МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__11__» ____04_____ 2023 г.

Теория делимости и непрерывные дроби

Методические рекомендации

для выполнения практических заданий по дисциплинам

«Элементы алгебры и теории чисел» и «Алгебра и теория чисел»

Направления подготовки: 10.03.01 «Информационная безопасность»;
02.03.03 «Математическое обеспечение и администрирование информационных систем».

Курск – 2023

УДК 511+512(075.8)
Составители:
д. ф-м. н., профессор В.П. Добрица
к.т.н. Е.А. Кулешова
к.т.н., доцент Ю.А. Халин

Рецензент

Кандидат технических наук, доцент кафедры вычислительной техники А.В. Киселев

Теория делимости и непрерывные дроби: методические рекомендации для выполнения практических заданий / Юго-Зап. гос. ун-т; сост.: В.П. Добрица, Е.А. Кулешова, Ю.А. Халин. – Курск, 2023. – 33 с. – Библиогр.: с. 33.

В методических указания описываются основы алгебры и теории чисел. Изложены краткие теоретические сведения, приведены примеры решения задач, а также задачи для самостоятельного решения.

Методические рекомендации предназначены для студентов, обучающихся по направлениям подготовки 10.03.01 «Информационная безопасность» и 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. 233
Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Введение

В данных методических рекомендациях изложены материалы по разделу «Делимость чисел, ее свойства и приложения» курсов «Элементы алгебры и теории чисел» и «Алгебра и теория чисел».

Рассмотрены следующие темы: теорема деления с остатком, свойства делимости чисел, простые и составные числа, НОД и НОК, целая и дробная часть числа, функция Эйлера, число и сумма делителей натурального числа, цепные дроби.

По каждой теме представлены:

1) краткие теоретические положения;
2) перечень вопросов, выносимых на практическое задание;
3) примеры решения типов задач, выносимых на практическое занятие;
4) задачи, выносимые на самостоятельную работу студентов.

Данные методические рекомендации предназначены для проведения практических занятий по дисциплинам «Алгебра и теория чисел» и «Элементы алгебры и теории чисел» для студентов Юго-Западного государственного университета направлений подготовки: «Информационная безопасность», «Математическое обеспечение и администрирование информационных систем».

По изложенным в данных методических рекомендациях материалам можно рекомендовать преподавателю проведение 8-ми часов практических занятий по следующему плану:

- Простые и составные числа. Каноническое представление целого числа. (2 часа)

- Целая и дробная часть числа. Функция Эйлера. Число и сумма делителей натурального числа. (2 часа)
- НОД и его линейное представление, НОК. (2 часа)
- Непрерывные и подходящие дроби. (2 часа)

При выполнении практических заданий в каждой задаче выберете задание из своего варианта. Вариант определяется по последней цифре номера зачетной книжки. Отчет по работе должен содержать решения задач и выводы с полным их обоснованием. Отчет по работе оформить на листах формата А 4. На титульном листе должно быть указано: университет, факультет, кафедра, предмет, номер практического занятия, вариант, группа, исполнитель, проверяющий.

РАБОТА № 1 Простые и составные числа, каноническое представление составного числа

Цель: изучить понятия простого и составного числа, теорему о бесконечности множества простых чисел, теорему деления с остатком, научиться проверять простоту числа и находить каноническое представление составного числа.

Вопросы, выносимые на практическое занятие.

1. Теорема делимости с остатком. Делимость и ее свойства.
2. Простое и составное натуральные числа.
3. Решето Эратосфена, бесконечность множества простых чисел.
4. Разложение целого числа на простые множители, каноническое представление составного числа.

Краткие теоретические сведения.

Теория чисел занимается изучением свойств целых чисел. Целыми мы будем называть не только числа натурального ряда 1, 2, 3, .. . (положительные целые), но также нуль и отрицательные целые —1 , —2, —3 , .. . Так что, расположив целые числа в возрастающем порядке, получим ряд, в котором разность между большим и меньшим соседними членами всегда будет равна единице.

На множестве целых чисел будем рассматривать операции суммы $a+b$, разности $a-b$ и произведение ab двух целых a и b, которые также являются целыми.

В случае, когда для целых a и b существует целое q, что имеем равенство $a=bq$, то будем говорить, что a делится на b ($a:b$), или что b делит a ($b|a$). В это случае еще говорят, что a кратно b или b делитель a.

ТЕОРЕМА. а) Если a кратно c, c кратно b, то а кратно b.

b) Если $(a \pm c) \vdots b$ и $a \vdots b$, то и $c \vdots b$. Причем, верно и обратное: если $a \vdots b$ и $c \vdots b$, то $(a \pm c) \vdots b$.

c) Если $a \vdots b$, то $a^n \vdots b^n$.

ТЕОРЕМА. Всякое целое a представляется единственным способом с при положительном целом b равенством вида $a = bq + r$ и $0 \leq r < b$.

В этом случае q называется неполным частным, а r остатком от деления a на b.

Если положительное число p делится только на положительные числа 1 и p, то оно называется простым. В противном случае, т.е. когда есть и другие положительные делители, это число называется составным. 1 совершенно особое число, у него единственный делитель.

Если в ряду натуральных чисел исключить 1, то первое число 2 будет простым. Вычеркивая в дальнейшем числа, кратные 2, мы получим первое не вычеркнутое число 3. Оно будет простым. Вычеркивая далее числа кратные 3, мы получим первое не вычеркнутое число 5. Оно тоже является простым. Этот процесс можно продолжать и мы получим последовательность простых чисел. Сам процесс напоминает «просеивание», и получил название «решето Эратосфена».

ТЕОРЕМА. Если натуральное число q не делится на простые числа p такие, что $p^2 \leq q$, то это число q простое.

ТЕОРЕМА. Множество простых чисел бесконечно.

ТЕОРЕМА. Для любого натурального числа n существует промежуток подряд идущих натуральных чисел длинны n, не содержащий простых чисел.

ТЕОРЕМА. Пусть натуральное число больше 1. Тогда наименьший положительный делитель числа, отличный от 1, является простым числом.

ТЕОРЕМА. Каждое натуральное число a представляется единственным образов в виде произведения степеней простых чисел $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.

Это представление натурального числа называется каноническим.

Для целого числа имеет место такое же представление, просто перед ним ставится знак - .

ТЕОРЕМА. Число $b = p_1^{\beta_1} \dots p_k^{\beta_k}$ является делителем числа $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ тогда и только тогда, когда для каждого i имеет место неравенство $\beta_i \leq \alpha_i$.

Примеры выполнения заданий.

Задача 1. Найти все простые числа от 10 до 20.

Выпишем эти числа и применим «решето Эратосфена».

10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20.

Вычеркнем сначала числа, кратные 2. Останутся следующие числа.

11, 13, 15, 17, 19.

Теперь вычеркнем числа, кратные 3. Получим последовательность чисел

11, 13, 17, 19.

Уже проверять делимость на 5 нет необходимости, т.к. 5^2>20.

Задача 2. **Разложить на простые множители 6!.**

Вынесем сначала 2 из тех множителей, которые краны 2, затем вынесем еще раз 2 из оставшихся множителей, кратных 2. Из оставшихся после этого множителей вынесем 3 . Получим следующее представление.

$6!=1\cdot2\cdot3\cdot4\cdot5\cdot6=2\cdot2\cdot2\cdot(3\cdot2\cdot5\cdot3)=2^4\cdot3^2\cdot5$.

Задача 3. **Выясните, является ли данное число простым или составным.**

$a = 29$. Проверяем делимость этого числа на простые числа, квадрат которых не превосходит a. Это простые числа 2, 3, 5. Ни на одно из них 29 не делится, значит, оно является простым.

Задача 4. **Найти высшую степень числа 2 в разложении числа 8!.**

Будем действовать так же как в задаче 2 относительно только простого числа 2.

$8!=1\cdot2\cdot3\cdot4\cdot5\cdot6\cdot7\cdot8=2\cdot2\cdot2\cdot2\cdot(3\cdot2\cdot5\cdot3\cdot7\cdot4)=2^4\cdot2\cdot2\cdot(3\cdot5\cdot7\cdot2)=2^4\cdot2^2\cdot2\cdot(3\cdot5\cdot7)=$

$=2^7\cdot(3\cdot5\cdot7)$. Таким образом, степень 2 в разложении числа 8! равна 7.

Задача 5. **Представить в канонической форме число 2015.**

$2025=5\cdot405=5\cdot5\cdot81=5^2\cdot3\cdot27=5^2\cdot3\cdot3\cdot9=5^2\cdot3\cdot\ 3\ \cdot\ 3=3^4\cdot5^2$.

Задача 6. **Разделить число *a* на положительное число *b* с остатком**.

a= 20974, b = 37.

Можно число а делить на число б «уголком».

```
20974 | 37
205   | 512
 47
 37
 104
 74
 30
```

Таким образом, получаем $20974=37\cdot512+30$, причем $0 \leq 30 < 37$.

Практические задания по вариантам.

Задание 1. Найти все простые числа между числами *a, b:*

Вариант 1. *a* =150; *b* =180; **Вариант 2. *a* =250; *b* =280;**

Вариант 3. *a* =130; *b* =160; **Вариант 4. *a* =230; *b* =260;**

Вариант 5. *a* =110; *b* =140; **Вариант 6. *a* =200; *b* =240;**

Вариант 7. *a* =90; *b* =120; **Вариант 8. *a* =250; *b* =290;**

Вариант 9. *a* =40; *b* =90; **Вариант 10. *a* =230; *b* =270.**

Задание 2. Разложить на простые множители:

Вариант 1. n =10!; **Вариант 2. n=14!;**

Вариант 3. n =11!; **Вариант 4. n = 8!;**

Вариант 5. n =14!; **Вариант 6. n=16!;**

Вариант 7. n =13!; **Вариант 8. n = 11!;**

Вариант 9. n=18!; **Вариант 10. n=19!.**

Задание 3. Выясните, являются ли числа простыми или составными:

Вариант 1. 2657; **Вариант 2. 101;**

Вариант 3. 401; **Вариант 4. 103;**

Вариант 5. 2667; **Вариант 6. 1001;**

Вариант 7. 104; **Вариант 8. 1003;**

Вариант 9. 2669; **Вариант 10. 203.**

Задание 4. Найти высшие степени чисел 2, 3, 5, 7, 11, 13, на которые делится число n!:

Вариант 1. n =40!; **Вариант 2. n=34!;**

Вариант 3. n =31!; **Вариант 4. n = 18!;**

Вариант 5. n =34!; **Вариант 6. n=26!;**

Вариант 7. n =23!; **Вариант 8. n = 21!;**

Вариант 9. n=28!; **Вариант 10. n=39!.**

Задание 5. Представить в канонической форме число:

Вариант 1. *a* =8279884; **Вариант 2. *a* = 8105722;**

Вариант 3. *a* =1488972; **Вариант 4. *a* = 6223781;**

Вариант 5. *a* =1101433; **Вариант 6. *a* =2024013;**

Вариант 7. *a* =9090117; **Вариант 8. *a* =2501313;**

Вариант 9. *a* =4091334; **Вариант 10. *a* =2301027.**

Задание 6. Разделить число *a* на положительное число *b* с статком.

Вариант 1. *a* =2024013, *b* =90; **Вариант 2 *a* =1488972, *b* =270;**

Вариант 3. *a* =2301027, *b* =120; **Вариант 4. *a* =1101433, *b* =290;**

Вариант 5. *a* =2501313, *b* =140; **Вариант 6. *a* =9090117, *b* =240;**

Вариант 7. *a* =8279884, *b* =160; **Вариант 8. *a* =4091334, *b* =260;**

Вариант 9. *a* = 6223781, *b* =180; **Вариант 10. *a* = 8105722, *b* =280.**

РАБОТА № 2 Целая и дробная части числа. Функция Эйлера. Число и сумма делителей натурального числа.

Цель: изучить понятия целой и дробной части действительного числа, мультипликативной функции, функцию Эйлера для натурального аргумента, функции числа и суммы делителей натурального числа.

Вопросы, выносимые на практическое занятие.

1. Целая и дробная часть действительного числа. Их свойства.
2. Мультипликативные функции и их свойства.
3. Число натуральных делителей целого числа.
4. Сумма натуральных делителей целого числа.
5. Функция Эйлера и ее свойства.

Краткие теоретические сведения.

Наибольшее целое число, не превосходящее данного действительного числа a называется его целой частью, которая обозначается как $[a]$.

ТЕОРЕМА. a) $[a] \leq a$.

b) [a+n]=n+[a], где n целое число.

Разность между числом и его целой частью называется его дробной частью. $a - [a] = \{a\}$.

ТЕОРЕМА. a) $0 \leq \{a\} < 1$;

b) a=[a]+{a}.

ТЕОРЕМА. Показатель, с которым данное простое p входит в произведение n!, равен $\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$.

Функция на натуральном аргументе называется мультипликативной, если она удовлетворяет следующим условиям:

1) f(1)=1;

2) *f(ab)=f(a)f(b).*

ТЕОРЕМА. Пусть натуральное число имеет каноническое представление $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Тогда сумма значений мультипликативной функции *f* от всех делителей этого числа *a* вычисляется по формуле:

$\sum_{d/a} f(d) = \left(1 + f(p_1) + f(p_1^2) + \cdots + f\left(p_1^{\alpha_1}\right)\right) \cdot \dots \cdot (1 + f(p_k) + f(p_k^2) + \cdots + f\left(p_k^{\alpha_k}\right))$, причем, в случае a = 1, правая часть считается равной 1.

Обозначим через $\tau(a)$ число положительных делителей числа a.

ТЕОРЕМА. Если $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то

$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_k + 1).$

Заметим, что для $a = p^{\alpha}$ имеем $\tau(a) = (\alpha + 1)$.

Обозначим через $\sigma(a)$ сумму положительных делителей числа a.

ТЕОРЕМА. Если $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то

$$\sigma(a) = \frac{p_1^{\alpha_1+1}-1}{p_1-1} \cdot \dots \cdot \frac{p_k^{\alpha_{k+1}}-1}{p_k-1}, \text{ или}$$

$$\sigma(a) = \left(1 + p_1 + \cdots + p_1^{\alpha_1}\right) \cdot \dots \cdot (1 + p_k + \cdots + p_k^{\alpha_k}).$$

Функция Эйлера $\varphi(a)$ определяется для всех целых положительных a и представляет собою число представителей ряда 0, 1 … (*a-1*) взаимно простых с a.

ТЕОРЕМА. $\varphi(a) \leq a - 1$.

Заметим, что $\varphi(a) = a - 1$ тогда и только тогда, когда a является простым числом.

ТЕОРЕМА. Если $a = p^{\alpha}$, то $\varphi(\alpha) = p^{\alpha} - p^{\alpha-1}$.

ТЕОРЕМА. Если $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то

$$\varphi(a) = a \cdot (\prod_i (1 - \frac{1}{p_i})) .$$

ТЕОРЕМА. Если $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то

$\varphi(a) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})$.

ТЕОРЕМА. Если $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, то

$\sum_{d|a} \varphi(d) = \varphi(a)$.

Примеры выполнения заданий.

Задание 1. Найти целую и дробную части от $3+\sqrt{12}$.

Заметим, что $3^2 < 12 < 4^2$, значит $3 < \sqrt{12} < 4$. А потому $[3+\sqrt{12}]= 3+[\sqrt{12}]= 3+3=6$. На основании определения дробной части имеем $\{3+\sqrt{12}\}=3+\sqrt{12} - [3+\sqrt{12}]=3+\sqrt{12} -6= \sqrt{12} - 3$.

Задание 2. Вычислить функцию Эйлера $\varphi(a)$ для числа 725.

Найдем каноническое представление числа 725.

$$725 = 5^2 \cdot 29.$$

Тогда $\varphi(725) = 725 \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{29}\right) = 5 \cdot 4 \cdot 28 = 560$.

Задание 3. Вычислить число делителей τ(а) для числа, указанного в задании 2.

$$\tau(725) = (2+1)(1+1) = 6.$$

Задание 4. Вычислить сумму делителей σ(а), для числа, указанного в задании 2.

$$\sigma(725) = \frac{5^{2+1}-1}{5-1} \cdot \frac{29^{1+1}-1}{29-1} = \frac{125-1}{4} \cdot \frac{841-1}{28} = 31 \cdot 30 = 930.$$

Задание 5. Найти показатель, с которым число a входит в $n!$:

$$\boldsymbol{a = 3, n = 7}.$$

Показатель числа 3 в разложении числа 7! равен $[\frac{7}{3}]+[\frac{7}{9}]=2+0=2$.

Задание 6. По известной функции Эйлера $\varphi(a)$ найти число $\boldsymbol{a = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma} \cdot 7^{\delta}}$. $\boldsymbol{\varphi(a) = 64}$

Ясно, что $\alpha \geq 0,\ \beta \geq 0, \gamma \geq 0, \delta \geq 0$.

1) Сначала предположим, что все они строго больше 0. Тогда в соответствии с формулой $\varphi(a) = a \cdot \sum_{p_i}\left(1 - \frac{1}{p_i}\right)$ получим равенство:

   $64 = a \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) = a \cdot \frac{8}{35}$.

   После сокращения получим $35 \cdot 8 = a$, т.е. $a = 280$. Но это число не делится на 3, значит наше предположение, что $\beta > 0$, не верно.

2) Будем предполагать теперь, что один из показателей равен 0. Рассмотрим первый из них $\alpha = 0$, а остальные больше 0.

   Тогда будем иметь равенство: $64 = a \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) = \frac{64}{35}$

   Отсюда $a = 35$. Но 35 не делится на 3, т.е. предположение, что $\beta > 0$ не верно.

3) Предположим, что $\beta = 0$, а остальные показатели положительные. В этом случае имеем $64 = a \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{7}\right) = \frac{12}{35}$.

Отсюда $3a = 35 \cdot 16$. Левая часть делится на 3, а правая нет. Полученное противоречие доказывает, что этого случая тоже быть не может.

4) Предположим, что $\gamma = 0$, а остальные показатели положительные. В этом случае имеем $64 = a \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{7}\right) = \frac{4}{7}a$, т.е.

$$a = 7 \cdot 32 = 2^5 \cdot 7^1$$

Но в этом разложении нет 3, что противоречит предположению.

5) Наконец, предположим, что $\delta = 0$, а остальные показатели положительные. В этом случае имеем:

$64 = a \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = \frac{4}{15}a$,т.е. $a = 240 = 2^4 \cdot 3^1 \cdot 5^1$.

Сделаем проверку.

$$240 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 240 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 64$$

Ответ: $a = 240$.

Практические задания по вариантам.

Задание 1. Найти целую и дробную части от:

Вариант 1. а) 3,75; б) $-\frac{15}{7}$; **в)** $5 + \sqrt{17}$; **г) 3+sin** $\frac{\pi}{4}$; **д)** $1,5 - \tan\frac{\pi}{4}$;

Вариант 2. а) $-3,75$; **б)** $\frac{15}{7}$; **в)** $-5 + \sqrt{17}$; **г) 3-sin** $\frac{\pi}{4}$; **д)**$-1,5 - \tan\frac{\pi}{4}$;

Вариант 3. а) 6,7; б) $2 - \frac{15}{7}$; **в)** $1,3 + \cos\frac{\pi}{6}$; **г)** $2 + \cos\frac{\pi}{3}$; **д)** $1 + \sin\frac{\pi}{6}$;

Вариант 4. а) $-6,7$; **б)**$-2 - \frac{15}{7}$; **в)** $1,3 - \cos\frac{\pi}{6}$; **г)** $\sqrt[4]{200}$; **д)** $1 - \sin\frac{\pi}{6}$;

Вариант 5. а) $\frac{1+\sqrt{2}}{3}$; **б)** $3 - \lg 0,7$; **в)** $\frac{67}{5}$; **г)** $\sqrt[3]{20}$; **д)**$-1 - \sin\frac{\pi}{6}$;

Вариант 6. а) e**=2,718..;** **б)** $\frac{1+\sqrt{52}}{2}$; **в)** $\sqrt{110}$; **г)** $-4,15$; **д)**$1,25 + \sqrt{17}$;

Вариант 7. а) -e**=-2,718..;** **б)** $\frac{1-\sqrt{52}}{2}$; **в)** $-\sqrt{110}$; **г)** $4,15$; **д)**$1,25 - \sqrt{17}$;

Вариант 8. а) -16,7; б)$\frac{1-\sqrt[4]{20}}{4}$; **в)** $1,3 + \sin\frac{\pi}{6}$; **г)** $-(\sqrt[4]{580} + 1)$; **д)**$-\frac{57}{8}$;

Вариант 9. а) -7,75; б) $3-\frac{15}{7}$**; в)** $-5+\sqrt{17}$**; г) -3-**$\sin\frac{\pi}{4}$**; д)** $1,5+\tan\frac{\pi}{4}$**;**

Вариант 10. а) $1-\sqrt{21}$**; б)** $\sqrt[4]{117}$**; в)** $\ln 12$ **; г)** $4+\cos\frac{101\pi}{204}$**; д)**$-\frac{\pi}{2}$**;**

Задание 2. Вычислить функцию Эйлера $\varphi(a)$ **для чисел:**

Вариант 1. (а=820);
Вариант 2. (а = 460);
Вариант 3. (а = 825);
Вариант 4. (а=396);
Вариант 5. (а =2310);
Вариант 6. (а=2520);
Вариант 7. (а = 720);
Вариант 8. (а = 3630);
Вариант 9. (а = 375);
Вариант 10. (а = 390);
Вариант 15. (а = 320).
Вариант 16. (а = 5610).

Задание 3. Вычислить число делителей τ**(а) для чисел, указанных в задании 2.**

Задание 4. Вычислить сумму делителей σ**(а), для чисел, указанных в задании 2.**

Задание 5. Найти показатель, с которым число ***а*** **входит в** ***n!*****:**

Вариант 1. а=2, n =110!;
Вариант 2. а=3, n=140!;
Вариант 3. а=5, n =101!;
Вариант 4. а=7, n = 80!;
Вариант 5. а = 11, n =314!;
Вариант 6. а=2, n=160!;
Вариант 7. а=3, n =130!;
Вариант 8. а=5, n = 11!;
Вариант 9. а=7, n=180!;
Вариант 10. а=11, n=190!.

Задание 6. По значению известной функции Эйлера $\varphi(a)$ **найти число** $a=2^{\alpha}\cdot 3^{\beta}\cdot 5^{\gamma}\cdot 7^{\delta}$**.**

Вариант 1. $\varphi(a)$**=48;**
Вариант 2. $\varphi(a)$**=320;**
Вариант 3. $\varphi(a)$**=1152;**
Вариант 4. $\varphi(a)$**=128;**
Вариант 5. $\varphi(a)$**=560;**
Вариант 6. $\varphi(a)$**=144;**
Вариант 7. $\varphi(a)$**=768;**
Вариант 8. $\varphi(a)$**=432;**
Вариант 9. $\varphi(a)$**=240;**
Вариант 10. $\varphi(a)$**=320.**

РАБОТА №3. Наибольший общий делитель и его линейное представление. Наименьшее общее кратное.

Цель: изучить понятия НОД и НОК, их свойства, теорему Евклида о НОД, научиться находить линейное представление НОД.

Вопросы, выносимые на практическое занятие.

1. Понятие общего делителя, наибольшего общего делителя, способы его вычисления.
2. Понятие общего кратного, наименьшего общего кратного, способы его вычисления.
3. Теорема Евклида и нахождение НОД, его линейного представления.
4. Свойства НОД и НОК.

Краткие теоретические сведения.

Всякое целое, делящее одновременно целые числа *a, b, ..., t*, называется их общим делителем.

Делитель d, который делится на любой другой общий делитель чисел *a, b, ..., t,* называется их наибольшим общим делителем и обозначается символом НОД(a, *b*, ... t) или просто (a, *b*, ... t).

ТЕОРЕМА. Наибольший по величине из общих делителей является наибольшим общим делителем.

Если (a, *b*, ..., *t)*=1 , то числа *a, b, ..., t* называются взаимно простыми. Если каждое из чисел *a, b, ..., t* взаимно просто с каждым другим из них, то последовательность *a, b, ..., t* называются последовательность попарно простых чисел.

Очевидно, числа попарно простые всегда и взаимно простые. В случае же двух чисел понятия «попарно простые» и «взаимно простые» совпадают.

ТЕОРЕМА. Если *a* кратно *b*, то совокупность общих делителей чисел *a* и b совпадает с совокупностью делителей одного *b*; в частности в этом случае *(a, b) = b*.

ТЕОРЕМА. Если $a = bq + c$, то совокупность общих делителей чисел *a* и *b* совпадает с совокупностью общих делителей чисел *b* и *c*; в частности

(a, b) = (b, c).

АЛГОРИТМ ЕВКЛИДА. Пусть *a* и *b* — положительные целые и *a*> *b* . Находим ряд равенств:

$a = bq_1 + r_1, 0 < r_1 < b$

$b = r_1q_2 + r_2, 0 < r_2 < r_1$

$r_1 = r_2q_3 + r_3, 0 < r_3 < r_2$

……

$r_{n-2} = r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}$

$r_{n-1} = r_nq_{n+1}$, т.е. $r_{n+1} = 0$.

ТЕОРЕМА. В соответствии с алгоритмом Евклида имеют место равенства *(a, b) = (b,* r_1*)=* (r_1, r_2)*=…=* $(r_{n-1}, r_n)= r_n$. Другими словами, наибольший общий делитель двух положительных чисел равен последнему отличному от 0 остатку в алгоритме Евклида.

ТЕОРЕМА. Для любых целых чисел *a* и *b* существуют такие целые *x* и *y* , что имеет место равенство *(a, b)= x a+ y b.*

ТЕОРЕМА. *((a, b), c)=(a, (b, c))=(a, b, c).*

ТЕОРЕМА. a) *(ma, mb)= m(a, b);*

b) Если *d* общий делитель чисел *a* и *b*, то имеет место равенство: $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$.

ТЕОРЕМА. а) Если *(a, b)=1*, то *(ac, b)= (c, b).*

b) Если *(a, b)=1* и *ac* делится на *b*, то *c* делится на *b*.

ТЕОРЕМА. $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \dots p_k^{\beta_k}$, то *(a, b)*= $p_1^{\gamma_1} \dots p_k^{\gamma_k}$, где $\gamma_i = \min(\alpha_i, \beta_i)$.

Всякое целое *k*, кратное всех данных чисел *a, b, ..., t* , называется их общим кратным и обозначается: *k*=ОК[*a, b, ..., t*].

Всякое целое *k*, кратное всех данных чисел *a, b, ..., t* и делящееся на любое другое общее кратное этих чисел, называется их наименьшим общим кратным и обозначается: *k=HOK*[*a, b, ..., t*] = [*a, b, ..., t*].

ТЕОРЕМА. Наименьшее положительное кратное чисел *a, b, ..., t* будет являться их наименьшим общим кратным.

ТЕОРЕМА. [*a, b*]=$\frac{ab}{(a,b)}$.

ТЕОРЕМА. [[*a, b*], c]=[*a*, [*b, c*]]=[*a, b, c*].

ТЕОРЕМА. $a = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \dots p_k^{\beta_k}$, то [*a, b*]= $p_1^{\gamma_1} \dots p_k^{\gamma_k}$, где $\gamma_i = \max(\alpha_i, \beta_i)$ для каждого *i*.

Примеры выполнения заданий.

Задание 1. Вычислить НОД *d = (a;b;c)* двумя способами: (347, 327, 630).

1) Разложим данные числа на простые множители.
   347=347 – простое число; 327=3·109; 630=$2^3 \cdot 3^2 \cdot 5$.
   Из разложений видно, что общих простых делителей нет. Поэтому НОД(347, 327, 630)=1.
2) Так как 347 простое число, а 327 < 347, то (347, 327)=1. А тогда имеем (347, 327, 630)=((347, 327), 630)=(1, 630)=1.

Задание 2. Пользуясь алгоритмом Евклида вычислить НОД и выразить его через исходные числа: 347, 327.

Применим алгоритм Евклида к данным числа. Запишем его поэтапно соответствующими равенствами.

$347 = 1 \cdot 327 + 20$, причем $0 < 20 < 327$.

$327 = 16 \cdot 20 + 7$, $0 < 7 < 20$.

$20 = 2 \cdot 7 + 6$, $0 < 6 < 7$.

$7 = 1 \cdot 6 + 1$, $0 < 1 < 6$.

Ясно, что 1 последний отличный от 0 остаток в алгоритме Евклида. Поэтому $(347, 327) = 1$.

Для нахождения линейного представления этого НОД через исходные числа будем последовательно выражать остатки через исходные числа.

$20 = 347 - 1 \cdot 327 = 1 \cdot 347 - 1 \cdot 327$. Подставим это выражение во второе равенство из алгоритма Евклида.

$327 = 16 \cdot (1 \cdot 347 - 1 \cdot 327) + 7 = 16 \cdot 347 - 16 \cdot 327 + 7$.

Отсюда выразим остаток 7 через исходные числа.

$7 = 327 - (16 \cdot 347 - 16 \cdot 327) = -16 \cdot 347 + 17 \cdot 327$. Подставим это линейное представление остатка 7 в третье равенство из алгоритма Евклида.

$20 = 2 \cdot 7 + 6 = 2 \cdot (-16 \cdot 347 + 17 \cdot 327) + 6$.

Выразим остаток 6 линейно через исходные числа.

$6 = 20 - (2 \cdot (-16 \cdot 347 + 17 \cdot 327)) = (1 \cdot 347 - 1 \cdot 327) - 2 \cdot (-16 \cdot 347 + 17 \cdot 327) =$

$= 33 \cdot 347 - 35 \cdot 327$. Подставим это линейное представление остатка 6 в последнее равенство в алгоритме Евклида.

7 = 1· (33·347-35·327) +1. Заменим 7 на его линейное представление через исходные числа.

(- 16·347+17·327) = 1· (33·347-35·327) +1. Отсюда выражаем последний отличный от 0 остаток в алгоритме Евклида через исходные числа.

1 = (- 16·347+17·327) - 1· (33·347-35·327) = -49·347 + 52·327.

Сделаем проверку. -49·347 + 52·327 = -17003 + 17004 = 1.

Ответ НОД(347, 327)= 1 = -49·347 + 52·327.

Задание 3. Для пар чисел задания 2 найти наименьшее общее кратное. Результат вычисления НОК проверить разложением чисел на простые множители.

НОК(347, 327)= $\frac{347 \cdot 327}{\text{НОД}(347,327)} = \frac{113469}{1} = 113469.$

НОК(347, 327)= 347·3·109=1134369.

Задание 4. Сократите следующие дроби, представив числитель и знаменатель дроби в каноническом виде: $\frac{1599}{2058}$.

$\frac{1599}{2058} = \frac{2 \cdot 3 \cdot 7^3}{3 \cdot 13 \cdot 41} = \frac{2 \cdot 7^3}{13 \cdot 41} = \frac{686}{533}$.

Задание 5. Пользуясь расширенным алгоритмом Евклида вычислить НОД и выразить его через исходные числа: 347, 327, 630.

Ранее было установлено, что (347, 327, 630) = ((347, 327), 630) = (1, 630) = 1.

Причем, (347, 327) = 1 и 1= -49·347 + 52·327.

Заметим, что из равенства (1, 630)=1следует, что 1=1· 1 + 0· 630. Учитывая полученное представление для 1 через исходные два числа, получаем

1=1· 1 + 0· 630= 1=1· (-49·347 + 52·327) + 0· 630 = -49·347 + 52·327 + 0· 630.

Это и будет линейным представлением НОД.

НОД (347, 327, 630) = -49·347 + 52·327 + 0· 630.

Практические задания по вариантам.

Задание1. Вычислить НОД *d = (a;b;c)* двумя способами:

Вариант 1. (2737; 9163; 9639).
Вариант 2. (1411; 4641; 5253).
Вариант 3. (9163; 2737; 9639).
Вариант 4. (374; 1599; 9061).
Вариант 5. (299; 391; 667).
Вариант 6. (588; 2058; 2849).
Вариант 7. (31605; 13524; 12915).
Вариант 8. (279; 372; 1395).
Вариант 9. (2988; 3735; 8134).
Вариант 10. (420; 630; 1155).

Задание 2. Пользуясь алгоритмом Евклида вычислить НОД и выразить его через исходные числа:

Вариант 1. (822; 1734).
Вариант 2. (4623; 3743).
Вариант 3. (4373; 826).
Вариант 4. (3791; 3281).
Вариант 5. (1073; 3683).
Вариант 6. (2576; 154).
Вариант 7. (546; 231).
Вариант 8. (1001; 6253).
Вариант 9. (1517; 2257).
Вариант 10. (2737; 9639).

Задание 3. Для пар чисел задания 2 найти наименьшее общее кратное. Результат вычисления НОК проверить разложением чисел на простые множители.

Задание 4. Сократите следующие дроби, представив числитель и знаменатель дроби в каноническом виде:

Вариант 1. 17501/11137.
Вариант 2. 1491/2247.
Вариант 3. 237419/294817.
Вариант 4. 1253/406.
Вариант 5. 438875/747843.
Вариант 6. 127936/161919.
Вариант 7. 2227/9911.
Вариант 8. 22243/23777.

Вариант 9. 2405/4433. **Вариант 10. 3587/2743.**

Задание 5. Пользуясь расширенным алгоритмом Евклида вычислить НОД и выразить его через исходные числа:

Вариант 1. (943; 2737; 667);
Вариант 2. (3655; 2516; 154);
Вариант 3. (667; 299; 12915);
Вариант 4. (731; 663, 9639);
Вариант 5. (899; 493; 9639);
Вариант 6. (91476; 3960; 1395);
Вариант 7. (1445; 629; 2257);
Вариант 8. (588; 2058; 9061);
Вариант 9. (903; 731; 13524);
Вариант 10. (689; 702; 5253).

РАБОТА №4. Цепные дроби.

Цель: Познакомиться с понятиями цепных и подходящих дробей, способами их вычисления и применения.

Вопросы, выносимые на практическое занятие.

1. Правильная цепная дробь и способы ее вычисление.
2. Подходящие дроби и их свойства.
3. Нахождение числа по значению его цепной дроби.
4. Приближенное вычисление числа через подходящие дроби.

Краткие теоретические сведения.

Пусть a -любое вещественное число. Обозначим буквою $q_1 = [a]$ целую часть числа a . Если число a не целое, тогда $a = q_1 + \frac{1}{a_1}$, где $a_1 > 1$. Точно так же при нецелых $a_1, a_2, \dots, a_{s-2}$ имеем

$$a = q_0 + \frac{1}{a_1}, \text{ где } a_1 > 1;$$

$$a_1 = q_1 + \frac{1}{a_2}, \text{ где } a_2 > 1;$$

$$\dots\dots\dots\dots\dots\dots\dots\dots$$

$$a_{s-2} = q_{s-1} + \frac{1}{a_s}, \text{ где } a_s > 1.$$

ввиду чего получаем следующее разложение a в непрерывную дробь:

$$a = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots}}$$
$$\cdots$$
$$\cdots$$
$$+ \cfrac{1}{q_{s-1} + \cfrac{1}{a_s}}$$

При иррациональном a всякое a_s будет иррациональным и процесс может быть продолжен сколь угодно долго (неограниченно). Если же a рациональное число, то оно может быть представлено несократимой дробью $a = \frac{n}{m}$ с положительным знаменателем. Тогда этот процесс конечен и представляется через алгоритм Евклида.

$$n = m \cdot q_0 + r_1, 0 < r_1 < m;$$

$$m = r_1 \cdot q_1 + r_2, 0 < r_2 < r_1;$$

……..

$$r_{s-2} = r_{s-1}q_{s-1} + r_s, 0<r_s < r_{s-1};$$

$$r_{s-1} = r_s q_s.$$

Или разделив каждое равенство на делитель и в последней дроби перенеся числитель в знаменатель получим:

$$a = \frac{n}{m} = q_0 + \frac{1}{\frac{m}{r_1}}$$

$$\frac{m}{r_1} = q_1 + \frac{1}{\frac{r_2}{r_1}}$$

… … … … … …

$$\frac{r_{s-2}}{r_{s-1}} = q_{s-1} + \frac{1}{\frac{r_{s-1}}{r_s}}$$

$$\frac{r_{s-1}}{r_s} = q_s.$$

Подставляя неполные частные в каждое предыдущее выражение окончательно получим:

$$a = \frac{n}{m} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cdots}}$$

$$\cdots$$

$$\cdots$$

$$+ \cfrac{1}{q_{s-1} + \cfrac{1}{q_s}}$$

Кратко это принято записывать следующим образом:

$$a = \frac{n}{m} = [q_0; q_1, q_2, \dots, q_{s-1}, q_s]$$

Дроби $\delta_0 = q_0,\ \delta_1 = q_0 + \frac{1}{q_1} = [q_0; q_1],\ \dots$ называются подходящими дробями.

Предполагая, что $\delta_i = \frac{P_i}{Q_i}$ можно записать рекуррентные соотношения для вычислений числителей и знаменателей.

ТЕОРЕМА. $P_i = q_i \cdot P_{i-1} + P_{i-2}$;

$$Q_i = q_i \cdot Q_{i-1} + Q_{i-2}.$$

Для единообразия принято считать, что $P_0 = 1,\ Q_0 = 0$. Тогда вычисление подходящих дробей удобно проводить через заполнение следующей таблицы.

q		q_0	q_1	q_2	$\cdots$	q_{i-1}	q_i	$\cdots$	q_s
P	1	P_0	P_1	P_2	$\cdots$	P_{i-1}	$P_i = q_i \cdot P_{i-1} + P_{i-2}$	$\cdots$	P_s
Q	0	Q_0	Q_1	Q_2	$\cdots$	Q_{i-1}	$Q_i = q_i \cdot Q_{i-1} + Q_{i-2}$	$\cdots$	Q_s

ТЕОРЕМА. Для любого i Q_i является целым числом, а P_i – натуральным.

ТЕОРЕМА. Для любого i $P_i < P_{i+1}$.

ТЕОРЕМА. Для i>0 имеем $P_i \cdot Q_{i-1} - Q_i \cdot P_{i-1} = (-1)^i$.

ТЕОРЕМА. $(P_i, Q_i) = 1$.

ТЕОРЕМА. Если последнее частное в алгоритме Евклида отлично от 1, то представление рационального числа в виде непрерывной дроби единственно.

ТЕОРЕМА. Для любого i $\frac{Q_{2i-2}}{P_{2i-2}} < \frac{Q_{2i}}{P_{2i}}$ и $\frac{Q_{2i-1}}{P_{2i-1}} > \frac{Q_{2i+1}}{P_{2i+1}}$, т.е. подходящие дроби с четными номерами только возрастают, а с нечетными – убывают.

ТЕОРЕМА. Для i >1 выполняется равенство $\delta_i - \delta_{i-1} = \frac{(-1)^i}{Q_i \cdot Q_{i-1}}$.

ТЕОРЕМА. Для i >1 выполняется неравенство
$\left|\frac{n}{m} - \delta_i\right| < \frac{1}{|Q_i \cdot Q_{i-1}|}$.

Примеры выполнения заданий.

Задание 1. Разложить простую дробь $\frac{a}{b}$ в правильную цепную дробь и найти все её подходящие дроби, если $\frac{a}{b} = \frac{143}{31}$.

Применим алгоритм Евклида.

143=31·4+19, т.е. $q_0 = 4$.

31=19·1+12, т.е. $q_1 = 1$.

19=12·1+7, т.е. $q_2 = 1$.

12=7·1 +5, т.е. $q_3 = 1$.

7=5·1+2, т.е. $q_4 = 1$.

5=2·2+1, т.е. $q_5 = 2$.

2=1·2+0.

Таким образом $\frac{143}{31} = [4; 1, 1, 1, 1, 2]$.

Составим таблицу вычисления подходящих дробей.

q		$q_0 = 4$	$q_1 = 1$	$q_2 = 1$	$q_3 = 1$	$q_4 = 1$	$q_5 = 2$	$q_6 = 2$
P	1	4	5	9	14	23	60	143
Q	0	1	1	2	3	5	13	31

Таким образом, получаем $\delta_0 = 4,\ \delta_1 = 5,\ \delta_2 = \frac{9}{2},\ \delta_3 = \frac{14}{3},\ \delta_4 = \frac{23}{5},$

$\delta_5 = \frac{60}{13},\ \delta_6 = \frac{143}{31}$.

Задание 2. Сократить следующие дроби, пользуясь их разложением в цепную дробь. $\frac{a}{b} = \frac{143}{31}$ **.**

Как мы знаем, подходящие дроби не сократимы. В решении предыдущей задачи мы получили, что $\delta_6 = \frac{143}{31}$. Следовательно, эта дробь не сократима.

Задание 3. Найти значение несократимой дроби $\frac{a}{b} = \frac{141}{31}$ **по значению цепной дроби.**

Как и в задаче 1 применим алгоритм Евклида.

141=31·4+17, 31=17·1+14, 17=14·1+3, 14=3· 4+2, 3=2·1+1, 2=1·2+0.

Значит, имеем: $q_0 = 4,\ q_1 = 1, q_2 = 1, q_3 = 4, q_4 = 1, q_5 = 2$.

Составим таблицу для вычисления подходящих дробей.

q		$q_0 = 4$	$q_1 = 1$	$q_2 = 1$	$q_3 = 4$	$q_4 = 1$	$q_5 = 2$
P	1	4	5	9	41	50	141
Q	0	1	1	2	9	11	31

Последняя подходящая дробь равна исходному числу, а подходящие дроби являются несократимыми дробями. Следовательно исходная дробь является несократимой.

Задание 4. Разложить в цепную дробь $\frac{a}{b}$ **и заменить подходящей дробью** $\frac{P_k}{Q_k}$**, если** $k = 6$. $\frac{a}{b} = \frac{51521}{1423}$.

Применим алгоритм Евклида.

15521=1423·10+1291, т.е. $q_0 = 10$.

1423=1291·1+132, т.е. $q_1 = 1$.

1291=132·9+103, т.е. $q_2 = 9$.

132=103·1+29, т.е. $q_3 = 1$.

103=29·3+16, т.е. $q_4 = 3$.

29=16·1+13, т.е. $q_5 = 1$.

16=13·1+3, т.е. $q_6 = 1$.

13=3·4+1, т.е. $q_7 = 4$.

3=1·3+0, т.е. $q_8 = 3$.

Составим таблицу для вычисления подходящих дробей.

q		$q_0 = 10$	1	9	1	3	1	$q_6 = 1$	4	3
P	1	10	11	109	120	469	589	1058	4821	15521
Q	0	1	1	10	11	43	54	97	442	1423

Таким образом, имеем $\frac{P_6}{Q_6} = \frac{1058}{97}$ **.**

Задание 5. Для задания № 1 с помощью подходящих дробей найти приближение к дроби $\frac{a}{b}$ с точностью до 0,001.

Чтобы получить точность 0,001 у нас должно быть произведение $Q_i \cdot Q_{i-1}$ быть боле, или равно 1000.

Будем находить эти произведения последовательно для разных i.

i=1: $Q_1 \cdot Q_0 = 1 \cdot 1 = 1 < 1000$.

i=2: $Q_2 \cdot Q_1 = 2 \cdot 1 = 2 < 1000$.

i=3: $Q_3 \cdot Q_2 = 3 \cdot 2 = 6 < 1000$.

i=4: $Q_4 \cdot Q_3 = 5 \cdot 3 = 15 < 1000$.

i=5: $Q_5 \cdot Q_4 = 13 \cdot 5 = 45 < 1000$.

i=6: $Q_6 \cdot Q_5 = 31 \cdot 13 = 403 < 1000$.

Но уже последняя подходящая дробь $\delta_6 = \frac{143}{31}$ равна исходному числу, т.е. разность $\frac{a}{b} - \delta_6 = \frac{143}{31} - \frac{143}{31} = 0$. Поэтому данная подходящая дробь обеспечивает необходимую точность.

Практические задания по вариантам.

Задание 1. Разложить простую дробь $\frac{a}{b}$ в правильную цепную дробь и найти все её подходящие дроби, если $\frac{a}{b}$ равно:

Вариант 1. $\frac{137}{31}$**;** **Вариант 2.** $\frac{521}{143}$**;**

Вариант 3. $\frac{247}{74}$**;** **Вариант 4.**$-\frac{313}{57}$**;**

Вариант 5. $\frac{77}{187}$**;** **Вариант 6.**$-\frac{53}{217}$**;**

Вариант 7. $\frac{23}{18}$**;** **Вариант 8.** $\frac{521}{143}$**;**

Вариант 9. $\frac{36}{19}$**;** **Вариант 10.** $-\frac{83}{217}$**.**

Задание 2. Сократить следующие дроби, пользуясь их разложением в цепную дробь.

Вариант 1. $\frac{871}{3953}$; **Вариант 2.**$\frac{1241}{6059}$;

Вариант 3.$\frac{6821}{2147}$; **Вариант 4.**$\frac{32671}{10027}$;

Вариант 5. $\frac{1180}{1829}$; **Вариант 6.** $\frac{2227}{9911}$;

Вариант 7. $\frac{1043}{3427}$; **Вариант 8.** $\frac{1857}{9153}$;

Вариант 9. $\frac{1241}{6059}$; **Вариант 10.** $\frac{3953}{1027}$**.**

Задание 3. Найти значение несократимой дроби $\frac{a}{b}$ по значению цепной дроби:

Вариант 1. $\frac{a}{b} = [-2;\ 1,3,1,1,5]$; **Вариант 2.** $\frac{a}{b} = [2;\ 1,19,1,3]$;

Вариант 3. $\frac{a}{b} = [2;\ 1,1,3,1,2]$; **Вариант 4.** $\frac{a}{b} = [1;1,2,3,4]$;

Вариант 5. $\frac{a}{b} = [0;\ 4,1,2,5,6]$; **Вариант 6.** $\frac{a}{b} = [-3;\ 1,2,1,1,5]$;

Вариант 7. $\frac{a}{b} = [-5;\ 2, 1, 1, 3, 2]$; **Вариант 8**. $\frac{a}{b} = [1;\ 3, 2, 4, 3, 1, 1, 1, 5]$;

Вариант 9. $\frac{a}{b} = [\ 1;\ 3, 1, 1, 5]$; **Вариант 10**. $\frac{a}{b} = [2;\ 1, 3, 1, 1, 5]$.

Задание 4. Разложить в цепную дробь $\frac{a}{b}$ и заменить подходящей дробью $\frac{P_k}{Q_k}$, если $k = 6$.

Вариант 1. $\frac{2121}{1500}$; **Вариант 2**. $\frac{314}{450}$;

Вариант 3. $\frac{652}{636}$; **Вариант 4**. $\frac{9321}{10959}$;

Вариант 5. $-\frac{2485}{1638}$; **Вариант 6**. $-\frac{840}{1872}$;

Вариант 7. $\frac{891}{1530}$; **Вариант 8**. $-\frac{1872}{1560}$;

Вариант 9. $\frac{3129}{10281}$; **Вариант 10**. $-\frac{3523}{1300}$.

Задание 5. Для задания № 1 с помощью подходящих дробей найти приближение к дроби $\frac{a}{b}$ с точностью до 0,001.

Список литературы

1. Веселова, Л. В. Алгебра и теория чисел: Учебное пособие / Л. В. Веселова, О. Е. Тихонов. – Казань: Казанский национальный исследовательский технологический университет, 2014. – 107 с. – ISBN 978-5-7882-1636-2.
2. Ларин, С. В. Алгебра и теория чисел. Группы, кольца и поля: Учебное пособие / С. В. Ларин. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2020. – 1 с. – (Высшее образование). – ISBN 978-5-534-05567-2.
3. Швед, Е. А. Практикум по алгебре: элементы теории чисел / Е. А. Швед, В. А. Федоров. – Омск: Омский государственный университет путей сообщения, 2022. – 39 с.
4. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел: учебное пособие / Л. Б. Шнеперман; Л. Б. Шнеперман. – 3-е изд., стер.. – Санкт-Петербург [и др.]: Лань, 2008. – (Учебники для вузов. Специальная литература). – ISBN 978-5-8114-0885-6.
5. Виноградов, И. М. Основы теории чисел [Текст]: учебное пособие / И. М. Виноградов. - Изд. 12-е, стер. - СПб. [и др.]: Лань, 2009. -176 с.
6. Виноградов, И. М. Элементы высшей математики: аналитическая геометрия, дифференциальное исчисление: учебник для студентов высших учебных заведений, обучающихся по инженерно-техническим специальностям / И. М. Виноградов; И. М. Виноградов. – Москва: Дрофа, 2010. – 319 с. – (Высшее образование. Современный учебник). – ISBN 978-5-358-06101-9.
7. Гончаренко, В. М. Элементы высшей математики / В. М. Гончаренко, Л. В. Липагина, А. А. Рылов. – МОСКВА: Компания КноРус, 2019. – 364 с. – ISBN 978-5-406-06878-6.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«_11_» _04_____2023 г.

Теория сравнений

Методические рекомендации

для выполнения практических заданий по дисциплинам

«Элементы алгебры и теории чисел» и «Алгебра и теория чисел»

Направления подготовки: 10.03.01 «Информационная безопасность»;
02.03.03 «Математическое обеспечение и администрирование
информационных систем».

Курск – 2023

УДК 511+512(075.8)
Составители:
д. ф-м. н., профессор В.П. Добрица
к.т.н. Е.А. Кулешова
к.т.н., доцент Ю.А. Халин

Рецензент

Кандидат технических наук, доцент кафедры вычислительной техники А.В. Киселев

Теория сравнений: методические рекомендации для выполнения практических заданий / Юго-Зап. гос. ун-т; сост.: В.П. Добрица, Е.А. Кулешова, Ю.А. Халин. – Курск, 2023. – 36 с. – Библиогр.: с. 36.

В методических указания описываются основны алгебры и теории чисел. Изложены краткие теоретические сведения, приведены примеры решения задач, а также задачи для самостоятельного решения.

Методические рекомендации предназначены для студентов, обучающихся по направлениям подготовки 10.03.01 «Информационная безопасность» и 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. 232
Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

В данных методических рекомендациях изложены материалы по разделам «Сравнения чисел. Сравнений с неизвестным. Системы сравнений. Первообразные корни и индексы.» курсов «Элементы алгебры и теории чисел» и «Алгебра и теория чисел».

Рассмотрены следующие темы: сравнение чисел, системы вычетов, свойства числовых сравнений, приложения числовых сравнений, сравнения с одним неизвестным, решения сравнений с неизвестным, системы сравнений с неизвестным и способы их решения, первообразные корни и индексы, нахождение первообразных корней и вычисление индексов.

По каждой теме представлены:

1) краткие теоретические положения;
2) перечень вопросов, выносимых на практическое задание;
3) примеры решения типовых задач, выносимых на практическое занятие;
4) задачи, выносимые на самостоятельную работу студентов.

Данные методические рекомендации предназначены для проведения практических занятий по дисциплинам «Элементы алгебры и теории чисел» и «Алгебра и теория чисел» для студентов Юго-Западного государственного университета направлений подготовки: информационная безопасность, математическое обеспечение и администрирование информационных систем.

По изложенным в данных методических рекомендациях материалам можно рекомендовать преподавателю проведение 8-ми часов практических занятий по следующему плану:

- Числовые сравнения и их свойства.(2 часа)
- Системы вычетов по модулю. Приложения числовых сравнений. (2 часа)
- Сравнения с неизвестным. Сравнения первой степени. (2 часа)
- Системы сравнений. Первообразные корни и индексы. (2 часа)

При выполнении практических заданий в каждой задаче выберете задание из своего варианта. Вариант определяется по последней цифре номера зачетной книжки. Отчет по работе должен содержать решения задач и выводы с полным их обоснованием. Отчет по работе оформить на листах формата А4 в формате WORD. На титульном листе должно быть указано: университет, факультет, кафедра, предмет, номер практического занятия, вариант, группа, исполнитель, проверяющий.

РАБОТА № 1 (5) Числовые сравнения и их свойства

Цель: изучить понятие сравнения по числовому модулю, свойства числовых сравнений, познакомиться с приложениями числовых сравнений.

Вопросы, выносимые на практическое занятие.

1. Проверка сравнимости чисел по модулю.
2. Классы и системы вычетов по числовому модулю.
3. Свойства числовых сравнений.
4. Приложения теории числовых сравнений.

Краткие теоретические сведения.

Два целых числа a и b называются сравнимыми по положительному модулю m $(a \equiv b\ (mod\ m))$, если их разность $a - b$ делится на m.

ТЕОРЕМА. Отношение сравнения чисел ≡ является

1) рефлексивным, т.е. $a \equiv a\ (mod\ m)$,
2) симметричным, т.е. если $a \equiv b\ (mod\ m)$, то $b \equiv a\ (mod\ m)$,
3) транзитивным, т.е. если $a \equiv b\ (mod\ m)$ и $b \equiv c\ (mod\ m)$, то $a \equiv c\ (mod\ m)$.

Рефлексивные, симметричные и транзитивные бинарные отношения называются отношениями эквивалентности.

ТЕОРЕМА. $a \equiv b\ (mod\ m)$ тогда и только тогда, когда остатки от деления чисел a и b на m будут одинаковыми.

Поэтому сравнимые числа называют равноостаточными.

ТЕОЕРЕМА. Если $a \equiv b\ (mod\ m)$, то число a может быть представлено в следующем виде $a = b + m \cdot t$ при некотором t .

ТЕОРЕМА. Сравнения можно почленно складывать, т.е. если $a \equiv b\ (mod\ m)$ и $c \equiv d\ (mod\ m)$, то имеем $a + c \equiv b + d\ (mod\ m)$.

ТЕОРЕМА. Слагаемое, стоящее в какой либо части сравнения, можно перенести в другую часть сравнений с противоположным знаком.

ТЕОРЕМА. К любой из частей сравнения можно прибавить число, кратное модулю.

ТЕОРЕМА. Сравнения можно почленно перемножать.

ТЕОРЕМА. Обе части сравнения можно умножать на одно и то же целое число.

ТЕОРЕМА. Обе части сравнения можно возводить в любую натуральную степень.

ТЕОРЕМА. Если $a \equiv b\ (mod\ m)$, $(a, b) = d$ и $(m, d)=1$, то имеем верное сравнение $\frac{a}{d} \equiv \frac{b}{d}(mod\ m)$.

ТЕОРЕМА. Если $a \equiv b\ (mod\ m)$, и $d|m$, то $a \equiv b\ (mod\ d)$.

ТЕОРЕМА. Если $a \equiv b\ (mod\ m_1)$ и $a \equiv b\ (mod\ m_2)$, а $m = [m_1, m_2]$, то $a \equiv b\ (mod\ m)$.

ТЕОРЕМА. Если $a \equiv b\ (mod\ m)$ и $d|m$, $d|a$, то $d|b$.

ТЕОРЕМА. Если $a \equiv b\ (mod\ m)$, то $(a, m) = (b, m)$.

Примеры выполнения заданий

Задача 1. **Какие из следующих сравнений являются верными:**

$11 \equiv -2\ (mod\ 7), -5 \equiv 9\ (mod\ 7)$.

Для первого сравнения рассмотрим разность 11-(-2)=13. Оно не делится на 7, значит первое сравнение не верно. Можно это установить через остатки от деления чисел на модуль. 11=7+4, -2= (-1)·7+5. Остатки не равны: 4≠5. Поэтому сравнение не верно.

Для второго сравнения разность (-5)-9=-14 делится на 7. Следовательно, сравнение верное. -5=(-1) ·7+2, 9=1 ·7+2, т.е. остатки от деления на 7 равны, что подтверждает верность сравнения.

Задача 2. **Найти две последние цифры числа a^n: 11^9.**

Найти две последние цифры числа это значит надо сравнить это число с наименьшим неотрицательным вычетом по модулю 100.

$11^9 \equiv r\ (mod\ 100)$. На основании свойств сравнений проведем преобразование данного сравнения.

$$11^9 \equiv (11^8) \cdot 11 \equiv (11^2)^4 \cdot 11 \equiv r(mod\ 100)$$

$11^2 = 121 \equiv 21(mod\ 100)$, значит $11^9 \equiv (21)^4 \cdot 11 \equiv (21^2)^2 \cdot 11\ (mod\ 100)$

$21^2 = 441 \equiv 41(mod\ 100)$, значит $11^9 \equiv (41)^2 \cdot 11\ (mod\ 100)$

$(41)^2$ =1681≡ $81(mod\ 100)$, поэтому $11^9 \equiv 81 \cdot 11 \equiv 191 \equiv 91(mod\ 100)$.

Таким образом, две последние цифры числа 11^9 представляют собой число 91.

Задача 3. **Найти остаток от деления числа a^n на m: $a = 29^9$, m =7.**

29=28+1, т.е. $29 \equiv 1\ (mod\ 7)$, а потому $29^9 \equiv (1)^9 \equiv 1\ (mod\ 7)$

Таким образом, остаток от деления числа 29^9 на 7 равен 1.

Задача 4. **Найти остаток от деления суммы $a + b + c$ на число m:**

$13^{80} + 7^{80} + 12^{1231}$, m =11.

Сначала вычислим остатки от деления на 11 каждого слагаемого из данной суммы.

$13^{80} \equiv 2^{80} \equiv ((2)^4)^{20} \equiv 16^{20} \equiv 5^{20} \equiv 25^{10} \equiv 3^{10} \equiv 9^5 \equiv (-2)^5 \equiv -32 \equiv 1(mod\ 11)$,

$7^{80} \equiv ((7)^2)^{40} \equiv (49)^{40} \equiv 5^{40} \equiv (5^{20})^2 \equiv 1^2 \equiv 1(mod\ 11)$,

$12^{1231} \equiv 1^{1231} \equiv 1(mod\ 11)$,

Отсюда имеем $13^{80} + 7^{80} + 12^{1231} \equiv (1 + 1 + 1) \equiv 3(mod\ 11)$.

Таким образом, остаток от деления числа $13^{80} + 7^{80} + 12^{1231}$ на 11 равен 3.

Задача 5. **Выведите признаки делимости на 3.**

Заметим, что каждое число $a_n a_{n-1} \dots a_1 a_0$ можно представить в виде суммы $a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$. Кроме того, заметим, что $10 \equiv 1(mod\ 3)$ и значит $10^k \equiv 1(mod\ 3)$. А потому имеем:

$a_n a_{n-1} \dots a_1 a_0 = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0 \equiv a_n + a_{n-1} + \dots + a_1 + a_0 (mod\ 3)$.

Из этой формулы и получаем признак делимости на 3.

Число делится на 3 тогда и только тогда, когда сумма его цифр делится на 3.

Практические задания по вариантам

Задание 1. Какие из следующих сравнений являются верными:

Вариант 1. 1 ≡ -5(mod 6); **Вариант 2. 546 ≡ 0(mod 13);**

Вариант 3. 21 ≡ 1 (mod 4); **Вариант 4. 121347 ≡ 92817(mod 10);**

Вариант 5. 31 ≡ -9(mod 10); **Вариант 6. 35 ≡ 27(mod 8);**

Вариант 7. 99 ≡ 11 (mod 4); **Вариант 8. 1347 ≡ 817(mod 10);**

Вариант 9. 10 ≡ -14(mod 6); **Вариант 10. 546 ≡ 0(mod 13).**

Задание 2. Найти две последние цифры числа a^n:

Вариант 1. 9^{10} ; **Вариант 2. 9^9;**

Вариант 3. 6^{32}; **Вариант 4.** 8^{18} ;

Вариант 5. 4^{20} ; **Вариант 6.** 2^{100};

Вариант 7. 19^{321}; **Вариант 8.** 131^{61} ;

Вариант 9. 243^{402}; **Вариант 10.** 17^{161}.

Задание 3. Найти остаток от деления числа a^n на m:

Вариант 1. 20^{11} **, m=9;** **Вариант 2.** 383^{175}**, m=45;**

Вариант 3. 109^{345}**, m=14;** **Вариант 4.** 439^{291} **, m=60;**

Вариант 5. 293^{275} **, m=48;** **Вариант 6.** 93^{41}**, m=11;**

Вариант 7. 3^{80}**, m=11;** **Вариант 8.** 20^{17} **, m=9;**

Вариант 9. 3^{200}**, m=101;** **Вариант 10.** 11^{65}**, m=80.**

Задание 4. Найти остаток от деления суммы $a + b + c$ на число m:

Вариант 1. $3^{80} + 7^{80}+12^{1231}$**, m=11;** **Вариант 2.** $3^{100} + 5^{100}+14^{4324}$**, m=7;**

Вариант 3. $2^{100}+3^{100}+11^{65}$**, m=5;** **Вариант 4.** $5^{70} +7^{50}+11^{65}$**, m=12;**

Вариант 5. $12^{1231} + 14^{4324}+7^{80}$**, m=13;** **Вариант 6.** $7^{65} + 11^{65}+15^{9}$**, m=80;**

Вариант 7. $3^{200} + 7^{200}+15^{9}$**, m=101;** **Вариант 8.** $5^{80} + 7^{100}+12^{1231}$**, m=13;**

Вариант 9. $5^{70} + 7^{50}+11^{65}$**, m=12;** **Вариант 10.** $13^{100} + 5^{50}+15^{9}$**, m=18.**

Задание 5. Выведите признаки делимости на:

Вариант 1. m=9; **Вариант 2. m=45;**

Вариант 3. m=14; **Вариант 4. m=61;**

Вариант 5. m=15; **Вариант 6. m=16;**

Вариант 7. m=13; **Вариант 8. m=12;**

Вариант 9. m=11; **Вариант 10. m=8.**

РАБОТА № 2 (6) Различные системы вычетов по модулю.

Цель: изучить понятия системы вычетов и их различные виды, познакомиться с различными способами нахождения систем вычетов, освоить способы проверки набора чисел на соответствие определенной системе вычетов.

Вопросы, выносимые на практическое занятие.

1. Нахождение различных вычетов по числовому модулю.
2. Описание классов вычетов по модулю.
3. Составление полных систем вычетов.
4. Нахождение приведенных систем вычетов.

Краткие теоретические сведения.

Множество чисел $\{ a = b + m \cdot t \mid$ где $t -$ целое число$\}$ называется классом чисел, сравнимых с b по модулю m, или классом вычетов.

Любое число этого класса называется представителем, или вычетом этого класса по модулю m.

ТЕОРЕМА. Если $\{a = b + m \cdot t \mid$ где t – целое число$\}$ и $b = m \cdot q + r, 0 \leq r < m$, то класс $\{a = b + m \cdot t \mid$ где t – целое число$\}$ равен классу $\{a = r + m \cdot t \mid$ где t – целое число$\}$.

При этом число r называется наименьшим неотрицательным вычетом этого класса. Вычет из этого класса, имеющий наименьшее абсолютное значений, называется абсолютно наименьшим вычетом. Класс вычетов может определяться любым своим представителем.

Совокупность вычетов строго по одному из каждого класса называется полной системой вычетов по данному модулю.

ТЕОРЕМА. Различные m чисел, попарно не сравнимых между собой по модулю m, образуют полную систему вычетов.

ТЕОРЕМА. Числа $0,1,\dots,m-1$ образуют полную систему наименьших неотрицательных вычетов по модулю m.

ТЕОРЕМА. Числа $1,\dots,m$ образуют полную систему наименьших положительных вычетов по модулю m.

ТЕОРЕМА. При нечетном m полной системой абсолютно наименьших вычетов является совокупность: $-\frac{m-1}{2},\dots,-1,0,1,\dots,\frac{m-1}{2}$.

ТЕОРЕМА. При четном m полной системой абсолютно наименьших вычетов является одна из следующих последовательностей:

$-\frac{m}{2}+1,\dots,-1,0,1,\dots,\frac{m}{2}$ или $-\frac{m}{2},\dots,-1,0,1,\dots,\frac{m}{2}-1$.

Класс называется взаимно простым с модулем, если его представитель взаимно прост с этим модулем.

ТЕОРЕМА. Если класс взаимно прост с модулем, то это же верно для любого представителя этого класса.

Приведенной системой вычетов по модулю m называется система вычетов, взятых по одному из каждого класса, взаимно простого с модулем m.

ТЕОРЕМА. В приведенной системе вычетов по модулю m содержится $\varphi(m)$ элементов. ($\varphi(m)$ – функция Эйлера.)

ТЕОРЕМА. Любые $\varphi(m)$ чисел, попарно несравнимые по модулю m и взаимно простые с этим модулем, образуют приведенную систему вычетов.

Примеры выполнения заданий.

Задание 1. Заменить число *a* наименьшим по абсолютной величине, а также наименьшим положительным вычетом по модулю m.

$$a = 82, m = 87.$$

Заметим, что 0<82<87. Поэтому 82 является наименьшим положительным вычетом класса по модулю 87. Для нахождения наименьшего по абсолютной величине вычета рассмотрим два числа 82 и 82-87=-5 из этого же класса. Ясно, что $|-5| < |82|$. Поэтому наименьшим по абсолютной величине вычетом данного класса будет число -5.

Задание 2. Записать полную систему наименьших неотрицательных и наименьших по абсолютной величине вычетов по модулю m. $m = 25$.

В соответствии с теорией полной системой наименьших неотрицательных чисел будет являться последовательность:

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24.

Число 25 является нечетным, поэтому полной системой абсолютно наименьших вычетов будет являться последовательность:

-12, -11, -10, -9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.

Задание 3. Проверить, образуют ли числа $(a_1, a_2,\ldots,a_n)$ полную систему вычетов по модулю m:

(-23, - 43, -33, 36, 25, 21, 31, -2, 11, 13, -12, -5, 8, 9, -10), m=15.

В данном множестве 15 различных чисел, т.е. требование о числе элементов в системе вычетов выполняется. Для сравнения их по принадлежности одному классу вычислим их остатки при делении на 15.

-23=15·(-2)+7, т.е. в данном случае остаток равен 7.

-43=15·(-3)+2, т.е. в данном случае остаток равен 2.

-33=15·(-3)+12, т.е. в данном случае остаток равен 12.

36=15·2+6, т.е. в данном случае остаток равен 6.

25=15·1+10, т.е. в данном случае остаток равен 10.

21=15·1+6, т.е. в данном случае остаток равен 6.

31=15·2+1, т.е. в данном случае остаток равен 1.

-2=15·(-1)+13, т.е. в данном случае остаток равен 13.

11=15·0+11, т.е. в данном случае остаток равен 11.

13=15·0+13, т.е. в данном случае остаток равен 13.

-12=15·(-1)+ 3, т.е. в данном случае остаток равен 3.

-5=15·(-1)+10, т.е. в данном случае остаток равен 10.

8=15· 0+8, т.е. в данном случае остаток равен 8.

9=15· 0+9, т.е. в данном случае остаток равен 9.

-10=15·(-1)+ 5, т.е. в данном случае остаток равен 5.

Так как остатки 6, 10, 13 повторяются, то соответствующие пары чисел взяты из одинаковых классов вычетов, а значит, данная совокупность чисел не является полной системой вычетов по модулю 15.

Задание 4. Проверить, образуют ли числа *($a_1, a_2,\ldots,a_n$)* приведенную систему вычетов по модулю *m*: (-21, - 13, -19, 3, 11, 19, 20), *m*=25.

Вычислим функцию Эйлера от модуля. $25=5^2$. Поэтому

$$\varphi(25) = 25 \cdot \left(1 - \frac{1}{5}\right) = 20.$$

А в данной по условию последовательности чисел только 7 элементов, поэтому она не является приведенной системой вычетов по модулю 25.

Задание 5. Сколько элементов входит в приведенную систему вычетов по модулю *m*: *m*=15.

Из теории известно, что приведенная система вычетов по модулю m содержится $\varphi(m)$ элементов. Вычислим значение функции Эйлера от модуля: $\varphi(15) = 15 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 8$, т.к. 15=3·5.

Следовательно, в приведенной системе вычетов по модулю 15 содержится 8 элементов.

Практические задания по вариантам

Задание 1. Заменить число *a* наименьшим по абсолютной величине, а также наименьшим положительным вычетом по модулю *m*.

Вариант 1. *a* = 185, m = 12; **Вариант 2. a = 84, m = 9;**

Вариант 3. *a* = 180, m = 10; **Вариант 4. a = 82, m = 9;**

Вариант 5. *a* = 85, m = 11; **Вариант 6. a = 84, m = 8;**

Вариант 7. *a* = 103, m = 87; **Вариант 8. a = 84, m = 16;**

Вариант 9. *a* = 15, m = 10; **Вариант 10. a = 81, m = 9.**

Задание 2. Записать полную систему наименьших неотрицательных и наименьших по абсолютной величине вычетов по модулю m.

Вариант 1. m = 12; **Вариант 2. m = 9;**

Вариант 3. m = 10; **Вариант 4. m = 13;**

Вариант 5. m = 22; **Вариант 6. m = 29;**

Вариант 7. m = 20; **Вариант 8. m = 23;**

Вариант 9. m = 11; **Вариант 10. m = 19.**

Задание 3. Проверить, образуют ли числа $(a_1, a_2,\ldots,a_n)$ полную систему вычетов по модулю m:

Вариант 1. (-253, - 138, 170, 393, 965, 2000, 47, 1660), m=8;

Вариант 2. (-181, - 303, 597, 242, 135, 186, -43, 32), m=8;

Вариант 3. (-40, - 45, 31, 26, - 48, - 34), m=6;

Вариант 4. (-23, - 43, -33, 36, 25, 21, 31), m=7;

Вариант 5. (- 18, - 11, -4, 15, 22, 17), m=6;

Вариант 6. (- 15, 11, 12, 18, 19), m=5;

Вариант 7. (- 17, 18, 20, - 9, 10, 23), m=6;

Вариант 8. (- 14, - 13, 16, 10, 18, 20, -16), m=7;

Вариант 9. (- 12, 13, -16, 9, 16, 23), m=6;

Вариант 10. (-21, - 13, -19, 3, 11, 19, 20), m=7.

Задание 4. Проверить, образуют ли числа $(a_1, a_2,\ldots,a_n)$ приведенную систему вычетов по модулю m:

Вариант 1. (- 349, - 193, 231, 401), m=12;

Вариант 2. (-247, - 133, -197, 385), m=13;

Вариант 3. (13, -13, 29, -9, 12, 32), m=10;

Вариант 4. (-4, - 2, -1, 1, 2, 4), m=9;

Вариант 5. (13, - 13, 29, -9, -1, 2,-3, 28, 9, 10), m=11;

Вариант 6. (1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41, -2), m=14;

Вариант 7. (-253, - 138, 170, 393, 965, 2000, 47, 1660), m=8;

Вариант 8. (-15, 27, 104, -117, 15, 29), m=7;

Вариант 9. (11, 13, -13, -1, 2, -2, 9, 19, 23, 101, 21, 25), m=11;

Вариант 10. (-13, -1, 2, -2, 9, 19, 23, 101), m=13.

Задание 5. Сколько элементов входит в приведенную систему вычетов по модулю m:

Вариант 1. m = 95; **Вариант 2. m = 90;**

Вариант 3. m = 70; **Вариант 4. m = 23;**

Вариант 5. m = 12; **Вариант 6. m = 9;**

Вариант 7. m = 10; **Вариант 8. m = 13;**

Вариант 9. m = 22; **Вариант 10. m = 19.**

РАБОТА № 3 (7) Сравнения первой степени и их решение.

Цель: познакомиться со сравнениями с одним неизвестным, изучить способы решения сравнений первой степени.

Вопросы, выносимые на практическое занятие.

1. Сравнения с неизвестным.
2. Сравнения первой степени.
3. Решение сравнений первой степени через системы вычетов.
4. Решение сравнений первой степени методом Эйлера.
5. Решение сравнений первой степени с помощью подходящих дробей.

Краткие теоретические сведения.

Рассмотрим сравнение $a_n \cdot x^n + \cdots + a_1 \cdot x + a_0 \equiv 0(mod\ m)$ содержащее неизвестное. Если a_n не делится на m, то n называется степенью сравнения. Решить сравнение — значит найти все значения x, ему удовлетворяющие. Два сравнения, которым удовлетворяют одни и те же значения x, называются равносильными.

ТЕОРЕМА. Если x является решением данного сравнения, то любой $y \equiv x(mod\ m)$ так же является решением этого сравнения.

Поэтому весь класс вычетов считается одним решением этого сравнения.

ТЕОРЕМА. Сравнение с неизвестным имеет столько решений, сколько чисел из полной системы вычетов ему удовлетворяет.

ТЕОРЕМА. Если $(a, m) = 1$, то сравнение $ax \equiv b\ (mod\ m)$ имеет единственное решение.

ТЕОРЕМА. Если $(a, m) = d$, и b не делится на d, то сравнение

$ax \equiv b\ (mod\ m)$ не имеет решения.

ТЕОРЕМА. Если $(a, b) = d$, и $(d, m) = 1$, то исходное сравнение $ax \equiv b\ (mod\ m)$ равносильно сравнению $\frac{a}{d}x \equiv \frac{b}{d}\ (mod\ m)$.

ТЕОРЕМА. Если $(a, m) = d$, и b делится на d, то сравнение $ax \equiv b\ (mod\ m)$ имеет d различных решений по модулю m, получаемых из решения сравнения $\frac{a}{d}x \equiv \frac{b}{d}\ (mod\ \frac{m}{d})$.

ТЕОРЕМА (Эйлера). Если $m > 1$ и $(a, m) = 1$, то имеет место сравнений $a^{\varphi(m)} \equiv 1\ (mod\ m)$.

ТЕОРЕМА (Ферма). Если $(a, p) = 1$ и p простое число, то имеет место сравнений $a^{p-1} \equiv 1\ (mod\ p)$.

ТЕОРЕМА (Ферма). Если p простое число, то имеет место сравнение $a^p \equiv a\ (mod\ p)$ при любом a.

ТЕОРЕМА. Если $(a, m) = 1$, то для сравнения $ax \equiv b\ (mod\ m)$ решением является $x \equiv a^{\varphi(m)-1}b\ (mod\ m)$.

ТЕОРЕМА. Если $(a, m) = 1$, то для сравнения $ax \equiv b\ (mod\ m)$ решением является $x \equiv (-1)^n P_{n-1}b\ (mod\ m)$, где P_{n-1} числитель предпоследней подходящей дроби для $\frac{m}{a}$. (Заметим, что q_0-это целая часть дроби $\frac{m}{a}$.)

Примеры выполнения заданий.

Задание 1. Решить сравнение $ax \equiv b\ (mod\ m)$ методами подбора и прибавлением в правой части сравнения величины km до получения величины, кратной a: $2x \equiv 3\ (mod\ 7)$.

Решим это сравнение сначала методом подбора.

Выпишем полную систему вычетов по модулю 7: 0, 1, 2, 3, 4, 5, 6. Проверим каждый ее элемент на решение сравнения.

$2 \cdot 0 \equiv 3 (\mathrm{mod}\ 7)$ Неверное сравнение, т.к. 3-0 не делится на 7.

$2 \cdot 1 \equiv 3 (\mathrm{mod}\ 7)$ Неверное сравнение, т.к. 3-2 не делится на 7.

$2 \cdot 2 \equiv 3 (\mathrm{mod}\ 7)$ Неверное сравнение, т.к. 3-4 не делится на 7.

$2 \cdot 3 \equiv 3 (\mathrm{mod}\ 7)$ Неверное сравнение, т.к. 3-6 не делится на 7.

$2 \cdot 4 \equiv 3 (\mathrm{mod}\ 7)$ Неверное сравнение, т.к. 3-8 не делится на 7.

$2 \cdot 5 \equiv 3 (\mathrm{mod}\ 7)$ Верное сравнение, т.к. 3-10 делится на 7.

$2 \cdot 6 \equiv 3 (\mathrm{mod}\ 7)$ Неверное сравнение, т.к. 3-12 не делится на 7.

Таким образом, решением является $x \equiv 5 (\mathrm{mod}\ 7)$.

Теперь решим это сравнение втором способом. К числу 3 будем прибавлять 7. Получаем уже при первом прибавлении 3+7=10=2·5. Отсюда делаем вывод, что решением является $x \equiv 5 (\mathrm{mod}\ 7)$.

Задание 2. Решить сравнение с одним неизвестным методом подбора:

$\boldsymbol{7x^4 + x^2 - 10x \equiv 5 (mod\ 7)}$**.**

Заметим сначала, что $7x^4 \equiv 0\ (mod\ 7)$ и $7x \equiv 0\ (mod\ 7)$ при любом x. Поэтому исходное сравнение можно упростить:

$$x^2 - 3x \equiv 5 (\mathrm{mod}\ 7)$$

Выпишем полную систему вычетов по модулю 7: 0, 1, 2, 3, 4, 5, 6. Проверим каждый ее элемент на решение сравнения.

$0^2 - 3 \cdot 0 \equiv 5 (\mathrm{mod}\ 7)$. Неверное сравнение, т.к. 5-0 не делится на 7.

$1^2 - 3 \cdot 1 \equiv 5 (\mathrm{mod}\ 7)$. Верное сравнение, т.к. 5-(-2) делится на 7.

$2^2 - 3 \cdot 2 \equiv 5 (\mathrm{mod}\ 7)$. Верное сравнение, т.к. 5-(-2) делится на 7.

$3^2 - 3 \cdot 3 \equiv 5 (\mathrm{mod}\ 7)$. Неверное сравнение, т.к. 5-0 не делится на 7.

$4^2 - 3 \cdot 4 \equiv 5 (\mathrm{mod}\ 7)$. Неверное сравнение, т.к. 5-4 не делится на 7.

$5^2 - 3 \cdot 5 \equiv 5 (\mathrm{mod}\ 7)$. Неверное сравнение, т.к. 5-10 не делится на 7.

$6^2 - 3 \cdot 6 \equiv 5 (\mathrm{mod}\ 7)$. Неверное сравнение, т.к. 5-18 не делится на 7.

Таким образом, решениями являются $x \equiv 1 (\mathrm{mod}\ 7)$ и $x \equiv 2 (\mathrm{mod}\ 7)$.

Задание 3. Решить сравнения первой степени с одним неизвестным методом Эйлера. Правильность ответов проверить подстановкой:

$$-\mathbf{10}\boldsymbol{x} \equiv \mathbf{5}(\boldsymbol{mod}\ \mathbf{7}).$$

Преобразуем сначала это сравнение, прибавив к левой части $14x$, которое сравнимо с 0. Получим: $4x \equiv 5(mod\ 7)$. Заметим, что (4,7)=1. Поэтому это сравнение имеет единственное решение, которое можно найти по формуле Эйлера.

$x \equiv a^{\varphi(m)-1}b\ (mod\ m)$. $x \equiv 4^5 \cdot 5\ (mod\ 7)$. $x \equiv 1024 \cdot 5\ (mod\ 7)$. Учитывая, что $1024 \equiv 2(mod\ 7)$, решение можно упростить $x \equiv 2 \cdot 5 \equiv 10\ (mod\ 7)$, т.е. $x \equiv 3\ (mod\ 7)$. Проверим правильность решения: -10·3≡ $5(mod\ 7)$, т.к. 5-(-30)=35 делится на 7.

Ответ: решением является $x \equiv 3\ (mod\ 7)$.

Задание 4. Решить сравнение разложением в цепную дробь отношения $\frac{\boldsymbol{m}}{\boldsymbol{a}}$: $-\mathbf{10}\boldsymbol{x} \equiv \mathbf{5}(\boldsymbol{mod}\ \mathbf{7})$.

Сначала упростим сравнение, прибавив к левой части $14x$, сравнимое с 0. Получим $4x \equiv 5(mod\ 7)$. Найдем числители подходящих дробей для частного $\frac{7}{4}$. Сначала выпишем алгоритм Евклида: 7=4·1+3, 4=3·1+1, 3=1·3. Составим таблицу вычисления числителей подходящих дробей.

q		$q_0 = 1$	$q_1 = 1$	$q_2 = 3$
P_i	1	1	2	7

Таким образом: $n = 2$, $P_{n-1} = P_1 = 2$. Поэтому из формулы

$x \equiv (-1)^n \cdot P_{n-1} \cdot b\ (mod\ m)$ имеем: $x \equiv (-1)^2 \cdot 2 \cdot 5\ (mod\ 7)$. А так как

$10 \equiv 3\ (mod\ 7)$, то получаем решение $x \equiv 3\ (mod\ 7)$. Проверка была проведена ранее.

Практические задания по вариантам.

Задание 1. Решить сравнение $ax \equiv b$ (mod m) методами подбора и прибавлением в правой части сравнения величины km до получения величины, кратной a:

Вариант 1. $2x \equiv 5\ (mod\ 9)$. **Вариант 2.** $4x \equiv 3(mod\ 7)$.

Вариант 3. $3x \equiv 1\ (mod\ 11)$. **Вариант 4.** $10x \equiv 4(mod\ 8)$.

Вариант 5. $7x \equiv 5\ (mod\ 5)$. **Вариант 6.** $12x \equiv 3(mod\ 6)$.

Вариант 7. $9x \equiv 3\ (mod\ 9)$. **Вариант 8.** $9x \equiv 7(mod\ 5)$.

Вариант 9. $2x \equiv 5\ (mod\ 11)$. **Вариант 10.** $4x \equiv 3(mod\ 9)$.

Задание 2. Решить сравнение с одним неизвестным методом подбора:

Вариант 1. $x^4 + x^2 - x \equiv 5\ (mod\ 5)$;

Вариант 2. $4x^5 - 2x^2 + x \equiv 3(mod\ 7)$;

Вариант 3. $3x^3 - 8x^2 + x \equiv 1\ (mod\ 4)$;

Вариант 4. $2x^4 - 10x \equiv 4(mod\ 8)$;

Вариант 5. $7x^2 - 7x \equiv 5\ (mod\ 5)$;

Вариант 6. $6x^{11} + 5x^4 - 12x \equiv 3(mod\ 6)$;

Вариант 7. $9x^5 - 2x^2 + x \equiv 3\ (mod\ 9)$;

Вариант 8. $9x^3 - 2x^2 + x \equiv 2\ (mod\ 5)$;

Вариант 9. $7x^3 - 2x^2 + 7x \equiv 5\ (mod\ 7)$;

Вариант 10. $4x^5 - 2x^2 + x \equiv 3(mod\ 8)$.

Задание 3. Решить сравнения первой степени с одним неизвестным методом Эйлера. Правильность ответов проверить подстановкой:

Вариант 1. $29x \equiv 1(mod\ 17)$; **Вариант 2.** $21x \equiv -5(mod\ 29)$;

Вариант 3. $7x \equiv 15(mod\ 9)$; **Вариант 4.** $7x \equiv 9(mod\ 10)$;

Вариант 5. $12x \equiv 7(mod\ 13)$; **Вариант 6.** $5x \equiv 3(mod\ 17)$;

Вариант 7. $3x \equiv 5(mod\ 11)$; **Вариант 8.** $9x \equiv 2(mod\ 14)$;

Вариант 9. $7x \equiv 11(mod\ 15)$; **Вариант 10.** $3x \equiv 4(mod\ 7)$.

Задание 4. Решить сравнение разложением в цепную дробь отношения $\frac{m}{a}$:

Вариант 1. $15x \equiv 37 (mod\ 98)$; **Вариант 2.** $32x \equiv 182 (mod\ 119)$;

Вариант 3. $105x \equiv 72 (mod\ 147)$; **Вариант 4.** $97x \equiv 53 (mod\ 169)$;

Вариант 5. $-50x \equiv 67 (mod\ 177)$; **Вариант 6.** $69x \equiv 393 (mod\ 201)$;

Вариант 7. $192x \equiv 9 (mod\ 327)$; **Вариант 8.** $365x \equiv 50 (mod\ 395)$;

Вариант 9. $639x \equiv 177 (mod\ 924)$;

Вариант 10. $296x \equiv 1105 (mod\ 2413)$.

РАБОТА №4 (8) Системы сравнений. Первообразные корни и индексы.

Цель: Познакомиться с понятиями систем сравнений первой степени, сравнениями второй и больших степеней, первообразными корнями и индексами. Освоить методы решения систем сравнений первой степени и сравнений второй степени, нахождения первообразных корней, вычисление индексов.

Вопросы, выносимые на практическое занятие.

1. Решение сравнений второй степени.
2. Системы сравнений первой степени.
3. Методы решения систем сравнений первой степени.
4. Первообразные корни и индексы.
5. Нахождение первообразных корней и вычисление индексов.

Краткие теоретические сведения.

Целое число a называется квадратным вычетом по модулю p , если сравнений $x^2 \equiv a\ (mod\ p)$ имеет решение. В противном случае число a называется квадратным невычетом по модулю p .

ТЕОРЕМА. Если $(a, p) = 1$ и a - квадратный вычет по модулю p, то сравнений $x^2 \equiv a\ (mod\ p)$ имеет два решения.

ТЕОРЕМА. Если $(a, p) = 1$ и a - квадратный невычет по модулю p, то сравнений $x^2 \equiv a\ (mod\ p)$ не имеет решений.

ТЕОРЕМА. Приведенная система вычетов по простому модулю p состоит из $\frac{p-1}{2}$ квадратных вычетов, сравнимых по модулю p с числами $1^2, 2^2, \dots, (\frac{p-1}{2})^2$, и $\frac{p-1}{2}$ квадратных невычетов.

Для $(a,p)=1$ определяется символ Лежандра $(\frac{a}{p})$ (символ Лежандра a по p , где a - числитель символа, а p – знаменатель) так, что $\left(\frac{a}{p}\right)=1$, если a - квадратичный вычет по модулю p, и $\left(\frac{a}{p}\right)=-1$, если a - квадратичный невычет по модулю p.

ТЕОРЕМА. (Критерий Эйлера) Если $(a,p)=1$, то $a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\ (mod\ p)$.

Рассмотрим систему сравнений первой степени

$$\begin{cases} a_1\cdot x\equiv b_1(mod\ m_1) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_n\cdot x\equiv b_n(mod\ m_n) \end{cases} \qquad (1)$$

ТЕОРЕМА. Если x_0 решением данной системы, то любое $x\equiv x_0(mod\ K)$, где К=НОК[m_1,…, m_n], является решением этой же системы (1) сравнений первой степени.

Прежде чем решать систему сравнений первой степени (1) необходимо решить каждое сравнение из этой системы. Другими словами, исходную систему необходимо привести к виду (где свободные члены конечно же другие):

$$\begin{cases} x\equiv b_1'(mod\ m_1) \\ \dots\dots\dots\dots\dots\dots \\ x\equiv b_n'(mod\ m_n) \end{cases} \qquad (2)$$

ТЕОРЕМА. Системы (1) и (2) равносильны, т.е. они обладают одним и тем же множеством решений.

Если система не совместна, т.е. не имеет решений, то ее множество решений считается пустым. В дальнейшем для упрощения записи вместо b_i' будем писать b_i.

ТЕОРЕМА. Система (2) имеет решение тогда и только тогда, когда при любых $i \neq j, 1 \leq i, j \leq n$ имеем $b_i \equiv b_j (mod\ D)$, где D=НОД(m_i, m_j).

ТЕОРЕМА. Если все модули попарно взаимно просты, т.е. при любых $i \neq j, 1 \leq i, j \leq n$ имеем НОД(m_i, m_j)=1, и $M = m_1 \cdot \ldots \cdot m_n$, $M_i = \frac{M}{m_i}$, $M_i \cdot M_i' \equiv 1 (mod\ m_i)$, то $x_0 = M_1 \cdot M_1' \cdot b_1 + \cdots + M_n \cdot M_n' \cdot b_n$ является решением системы (2), т.е. то система (2) имеет решения при любых значениях b_i.

Так как в условиях теоремы К=НОК[m_1,…, m_n]= $m_1 \cdot \ldots \cdot m_n$, то множество всех решений системы (2) определяется сравнением

$x \equiv x_0 (mod\ m_1 \cdot \ldots \cdot m_n)$.

Универсальным методом решения системы сравнений первой степени является метод последовательной подстановки. Он заключается в следующем. Из первого сравнения системы (2) находится решение

$x = b_1 + z \cdot m_1$ Его подставляем во второе сравнение.

$$b_1 + z \cdot m_1 \equiv b_2 (mod\ m_2)$$

Затем решаем это сравнение относительно z с некоторой переменной *t*. Полученное решение подставляем в $x = b_1 + z \cdot m_1$, а затем полученное выражение x через t подставляем в третье сравнение. Всегда нужно выражать неизвестные в явном виде. Этот процесс продолжается до последнего сравнения. Если на каком-то шаге решение одного сравнения не находится, то в этом случае вся система не имеет решения. Решение для последнего сравнения даст одно решение x_0. А множество всех решений, как уже отмечалось, будет находится из сравнения $x \equiv x_0 (mod\ K)$, где К=НОК[m_1,…, m_n].

Если $(a,m)=1$, то существуют такие k, что $a^k \equiv 1(mod\, m)$. Например $k=\varphi(m)$. $k_0 = min\{k|\, a^k \equiv 1(mod\, m)\}$ называется показателем, которому принадлежит a по модулю m.

ТЕОРЕМА. Если a по модулю m принадлежит показателю k , то числа $1 = a^0, a^1, \dots, a^{k-1}$ по модулю m несравнимы.

ТЕОРЕМА. Если a по модулю m принадлежит показателю k, то $a^r \equiv a^t(mod\, m)$ тогда и только тогда, когда $r \equiv t(mod\, k)$.

ТЕОРЕМА. Показатели, которым принадлежат числа по модулю, являются делителями числа $\varphi(m)$.

ТЕОРЕМА. Если x по модулю принадлежит показателю $k \cdot t$, то число x^k принадлежит показателю t.

ТЕОРЕМА. Если x по модулю принадлежит показателю k, а y принадлежит показателю t, причем $(k,\ t)$=1, то $x \cdot y$ принадлежит показателю $k \cdot t$.

Числа, принадлежащие показателю $\varphi(m)$ (если они существуют) называются первообразными корнями по модулю m.

ТЕОРЕМА. Если модуль p является простым числом, то существуют первообразные корни.

ТЕОРЕМА. Пусть g первообразный корень по простому модулю p . Существует такое t, что k из равенства $g + p \cdot k = (g + p \cdot t)^{p-1}$ не делится на p, а $g + p \cdot t$ будет являться первообразным корнем по модулю p^α при любом $\alpha > 1$.

ТЕОРЕМА. Пусть $\alpha \geq 1$ и g – первообразный корень по модулю p^{α}.Тогда нечетное из чисел g и $g + p^{\alpha}$ является первообразным корнем по модулю $2 \cdot p^{\alpha}$.

ТЕОРЕМА. Пусть $d_1, \dots, d_k$ – все различные простые делители числа $\varphi(m)$. Число g , взаимно простое с $\varphi(m)$, является первообразным корнем по модулю m тогда и только тогда, когда g не удовлетворяет ни одному из сравнений $g^{\frac{\varphi(m)}{d_1}} \equiv 1(mod\ m), \dots, g^{\frac{\varphi(m)}{d_k}} \equiv 1(mod\ m)$.

Пусть $(\alpha, m) = 1$, g- первообразный корень по модулю m и $\alpha = g^{\delta}(mod\ m)$, где $\delta \geq 0$, то δ называется индексом числа α по модулю m при основании g. $\delta = ind_g a$.

Обозначим через *c* значение функции Эйлера от модуля m. $c = \varphi(m)$.

ТЕОРЕМА. $ind(a \cdot b \cdot \dots \cdot l) \equiv (ind(a) + ind(b) + \dots + ind(l))(mod\ c)$.

ТЕОРЕМА. $ind(a^k) \equiv k \cdot ind(a)(mod\ c)$.

ТЕОРЕМА. Пусть $(n, c) = d$. Тогда в приведенной системе вычетов по модулю m число вычетов степени n равно $\frac{c}{d}$.

ТЕОРЕМА. Пусть $(n, c) = d$, $(a, m) = 1$. Сравнение $x^n \equiv a\ (mod\ m)$ разрешимо тогда и только тогда, когда $ind(a)$ кратен d .

ТЕОРЕМА. Число a есть вычет степени n по модулю m тогда и только тогда, когда $a^{\frac{c}{d}} \equiv 1(mod\ m)$.

ТЕОРЕМА. Число a принадлежит к числу первообразных коней по модулю m тогда и только тогда, когда $(ind\ a, c) = 1$.

Примеры выполнения заданий.

Задание 1. С помощью символа Лежандра определить является ли число *a* квадратным вычетом по модулю *p*. *a*=5, *p*=13.

Воспользуемся критерием Эйлера. $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (mod\ p)$.

$5^{\frac{13-1}{2}} \equiv \left(\frac{5}{13}\right) (mod\ 13)$, т.е. $5^6 \equiv \left(\frac{5}{13}\right) (mod\ 13)$.

Но $5^2 \equiv (-1) (mod\ 13)$, поэтому $\left(\frac{5}{13}\right) = -1$. Следовательно, 5 не является квадратным вычетом по модулю 13.

Задание 2. Найти квадратные вычеты или невычеты по модулю *p* =37.

Согласно теории квадратных вычетов будет $\frac{37-1}{2} = 18$, сравнимых соответственно с числами $1^2, 2^2, \dots, (\frac{37-1}{2})^2$. Будем последовательно их выписывать, выбирая соответствующий наименьший положительный вычет по модулю 37. Получим последовательность квадратных вычетов по модулю 37: 1, 4, 9, 16, 25, 36, 12, 27, 7, 26, 10, 33, 21, 11, 3, 34, 30, 28.

Для того, чтобы выписать квадратные невычеты надо из приведенной системы наименьших положительных вычетов удалить найденные квадратные вычеты. Получим множество квадратных невычетов: 2, 5, 6, 8, 13, 14, 15, 17, 18, 19, 20, 22, 23, 24, 29, 31, 32, 35. Вместе эти две последовательности составляют приведенную систему вычетов по модулю 37.

Задание 3. Решить системы сравнений:

$$\begin{cases} \boldsymbol{3x \equiv 5 (mod\ 7)} \\ \boldsymbol{x \equiv 2 (mod\ 13)} \end{cases}$$

Заметим, что (7, 13)=1. Поэтому 5 и 2 конечно будут сравнимы по этому модулю, т.е. система сравнений будет совместна.

Решим сначала первое сравнение. Так как (3,7)=1, то сравнение имеет единственное решение. Составим таблицу вычисления числителей подходящих дробей дроби $\frac{7}{3}$.

q		$q_0 = 2$	$q_1 = 3$
P_i	1	2	7

Предпоследний числитель подходящей дроби равен 2. Найдем решение сравнения по формуле $x \equiv (-1)^n \cdot P_{n-1} \cdot b\ (mod\ m)$, где n=1.

$x \equiv (-1)^1 \cdot 2 \cdot 5\ (mod\ 7) \equiv -3(mod\ 7) \equiv 4(mod\ 7).$

Таким образом, получаем систему в преобразованном виде.

$$\begin{cases} x \equiv 4(mod\ 7) \\ x \equiv 2(mod\ 13) \end{cases}$$

Запишем решение первого сравнения через прибавление кратного модуля.

$$x = 4 + 7y$$

Подставим этот вид решения во второе сравнение.

$$4 + 7y \equiv 2(mod\ 13)$$

Теперь решим это сравнение относительно y.

$$7y \equiv -2(mod\ 13), 7y \equiv 11(mod\ 13)$$

Заметим, что (7,13)=1, поэтому существует единственное решение. Решим подбором, подставляя последовательно числа из полной системы вычетов

0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12. Подставляя в сравнение установим, что решением является 9: 7·9=63≡ $11(mod\ 13)$. $y \equiv 9(mod\ 13)$. В другой записи $y = 9 + 13 \cdot t$. Подставим это выражение в формулу с x.

$$x = 4 + 7 \cdot y = 4 + 7 \cdot (9 + 13 \cdot t) = 67 + 91 \cdot t$$

Таким образом, имеем решение системы $x \equiv 67(mod\ 91)$. Проверка правильности решения не представляет трудности через простую подстановку числа 67 в каждое из сравнений. Заметим, что $91 = НОК[7, 13]$.

Задание 4. Решить системы сравнений:

$$\begin{cases} \boldsymbol{3x \equiv 5(mod\ 7)} \\ \boldsymbol{x \equiv 2(mod\ 13)} \\ \boldsymbol{14x \equiv 11(mod\ 18)} \end{cases}$$

Как мы знаем систему надо привести к виду, когда слева неизвестное без дополнительного множителя. Как следует из предыдущего примера первое сравнение приводится к виду $x \equiv 4(mod\ 7)$. Второе сравнение уже имеет нужный вид. Рассмотрим третье сравнение. Для него (14, 18)=2. Однако свободный член 11 на 2 не делится. Следовательно, у этого сравнения нет решения. А тогда и вся исходная система будет несовместной.

Задание 5. Проверить разрешимость сравнения второй степени. И в случае наличия решений найти их: $\boldsymbol{x^2 \equiv 6\ (mod\ 11)}$.

Первый способ. $c = \varphi(11) = 10$. (n, c)=(2, 10)=2 =d. $ind_{11}6 = 9$. Число 9 не делится на 2, следовательно сравнение не имеет решений.

Второй способ. Заметим, что (2, 11)=1 . Вычислим символ Лежандра. $6^{\frac{11-1}{2}} = 6^5 = 36 \cdot 36 \cdot 6 \equiv 3 \cdot 3 \cdot 6 \equiv 3 \cdot 18 \equiv 3 \cdot 7 = 21 \equiv -1(mod\ 11)$. Это означает, что 6 не является квадратным вычетом по модулю 11, т.е. сравнение неразрешимо.

Третий способ. Проведем проверку непосредственной подстановкой элементов полной системы вычетов в данное сравнение. Выпишем сначала полную систему вычетов по модулю 11. 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

$0^2 = 0 \equiv 6(mod\ 11)$ – сравнение не верно.

$1^2 = 1 \equiv 6(mod\ 11)$ – сравнение не верно.

$2^2 = 4 \equiv 6(mod\ 11)$ – сравнение не верно.

$3^2 = 9 \equiv 6(mod\ 11)$ – сравнение не верно.

$4^2 = 16 \equiv 6(mod\ 11)$ – сравнение не верно.

$5^2 = 25 \equiv 6(mod\ 11)$ – сравнение не верно.

$6^2 = 36 \equiv 6(mod\ 11)$ – сравнение не верно.

$7^2 = 49 \equiv 6(mod\ 11)$ – сравнение не верно.

$8^2 = 64 \equiv 6(mod\ 11)$ – сравнение не верно.

$9^2 = 81 \equiv 6(mod\ 11)$ – сравнение не верно.

$10^2 = 100 \equiv 6(mod\ 11)$ – сравнение не верно.

Таким образом, исходное сравнение не имеет решений.

Задание 6. Найти первообразные корни по простому модулю *p*. *p*=37.

Найдем каноническое разложение числа $\varphi(p) = \varphi(37) = 36 = 2^2 \cdot 3^2$.

Смотрим такие g, что $\big(g, \varphi(p)\big) = 1$. И для каждого из них проверим выполнимость сравнений $g^{\frac{36}{2}} \equiv 1(mod\ 37)$ и $g^{\frac{36}{3}} \equiv 1(mod\ 37)$. Как следует из теоремы, если хотя бы одно сравнение будет выполняться, то число g не будет являться первообразным корнем. В качестве g надо рассматривать числа, не превосходящие $\varphi(37) = 36$ и взаимно простые с ним.

$g = 1.\ 1^{\frac{36}{2}} = 1^{18} \equiv 1(mod\ 37)$ сравнение верное, т.е. 1 первообразным корнем не является.

$g = 5.\ 5^{\frac{36}{2}} = 5^{18} = (5^2)^9 = 25^9 \equiv (-2)^9 = \ (-2)^4 \cdot (-2)^4 \cdot (-2) =$

$= 16 \cdot 16 \cdot (-2) = 16 \cdot (-32) \equiv 16 \cdot 5 = 80 \equiv 6(mod\ 37)$, что не сравнимо с 1.

Проведем проверку второго условия. $5^{\frac{36}{3}} = 5^{12} = (5^2)^6 = 25^6 \equiv (-2)^6 =$

$= 64 \equiv 27(mod\ 37)$, что не сравнимо с 1. Поэтому число 5 является первообразным корнем по модулю 37.

$g = 7.\ 7^{\frac{36}{2}} = 7^{18} = (7^2)^9 = 49^9 \equiv 12^9 = 12^{2^4} \cdot 12 \equiv (-4)^4 \equiv 256 \cdot 12 \equiv$

$\equiv (-3) \cdot 12 = -36 \equiv 1\ (mod\ 37)$. Поэтому число 7 не является первообразным корнем по модулю 37.

$g = 11.\ 11^{\frac{36}{2}} = 11^{18} = (11^2)^9 = 10^9 \equiv 10^{2^4} \cdot 10 \equiv (-11)^4 \cdot 10 =$

$$= (-121)^2 \cdot 10 \equiv (-10)^2 \cdot 10 \equiv (-11) \cdot 10 = -110 \equiv 1(mod\ 37)$$

Следовательно, число 11 не является первообразным корнем для модуля 37.

$g = 13.\ 13^{\frac{36}{2}} = 13^{18} = (13^2)^9 \equiv (-16)^9 = (-16)^{2^4} \cdot (-16) =$

$= (256)^4 \cdot (-16) \equiv (-3)^4 \cdot (-16) = 81 \cdot (-16) = -1296 \equiv -1(mod\ 37)$, что не сравнимо с 1. Проведем проверку второго условия. $13^{\frac{36}{3}} = 13^{12} = (13^2)^6 \equiv (-16)^6 = (-16)^{2^3} = (-256)^3 \equiv (-3)^3 = -27 \equiv 10(mod\ 37)$, что так же не сравнимо с 1. Поэтому, число 13 является первообразным корнем по модулю 37.

$g = 17.\ 17^{\frac{36}{2}} = 17^{18} = (17^2)^9 = (289)^9 \equiv (-7)^9 = (-7)^{2^4} \cdot (-7) =$

$= (49)^4 \cdot (-7) \equiv (12)^4 \cdot (-7) \equiv (-4)^2 \cdot (-7) = 16 \cdot (-7) = -126 \equiv$

$\equiv -15(mod\ 37)$, что не сравнимо с 1. Проведем проверку второго условия. $17^{\frac{36}{3}} = 17^{12} = (17^2)^6 = (289)^6 \equiv\equiv (-7)^6 = (-7)^{2^3} = (49)^3 \equiv (12)^3 = 144 \cdot 12 \equiv (-4) \cdot 12 \equiv -11(mod\ 37)$, что так же не сравнимо с 1. Поэтому число 17 является первообразным корнем по модулю 37.

$g = 19.\ 19^{\frac{36}{2}} = 19^{18} = (19^2)^9 = (361)^9 = (-9)^9 = (-9)^{2^4} \cdot (-9) =$

$=(81)^4 \cdot (-9) \equiv (7)^4 \cdot (-9) = (49)^2 \cdot (-9) \equiv 12 \cdot (-9) = -108 \equiv$

$3(mod\ 37)$, что не сравнимо с 1. Проведем проверку второго условия. $19^{\frac{36}{3}} = 19^{12} = (19^2)^6 = (361)^6 \equiv\equiv (-9)^6 = (-9)^{2^3} = (81)^3 \equiv (7)^3 = 49 \cdot 7 \equiv 12 \cdot 7 = 94 \equiv 20(mod\ 37)$, что так же не сравнимо с 1. Поэтому число 19 является первообразным корнем по модулю 37.

$g = 23.\ 23^{\frac{36}{2}} = 23^{18} = (23^2)^9 = (529)^9 = (18)^9 = (18)^{2^4} \cdot (18) =$

$= (324)^4 \cdot (18) \equiv (-9)^4 \cdot 18=(-9)^{2^2} \cdot (18) = (81)^2 \cdot 18 \equiv 7 \cdot 18 = 126 \equiv$

$\equiv 15(mod\ 37)$, что не сравнимо с 1. Проведем проверку второго условия. $23^{\frac{36}{3}} = 23^{12} = (23^2)^6 = (529)^6 \equiv\equiv (11)^6 = (11)^{2^3} = (121)^3 \equiv (10)^3 = 1000 \equiv 1(mod\ 37)$, т.е. второе сравнение выполняется, поэтому 23 не является первообразным корнем по модулю 37.

$g = 25.\ 25^{\frac{36}{2}} = 25^{18} = (25^2)^9 = (625)^9 \equiv (-4)^8 \cdot (-4) = 256 \cdot (-4) \equiv$

$\equiv 24 \cdot (-4) \equiv 15(mod\ 37)$, что не сравнимо с 1. Проведем проверку второго условия. $25^{\frac{36}{3}} = 25^{12} = (25^2)^6 = (625)^6 \equiv\equiv (-4)^6 = 256 \equiv -3(mod\ 37)$, что так же не сравнимо с 1. Поэтому число 25 является первообразным корнем по модулю 37.

$g = 29.\ 29^{\frac{36}{2}} = 29^{18} = (29^2)^9 = (841)^9 \equiv (-10)^8 \cdot (-10) =$

$= 10^3 \cdot 10^3 \cdot (-10) \equiv -10(mod\ 37)$, что не сравнимо с 1. Проведем проверку второго условия. $29^{\frac{36}{3}} = 29^{12} = (29^2)^6 = (841)^6 \equiv\equiv (-10)^6 \equiv 1(mod\ 37)$, т.е. второе сравнение выполняется, поэтому 29 не является первообразным корнем по модулю 37.

$g = 31.\ 31^{\frac{36}{2}} = 31^{18} = (31^2)^9 = (961)^9 \equiv (-1)^9 \equiv -1(mod\ 37)$, т.е. первое сравнение не выполняется. Проведем проверку второго условия. $31^{\frac{36}{3}} = 31^{12} = (31^2)^6 = (961)^6 \equiv\equiv (-1)^6 \equiv 1(mod\ 37)$, т.е. второе сравнение выполняется, поэтому 31 не является первообразным корнем по модулю 37.

$g = 35.\ 35^{\frac{36}{2}} = 35^{18} = (35^2)^9 = (1225)^9 \equiv (4)^9 = (4^4)^2 \cdot 4 = (256)^2 \cdot 4 \equiv$

$\equiv (-3)^2 \cdot 4 \equiv -1(mod\ 37)$, что так же не сравнимо с 1. Проведем проверку второго условия. $35^{\frac{36}{3}} = 35^{12} = (35^2)^6 = (1225)^6 \equiv (0)^6 \equiv 0(mod\ 37)$, что так же не сравнимо с 1. Поэтому число 35 является первообразным корнем по модулю 37.

Таким образом, первообразными корнями по модулю 37 являются числа 5, 13, 17, 19, 25 и 35.

Задание 7. Пользуясь таблицами индексов найти индекс числа и число по индексу для модуля *p*. *p=7, N=5, i=2.*

N	1	2	3	4	5	6
i	0	2	1	4	5	3

Из таблицы легко видеть, что для числа 5 индексом является тоже 5. А для индекса 2 соответствующим числом является так же 2.

Практические задания по вариантам.

Задание 1. С помощью символа Лежандра определить является ли число *a* квадратным вычетом по модулю *p*.

Вариант	*a*	*p*		Вариант	*a*	*p*
1	2	7		2	5	11
3	13	5		4	8	13
5	6	11		6	15	7
7	11	5		8	12	7
9	6	13		10	13	11

Задание 2. Найти квадратные вычеты или невычеты по модулю *p*.

Вычеты			Невычеты	
Вариант	*p*		Вариант	*p*
1	11		2	7
3	17		4	23
5	29		6	3
7	5		8	13
9	31		10	19

Задание 3. Решить системы сравнений:

Вариант 1. $x \equiv 19(mod\ 24);\ x \equiv 10(mod\ 21);$

Вариант 2. $x \equiv 23(mod\ 35); x \equiv 13(mod\ 20);$

Вариант 3. $x \equiv 12(mod\ 15);\ x \equiv 3(mod\ 33);$

Вариант 4. $x \equiv 32(mod\ 40); x \equiv 23(mod\ 72).$

Вариант 5. $3x \equiv 5(mod\ 7),\ 2x \equiv 1(mod\ 5);$

Вариант 6. $3x \equiv 1(mod\ 20), 2x \equiv 3(mod\ 15);$

Вариант 7. $3x \equiv 1(mod\ 5),\ 5x \equiv 4(mod\ 7);$

Вариант 8. $14x \equiv 12(mod\ 18), x \equiv 5(mod\ 25);$

Вариант 9. $x \equiv 3(mod\ 11),\ x \equiv 5(mod\ 7);$

Вариант 10. $x \equiv 6(mod\ 7), x \equiv 2(mod\ 13).$

Задание 4. Решить системы сравнений:

Вариант 1. $x \equiv 6(mod\ 15); x \equiv 18(mod\ 21);\ x \equiv 3(mod\ 12);$

Вариант 2. $x \equiv 13(mod\ 14); x \equiv 6(mod\ 35);\ x \equiv 26(mod\ 45);$

Вариант 3. $x \equiv 19(mod\ 56); x \equiv 3(mod\ 24);\ x \equiv 7(mod\ 20);$

Вариант 4. $x \equiv 19(mod\ 22); x \equiv 8(mod\ 33);\ x \equiv 14(mod\ 21).$

Вариант 5. $x \equiv 3(mod\ 8),\ x \equiv 11(mod\ 20),\ x \equiv 1(mod\ 15);$

Вариант 6. $x \equiv 2(mod\ 3),\ x \equiv 3(mod\ 4),\ x \equiv 4(mod\ 5);$

Вариант 7. $x \equiv 1(mod\ 2),\ x \equiv 3(mod\ 5),\ x \equiv 6(mod\ 9);$

Вариант 8. $x \equiv 2(mod\ 7),\ x \equiv 5(mod\ 9),\ x \equiv 11(mod\ 15);$

Вариант 9. $x \equiv 4(mod\ 7),\ x \equiv 9(mod\ 13),\ x \equiv 1(mod\ 17);$

Вариант 10. $x \equiv 5(mod\ 12),\ x \equiv 2(mod\ 8),\ x \equiv 2(mod\ 11).$

Задание 5. Проверить разрешимость сравнения второй степени. И в случае наличия решений найти их:

Вариант 1. $x^2 \equiv 6(mod\ 13);$ **Вариант 2.** $x^2 \equiv 3(mod\ 11);$

Вариант 3. $x^2 \equiv 6(mod\ 17);$ **Вариант 4.** $x^2 \equiv 5(mod\ 7);$

Вариант 5. $x^2 \equiv 3 (mod\ 5)$; **Вариант 6.** $x^2 \equiv 6 (mod\ 19)$;

Вариант 7. $x^2 \equiv 7 (mod\ 13)$; **Вариант 8.** $x^2 \equiv 9 (mod\ 17)$;

Вариант 9. $x^2 \equiv 15 (mod\ 11)$; **Вариант 10.** $x^2 \equiv 11 (mod\ 3)$.

Задание 6. Найти первообразные корни по простому модулю *p*.

Вариант	*p*		Вариант	*p*
1	11		2	13
3	7		4	29
5	17		6	19
7	3		8	23
9	31		10	5

Задание 7. Пользуясь таблицами индексов найти индекс числа и число по индексу для модуля *p*.

Вариант	Модуль *p*	Число	Индекс
1	5	4	3
2	13	12	12
3	11	7	7
4	17	6	6
5	13	8	8
6	7	6	6
7	11	3	8
8	5	3	4
9	7	4	3
10	3	2	2

Список литературы

1. Веселова, Л. В. Алгебра и теория чисел: Учебное пособие / Л. В. Веселова, О. Е. Тихонов. – Казань: Казанский национальный исследовательский технологический университет, 2014. – 107 с. – ISBN 978-5-7882-1636-2.
2. Ларин, С. В. Алгебра и теория чисел. Группы, кольца и поля: Учебное пособие / С. В. Ларин. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2020. – 1 с. – (Высшее образование). – ISBN 978-5-534-05567-2.
3. Швед, Е. А. Практикум по алгебре: элементы теории чисел / Е. А. Швед, В. А. Федоров. – Омск: Омский государственный университет путей сообщения, 2022. – 39 с.
4. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел: учебное пособие / Л. Б. Шнеперман; Л. Б. Шнеперман. – 3-е изд., стер.. – Санкт-Петербург [и др.] : Лань, 2008. – (Учебники для вузов. Специальная литература). – ISBN 978-5-8114-0885-6.
5. Виноградов, И.М. Основы теории чисел [Текст]: учебное пособие / И. М. Виноградов. - Изд. 12-е, стер. - СПб. [и др.]: Лань, 2009. - 176 с.
6. Виноградов, И. М. Элементы высшей математики: аналитическая геометрия, дифференциальное исчисление: учебник для студентов высших учебных заведений, обучающихся по инженерно-техническим специальностям / И. М. Виноградов; И. М. Виноградов. – Москва : Дрофа, 2010. – 319 с. – (Высшее образование. Современный учебник). – ISBN 978-5-358-06101-9.
7. Гончаренко, В. М. Элементы высшей математики / В. М. Гончаренко, Л. В. Липагина, А. А. Рылов. – МОСКВА: Компания КноРус, 2019. – 364 с. – ISBN 978-5-406-06878-6.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждения
высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__11__»__04__2023 г.

Элементы общей алгебры

Методические рекомендации

для выполнения практических заданий по дисциплинам

«Элементы алгебры и теории чисел» и «Алгебра и теория чисел»

Направления подготовки: 10.03.01 «Информационная безопасность»;
02.03.03 «Математическое обеспечение и администрирование информационных систем».

Курск – 2023

УДК 511+512(075.8)
Составители:
д. ф-м. н., профессор В.П. Добрица
к.т.н. Е.А. Кулешова
к.т.н., доцент Ю.А. Халин

Рецензент

Кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Элементы общей алгебры: методические рекомендации для выполнения практических заданий / Юго-Зап. гос. ун-т; сост.: В.П. Добрица, Е.А. Кулешова, Ю.А. Халин. – Курск, 2023. – 24 с. – Библиогр.: с. 24.

В методических указания описываются основны алгебры и теории чисел. Изложены краткие теоретические сведения, приведены примеры решения задач, а также задачи для самостоятельного решения.

Методические рекомендации предназначены для студентов, обучающихся по направлениям подготовки 10.03.01 «Информационная безопасность» и 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. 231
Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

В данных методических рекомендациях изложены материалы по разделу «Группы, кольца, поля» курсов «Элементы алгебры и теории чисел», «Алгебра и теория чисел».

Рассмотрены следующие темы: Бинарные операции и их свойства. Полугруппы, моноиды, группы, подгруппы и их свойства. Полукольца, кольца, подкольца, идеалы кольца и их свойства. Поля, подполя, простые подполя и их свойства. Расширения полей. Гомоморфизм и изоморфизм алгебраических структур.

По теме представлены:

1) краткие теоретические положения;
2) перечень вопросов, выносимых на практическое занятие;
3) примеры решения типовых задач, выносимых на практическое занятие;
4) задачи, выносимые на самостоятельную работу студентов.

Данные методические рекомендации предназначены для проведения практических занятий по дисциплинам «Элементы алгебры и теории чисел» и «Алгебра и теория чисел» для студентов Юго-Западного государственного университета направлений подготовки: информационная безопасность, математическое обеспечение и администрирование информационных систем.

По изложенным в данных методических рекомендациях материалам можно рекомендовать преподавателю проведение 4-х часов практических занятий по следующему плану:

- Алгебраические структуры (Группы, кольца, поля).(4 часа)

При выполнении практических заданий в каждой задаче выберете задание из своего варианта. Вариант определяется по последней цифре номера зачетной книжки. Отчет по работе должен содержать решения задач и выводы с полным их обоснованием. Отчет по работе оформить на листах формата А4 в редакторе WORD. На титульном листе должно быть указано: университет, факультет, кафедра, предмет, номер практического занятия, вариант, группа, исполнитель, проверяющий.

РАБОТА № 1 (9) Алгебраические структуры

Цель: изучить основные алгебраические структуры (группы, кольца, поля).

Вопросы, выносимые на практическое занятие.

1. Бинарные операции и их свойства.
2. Аксиомы полугруппы, моноида, группы. Подгруппы. Основные свойства.
3. Аксиомы полукольца, кольца. Подкольца. Идеалы. Основные свойства.
4. Аксиомы теории полей. Подполя. Простое подполе. Замкнутые поля. Основные свойства.
5. Гомоморфизм и изоморфизм алгебраических структур.

Краткие теоретические сведения.

Отображение $f: M \to M$ называется бинарной операцией на множестве M. Вместо записи $f(x, y) = z$ принято писать $xfy = z$. В дальнейшем бинарную операцию будем обозначать одним из символов $*, \cdot, +$ или чем-то подобным.

Множество M, рассматриваемое совместно с заданными на нем операциями $< M, f_1, \dots, f_k >$ называется алгеброй (алгебраической структурой).

Бинарная операция называется коммутативной, если $x * y = y * x$ при любых x и y.

Если при любых значениях переменных выполняется равенство $(x * y) * z = = x * (y * z)$, то операция называется ассоциативной.

Алгебра <A, *> с одной бинарной операцией называется группоидом.

Алгебра с одной ассоциативной бинарной операцией $< A, * >$ называется полугруппой, т.е. это группоид с ассоциативной операцией.

Элемент $e \in A$ называется нейтральным (единичным) относительно бинарной операции $*$ если при любом $x \in A$ выполняются равенства

$x * e = e * x = x.$

Алгебра с одной бинарной операцией и с единичным элементом $< M, *, e >$ называется моноидом.

ТЕОРЕМА. Единичный элемент в моноиде единственный.

Если в моноиде $< M,*,e >$ для элемента $x \in M$ существует такой элемент $y \in M$, что выполняются равенства $x * y = y * x = e$, то элемент y называется обратным (противоположным) к x. Он обычно обозначается как x^{-1} $(-x)$.

ТЕОРЕМА. Для каждого элемента $x \in M$ моноида $< M,*,e >$ если существует обратный элемент, то он единственный.

Гомоморфизмом алгебры <*A*, { f_i }> в однотипную ей алгебру <*B*, {g_i}> называется отображение φ*:* *A*—>*B* такое, что при каждом i выполняется условие гомоморфности:

$\forall a_1, ..., a_n \in A, \varphi(f_i(a_1, ..., a_n))=g_i(\varphi(a_1), , \varphi(a_n))$

Говорят также, что отображение φ сохраняет все операции, заданные на множестве *A*.

Алгебры *A* и *B* называются гомоморфными алгебрами, если существует гомоморфизм φ алгебры *A* в алгебру *B*.

Гомоморфизм φ*:* *A*—>*B* алгебры *A* в алгебру*B* называется:

а) мономорфизмом (или вложением *A* в *B*), если отображение φ - инъективно;

б) эпиморфизмом (наложением *A* на *B*), если отображение φ – сюръективно;

в) изоморфизмом, если отображение φ - биективно.

Если алгебра *A* изоморфна алгебре *B,* то пишут *A*≅*B.*

Гомоморфизм φ*:A*—>*A* на себя называется:

а) эндоморфизмом, если отображение φ - инъективно;

б) автоморфизмом, если отображение φ - биективно.

Группой <*G*,*> называется моноид, в котором каждый элемент обратим. Другими словами <*G*,*> группа, если бинарная операция удовлетворяет условиям, называемыми также аксиомами группы:

A_1: $\forall$ *a, b, c*∈ *G, (a*b)*c = a*(b*c)* (ассоциативность);

A_2: $\exists$ *e*∈ *G* $\forall$ *a* ∈ *G, e*a=a*e=a* (существование нейтрального элемента);

A_3: $\forall$ $a \in G$, $\exists$ $a' \in G$ | *a*a′=a′*a=e* (обратимость, или симметризуемость каждого элемента).

Группа $<G,*>$ называется коммутативной (или абелевой), если операция * коммутативна,то есть выполняется аксиома:

A_4: $\forall\, a, b \in G, a*b=b*a$ (коммутативность).

Группу можно определить и по другому: Алгебра $<G, *>$ с бинарной операцией *называется группой, если выполняются следующие условия:

а) $\forall\, a, b, c \in G, (a*b)*c = a*(b*c)$

б) $\forall\, a, b \in G$ каждое из уравнений $a*x=b$ *и* $y*a=b$ имеет хотя бы одно решение.

Алгебра $<K, +, \cdot>$ называется кольцом, если бинарные операции $+, \cdot$ удовлетворяют условиям (аксиомам):

1-4) $<K, +>$ - коммутативная группа;

5)$\forall\, a,b,c \in K\ \ a(b+c)=ab+ac\ (b+c)a=ba+ca.$

Из этого определения следует, что любое кольцо – это аддитивная абелева группа, в которой операция умножения связана с операцией сложения дистрибутивными законами. На операцию умножения, в общем случае, никаких ограничений не накладывается. Однако, если операция умножения обладает свойствами коммутативности, ассоциативности и нейтральным элементом, то кольцо $<K, +, \cdot>$ называют ассоциативно-коммутативным кольцом с единицей. Если же вместо абелевой группы взят коммутативный моноид, то эта алгебра называется полукольцом.

Подмножество $I \subseteq K$ основного множества кольца $<K, +, \cdot>$ называется идеалом, если оно замкнуто относительно сложения элементов и взхятия противоположного элемента, а так же если любой элемент $a \in I$, умноженный на любой элемент кольца $b \in K$, снова лежит в множестве I: $b \cdot a \in I$.

ТЕОРЕМА. Идеал кольца является его подкольцом.

Кольцо $<K, +, \cdot>$ называется кольцом без делителей нуля, если $\forall\, a, b \in K\ ab=0$ следует, что либо $a=0$ либо $b=0$. Такие кольца называют областями целостности.

Если же $a \cdot b=0$ и при этом $a \neq 0$ и $b \neq 0$, то эти элементы называются

делителями нуля.

Алгебра $<P, +, \cdot>$ называется полем, если бинарные операции сложения и умножения удовлетворяют условиям:

1-4) $<P, + >$ - абелева группа;

5-8) $<P\backslash\{0\}, \cdot>$ - абелева группа,

9) $\forall\, a, b, c \in K \quad a \cdot (b+c)=ab+ac$ и $(b+c) \cdot a=ba+ca.$

Другими словами полем является ассоциативно - коммутативным кольцом с единицей, без делителей нуля, с делением на ненулевые элементы.

Подмножество $H \subseteq A$ алгебры $<A, \{ f_i \}>$ называется замкнутым, если результат любой операции над элементами из H является элементом этого же множества H.

ТЕОРЕМА. Замкнутое подмножество группы является группой относительно той же самой операции, которая называется подгруппой.

$$< H,*> \leq < A,*>$$

ТЕОРЕМА. Замкнутое подмножество кольца является кольцом относительно тех же самых операций, которое называется подкольцом исходного кольца.

$$<H, +, \cdot> \leq <K, +, \cdot>$$

ТЕОРЕМА. Замкнутое подмножество поля является полем относительно тех же самых операций, которое называется подполем исходного поля.

$$<H, +, \cdot> \leq <P, +, \cdot>$$

Причем поле $<P, +, \cdot>$ называется расширением поля $<H, +, \cdot>$.

Поле, не имеющее собственных подполей, называется простым.

ТЕОРЕМА. Пересечение подполей является подполем.

ТЕОРЕМА. В каждом поле $<P, +, \cdot>$ содержится одно и только одно простое подполе $<P_0, +, \cdot>$.

ТЕОРЕМА. Если $<K, +, \cdot>$ - произвольное кольцо, то

а) $\forall\, a \in K, \ -(-a)=a;$

б) $\forall\, a, b \in K$ $b\text{-}a=b+(-a);$

в) $\forall\, a, b \in K$ $-(a+b)=(-a)+(-b);$

г) $\forall\, a \in K$ $a\text{-}a=0;$

д) $\forall\, a, b \in K$ $a(b\text{-}c)=ab\text{-}ac;$

е) $\forall\, a \in K$ $0\cdot a=0;$

ж) $\forall\, a, b \in K$ $(-a)\cdot b=-ab.$

ТЕОРЕМА. Если $<P, +, \cdot>$ поле, то

а) $\forall\, a \in P$ $-a=(-1)\cdot a$;

б) $\forall a, b \in P$ $\frac{a}{b} = a \cdot b^{-1}$;

в) $\forall a, b \in P$ $(a \cdot \mathrm{b})^{-1} = a^{-1} \cdot b^{-1} = b^{-1} \cdot a^{-1}$.

Примеры выполнения заданий

Задание 1. Какими свойствами из ниже указанных обладает операция, заданная таблицей на конечном множестве (коммутативность, ассоциативность, обладает нейтральным элементом, обратимостью.)

	a	b	c
a	a	c	c
b	c	a	b
c	c	b	a

Рассмотрим сначала произведение $(ab)c = cc=a$, с другой стороны $a(bc)=ab=c$. Таким образом $(ab)c \neq a(bc)$, т.е. ассоциативности нет.

Для коммутативности должно выполняться равенство $xy = yx$ при любых значениях x и y из данного множества $\{a, b, c\}$. А это, очевидно, равносильно симметричности таблицы задания операции относительно главной диагонали. Легко заметить, что это так. Значит, эта операция коммутативна.

Как известно нейтральный элемент должен удовлетворять равенству $xe = ex = x$ при любом x. Заметим, что $(ab) = c$, т.е. ни a , ни b не могут быть

нейтральными элементами. Из таблицы видно, что $cc=a$, а не c. Таким образом, и элемент c не является нейтральным.

Говорить об обратном элементе можно только при наличии нейтрального элемента. А так как его нет, то обратимости операции нет.

Задание 2. На каких из множеств: *N* (множество натуральных чисел), *Z* (множество целых чисел), *2Z* (множество четных целых чисел), *2Z+1* (множество нечетных целых чисел), *Q* (множество рациональных чисел), *R* (множество действительных чисел), R^+ (множество действительных положительных чисел) задана бинарная алгебраическая операция *.

Заметим, если $a \in N, b \in N$, то и $a + 2b \in N$, т.е. формула $a * b = a + 2b$ определяет операцию на множестве N.

Аналогично устанавливается, что выражение $a * b = a + 2b$ определяет операцию на множествах *Z, Q, R.* А так как сумма и произведение положительных действительных чисел остается положительным действительным числом, то и на множестве R^+ формула $a * b = a + 2b$ определяет операцию.

Теперь рассмотрим множество четных целых чисел ***2Z.*** Очевидно, что при четных a и b выражение $a + 2b$ так же является четным, т.е. эта формула определяет операцию на множестве $2Z$ четных целых чисел.

При нечетных a и b выражение $a * b = a + 2b$ так же является нечетным числом как сумма нечетного и четного числа. Значит, на множестве $2Z+1$ эта формула определяет операцию.

Задание 3. Является ли операция * из задания 2 на тех же множествах, на которых она задана, а) коммутативной, б) ассоциативной, в) обладающей нейтральным элементом, г) обратимой?

Заметим, что $(a * b) * c = a * b + 2c = (a + 2b) + 2c = a + 2b + 2c.$ С другой стороны $a * (b * c) = a * (b + 2c) = a + 2(b + 2c) = a + 2b + 4c$. Поэтому

$(a * b) * c \neq a * (b * c)$, т.е. операция не ассоциативна сразу на всех рассматриваемых множествах.

Аналогично нет и коммутативности так же на всех указанных множествах. $a * b = a + 2b \neq b + 2a = b * a$.

С одной стороны $a * 0 = a$, но с другой стороны в силу отсутствия коммутативности имеем $0 * b = 2b$. Т.е. 0 нейтральным элементом по этой операции быть не может. А отличные от 0 элементы тем более не могут выполнять его роль, что легко заметить по тому же свойству отсутствия коммутативности.

А раз нет нейтрального элемента, то и обратимости этой операции нет.

Задание 4. Какой алгеброй является данное множество с одной бинарной операцией? (Полугруппа, моноид, группа, абелева группа.) $< \boldsymbol{Z^+}, + >$**.**

Сумма положительных целых чисел, очевидно, является положительным и целым, т.е. + является операцией на $\boldsymbol{Z^+}$**.** Известно из школьного курса, что сумма чисел является ассоциативной и коммутативной операцией. Заметим, что $0 \notin \boldsymbol{Z^+}$. Следовательно, это коммутативная полугруппа.

Задание 5. Какой алгеброй из указанных видов может являться данное множество с двумя бинарными операциями? (Полукольцо, кольцо, поле.) $< \boldsymbol{Z^+ \cup \{0\}}, +, \times >$**.**

Если учесть решение предыдущей задачи и что это множество содержит нейтральный элемент 0, то алгебра $< Z^+ \cup \{0\}, + >$ является коммутативным моноидом. Умножение на множестве неотрицательных целых чисел является ассоциативным и коммутативным, причем умножение на 0 всегда дает 0 и оно дистрибутивно относительно сложения. Следовательно, эта алгебра является коммутативным полукольцом. Так как в этом множестве нет противоположных для элементов, отличных от 0, то ни кольцом, ни полем оно являться не может.

Задание 6. Образует ли указанное множество *M* относительно указанной операции какую либо алгебраическую структуру и какую, если образует?

Множество $M = \{x \mid x = 2a + \sqrt{2}b,\ a,b \in Q\}$ относительно операции сложения.

Смотрим сумму двух элементов из множества *M*.

$$(2a + \sqrt{2} \cdot c) + (2b + \sqrt{2} \cdot d) = 2(a + b) + \sqrt{2} \cdot (c + d) =$$

$$= (2b + \sqrt{2} \cdot d) + (2a + \sqrt{2} \cdot c)$$

Так как из $a, b, c, d \in Q$ следует, что $(a + b), (c + d) \in Q$, то сложение на множестве *M* будет являться коммутативной операцией. Проверим выполнение аксиомы ассоциативности. $\big((2a + \sqrt{2} \cdot c) + (2b + \sqrt{2} \cdot d)\big) + (2l + \sqrt{2} \cdot m) = \big(2(a + b) +$

$+\sqrt{2} \cdot (c + d)\big) + (2l + \sqrt{2} \cdot m) = 2(a + b + l) + \sqrt{2} \cdot (c + d + m) = (2a + \sqrt{2} \cdot c) +$

$+(b + l) + \sqrt{2} \cdot (d + m) = (2a + \sqrt{2} \cdot c) + ((2b + \sqrt{2} \cdot d) + (2l + \sqrt{2} \cdot m))$

В качестве нейтрального элемента, очевидно, надо взять простой 0, но представив его в том же виде $0 = 20 + \sqrt{2} \cdot 0$. Легко понять, что к элементу $2a + \sqrt{2} \cdot c$ противоположным будет являться следующий элемент $2(-a) + \sqrt{2} \cdot (-c)$.

Таким образом, множество *M* со сложением + образует абелевую группу $<$ M, $+>$.

Задание 7. Какую алгебраическую структуру образует указанное множество *M* относительно указанной операции? $M = \{1, 2, 4, 8\}$ относительно операции нахождения минимума элементов множества *M*.

Для любых двух элементов $a, b \in M$ всегда существует минимум этих элементов, причем $\min(a, b) = \min(b, a)$, поэтому это коммутативная операция $a * b = \min(a, b)$ на множестве ***M***. Ассоциативность этой операции так же легко понять: $(a * b) * c = \min(\ \min(a, b)\ , c) = \min(\mathrm{a}, \mathrm{b}, \mathrm{c}) = \min(\mathrm{a}, \min(\mathrm{b}, \mathrm{c})) =$

$= a * (b * c)$.

Как мы знаем, нейтральный элемент $e \in M$ должен удовлетворять свойству $e * a = a = a * e$ для любого элемента $a \in M$. Рассмотрим в качестве этого элемента $e = 8$. Из определения min имеем: $\min(8, 1) = 1,\ \min(8, 2) = 2,\ \min(8, 4) = 4,\ \min(8, 8) = 8$, т.е. 8 действительно является нейтральным элементов для определенной нами операции $*$ на множестве ***M***. А вот противоположного элемента определить не возможно. Поэтому алгебра $<$ M,$*>$ является коммутативным моноидом.

Задание 8. Выяснить, образует ли множество *M* относительно операций сложения и умножения кольцо или поле. *M* – множество матриц вида $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$, где $x, y \in R$.

Как известно из курса высшей математики сложение матриц является ассоциативной и коммутативной операцией. В качестве нейтрального элементе по сложению выступает нулевая матрица $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Противоположным элементом к матрице $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$ является матрица $\begin{pmatrix} -x & -y \\ -y & -x \end{pmatrix}$.

Рассмотрим теперь выполнение аксиом поля относительно умножения матриц. Нейтральным элементом по умножению является единичная матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ в чем легко убедиться, применив правило умножения матриц «строка на столбец»:

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} x \cdot 1 + y \cdot 0 & x \cdot 0 + y \cdot 1 \\ y \cdot 1 + x \cdot 0 & y \cdot 0 + x \cdot 1 \end{pmatrix} = \begin{pmatrix} x & y \\ y & x \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \times \begin{pmatrix} x & y \\ y & x \end{pmatrix} = \begin{pmatrix} 1 \cdot x + 0 \cdot y & 1 \cdot y + 0 \cdot x \\ 0 \cdot x + 1 \cdot y & 0 \cdot y + 1 \cdot x \end{pmatrix} = \begin{pmatrix} x & y \\ y & x \end{pmatrix}$$

Проверим теперь коммутативность умножения матриц данного вида.

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} x \cdot a + y \cdot b & x \cdot b + y \cdot a \\ y \cdot a + x \cdot b & y \cdot b + x \cdot a \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} x & y \\ y & x \end{pmatrix} = \begin{pmatrix} a \cdot x + b \cdot y & a \cdot y + b \cdot x \\ b \cdot x + a \cdot y & a \cdot y + b \cdot x \end{pmatrix}$$

Очевидно, что справа стоят равные матрицы. Поэтому для матриц данного вида коммутативность умножения выполняется, хотя в общем случае умножение матриц свойством коммутативности не обладают.

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \times \begin{pmatrix} x & y \\ y & x \end{pmatrix}$$

Предположим теперь, что $\begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \begin{pmatrix} a & b \\ b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Тогда имеем равенство $\begin{pmatrix} x \cdot a + y \cdot b & x \cdot b + y \cdot a \\ y \cdot a + x \cdot b & y \cdot b + x \cdot a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Что равносильно системе уравнений:

$$\begin{cases} x \cdot a + y \cdot b = 0 \\ y \cdot a + x \cdot b = 0 \end{cases}$$

Заметим, что если матрица $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$ не нулевая, то либо $x \neq 0$, либо $y \neq 0$. А определители таких матриц $\begin{vmatrix} x & y \\ y & x \end{vmatrix} = x^2 - y^2 \neq 0$, отличны от 0 только при $x \neq y$, чего в общем случае может и не быть. Следовательно, не все элементы множества *M* обратимы. Ассоциативность умножения матриц известна из курса высшей математики. Рассмотрим теперь свойство дистрибутивности умножения относительно сложения матриц данного типа.

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} c & d \\ d & c \end{pmatrix} \right) = \begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \begin{pmatrix} a+c & b+d \\ b+d & a+c \end{pmatrix}$$

$$= \begin{pmatrix} x(a+c)+y(b+d) & x(b+d)+y(a+c) \\ y(a+c)+x(b+d) & y(b+d)+x(a+c) \end{pmatrix}$$

С другой стороны имеем: $\begin{pmatrix} x & y \\ y & x \end{pmatrix} \times \left(\begin{pmatrix} a & b \\ b & a \end{pmatrix} + \begin{pmatrix} c & d \\ d & c \end{pmatrix} \right) =$

$$= \begin{pmatrix} x \cdot a + y \cdot b & x \cdot b + y \cdot a \\ y \cdot a + x \cdot b & y \cdot b + x \cdot a \end{pmatrix} + \begin{pmatrix} x \cdot c + y \cdot d & x \cdot d + y \cdot c \\ y \cdot c + x \cdot d & y \cdot d + x \cdot c \end{pmatrix} =$$

$$= \begin{pmatrix} x(a+c)+y(b+d) & x(b+d)+y(a+c) \\ y(a+c)+x(b+d) & y(b+d)+x(a+c) \end{pmatrix}$$

Таким образом, все аксиомы кольца выполнены. Мы имеем ассоциативное, коммутативной кольцо $< M, +, \cdot >$ с единичным элементом относительно умножения, но которое не является полем.

Задание 9. В задачах вариантов 1-3 проверить, является ли $(H, *)$ подгруппой группы $(G, *)$. В задачах вариантов 4-7 проверить, является ли $(H, *, \circ)$ подкольцом кольца $(K, *, \circ)$. В задачах вариантов 8-10 проверить, является ли $(H, *, \circ)$ подполем поля $(P, *, \circ)$.

1) *H* – множество векторов плоскости, параллельных фиксированной прямой, *G* – множество всех векторов плоскости, * – операция сложения векторов.

4) *H* – множество матриц вида $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, где $x, y \in Z$,

***K* – множество квадратных матриц 2-го порядка, относительно двух операций: * – операция сложения, ° – операция умножения.**

8) *H* =Q, $P = R$, относительно двух операций: * – операция сложения, ° – операция умножения.

1) Алгебра $< \boldsymbol{G}, * >$ является абелевой группой, т.к. сложение векторов удовлетворяет всем аксиомам коммутативной группы. Заметим, что сложение векторов, параллельных фиксированной прямой даст вектор, параллельный этой же прямой. Противоположный вектор параллельность не нарушает. А нулевой вектор «параллелен» любой прямой. То есть вектора, параллельные фиксированной прямой составляют замкнутое множество, а потому это будет подгруппа.

4) Алгебра $< \boldsymbol{K}, +, \times >$ представляет собой ассоциативное кольцо с единицей, в качестве которой выступает единичная матрица второго порядка. Нулевым элементом, естественно является нулевая матрица. Проверим замкнутость множества ***H*** матриц вида $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, где x, y из множества целых чисел. Так как сумма и произведение целых чисел будет целым числом, то сумма и произведение матриц такого вида тоже будет матрицей такого вида.

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} + \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} x+a & y+b \\ -(y+b) & x+a \end{pmatrix}$$

$$\begin{pmatrix} x & y \\ -y & x \end{pmatrix} \times \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} xa-yb & xb+ya \\ -ya-xb & -yb+xa \end{pmatrix} =$$

$$= \begin{pmatrix} xa-yb & xb+ya \\ -(xb+ya) & xa-yb \end{pmatrix}$$

Нулевая и единичная матрицы, очевидно, имеют такой же вид. Следовательно алгебра $< \boldsymbol{H}, +, \times >$ является подкольцом кольца $< \boldsymbol{K}, +, \times >$, причем содержащим 1.

8) Рассмотрим поле $< \boldsymbol{R}, +, \cdot >$ действительных чисел. Множество Q рациональных чисел является подмножеством множества действительных чисел. 0 и 1 очевидно являются рациональными числами. Каждое рациональное число представляется в виде дроби $r = \frac{n}{m}$. Если оно отлично от 0, то и $n \neq 0$. А тогда

имеем $(r)^{-1} = \frac{m}{n} \in Q$. Сумма и произведение рациональных чисел снова является рациональным числом. Таким образом множество Q является замкнутым числом относительно операций в множестве ***R***. Следовательно, поле рациональных чисел

$< Q, +, \cdot >$ является подполем поля действительных чисел $< \boldsymbol{R}, +, \cdot >$.

Задание 10. Доказать, что указанные структуры являются изоморфными. Аддитивные группы множества целых чисел и множества целых чисел, кратных некоторому числу *n*.

По условию мы имеем две структуры $< Z, + >$ и $< nZ, + >$, где $nZ =$

$= \{na | a \in Z\}$. Определим отображение $\varphi: Z \to nZ$ формулой: $\varphi(z) = n \cdot z$. Очевидно, что оно является взаимно - однозначным, т.е. биективным, т.к. $a = b \leftrightarrow$

$\leftrightarrow n \cdot a = n \cdot b$. Проверим сохранение операции. $\varphi(a + b) = n \cdot (a + b) =$

$= n \cdot a + n \cdot z = \varphi(a) + \varphi(b)$. Тем самым изоморфизм установлен.

Практические задания по вариантам

Задание 1. Какими свойствами из ниже указанных обладает операция, заданная таблицей на конечном множестве (коммутативность, ассоциативность, обладает нейтральным элементом, обратимостью.)

Вариант 1.

*	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	a	a
d	a	a	a	a

Вариант 2.

*	a	b	c	d
a	a	b	c	d
b	b	c	d	a
c	c	d	a	b
d	d	a	b	c

Вариант 3.

*	a	b	c	d
a	b	b	c	d
b	b	d	d	a
c	c	d	c	b
d	d	a	b	d

Вариант 4.

*	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

Вариант 5.

*	a	b	c	d
a	a	b	c	d
b	b	a	d	b
c	c	d	a	c
d	d	b	c	a

Вариант 6.

*	a	b	c	d
a	a	b	c	d
b	b	c	c	d
c	c	c	d	a
d	d	d	a	b

Вариант 7.

*	a	b	c	d
a	b	c	d	a
b	c	d	a	b
c	d	a	b	c
d	a	b	c	d

Вариант 8.

*	a	b	c	d
a	a	c	d	b
b	c	b	a	b
c	d	a	c	c
d	a	b	c	d

Вариант 9.

*	a	b	c	d
a	a	b	a	b
b	a	b	a	b
c	a	b	a	b
d	a	b	a	b

Вариант 10.

*	a	b	c	d
a	d	c	b	a
b	c	b	a	d
c	b	a	d	c
d	a	b	c	d

Задание 2. На каких из множеств: *N* (множество натуральных чисел), *Z* (множество целых чисел), *2Z* (множество четных чисел), *2Z+1* (множество нечетных чисел), *Q* (множество рациональных чисел), *R* (множество действительных чисел), R^+ (множество действительных положительных чисел) задана бинарная алгебраическая операция *. $a * b = a + 2b$.

Вариант	Задание	Вариант	Задание
1	$a * b = \frac{a+b}{3}$	2	$a * b = \frac{a}{b^2+1}$
3	$a * b = (a-b)^2$	4	$a * b = b : a$
5	$a * b = b^a$	6	$a * b = \lvert a \cdot b \rvert$
7	$a * b = \sqrt{a \cdot b}$	8	$a * b = \min(a,b)$
9	$a * b = (a+b)^3$	10	$a * b = a^{b+1}$

Задание 3. Является ли операция * из задания 2 на тех же множествах, на которых она задана, а) коммутативной, б) ассоциативной, в) обладающей нейтральным элементом, г) обратима?

Задание 4. Какой алгеброй является данное множество с одной бинарной операцией? (Полугруппа, моноид, группа, абелева группа.)

Вариант 1. <N; +>; Вариант 2. <N; ×>; Вариант 3. <Z;+>;
Вариант 4. <Z; ×>; Вариант 5. <Q; +>; Вариант 6. <Q; ×>;
Вариант 7. <R; +>; Вариант 2. <R; ×>; Вариант 9. <C; +>;
Вариант 10. <C; ×>.

Задание 5. Какой алгеброй из указанных видов может являться данное множество с двумя бинарными операциями? (Полукольцо, кольцо, поле.)

Вариант 1. <N; +, ×>; Вариант 2. <N; +, :>; Вариант 3. <Z;+, ×>;
Вариант 4. <Z; +, :>; Вариант 5. <Q; +,×>; Вариант 6. <Q; +, :>;
Вариант 7. <R; +, ×>; Вариант 2. <R; +, :>; Вариант 9. <C; +, ×>;
Вариант 10. <C; +, :>.

Задание 6. Образует ли указанное множество *M* относительно указанной операции какую либо алгебраическую структуру и какую, если образует?

Вариант	Задание
1	Множество целых чисел, запись которых оканчивается 0, относительно операции сложения.
2	Множество $\left\{x \middle\| x = 2a + \sqrt{3}b,\ a,b \in Q\right\}$ относительно операции сложения.
3	Множество целых чисел, кратных 3, относительно операции умножения.
4	Множество целых чисел, которые при делении на 4 дают в остатке 1, относительно операции умножения.
5	Множество $\left\{x \middle\| x = 2a + \sqrt{3}b,\ a,b \in Z \setminus \{0\}\right\}$ относительно операции сложения.
6	Множество целых чисел, запись которых оканчивается 0, относительно операции умножения.
7	Множество целых чисел, сумма цифр которых делится на 3, относительно операции умножения.
8	Множество целых чисел, сумма цифр которых делится на 9,

	относительно операции сложения.
9	Множество целых чисел, которые при делении на 5 дают в остатке 1, относительно операции сложения.
10	Множество $\left\{x \middle\| x = 3a + \sqrt{3}b,\ a,b \in Z \setminus \{0\}\right\}$ относительно операции сложения.

Задание 7. Какую алгебраическую структуру образует указанное множество *M* относительно указанной операции?

Вариант	Задание
1	*M* – множество квадратных матриц фиксированного порядка, определитель которых равен 1, относительно умножения.
2	*M* – множество пар (a,b), где $a,b \in R,\ a \neq 0$ относительно операции *, если $(a,b) * (a',b') = (a \cdot a', a \cdot b' + b \cdot a)$.
3	$M = \{-1,1\}$ относительно операции умножения.
4	$M = \{1,2,4,8\}$ относительно операции нахождения наименьшего общего кратного элементов множества *M.*
5	*M* – множество матриц вида $\begin{pmatrix} x & 5y \\ y & x \end{pmatrix}$, $x,y \in Q$ относительно операции умножения.
6	*M* – множество всех подмножеств множества $\{1,2\}$ относительно операции объединения.
7	*M* – множество прямоугольных матриц размера $m \times n$ относительно вычитания.
8	*M* – множество всех векторов, параллельных фиксированной прямой, относительно операции сложения.
9	$M = \{1,2,4,8\}$ относительно операции нахождения наибольшего общего делителя элементов множество *M*.

10	M – множество пар (a,b), где $a,b \in R$, $a \neq 0$ относительно операции *, если $(a,b)*(a',b') = (a \cdot a', b \cdot b')$.

Задание 8. Выяснить, образует ли множество *M* относительно операций сложения и умножения кольцо или поле.

Вариант	Задание
1	M – множество многочленов с целыми коэффициентами.
2	M – множество функций действительного переменного, непрерывных на отрезке $[-2;2]$.
3	M – множество ненулевых матриц вида $\begin{pmatrix} x & y \\ 2y & x \end{pmatrix}$, $x, y \in Q$.
4	M – множество квадратных матриц третьего порядка, у которых две последние строки нулевые.
5	M – множество квадратных симметричных матриц фиксированного порядка.
6	M – множество чисел вида $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, где $a,b,c \in Q$.
7	M – множество всех подмножеств множества $\{x,y\}$, роль операции сложения играет симметрическая разность, роль операции умножения играет пересечение.
8	M – множество рациональных дробей вида $\frac{f(x)}{g(x)}$, где $f(x), g(x)$ – функции действительного переменного, $g(x) \neq 0$.
9	$M = \{0;1\}$, операции сложения и умножения задаются таблицами: $\begin{array}{c\|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array}$ $\quad$ $\begin{array}{c\|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}$

10	M – множество всех рациональных чисел, которые можно представить в виде дроби со знаменателем, равным степени числа 2.

Задание 9. В задачах вариантов 1-3 проверить, является ли $(H,*)$ подгруппой группы $(G,*)$. В задачах вариантов 4-7 проверить, является ли $(H,*,\circ)$ подкольцом кольца $(K,*,\circ)$. В задачах вариантов 8-10 проверить, является ли $(H,*,\circ)$ подполем поля $(P,*,\circ)$.

Вариант	Задание
1	$H = nZ$, где n – некоторое натуральное число, $G = Z$, * – операция сложения.
2	H – множество квадратных матриц фиксированного порядка, определитель которых равен 1, G – множество квадратных матриц фиксированного порядка, определитель которых отличен от 0, * – операция умножения матриц.
3	H – множество пар вида $(0;b)$, где $b \in R$, G – множество пар вида $(a;b)$, где $a, b \in R$, * определяется следующим образом: $(a,b)*(a',b') = (a+a', b+b')$.
4	$H=N$, $K=Z$, с двумя бинарными операциями: * – операция сложения, ° – операция умножения.
5	H – множество матриц вида $\begin{pmatrix} x & y \\ -y & x \end{pmatrix}$, где $x, y \in Z$, K – множество квадратных невырожденных матриц 2-го порядка, относительно двух операций: * – операция сложения, ° – операция умножения.
6	H – множество многочленов 1-ой степени, K – множество всех многочленов, относительно двух операций: * – операция сложения, ° – операция

	умножения
7	H – множество целых чисел, кратных 5, K=Z, относительно двух операций: * – операция сложения, ° – операция умножения.
8	$H = \{x \mid x = a + b\sqrt{3},\ a,b \in Q\}$, $P = R$, относительно двух операций: * – операция сложения, ° – операция умножения.
9	$H = \{x \mid x = a + b\sqrt{2},\ a,b \in Z\}$, $P = \{x \mid x = a + b\sqrt{2},\ a,b \in Q\}$, относительно двух операций * – операция сложения, ° – операция умножения.
10	H – множество пар вида $(b;0)$, где $b \in Q$, P – множество пар вида $(a;0)$, где $a \in R$, относительно двух операций: $(a,0)+(a',0)=(a+a',0)$, $(a,0)\cdot(a',0)=(a\cdot a',0)$.

Задание 10. Доказать, что указанные структуры являются изоморфными.

Вариант	Задание
1	Поле $(M,+,\cdot)$ и поле $(C,\otimes,\circ)$, где M – множество матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, $a,b \in R$, C – множество пар вида (a,b), $a,b \in R$, операции $\oplus$ и $\circ$ определены следующим образом: $(a,b)\oplus(c,d)=(a+c,b+d)$, $(a,b)\circ(c,d)=(ac-bd,ad+bc)$
2	Группа $(S_2,\circ)$ и группа $(M,*)$, где S_2 – множество поворотов плоскости на 0^0 и на 180^0, $\circ$ – операция композиции, $M=\{-1,1\}$, * определена так: <table><tr><td>*</td><td>-1</td><td>1</td></tr><tr><td>-1</td><td>1</td><td>-1</td></tr><tr><td>1</td><td>-1</td><td>1</td></tr></table>
3	Кольцо $(Q,+,\cdot)$ и кольцо $(M,+,\cdot)$, где M – множество матриц вида $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$, $a \in Q$.

4	Алгебра $(M,+,\cdot)$ и алгебра $(G,+,\cdot)$, где M – множество матриц вида $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, $a,b \in Q$, G – множество чисел вида $a+b\sqrt{2}$, $a,b \in Q$.
5	Группа S_3 = <(1,2,3),°> множества всех подстановок с операцией умножения и группа симметрий правильного треугольника на плоскости: поворотов вокруг центра треугольника на 120°, 240°.
6	Поле $(R,+,\cdot)$ и поле $(K,\otimes,\circ)$, где K – множество пар вида $(a,0)$, $a \in R$, операции $\oplus$ и $\circ$ определены так: $(a,0)\oplus(c,0)=(a+c,0)$, $(a,0)\circ(c,0)=(a\cdot c,0)$.
7	Группа симметрий куба и группа S_4 подстановок с операцией умножения.
8	Алгебра $(M,+,\cdot)$ и алгебра $(D,\otimes,\circ)$, где M – множество матриц вида $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$, $a,b \in R$, D – множество пар вида (a,b), $a,b \in R$, операции $\oplus$ и $\circ$ определены следующим образом: $(a,b)\oplus(c,d)=(a+c,b+d)$, $(a,b)\circ(c,d)=(ac+bd,ad+bc)$.
9	Группа $(R\setminus\{0\},\cdot)$ и группа $(R\setminus\{0\},\cdot)$, если задано отображение φ, где $\varphi: x \mapsto \frac{1}{x}$.
10	Группа $(R,+)$ и группа $(M,\times)$, где M – множество матриц вида $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $x \in R$.

Список литературы

1. Веселова, Л. В. Алгебра и теория чисел : Учебное пособие / Л. В. Веселова, О. Е. Тихонов. – Казань : Казанский национальный исследовательский технологический университет, 2014. – 107 с. – ISBN 978-5-7882-1636-2.
2. Ларин, С. В. Алгебра и теория чисел. Группы, кольца и поля : Учебное пособие / С. В. Ларин. – 2-е изд., испр. и доп. – Москва : Издательство Юрайт, 2020. – 1 с. – (Высшее образование). – ISBN 978-5-534-05567-2.
3. Швед, Е. А. Практикум по алгебре: элементы теории чисел / Е. А. Швед, В. А. Федоров. – Омск : Омский государственный университет путей сообщения, 2022. – 39 с.
4. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел : учебное пособие / Л. Б. Шнеперман ; Л. Б. Шнеперман. – 3-е изд., стер.. – Санкт-Петербург [и др.]: Лань, 2008. – (Учебники для вузов. Специальная литература). – ISBN 978-5-8114-0885-6.
5. Виноградов, И. М. Основы теории чисел [Текст]: учебное пособие / И. М. Виноградов. - Изд. 12-е, стер. - СПб. [и др.]: Лань, 2009. - 176 с.
6. Виноградов, И. М. Элементы высшей математики : аналитическая геометрия, дифференциальное исчисление : учебник для студентов высших учебных заведений, обучающихся по инженерно-техническим специальностям / И. М. Виноградов ; И. М. Виноградов. – Москва : Дрофа, 2010. – 319 с. – (Высшее образование. Современный учебник). – ISBN 978-5-358-06101-9.
7. Гончаренко, В. М. Элементы высшей математики / В. М. Гончаренко, Л. В. Липагина, А. А. Рылов. – МОСКВА : Компания КноРус, 2019. – 364 с. – ISBN 978-5-406-06878-6.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждения высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__11__» ____04_____2023 г.

Комплексные числа и элементы теории многочленов

Методические рекомендации

для выполнения практических заданий по дисциплинам

«Элементы алгебры и теории чисел» и «Алгебра и теория чисел»

Направления подготовки: 10.03.01 «Информационная безопасность»;
02.03.03 «Математическое обеспечение и администрирование
информационных систем».

Курск – 2023

УДК 511+512(075.8)
Составители:
д. ф-м. н., профессор В.П. Добрица
к.т.н. Е.А. Кулешова
к.т.н., доцент Ю.А. Халин

Рецензент

Кандидат технических наук, доцент кафедры вычислительной техники А.В. Киселев

Комплексные числа и элементы теории многочленов: методические рекомендации для выполнения практических заданий / Юго-Зап. гос. ун-т; сост.: В.П. Добрица, Е.А. Кулешова, Ю.А. Халин. – Курск, 2023. – 39 с. – Библиогр.: с. 39.

В методических указания описываются основны алгебры и теории чисел. Изложены краткие теоретические сведения, приведены примеры решения задач, а также задачи для самостоятельного решения.

Методические рекомендации предназначены для студентов, обучающихся по направлениям подготовки 10.03.01 «Информационная безопасность» и 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. 234
Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

В данных методических рекомендациях изложены материалы по разделам «Комплексные числа» и «Элементы теории многочленов».

По каждой теме представлены:

1) краткие теоретические положения;
2) перечень вопросов, выносимых на практическое задание;
3) примеры решения типовых задач, выносимых на практическое занятие;
4) задачи, выносимые на самостоятельную работу студентов.

Данные методические рекомендации предназначены для проведения практических занятий по дисциплинам «Элементы алгебры и теории чисел» и «Алгебра и теория чисел» для студентов Юго-Западного государственного университета направлений подготовки: информационная безопасность, математическое обеспечение и администрирование информационных систем.

При выполнении практических заданий в каждой задаче выберете задание из своего варианта. Вариант определяется по последней цифре номера зачетной книжки. Отчет по работе должен содержать решения задач и выводы с полным их обоснованием. Отчет по работе оформить на листах формата А4 в формате WORD. На титульном листе должно быть указано: университет, факультет, кафедра, предмет, номер практического занятия, вариант, группа, исполнитель, проверяющий.

РАБОТА № 1 (10) Комплексные числа.

Цель: изучить свойства комплексных чисел.

Вопросы, выносимые на практическое занятие.

1. Поле комплексных чисел.
2. Алгебраическая и тригонометрическая запись комплексного числа.
3. Операции над комплексными числами.
4. Нахождение корней из комплексных чисел.

Краткие теоретические сведения.

Под множеством комплексных чисел будем понимать множество упорядоченных пар $C = \{(a, b) | \, a \in R, b \in R\}$. Первое координата a пары (a,b) называется действительной частью комплексного числа z и обозначается символом $a=Re\ z$, второе число b пары (a,b) называется мнимой частью комплексного числа z и обозначается символом $b=Im\ z$.

Два комплексных числа $z_1=(a_1,b_1)$ и $z_2=(a_2,b_2)$ равны тогда и только тогда, когда равны их действительные и мнимые части, т.е. $z_1=z_2$ лишь тогда, когда $a_1=a_2$, $b_1=b_2$.

Суммой двух комплексных чисел $z_1=(a_1,b_1)$ и $z_2=(a_2,b_2)$ называется комплексное число $z=(a,b)$, где $a=a_1+a_2$, $b=b_1+b_2$. Нулем называется такое комплексное число**,** сумма которого с любым комплексным числом z равно этому числу z, т.е. $z+0=z$. В качестве нуля следует рассматривать пару (0, 0).

ТЕОРЕМА. Система $< C, + >$ является абелевой группой.

Произведением двух комплексных чисел $z_1=(a_1,b_1)$ и $z_2=(a_2,b_2)$ называется комплексное число $z=(a,b)$ такое, что $a=a_1 \cdot a_2-b_1 \cdot b_2$, $b=a_1 \cdot b_2+a_2 \cdot b_1$.

ТЕОРЕМА. Система $< C, +, \cdot >$ является полем.

ТЕОРЕМА. Если в поле комплексных чисел рассматривать подмножество действительных частей вида *(a,0)*, то система $< \{(a,0) | \, a \in R\}, +, \cdot >$ является полем, изоморфным полю действительных чисел$< R, +, \cdot >$.

Полагая $z_r=(a,0)=a$, будем считать, что поле действительных чисел являются подполем поля комплексных чисел.

Комплексные числа $z_i=(0,b)$ будем называть чисто мнимыми. Обозначим комплексное число $z_i=(0,1)=i$ и назовем его мнимой единицей. Согласно определению произведения двух комплексных чисел имеем: $i^2=(0,1)\cdot(0,1)=(-1,0)=\mathbf{-1}$.

ТЕОРЕМА. Число $z_i=(0,b)$ есть произведение мнимой единицы на действительное число b: $z_i=(0,b)=i\cdot b$.

В соответствии с введенными обозначениями можем записать:

$z=(a,b)=(a,0)+(0,b)=a+i\cdot b$, т.е. придать алгебраический смысл так называемой алгебраической форме комплексного числа для того, чтобы производить операции сложения и умножения по обычным правилам алгебры многочленов. Заметим, что $0 = 0 + i \cdot 0$.

Комплексное число $\bar{z} = a - i \cdot b$ называется комплексно сопряженным числу $z = a + i \cdot b$.

ТЕОРЕМА. Для произвольного комплексного числа $z \in C$ выполняются соотношения $z \cdot \bar{z} = a^2 + b^2 \in R$ и $z + \bar{z} = 2 \cdot a \in R$.

Операция деления комплексных чисел определяется как операция обратная умножению. Комплексное число $z=a+ib$ называется частным комплексных чисел $z_1=a_1+ib_1$ и $z_2=a_2+ib_2$, если $z_1=z\cdot z_2$.

ТЕОРЕМА. Действительная и мнимая часть частного z определяются из решения системы:

$$\begin{cases} a_2 \cdot a - b_2 \cdot b = a_1, \\ b_2 \cdot a + a_2 \cdot b = b_1. \end{cases}$$

То есть имеем:

$$z = \frac{z_1}{z_2} = \frac{a_1 \cdot a_2 + b_1 \cdot b_2}{a_2^2 + b_2^2} + i\frac{b_1 \cdot a_2 - a_1 \cdot b_2}{a_2^2 + b_2^2}$$

ТЕОРЕМА. $\frac{z_1}{z_2} = \frac{z_1 \cdot \overline{z_2}}{z_2 \cdot \overline{z_2}}$.

Комплексное число *z* можно представлять как точку в двумерном пространстве - плоскости *(X,Y)* с декартовыми координатами *x=a*, *y=b*. Комплексному числу *z=0* поставим в соответствие начало координат (рис.1.).

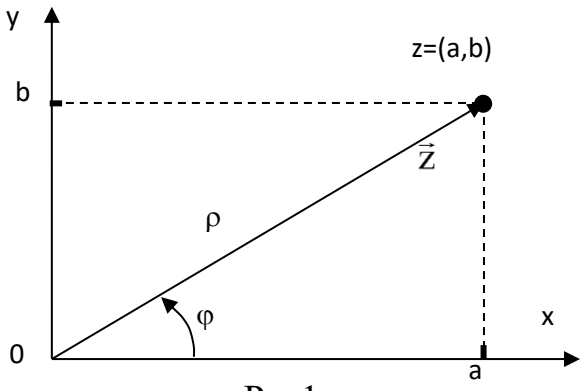


Рис1.
Геометрический смысл комплексного числа.

Такую плоскость называют комплексной плоскостью *C*, ось абсцисс *x* - действительной, а ось ординат *y* - мнимой осью комплексной плоскости.

Каждой точке на плоскости можно взаимно однозначно сопоставить вектор $\vec{z} = a \cdot \vec{1} + b \cdot \vec{i}$, где $\vec{1}$ - вектор единичной длины, выходящий из начала координат в направлении оси *x*, а $\vec{i}$ - вектор единичной длины, исходящий из начала координат в направлении оси y. Проекции вектора $\vec{z}$ на ось абсцисс *x* и ось ординат *y* соответственно равны *a* и *b*. Таким образом, комплексное число можно представлять как точку или вектор на комплексной плоскости.

Для определения точки на плоскости или вектора используются также полярные координаты *(ρ,φ)*, где *ρ≥0* - расстояние от начала координат до точки (длина вектора), а *φ* - угол, который составляет радиус-вектор данной точки с осью *OX* (угол между вектором и осью *OX*, положительное направление против часовой стрелки).

ТЕОРЕМА. $a=\rho\cdot\cos\varphi$, $b=\rho\cdot\sin\varphi$.

Положительным направлением изменения угла *φ* считается направление против часовой стрелки (*-∞<φ<∞*). Следовательно, имеем:

$$z = \rho \cdot \cos\varphi + i \cdot \rho \cdot \sin\varphi = \rho \cdot (\cos\varphi + i \cdot \sin\varphi),$$

где

$$\rho = \sqrt{a^2 + b^2}; \qquad \operatorname{tg}\ \varphi = \frac{b}{a}\ .$$

Такая форма называется тригонометрической формой записи комплексного числа. При этом ρ называют модулем комплексного числа, который обозначается как $\rho=|z|$, а φ - аргументом комплексного числа и его обозначают $\varphi = Arg\ z$.

Так как одному и тому значению комплексного числа z соответствует бесконечное число значений аргумента $Arg\ z$, отличающихся на величину $2\pi k$ $(k=1,2,...)$, то имеем:

$$z = \rho \cdot (\cos\varphi_0 + i \cdot \sin\varphi_0) = \rho \cdot [\cos(\varphi) + i \cdot \sin(\varphi)],$$

где $0 \le \varphi_0 < 2\pi, \quad \varphi = \varphi_0 + 2\pi k, \ (k=0,\pm1,\pm2,...)$.

Удобно ввести следующее общепринятое обозначение основного значения аргумента $arg\ z=\varphi$, $0 \le \varphi < 2\pi$. Тогда можем записать $Arg\ z = arg\ z + 2\pi k$, $(k=0,\pm1,\pm2,...)$.

Аргумент комплексного числа $z=0$ вообще не определен, т.к. $b=a=0$, а его модуль равен нулю.

Сопоставим двум комплексным числам z_1 и z_2 на комплексной плоскости два вектора $\vec{z}_1$ и $\vec{z}_2$.

Операции сложения и вычитания двух комплексных чисел z_1 и z_2 можно отождествлять с операциями сложения и вычитания двух векторов $\vec{z}_1, \vec{z}_2$, т.е. по правилу параллелограмма.

ТЕОРЕМА. $|z_1+z_2| \le |z_1|+|z_2|$ и $|z_1-z_2| \ge |z_1|-|z_2|$.

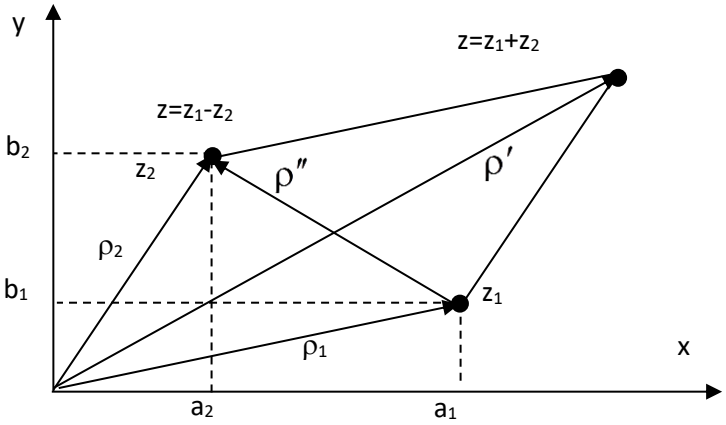


Рис. 2.
Сложение и вычитание двух комплексных чисел.

Используя формулу Эйлера:

$$e^{i\cdot\varphi} = \cos\varphi + i\cdot\sin\varphi, \qquad (1.7)$$

получаем показательную формулу представления комплексного числа:

$$z = \rho\cdot e^{i\cdot\varphi}$$

ТЕОРЕМА. (Эйлер) $e^z = e^x\cdot e^{iy} = e^x\cdot(cosy + i\cdot siny)$

для $z = x + iy$.

ТЕОРЕМА. $z = \rho\cdot e^{i\cdot\varphi} = z_1\cdot z_2 = (\rho_1\cdot\rho_2)\cdot e^{i(\varphi_1+\varphi_2)}$
$z = \rho\cdot e^{i\cdot\varphi} = z_1 / z_2 = (\rho_1/\rho_2)\cdot e^{i\cdot(\varphi_1-\varphi_2)}$.

То есть получаем соответствующие формулы для операций умножения и деления комплексных чисел:

ТЕОРЕМА. $\rho=\rho_1\cdot\rho_2$, $\varphi=\varphi_1+\varphi_2$;

$\rho=\rho_1/\rho_2$, $\varphi=\varphi_1-\varphi_2$.

Комплексное число $z_1 = \sqrt[n]{z}$ называется корнем n-ой степени из комплексного числа z, если $z_1{}^n=z$. Пусть $z_1 = \rho_1\cdot e^{i\cdot\varphi_1}$ и $z = \rho\cdot e^{i\cdot\varphi}$. Из определения следует, что

$$(\rho_1\cdot e^{i\cdot\varphi_1})^n = \rho_1^n\cdot e^{i\cdot n\cdot\varphi} = \rho\cdot e^{i\cdot\varphi};$$
$$\rho_1 = \sqrt[n]{\rho}, \qquad \varphi_1 = \frac{\varphi}{n}.$$

ТЕОРЕМА. Для корня $z_1 = \sqrt[n]{z}$ из комплексного числа $z = \rho\cdot e^{i\cdot\varphi}$ имеют место равенства $\rho_1 = \sqrt[n]{\rho}$, $\varphi_1 = \frac{\varphi}{n}$.

Так как аргумент φ комплексного числа z определен с точностью до слагаемого $2\pi k$: $\varphi=\varphi_0+2\pi k$ $(k=0,\pm1,\pm2,...)$, $0\le\varphi_0<2\pi$, то можем записать:

$$\varphi_1 = \frac{\varphi_0}{n} + \frac{2\pi k}{n}, \qquad k = 0,\pm1,\pm2,\ldots$$

Введем новые индексы: $k=l\cdot n+k'$, где $l=0,\pm1,\pm2,...$ $k'=0,1,2,...,n-1$. Получаем:

$$\varphi_1 = \frac{\varphi_0}{n} + 2\pi l + \frac{2\pi k'}{n}, \qquad \begin{matrix} l = 0,\pm1,\pm2,\ldots; \\ k' = 0,1,2,\ldots,n-1. \end{matrix}$$

Так как нас интересуют значения аргумента, которые лежат в интервале [0,2π] (поскольку комплексные числа равны, если аргументы отличаются на 2πl, l=±1,...), то мы имеем всего n различных значений аргумента, которые расположены в интервале [0,2π]:

$$\varphi_1 = \frac{\varphi_0}{n} + \frac{2\pi k'}{n}, \qquad k' = 0,1,2,\ldots,n-1.$$

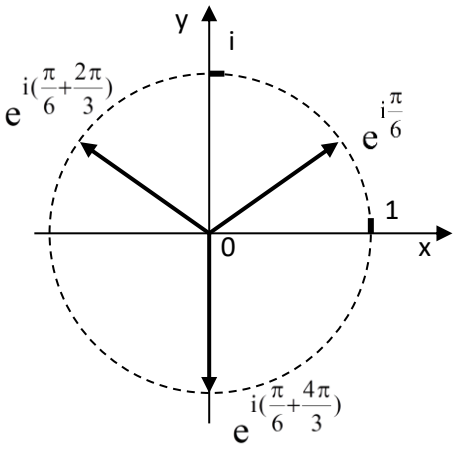


Рис.3

ТЕОРЕМА. Для $z_1 = \sqrt[n]{z}$ имеется *n* различных корней из комплексного числа *z*, *y* которых одинаковые модули $\rho_1 = \sqrt[n]{\rho}$, а аргументы $\varphi_1 = \frac{\varphi_0}{n} + \frac{2\pi k'}{n}, \quad k' = 0,1,2,\ldots,n-1.$ отличаются на величину $\frac{2\pi k'}{n}$, $k' = 0,1,2,\ldots,n-1$.

Точки на комплексной плоскости, соответствующие различным корням *n*-ой степени из комплексного числа *z*, расположены в вершинах правильного *n*-угольника, вписанного в окружность радиуса $\sqrt[n]{\rho}$ с центром в точке *z=0*.

Возведение комплексного числа в натуральную степень производится по формуле Муавра.

ТЕОРЕМА. $z^n = r^n(\cos n\varphi + i\sin n\varphi)$

Примеры выполнения заданий.

Пример 1. Найти $z_1 + z_2$, $z_1 \cdot z_2$, z_1^2, $\frac{z_1}{z_2}$, **если** $z_1 = 4 - 5i$, $z_2 = 2 + 3i$.

Решение:

$$z_1 + z_2 = 4 - 5i + 2 + 3i = (4+2) + (-5+3)i = 6 - 2i$$

$$z_1 \cdot z_2 = (4-5i)\cdot(2+3i) = 8 + 12i - 10i - 15i^2 = 8 + 2i - 15(-1) = 23 + 2i$$

$$z_1^2 = (4-5i)^2 = 16 - 40i + 25i^2 = 16 - 40i - 25 = -9 - 40i$$

$$\frac{z_1}{z_2}=\frac{4-5i}{2+3i}=\frac{(4-5i)\cdot(2-3i)}{(2+3i)\cdot(2-3i)}=\frac{8-10i-12i+15i^2}{2^2-(3i)^2}=\frac{8-22i-15}{4+9}=$$
$$=\frac{-7-22i}{13}=-\frac{7}{13}-\frac{22}{13}i.$$

Пример 2. Найти i^9, i^{27}.

Решение: Для любых $q,r\in N$ имеет место равенство $i^{4q+r}=i^r$, т.к. $i^4=1$. Следовательно,

$$i^9=i^{4\cdot2+1}=i^1=i,$$
$$i^{27}=i^{6\cdot4+3}=i^3=i^2\cdot i=-1\cdot i=-i.$$

Пример 3. Найти действительные решения уравнения

$$(-2+5i)x+2i=(1-2i)y+3ix-3.$$

Решение: Представим выражения в левой и правой части уравнения в виде $a+bi$.

$$(-2+5i)x+2i=(1-2i)y+3ix-3$$
$$-2x+5ix+2i=y-2iy+3ix-3$$
$$-2x+(5x+2)i=y-3+(-2y+3x)i$$

Исходя из определения равенства комплексных чисел, имеем систему уравнений:

$$\begin{cases}-2x=y-3,\\5x+2=-2y+3x;\end{cases}\Leftrightarrow\begin{cases}y=-2x+3,\\5x+2=-2(-2x+3)+3x;\end{cases}\Leftrightarrow$$
$$\Leftrightarrow\begin{cases}y=-2x+3,\\5x+2=4x-6+3x;\end{cases}\Leftrightarrow\begin{cases}y=-2x+3,\\-2x=-8;\end{cases}\Leftrightarrow$$
$$\Leftrightarrow\begin{cases}y=-2x+3,\\-2x=-8;\end{cases}\Leftrightarrow\begin{cases}y=-5,\\x=4.\end{cases}$$

Ответ: $x=4$, $y=5$.

Пример 4. Дать геометрическое описание множества точек комплексной плоскости, удовлетворяющих условию $|\mathrm{Re}(z+3-i)|<1$.

Решение:

$\mathrm{Re}(z+3-i)$ – действительная часть числа $z+3-i$. Если $z = a + i \cdot b$, то

$$z+3-i = a+bi+3-i = (a+3)+(b-1)i$$

Следовательно $\mathrm{Re}(z+3-i) = a+3$.

Итак, $|a+3|<1$

$$|a+3|<1 \Leftrightarrow -1<a+3<1 \Leftrightarrow -4<a<-2$$

Изображением множества точек $M(a,b)$ на комплексной плоскости, удовлетворяющих условию $-4<a<-2$, служит бесконечная полоса, заключенная между прямыми $a=-4$ и $a=-2$, не включая точки этих прямых. (Рис. 3)

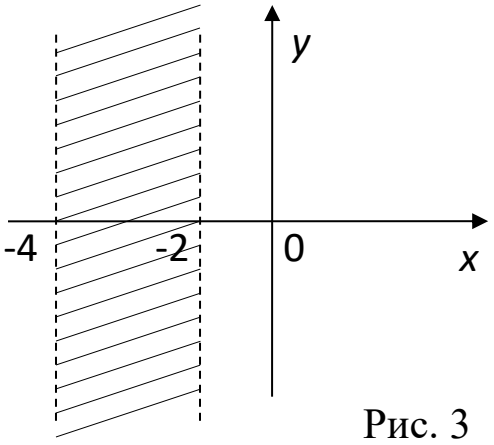


Рис. 3

Пример 5. Представить комплексные числа $z_1 = 1+i$ и $z_2 = 1-\sqrt{3}i$ в тригонометрической и экспоненциальной формах.

Решение: Любое комплексное число можно представить в виде:

$$z = a+bi = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{bi}{\sqrt{a^2+b^2}}\right) = r(\cos\varphi + i\sin\varphi),$$

где $r = \sqrt{a^2 + b^2}$ – модуль комплексного числа z, φ – аргумент комплексного числа z, обычно выбирают $\varphi \in [0, 2\pi)$, реже берут $\varphi \in (-\pi, \pi]$. φ находят из условий:

$$\cos\varphi = \frac{a}{r},\ \sin\varphi = \frac{b}{r}.$$

Символом $e^{i\varphi}$ обозначают экспоненциальную запись комплексного числа $\cos\varphi + i\sin\varphi$. Поэтому любое комплексное число можно представить в виде:

$$z = a + bi = r\,e^{i\varphi}$$

Для представления комплексного числа $z_1 = 1 + i$ в тригонометрической и экспоненциальной формах, найдем модуль и аргумент этого числа.

$a_1 = 1,\ b_1 = 1,$

$r_1 = \sqrt{a_1^2 + b_1^2} = \sqrt{1+1} = \sqrt{2},$

$$\varphi_1 : \begin{cases} \cos\varphi_1 = \dfrac{a_1}{r_1} = \dfrac{1}{\sqrt{2}} = \dfrac{\sqrt{2}}{2}, \\ \sin\varphi_1 = \dfrac{b_1}{r_1} = \dfrac{1}{\sqrt{2}} = \dfrac{\sqrt{2}}{2} \end{cases} \Rightarrow \varphi_1 = \frac{\pi}{4}.$$ (Рис. 4)

Следовательно,

$z_1 = \sqrt{2}\left(\cos\dfrac{\pi}{4} + i\sin\dfrac{\pi}{4}\right)$ – тригонометрическая форма записи z_1.

$z_1 = \sqrt{2}\,e^{i\frac{\pi}{4}}$ –экспоненциальная форма записи z_1.

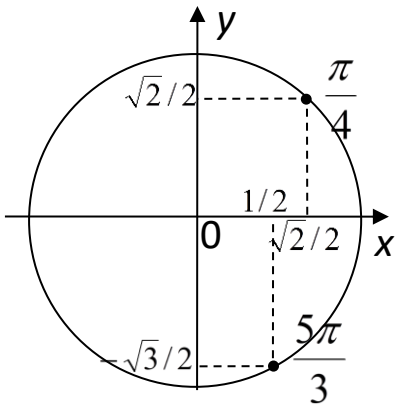


Рис. 4

Представим $z_2 = 1 - \sqrt{3}i$ в тригонометрической и экспоненциальной формах.

$a_2 = 1,\ b_2 = -\sqrt{3},$

$r_2 = \sqrt{a_2^2 + b_2^2} = \sqrt{1 + (-\sqrt{3})^2} = \sqrt{4} = 2,$

$$\varphi_2 : \begin{cases} \cos\varphi_2 = \dfrac{a_2}{r_2} = \dfrac{1}{2}, \\ \sin\varphi_2 = \dfrac{b_2}{r_2} = \dfrac{-\sqrt{3}}{2} \end{cases} \Rightarrow \varphi_2 = \frac{5\pi}{3}.$$ (Рис. 4)

Следовательно,

$z_2 = 2\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right)$ – тригонометрическая форма записи z_2.

$z_2 = 2e^{i\frac{5\pi}{3}}$ –экспоненциальная форма записи z_2.

Пример 6. Для комплексных чисел $z_1 = 1 + i$ и $z_2 = 1 - \sqrt{3}i$, записав их в тригонометрической форме, выполнить действия:

1) $z_1 \cdot z_2$, **2)** $\frac{z_1}{z_2}$, **3)** z_2^5, **4)** $\sqrt[3]{z_2}$.

Решение: В примере 4 была получена тригонометрическая форма каждого из данных комплексных чисел:

$$z_1 = \sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right),\ z_2 = 2\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right)$$

1) Чтобы перемножить два комплексных числа, записанных в тригонометрической форме, нужно перемножить их модули, а аргументы сложить:

$$z_1 \cdot z_2 = r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) =$$

$$= r_1 r_2(\cos(\varphi_1 + \varphi_2) + i\sin(\varphi_1 + \varphi_2))$$

$$z_1 \cdot z_2 = 2\sqrt{2}\left(\cos\left(\frac{\pi}{4} + \frac{5\pi}{3}\right) + i\sin\left(\frac{\pi}{4} + \frac{5\pi}{3}\right)\right) = 2\sqrt{2}\left(\cos\frac{23\pi}{12} + i\sin\frac{23\pi}{12}\right)$$

2) Чтобы найти частное от деления двух комплексных чисел, нужно найти частное от деления их модулей и разность их аргументов:

$$\frac{z_1}{z_2} = \frac{r_1(\cos\varphi_1 + i\sin\varphi_1)}{r_2(\cos\varphi_2 + i\sin\varphi_2)} = \frac{r_1}{r_2}(\cos(\varphi_1 - \varphi_2) + i\sin(\varphi_1 - \varphi_2))$$

$$\frac{z_1}{z_2} = \frac{\sqrt{2}}{2}\left(\cos\left(\frac{\pi}{4} - \frac{5\pi}{3}\right) + i\sin\left(\frac{\pi}{4} - \frac{5\pi}{3}\right)\right) = \frac{\sqrt{2}}{2}\left(\cos\left(-\frac{17\pi}{12}\right) + i\sin\left(-\frac{17\pi}{12}\right)\right) =$$

$$= \frac{\sqrt{2}}{2}\left(\cos\left(-\frac{17\pi}{12} + 2\pi\right) + i\sin\left(-\frac{17\pi}{12} + 2\pi\right)\right) = \frac{\sqrt{2}}{2}\left(\cos\left(\frac{7\pi}{12}\right) + i\sin\left(\frac{7\pi}{12}\right)\right).$$

В рассмотренном примере к полученному аргументу добавлено выражение 2π (период тригонометрических функций $\rho = \cos\varphi$ и $\rho = \sin\varphi$) для того, чтобы получить значение аргумента из промежутка $[0, 2\pi)$.

3) Возведение комплексного числа в натуральную степень производится по формуле Муавра:

$$z^n = r^n(\cos n\varphi + i\sin n\varphi).$$

$$z_2^5 = 2^5\left(\cos\left(5\cdot\frac{5\pi}{3}\right) + i\sin\left(5\cdot\frac{5\pi}{3}\right)\right) = 32\left(\cos\frac{25\pi}{3} + i\sin\frac{25\pi}{3}\right) =$$

$$= 32\left(\cos\left(8\pi + \frac{\pi}{3} \right) + i \sin\left(8\pi + \frac{\pi}{3} \right) \right) = 32\left(\cos\frac{\pi}{3} + i \sin\frac{\pi}{3} \right).$$

4) Существует ровно *n* корней *n*-ой степени из комплексного числа:

$$\sqrt[n]{z} = \sqrt[n]{r(\cos\varphi + i\sin\varphi)} = \sqrt[n]{r}\left(\cos\frac{\varphi + 2\pi k}{n} + i\sin\frac{\varphi + 2\pi k}{n} \right),$$

где $k = 0,1,\ldots,n-1.$

В рассматриваемом примере получаем:

$$\sqrt[3]{z} = \sqrt[3]{2}\left(\cos\frac{\frac{5\pi}{3} + 2\pi k}{3} + i\sin\frac{\frac{5\pi}{3} + 2\pi k}{3} \right), \text{ где } k = 0,1,2$$

при *k*=0 $\sqrt[3]{2}\left(\cos\frac{5\pi/3}{3} + i\sin\frac{5\pi/3}{3} \right) = \sqrt[3]{2}\left(\cos\frac{5\pi}{9} + i\sin\frac{5\pi}{9} \right),$

при *k*=1 $\sqrt[3]{2}\left(\cos\frac{\frac{5\pi}{3} + 2\pi}{3} + i\sin\frac{\frac{5\pi}{3} + 2\pi}{3} \right) = \sqrt[3]{2}\left(\cos\frac{11\pi}{9} + i\sin\frac{11\pi}{9} \right),$

при *k*=2 $\sqrt[3]{2}\left(\cos\frac{\frac{5\pi}{3} + 4\pi}{3} + i\sin\frac{\frac{5\pi}{3} + 4\pi}{3} \right) = \sqrt[3]{2}\left(\cos\frac{17\pi}{9} + i\sin\frac{17\pi}{9} \right).$

Заметим, что аргументы получившихся комплексных чисел разбивают единичную окружность на три равные дуги. (Рис. 5).

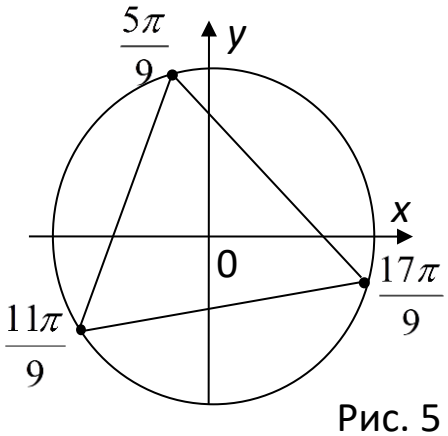


Рис. 5

Пример 7. Выразить через $sinx$ и cosx функцию $sin\ 5x$.

Решение: На основании формулы Эйлера имеем равенство

$$cos5x + i \cdot sin5x = (cosx + isinx)^5$$

Раскроем правую часть по формуле бинома Ньютона.

$$(cosx + isinx)^5 =$$
$$= (cosx)^5 + 5(cosx)^4 \cdot i \cdot sinx + 10(cosx)^3 \cdot i^2 \cdot (sinx)^2$$
$$+ 10(cosx)^2 \cdot i^3 \cdot (sinx)^3 + 5cosx \cdot i^4 \cdot (sinx)^4 + i^5 \cdot (sinx)^5$$

Учитывая, что $i^2 = -1$, а $i^4 = 1$, и собирая действительные и мнимые члены получим, что

$$(cosx + isinx)^5 = ((cosx)^5 - 10(cosx)^3 \cdot (sinx)^2 + 5cosx \cdot (sinx)^4)) +$$

$$+i \cdot (5(cosx)^4 \cdot sinx - 10(cosx)^2 \cdot (sinx)^3 + (sinx)^5) = cos5x + i \cdot sin5x.$$

Исходя из понятия равенства двух комплексных чисел, приравняем мнимые части.

$$sin5x = 5(cosx)^4 \cdot sinx - 10(cosx)^2 \cdot (sinx)^3 + (sinx)^5$$

А это и дает решение данной задачи.

Практические задания по вариантам

Задание 1. Выполнить указанные действия.

n	Задание	n	Задание
1.	$(1+4i)\cdot(2-3i)+\frac{2i(5+2i)}{1+2i}$	2.	$\frac{(2-6i)\cdot i}{-4+2i}-(1-i)^2$
3.	$\frac{5+i}{-1-2i}+\frac{2+3i}{i}\cdot(2+i)$	4.	$\frac{(1-5i)\cdot(2+i)}{-1+i}-i^7(2-3i)$
5.	$(2-i)^2+\frac{3+i}{1-2i}$	6.	$\frac{4-5i^3}{1+i}-3i(5+2i)$
7.	$\frac{(1-2i)(1+i)}{3-i}-2i(2-i)$	8.	$\frac{5+3i}{1+3i}-i(2+3i)$
9.	$(3-2i)^2+\frac{9-8i}{4+2i}-i^5$	10.	$(-1+i)\cdot(3+2i)+\frac{i(6-4i)}{2+2i}$

Задание 2. Найти i^n, i^m.

Вариант	Задание	Вариант	Задание
1.	$n=3, m=8$	2.	$n=9, m=8$
3.	$n=4, m=11$	4.	$n=33, m=28$
5.	$n=13, m=81$	6.	$n=30, m=15$
7.	$n=23, m=38$	8.	$n=7, m=83$
9.	$n=15, m=24$	10.	$n=17, m=21$

Задание 3. Найти действительные решения уравнения.

n	Задание
1.	$(2-i)^2 x+(3-2i) y=-2i$
2.	$(5+2i) x+(1-3i) y=x+y+8-5i$
3.	$(1+4i) x+(5-2i) y=(3+i)x-(2+3i)y+3+7i$
4.	$(3+5i) x+(1-2i) y=(3-4i)i$
5.	$(5+i)^2 x-y=(1+i) x+9i$
6.	$(2+i) ix+(4-i) y=y+5i$
7.	$(5+i) x+(4-2i) y=ix-(2+i)y+4+i$
8.	$(2-i) x+(-5+2i) y=1-i$
9.	$(1+3i) x+(2-i)^2 y=(-1-4i)i$
10.	$(3-i) x+(2+2i) y=(1+2i)x-iy$

Задание 4. Дать геометрическое описание множества точек комплексной плоскости, удовлетворяющих указанному условию.

n	Задание	*n*	Задание
1.	$\lvert Im(\bar{z})\rvert > 1$	2.	$-1 \le \mathrm{Re}\,(z) \le 3$
3.	$0 < \arg z < \frac{\pi}{2}$	4.	$1 \le \lvert z-3\rvert \le 3$
5.	$\lvert z-i\rvert < 5$	6.	$\lvert z\rvert^2 = (\mathrm{Re}\,z)^2 + 9$
7.	$\mathrm{Im}\,(z-4i) > 0$	8.	$\lvert z+4i\rvert < 4$
9.	$\mathrm{Re}\,(z\cdot i) > 3$	10.	$\mathrm{Im}\,(z^2) \le 2$

Задание 5. Представить комплексные числа z_1 и z_2 в тригонометрической и экспоненциальной формах и изобразить точками на комплексной плоскости.

n	Задание	*n*	Задание
1.	$z_1 = 2 + 2\sqrt{3}\,i,$ $z_2 = 3 - 3i$	2.	$z_1 = -4\sqrt{3} + 4\,i,$ $z_2 = 0{,}5 + 0{,}5i$
3.	$z_1 = -3 + 3i,$ $z_2 = \sqrt{3} + i$	4.	$z_1 = -7 + 7\sqrt{3}\,i,$ $z_2 = 3\sqrt{3} + 3i$
5.	$z_1 = -\sqrt{3} - i\ ,\ z_2 = -5i$	6.	$z_1 = 4 - 4\sqrt{3}\,i\ ,\ z_2 = 0{,}5\,i$
7.	$z_1 = -2 - 2\,i,$ $z_2 = 1 + i\sqrt{3}$	8.	$z_1 = 6\sqrt{3} + 6i,$ $z_2 = -\sqrt{2} - \sqrt{2}\,i$
9.	$z_1 = -3 - 3\sqrt{3}\,i\ ,\ z_2 = -2i$	10.	$z_1 = -2 + 2\sqrt{3}\,i\ ,\ z_2 = -0{,}5i$

Задание 6. Для комплексных чисел z_1 и z_2, записанных в тригонометрической форме, из задания 4 выполнить указанные действия.

n	Задание	*n*	Задание
1.	$z_1^5 \cdot z_2,\ \frac{z_1}{z_2},\ \sqrt[4]{z_2}$	2.	$z_1 \cdot z_2,\ \frac{z_1^5}{z_2},\ \sqrt[3]{z_2}$
3.	$z_1 \cdot z_2^5,\ \frac{z_1}{z_2},\ \sqrt[3]{z_2^5}$	4.	$z_1 \cdot z_2,\ \frac{z_1}{z_2^5},\ \sqrt[3]{z_1}$
5.	$z_1^7 \cdot z_2,\ \frac{z_1}{z_2},\ \sqrt[4]{z_2}$	6.	$z_1 \cdot z_2,\ \frac{z_1^4}{z_2},\ \sqrt[4]{z_1}$
7.	$z_1 \cdot z_2,\ \frac{z_1^8}{z_2},\ \sqrt[4]{z_2}$	8.	$z_1^5 \cdot z_2,\ \frac{z_1}{z_2},\ \sqrt[4]{z_1^5}$
9.	$z_1 \cdot z_2,\ \frac{z_1^3}{z_2},\ \sqrt[5]{z_2}$	10.	$z_1 \cdot z_2,\ \frac{z_1}{z_2},\ \sqrt[4]{z_1^3}$

Задание 7. Решить задачу, используя формулу Муавра или формулы Эйлера.

n	Задание
1.	Выразить $\cos 3\varphi$ через $\cos\varphi$
2.	Выразить $\cos 4\varphi$ через $\cos\varphi$ и $\sin\varphi$
3.	Выразить $\sin 3\varphi$ через $\sin\varphi$
4.	Выразить $\sin 4\varphi$ через $\cos\varphi$ и $\sin\varphi$
5.	Выразить $tg3\varphi$ через $tg\varphi$
6.	Выразить $ctg3\varphi$ через $ctg\varphi$
7.	Вычислить сумму $\cos\varphi+\cos 2\varphi+\cos 3\varphi+...+\cos n\varphi$
8.	Вычислить сумму $\cos 2\varphi+\cos 4\varphi+...+\cos 2n\varphi$
9.	Вычислить сумму $\sin\varphi+\sin 2\varphi+\sin 3\varphi+...+\sin n\varphi$
10.	Вычислить сумму $\sin 2\varphi+\sin 4\varphi+...+\sin 2n\varphi$

РАБОТА № 2 (11) Элементы теории многочленов.

Цель: изучить кольца многочленов над кольцом и полем.

Вопросы, выносимые на практическое занятие.

1. Кольцо многочленов над кольцом.
2. Кольцо многочленов над полем.
3. Алгебраически замкнутые поля.
4. Схема Горнера.
5. Решение уравнений 3 степени (формулы Кардано).

Краткие теоретические сведения.

Над кольцом K рассмотрим множество $K[x]$ многочленов вида $p(x) = a_0 + a_1x + \cdots + a_nx^n$, где $a_i \in K$. Если $a_n \neq 0$, то $n = \deg(p(x))$ называется степенью многочлена. Операции сложения + и умножения · многочленов определяются естественным образом.

Тогда алгебра $< K[x], +, \cdot >$ называется кольцом многочленов от одной переменной над кольцом K.

ТЕОРЕМА. Кольцо многочленов удовлетворяет следующим свойствам:

1) Если кольцо K ассоциативно, то и кольцо $< K[x], +, \cdot >$ ассоциативно.
2) Если кольцо K коммутативно, то и кольцо <K[x],+,·> коммутативно.
3) Если в кольце K имеется единичный элемент, то и в кольце <K[x],+,·> имеется единичный элемент.
4) Если кольцо K без делителей 0, то и кольцо <K[x],+,·> без делителей 0.
5) Кольцо K является подкольцом кольца <K[x],+,·>.

Поле называется алгебраически замкнутым, если для любого многочлена над этим полем имеется хотя бы один корень из этого поля.

ТЕОРЕМА. Кольцо С комплексных чисел является алгебраически замкнуты полем.

В частности, как мы уже убедились в предыдущей работе, для любого не нулевого комплексного числа a уравнение $x^n = a$ имеет решение, т.к. из a извлекается корень степени n.

ТЕОРЕМА. Если в многочлене $p(x) = a_0 + a_1x + \cdots + a_nx^n$ над кольцом K, старший коэффициент $a_n \neq 0$ которого обратим, то для любого многочлена $g(x) = b_0 + b_1x + \cdots + b_mx^m$ существуют такие $q(x) = c_0 + c_1x + \cdots + c_sx^s$ и $r(x) = d_0 + d_1x + \cdots + d_kx^k$, что $k < n$ и выполняется равенство $g(x) = p(x) \cdot q(x) + r(x)$.

Заметим если K поле, то теорема деления многочленов с остатком выполняется в кольце многочленов от одной переменной над этим полем.

ТЕОРЕМА. Если многочлен $p(x) = a_0 + a_1x + \cdots + a_nx^n$ над полем действительных чисел имеет действительный корень $x=a$, то существует такой многочлен $g(x) = b_0 + b_1x + \cdots + x^{n-1}$, что выполняется равенство

$$p(x) = a_0 + a_1x + \cdots + a_nx^n = a_n \cdot (x - a) \cdot g(x).$$

Разделим многочлен степени n $P(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0$ на многочлен первой степени $(x - x_0)$, то получим многочлен степени n-1 $Q(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + ... + b_1x + b_0$ и числовой остаток r. Тогда имеет место равенство $P(x) = (x - x_0)Q(x) + r$. Деление многочленов можно проводить по правилам деления «уголком», ориентируясь на степени многочленов.

В этом случае деление можно осуществлять по схеме Горнера, которая позволяет найти коэффициенты многочлена $Q(x)$ и остаток *r*. В случае, если x_0 – корень многочлена $P(x)$, то остаток *r*=0. Она представлена в следующей таблице:

	a_n	a_{n-1}	a_{n-2}	$\cdots$	a_0
x_0	$b_{n-1} = a_n$	$b_{n-2} = a_{n-1} + x_0 \cdot b_{n-1}$	$b_{n-3} = a_{n-2} + x_0 \cdot b_{n-2}$	$\cdots$	r

ТЕОРЕМА. Если многочлен над полем действительных чисел имеет комплексный корень $z=a+ib$, то и сопряженное число $\bar{z}=a-ib$ является корнем этого многочлена.

ТЕОРЕМА. Если многочлен $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ с целыми коэффициентами имеет рациональный корень $\frac{p}{q}$, то число p есть делитель свободного члена a_0, а число q есть делитель старшего коэффициента a_n.

ТЕОРЕМА. Квадратное уравнение $a \cdot x^2 + b \cdot x + c = 0$ над полем комплексных чисел имеет два корня (быть может, совпадающих), которые находятся по формуле

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

ТЕОРЕМА. Уравнение третьей степени общего вида над полем $a \cdot x^3 + b \cdot x^2 + c \cdot x + d = 0$ заменой $x = z - \frac{b}{3a}$ приводится к каноническому виду $z^3 + p \cdot z + q = 0$.

ТЕОРЕМА. Если для канонического уравнения третьей степени $z^3 + p \cdot z + q = 0$ дискриминант кубического уравнения обозначить через

$\Delta = \frac{q^2}{4} + \frac{p^3}{27}$, то

1) для $\Delta > 0$ у канонического уравнения над полем действительных чисел один вещественный корень и два сопряженных комплексных;
2) для $\Delta > 0$ и $p^2 + q^2 \neq 0$ у уравнения один однократный и один двукратный корень;
3) для $\Delta \geq 0$ и $p^2 + q^2 = 0$ у уравнения один трехкратный вещественный корень;
4) для $\Delta < 0$ у уравнения три вещественных корня.

ТЕОРЕМА. Дискриминант и корни уравнения третьей степени над полем действительных чисел в канонической форме $z^3 + p \cdot z + q = 0$ обозначим буквами $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$, $\alpha = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$ и $\beta = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$, тогда решения уравнения находятся по формулам Кардано: $z_1 = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \alpha + \beta;$

$z_2 = -\frac{\alpha+\beta}{2} + i \cdot \frac{\alpha-\beta}{2} \cdot \sqrt{3};$

$z_3 = -\frac{\alpha+\beta}{2} - i \cdot \frac{\alpha-\beta}{2} \cdot \sqrt{3}.$

Примеры выполнения заданий.

Пример 1. Выполнить указанные действия над многочленами в кольце *R[x]*. $(\boldsymbol{x^2 - 2x + 1}) \cdot (\boldsymbol{x - 1})^3$**.**

$(\mathrm{x}^2 - 2\mathrm{x} + 1) \cdot (\mathrm{x} - 1)^3 = (\mathrm{x}^2 - 2\mathrm{x} + 1) \cdot (x^3 - 3x^2 + 3x - 1) =$

$= x^5 - 2x^4 + x^3 - 3x^4 + 6x^3 - 3x^2 + 3x^3 - 6x^2 + 3x - x^2 + 2x - 1 =$

$= x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1.$

Пример 2. Выполнить деление многочленов в кольце R[x]. Делимое $\boldsymbol{x^4 - 2x^2 - 3x + 1}$**, делитель** $\boldsymbol{x^2 + 1}$**.**

$\mathrm{x}^4 - 2\mathrm{x}^2 - 3\mathrm{x} + 1 \quad | \quad \mathrm{x}^2 + 1$

$$\begin{array}{ll} x^4+x^2 & x^2-3 \\ \hline -3x^2-3x+1 & \\ -3x^2-3 & \\ \hline -3x+4 & \end{array}$$

Таким образом имеем равенство:

$\mathrm{x}^4-2\mathrm{x}^2-3\mathrm{x}+1=(\mathrm{x}^2+1)\cdot(x^2-3)+(-3x+4)$.

Пример 3. Провести сокращение дробей над кольцом *R[x]*.

$$\frac{(\boldsymbol{x^3+1})(\boldsymbol{x^2-1})}{\boldsymbol{x^2+x}}$$

$$\frac{(\mathrm{x}^3+1)(\mathrm{x}^2-1)}{\mathrm{x}^2+\mathrm{x}}=\frac{(\mathrm{x}+1)\cdot(x^2-x+1)\cdot(\mathrm{x}-1)\cdot(\mathrm{x}+1)}{x\cdot(\mathrm{x}+1)}=\frac{(x^2-x+1)\cdot(\mathrm{x}-1)\cdot(\mathrm{x}+1)}{x}.$$

Пример 4. Пользуясь расширенным алгоритмом Евклида вычислить НОД и выразить его через исходные многочлены над кольцом *R[x]*. $\boldsymbol{x^4-2x^2-3x+1}$, $\boldsymbol{x^2+1}$.

Из примера 2 мы уже имеем равенство:

$\mathrm{x}^4-2\mathrm{x}^2-3\mathrm{x}+1=(\mathrm{x}^2+1)\cdot(x^2-3)+(-3x+4)$

Проведем деление предыдущего делителя на первый остаток.

$\mathrm{x}^2+1=(-3\mathrm{x}+4)\left(-\frac{1}{3}\mathrm{x}-\frac{4}{9}\right)+\frac{25}{9}$.

Из этого равенства следует, что исходные многочлены взаимно просты. На основании последнего равенства выразим 1 :

$1=\frac{9}{25}(\mathrm{x}^2+1)-\frac{9}{25}(-3\mathrm{x}+4)\left(-\frac{1}{3}\mathrm{x}-\frac{4}{9}\right)$.

А из первого равенства имеем

$(-3x+4)=(\mathrm{x}^4-2\mathrm{x}^2-3\mathrm{x}+1)-(\mathrm{x}^2+1)\cdot(x^2-3)$.

Подставим это представление остатка в предыдущее равенство.

$1=\frac{9}{25}(\mathrm{x}^2+1)-\frac{9}{25}\left((\mathrm{x}^4-2\mathrm{x}^2-3\mathrm{x}+1)-(\mathrm{x}^2+1)\cdot(x^2-3)\right)\left(-\frac{1}{3}\mathrm{x}-\frac{4}{9}\right)=$

$=\frac{9}{25}(\mathrm{x}^2+1)-\frac{9}{25}(\mathrm{x}^4-2\mathrm{x}^2-3\mathrm{x}+1)\left(-\frac{1}{3}\mathrm{x}-\frac{4}{9}\right)+\frac{9}{25}(\mathrm{x}^2+1)\cdot$

$(x^2-3)\left(-\frac{1}{3}\mathrm{x}-\frac{4}{9}\right)$.

Таким образом, получаем:

$$1 = (\mathrm{x}^4 - 2\mathrm{x}^2 - 3\mathrm{x} + 1) \cdot \left(\frac{3}{25}\mathrm{x} + \frac{4}{25}\right) + (\mathrm{x}^2 + 1) \cdot \frac{9}{25}((x^2 - 3)\left(-\frac{1}{3}\mathrm{x} - \frac{4}{9}\right) +$$

$$+1) = (\mathrm{x}^4 - 2\mathrm{x}^2 - 3\mathrm{x} + 1) \cdot \left(\frac{3}{25}\mathrm{x} + \frac{4}{25}\right) +$$

$$+(\mathrm{x}^2 + 1) \cdot \frac{9}{25}((x^2 - 3)\left(-\frac{1}{3}\mathrm{x} - \frac{4}{9}\right) + 1) =$$

$$= (\mathrm{x}^4 - 2\mathrm{x}^2 - 3\mathrm{x} + 1) \cdot \left(\tfrac{3}{25}\mathrm{x} + \tfrac{4}{25}\right) + (\mathrm{x}^2 + 1) \cdot (-\tfrac{3}{25}x^3 - \tfrac{4}{25}x^2 + \tfrac{9}{25}x + \tfrac{21}{25}).$$

В правильности найденного линейного представления легко проверить приведя подобные в правой части равенства.

Пример 5. Проверить имеются ли у многочлена над кольцом целых чисел рациональные корни. $f(x) = 5x^4 + 4x^3 + 4x^2 + 4x - 1$.

Согласно теории если есть корень $\frac{p}{q}$ многочлена $f(x)$, то число p есть делитель свободного члена a_0=1, а число q есть делитель старшего коэффициента a_n=5. Составим все такие дроби и проверим их на решение уравнения $f(x) = 0$.

$$\left\{-1, 1, -\frac{1}{5}, \frac{1}{5}\right\}$$

$$f(-1) = 5(-1)^4 + 4(-1)^3 + 4(-1)^2 + 4(-1) - 1 = 0$$

$$f(1) = 5(1)^4 + 4(1)^3 + 4(1)^2 + 4(1) - 1 \neq 0$$

$$f(-\frac{1}{5}) = 5(-\frac{1}{5})^4 + 4(-\frac{1}{5})^3 + 4(-\frac{1}{5})^2 + 4\left(-\frac{1}{5}\right) - 1 \neq 0$$

$$f(\frac{1}{5}) = 5(\frac{1}{5})^4 + 4(\frac{1}{5})^3 + 4(\frac{1}{5})^2 + 4\left(\frac{1}{5}\right) - 1 = 0$$

Таким образом, у данного многочлена два рациональных корня -1 и $\frac{1}{5}$.

Пример 6. Найти корни многочлена второй степени (с комплексными коэффициентами) на множестве комплексных чисел и разложить его на множители. $Q(x) = ix^2 + 2ix + x + 13i + 1$ **.**

Так как многочлен второй степени имеет в множестве комплексных чисел ровно 2 корня, то его разложение $Q(x)=a_2x^2+a_1x+a_0$ на множители имеет вид:

$$Q(x)=a_2(x-x_1)(x-x_2).$$

Найдем корни многочлена, решив соответствующее квадратное уравнение.

$$ix^2+2ix+x+13i+1=0$$
$$ix^2+(2i+1)x+(13i+1)=0$$
$$D=(2i+1)^2-4i(13i+1)=4i^2+4i+1-52i^2-4i=-4+1+52=49$$
$$x_1=\frac{-(2i+1)+7}{2i}=\frac{-2i+6}{2i}=-1-3i,$$
$$x_2=\frac{-(2i+1)-7}{2i}=\frac{-2i-8}{2i}=-1+4i$$

Следовательно, имеем:

$$Q(x)=i(x-(-1-3i))(x-(-1+4i)=i\ (x+1+3i)(x+1-4i)$$

Правильность решения следует проверить раскрытием скобок и приведением подобных.

$i(x+1+3i)(x+1-4i)=ix^2+i(1+3i)x+i(1-4i)x+$
$+i(1+3i)(1-4i)=ix^2+(i-3)x+(i+4)x+i+3i^2-4i^2-12i^3=$
$ix^2+(2i+1)x+13i+1.$

Пример 7. Найти корни многочлена с действительными коэффициентами $P(x)=3x^4-4x^3+x^2+6x-2$. Над множеством комплексных чисел разложить $P(x)$ на множители.

Найдем рациональные корни данного многочлена (если они существуют). Для этого выпишем все делители свободного члена и старшего коэффициента.

Делители $a_0=-2:\pm1,\pm2$.

Делители $a_n=3:\pm1,\pm3$.

Следовательно, возможные рациональные корни многочлена:

$$\pm 1, \pm \frac{1}{3}, \pm 2, \pm \frac{2}{3}.$$

Проверить, является ли число корнем многочлена, можно непосредственной подстановкой, но удобнее это сделать, воспользовавшись схемой Горнера.

Составим схему Горнера для рассматриваемого примера и проверим, какой из возможных рациональных корней действительно является корнем многочлена $P(x) = 3x^4 - 4x^3 + x^2 + 6x - 2$.

	3	-4	1	6	-2
$x_0 = 1$	3	$-4+1\cdot 3 = = -1$	$1+1\cdot(-1) = = 0$	$6+1\cdot 0 = = 6$	$-2+1\cdot 6 = = 4$
$x_0 = -1$	3	$-4+(-3) = = -7$	$1+7 = = 8$	$6+(-8) = = -2$	$-2+2 = = 0$

Как видно из таблицы, число $x_0 = 1$ не является корнем многочлена, так как остаток $r \neq 0$. (Кстати, он равен значению многочлена в точке $x_0 = 1$, то есть $r = P(1)$).

Число $x_0 = -1$ является корнем многочлена, так как $r = 0$.

Следовательно, разделив исходный многочлен на $x + 1$, получаем равенство

$$P(x) = 3x^4 - 4x^3 + x^2 + 6x - 2 = (x+1)(3x^3 - 7x^2 + 8x - 2).$$

Остальные рациональные корни можем искать, используя уже многочлен меньшей степени: $Q(x) = 3x^3 - 7x^2 + 8x - 2$.

Так как число $x_0 = 1$ не является корнем исходного многочлена, то оно не может быть и корнем многочлена $Q(x)$.

Проверим остальные возможные корни. При этом число $x_0 = -1$ может еще раз оказаться корнем (тогда его кратность в исходном многочлене будет >1).

	3	-7	8	-2
$x_0 = -1$	3	-10	18	-20
$x_0 = \frac{1}{3}$	3	-6	6	0

Число $x_0 = \frac{1}{3}$ является корнем, поэтому имеют место равенства:

$Q(x) = 3x^3 - 7x^2 + 8x - 2 = (x - 1/3)(3x^2 - 6x + 6)$, т.е.

$P(x) = (x+1)(x - 1/3)(3x^2 - 6x + 6)$.

Далее рассмотрим многочлен $3x^2 - 6x + 6$. Можем и дальше, использовать схему Горнера, но так как заранее неизвестно, есть ли еще рациональные корни и так как полученный многочлен является многочленом второй степени, можем решить соответствующее уравнение как обычное квадратное уравнение.

$3x^2 - 6x + 6 = 0$

$x^2 - 2x + 2 = 0$

$D = (-2)^2 - 4 \cdot 2 = -4$

$x = \frac{2 \pm 2i}{2} = 1 \pm i$

Итак, исходный многочлен имеет 4 корня: $-1, \frac{1}{3}, 1+i, 1-i$.

Разложение исходного многочлена на множители имеет вид:

$$P(x) = 3x^4 - 4x^3 + x^2 + 6x - 2 = 3(x+1)(x - \frac{1}{3})(x - (1+i))(x - (1-i)).$$

Пример 8. Составить многочлен с действительными коэффициентами четвертой степени, если $x = -1 + 2i$ – корень многочлена кратности 2.

Так как по условию многочлен имеет действительные коэффициенты, то его комплексные корни являются сопряженными, причем одной и той же кратности.

$x=-1+2i$ – корень кратности 2 , поэтому $\bar{x}=-1-2i$ также корень кратности 2.

Следовательно, искомый многочлен может быть представлен в виде

$$M(x)=((x-(-1+2i))^2(x-(-1-2i))^2=$$

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

$$=\left((x+1)^2-4i^2\right)^2=\left(x^2+2x+1-4i^2\right)^2=\left(x^2+2x+1+4\right)^2=\left(x^2+2x+5\right)^2=$$

$$=x^4+4x^3+4x^2+10x^2+20x+25=x^4+4x^3+14x^2+20x+25.$$

Задание 9. Решить уравнение третьей степени на множестве комплексных чисел, используя формулы Кардано. $x^3-3x^2-6x+4=0$.

Приведем данное уравнение к каноническому виду заменой

$x=z-\frac{b}{3a}=z-\frac{-3}{3\cdot1}=z+1$.

$(z+1)^3-3(z+1)^2-6(z+1)+4=0.\ z^3-9z-4=0.$

Вычислим дискриминант этого уравнения с действительными коэффициентами.

$$\Delta=\frac{q^2}{4}+\frac{p^3}{27}=\frac{(-4)^3}{4}+\frac{(-9)^3}{27}=4-27=-23.$$

Т.к. $\Delta<0$, то данное кубическое уравнение имеет три вещественных корня. Для их нахождения необходимо сначала вычислить вспомогательные величины α и β.

$$\alpha=\sqrt[3]{-\frac{q}{2}-\sqrt{\frac{q^2}{4}+\frac{p^3}{27}}}=\sqrt[3]{-\frac{q}{2}-\sqrt{\Delta}}=\sqrt[3]{-\frac{(-4)}{2}-\sqrt{-23}}=\sqrt[3]{2-i\sqrt{23}}.$$

Для вычисления основного значения этого корня переведем подкоренное выражение в тригонометрическую форму записи комплексного числа.

$$\rho=\sqrt{2^2+(\sqrt{23})^2}=\sqrt{4+23}=\sqrt{27}.$$

$$\varphi=arctg\left(\frac{2}{-\sqrt{23}}\right)=-arctg\left(\frac{2}{\sqrt{23}}\right).$$

$$\alpha = \rho(cos\varphi + isin\varphi) =$$

$$= \sqrt{27}\left(\cos\left(-arctg\left(\frac{2}{\sqrt{23}}\right)\right) + i \cdot \sin\left(-arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right) =$$

$$=\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right) - i \cdot \sin\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right).$$

$$\beta = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \sqrt[3]{-\frac{q}{2} + \sqrt{\Delta}} = \sqrt[3]{-\frac{(-4)}{2} + \sqrt{-23}} = \sqrt[3]{2 + i\sqrt{23}} =$$

$$=\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right) + i \cdot \sin\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right).$$

Тогда имеем $z_1 = \alpha + \beta = \sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right) - i \cdot \sin\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right) + +\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right) + i \cdot \sin\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right) =$

$$= 2\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right);$$

$$z_2 = -\frac{\alpha+\beta}{2} + i \cdot \frac{\alpha-\beta}{2} \cdot \sqrt{3} = -\frac{2\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right)}{2} + i \cdot \frac{-2i\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right)}{2}\sqrt{3} = -\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right) + \sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right)\sqrt{3} =$$

$$= \sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right) \cdot (\sqrt{3} - 1);$$

$$z_3 = -\frac{\alpha + \beta}{2} - i \cdot \frac{\alpha - \beta}{2} \cdot \sqrt{3} =$$

$$= -\frac{2\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right)}{2} - i\frac{-2i\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right)}{2}\sqrt{3} =$$

$$= \sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right) \cdot (-\sqrt{3} - 1).$$

Тогда для исходного уравнений имеем следующие решения:

$$x_1 = z_1 + 1 = 1+2\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right).$$

$$x_2 = z_2 + 1 = 1+\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right)\cdot(\sqrt{3}-1).$$

$$x_3 = z_3 + 1 = 1+\sqrt{27}\left(\cos\left(arctg\left(\frac{2}{\sqrt{23}}\right)\right)\right)\cdot(-\sqrt{3}-1).$$

Практические задания по вариантам

Задание 1. Выполнить указанные действия над многочленами в кольце *R[x]*.

Вариант 1. $(x^3+2x-1)\cdot(x-5)$; **Вариант 2.** $(x^3+2x-1)^2\cdot(x-5)$;

Вариант 3. $(x^3+2x-1)\cdot(x-5)^3$; **Вариант 4.** $(x^3+2x-1)^2\cdot(x-5)^2$;

Вариант 5. $(x^3+2x-1)\cdot(x-5)^2$; **Вариант 6.** $(x^3+2x-1)^2\cdot(x-5)^3$;

Вариант 7. $(x^3+2x-1)^3\cdot(x-5)^2$; **Вариант 8.** $(x^3+2x-1)\cdot(x-5)^4$;

Вариант 9. $(x^3+2x-1)^2\cdot(x-5)^4$; **Вариант 2.** $(x^3+2x-1)^3\cdot(x-5)$.

Задание 2. Выполнить деление многочленов в кольце R[x].

Вариант	Делимое	Делитель
1	x^4-x^2+1	$x-5$
2	x^4+x^2+1	$x+2$
3	x^4-x^2-1	$x+5$
4	x^4-2x^2+1	x^2-2
5	x^4+3x^2+1	$3x-2$
6	x^4-3x^2+1	$3x+2$
7	$4x^4+3x^2+1$	$2x+5$
8	$4x^4-3x^2+1$	$2x-5$
9	x^4-3x^2-1	x^2+1
10	x^4+3x^2-1	x^2-1

Задание 3. Провести сокращение дробей над кольцом *R[x]*.

Вариант 1. $\frac{(x^3+1)(x^2+1)}{x^2+x}$**.** **Вариант 2.** $\frac{(x^3-1)(x^2+1)}{x^2+x}$**.**

Вариант 3. $\frac{(x^3+1)(x^2-1)}{x^2+x}$**.** **Вариант 4.** $\frac{(x^3+1)(x^2-1)}{x^2-x}$**.**

Вариант 5. $\frac{(x^3-1)(x^2-1)}{x^2-x}$**.** **Вариант 6.** $\frac{(x^3-1)(x^2+1)}{x^2-x}$**.**

Вариант 7. $\frac{(x^3+1)(x^3-1)}{x^2-x}$**.** **Вариант 8.** $\frac{(x^3+1)(x^3-1)}{x^2+x}$**.**

Вариант 9. $\frac{(x^3+1)(x^2-1)}{x^3-x}$**.** **Вариант 10.** $\frac{(x^3-1)(x^2-1)}{x^3-x}$**.**

Задание 4. Пользуясь расширенным алгоритмом Евклида вычислить НОД и выразить его через исходные многочлены над кольцом *R[x]*.

Вариант	**Многочлен $f(x)$.**	**Многочлен $g(x)$.**
1	$4x^4-3x^2+1$	x^2+1
2	x^4-x^2+1	x^2-1
3	x^4+x^2+1	x^2+2
4	x^4-x^2-1	x^2-2
5	x^4-2x^2+1	x^2+1
6	x^4+3x^2+1	x^2-1
7	x^4-3x^2+1	x^2+2
8	$4x^4+3x^2+1$	x^2-2
9	$4x^4-3x^2+1$	$2x^2-1$
10	x^4-3x^2-1	$2x^2+2$

Задание 5. Проверить имеются ли у многочлена над кольцом целых чисел рациональные корни.

n	Задание
1.	$P(x)=-3x^4-x^3+6x^2+14x+4$
2.	$P(x)=-2x^4-5x^3+x^2+11x-5$
3.	$P(x)=3x^4+2x^3+8x^2-18x+5$
4.	$P(x)=2x^4+11x^3+19x^2-19x-13$
5.	$P(x)=3x^4-10x^3+15x^2-10x+2$

6.	$P(x) = 2x^4 + 11x^3 + 23x^2 + 19x + 5$
7.	$P(x) = -3x^4 + 4x^3 - 4x^2 + 4x - 1$
8.	$P(x) = 3x^4 + 8x^3 + 18x^2 + 8x - 5$
9.	$P(x) = 2x^4 + 19x^3 + 41x^2 - 36x - 26$
10.	$P(x) = 3x^4 + 4x^3 + 25x^2 - 22x - 10$

Задание 6. Найти корни многочлена второй степени (с комплексными коэффициентами) на множестве комплексных чисел и разложить его на множители.

n	Задание
1.	$Q(x) = x^2 - 2x - 4ix + 6 + 4i$
2.	$Q(x) = x^2 + x - 6ix - 11 - 3i$
3.	$Q(x) = ix^2 + 2x - 5ix + 5i - 5$
4.	$Q(x) = x^2 - 4x + 2ix + 7 - 4i$
5.	$Q(x) = x^2 - 2x + 2ix + 9 - 2i$
6.	$Q(x) = x^2 - 6x - ix + 15 + 3i$
7.	$Q(x) = ix^2 - 4ix + 4x - i - 8$
8.	$Q(x) = x^2 - 6x - ix + 11 + 3i$
9.	$Q(x) = x^2 - 7x + 2ix + 9 - 7i$
10.	$Q(x) = x^2 - 4x + 4ix + 9 - 8i$

Задание 7. Найти корни многочлена четвертой степени (с действительными коэффициентами) на множестве комплексных чисел и разложить его на множители.

n	Задание
1.	$P(x)=2x^4+9x^3+13x^2+x-5$
2.	$P(x)=3x^4-4x^3+x^2+6x-2$
3.	$P(x)=2x^4+5x^3+15x^2-35x+13$
4.	$P(x)=3x^4+2x^3-x^2-6x+2$
5.	$P(x)=5x^4-6x^3+6x^2-6x+1$
6.	$P(x)=2x^4+x^3-x^2-4x+2$
7.	$P(x)=2x^4+x^3+5x^2-13x+5$
8.	$P(x)=-3x^4-x^3+6x^2+14x+4$
9.	$P(x)=2x^4+9x^3+9x^2-33x+13$
10.	$P(x)=5x^4+4x^3-x^2-10x+2$

Задание 8. Составить многочлен по заданным условиям.

<table>
<tr><th>n</th><th>Задание</th></tr>
<tr><td>1.</td><td>Многочлен с действительными коэффициентами третьей степени, если $x_1 = 2{,}5$ и $x_2 = -3 + i$ – два из его корней</td></tr>
<tr><td>2.</td><td>Многочлен с действительными коэффициентами четвертой степени, если $x_1 = 3$ – корень многочлена кратности 2 и $x_2 = 2 + i$ – один из других корней многочлена</td></tr>
<tr><td>3.</td><td>Многочлен, если все его корни и соответствующие их кратности приведены в таблице:
<table>
<tr><td>корень</td><td>1</td><td>-2</td><td>$-1+i$</td></tr>
<tr><td>кратность</td><td>2</td><td>1</td><td>1</td></tr>
</table></td></tr>
<tr><td>4.</td><td>Многочлен с действительными коэффициентами четвертой степени, если $x_1 = i$ – корень многочлена кратности 2</td></tr>
<tr><td>5.</td><td>Многочлен с действительными коэффициентами третьей степени, если $x_1 = -4$ и $x_2 = 1 + 2i$ – два из его корней</td></tr>
<tr><td>6.</td><td>Многочлен, если все его корни и соответствующие их кратности приведены в таблице:
<table>
<tr><td>корень</td><td>3</td><td>-1</td><td>i</td></tr>
<tr><td>кратность</td><td>2</td><td>2</td><td>1</td></tr>
</table></td></tr>
<tr><td>7.</td><td>Многочлен с действительными коэффициентами четвертой степени, если $x_1 = 1 - 2i$ и $x_2 = 2 - i$ – два из его корней</td></tr>
<tr><td>8.</td><td>Многочлен с действительными коэффициентами четвертой степени, если $x_1 = 1 + 2i$ – корень многочлена кратности 2</td></tr>
<tr><td>9.</td><td>Многочлен с действительными коэффициентами третьей степени, если $x_1 = -0{,}5$ и $x_2 = 6 - i$ – два из его корней</td></tr>
<tr><td>10.</td><td>Многочлен, если все его корни и соответствующие их кратности приведены в таблице:
<table>
<tr><td>корень</td><td>1</td><td>1+i</td><td>1-i</td></tr>
<tr><td>кратность</td><td>3</td><td>1</td><td>1</td></tr>
</table></td></tr>
</table>

Задание 9. Решить уравнение третьей степени на множестве комплексных чисел, используя формулы Кардано.

n	Задание	n	Задание
1.	$x^3-3x^2-6x+20=0$	2.	$x^3+6x-2=0$
3.	$x^3+3x-2i=0$	4.	$x^3+18x+15=0$
5.	$x^3-6x-2=0$	6.	$x^3-6ix+4(1-i)=0$
7.	$x^3+3x^2-15x-59=0$	8.	$x^3-3x^2-6x-4=0$
9.	$x^3+3x^2-6x+4=0$	10.	$x^3+9x^2+21x+5=0$

Список литературы

1. Веселова, Л. В. Алгебра и теория чисел: Учебное пособие / Л. В. Веселова, О. Е. Тихонов. – Казань: Казанский национальный исследовательский технологический университет, 2014. – 107 с. – ISBN 978-5-7882-1636-2.
2. Ларин, С. В. Алгебра и теория чисел. Группы, кольца и поля: Учебное пособие / С. В. Ларин. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2020. – 1 с. – (Высшее образование). – ISBN 978-5-534-05567-2.
3. Швед, Е. А. Практикум по алгебре: элементы теории чисел / Е. А. Швед, В. А. Федоров. – Омск: Омский государственный университет путей сообщения, 2022. – 39 с.
4. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел: учебное пособие / Л. Б. Шнеперман; Л. Б. Шнеперман. – 3-е изд., стер.. – Санкт-Петербург [и др.]: Лань, 2008. – (Учебники для вузов. Специальная литература). – ISBN 978-5-8114-0885-6.
5. Виноградов, И. М. Основы теории чисел [Текст]: учебное пособие / И. М. Виноградов. - Изд. 12-е, стер. - СПб. [и др.]: Лань, 2009. -176 с.
6. Виноградов, И. М. Элементы высшей математики: аналитическая геометрия, дифференциальное исчисление: учебник для студентов высших учебных заведений, обучающихся по инженерно-техническим специальностям / И. М. Виноградов; И. М. Виноградов. – Москва: Дрофа, 2010. – 319 с. – (Высшее образование. Современный учебник). – ISBN 978-5-358-06101-9.
7. Гончаренко, В. М. Элементы высшей математики / В. М. Гончаренко, Л. В. Липагина, А. А. Рылов. – МОСКВА: Компания КноРус, 2019. – 364 с. – ISBN 978-5-406-06878-6.

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
Факультет: «Фундаментальной и прикладной информатики»
Кафедра: «Информационной безопасности»

УТВЕРЖДАЮ
Проректор по учебной работе
_____О.Г.Локтионова
«___» _____2024 г.

Эллиптические кривые

Методические рекомендации
для выполнения практических заданий по дисциплинам
«Элементы алгебры и теории чисел» и «Алгебра и теория чисел»
Направления подготовки: 10.03.01 «Информационная безопасность»; 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Курск – 2024

УДК 511+512(075.8)
Составители:
д. ф-м. н., профессор В.П. Добрица
к.т.н., Е.А. Кулешова
к.т.н., доцент Ю.А. Халин

Рецензент

кандидат технических наук, доцент кафедры
вычислительной техники А.В. Киселев

Эллиптические кривые : методические рекомендации для выполнения практических заданий / Юго-Зап. гос. ун-т; сост.: В.П. Добрица, Е.А. Кулешова, Ю.А. Халин. – Курск, 2024. – 35 с. – Библиогр.: с. 35.

В методических указания описываются основы теории эллиптических кривых. Изложены краткие теоретические сведения, приведены примеры решения задач, а также задачи для самостоятельного решения.

Методические рекомендации предназначены для студентов, обучающихся по направлениям подготовки 10.03.01 «Информационная безопасность» и 02.03.03 «Математическое обеспечение и администрирование информационных систем».

Текст печатается в авторской редакции

Подписано в печать . Формат 60x84 1/16.
Усл.печ. л. 1,34. Уч.-изд. л. 1,21. Тираж 100 экз. 80
Заказ. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

В данных методических рекомендациях изложены материалы по разделу «Эллиптические кривые» курсов «Элементы алгебры и теории чисел» и «Алгебра и теория чисел».

Рассмотрены следующие темы: Группы по сложению точек на эллиптических кривых над полем действительных чисел, группы по сложению точек на эллиптических кривых над конечными полями.

По теме представлены:

1) краткие теоретические положения;
2) перечень вопросов, выносимых на практическое занятие;
3) примеры решения типовых задач, выносимых на практическое занятие;
4) задачи, выносимые на самостоятельную работу студентов.

Данные методические рекомендации предназначены для проведения практических занятий по дисциплинам «Элементы алгебры и теории чисел» и «Алгебра и теория чисел» для студентов Юго-Западного государственного университета направлений подготовки: информационная безопасность, математическое обеспечение и администрирование информационных систем.

По изложенным в данных методических рекомендациях материалам можно рекомендовать преподавателю проведение 4-х часов практических занятий по следующему плану:

- Группы по сложению точек на эллиптических кривых над полем действительных чисел. (2 часа)
- Группы по сложению точек на эллиптических кривых над конечными полями. (2 часа)

При выполнении практических заданий в каждой задаче выберете задание из своего варианта. Вариант определяется по последней цифре номера зачетной книжки. Отчет по работе должен содержать решения задач и выводы с полным их обоснованием. Отчет по работе оформить на листах формата А4 в редакторе WORD. На титульном листе должно быть указано: университет, факультет, кафедра, предмет, номер практического занятия, вариант, группа, исполнитель, проверяющий.

РАБОТА № 1 (12) Группы по сложению точек на эллиптических кривых над полем действительных чисел.

Цель: изучить понятие эллиптической кривой над полем действительных чисел, геометрическое и алгебраическое сложение точек эллиптической кривой, проверка свойств группы для точек эллиптической кривой по сложению.

Вопросы, выносимые на практическое занятие.

1. Уравнения эллиптических кривых над полем действительных чисел.
2. Геометрическое сложение точек на эллиптических кривых.
3. Алгебраическое сложение точек на эллиптических кривых.
4. Проверка аксиом группы множества точек эллиптической кривой относительно их сложения.
5. Логарифмирование на эллиптических кривых.

Краткие теоретические сведения.

Тем, кто знаком с криптографией с открытым ключом, наверно известны аббревиатуры **ECC**, **ECDH** и **ECDSA**. Первая — это сокращение от Elliptic Curve Cryptography (криптография на эллиптических кривых), остальные — это названия основанных на ней алгоритмов. Сегодня криптосистемы на эллиптических кривых используются в TLS, PGP и SSH, важнейших технологиях, на которых базируются современный веб и мир ИТ.

Эллиптические кривые

Для нас достаточно того, что эллиптическая кривая — это просто множество точек, описываемое уравнением:

$$y^2 = x^3 + ax + b$$

где $4a^3 + 27b^2 \neq 0$, (это необходимо, чтобы исключить особые кривые). Приведённое выше уравнение называется *обычной формулировкой Вейерштрасса* для эллиптических кривых.

Различные формы эллиптических кривых ($b = 1$, а изменяется от 2 до -3).

Виды особенностей: слева — кривая с точкой возврата (каспом) ($y^2 = x^3$). Справа — кривая с самопересечением ($y^2 = x^3 - 3x + 2$). Оба этих примера не являются полноценными эллиптическими кривыми.

Эллиптические кривые симметричны относительно оси OX.

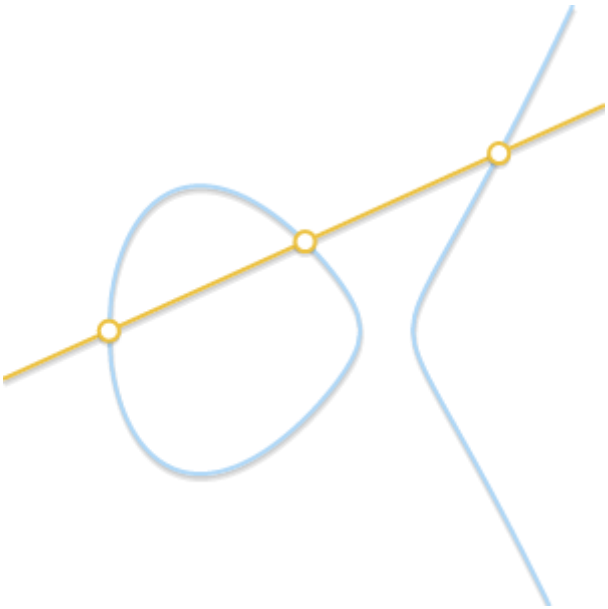
Также понадобится, чтобы частью кривой являлась бесконечно удалённая точка (также известная как идеальная точка). С этого момента мы будем обозначать бесконечно удалённую точку символом 0 (ноль).

Определение эллиптической кривой можно уточнить следующим образом:

$$\{(x, y) \in R^2 | y^2 = x^3 + ax + b, 4a^3 + 27b^2 \neq 0 \} \cup \{0\}$$

Определим группу для эллиптических кривых. А именно:

- элементы группы являются точками эллиптической кривой;
- единичный элемент — это бесконечно удалённая точка *0*;
- обратная величина точки *P* — это точка, симметричная относительно оси *OX*;
- сложение задаётся следующим правилом: сумма трёх ненулевых точек *P*, *Q* и *R*, лежащих на одной прямой, будет равна *P+Q+R=0*.

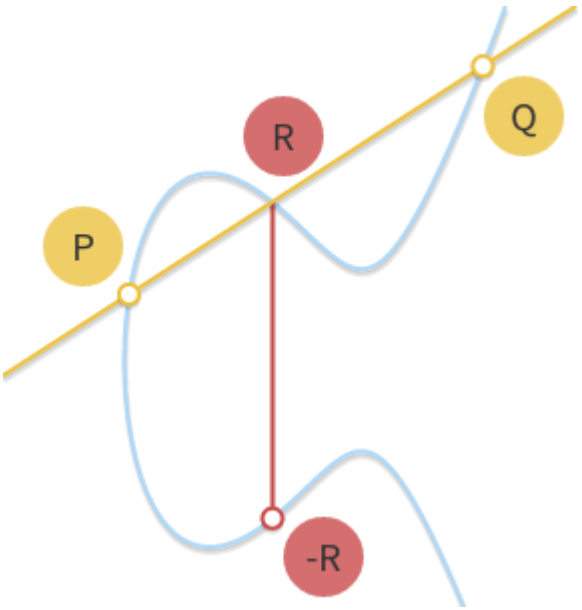


Сумма трёх точек, находящихся на одной прямой, равна 0.

Стоит учесть, что в последнем правиле нам требуются только три точки на одной прямой, и порядок расположения этих трёх точек не важен. Это значит, что если три точки *P*, *Q* и *R* лежат на одной прямой, то *P+(Q+R)= Q +(P + R)= P+(R + Q)=...=0*. Таким образом мы интуитивно показали, что наш оператор + обладает свойствами ассоциативности и коммутативности, т.е. мы находимся в абелевой группе.

Геометрическое сложение

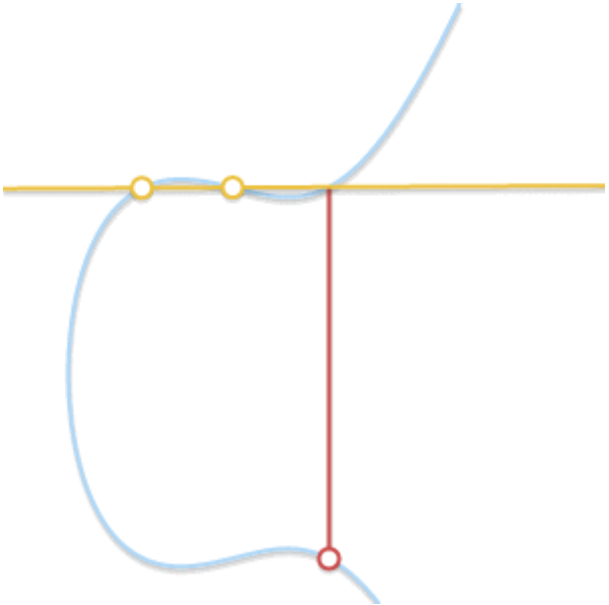
Благодаря тому, что мы находимся в абелевой группе, то можем записать *P+Q+R=0* как *P+Q=-R* . Это уравнение в такой форме позволяет нам вывести геометрический способ вычисления суммы двух точек *P* и *Q*: если мы проведём линию, проходящую через *P* и *Q*, эта прямая пересечёт третью точку кривой *R* (это подразумевается, потому что *P*, *Q* и *R* находятся на одной прямой). Если мы возьмём обратную величину этой точки *-R*, мы найдём сумму *P+Q*.



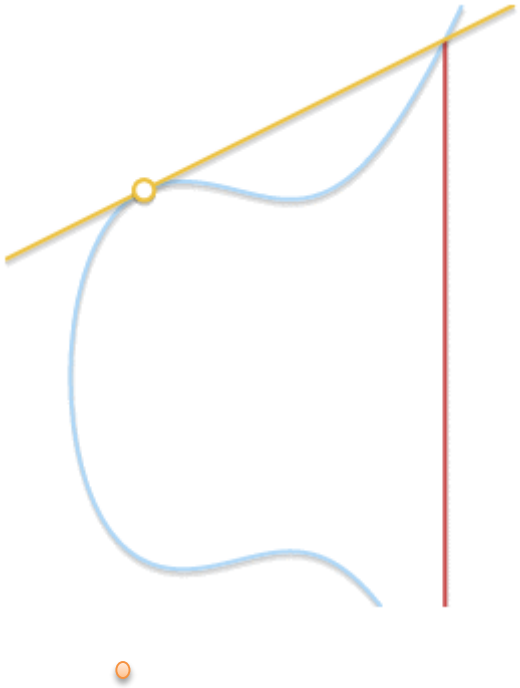
Проводим прямую через P и Q. Прямая пересекает третью точку R. Симметричная ей точка -R является результатом P+Q .

Геометрический способ работает, но требует усовершенствования. В частности, нам нужно ответить на несколько вопросов:

- Что если $P=0$ или $Q=0$? Разумеется, мы не сможем провести прямую (0 не находится на плоскости XOY). Но поскольку мы определили 0 как единичный элемент, $P+0= P$ и $0+Q= Q$ для любой P и любой Q.
- Что если $P= -Q$? В этом случае прямая, проходящая через две точки, вертикальна, и не пересекает третью точку. Но если P является обратной величиной Q , то $P+Q= P+(- P)=0$ из определения обратной величины.
- Что если $P= Q$? В этом случае через точку проходит бесконечное количество прямых. Здесь всё становится немного сложнее. Но представим, что точка $P\neq Q'$. Что произойдёт, если мы заставим Q' стремиться к P, всё больше приближаясь к ней?



При сближении двух точек проходящая через них прямая становится касательной к кривой.

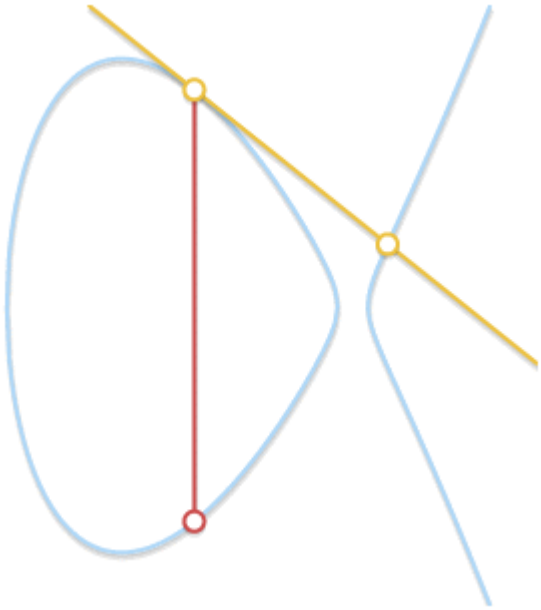


Поскольку Q' стремится к P, прямая, проходящая через P и Q' становится касательной к кривой. В свете этого мы можем сказать, что $P+P=-R$, где R — это точка пересечения между кривой и касательной к кривой в точке P .

- Что если $P \neq Q$, но третьей точки R нет? В этом случае ситуация похожа на предыдущую. На самом деле, в этой ситуации прямая, проходящая через P и Q, является касательной к кривой.

Предположим, что P является точкой касания. В предыдущем случае мы записали P+ P=-R. В данном случае R= Q. Это уравнение теперь превращается в P+ Q =-P . С другой стороны, если бы точкой касания была Q, то правильным было бы уравнение P+ Q =- Q.

Геометрический способ теперь полон и учитывает все случаи. С помощью карандаша и линейки можно выполнить сложение всех точек любой эллиптической кривой. Имеется визуальный инструмент на HTML5/JavaScript (https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html), созданный для вычисления сумм точек эллиптических кривых.



Алгебраическое сложение

Для того, чтобы сложением точек занимался компьютер, нужно превратить геометрический способ в алгебраический. Преобразование вышеизложенных правил в набор уравнений может казаться простым, но на самом деле оно довольно утомительно, потому что требует решения кубических уравнений. Поэтому изложим только результаты.

Для начала давайте избавимся от самых раздражающих тупиковых ситуаций. Мы уже знаем, что $P+(-P)=0$, и знаем, что $P+0=0+P=P$. Поэтому в наших уравнениях мы будем избегать этих двух случаев и рассмотрим только две ненулевые несимметричные точки $P = (x_P, y_P)$ и $Q = (x_Q, y_Q)$.

Если P и Q не совпадают ($x_P \neq x_Q$), то проходящая через них прямая имеет коэффициент наклон:

$$m = \frac{y_P - y_Q}{x_P - x_Q}$$

Пересечение этой прямой с эллиптической кривой — это третья точка $R = (x_R, y_R)$:

$$x_R = m^2 - x_P - x_Q$$

$$y_R = y_P + m(x_R - x_P)$$

или, аналогично:

$$y_R = y_Q + m(x_R - x_Q)$$

Поэтому $(x_P, y_P) + (x_Q, y_Q) = (x_R, -y_R)$ (обратите внимание на знаки и помните, что $P + Q = -R$).

Можно поэкспериментировать с примером: согласно визуальному инструменту (https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html).

Заметьте, что эти уравнения работают даже в случае, когда **точка P или Q является точкой касания**. Давайте проверим на $P = (-1,4)$ и $Q = (1,2)$.

$$m = \frac{y_P - y_Q}{x_P - x_Q} = \frac{4-2}{-1-1} = -1$$
$$x_R = m^2 - x_P - x_Q = (-1)^2 - (-1) - 1 = 1$$

$$y_R = y_P + m(x_R - x_P) = 4 + (-1)\big(1 - (-1)\big) = 2$$

Мы получили результат $P + Q = (1, -2)$, который совпадает с результатом, получаемым в визуальном инструменте (https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html?px=-1&py=4&qx=1&qy=2).

К случаю $P = Q$ нужно относиться немного иначе: уравнения для x_R и y_R остаются теми же, но с учётом того, что $x_P = x_Q$ нам придётся использовать для коэффициента наклона другое уравнение:

$$m = \frac{3x_P^2 + a}{2y_P}$$

Заметьте, что, как и можно было ожидать, это выражение для m является первой производной от выражения функции:

$$y_P = \pm\sqrt{x_P^3 + ax + b}$$

Чтобы доказать правильность этого результата, достаточно убедиться, что R принадлежит кривой и что прямая, проходящая через P и R, имеет только два пересечения с кривой. Не будем доказывать это, а вместо этого разберём пример: $P = Q = (1,2)$.

$$m = \frac{3x_P^2 + a}{2y_P} = \frac{3 \cdot 1^2 - 7}{2 \cdot 2} = -1$$
$$x_R = m^2 - x_P - x_Q = (-1)^2 - 1 - 1 = -1$$

$$y_R = y_P + m(x_R - x_P) = 2 + (-1) \cdot (-1 - 1) = 4$$

Что даёт нам $P + P = -R = (-1, -4)$.

Хотя процедура получения результатов очень утомительна, наши уравнения довольно кратки. Всё это благодаря обычной формулировке Вейерштрасса!

Скалярное умножение

Кроме сложения, мы можем определить и другую операцию: скалярное умножение, то есть: $n \cdot P = \underbrace{P + P + \cdots + P}_{n \text{ раз}}$

где n — натуральное число. Имеется визуальный инструмент и для скалярного умножения.

При записи в такой форме очевидно, что вычисление $n \cdot P$ требует n сложений. Если P состоит из k десятичных разрядов, то алгоритм будет иметь сложность $O(2^k)$, что не очень хорошо. Но существуют и более быстрые алгоритмы.

Один из них — алгоритм удвоения-сложения. Принцип его работы проще объяснить на примере. Возьмём 151. В двоичном форме оно имеет вид 10010111_2. Такую двоичную форму можно представить как сумму степеней двойки:

$151 = 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$

т.е. $151 = 2^7 + 2^4 + 2^2 + 2^1 + 1$.

С учётом этого можно записать:

$$151 \cdot P = 2^7 \cdot P + 2^4 \cdot P + 2^2 \cdot P + 2^1 \cdot P + 1 \cdot P$$

Алгоритм удвоения-сложения задаёт следующий порядок действий:

- Взять P.
- *Удвоить* его, чтобы получить $2 \cdot P$.
- *Сложить* P и $2 \cdot P$ (чтобы получить результат $2^1 \cdot P + 1 \cdot P$).
- *Удвоить* $2 \cdot P$, чтобы получить $2^2 \cdot P$.
- *Сложить* с результатом (чтобы получить $2^2 \cdot P + 2^1 \cdot P + 1 \cdot P$).
- *Удвоить* $2^2 \cdot P$, получить $2^3 \cdot P$.
- Не выполнять сложение с $2^2 \cdot P + 2^1 \cdot P + 1 \cdot P$.
- *Удвоить* $2^3 \cdot P$, чтобы получить $2^4 \cdot P$.
- *Сложить* с результатом (чтобы получить $2^4 \cdot P + 2^2 \cdot P + 2^1 \cdot P + 1 \cdot P$).
- ...

В результате мы вычислим$151 \cdot P$, выполнив всего семь удвоений и четыре сложения.

Dot скрипт на Python, реализующий этот алгоритм:

```
def bits(n):
    """
    Генерирует двоичные разряды n, начиная
    с наименее значимого бита.

    bits(151) -> 1, 1, 1, 0, 1, 0, 0, 1
    """
    while n:
        yield n & 1
        n >>= 1
```

```
def double_and_add(n, x):
    """
    Возвращает результат n * x, вычисленный
    алгоритмом удвоения-сложения.
    """
    result = 0
    addend = x

    for bit in bits(n):
        if bit == 1:
            result += addend
        addend *= 2

    return result
```

Если удвоение и сложение являются операциями $O(1)$, то этот алгоритм имеет сложность $O(logn)$ (или $O(k)$, если учитывать битовую длину), намного лучше, чем изначальный алгоритм $O(n)$!

Логарифм

Для заданных n и P у нас имеется по крайней мере один полиномиальный алгоритм вычисления $Q = n \cdot P$. Но как насчёт обратной задачи? Что если мы знаем Q и P , а нам нужно определить n? Эта задача известна как задача логарифмирования. Мы употребляем слово «логарифм» вместо термина «деление» для согласованности с другими криптосистемами (в которых вместо умножения используется возведение в степень).

Не известно ни одного «простого» алгоритма для решения задачи логарифмирования.

Примеры выполнения заданий

Задание 1. Начертить график эллиптической кривой над полем действительных чисел. $y^2 = x^3 + x + 4$.

Решение будет опираться на визуальный инструмент (https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html)

Задание 2. Геометрическим методом найти сумму двух точек эллиптической кривой над полем действительных чисел.

$y^2 = x^3 - x + 1,$ $(0,1); (1,1)$

Решение будет опираться на визуальный инструмент (https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html)

Задание 3. Алгебраическим методом найти сумму двух точек эллиптической кривой над полем действительных чисел, заданных в условии задания 2.

Обозначим через P точку $(0,1)$, а через Q - $(1,1)$. Вычислим сначала коэффициент наклон прямой проходящей через эти точки: $m = \frac{y_P - y_Q}{x_P - x_Q} = \frac{1-1}{0-1} = 0.$

Вычислим первую координату точки R, являющейся обратной к сумме точек P и Q.

$$x_R = m^2 - x_P - x_Q = (0)^2 - 0 - 1 = -1.$$

Теперь вычислим вторую координату этой точки R:

$$y_R = y_P + m(x_R - x_P) = 1 + 0(-1 - 0) = 1$$

Или, аналогично: $y_R = y_Q + m(x_R - x_Q) = 1 + 0(-1 - 1) = 1.$

Таким образом, для данной эллиптической кривой получили сумму двух точек P и Q: (0,1)+(1,1) = (-1,-1).

Задание 4. Геометрическим методом найти обратный элемент точки эллиптической кривой над полем действительных чисел.

$y^2 = x^3 - x + 1,$ $(0,1)$

Решение будет опираться на визуальный инструмент (https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/reals-add.html)

Задание 5. Алгебраическим методом найти обратный элемент точки эллиптической кривой над полем действительных чисел.

$y^2 = x^3 - x + 1,$ $(1,1)$

В данном случае P= -Q =(1,-1). Но тогда прямая, проходящая через эти две точки, вертикальна, и не дает в пересечении третью точку. Но если P является обратной величиной Q, то $P+Q= P+(- P)=0$, как следует из определения обратной величины.

Задание 6. Найти скалярное умножение точки Q=(1,1) из задачи 2 на число $n = 3$.

В этом случае мы должны найти сумму $T = Q + Q + Q$. Сначала найдем сумму $Q + Q$. В этом случае $P = Q$ и нужно поступать немного иначе: уравнения для x_R и y_R остаются теми же, но с учётом того, что $x_P = x_Q$ нам придётся использовать для коэффициента наклона другое уравнение:

$$m = \frac{3x_P^2 + a}{2y_P} = \frac{3 \cdot (1)^2 - 1}{2 \cdot 1} = 1$$

$$x_R = m^2 - x_P - x_Q = 1^2 - 1 - 1 = -1$$

$$y_R = y_P + m(x_R - x_P) = 1 + 1(-1 - 1) = -1.$$

Таким образом имеем $R = Q + Q = (-1, 1)$

Теперь найдем сумму $T = (Q + Q) + Q = R + Q$. Заметим, что $R \neq Q$, поэтому

$$m = \frac{y_R - y_Q}{x_R - x_Q} = \frac{1-1}{-1-1} = 0,$$

$$x_T = m^2 - x_R - x_Q = (0)^2 - (-1) - 1 = 0,$$

$$y_T = y_Q + m\big(x_R - x_Q\big) = 1 - 0((-1) - 1) = 1.$$

Таким образом, имеем $T = 3Q = (1, -1)$.

Практические задания по вариантам

Задание 1. Начертить график эллиптической кривой над полем действительных чисел.

Вариант	Уравнение кривой
1	$y^2 = x^3 - x + 1$
2	$y^2 = x^3 - x - 1$
3	$y^2 = x^3 - x + 4$
4	$y^2 = x^3 - x - 4$
5	$y^2 = x^3 + 2x + 1$
6	$y^2 = x^3 + 2x - 1$
7	$y^2 = x^3 - 2x - 1$

8	$y^2 = x^3 - 2x + 1$
9	$y^2 = x^3 + x + 1$
10	$y^2 = x^3 + x - 1$

Задание 2. Геометрическим методом найти сумму двух точек эллиптической кривой над полем действительных чисел.

Вариант	Уравнение кривой	Координаты точек на кривой
1	$y^2 = x^3 + 2x + 1$	$(0,1); (1,2)$
2	$y^2 = x^3 + 2x + 1$	$(0,-1); (1,2)$
3	$y^2 = x^3 + 2x + 1$	$(0,-1); (1,-2)$
4	$y^2 = x^3 + 2x + 1$	$(0,1); (1,-2)$
5	$y^2 = x^3 - x + 4$	$(0,2); (1,2)$
6	$y^2 = x^3 - x + 4$	$(0,-2); (1,-2)$
7	$y^2 = x^3 - x + 4$	$(0,2); (1,-2)$
8	$y^2 = x^3 - x + 4$	$(0,-2); (1,2)$
9	$y^2 = x^3 - x + 1$	$(0,-1); (1,-1)$
10	$y^2 = x^3 - x + 1$	$(0,1); (1,-1)$

Задание 3. Алгебраическим методом найти сумму двух точек эллиптической кривой над полем действительных чисел, заданных в условии задания 2.

Задание 4. Геометрическим методом найти обратный элемент точки эллиптической кривой над полем действительных чисел.

Вариант	Уравнение кривой	Координаты точки на кривой
1	$y^2 = x^3 + 2x + 1$	$(1,2)$
2	$y^2 = x^3 + 2x + 1$	$(0,-1)$
3	$y^2 = x^3 + 2x + 1$	$(1,-2)$
4	$y^2 = x^3 + 2x + 1$	$(0,1)$
5	$y^2 = x^3 - x + 4$	$(1,2)$
6	$y^2 = x^3 - x + 4$	$(0,-2)$
7	$y^2 = x^3 - x + 4$	$(1,-2)$
8	$y^2 = x^3 - x + 4$	$(0,2)$
9	$y^2 = x^3 - x + 1$	$(0,-1)$

10	$y^2 = x^3 - x + 1$	$(1, -1)$

Задание 5. Алгебраическим методом найти обратный элемент точки эллиптической кривой над полем действительных чисел.

Вариант	Уравнение кривой	Координаты точек на кривой
1	$y^2 = x^3 + 2x + 1$	$(0,1))$
2	$y^2 = x^3 + 2x + 1$	$(1,2)$
3	$y^2 = x^3 + 2x + 1$	$(0, -1)$
4	$y^2 = x^3 + 2x + 1$	$(1, -2)$
5	$y^2 = x^3 - x + 4$	$(0, 2)$
6	$y^2 = x^3 - x + 4$	$(1, -2)$
7	$y^2 = x^3 - x + 4$	$(0, 2)$
8	$y^2 = x^3 - x + 4$	$(1,2)$
9	$y^2 = x^3 - x + 1$	$(1, -1)$
10	$y^2 = x^3 - x + 1$	$(0, 1)$

Задание 6. Найти скалярное умножение точки Q из задачи 2 на число $n = k + 1$, где k – номер Вашего варианта.

РАБОТА № 2 (13) Группы по сложению точек на эллиптических кривых над конечными полями.

Конечное поле — это, в первую очередь, множество конечного числа элементов. Примером конечного поля является множество целых чисел по модулю p, где p — простое число. В общем виде это записывается как

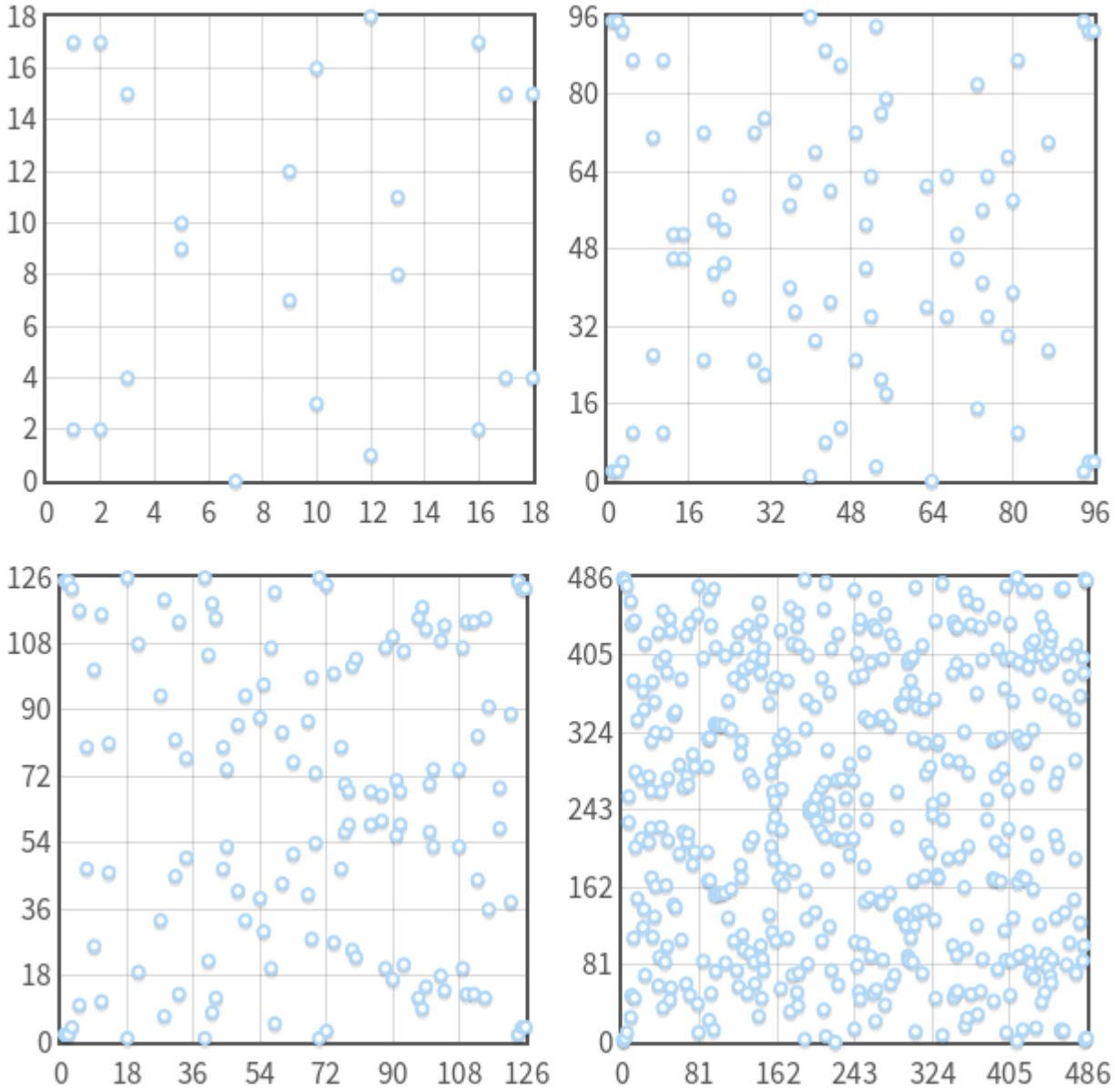
Z/p, $GF(p)$ или F_p. Мы будем использовать последнюю запись.

Множество **целых чисел по модулю** p **состоит из всех целых чисел от** 0 **до** $p-1$. Сложение и умножение работают как в теории сравнений. Нужно чётко понимать, что x/y означает над F_p. Попросту говоря: $x/y = x \cdot y^{-1}$.

Эллиптические кривые над F_p множество точек

$$\{(x, y) \in Fp^2 | y^2 \equiv x^3 + ax + b (mod\ p), 4a^3 + 27b^2 \not\equiv 0\ (mod\ p)\} \cup \{0\}$$

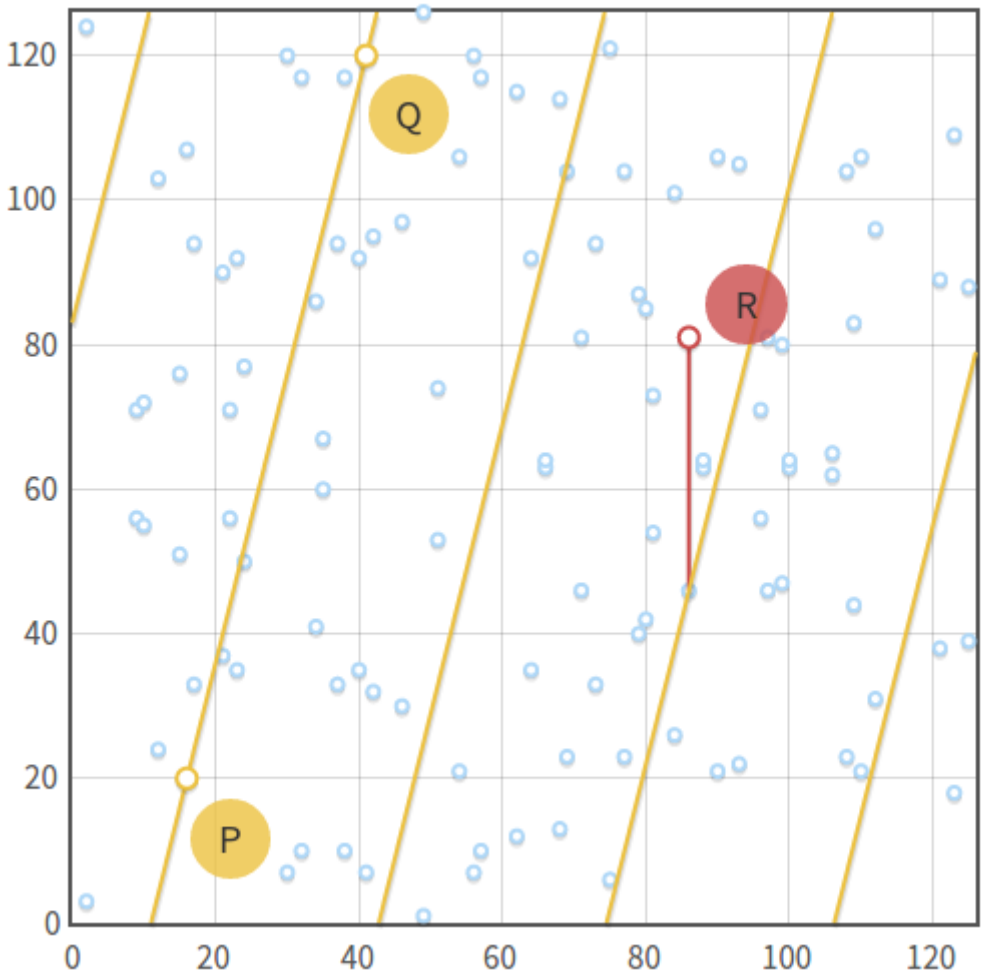
где 0 — по-прежнему точка в бесконечности, а a и b — два целых числа в F_p. Заметим, что для каждого x существует максимум две точки на этой кривой. Также отметим симметрию кривой относительно $y = p/2$.



Кривая $y^2 \equiv x^3 - 7x + 10 (mod\ p)$, *с* $p = 19, 97, 127, 487.$

Несмотря на ограничение области определения, эллиптические кривые над F_p всё равно создают абелеву группу. Прямая над F_p — это множество точек *(x,y)*, удовлетворяющих уравнению

ax+by+c≡ $0 (mod\ p)$ (это стандартное уравнение прямой с добавленной частью "$(mod\ p)$"). Три точки находятся на одной прямой, если существует прямая, соединяющая их.



Сложение точек для кривой $y^2 \equiv x^3 - x + 3 (mod\ 127)$*, при P=(16,20) и Q=41,120). Заметьте, как соединяющая точки прямая P,Q «повторяет» себя на плоскости.*

Учитывая то, что мы по-прежнему находимся в группе, сложение точек сохраняет уже известные нам свойства:

- *Q+0=0+Q=Q* (из определения единичного элемента).
- Для *Q* обратная величина *–Q* — это точка, имеющая ту же абсциссу, но обратную ординату. То есть *-Q≡ (x_Q,-y_Q)(mod p)*. Например, если кривая над F_{29} имеет точку *Q=(2,5)*, то обратной величиной будет –Q≡ (2,-5)*(mod 29) =(2, 24)*.
- Кроме того, *P+(-P)=0* (из определения обратной величины).

Если $P = (x_P, y_P), Q = (x_Q, y_Q)$ и *R=(x_R,y_R)*, то *P+Q=-R* можно вычислить следующим способом:

$$x_R \equiv (m^2 - x_P - x_Q)(mod\ p)$$

$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv [y_Q + m(x_R - x_Q)](mod\ p).$$

Если $P \neq Q$, то коэффициент наклона m принимает форму:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p)$$

Иначе, если P=Q, то применяем формулу:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p)$$

Уравнения не изменились, и это не совпадение: на самом деле, эти уравнения работают над любым полем, и над конечным, и над бесконечным (за исключением F_2 и F_3, которые являются особыми случаями).

Имеется интерактивный инструмент (Оригинальный текст: <label for="coefficient-p">p</label><input id="coefficient-p" name="p" value="97" type="number" step="1">) для выполнения сложения точек.

Эллиптическая кривая, определённая над конечным полем, имеет конечное количество точек, что соответствует порядку этой группы.

В общем случае проверка всех возможных значений для x в интервале от 0 до $p - 1$ будет невыполнимым способом подсчёта точек, потому что потребует $O(p)$ шагов, а эта задача «сложна», если p — большое простое число.

Однако, для вычисления порядка существует более быстрый алгоритм: алгоритм Шуфа. Он выполняется за полиномиальное время, а именно это и нужно.

Если мы складываем два значения, кратных P, то получаем значение, кратное P (т.е. значения, кратные P, замкнуты относительно операции сложения).

$$n \cdot P + m \cdot P = \underbrace{P + P + \cdots + P}_{n \text{ раз}} + \underbrace{P + P + \cdots + P}_{m \text{ раз}} = (n + m) \cdot P$$

Множество кратных P значений — это циклическая подгруппа группы, образованной эллиптической кривой.

Точка P называется порождающим элементом, генератором или базовой точкой циклической подгруппы.

Порядок P связан с порядком эллиптической кривой теоремой Лагранжа, согласно которой порядок подгруппы — это делитель порядка исходной группы.

Определить порядок подгруппы с базовой точкой P можно по следующему алгоритму:

1. Вычисляем порядок эллиптической кривой N с помощью алгоритма Шуфа.
2. Находим все делители N.
3. Для каждого делителя n порядка N вычисляем $n \cdot P$.
4. Наименьшее n, такое, что $n \cdot P = 0$, является порядком подгруппы, порожденной точкой P.

Подгруппы группы простого порядка p могут иметь порядок только $n = 1$ или $n = p$. Когда $n = 1$, подгруппа содержит только бесконечно удалённую точку;

когда $n = p$, подгруппа содержит все точки эллиптической кривой, т.е. это сама группа.

Для алгоритмов криптосистем на эллиптических кривых требуются подгруппы с высоким порядком. Поэтому обычно выбирается эллиптическая кривая, вычисляется её порядок (N), в качестве порядка группы (n) выбирается большой делитель, а потом находится подходящая базовая точка.

Теорема Лагранжа подразумевает, что число $h = \frac{N}{n}$ всегда целое (потому что n — делитель N). Число h имеет собственное название: это кофактор подгруппы.

Исходя из определения кофактора, мы можем записать:

$$n(hP) = 0$$

Теперь допустим, что n — простое число. Это уравнение, записанное в такой форме, говорит нам, что точка $G = hP$ создаёт подгруппу порядка n (за исключением случая $G = hP = 0$, в котором подгруппа имеет порядок 1).

В свете этого мы можем определить следующий алгоритм:

1. Вычисляем порядок N эллиптической кривой.
2. Выбираем порядок n подгруппы. Чтобы алгоритм сработал, число должно быть простым и быть делителем N.
3. Вычисляем кофактор $h = \frac{N}{n}$.
4. Выбираем на кривой случайную точку P.
5. Вычисляем $G = hP$.
6. Если G равно 0, то возвращаемся к шагу 4. В противном случае мы нашли генератор подгруппы с порядком n и кофактором h.

Задача дискретного логарифмирования состоит в следующем: если мы знаем P и Q, то каким будет k , такое, что $Q = kP$?

В известных алгоритмах, основанных на теории чисел, используется не скалярное умножение, а возведение в степень по модулю. Их задачу дискретного логарифмирования можно сформулировать так: если известны a и b , то каким будет k, такое, что $b \equiv a^k (mod\ p)$?

Обе эти задачи «дискретны», потому что в них используются конечные множества (а конкретнее — циклические подгруппы). И они являются «логарифмами», потому что аналогичны обычным логарифмам.

Крипто система на основе эллиптических кривых интересна тем, что на сегодняшний момент задача дискретного логарифмирования для эллиптических кривых кажется «сложнее» по сравнению с другими схожими задачами, используемыми в криптографии. Это подразумевает, что нам потребуется меньше бит для целого k, чтобы получить тот же уровень защиты, что и в других криптосистемах.

Примеры выполнения заданий

Задание 1. Найти все точки эллиптической кривой по уравнению над конечным полем.

$$y^2 = x^3 + x + 1 \ (mod\ p),\ F_5.$$

Сначала проверим необходимое условие эллиптической кривой.

$$4a^3 + 27b^2 \neq 0(mod\ 5)$$

Действительно: $4(1)^3 + 27(1)^2 = 31 \equiv 1(mod\ 5)$.

Теперь будем придавать x значения из полной системы вычетов по модулю 5 и вычислять возможные значения y, чтобы найти точки эллиптической кривой.

$$x = 0, y^2 = x^3 + x + 1 = 1 \equiv 1(mod\ 5).$$

Этому удовлетворяют значения $y = 1 \equiv 1(mod\ 5)$ и $y = -1 \equiv 4(mod\ 5)$.

Таким образом, получили две точки эллиптической кривой $P_1 = (0,1);\ P_2 = (0,4)$.

$$x = 1, y^2 = x^3 + x + 1 = 3 \equiv 3(mod\ 5)$$

Легко убедиться, что ни одно число из полной системы вычетов по модулю 5 от 0 до 4 в квадрате не дает числа, сравнимого с 3 по модулю 5.

$$x = 2, y^2 = x^3 + x + 1 = 11 \equiv 1(mod\ 5)$$

Как и при $x = 0$ получаем две точки эллиптической кривой

$P_3 = (2,1);\ P_4 = (2,4)$.

$$x = 3, y^2 = x^3 + x + 1 = 31 \equiv 1(mod\ 5)$$

Вновь получаем две точки эллиптической кривой $P_5 = (3,1);\ P_6 = (3,4)$.

$$x = 4, y^2 = x^3 + x + 1 = 69 \equiv 4(mod\ 5)$$

Данному сравнению удовлетворяют два значения $y = 2 \equiv 2(mod\ 5)$ и

$y = -2 \equiv 3(mod\ 5)$, т.е. получаем еще две точки эллиптической кривой

$P_7 = (4,2);\ P_8 = (4,3)$.

Таким образом, данная эллиптическая кривая $y^2 = x^3 + x + 1\ (mod\ 5)$ над полем F_5 содержит 9 точек: $P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8$ и бесконечно удаленную точку 0.

Задание 2. Проверить выполнение аксиом группы для сложения точек эллиптической кривой из задачи 1.

Для проверки выполнения аксиом группы вначале необходимо убедиться, что сложение точек эллиптической кривой является операцией, т.е. сложение любых двух элементов и множества $\{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, 0\}$ дает точку из этого же множества. Из определения бесконечно удаленной точки, т.е. точки 0, ясно, что $P_i + 0 = 0 + P_i = P_i$ для $i = 1, \dots, 6$. Значит, точка 0 является нейтральным элементом.

Заметим, что сумма коммутативна, т.к. прямая проходящая через две точки не зависит от рассмотрения их порядка. Поэтому, будем искать только следующие парные суммы $P_1 + P_1,\ P_1 + P_2,\ P_1 + P_3,\ P_1 + P_4,\ P_1 + P_5,\ P_1 + P_6,\ P_1 + P_7,\ P_1 + P_8\ \ P_2 + P_2,$

$P_2 + P_3$, $P_2 + P_4$, $P_2 + P_5$, $P_2 + P_6$, $P_2 + P_7$, $P_2 + P_8$ $P_3 + P_3$, $P_3 + P_4$, $P_3 + P_5$, $P_3 + P_6$, $P_3 + P_7$, $P_3 + P_8$, $P_4 + P_4$, $P_4 + P_5$, $P_4 + P_6$, $P_4 + P_7$, $P_4 + P_8$, $P_5 + P_5$, $P_5 + P_6$, $P_5 + P_7$, $P_5 + P_8$, $P_6 + P_6$, $P_6 + P_7$, $P_6 + P_8$, $P_7 + P_7$, $P_7 + P_8$, $P_8 + P_8$.

$P_1 + P_1$, $P_1 = (0,1)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3 \cdot 0^2 + 1)(2 \cdot 1)^{-1}(mod\ 5) \equiv (1) \cdot (2)^{-1}(mod\ 5)$$
$$\equiv (1) \cdot (3)(mod\ 5) \equiv 3(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - 2x_{P_1}\right)(mod\ p) \equiv (3^2 - 0)(mod\ 5) \equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_1} + m\left(x_R - x_{P_1}\right)\right](mod\ p) \equiv$$
$$\equiv [1 + 3(4 - 0)](mod\ 5) \equiv 3(mod\ 5)$$

Поэтому $P_1 + P_1 \equiv (4, -3) \equiv (4,2)(mod\ 5)$, т.е. $P_1 + P_1 = P_7$.

$P_1 + P_2$, $P_1 = (0,1)$, $P_2 = (0,4)$:

Заметим, что $P_2 = -P_1$, поэтому $P_1 + P_2 = 0$.

$P_1 + P_3$, $P_1 = (0,1)$, $P_3 = (2,1)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_1} - y_{P_3})(x_{P_1} - x_{P_3})^{-1}(mod\ 5)$$
$$\equiv (1 - 1)(0 - 2)^{-1}(mod\ 5) \equiv 0(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_1} - x_{P_3}\right)(mod\ 5) \equiv \left(0^2 - 0 - 2\right)(mod\ 5)$$
$$\equiv (-2)(mod\ 5) \equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_1} + m\left(x_R - x_{P_1}\right)\right](mod\ 5)$$
$$\equiv [1 + 0(3 - 0)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_1 + P_3 = (3, -1) \equiv (3,4)\ (mod\ 5)$, следовательно $P_1 + P_3 = P_6$.

$P_1 + P_4$, $P_1 = (0,1)$, $P_4 = (2,4)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_1} - y_{P_4})(x_{P_1} - x_{P_4})^{-1}(mod\ 5)$$
$$\equiv (1 - 4)(0 - 2)^{-1}(mod\ 5) \equiv (-3)(-2)^{-1}(mod\ 5) \equiv (2)(3)^{-1}(mod\ 5)$$
$$\equiv (2)(2)(mod\ 5) \equiv 4(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_1} - x_{P_4}\right)(mod\ 5) \equiv \left(4^2 - 0 - 2\right)(mod\ 5)$$
$$\equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_1} + m\left(x_R - x_{P_1}\right)\right](mod\ 5)$$
$$\equiv [1 + 4(4 - 0)](mod\ 5) \equiv 2(mod\ 5)$$

Поэтому $P_1 + P_4 = (4, -2)\ (mod\ 5) = (4,3)\ (mod\ 5)$, следовательно $P_1 + P_4 = P_8$.

$P_1 + P_5$, $P_1 = (0,1)$, $P_5 = (3,1)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_1} - y_{P_5})(x_{P_1} - x_{P_5})^{-1}(mod\ 5)$$
$$\equiv (1 - 1)(0 - 3)^{-1}(mod\ 5) \equiv (0)(-2)^{-1}(mod\ 5) \equiv 0(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_1} - x_{P_5}\right)(mod\ 5) \equiv \left(0^2 - 0 - 3\right)(mod\ 5)$$
$$\equiv 2(mod\ 5)$$

$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_1} + m\left(x_R - x_{P_1}\right)\right](mod\ 5)$$
$$\equiv [1 + 0(2 - 0)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_1 + P_5 = (2, -1)\ (mod\ 5) \equiv (2, 4)\ (mod\ 5)$, следовательно $P_1 + P_5 = P_4$.

$P_1 + P_6, P_1 = (0, 1),\ P_6 = (3, 4)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_1} - y_{P_6})(x_{P_1} - x_{P_6})^{-1}(mod\ 5)$$
$$\equiv (1 - 4)(0 - 3)^{-1}(mod\ 5) \equiv (-3)(2)^{-1}(mod\ 5) \equiv (2)3(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_1} - x_{P_6}\right)(mod\ 5) \equiv \left(1^2 - 0 - 3\right)(mod\ 5)$$
$$\equiv (-2)(mod\ 5) \equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_1} + m\left(x_R - x_{P_1}\right)\right](mod\ 5)$$
$$\equiv [1 + 1(3 - 0)](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_1 + P_6 = (3, -4) \equiv (3,1)\ (mod\ 5)$, следовательно $P_1 + P_6 = P_5$.

$P_1 + P_7, P_1 = (0, 1),\ P_7 = (4, 2)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_1} - y_{P_7})(x_{P_1} - x_{P_7})^{-1}(mod\ 5)$$
$$\equiv (1 - 2)(0 - 4)^{-1}(mod\ 5) \equiv (-1)(1)^{-1}(mod\ 5) \equiv 4(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_1} - x_{P_7}\right)(mod\ 5)$$
$$\equiv (4^2 - 0 - 4)(mod\ 5) \equiv 12(mod\ 5) \equiv 2(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_1} + m\left(x_R - x_{P_1}\right)\right](mod\ 5)$$
$$\equiv [1 + 4(2 - 0)](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_1 + P_7 = (2, -4) \equiv (2,1)\ (mod\ 5)$, следовательно $P_1 + P_7 = P_3$.

$P_1 + P_8, P_1 = (0, 1),\ P_8 = (4, 3)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_1} - y_{P_8})(x_{P_1} - x_{P_8})^{-1}(mod\ 5)$$
$$\equiv (1 - 3)(0 - 4)^{-1}(mod\ 5) \equiv (-2)(1)^{-1}(mod\ 5) \equiv (3)(1)^{-1}(mod\ 5) \equiv 3(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_1} - x_{P_8}\right)(mod\ 5)$$
$$\equiv (3^2 - 0 - 4)(mod\ 5) \equiv (5)(mod\ 5) \equiv 0(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_1} + m\left(x_R - x_{P_1}\right)\right](mod\ 5)$$
$$\equiv [1 + 3(0 - 0)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_1 + P_8 = (0, -1) \equiv (0,4)\ (mod\ 5)$, следовательно $P_1 + P_8 = P_2$.

$P_2 + P_2, P_2 = (0, 4)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3 \cdot 0^2 + 1)(2 \cdot 4)^{-1}(mod\ 5) \equiv (1)(3)^{-1}(mod\ 5)$$
$$\equiv (1)(2)(mod\ 5) \equiv 2(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_2} - x_{P_2}\right)(mod\ 5) \equiv \left(2^2 - 0 - 0\right)(mod\ 5)$$
$$\equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_2} + m\left(x_R - x_{P_2}\right)\right](mod\ 5)$$
$$\equiv [4 + 2(4 - 0)](mod\ 5) \equiv 2(mod\ 5)$$

Поэтому $P_2 + P_2 = (4, -2) \equiv (4,3)\ (mod\ 5)$, следовательно $P_2 + P_2 = P_8$.

$P_2 + P_3$, $P_2 = (0,4)$, $P_3 = (2,1)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_2} - y_{P_3})(x_{P_2} - x_{P_3})^{-1}(mod\ 5)$$
$$\equiv (4-1)(0-2)^{-1}(mod\ 5) \equiv (3)(3)^{-1}(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_2} - x_{P_3}\right)(mod\ 5) \equiv \left(1^2 - 0 - 2\right)(mod\ 5)$$
$$\equiv (-1)(mod\ 5) \equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_2} + m\left(x_R - x_{P_2}\right)\right](mod\ 5)$$
$$\equiv [4 + 1(4-0)](mod\ 5) \equiv 3(mod\ 5)$$

Поэтому $P_2 + P_3 = (4,-3) \equiv (4,2)(mod\ 5)$, следовательно $P_2 + P_3 = P_7$.

$P_2 + P_4$, $P_2 = (0,4)$, $P_4 = (2,4)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_2} - y_{P_4})(x_{P_2} - x_{P_4})^{-1}(mod\ 5)$$
$$\equiv (4-4)(0-2)^{-1}(mod\ 5) \equiv 0(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_2} - x_{P_4}\right)(mod\ 5) \equiv \left(0^2 - 0 - 2\right)(mod\ 5)$$
$$\equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_2} + m\left(x_R - x_{P_2}\right)\right](mod\ 5)$$
$$\equiv [4 + 0(2-0)](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_2 + P_4 = (3,-4) \equiv (3,1)(mod\ 5)$, следовательно $P_2 + P_4 = P_5$.

$P_2 + P_5$, $P_2 = (0,4)$, $P_5 = (3,1)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_2} - y_{P_5})(x_{P_2} - x_{P_5})^{-1}(mod\ 5)$$
$$\equiv (4-1)(0-3)^{-1}(mod\ 5) \equiv (4-1)(-3)^{-1}(mod\ 5) \equiv (3)(2)^{-1}(mod\ 5)$$
$$\equiv 3(3)(mod\ 5) \equiv 4(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_2} - x_{P_5}\right)(mod\ 5) \equiv \left(4^2 - 0 - 3\right)(mod\ 5)$$
$$\equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_2} + m\left(x_R - x_{P_2}\right)\right](mod\ 5)$$
$$\equiv [4 + 4(3-0)](mod\ 5) \equiv [16](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_2 + P_5 = (3,-1) \equiv (3,4)(mod\ 5)$, следовательно $P_2 + P_5 = P_6$.

$P_2 + P_6$, $P_2 = (0,4)$, $P_6 = (3,4)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_2} - y_{P_6})(x_{P_2} - x_{P_6})^{-1}(mod\ 5)$$
$$\equiv (4-4)(0-3)^{-1}(mod\ 5) \equiv (0)(2)^{-1}(mod\ 5) \equiv 0(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_2} - x_{P_6}\right)(mod\ 5) \equiv \left(0^2 - 0 - 3\right)(mod\ 5)$$
$$\equiv (-3)(mod\ 5) \equiv 2(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_2} + m\left(x_R - x_{P_2}\right)\right](mod\ 5)$$
$$\equiv [4 + 0(2-0)](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_2 + P_6 = (2,-4) \equiv (2,1)(mod\ 5)$, следовательно $P_2 + P_6 = P_3$.

$P_2 + P_7$, $P_2 = (0,4)$, $P_7 = (4,2)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_2} - y_{P_7})(x_{P_2} - x_{P_7})^{-1}(mod\ 5)$$
$$\equiv (4-2)(0-4)^{-1}(mod\ 5) \equiv (2)(1)^{-1}(mod\ 5) \equiv 2(mod\ 5)$$

$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_2} - x_{P_7}\right)(mod\ 5) \equiv \left(2^2 - 0 - 4\right)(mod\ 5)$$
$$\equiv (0)(mod\ 5) \equiv 0(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_2} + m\left(x_R - x_{P_2}\right)\right](mod\ 5)$$
$$\equiv [4 + 2(0 - 0)](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_2 + P_7 = (0, -4) \equiv (0,1)(mod\ 5)$, следовательно $P_2 + P_7 = P_1$.

$P_2 + P_8$, $P_2 = (0, 4)$, $P_8 = (4, 3)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_2} - y_{P_8})(x_{P_2} - x_{P_8})^{-1}(mod\ 5)$$
$$\equiv (4 - 3)(0 - 4)^{-1}(mod\ 5) \equiv (1)(1)^{-1}(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_2} - x_{P_8}\right)(mod\ 5) \equiv \left(1^2 - 0 - 4\right)(mod\ 5)$$
$$\equiv (-3)(mod\ 5) \equiv 2(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_2} + m\left(x_R - x_{P_2}\right)\right](mod\ 5)$$
$$\equiv [4 + 1(2 - 0)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_2 + P_8 = (2, -1) \equiv (2,4)(mod\ 5)$, следовательно $P_2 + P_8 = P_4$.

$P_3 + P_3$, $P_3 = (2, 1)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3x_{P_3}^2 + a)(2y_{P_3})^{-1}(mod\ p)$$
$$\equiv (3 \cdot 2^2 + 1)(2 \cdot 1)^{-1}(mod\ 5) \equiv (13)(2 \cdot 1)^{-1}(mod\ 5)$$
$$\equiv (3)(2)^{-1}(mod\ 5) \equiv (3)(3)(mod\ 5) \equiv 4(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_3} - x_{P_3}\right)(mod\ 5) \equiv \left(4^2 - 2 - 2\right)(mod\ 5)$$
$$\equiv (12)(mod\ 5) \equiv 2(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_3} + m\left(x_R - x_{P_3}\right)\right](mod\ 5)$$
$$\equiv [1 + 4(2 - 2)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_3 + P_3 = (2, -1) \equiv (2,4)(mod\ 5)$, следовательно $P_3 + P_3 = P_4$.

$P_3 + P_4$, $P_3 = (2, 1)$, $P_4 = (2, 4)$:

Заметим, что $P_4 = -P_3$, поэтому $P_3 + P_4 = 0$.

$P_3 + P_5$, $P_3 = (2, 1)$, $P_5 = (3, 1)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_3} - y_{P_5})(x_{P_3} - x_{P_5})^{-1}(mod\ 5)$$
$$\equiv (1 - 1)(2 - 1)^{-1}(mod\ 5) \equiv (0)(1)^{-1}(mod\ 5) \equiv 0(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_3} - x_{P_5}\right)(mod\ 5) \equiv \left(0^2 - 2 - 3\right)(mod\ 5)$$
$$\equiv (-5)(mod\ 5) \equiv 0(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_3} + m\left(x_R - x_{P_3}\right)\right](mod\ 5)$$
$$\equiv [1 + 0(0 - 2)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_3 + P_5 = (0, -1) \equiv (0,4)(mod\ 5)$, следовательно $P_3 + P_5 = P_2$.

$P_3 + P_6$, $P_3 = (2, 1)$, $P_6 = (3, 4)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_3} - y_{P_6})(x_{P_3} - x_{P_6})^{-1}(mod\ 5)$$
$$\equiv (1 - 4)(2 - 3)^{-1}(mod\ 5) \equiv (-3)(-1)^{-1}(mod\ 5) \equiv (2)(4)^{-1}(mod\ 5)$$
$$\equiv (2)(4)(mod\ 5) \equiv 3(mod\ 5)$$

$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_3} - x_{P_6}\right)(mod\ 5) \equiv \left(3^2 - 2 - 3\right)(mod\ 5)$$
$$\equiv (4)(mod\ 5) \equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_3} + m\left(x_R - x_{P_3}\right)\right](mod\ 5)$$
$$\equiv [1 + 3(4 - 2)](mod\ 5) \equiv 2(mod\ 5)$$

Поэтому $P_3 + P_6 = (4, -2) \equiv (4,3)(mod\ 5)$, следовательно $P_3 + P_6 = P_8$.

$P_3 + P_7$, $P_3 = (2,1)$, $P_7 = (4,2)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_3} - y_{P_7})(x_{P_3} - x_{P_7})^{-1}(mod\ 5)$$
$$\equiv (1 - 2)(2 - 4)^{-1}(mod\ 5) \equiv (-1)(-2)^{-1}(mod\ 5) \equiv (4)(3)^{-1}(mod\ 5)$$
$$\equiv (4)(2)(mod\ 5) \equiv 3(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_3} - x_{P_7}\right)(mod\ 5) \equiv \left(3^2 - 2 - 4\right)(mod\ 5)$$
$$\equiv (3)(mod\ 5) \equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_3} + m\left(x_R - x_{P_3}\right)\right](mod\ 5)$$
$$\equiv [1 + 3(3 - 2)](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_3 + P_7 = (3, -4) \equiv (3,1)(mod\ 5)$, следовательно $P_3 + P_7 = P_5$.

$P_3 + P_8$, $P_3 = (2,1)$, $P_8 = (4,3)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_3} - y_{P_7})(x_{P_3} - x_{P_8})^{-1}(mod\ 5)$$
$$\equiv (1 - 3)(2 - 4)^{-1}(mod\ 5) \equiv (-2)(-2)^{-1}(mod\ 5) \equiv (3)(3)^{-1}(mod\ 5)$$
$$\equiv (3)(2)(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_3} - x_{P_8}\right)(mod\ 5) \equiv \left(1^2 - 2 - 4\right)(mod\ 5)$$
$$\equiv (-5)(mod\ 5) \equiv 0(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_3} + m\left(x_R - x_{P_3}\right)\right](mod\ 5)$$
$$\equiv [1 + 1(0 - 2)](mod\ 5) \equiv (-1)(mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_3 + P_8 = (0, -4) \equiv (0,1)(mod\ 5)$, следовательно $P_3 + P_8 = P_1$.

$P_4 + P_4$, $P_4 = (2,4)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3x_{P_4}^2 + a)(2y_{P_4})^{-1}(mod\ p)$$
$$\equiv (3 \cdot 2^2 + 1)(2 \cdot 4)^{-1}(mod\ 5) \equiv (13)(3)^{-1}(mod\ 5)$$
$$\equiv (3)(3)^{-1}(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_4} - x_{P_4}\right)(mod\ 5) \equiv \left(1^2 - 2 - 2\right)(mod\ 5)$$
$$\equiv -3(mod\ 5) \equiv 2(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_4} + m\left(x_R - x_{P_4}\right)\right](mod\ 5)$$
$$\equiv [4 + 1(2 - 2)](mod\ 5) \equiv (4)(mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_4 + P_4 = (2, -4) \equiv (2,1)(mod\ 5)$, следовательно $P_4 + P_4 = P_3$.

$P_4 + P_5$, $P_4 = (2,4)$, $P_5 = (3,1)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_4} - y_{P_5})(x_{P_4} - x_{P_5})^{-1}(mod\ 5)$$
$$\equiv (4-1)(2-3)^{-1}(mod\ 5) \equiv (3)(-1)^{-1}(mod\ 5) \equiv (3)(4)^{-1}(mod\ 5)$$
$$\equiv (3)(4)(mod\ 5) \equiv 2(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_4} - x_{P_5}\right)(mod\ 5) \equiv \left(2^2 - 2 - 3\right)(mod\ 5)$$
$$\equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_4} + m\left(x_R - x_{P_4}\right)\right](mod\ 5)$$
$$\equiv [4 + 2(4-2)](mod\ 5) \equiv 3(mod\ 5)$$

Поэтому $P_4 + P_5 \equiv (4,-3)\left(mod\ 5 \equiv (4,2)(mod\ 5)\right)$, следовательно $P_4 + P_5 = P_7$.

$P_4 + P_6$, $P_4 = (2,4)$, $P_6 = (3,4)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_4} - y_{P_6})(x_{P_4} - x_{P_6})^{-1}(mod\ 5)$$
$$\equiv (4-4)(2-4)^{-1}(mod\ 5) \equiv (0)(-2)^{-1}(mod\ 5) \equiv 0(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_4} - x_{P_6}\right)(mod\ 5) \equiv \left(0^2 - 2 - 3\right)(mod\ 5)$$
$$\equiv 0(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_4} + m\left(x_R - x_{P_4}\right)\right](mod\ 5)$$
$$\equiv [4 + 0(0-2)](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_4 + P_6 \equiv (0,-4)(mod\ 5) \equiv (0,1)(mod\ 5)$, следовательно $P_4 + P_6 = P_1$.

$P_4 + P_7$, $P_4 = (2,4)$, $P_7 = (4,2)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_4} - y_{P_7})(x_{P_4} - x_{P_7})^{-1}(mod\ 5)$$
$$\equiv (4-2)(2-4)^{-1}(mod\ 5) \equiv (2)(-2)^{-1}(mod\ 5) \equiv (2)(3)^{-1}(mod\ 5)$$
$$\equiv (2)(2)(mod\ 5) \equiv 4(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_4} - x_{P_7}\right)(mod\ 5) \equiv \left(4^2 - 2 - 4\right)(mod\ 5)$$
$$\equiv 0(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_4} + m\left(x_R - x_{P_4}\right)\right](mod\ 5)$$
$$\equiv [4 + 4(0-2)](mod\ 5) \equiv [4 + 4(3)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_4 + P_7 \equiv (0,-1)(mod\ 5) \equiv (0,4)(mod\ 5)$, следовательно $P_4 + P_7 = P_2$.

$P_4 + P_8$, $P_4 = (2,4)$, $P_8 = (4,3)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_4} - y_{P_8})(x_{P_4} - x_{P_8})^{-1}(mod\ 5)$$
$$\equiv (4-3)(2-4)^{-1}(mod\ 5) \equiv (1)(-2)^{-1}(mod\ 5) \equiv (1)(3)^{-1}(mod\ 5)$$
$$\equiv (2)(mod\ 5) \equiv 2(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_4} - x_{P_8}\right)(mod\ 5) \equiv \left(2^2 - 2 - 4\right)(mod\ 5)$$
$$\equiv (-2)(mod\ 5) \equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_4} + m\left(x_R - x_{P_4}\right)\right](mod\ 5)$$
$$\equiv [4 + 2(3-2)](mod\ 5) \equiv [4 + 2(1)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_4 + P_8 \equiv (3,-1)(mod\ 5) \equiv (3,4)(mod\ 5)$, следовательно $P_4 + P_8 = P_6$.

$P_5 + P_5, P_5 = (3,1)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3x_{P_5}^2 + a)(2y_{P_5})^{-1}(mod\ p)$$
$$\equiv (3 \cdot 3^2 + 1)(2 \cdot 1)^{-1}(mod\ 5) \equiv (28)(2 \cdot 1)^{-1}(mod\ 5)$$
$$\equiv (3)(2)^{-1}(mod\ 5) \equiv (3)(3)(mod\ 5) \equiv 4(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_5} - x_{P_5}\right)(mod\ 5) \equiv \left(4^2 - 3 - 3\right)(mod\ 5)$$
$$\equiv 10(mod\ 5) \equiv 0(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_5} + m\left(x_R - x_{P_5}\right)\right](mod\ 5)$$
$$\equiv [1 + 4(0 - 3)](mod\ 5) \equiv [-11](mod\ 5) \equiv (-1)(mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_5 + P_5 = (0, -4) \equiv (0,1)(mod\ 5)$, следовательно $P_5 + P_5 = P_1$.

$P_5 + P_6, P_5 = (3,1), P_6 = (3,4)$:

Заметим, что $P_6 = -P_5$, поэтому $P_5 + P_6 = 0$.

$P_5 + P_7, P_5 = (3,1), P_7 = (4,2)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_5} - y_{P_7})(x_{P_5} - x_{P_7})^{-1}(mod\ 5)$$
$$\equiv (1 - 2)(3 - 4)^{-1}(mod\ 5) \equiv (-1)(-1)^{-1}(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_5} - x_{P_7}\right)(mod\ 5) \equiv \left(1^2 - 3 - 4\right)(mod\ 5)$$
$$\equiv -6(mod\ 5) \equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_5} + m\left(x_R - x_{P_5}\right)\right](mod\ 5)$$
$$\equiv [1 + 1(4 - 3)](mod\ 5) \equiv 2(mod\ 5)$$

Поэтому $P_5 + P_7 = (4, -2) \equiv (4,3)(mod\ 5)$, следовательно $P_5 + P_7 = P_8$.

$P_5 + P_8, P_5 = (3,1), P_8 = (4,3)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_5} - y_{P_8})(x_{P_5} - x_{P_8})^{-1}(mod\ 5)$$
$$\equiv (1 - 3)(3 - 4)^{-1}(mod\ 5) \equiv (-2)(-1)^{-1}(mod\ 5) \equiv (3)(4)^{-1}(mod\ 5)$$
$$\equiv (3)(4)(mod\ 5) \equiv 2(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_5} - x_{P_8}\right)(mod\ 5) \equiv \left(2^2 - 3 - 4\right)(mod\ 5)$$
$$\equiv -3(mod\ 5) \equiv 2(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_3} + m\left(x_R - x_{P_5}\right)\right](mod\ 5)$$
$$\equiv [1 + 2(2 - 3)](mod\ 5) \equiv (-1)(mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_5 + P_8 = (2, -4) \equiv (2,1)(mod\ 5)$, следовательно $P_5 + P_8 = P_3$.

$P_6 + P_6, P_6 = (3,4)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3x_{P_6}^2 + a)(2y_{P_6})^{-1}(mod\ p)$$
$$\equiv (3 \cdot 3^2 + 1)(2 \cdot 4)^{-1}(mod\ 5) \equiv (28)(8)^{-1}(mod\ 5)$$
$$\equiv (3)(3)^{-1}(mod\ 5) \equiv (3)(2)(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_6} - x_{P_6}\right)(mod\ 5) \equiv \left(1^2 - 3 - 3\right)(mod\ 5)$$
$$\equiv (-5)(mod\ 5) \equiv 0(mod\ 5)$$

$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_6} + m\left(x_R - x_{P_6}\right)\right](mod\ 5)$$
$$\equiv [4 + 1(0 - 3)](mod\ 5) \equiv [1](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_6 + P_6 = (0, -1) \equiv (0,4)(mod\ 5)$, следовательно $P_6 + P_6 = P_2$.

$P_6 + P_7$, $P_6 = (3,4)$, $P_7 = (4,2)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_6} - y_{P_7})(x_{P_6} - x_{P_7})^{-1}(mod\ 5)$$
$$\equiv (4 - 2)(3 - 4)^{-1}(mod\ 5) \equiv (2)(-1)^{-1}(mod\ 5) \equiv (2)(4)^{-1}(mod\ 5)$$
$$\equiv (2)(4)(mod\ 5) \equiv 3(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_6} - x_{P_7}\right)(mod\ 5) \equiv \left(3^2 - 3 - 4\right)(mod\ 5)$$
$$\equiv 2(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_6} + m\left(x_R - x_{P_6}\right)\right](mod\ 5)$$
$$\equiv [4 + 3(2 - 3)](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_6 + P_7 = (2, -1) \equiv (2,4)(mod\ 5)$, следовательно $P_6 + P_7 = P_4$.

$P_6 + P_8$, $P_6 = (3,4)$, $P_8 = (4,3)$:

$$m \equiv (y_P - y_Q)(x_P - x_Q)^{-1}(mod\ p) \equiv (y_{P_6} - y_{P_8})(x_{P_6} - x_{P_8})^{-1}(mod\ 5)$$
$$\equiv (4 - 3)(3 - 4)^{-1}(mod\ 5) \equiv (1)(-1)^{-1}(mod\ 5) \equiv (1)(4)^{-1}(mod\ 5)$$
$$\equiv (1)(4)(mod\ 5) \equiv 4(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_6} - x_{P_8}\right)(mod\ 5) \equiv \left(4^2 - 3 - 4\right)(mod\ 5)$$
$$\equiv 4(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_6} + m\left(x_R - x_{P_6}\right)\right](mod\ 5)$$
$$\equiv [4 + 4(4 - 3)](mod\ 5) \equiv 3(mod\ 5)$$

Поэтому $P_6 + P_8 = (4, -3) \equiv (4,2)(mod\ 5)$, следовательно $P_6 + P_8 = P_7$.

$P_7 + P_7$, $P_7 = (4,2)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3x_{P_7}^2 + a)(2y_{P_7})^{-1}(mod\ p)$$
$$\equiv (3 \cdot 4^2 + 1)(2 \cdot 2)^{-1}(mod\ 5) \equiv (49)(4)^{-1}(mod\ 5)$$
$$\equiv (4)(4)(mod\ 5) \equiv 1(mod\ 5)$$
$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_7} - x_{P_7}\right)(mod\ 5) \equiv \left(1^2 - 4 - 4\right)(mod\ 5)$$
$$\equiv (-2)(mod\ 5) \equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_7} + m\left(x_R - x_{P_7}\right)\right](mod\ 5)$$
$$\equiv [2 + 1(3 - 4)](mod\ 5) \equiv [1](mod\ 5) \equiv 1(mod\ 5)$$

Поэтому $P_7 + P_7 = (3, -1) \equiv (3,4)(mod\ 5)$, следовательно $P_7 + P_7 = P_6$.

$P_7 + P_8$, $P_7 = (4,2)$, $P_8 = (4,3)$:

Заметим, что $P_8 = -P_7$, поэтому $P_7 + P_8 = 0$.

$P_8 + P_8$, $P_8 = (4,3)$:

$$m \equiv (3x_P^2 + a)(2y_P)^{-1}(mod\ p) \equiv (3x_{P_8}^2 + a)(2y_{P_8})^{-1}(mod\ p)$$
$$\equiv (3 \cdot 4^2 + 1)(2 \cdot 3)^{-1}(mod\ 5) \equiv (49)(1)^{-1}(mod\ 5)$$
$$\equiv (4)(1)(mod\ 5) \equiv 4(mod\ 5)$$

$$x_R \equiv \left(m^2 - x_P - x_Q\right)(mod\ p) \equiv \left(m^2 - x_{P_8} - x_{P_8}\right)(mod\ 5) \equiv \left(4^2 - 4 - 4\right)(mod\ 5)$$
$$\equiv (8)(mod\ 5) \equiv 3(mod\ 5)$$
$$y_R \equiv [y_P + m(x_R - x_P)](mod\ p) \equiv \left[y_{P_8} + m\left(x_R - x_{P_8}\right)\right](mod\ 5)$$
$$\equiv [3 + 4(3 - 4)](mod\ 5) \equiv [-1](mod\ 5) \equiv 4(mod\ 5)$$

Поэтому $P_8 + P_8 = (3, -4) \equiv (3,1)(mod\ 5)$, следовательно $P_8 + P_8 = P_5$

Теперь рассмотрим выполнение аксиом группы.

Ясно по определению, что нейтральным элементом является 0 – бесконечно удаленная точка.

Для каждого элемента существует противоположный, что установлено выше:

$$P_1 + P_2 = P_2 + P_1 = 0;$$
$$P_3 + P_4 = P_4 + P_3 = 0;$$
$$P_5 + P_6 = P_6 + P_5 = 0;$$
$$P_7 + P_8 = P_8 + P_7 = 0.$$

Формально для того, чтобы установить ассоциативность $a + (b + c) = (a + b) + c$ в группе, потребуется 9^3 проверок, что очень много. Мы все проверки проводить не будем, но некоторые приведет для понимания.

При любом элементе a выполняется равенство $a + (a + a) = (a + a) + a$ в силу коммутативности сложения точек.

Если хотя бы один из трех элементов a, b, c равен 0, то соответствующее равенство очевидно выполняется из-за свойств нейтрального элемента:

Например при $b = 0$ имеем

$a + (0 + c) = (a + 0) + c = a + c$.

Рассмотрим теперь для некоторых других элементов.

$$P_1 + (P_2 + P_3) = P_1 + P_7 = P_3$$
$$(P_1 + P_2) + P_3 = 0 + P_3 = P_3$$

Так как правые части равенств равны, то и левые равны, т.е.

$$P_1 + (P_2 + P_3) = (P_1 + P_2) + P_3.$$

$$P_2 + (P_4 + P_6) = P_2 + P_1 = 0$$
$$(P_2 + P_4) + P_6 = P_5 + P_6 = 0$$

Следовательно и в этом случае выполняется равенство:

$$P_2 + (P_4 + P_6) = (P_2 + P_4) + P_6\ .$$

$$P_1 + (P_4 + P_7) = P_1 + P_2 = 0$$
$$(P_1 + P_4) + P_7 = P_8 + P_7 = 0$$

И в этом случае получаем $P_1 + (P_4 + P_7) = (P_1 + P_4) + P_7$.

Проведем еще одну проверку.

$$P_3 + (P_5 + P_7) = P_3 + P_8 = P_1$$
$$(P_3 + P_5) + P_7 = P_2 + P_7 = P_1$$

Т.е. и в этом случае равенство выполняется.

Таким образом можно убедиться в выполнении аксиомы ассоциативности для сложения точек эллиптической кривой.

На множестве точек эллиптической кривой выполнены все три аксиомы группы: ассоциативность сложения, существования нейтрального элемента и для каждого элемента существует противоположный. Кроме того ранее отмечалось, что сложение точек эллиптической кривой коммутативно. Т.е. точки эллиптической кривой по сложению образуют коммутативную группу.

Задание 3. Найти порядки всех элементов группы точек эллиптической кривой задачи 1.

Напомним, что порядком элемента a называется такое наименьшее натуральное число n , что $n \cdot a = 0$.

Очевидно порядком элемента 0 является 1.

Найдем порядок элемента P_1. $2P_1 = P_1 + P_1 = P_7$; $3P_1 = (P_1 + P_1) + P_1 = P_7 + P_1 = P_1 + P_7 = P_3$; $4P_1 = P_1 + 3P_1 = P_1 + P_3 = P_6$; $5P_1 = P_1 + 4P_1 = P_1 + P_6 = P_5$; $6P_1 = P_1 + 5P_1 = P_1 + P_5 = P_4$; $7P_1 = P_1 + 6P_1 = P_1 + P_4 = P_8$; $8P_1 = P_1 + 7P_1 = P_1 + P_8 = P_2$; $9P_1 = P_1 + 8P_1 = P_1 + P_2 = 0$. Таким образом порядок элемента P_1 равен O(P_1)=9.

Найдем порядок элемента P_2. $2P_2 = P_2 + P_2 = P_8$; $3P_2 = (P_2 + P_2) + P_2 = P_8 + P_2 = P_2 + P_8 = P_4$; $4P_2 = P_2 + 3P_2 = P_2 + P_4 = P_5$; $5P_2 = P_2 + 4P_2 = P_2 + P_5 = P_6$; $6P_2 = P_2 + 5P_2 = P_2 + P_6 = P_3$; $7P_2 = P_2 + 6P_2 = P_2 + P_3 = P_7$; $8P_2 = P_2 + 7P_2 = P_2 + P_7 = P_1$; $9P_2 = P_2 + 8P_2 = P_2 + P_1 = 0$. Таким образом порядок элемента P_2 равен O(P_2)=9.

Найдем порядок элемента P_3. $2P_3 = P_3 + P_3 = P_4$; $3P_3 = (P_3 + P_3) + P_3 = P_4 + P_3 = 0$. Таким образом порядок элемента P_3 равен O(P_3)=3.

Найдем порядок элемента P_4. $2P_4 = P_4 + P_4 = P_3$; $3P_4 = (P_4 + P_4) + P_4 = P_3 + P_4 = 0$. Таким образом порядок элемента P_4 равен O(P_4)=3.

Найдем порядок элемента P_5. $2P_5 = P_5 + P_5 = P_1$; $3P_5 = 2P_5 + P_5 = P_1 + P_5 = = P_4$; $4P_5 = P_5 + 3P_5 = P_5 + P_4 = P_7$; $5P_5 = P_5 + 4P_5 = P_5 + P_7 = P_8$; $6P_5 = P_5 + 5P_5 = P_5 + P_8 = P_3$; $7P_5 = P_5 + 6P_5 = P_5 + P_3 = P_2$; $8P_5 = P_5 + 7P_5 = P_5 + P_2 = P_6$; $9P_5 = P_5 + 8P_5 = P_5 + P_6 = 0$. Таким образом порядок элемента P_5 равен O(P_5)=9.

Найдем порядок элемента P_6. $2P_6 = P_6 + P_6 = P_2$; $3P_6 = 2P_6 + P_6 = P_2 + P_6 = = P_3$; $4P_6 = P_6 + 3P_6 = P_6 + P_3 = P_8$; $5P_6 = P_6 + 4P_6 = P_6 + P_8 = P_3$; $6P_6 = P_6 + 5P_6 = P_6 + P_3 = P_8$; $7P_6 = P_6 + 6P_6 = P_6 + P_8 = P_3$; $8P_6 = P_6 + 7P_6 = P_6 + P_3 = P_8$; $9P_6 = P_6 + 8P_6 = P_6 + P_5 = 0$. Таким образом порядок элемента P_6 равен O(P_6)=9.

Найдем порядок элемента P_7. $2P_7 = P_7 + P_7 = P_6$; $3P_5 = 2P_7 + P_7 = P_6 + P_7 = = P_4$; $4P_7 = P_7 + 3P_7 = P_7 + P_4 = P_2$; $5P_7 = P_7 + 4P_7 = P_7 + P_2 = P_1$;

$6P_7 = P_7 + 5P_7 = P_7 + P_1 = P_3$; $7P_7 = P_7 + 6P_7 = P_7 + P_3 = P_5$; $8P_7 = P_7 + 7P_7 = P_7 + P_5 = P_8$; $9P_7 = P_7 + 8P_7 = P_7 + P_8 = 0$. Таким образом порядок элемента P_7 равен O(P_7)=9.

Найдем порядок элемента P_8. $2P_8 = P_8 + P_8 = P_5$; $3P_8 = 2P_8 + P_8 = P_5 + P_8 = = P_3$; $4P_8 = P_8 + 3P_8 = P_8 + P_3 = P_1$; $5P_8 = P_8 + 4P_8 = P_8 + P_1 = P_2$;
$6P_8 = P_8 + 5P_8 = P_8 + P_2 = P_4$; $7P_8 = P_8 + 6P_8 = P_8 + P_4 = P_6$; $8P_8 = P_8 + 7P_8 = P_8 + P_6 = P_7$; $9P_8 = P_8 + 8P_8 = P_8 + P_7 = 0$. Таким образом порядок элемента P_8 равен O(P_8)=9.

Задание 4. Указать простые подгруппы группы по сложению точек эллиптической кривой из задачи 1.

Согласно теореме Лагранжа порядок группы является делителем порядка группы. У нас в группе 9 элементов. Делителями числа 9 являются 1, 3 и 9. 1 соответствует подгруппе, содержащей только 0. 9 соответствует всей группе. Значит собственными не одноэлементными подгруппами могут быть только подгруппы порядка 3. Это простой порядок. А группа простого порядка порождается одним элементом. Значит такими подгруппами будут являться подгруппы порожденный элементами порядка 3. Таких элементов два: P_3 и P_4. Оба эти элемента порождают одну и туже подгруппу $\{0, P_3, P_4\}$. Она будет в данном случае единственной подгруппой простого порядка.

Практические задания по вариантам

Задание 1. Найти все точки эллиптической кривой по уравнению над конечным полем.

№ варианта	Уравнение эллиптической кривой	Конечное поле F_p
1	$y^2 = x^3 - x + 1\ (mod\ p)$	F_5
2	$y^2 = x^3 - x + 1\ (mod\ p)$	F_7
3	$y^2 = x^3 - x + 4(mod\ p)$	F_5
4	$y^2 = x^3 - x + 4(mod\ p)$	F_7
5	$y^2 = x^3 + 2x + 1(mod\ p)$	F_5
6	$y^2 = x^3 + 2x + 1(mod\ p)$	F_7
7	$y^2 = x^3 - 2x + 1(mod\ p)$	F_7
8	$y^2 = x^3 - 2x - 1(mod\ p)$	F_7
9	$y^2 = x^3 + x + 4(mod\ p)$	F_5

10	$y^2 = x^3 + x + 4(mod\ p)$	F_7

Задание 2. Проверить выполнение аксиом группы для сложения точек эллиптической кривой из задачи 1.

Задание 3. Найти порядки всех элементов группы точек эллиптической кривой задачи 1.

Задание 4. Указать простые подгруппы группы по сложению точек эллиптической кривой из задачи 1.

Список литературы

1. Веселова, Л. В. Алгебра и теория чисел : Учебное пособие / Л. В. Веселова, О. Е. Тихонов. – Казань : Казанский национальный исследовательский технологический университет, 2014. – 107 с. – ISBN 978-5-7882-1636-2.
2. Ларин, С. В. Алгебра и теория чисел. Группы, кольца и поля : Учебное пособие / С. В. Ларин. – 2-е изд., испр. и доп. – Москва : Издательство Юрайт, 2020. – 1 с. – (Высшее образование). – ISBN 978-5-534-05567-2.
3. Швед, Е. А. Практикум по алгебре: элементы теории чисел / Е. А. Швед, В. А. Федоров. – Омск : Омский государственный университет путей сообщения, 2022. – 39 с.
4. Шнеперман, Л. Б. Сборник задач по алгебре и теории чисел : учебное пособие / Л. Б. Шнеперман ; Л. Б. Шнеперман. – 3-е изд., стер.. – Санкт-Петербург [и др.]: Лань, 2008. – (Учебники для вузов. Специальная литература). – ISBN 978-5-8114-0885-6.
5. Виноградов, И. М. Основы теории чисел [Текст]: учебное пособие / И. М. Виноградов. - Изд. 12-е, стер. - СПб. [и др.]: Лань, 2009. - 176 с.
6. Виноградов, И. М. Элементы высшей математики : аналитическая геометрия, дифференциальное исчисление : учебник для студентов высших учебных заведений, обучающихся по инженерно-техническим специальностям / И. М. Виноградов ; И. М. Виноградов. – Москва : Дрофа, 2010. – 319 с. – (Высшее образование. Современный учебник). – ISBN 978-5-358-06101-9.
7. Гончаренко, В. М. Элементы высшей математики / В. М. Гончаренко, Л. В. Липагина, А. А. Рылов. – МОСКВА : Компания КноРус, 2019. – 364 с. – ISBN 978-5-406-06878-6.
8. Болотов А.А., Гашов С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. -М.: КомКнига, 2006. -280 с. – ISBN 5-484-00444-6.