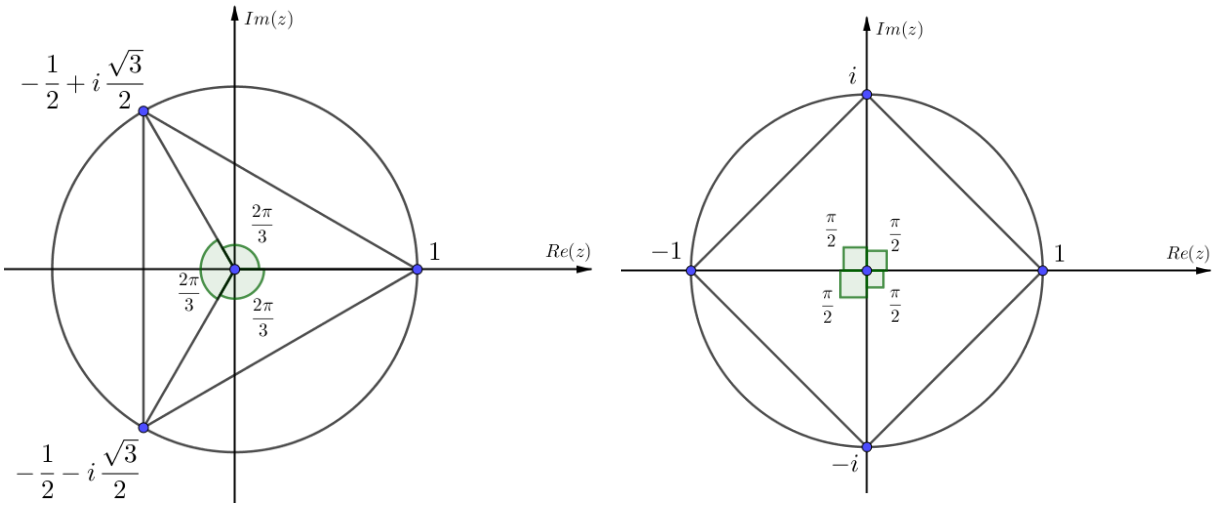


Рис. 7.

Задача 22.7 м) *Найти множество корней* $\sqrt[4]{8\sqrt{3}i - 8}$

Обозначим подкорневое комплексное число через z и представим его в комплексной форме:

$$z = 8\sqrt{3}i - 8 = 16\left(-\frac{1}{2} + i\frac{\sqrt{3}}{2}\right) = 16\left(\cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)\right).$$

Можно действовать по-разному. Можно вычислить в лоб по формуле, но так как мы уже знаем группу $\mathbb{U}_4$, то найдем w_0 и умножим его на каждый элемент группы.

$$w_0 = 2\left(\cos\left(\frac{\pi}{6}\right) + i\sin\left(\frac{\pi}{6}\right)\right) = 2\left(\frac{\sqrt{3}}{2} + i\frac{1}{2}\right) = \sqrt{3} + i.$$

Так как, чтобы перейти к w_1 нужно добавить аргумент $\pi/2$, то нужно умножать каждый раз на i :

$$w_1 = w_0 \cdot i = -1 + i\sqrt{3}, \quad w_2 = w_1 \cdot i = -\sqrt{3} - i, \quad w_3 = w_2 \cdot i = 1 - i\sqrt{3}.$$

Можно было не прибегать к аргументу, а написать сразу:

$$\sqrt[4]{8\sqrt{3}i-8} = w_0 \cdot \mathbb{U}_4 = \left\{\pm\sqrt{3} \pm i, \mp 1 \pm i\sqrt{3}\right\}.$$

Геометрическая иллюстрация (рис. 8) получается из геометрической иллюстрации для группы $\mathbb{U}_4$ поворотом против часовой стрелки на $\pi/6$, так как аргумент w_0 равен $\pi/6$.

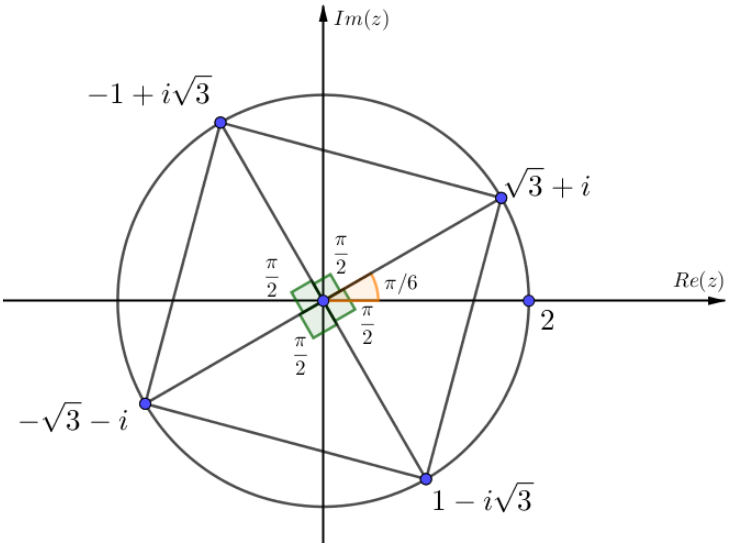


Рис. 8.

Обратим внимание, что комплексное число z и w_1 сонаправлены как вектора, так как имеют одинаковый аргумент.

5.3. Свойства корней из 1

Зададимся вопросом: чему равны сумма всех корней n степени из 1 и их произведение:

$$1)\ \varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{n-1} = ? \qquad 2)\ \varepsilon_0 \cdot \varepsilon_1 \cdot \ldots \cdot \varepsilon_{n-1} = ?$$

Чтобы это понять, нужно заметить следующий факт. Применим общую формулу $w_{k+l} = w_k\varepsilon_l$ к элементам группы $\mathbb{U}_n$:

$$\varepsilon_{k+1} = \varepsilon_k\varepsilon_1.$$

То есть последовательность ε_k образует геометрическую прогрессию с первым членом 1 и знаменателем $\varepsilon_1 \neq 1$. Таким образом, получаем:

$$\varepsilon_0 + \varepsilon_1 + \ldots + \varepsilon_{n-1} = \frac{1-\varepsilon_1^n}{1-\varepsilon_1} = \frac{1-1}{1-\varepsilon_1} = 0.$$

Для произведения нужно рассмотреть два случая.

1. n - четное. Для каждого корня выше действительной оси есть симметричный (сопряженный) корень ниже действительной оси (рис.8). То есть для ε_k симметричный корень ε_{n-k}. Их модули одинаковы и равны 1, а аргументы противоположны, значит $\varepsilon_k\varepsilon_{n-k} = 1$. Осталось рассмотреть числа на вещественной оси $k = 0$ и $k = n/2$. В первом случае это 1, во втором -1. В итоге получаем, что произведение равно -1.

2. n - нечетное. Рассуждения абсолютно такие же как в случае с четным n, только для ε_0 нет пары, но $\varepsilon_0 = 1$, следовательно, и все произведение равно 1.

Одной формулой можно записать так $\varepsilon_0 \cdot \varepsilon_1 \cdot \ldots \cdot \varepsilon_{n-1} = (-1)^{n-1}$.

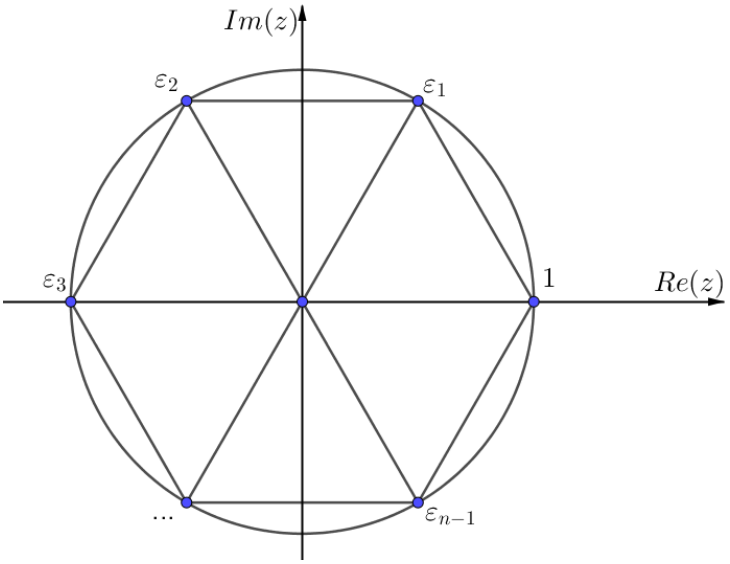


Рис. 9.

Можно рассуждать и с использованием факта о геометрической прогрессии:

$$\varepsilon_0 \cdot \varepsilon_1 \cdot \ldots \cdot \varepsilon_{n-1} = \varepsilon_1^{1+2+\ldots+n-1} = \varepsilon_1^{\frac{n(n-1)}{2}} = (\varepsilon_1^n)^{\frac{n-1}{2}} = 1^{\frac{n-1}{2}}.$$

Написать далее 1 нельзя, так как мы работаем в поле комплексным чисел. Если $n = 2k + 1$, то $1^k = 1$. Если же $n = 2k$, то $\sqrt{1^{2k-1}} = \sqrt{1} = \pm 1$. В этом случае мы получили, что есть две возможности, но так как они осуществляются без влияния k (в записи $\sqrt{1}$ отсутсвует k), то соответствующий знак будет верен при любом k. Группа $\mathbb{U}_2$ состоит из двух элементов 1 и -1, произведение которых равно -1. Поэтому в четном случае будет -1.

Отметим еще некоторые простейшие факты о корнях из 1. $\varepsilon_{n-k} = \varepsilon_k^{-1} = \overline{\varepsilon}_k$ при $k \neq 0$ и, если n четно, $k \neq n/2$, так как в этом случае $\varepsilon_{n/2} = -1$, то есть лежит на действительной оси. Отсюда следует, что достаточно найти все корни из 1 до номера

$\left[\frac{n+1}{2}\right] - 1$ включительно, а остальные получаются сопряжением найденных и, если случай четного n, добавлением -1.

5.4. Вычисление сумм с помощью комплексных чисел

Мы уже видели, что комплексные числа могут помогать в решение задач по геометрии, тригонометрии, а теперь обсудим как их использовать при подсчете сумм действительных чисел.

Выпишем суммы, которые получаются из бинома Ньютона

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$$

при соответствующих значениях a и b.

1. При $a = b = 1$ получаем: $C_n^0 + C_n^1 + C_n^2 + ... + C_n^n = 2^n$.
2. При $a = 1$ и $b = -1$ получаем: $C_n^0 - C_n^1 + C_n^2 - ... + (-1)^n C_n^n = 0$.
3. Из предыдущего пункта имеем: $C_n^0 + C_n^2 + C_n^4 + ... = C_n^1 + C_n^3 + C_n^5 + ... = 2^{n-1}$. Последнее равенство берется из первого пункта, так как первая и вторая часть этого равенства есть половины от суммы всех биномиальных коэффициентов.

Теперь с помощью комплексных чисел найдем две суммы:

$$x := C_n^0 - C_n^2 + C_n^4 - C_n^6 + ..., \quad y := C_n^1 - C_n^3 + C_n^5 - C_n^7 + ...$$

Рассмотрим бином Ньютона для комплексных чисел $a = 1$ и $b = i$:

$$(1+i)^n = C_n^0 + C_n^1 i + C_n^2 i^2 + C_n^3 i^3 + C_n^4 i^4 + C_n^5 i^5 + C_n^6 i^6 + C_n^7 i^7 + C_n^8 i^8 + ... =$$

$$= C_n^0 + C_n^1 i - C_n^2 - C_n^3 i + C_n^4 + C_n^5 i - C_n^6 - C_n^7 i + C_n^8 + ... =$$

$$\left(C_n^0 - C_n^2 + C_n^4 - C_n^6 + ...\right) + i\left(C_n^1 - C_n^3 + C_n^5 - C_n^7 + ...\right) = x + iy.$$

Таким образом, искомые суммы есть действительная и мнимая части числа $(1+i)^n$ соответственно. Рассмотрим это число в тригонометрической форме и применим формулу Муавра:

$$1 + i = \sqrt{2}\left(\cos\left(\frac{\pi}{4}\right) + i\sin\left(\frac{\pi}{4}\right)\right) \Rightarrow (1+i)^n = 2^{\frac{n}{2}}\left(\cos\left(\frac{\pi n}{4}\right) + i\sin\left(\frac{\pi n}{4}\right)\right).$$

Отсюда находим:

$$x = 2^{\frac{n}{2}}\cos\left(\frac{\pi n}{4}\right), \quad y = 2^{\frac{n}{2}}\sin\left(\frac{\pi n}{4}\right).$$

6. Теорема Безу, схема Горнера, алгоритм Евклида для многочлена

6.1. Деление многочленов с остатком. Схема Горнера

Пусть K - некоторое поле. $K[x]$ - кольцо многочленов над полем K.

Теорема 3. $\forall f, g \in K[x]\ \exists!\ q, r \in K[x] : f = gq + r,\ \deg r < \deg g.$

Теорема 4 (Безу)**.** $f(x) = (x - x_0)q(x) + f(x_0)$

Деление на линейный двучлен можно производить не только столбиком, но более компактным способом - схема Горнера. Введем обозначения:

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + ... + a_n,\ q(x) = b_0x^{n-1} + b_1x^{n-2} + b_2x^{n-2} + ... + b_{n-1},\ f(x_0) = c.$$

Два многочлена совпадают, если совпадают их соответствующие коэффициенты. Выпишем соответствующие коэффициенты при соответствующих степенях слева и справа:

$$\begin{cases} n: & a_0 = b_0 \\ n-1: & a_1 = b_1 - b_0x_0 \\ n-2: & a_2 = b_2 - b_1x_0 \\ \vdots & \vdots \\ k: & a_k = b_k - b_{k-1}x_0 \\ \vdots & \vdots \\ 1: & a_{n-1} = b_{n-1} - b_{n-2}x_0 \\ 0: & a_n = c - b_{n-1}x_0 \end{cases}$$

Эти равенства можно рассматривать как систему на b_i и c. Перепишем эту систему следующим образом:

$$\begin{cases} b_0 = a_0 \\ b_1 = a_1 + b_0x_0 \\ b_2 = a_2 + b_1x_0 \\ \vdots \\ b_k = a_k + b_{k-1}x_0 \\ \vdots \\ b_{n-1} = a_{n-1} + b_{n-2}x_0 \\ c = a_n + b_{n-1}x_0 \end{cases}$$

Это сразу нам дает решение: из первого равенства мы находим b_0. Зная b_0, из второго равенства находим b_1. Зная b_1, из третьего равенства находим b_2 и так далее.

Эту цепочку действий удобно записывать виде таблицы из двух рядов, которая и называется *схемой Горнера*.

	a_0	a_1	a_2	...	a_{k-1}	a_k	...	a_{n-1}	a_n
x_0	b_0	b_1	b_2	...	b_{k-1}	b_k	...	b_{n-1}	c

Дополнительное преимущество схемы Горнера: можно вычислять значение многочлена в точке x_0. Почему так стоит делать? Все дело в количестве выполняемых операций. При достаточно больших степенях вычисление может занять очень много времени.

Выясним, сколько мы делаем операций умножения, подставляя некоторое значение x_0 в многочлен, то есть обычным способом. Понятно, что вычислять каждый раз заново степень не имеет смысла, нужно использовать вычисленную ранее предыдущую степень. То есть на степени уходит $n-1$ умножение. Теперь нужно умножить на коэффициенты. Так как степеней n, то и умножений n. В итоге получается $2n-1$ умножение. Теперь сравним со схемой Горнера. Из таблицы видно, что умножать нужно от b_1 до c, то есть n раз. Таким образом, схема Горнера в 2 раза быстрее.

Задача 26.1 г) *Выполнить деление многочлена* $f(x) = x^4 - 3x^3 - 10x^2 + 2x + 5$ *на* $x + 2$ *с остатком и найти* $f(-2)$.

В данном случае $x_0 = -2$. Применим схему Горнера:

	1	−3	−10	2	5
−2	1				

Шаг 1 $\longrightarrow$

	1	−3	−10	2	5
−2	1	$-2\cdot 1 - 3 = -5$			

Шаг 2 $\longrightarrow$

	1	−3	−10	2	5
−2	1	−5	$-2\cdot -5 - 10 = 0$		

Шаг 3 $\longrightarrow$

	1	−3	−10	2	5
−2	1	−5	0	$-2\cdot 0 + 2 = 2$	

Шаг 4 $\longrightarrow$

	1	−3	−10	2	5
−2	1	−5	0	2	$-2\cdot 2 + 5 = 1$

Шаг 5 $\Rightarrow$

	1	−3	−10	2	5
−2	1	−5	0	2	1

Теперь можем написать результат деления с остатком:

$$f(x) = (x+2)\left(x^3 - 5x^2 + 2\right) + 1 \Rightarrow f(-2) = 1.$$

6.2. Разложение многочлена по степеням $x - x_0$

Применим теорему Безу несколько раз. Пусть $f(x) = (x - x_0)q_1(x) + c_0$. Поделим $q_1(x)$ на $(x - x_0) : q_1(x) = (x - x_0)q_2(x) + c_1$. Тогда

$$f(x) = (x - x_0)^2 q_2(x) + c_1(x - x_0) + c_0.$$

Продолжим эту процедуру для $q_i(x)$ до тех пор, пока степень $q_i(x)$ не станет равна 0 :

$$f(x) = c_0 + c_1(x - x_0) + c_2(x - x_0)^2 + ... + c_n(x - x_0)^n.$$

Это и есть разложение многочлена $f(x)$ по степеням $(x - x_0)$. Так как каждый раз мы делили на $x - x_0$, то это можно и удобно сделать по схеме Горнера. Коэффициенты c_k связаны с производными многочлена следующей формлуй:

$$c_k \cdot k! = f^{(k)}(x).$$

Здесь важно учитывать характеристику поля при вычислении $k!$.

Задача 26.2 а) *Разложить мночлен* $f(x) = x^5 - 4x^3 + 6x^2 - 8x + 10$ *по степеням* $x - 2$ *и вычислить все производные в точке* $x = 2$.

Будем действовать по схеме Горнера.

	1	0	−4	6	−8	10
2	1					

Шаг 1 $\longrightarrow$

	1	0	−4	6	−8	10
2	1	2				

Шаг 2 $\longrightarrow$

	1	0	−4	6	−8	10
2	1	2	0			

Шаг 3 $\longrightarrow$

	1	0	−4	6	−8	10
2	1	2	0	6		

Шаг 4 $\longrightarrow$

	1	0	−4	6	−8	10
2	1	2	0	6	4	

Шаг 5 $\longrightarrow$

	1	0	−4	6	−8	10
2	1	2	0	6	4	18

Шаг 6

В нижней строке мы получили коэффициенты $q_1(x)$ и $c_0 = 18$. Не начиная новой таблицы, продолжим данную просто вниз. Будем продолжать процедуру, пока не останется одна ячейка. Значения c_i выделим в рамку.

	1	0	−4	6	−8	10
2	1	2	0	6	4	$\boxed{18} = c_0$
2	1	4	8	22	$\boxed{48} = c_1$	
2	1	6	20	$\boxed{62} = c_2$		
2	1	8	$\boxed{36} = c_3$			
2	1	$\boxed{10} = c_4$				
2	$\boxed{1} = c_5$					

Тогда разложение по степеням $x - 2$ будет иметь вид:

$$f(x) = 18 + 48\,(x-2) + 62\,(x-2)^2 + 36\,(x-2)^3 + 10\,(x-2)^4 + (x-2)^5\,.$$

Значения $f^{(k)}(2), k \geqslant 0$ найдем по формуле $f^{(k)}(x) = c_k k!$:

$$f(2) = c_0 0! = 18, \quad f^{(1)}(2) = c_1 1! = 48, \quad f^{(2)}(2) = c_2 2! = 124, \quad f^{(3)}(2) = c_3 3! = 216,$$

$$f^{(4)}(2) = c_4 4! = 240, \quad f^{(5)}(2) = c_5 5! = 120, \quad f^{(m)}(2) = 0, m \geqslant 6.$$

6.3. Понятие кратности корня

Определение 5. *Корень x_0 является корнем многочлена $f(x)$ кратности k, если $f(x)$ делится нацело на $(x - x_0)^k$, но не делится нацело на $(x - x_0)^{k+1}$.*

Утверждение 3. *Корень x_0 кратности k тогда и только тогда, когда в разложении многочлена по степеням $x - x_0$ выполнены равенства: $c_0 = c_1 = ... = c_{k-1} = 0 \neq c_k$.*

Утверждение 3 в терминах производной переписывается так: $f(x_0) = f'(x_0) = f''(x_0) = ... = f^{(k-1)}(x_0) = 0 \neq f^{(k)}(x_0)$. Эта равносильность верна только при условии $\mathrm{char} K = 0$.

Задача 26.3 а) *Определить степень кратности числа x_0 для многочлена $f(x)$, если: $f(x) = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8, x_0 = 2$.*

Применим схему Горнера для $x - x_0$:

	1	-5	7	-2	4	-8
2	1	-3	1	0	4	$\boxed{0} = c_0$
2	1	-1	-1	-2	$\boxed{0} = c_1$	
2	1	1	1	$\boxed{0} = c_2$		
2	1	3	$\boxed{7} = c_3$			

Так как $c_0 = c_1 = c_2 = 0 \neq c_3$, кратность $x_0 = 2$ равна трем.

Задача 26.5 *Дан многочлен $f(x) = ax^{n+1} + bx^n + 1$. При каких значениях a и b этот многочлен делится нацело на $(x - 1)^2$?*

Так как требуется делимость на $(x - 1)^2$, то число $x_0 = 2$ является корнем кратности как минимум 2. Это означает, что $c_0 = c_1 = 0$, а это, в свою очередь, влечет $f(1) = f'(1) = 0$. Выпишем эти два условия:

$$\begin{cases} 0 = f(1) = a + b + 1 \\ 0 = f'(1) = (n+1)a + bn \end{cases} \Leftrightarrow \begin{cases} a = n \\ b = -n - 1 \end{cases}$$

6.4. НОД двух многочленов

Определение 6. *Мночлен $d(x)$ называется наибольшим общим делителем многочленов $f(x)$ и $g(x)$, если он делит каждый из многочленов, а любой другой общий делитель делит $d(x)$. Обозначается d=НОД(f,g).*

Наибольший общий делитель всегда существует и определен с точностью до умножения на ненулевую константу. НОД находится по алгоритму Евклида.

1. Делим многочлен f на g с остатком $f = gq_1 + r_1$.
2. Делим многочлен g на r_1 с остатком $g = r_1q_2 + r_2$.
3. Делим многочлен r_1 на r_2 с остатком $r_1 = r_2q_3 + r_3$.

...

4. Делим многочлен r_{k-1} на r_k с остатком $r_{k-1} = r_kq_{k+1} + r_{k+1}$.

...

5. Степени остатком убывают, поэтому в какой-то момент $r_{s-1} = r_sq_{s+1}$. Тогда НОД=r_s.

Задача 25.2 а) *Найти НОД двух многочленов* $f(x) = x^4+x^3-3x^2-4x-1, g(x) = x^3 + x^2 - x - 1$.

Заметим, что, если в процессе алгоритма Евклида умножить некоторый остаток r_{k-1} на некоторое ненулевое число, то остаток r_{k+1} также умножится на это число и так дойдет до НОДа. Но мы уже сказали, что НОД определен с точностью до умножения на ненулевую константу. Поэтому, если в процессе деления многочленов в столбик встретим дробные коэффициенты, то попытаемся этого избежать за счет домножения на некоторое ненулевое число. Так, на втором шаге многочлен $g(x)$ удобно будет умножить на 2, а первый остаток на -1.

$$\begin{array}{r|l} x^4 + x^3 - 3x^2 - 4x - 1 & x^3 + x^2 - x - 1 \\ \hline -\,x^4 + x^3 - x^2 - x & x \\ \hline -2x^2 - 3x - 1 & \end{array} \longrightarrow \begin{array}{r|l} 2x^3 + 2x^2 - 2x - 2 & 2x^2 + 3x + 1 \\ \hline -\,2x^3 + 3x^2 + x & x - \frac{1}{2} \\ \hline -x^2 - 3x - 2 & \\ -x^2 - \frac{3}{2}x - \frac{1}{2} & \\ \hline -\frac{3}{2}x - \frac{3}{2} & \end{array}$$

$$\longrightarrow \begin{array}{r|l} 2x^2 + 3x + 1 & x + 1 \\ \hline -\,2x^2 + 2x & 2x + 1 \\ \hline x + 1 & \\ x + 1 & \\ \hline 0 & \end{array}$$

Таким образом, НОД$(f, g) = x + 1$.

Алгоритм Евклида также говорит о том, что НОД двух многочленов можно выразить через эти многочлены:

$$\text{НОД}\,(f, g) = uf + vg,\ \ u, v \in K[x]. \tag{7}$$

Многочлены u и v определены неоднозначно. Так, например, если из v вычесть f, а к u прибавить g, то равенство сохранится. Однако, мы можем наложить некоторые ограничения, которых уже будет следовать одназначная определенность.

Обозначим через d НОД f и g. Поделим 7 на d. Тогда $f = d \cdot \overline{f}$ и $g = d \cdot \overline{g}$, где многочлены $\overline{f}$ и $\overline{g}$ взаимнопросты. Равенство 7 примет вид:

$$1 = u\overline{f} + v\overline{g}. \tag{8}$$

Поделим многочлен u с остатком на $\overline{g}$:

$$1 = (\overline{g}q + u_0)\,\overline{f} + v\overline{g} = u_0\overline{f} + \underbrace{\left(q\overline{f} + v\right)}_{=:v_0}\overline{g} = u_0\overline{f} + v_0\overline{g}. \tag{9}$$

Теперь у нас есть ограничение $\deg u_0 < \deg \overline{g}$. Тогда $\deg\left(u_0\overline{f}\right) < \deg\left(\overline{f}\overline{g}\right)$. Теперь, если $\deg v_0 \geqslant \deg \overline{f}$, то второе слагаемое имеет степень выше, чем $\deg\left(\overline{f}\overline{g}\right)$, но в сумме они должны давать константу, а значит старшие степени обязаны сократиться, что противоречит наличию разных степеней у слагаемых. Таким образом, $\deg v_0 < \deg \overline{f}$.

Теперь вернемся к представлению НОДа, домножив (9) на d :

$$d = u_0 f + v_0 g,\ \ \deg u_0 < \deg \overline{g} = \deg g - \deg d,\ \ \deg v_0 < \deg \overline{f} = \deg f - \deg d. \tag{10}$$

Докажем теперь, что такое разложение единственно. Предположим, что существует еще одно разложение с аналогичными условиями:

$$d = u_0 f + v_0 g = u_1 f + v_1 g, \tag{11}$$

$$\deg u_0, \deg u_1 < \deg g - \deg d, \quad \deg v_0, \deg v_1 < \deg f - \deg d.$$

Перепишем (11) следующим образом:

$$(u_0 - u_1)\,f = (v_1 - v_0)\,g\,\big|\,{:}\,d \ \Leftrightarrow (u_0 - u_1)\,\overline{f} = (v_1 - v_0)\,\overline{g}.$$

Левая часть, очевидно, делится на $\overline{f}$, значит, должна и правая, но в силу взаимной простоты $\overline{f}$ и $\overline{g}$ следует, что должна делиться на $\overline{f}$ разность $v_1 - v_0$. Однако, степень этой разности строго меньше степени $\overline{f}$. Поэтому такая ситуция возможно при $v_1 - v_0 = 0$, что равносильно равенству $v_1 = v_0$. А уже отсюда, подставив в (11), следует $u_1 = u_0$, так как $f \neq 0$. Таким образом, единственность доказана.

На практике используется метод неопределенных коэффициентов. Представляем u_0 и v_0 как многочлены с неизвестными коэффициентами. Мы можем так сделать в силу того, что знаем максимально возможную степень из указанных ограничений. Далее находим наибольший общий делить. Раскрываем в 7 скобки, приводим подобные и получаем на неизвестные коэффициенты систему линейных алгебраических уравнений, которую мы уже знаем как решать.

Задача 25.3 а) *Найти наибольший общий делитель многочленов* $f(x) = x^4 + 2x^3 - x^2 - 4x - 2$ *и* $g(x) = x^4 + x^3 - x^2 - 2x - 2$ *и его выражение в виде линейной комбинации* f *и* g.

Найдем НОД с помощью алгоритма Евклида.

$$\begin{array}{r|l} x^4+2x^3-x^2-4x-1 & x^4+x^3-x^2-2x-2 \\ \hline -\,x^4+x^3-x^2-2x-2 & x \\ \hline x^3\quad -2x & \end{array} \longrightarrow \begin{array}{rrrr|l} x^4 & +x^3 & -x^2 & -2x\ -2 & x^3-2x \\ \hline -\,x^4 & & -2x^2 & & x+1 \\ \hline & x^3 & +x^2 & -2x\ -2 & \\ & x^3 & & -2x & \\ \hline & & x^2 & -2 & \end{array}$$

$$\longrightarrow \begin{array}{r|l} x^3-2x & x^2-2 \\ \hline -\,x^3-2x & x \\ \hline 0 & \end{array}$$

Итак, $(f,g) = x^2 - 2$. Степень НОД равна двум. Значит, многочлены u_0 и v_0 должны быть не выше степени 2, то есть будем рассматривать линейными.

$$x^2 - 2 = (ax+b)\left(x^4+2x^3-x^2-4x-2\right) + (cx+d)\left(x^4+x^3-x^2-2x-2\right) =$$

$$= (a+c)\,x^5 + (2a+b+c+d)\,x^4 + (-a+2b-c+d)\,x^3 + (-4a-b-2c-d)\,x^2 +$$

$$+ (-2a-4b-2c-2d)\,x - 2b - 2c \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} x^5: & 0 = a + c \\ x^4: & 0 = 2a + b + c + d \\ x^3: & 0 = -a + 2b - c + d \\ x^2: & 1 = -4a - b - 2c - d \\ x^1: & 0 = -2a - 4b - 2c - 2d \\ x^0: & -2 = -2b - 2d \end{cases}$$

Из первого уравнения находим $c = -a$. С учетом этого из второго уравнения находим $d = -a - b$. С учетом первого и второго условия из третьего уравнения находим $b = a \Rightarrow d = -2a$. Мы выразили все переменные через a. Подставим найденное в четвертое уравнение и получим $a = -1 \Rightarrow b = -1, c = 1$ и $d = 2$. Нетрудно

проверить, что найденные значения удовлетворяют оставшимся двум уравнениям. Таким образом, разложение НОД в линейную комбинацию 10 имеет вид:

$$(f, g) = (-x - 1)\, f + (x + 2)\, g.$$

7. Неприводимые многочлены, редукция

7.1. Неприводимые многочлены

Теорема 5. *Неприводимых многочленов над произвольным полем бесконечно много.*

Это теорема аналог теоремы Евклида для простых чисел.

Доказательство: От противного. Пусть имеется только конечный набор неприводимых многочленов $p_1, ..., p_n \in K[x]$. Тогда рассмотрим многочлен $f = p_1 \cdot ... \cdot p_n + 1$. Очевидно, что он не делится ни на один из многочленов p_i. Но мы знаем, что любой многочлен раскладывается в произведение неприводимых множителей с точностью до ассоциирования. Выходит, что f должен раскладываться в произведение p_i, но это невозможно, так как не делится ни на один из них. Таким образом, либо существуют еще неприводимые многочлены помимо рассмотренных, либо f сам неприводим. В обоих случаях получаем противоречие с предположением о конечности количества неприводимых многочленов. ■

Если поле K бесконечно, то предъявить неприводимые очень легко. Рассмотрим линейный многочлен $x - x_0$, где x_0 пробегает все значения из поля. Все такие многочлены неприводимы и их бесконечно много. Поэтому считаем, что рассмотрение бесконечного поля не приводит к интересным результатам.

Пусть теперь поле K конечно. Если многочлен заданной степени n, то количество коэффициентов равно $n+1$ и каждый принимает значения из конечного поля, а значит, и количество неприводимых многочленов заданной степени конечное число. Соответственно, количество неприводимых многочленов не выше заданной степени также конечное число. Но по теореме 5 их бесконечное число, значит, существует неприводимый многочлен степени выше заданной, причем какую бы мы не взяли. В итоге получаем, что над неприводимым полем существуют неприводимые многочлены сколь угодно большой степени. Это вовсе не означает, что для каждой степени найдется неприводимый многочлен. Однако, оказывается, что существуют неприводимые многочлены любой степени.

На практике встает вопрос о поиске неприводимых многочленов или о понимание того, является предъявленный многочлен неприводимым или нет. Для целых чисел есть классический метод под названием Решето Эратосфена. Выписывается в ряд числа от 2 до рассматриваемого n. Число 2 простое, обводим его и вычеркиваем все числа, которые делятся на 2. Первое после 2 невычеркнутое является простым, так как оно не делится на два, а до двойки чисел не было. Обводим 3 и вычеркиваем все числа, делящиеся на 3. Первое невычеркнутое после 3 является простым, так как оно не делится ни на 2 ни на 3 (иначе бы вычеркнули), а до 2 и 3 чисел нет. Обводим

и продолжаем алгоритм. Конечно, его можно упростить в плане операци, но на суть это не влияет. Аналогичную процедуру можно предъявлить для многочленов над конечным полем.

7.2. Решето Эратосфена для многочленов над конечным полем

Если для целых чисел мы сравнивали величину числа, то у многочленов будем перебирать по степени. Начинаем с 1.

$\deg = 1$ Все многочлены первой степени неприводимы, выписываем их.

$\deg = 2$ Выписываем все многочлены второй степени. Вычеркиваем те, которые делятся на многочлены первой степени. Оставшиеся получаются неприводимыми.

$\deg = 3$ Выписываем все многочлены третьей степени. Вычеркиваем те, которые делятся на многочлены меньшей степени, причем достаточно смотреть делимость на неприводимые многочлены, которые как раз невычеркнуты, так как любой приводимый раскладывается в произведение неприводимых.

... ...

$\deg = n$ Выписываем все многочлены степени n и вычеркиваем те, которые деляется на ранее невычеркнутые.

Таким образом, для заданной степени n можно выписать все неприводимые многочлены степени не выше, чем n. Если рассматриваемый многочлен остался в списке, то он неприводим, если вычеркнут - приводим.

Этот алгоритм можно запрограммировать.

Задача 1 *Найти все неприводимые многочлены степени не выше* 5 *на полем* $\mathbb{Z}_2$.

Действуем по принципу решета Эратосфена. Под 0 и 1 будем подразумевать вычеты по модулю 2. Если у многочлена над полем есть корень, то он заведомо приводим. А так как в рассматриваемом поле всего два элемента 0 и 1, то удобно проверять подстановкой. Но этого недостаточно для неприводимости над конечным полем, так как возможна делимость на неприводимые многочлены степени выше 1.

$\deg = 1$	Все мночлены превой степени неприводимы.	$x, x+1$.
$\deg = 2$	$x^2, x^2+1, x^2+x, x^2+x+1$. Многочлены x^2 и x^2+x имеют корнем как минимум 0 - вычеркиваем. Многочлен x^2+1 имеет корнем 1. Оставшийся многочлен не имеет корней над данным полем и, значит, неприводим. Таким образом, неприводимых многочленов степени 2 всего один.	x^2+x+1

Понятно, что количество выписываемых далее многочленов сильно увеличивается, поэтому попробуем понять, как должен выглядеть многочлен, у которого нет

корней над полем $\mathbb{Z}_2$. Чтобы ноль не являлся корнем, нужно требовать, чтобы свободное слагаемое равнялось единице. Так как $1+1=0$, то единица не является корнем, если у многочлена нечетное количество слагаемых, включая свободный член. Таким образом, мы ищем многочлены степени n в следующем виде:

$$f = \underbrace{x^n + \ldots + 1}_{\text{нечетное количество слагаемых}}$$

$\deg = 3$	Два слагаемых уже есть: 1 и x^3. Количество слагаемых нечетно только в случае 3 слагаемых: x^3+x^2+1 и x^3+x+1. Если бы эти многочлены делились неприводимый многочлен степени 2, то делился бы и на многочлен степени 1, а это невозможно в силу отсутсвия корней.	x^3+x^2+1, x^3+x+1
$\deg = 4$	Два слагаемых 1 и x^4. Значит, количество слагаемых может быть либо 3, либо 5. Для трех получаем:x^4+x+1, x^4+x^2+1, x^4+x^3+1, а для пяти только один: $x^4+x^3+x^2+x+1$. Если бы многочлены делились на неприводимые степени 3, то делились бы и на неприводимые первой степени, а это невозможно. Если было бы деление на неприводимый второй степени, то было обязательно произведение из двух неприводимых второй степени (так как рассматриваемая степень равна 4), а неприводимый второй степени только один. Значит, единственная возможность заключается в том, что какой-то многочлен совпал с $(x^2+x+1)^2 = x^4+x^2+1$. Таким образом, остаются только три неприводимых.	x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$.

$\deg = 5$. Неприводимый многочлен пятой степени не может делиться ни на многочлен первой степени, ни на многочлен четвертой степени по тем же самым соображениям, что были даны ранее для степеней 3 и 4. Остаются две возможности: либо делится на неприводимый второй степени, либо третьей. Но, если многочлен делится на многочлен второй степени, то делится и на многочлен третьей степени и наоборот. Таким образом, приводимый многочлен может разложиться в проивезедение неприводимого второй степени и третьей степени. Неприводимых второй степени только один, а третьей - два. Остается их перемножить.

$$\left(x^2+x+1\right)\left(x^3+x^2+1\right) = x^5+x+1,$$

$$\left(x^2+x+1\right)\left(x^3+x+1\right) = x^5+x^4+1.$$

Количество слагаемых может быть 3 или 5. Выпишем их:

$$x^5+x^2+1,\ x^5+x^3+1,\ x^5+x^3+x^2+x+1,\ x^5+x^4+x^2+x+1,$$

$$x^5 + x^4 + x^3 + x + 1,\ x^5 + x^4 + x^3 + x^2 + 1.$$

В качестве задания для самостоятельного решения:

Задача *Найти все неприводимые многочлены степени не выше* 3 *на полем* $\mathbb{Z}_3$ *и со старшим коэффициентом* 1.

7.3. Разложение на неприводимые множители в $\mathbb{Q}[x]$

Задача 2 *В* $\mathbb{Q}[x]$ *существуют неприводимые многочлены любой степени.*

Достаточно привести пример многочлена некоторой степени nи доказать его неприводимость. Рассмотрим многочлен $f(x) = x^n - 2$. Докажем от противного. Пусть приводим и тогда раскладывается в произведение неприводимых $f = g \cdot h$, где многочлены g и h имеют степени меньше, чем n, а коэффициенты являются рациональных числами. Как разложить данный многочлен над полем рациональных чисел сразу может быть непонятно. Но зато ясно как разложить над полем комплексных чисел. Все корни являются корнями n степени из 2. Пусть $\sqrt[n]{2}$ - вещественный корень. Чтобы получить все остальные, нужно умножить данный корень на корни n степени из 1. Тогда многочлен разложится следующим образом:

$$f(x) = \left(x - \varepsilon_0 \sqrt[n]{2}\right)\left(x - \varepsilon_1 \sqrt[n]{2}\right) \cdot \ldots \cdot \left(x - \varepsilon_{n-1} \sqrt[n]{2}\right).$$

В то же время $f = gh$, откуда следует, что многочлен g это какие-то k скобок из этого разложения

$$g(x) = \left(x - \varepsilon_{i_1} \sqrt[n]{2}\right)\left(x - \varepsilon_{i_2} \sqrt[n]{2}\right) \cdot \ldots \cdot \left(x - \varepsilon_{i_k} \sqrt[n]{2}\right),$$

а многочлен h оставшиеся $n - k$ скобок. Посмотрим на свободный член многочлена g :

$$(-1)^k \varepsilon_{i_1}\varepsilon_{i_2} \cdot \ldots \cdot \varepsilon_{i_k} \left(\sqrt[n]{2}\right)^k.$$

Так как ε_{i_j} по модулю равны 1, то модуль свободного слагаемого равен $2^{k/n}$ (алгоритм такой же как в случае $\sqrt{2}$). А при условии $0 < k < n$ это число иррациональное. Но модуль рационального числа должен быть рациональным. Таким образом, многочлен g имеет свободное слагаемое не из поля рациональных чисел, противоречие.

Теперь перейдем к вопросу о поиске неприводимых многочленов. Пусть у нас есть многочлен

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n, \quad a_i \in \mathbb{Q}.$$

Если многочлен раскладывается на неприводимые, то умножение на константу, равную произведению всех знаменателей коэффициентов, переведет многочлен с целыми коэффициентами и не изменит самого разложения. Таким образом, без ограничения общности можно считать, что $f \in \mathbb{Z}[x]$.

Выделение линейных множителей равносильно нахождению рациональных корней многочлена. Поэтому мы должны понять как найти у многочлена все рациональные корни. Без ограничения общности можно считать, что рациональные корни мы ищем в виде $x_0 = p/q$, где p и q взаимнопросты (то есть дробь максимально сокращена). Найдем $f(x_0)$:

$$0 = f(x_0) = a_0 + a_1\frac{p}{q} + a_2\frac{p^2}{q^2} + ... + a_n\frac{p^n}{q^n} = \frac{a_0q^n + a_1pq^{n-1} + a_2p^2q^{n-2} + ... + a_np^n}{q^n} \Leftrightarrow$$

$$\Leftrightarrow \overbrace{a_0q^n + \underbrace{a_1pq^{n-1} + a_2p^2q^{n-2} + ...a_{n-1}p^{n-1}q}_{\text{делятся на } q} + a_np^n}^{\text{делятся на } p} = 0$$

Все слагаемые, кроме последнего делятся на q, а значит их сумма делится на q. Если мы поделим это равенство на q, то сумма всех слагаемых кроме последнего даст целое число. А так как полная сумма равна нулю, то последнее слагаемое при делении на q тоже должно давать целое число. В силу того, что p и q взаимнопросты, получаем, что a_n обязан делиться на q.

Теперь, если провести аналогичные рассуждения для всех слагаемых кроме первого, получим, что коэффициент a_0 должен делиться на p.

Мы получили необходимое условие $q|a_n$ и $p|a_0$. Это условие может быть недостаточно, но зато дает конечный список кандидатов, а дальше просто подставить и проверить.

Задача 28.2 а) *Найти все рациональные корни многочлена* $f(x) = x^3 - 6x^2 + 15x - 14$.

С помощью необходимого условия получаем возможные значения для p и q :

$$p = \pm1, \pm2, \pm7, \pm14, \quad q = 1.$$

Проверять все числа необязательно, если заметить, что при любом отрицательном значении x многочлен принимает только отрицальные значения, поэтому отрицательных корней нет. Нетрудно видеть, что $f(1) = -4$ и $f(2) = 0$. Делим многочлен $f(x)$ на $x - 2$ по схеме Горнера и находим его разложение:

$$f(x) = (x-2)\underbrace{\left(x^2 - 4x + 7\right)}_{=:q(x)}$$

Оставшиеся корни следует искать у многочлена $q(x)$. Свободное слагаемое равно 7, поэтому из рассматриваемых кандидатов можно сразу убрать 14. Поэтому остаются только 2 и 7. Находим $q(2) = 3$ и $q(7) = 28$. Таким образом, у многочлена только один рациональных корень 2 кратности 1. Для квадратного трехчлена, конечно, можно было найти дискриминант и убедиться, что действительных корней у $q(x)$ нет.

Задача 28.2 ж) *Найти все рациональные корни многочлена* $f(x) = 4x^4 - 7x^2 - 5x - 1$.

Действуем аналогично предыдущей задаче. Выпишем кандидатов:

$$p = \pm 1, \quad q = 1, 2, 4; \Rightarrow x_0 = \pm 1, \pm\frac{1}{2}, \pm\frac{1}{4}.$$

Вычисляем: $f(1) = -9, \ f(-1) = 1$. Для последующих значений применим схему Горнера:

	4	0	−7	−5	−1
1/2	4	2	−6	−8	−5

	4	0	−7	−5	−1
−1/2	4	−2	−6	−2	0

$$\Rightarrow f(1/2) = -5, \qquad f(-1/2) = 0 \Rightarrow$$

$$\Rightarrow f(x) = \left(x + \frac{1}{2}\right)\left(4x^3 - 2x^2 - 6x - 2\right) = (2x+1)\underbrace{\left(2x^3 - x^2 - 3x - 1\right)}_{=:q(x)}.$$

Теперь корни нужно искать среди корней $q(x)$. Отсюда следует, что мы сразу можем исключить из рассматриваемых кандидатов $\pm 1/4$. Среди оставшихся остается только проверить $-1/2$. Продолжим схему Горнера для $-1/2$ с более простыми коэффициентами:

	2	−1	−3	−1
−1/2	2	−2	−2	0

Таким образом, получаем разложение для $f(x)$:

$$f(x) = (2x+1)^2\underbrace{\left(x^2 - x - 1\right)}_{=:q_1(x)}.$$

У многочлена $q_1(x)$ кандидаты только ± 1, но их мы отвергли ранее. Таким образом, у многочлена $f(x)$ единственный рациональный корень $-1/2$ кратности 2.

7.4. Редукция

Линейные множители мы научились выделять. Но многочлен может раскладываться на неприводимые более высоких степеней. Как искать такие множители или доказывать, что рассматриваемый многочлен неприводим?

Будем считать, что раскладываем многочлен $f \in \mathbb{Z}[x]$ на множители с рациональными коэффициентами. Однако, оказывается, что разложение многочлена $f \in \mathbb{Z}[x]$ в кольце $\mathbb{Q}[x]$ равносильно тому, что f разложим в $\mathbb{Z}[x]$. В одну сторону очевидно: если многочлен раскладывается на многочлены с целыми коэффициентами, то он раскладывается на многочлены с рациональными коэффициентами. В обратну сторону. Предположим, что f раскладывается $f = f_1 f_2, \ f_i \in \mathbb{Q}[x], \deg f_i < \deg f$. У

многочленов f_1 и f_2 рациональные коэффициенты. Мы можем привести к общему знаменателю каждый и вынести его. Тогда останется многочлен с целыми коэффициентами, из которых мы можем вынести их наибольший общий делитель. Таким образом, вынесется рациональная дробь: $f_i = \lambda_i g_i,\ \lambda_i \in \mathbb{Q},\ g_i \in \mathbb{Z}[x]$, причем коэффициенты g_i взаимнопросты (такой многочлен называется примитивным). Получаем разложение:

$$f = \lambda_1 g_1 \cdot \lambda_2 g_2 = \lambda_1 \lambda_2 \cdot g_1 g_2.$$

Мы знаем, что произведение примитивных примитивно. Мы получили, многочлен с целыми коэффициентами f представим в виде произведения рациональной дроби $\lambda_1 \lambda_2 = p/q$ и примитивного многочлена. Если мы раскроем скобки, то коэффициенты должны совпасть. Но слева будет целое число, а справа будет дробь p/q, умноженная на коэффициент примитивного многочлена. Отсюда следует, что q должно делить все коэффициенты примитивного многочлена, но это возможно только в случае $q = 1$, так как у примитивного многочлены все коэффициенты взаимнопросты. Таким образом, дробь p/q целая, а значит, многочлен с целыми коэффициентами представим в виде произведения (если приводим) многочленов с целыми коэффициентами.

Полученный результат упрощает поиск, так как мы можем использовать некоторые соображения о делимости.

Следующий шаг - переход к рассмотрению многочлена в поле вычетов. Такой переход называется *редукцией по простому модулю* p.

Пусть мы рассматриваем многочлен

$$f(x) = a_0 + a_1 x + ... + a_n x^n \in \mathbb{Z}[x].$$

Теперь рассмотрим этот же многочлен, заменив каждый его коэффициент на соответствующий вычет по модулю p :

$$\overline{f}(x) = \overline{a}_0 + \overline{a}_1 x + ... + \overline{a}_n x^n \in \mathbb{Z}_p[x].$$

Многочлен $\overline{f}$ и есть редукция. Этот переход обладает двум важным свойствами:

1. Редукция суммы двух многочленов равна сумме редукций $\overline{f+g} = \overline{f} + \overline{g}$.
2. Редукция произведения двух многочленов равна произведению редукций $\overline{f \cdot g} = \overline{f} \cdot \overline{g}$.
3. $\deg \overline{f} \leqslant \deg f$. Коэффициент $\overline{a}_n$ может обнулиться.

Над полем $\mathbb{Z}_p$ работать удобнее, так как оно конечно.

Теорема 6 (Редукционный признак неприводимости)**.** *Пусть $f \in \mathbb{Z}[x]$, а его редукция $\overline{f}$ неприводима и $\deg \overline{f} = \deg f$. Тогда f неприводим над $\mathbb{Z}$.*

Доказательство: От противного. Пусть $f = f_1 \cdot f_2$, где $f_i \in \mathbb{Z}[x]$ и $\deg f_i < \deg f$. Произведем редукцию: $\overline{f} = \overline{f}_1 \cdot \overline{f}_2$, причем

$$\deg \overline{f}_i \leqslant \deg f_i < \deg f = \deg \overline{f}_i \Rightarrow \deg \overline{f}_i < \deg \overline{f},$$

следовательно, редукция разложима, но это противоречит условию неприводимости редукции. ■

Задача 3 *Рассмотрим многочлен* $f(x) = x^5 + 2x^3 + 3x^2 - 6x - 5$. *Выяснить как он раскладывается на неприводимые множители на полем рациональных чисел.*

Произведем редукцию по модулю $p = 2$:

$$\overline{f} = x^5 + x^2 + 1.$$

Из задачи 1 следует, что $\overline{f}$ неприводим. А так как степени редукции и исходного многочлена равны, то из редукционного признака следует, что многочлен f неприводим.

8. Признак Эйзенштейна, круговой многочлен. Поле рациональных дробей

8.1. Разбор домашнего задания

Задача 28.23 *Пусть имеется поле K из 9 элементов. Найти количество всех неприводимых многочленов со старшим коэффициентом 1 степени 2 и 3 над этим полем.*

$\deg f = 2$. Многочлены второй степени со старшим коэффициентов равным 1 имеют вид $f = x^2 + ax + b$. Для a и b есть 9 возможных значений, значит, многочленов второй степени всего 81. Приводимы те, что раскладываются в произведение двух линейных многочленов со старшим коэффициентом равным 1. И тут есть две возможности: либо $(x+c)^2$, либо $(x+c)(x+d), c \neq d$. Для первой возможности 9 многочленов, а для второй $C_9^2 = 36$. Тогда количество неприводимых равно $81 - 9 - 36 = 36$.

$\deg f = 3$. Многочлены третьей степени со старшим коэффициентов равным 1 имеют вид $f = x^3 + ax^2 + bx + c$. Для a, b и c есть 9 возможных значений, значит, многочленов третьей степени всего 9^3. Рассмотрим возможные разложения на неприводимые приводимых многочленов:

1. $f = f_1 \cdot f_2, \deg f_1 = 1, \deg f_2 = 2$. Для линейного 9 возможестей, а для второй степени (как выяснилось ранее) 36. В итоге $9 \cdot 36$.

2. $f = f_1 \cdot f_2 \cdot f_3, \deg f_i = 1$. Множители должны быть попарно различны, поэтому C_9^3.

3. $f = f_1 \cdot f_2^2, \deg f_1 = 1, \deg f_2 = 1$. Здесь важен порядок, так как один множитель в квадрате, поэтому A_9^2.

4. $f = f_1^3, \deg f_1 = 1$. Тут ровно 9.

Таким образом, получаем количество неприводимых третьей степени:

$$9^3 - 9 \cdot 36 - C_9^3 - A_9^2 - 9 = 729 - 324 - 84 - 72 - 9 = 240.$$

Теорема 7. *Пусть многочлен f раскладывается на неприводимые многочлены какой-то кратности. Тогда многочлен*

$$g := \frac{f}{НОД(f, f')}$$

раскладывается на те же самые неприводимые множители, но кратности 1.

Доказательство: Пусть f раскладывается на неприводимые:

$$f = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s} \;\Rightarrow\; f' = \sum_{i=0}^{s} p_1^{k_1} \cdot \ldots \cdot k_i p_i^{k_i - 1} \cdot \ldots \cdot p_s^{k_s} \;\Rightarrow$$

$$\Rightarrow\; \text{НОД}\,(f, f') = p_1^{k_1 - 1} \cdot \ldots \cdot p_s^{k_s - 1} \;\Rightarrow\; \frac{f}{\text{НОД}\,(f, f')} = p_1 \cdot \ldots \cdot p_s.$$

■

Задача 1 *Рассмотрим многочлен $f(x) = x^5 - 6x^3 + 2x^2 - 4x + 5$. Выяснить как он раскладывается на неприводимые множители на полем рациональных чисел.*

В наличии три метода: поиск корней, редукция и теорема 7. С чего начинать или что проще - вопрос "догадки". Начнем с редукции по модулю 2:

$$\overline{f} = x^5 + 1 = (x+1)\left(x^4 + x^3 + x^2 + x + 1\right).$$

Оба многочлена в скобках неприводимы над $\mathbb{Z}_2$ (обсуждалось на прошлом семинаре). Предположим, что мночлен f раскладывается на неприводимые g и h. Тогда из свойств редукции следует, что $\overline{f} = \overline{g} \cdot \overline{h}$. Но $\overline{f}$ разложим на неприводимые, тогда можно считать (в силу единственности разложения), что

$$\overline{g} = x + 1, \quad \overline{h} = x^4 + x^3 + x^2 + x + 1.$$

Имеем цепочку неравенств для оценки степеней:

$$1 = \deg \overline{g} \leqslant \deg g < \deg f = 5 \Leftrightarrow 1 \leqslant \deg g < 5$$

$$4 = \deg \overline{h} \leqslant \deg h < \deg f = 5 \Leftrightarrow 4 \leqslant \deg h < 5 \Rightarrow \deg h = 4$$

$$\deg g + \deg h = \deg f = 5 \Rightarrow \deg g = 1.$$

Таким образом, если многочлен раскладывается на неприводимые, то их степени обязательно должны быть равны 1 и 4. Отсюда следует, что этого многочлена должен быть корень над $\mathbb{Q}$.

Конечно, можно было выписать всех кандидатов, перебрать и понять имеется ли разложение или нет. Но мы применим другую идею. Произведем редуцирование теперь по модулю 3:

$$\overline{f} = x^5 - x^2 - x - 1.$$

Но так как мы предполагаем, что многочлен f раскладывается на g и h соответствующих степений, то редукция дает условия на степени:

$$\deg \overline{g} \leqslant \deg g = 1, \;\; \deg \overline{h} \leqslant \deg h = 4, \;\; \deg \overline{g} + \deg \overline{h} = \deg \overline{f} = 5 \Rightarrow \deg \overline{g} = 1, \; \deg \overline{h} = 4.$$

Выходит, что над $\mathbb{Z}_3$ у редукции есть корень. Переберем значения редукции в значениях элементов поля:

$$\deg \overline{f}\left(\overline{0}\right) = -1, \quad \deg \overline{f}\left(\overline{1}\right) = 1, \quad \deg \overline{f}\left(\overline{-1}\right) = 1.$$

Оказывается, что корней нет. Противоречие. Таким образом, предположение о разложении ошибочно и многочлен f является неприводимым над $\mathbb{Q}$.

8.2. Признак Эйзенштейна

К сожалению, метод редукции не всегда способен помочь. Так, например, бывают ситуации, когда многочлен неприводим, а любая редукция приводима. В качестве показательного примера задача для самостоятельного решения:

Задача * *Доказать, что многочлен $f(x) = x^4 - 10x^2 + 1$ неприводим над $\mathbb{Q}$, но любая его редукция будет приводимым многочленом.*

Теорема 8 (Признак Эйзенштейна)**.** *Пусть дан многочлен $f(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$ и некоторое просто число $p \in \mathbb{N}$ такое, что $p \nmid a_n, p|a_i, i = 0..n-1$ и $p^2 \nmid a_0$. Тогда многочлен f неприводим над $\mathbb{Q}$.*

Доказательство: От противного. предположим, что многочлен разложим $f = g \cdot h$, $\deg g = k < n$, $\deg h = l < n$. Запишем в коэффициентах:

$$g(x) = b_0 + ... + b_kx^k, \quad h(x) = c_0 + ... + c_lx^l.$$

Проредуцируем f по модулю p :

$$\overline{f} = \overline{g} \cdot \overline{h}.$$

Но все коэффициенты кроме a_n делятся на p, следовательно $\overline{f} = \overline{a}_nx^n$. Произведение многочленов является одночленом, если каждый из сомножителей является одночленом. В данном случае должна получиться степень n, следовательно $\overline{g} = b_kx^k, \overline{h} = c_lx^l$. Возвращаясь к многочленам g и h, получаем, что все коэффициенты кроме старших должны делиться на p : $p|b_0, b_1, ...b_{n-1}, c_0, c_1, ..., c_{n-1}$. Выходит, что свободное слагаемое многочлена f делится на p^2 : $a_0 = b_0c_0 \vdots p^2$, что противоречит условию теоремы. ■

Задача 16.19 б) *Доказать неприводимость многочлена $f(x) = 3x^5 - 2x^4 + 4x^2 + 12x - 18$ над $\mathbb{Q}$.*

Для $p = 2$ выполнены все условия признака Эйзенштейна, следовательно, многочлен f неприводим.

8.3. Круговые многочлены

Определение 7. *Многочленом деления круга на p частей (p-простое) называется многочлен вида*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + ... + x + 1.$$

Такое название следует из другой записи этого многочлена

$$\Phi_p(x) = \frac{x^p - 1}{x - 1}.$$

Корнями этого многочлена являются корни p степени из 1, кроме самой 1. Как известно, эти корни образуют правильный p-угольник вписанный в единичную окружность.

Теорема 9. *Многочлен $\Phi_p(x)$ неприводим над полем рациональных чисел.*

Доказательство: Применить признак Эйзенштейна напрямую нельзя, так как все коэффициенты равны 1. Сделаем замену переменной $x = y + 1$:

$$\Phi_p(y) = \frac{(y+1)^p - 1}{y} = \frac{y^p + C_p^1 y^{p-1} + C_p^2 y^{p-2} + ... + C_p^{p-1} y}{y} =$$

$$= y^{p-1} + C_p^1 y^{p-2} + C_p^2 y^{p-3} + ... + C_p^{p-1}.$$

Коэффициенты C_p^k делятся на p при $k \neq 0$ и $k \neq p$, так как в знаменателе p не появится в силу $0 < k < p$. Старший коэффициент равен 1, поэтому не делится на p. Свободное слагаемое $C_p^{p-1} = p$ не делится на p^2. Выполнены все условия признака Эйзенштейна, поэтому круговой многочлен в переменной y неприводим. Если бы круговой многочлен раскладывался бы на множители, то после рассмотренной замены разложение никуда не делось бы, а степени при такой замене сохранились. Но в нашем случае разложения нет, поэтому нет разложения и в исходном многочлене. ■

8.4. Поле рациональных дробей

Под полем рациональных дробей понимается поле, состоящее из классов эквивалентностей вида $\frac{f}{g}$, где $f, g \in K[x], g \neq 0$. Обозначение $K(x)$.

Дробь $\frac{f}{g}$ можно упростить максимально сократив, то есть можно считать, что НОД$(f, g) = 1$. Далее можно выделить целую часть, то есть делим с остатком и представляем виде:

$$\frac{f}{g} = q + \frac{r}{g}, \quad \deg r < \deg g.$$

Дробь $\frac{r}{g}$ с указанным условием на степени числителя и знаменателя называется правильной. Всякую правильную дробь можно разложить в сумму простейших дробей. Дробь называется простейшей, если знаменатель является степенью неприводимого многочлена, а числитель является многочленом степени меньшей, чем степень неприводимого.

Алгоритм разложения на простейшие:

1. Раскладываем знаменатель на неприводимые: $g = p_1^{k_1} \cdot ... \cdot p_s^{k_s}$. Причем неприводимые непропорциональны.

2. Правильную дробь можно разложить в сумму простейших:

$$\frac{r}{g} = \left(\frac{h_{11}}{p_1} + \frac{h_{12}}{p_1^2} + ... + \frac{h_{1k_1}}{p_1^{k_1}}\right) + \left(\frac{h_{21}}{p_2} + \frac{h_{22}}{p_2^2} + ... + \frac{h_{2k_2}}{p_2^{k_2}}\right) + ...$$

$$... + \left(\frac{h_{s1}}{p_s} + \frac{h_{s2}}{p_s^2} + ... + \frac{h_{sk_s}}{p_s^{k_s}}\right), \qquad \deg h_{ij} < \deg p_i \ \forall i, j.$$

3. Многочлены h_{ij} ищутся методом неопределенных коэффициентов после приведения к общему знаменателю.

Отдельного внимания заслуживают поля действительных и комплексных чисел.

Пусть $K = \mathbb{C}$. Неприводимые многочлены над полем комплексным чисел только линейные. Поэтому простейшие дроби имеют вид:

$$\frac{a}{(x - z_0)^k}, \ a, z_0 \in \mathbb{C}.$$

Таким образом, рациональную дробь над полем комплексным чисел можно представить в виде суммы многочлена и простейших дробей указанного вида.

Задача 29.1 ж) *Разложить дробь*

$$\frac{x^2}{x^4 - 1}$$

в сумму многочлена и простейших над полем комплексных чисел.

Целую часть выделять не нужно, так как степень числителя меньше степени знаменателя, поэтому дробь уже правильная.

Разложим знаменатель на неприводимые:

$$x^4 - 1 = \left(x^2 - 1\right)\left(x^2 + 1\right) = (x - 1)(x + 1)(x - i)(x + i).$$

Запишем искомое разложение с неопределенными коэффициентами:

$$\frac{x^2}{x^4 - 1} = \frac{A}{x - 1} + \frac{B}{x + 1} + \frac{C}{x - i} + \frac{D}{x + i}.$$

Приведем к общему знаменателю справа и приравняем числители:

$$x^2 \equiv A\,(x+1)\left(x^2+1\right) + B\,(x-1)\left(x^2+1\right) + C\,(x+i)\left(x^2-1\right) + D\,(x-i)\left(x^2-1\right).$$

Конечно, можно честно раскрыть скобки, привести подобные и написать уравнения. А можно сделать это сразу, подставив вместо x некоторые значения. В данном случае, удобно брать в качестве значений корни знаменателя, так как при каждом значении в сумме останется только одно слагаемое, а значит и одна буква.

$$\begin{cases} x=1: & 1=4A \\ x=-1: & 1=-4B \\ x=i: & -1=-4iC \\ x=-i: & -1=4iD \end{cases} \Leftrightarrow \begin{cases} A=\frac{1}{4} \\ B=-\frac{1}{4} \\ C=-\frac{i}{4} \\ D=\frac{i}{4} \end{cases}$$

Таким образом, разложение имеет вид:

$$\frac{x^2}{x^4-1} = \frac{\frac{1}{4}}{x-1} + \frac{-\frac{1}{4}}{x+1} + \frac{-\frac{i}{4}}{x-i} + \frac{\frac{i}{4}}{x+i}.$$

Пусть $K=\mathbb{R}$. Неприводимые многочлены над полем действительных есть двух видов: первой степени и второй степени с отрицательным дискриминантом.

$$\frac{a}{(x-x_0)^k},\ a,x_0\in\mathbb{R}, \qquad \frac{bx+c}{(x^2+px+q)^l},\ b,c,p,q\in\mathbb{R},\ p^2-4q<0.$$

Задача 29.2 в) *Разложить дробь*

$$\frac{x}{(x+1)\,(x^2+1)^2}$$

в сумму многочлена и простейших над полем действительных чисел.

Выделять целую не нужно, так как дробь правильная. Знаменатель уже разложен на неприводимые. Ищем разложение в виде:

$$\frac{x}{(x+1)\,(x^2+1)^2} = \frac{A}{x+1} + \frac{Bx+C}{x^2+1} + \frac{Dx+E}{(x^2+1)^2}.$$

Приводим к общему знаменателю справа и приравниваем числители:

$$x \equiv A\left(x^2+1\right)^2 + (Bx+C)\,(x+1)\left(x^2+1\right) + (Dx+E)\,(x+1)$$

Конечно, можно честно раскрыть скобки справа, привести подобные и написать уравнения, но хочется это сделать быстрее. В предыдущем номере мы подставляли корни знаменателя. Здесь действительных корней только один: -1. Заметим, что раз многочлены совпадают тождественно, то чтобы мы не подставили вместо x, равенство сохранится, в том числе комплексные числа. Поэтому подставим дополнительно i.

$$\begin{cases} x=-1: & -1=4A \\ x=i: & i=(Di+E)(i+1) \end{cases} \Leftrightarrow \begin{cases} A=-\frac{1}{4} \\ -D+E+i(D+E-1)=0 \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} A=-\frac{1}{4} \\ -D+E=0 \\ D+E-1=0 \end{cases} \Leftrightarrow \begin{cases} A=-\frac{1}{4} \\ D=E=\frac{1}{2} \end{cases}$$

Подстановка $x=-i$ даст такой же результат. Коэффициент при старшей степени x^4 справа равен $A+B$, а слева 0, следовательно, $B=-A=1/4$.

Теперь посмотрим на свободные слагаемые:$0=A+C+E$, следовательно $C=-1/4$. Выписываем итоговое разложение:

$$\frac{x}{(x+1)(x^2+1)^2}=\frac{-\frac{1}{4}}{x+1}+\frac{\frac{1}{4}x-\frac{1}{4}}{x^2+1}+\frac{\frac{1}{2}x+\frac{1}{2}}{(x^2+1)^2}.$$

9. Симметрические многочлены. Теорема Виета

9.1. Разбор домашнего задания

Задача 29.3 *Разложить дробь*

$$\frac{1}{x^p - x}$$

в сумму многочлена и простейших над полем вычетов по модулю p.

Раскладываем знаменатель на неприводимые. У многочлена $x^p - x$ корнями являются все элементы поля в силу малой теоремы Ферма. Таким образом

$$x^p - x = x\,(x-1)\,(x-2)\cdot\ldots\cdot(x-(p-1))\,.$$

Тогда разложение дроби будем искать в виде:

$$\frac{1}{x^p - x} = \frac{a_0}{x} + \frac{a_1}{x-1} + \ldots + \frac{a_{p-1}}{x-(p-1)}$$

Приводим к общему знаменателю и приравниваем числители:

$$1 \equiv \sum_{k=0}^{p-1} a_k x\,(x-1)\cdot\ldots\cdot\underbrace{(x-k)}_{\text{отсутствует}}\cdot\ldots\cdot(x-(p-1))\,.$$

Подставим как и ранее $x = k$:

$$1 = a_k k\,(k-1)\cdot\ldots\cdot\underbrace{(k-k)}_{\text{отсутствует}}\cdot\ldots\cdot(k-(p-1))\,.$$

Каждый из множителей $k - i$ при i пробегающем все поле кроме k, пробегают все поле кроме 0. То есть для любого k это произведение равно $1\cdot 2\cdot 3\cdot\ldots\cdot(p-1)$. По теореме Вильсона (в этом произведении для каждого элемента содержится ему обратный, поэтому убивают друг друга, кроме, конечно, 1 и -1.) это равно -1. Таким образом, $a_k = -1\ \forall k$.

Задача 28.9 д) *Доказать неприводимость над полем $\mathbb{Q}$ многочлена*

$$f(x) = (x-a_1)\,(x-a_2)\cdot\ldots\cdot(x-a_n) - 1,$$

где a_i различные целые.

Предположим, что он разложим: $f(x) = g(x)h(x), g, h \in \mathbb{Z}[x]$. Подставим в это равенство по очереди значения a_i :

$$g(a_i)h(a_i) = -1,\ \ i = 1..n.$$

Но многочлены g и h с целыми коэффициентами, поэтому и значения обязаны быть целыми. Отсюда следует две возможности:

$$g(a_i) = \pm 1, \qquad h(a_i) = \mp 1.$$

Другими словами, в точках n точках выполнено равенство $h = -g$. То есть два многочлена степени меньше n совпадают в n точках. Из интерполяционной теоремы Лагранжа следует, что эти два многочлена совпадают всюду $h \equiv -g$. (Можно было рассматривать сумму $g + h$, у которой степень ниже n, а корней ровно n.) Получаем, что $f = -g^2$. Если у g старший коэффициент c, то у g^2 - c^2. А страший коэффициент у f равен 1. Следовательно $1 = -c^2 \neq 0$. Противоречие.

9.2. Симметрические многочлены

Определение 8. *Многочлен от n переменных называется симметрическим, если при произвольной перестановке переменных многочлен не меняется.*

Любая перестановка может быть разложена на транспозиции, поэтому достаточно перестановки двух переменных.

Определение 9. *Элементарными симметрическими многочленами называются многочлены*

$$\sigma_k(x_1, ..., x_n) = \sum_{1 \leqslant < i_1 < ... < i_k \leqslant n} x_{i_1} \cdot ... \cdot x_{i_k}.$$

Слагаемых в $\sigma_k(x_1, ..., x_n)$ ровно C_n^k. Симметрических многочленов от n переменных ровно n.

$$\sigma_1 = x_1 + x_2 + ... + x_n, \quad ..., \quad \sigma_n = x_1 \cdot x_2 \cdot ... \cdot x_n.$$

Основная теорема о симметрических многочленах:

Теорема 10. *Любой симметрический многочлен можно выразить единственным образом через элементарные симметрические многочлены:*

$$\forall \textit{симм. } f \in K[x_1, ..., x_n] \ \exists!\ F \in K[x_1, ..., x_n] : \ f = F(\sigma_1, ..., \sigma_n).$$

Предъявим общий метод, с помощью которого можно найти F.

1. Разложим f на однородные компоненты

   $$f = f_0 + f_1 + ... + f_d.$$

   В однородную компоненту входят мономы одинаковой степени $\deg f_k = k$. Так как при перестановке переменных степень многочлена не меняется, то в силу симметричности f получаем симметричность однородных компонент f_k. Теперь достаточно для однородных компонент научиться находиться F. Будем считать теперь f однородным степени d.

2. Мы знаем ответ теоремы 10. Попробуем его проанализировать

$$f = F(\sigma_1, ..., \sigma_n) = a \cdot \sigma_1^{l_1} \cdot ... \cdot \sigma_n^{l_n} + b \cdot \sigma_1^{m_1} \cdot ... \cdot \sigma_n^{m_n} + ... + c \cdot \sigma_1^{p_1} \cdot ... \cdot \sigma_n^{p_n}. \quad (12)$$

Выделим отдельно старшие члены. Для этого нужно взять старший член каждого σ_i возвести в соответствующую степень и перемножить. Старший коэффициент будет единицей, так как у элементарных многочленов все коэффициенты равны 1. Пусть для первого слагаемого старший член выглядит как $x_1^{k_1} \cdot ... \cdot x_n^{k_n}$. Так как x_i впервые начинает входить в старшие члены только на i множителе, то только в этот момент начинает суммироваться его степень:

$$k_i = l_i + ... + l_n \ \Leftrightarrow \ l_i = k_i - k_{i+1}, i = 1..n-1, l_n = k_n. \quad (13)$$

Обозначим старшие слагаемые в (12) для второго и третьего слагаемого соответственно $x_1^{i_1} \cdot ... \cdot x_n^{i_n}$ и $x_1^{j_1} \cdot ... \cdot x_n^{j_n}$. Формулы (13) показывают, что разным произведениям σ_i соответствуют разные старшие члены. Поэтому самый старший из них ни с кем не сократится. Выпишем в порядке лексикографического убывания старшие члены:

$$x_1^{k_1} \cdot ... \cdot x_n^{k_n} \succ x_1^{i_1} \cdot ... \cdot x_n^{i_n} \succ ... \succ x_1^{j_1} \cdot ... \cdot x_n^{j_n} \quad (14)$$

Таким образом, старший член $x_1^{k_1} \cdot ... \cdot x_n^{k_n}$ является старшим членом f. Надо не забывать, что мы рассматриваем f однородным, поэтому суммы степеней совпадают:

$$k_1 + ... + k_n = i_1 + ... + i_n = ... = j_1 + ... + j_n = d. \quad (15)$$

А так как задан лексикографический порядок, то выполнено второе условие:

$$k_1 > ... > k_n; \quad i_1 > ... > i_n; \quad ...; \quad j_1 > ... > j_n. \quad (16)$$

Многочлен f нам задан. Поэтому мы можем его переписать (переставив слагаемые) так, чтобы он удовлетворял условию (16). А это уже дает нам кандидатов на старшие члены в формуле (12). Конечно, коэффициенты a, b и c могут обнулиться, но лишнего появиться там точно ничего не может. Кандидаты восстанавливаются с помощью формул (13).

3. Возникает следующая таблица, в которой на первую строку выписывают степени старшего члена, а затем, выписываются степени мономов, удовлетворяющих условиям (15) и (16), то есть одной степени и в лексикографическом порядке.

$$\begin{matrix} k_1 & ... & k_n \\ i_1 & ... & i_n \\ \vdots & \vdots & \vdots \\ j_1 & ... & j_n \end{matrix} \quad (17)$$

4. Напротив каждой строки таблицы (17) выписываем степени σ_i, в многочлене F, восстановленные с помощью формул (13) $l_i = k_i - k_{i+1}, l_n = k_n$.

$$\begin{array}{ccc|ccc} k_1 & \dots & k_n & l_1 & \dots & l_n \\ i_1 & \dots & i_n & m_1 & \dots & m_n \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ j_1 & \dots & j_n & p_1 & \dots & p_n \end{array} \tag{18}$$

   То есть мы получили возможные разложения многочлена F.

5. Коэффициенты многочлена F мы не знаем, поэтому выписываем многочлен F с неопределенными коэффициентами $a, b, ..., c$. Находим эти значения либо с помощью приравнивания коэффициентов при соответствующих степенях слева и справа, либо подставляем некоторые значения. Второй метод здесь более удобный, так как переменных много. Как правило, на практике достаточно подставлять значения $-1, 0$ и 1, но это необязательно. После подстановки мы получаем систему линейных алгебраических уравнений на неизвестные коэффициенты. Конечно, некоторые уравнения могут оказаться зависимыми. Но теорема 10 гарантирует нам существование и единственность, поэтому нужно продолжать подставить какие-то другие значения пока система не станет совместной и определенной.

   На практике это удобно записывать это в виде таблицы. Шапка таблицы имеет следующий вид:

$$\begin{array}{ccc|ccc|c} x_1 & \dots & x_n & \sigma_1 & \dots & \sigma_n & f \\ \hline \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{array} \tag{19}$$

   В первом столбце выписываются значения, которые мы собираемся подставить. Во втором столбце выписываются вычисленные значения симметрических элементарных многочленов в рассматриваемой подстановке. В третьем столбце выписывается значения f слева и значение многочлена F справа, то есть линейной уравнение $f(x_1, ..., x_n) = F(\sigma_1, ..., \sigma_n)$. Далее остается только решить.

   Заметим, что старшие коэффициенты слева и справа совпадают, так как старшему моному попросту не с кем сократиться. Таким образом, в указанных обозначениях коэффициент a можно написать сразу.

9.3. Выражение степенных сумм через элементарные симметрические многочлены

Определение 10. *Степенной суммой s_k называется многочлен вида:*

$$s_k(x_1, ..., x_n) = x_1^k + ... + x_n^k.$$

Степенные суммы являются симметрическими многочленами, поэтому в силу теоремы 10 многочлен F для них существует и единственен. Для малых значений k можно выписать сразу:

$$s_1 = x_1 + ... + x_n = \sigma_1, \quad s_2 = x_1^2 + ... + x_n^2 = \sigma_1^2 - 2\sigma_2.$$

Для s_3 воспользуемся описанным методом.

1. Выделять однородные компоненты не нужно, так как все слагаемые имеют одинаковую степень равную 3.

2. Заполняем таблицу (18). Самый старший моном x_1^3, поэтому первая строка будет 30...0. Далее идут строки со степенями по x_1 обязательно убывающим, но в сумме дающим $d = 3$ и сохраняющим порядок (16).

$$\begin{array}{cccccc|cccccc|ccc} 3 & 0 & 0 & 0 & ... & 0 & 3 & 0 & 0 & 0 & ... & 0 & \mapsto & \sigma_1^3 \\ 2 & 1 & 0 & 0 & ... & 0 & 1 & 1 & 0 & 0 & ... & 0 & \mapsto & \sigma_1\sigma_2 \\ 1 & 1 & 1 & 0 & ... & 0 & 0 & 0 & 1 & 0 & ... & 0 & \mapsto & \sigma_3 \end{array}$$

   Таким образом, разложение будем искать в виде:

$$f = \sigma_1^3 + a\sigma_1\sigma_2 + b\sigma_3, \quad a, b \in \mathbb{R}.$$

3. Заполняем таблицу (19).

x_1	x_2	x_3	x_4	...	x_n	σ_1	σ_2	σ_3	s_3		
1	1	0	0	...	0	2	1	0	$2 = 8 + a \cdot 2$	$\Leftrightarrow$	$a = -3$
1	1	1	0	...	0	3	3	1	$3 = 3^3 - 3 \cdot 3 \cdot 3 + b$	$\Leftrightarrow$	$b = 3$

   Получаем ответ:

$$f = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$

Найдем выражение через элементарные симметрические многочлены для s_4.

1. Выделять однородные компоненты не нужно, так как все слагаемые имеют одинаковую степень равную 4.

2. Заполняем таблицу (18). Самый старший моном x_1^4, поэтому первая строка будет $40...0$. Далее идут строки со степенями по x_1 обязательно убывающим, но в сумме дающим $d = 4$ и сохраняющим порядок (16).

$$\begin{array}{ccccccc|ccccccc} 4 & 0 & 0 & 0 & 0 & ... & 0 & 4 & 0 & 0 & 0 & 0 & ... & 0 \\ 3 & 1 & 0 & 0 & 0 & ... & 0 & 2 & 1 & 0 & 0 & 0 & ... & 0 \\ 2 & 2 & 0 & 0 & 0 & ... & 0 & 0 & 2 & 0 & 0 & 0 & ... & 0 \\ 2 & 1 & 1 & 0 & 0 & ... & 0 & 1 & 0 & 1 & 0 & 0 & ... & 0 \\ 1 & 1 & 1 & 1 & 0 & ... & 0 & 0 & 0 & 0 & 1 & 0 & ... & 0 \end{array} \quad \begin{array}{c} \mapsto \\ \mapsto \\ \mapsto \\ \mapsto \\ \mapsto \end{array} \quad \begin{array}{c} \sigma_1^4 \\ \sigma_1^2\sigma_2 \\ \sigma_2^2 \\ \sigma_1\sigma_3 \\ \sigma_4 \end{array}$$

Таким образом, разложение будем искать в виде:

$$f = \sigma_1^4 + a\sigma_1^2\sigma_2 + b\sigma_2^2 + c\sigma_1\sigma_3 + d\sigma_4, \quad a, b, c, d \in \mathbb{R}.$$

3. Заполняем таблицу (19).

x_1	x_2	x_3	x_4	x_5	...	x_n	σ_1	σ_2	σ_3	σ_4	s_3		
1	-1	0	0	0	...	0	0	-1	0	0	$2 = b$	$\Leftrightarrow$	$b = 2$
1	1	0	0	0	...	0	2	1	0	0	$2 = 16 + 4a + b$	$\Leftrightarrow$	$a = -4$
1	1	-1	0	0	...	0	1	-1	-1	0	$3 = 1 - a + b - c$	$\Leftrightarrow$	$c = 4$
1	1	-1	-1	0	...	0	0	-2	-1	1	$4 = 4b + d$	$\Leftrightarrow$	$d = -4$

Получаем ответ:

$$f = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 + 4\sigma_1\sigma_3 - 4\sigma_4.$$

9.4. Теорема Виета

Теорема 11 (Теорема Виета)**.** *Пусть дан многочлен* $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$. *Предположим, что у него ровно* n *корней* $\alpha_1, ..., \alpha_n$ *без учета кратности. Тогда выполнены соотношения*

$$\sigma(\alpha_1, ..., \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}.$$

Формулы Виета полезны тем, что с их помощью и помощью основной теоремы о симметрических многочленах (теорема 10) можно выразить любой симметрический многочлен от корней многочлена f через его коэффициенты, даже не зная самих корней (с помощью основной теоремы о симметрических многочленах выражаем данный многочлен через элементарные симметрические многочлены, а последние выражаются через коэффициенты многочлена по формулам Виета).

Задача 31.21 а) *Решить систему уравнений*

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1^2 + x_2^2 + x_3^2 = 0 \\ x_1^3 + x_2^3 + x_3^3 = 24 \end{cases}$$

над полем комплексных чисел.

В каждом уравнении слева написан симметрический многочлен (степенные суммы), то есть система симметрических уравнений. Теперь по теореме 10 их можно выразить через элементарные симметрические многочлены (для этого вспомним предыдущие результаты):

$$\begin{cases} \sigma_1 = 0 \\ \sigma_1^2 - 2\sigma_2 = 0 \\ \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = 24 \end{cases} \Leftrightarrow \begin{cases} \sigma_1 = 0 \\ \sigma_2 = 0 \\ \sigma_3 = 8 \end{cases}$$

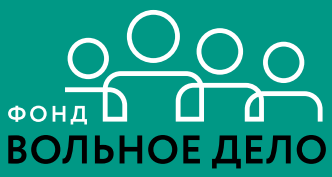
Теперь мы можем составить многочлен, корни которого будут совпадать с x_1, x_2 и x_3 с помощью теоремы Виета: коэффициенты с точностью до знака определяются элементарными симметрическими многочленами. Будем считать, что старший коэффициент равен 1. Составляем многочлен:

$$x^3 - \sigma_1 x^2 + \sigma_2 x - \sigma_3 = 0 \Leftrightarrow x^3 - 8 = 0 \Leftrightarrow x = \sqrt[3]{8} = \left\{ 2, 2\left(\frac{1}{2} \pm i\frac{\sqrt{3}}{2}\right) \right\}.$$

Но решение исходной системы есть упорядоченный набор из трех чисел, а так как система симметрическая, то всего решений 6:

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

МЕХАНИКО-
МАТЕМАТИЧЕСКИЙ
ФАКУЛЬТЕТ
МГУ ИМЕНИ
М.В. ЛОМОНОСОВА



teach-in
ЛЕКЦИИ УЧЕНЫХ МГУ