МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
«КАЗАНСКИЙ (ПРИВОЛЖСКИЙ) ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ МАТЕМАТИКИ И МЕХАНИКИ ИМЕНИ ЛОБАЧЕВСКОГО

КАФЕДРА АЛГЕБРЫ И МАТЕМАТИЧЕСКОЙ ЛОГИКИ

Специальность: 010100 — Математика

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
(Дипломная работа)

# Теорема Эйлера и её обобщения

Работа завершена:
«_____» _____ 2015 г. _____ А. А. Маркарян,
гр. 05-104

**Работа допущена к защите:**
Научный руководитель
к. ф.-м. н., доцент
«_____» _____ 2015 г. _____ А. Н. Абызов

Зав. кафедрой
д. ф-м. н., профессор
«_____» _____ 2015 г. _____ М. М. Арсланов

Казань — 2015 год

# Введение

Дипломная работа посвящена некоторым обобщениям таких классических теорем теории чисел как теорема Эйлера, теорема Вильсона и малой теоремы Ферма.

Малая теорема Ферма была открыта французом, советником парламента Тулузы, Пьером Ферма (1601-1665) в 1640 году. Формулировалась она очень коротко: если $p$ простое число, $a$ - целое число,то $a^p - a$ кратно $p$. Первое доказательство теоремы Ферма Эйлер даёт в статье 1741 года, исходя из рассмотрения частных случаев $a = 2, a = 3$. Сначала он показывает, что если $p$ - простое нечетное число, то $2^{p-1}$ всегда делится на $p$. Это следует из вида коэффициентов разложения $(1 + 1)^p$. Точно так же доказывается утверждение, что $3^{p-1} - 1$ всегда делится на простое $p$, не равное 3. Затем Эйлер доказывает, что если разность $a^p - a$ делится на $p$, то отсюда следует, что и разность $(a+1)^p - (a+1)$ делится на $p$. Таким образом, полной математической индукцией доказана теорема: разность $a^p - a$ делится на $p$. Вторично доказательство теоремы Ферма Эйлер дает в работе 1750 года. Он замечает, что из утверждения "$a^p - a$ всегда делится на $p$ "следует при $(a, p) = 1$, что $a^{p-1} - 1$ делится на $p$. Это уже обычная формулировка теоремы Ферма. В той же работе даны также различные утверждения относительно делителей сумм вида $a^{2^m} \pm b^{2^m}$. Третье доказательство малой теоремы Ферма, основанное на теории степенных вычетов, Эйлер дает в работе 1849 года. Четвертое доказательство этой теоремы вытекает как частный случай из теоремы Эйлера в том же году. На языке теории сравнений теорема Эйлера формулируется так: если $a$ и $n$ - натуральные числа, взаимно простые между собой, $\phi(n)$ - функция Эйлера, выражающая количество натуральных чисел, взаимно простых с $n$ и не превосходящих $n$, то имеет место сравнение:

$$a^{\phi(n)} = 1 \mod n.$$

Дипломная работа состоит из четырех глав. В первой главе приведены основные понятия и сведения, используемые в дальнейшем.

Вторая глава посвящена теореме Вильсона. В ней описан группой аналог теоремы, а также приведена теорема Гаусса, которая, в свою очередь, также является обобщение теоремы Вильсона.

Третья глава посвящена теореме Эйлера для целых Гауссовых чисел. В ней изложен материал о неразложимых элементах в кольце целых

Гауссовых числах. Также приведена теорема о фактор-кольцах колец целых Гауссовых чисел с иллюстрациями множества примеров.

И в четвертой главе, рассмотрен аналог малой теоремы Ферма в матричной форме.

# Содержание

# 1 Предварительные сведения

## 1.1 Кольца.Алгебры

**Определение 1.1.** *(Аддитивной) абелевой группой называется множество $A$ с операцией сложения обладающей следующими свойствами для любых $a, b, c \in A$:*

1. *$a + b = b + a$(коммутативность);*
2. *$(a + b) + c = a + (b + c)$(ассоциативность);*
3. *Существование нейтрального элемента,для любого $a \in A$: $a + 0 = a$;*
4. *Существование противоположного элемента,для любого $a \in A$: a+(-a)=0.*

**Определение 1.2.** *Кольцом называется множество $K$ с операциями сложения и умножения,обладающими следующими свойствами:*

1. *относительно сложения $K$ есть абелева группа(называемая аддитивной группой кольца $K$);*
2. *$a(b + c) = ab + ac$ и $(b + c)a = ba + ca$ для любых $a, b, c \in K$(дистрибутивность умножения относительно сложения).*

Примеры колец:

- Множество целых чисел.
- Множество рациональных чисел.
- Множество действительных чисел.

**Определение 1.3.** *Полем называется коммутативное,ассоциативное кольцо с единицей,в котором всякий ненулевой элемент обратим.*

**Определение 1.4.** *Векторным(или линейным) пространством над полем $K$ называется произвольное непустое множество $V$,на котором заданы операции сложения векторов(элементов из $V$) и умножения вектора на элемент поля $K$,удовлетворяющие следующим условиям,которые называются аксиомами векторного пространства:*

1. *Абелева группа по сложению;*

2. *Если* $x, y \in V$, *а* $a \in K$,*то* $a(x+y) = ax + ay$;

3. *Если* $x \in V$, *а* $a, b \in K$,*то* $(a+b)x = ax + bx$;

4. *Если* $x \in V$, *а* $a, b \in K$,*то* $a(bx) = (ab)x$;

5. *Если* $x \in V, 1 \in K$ *то* $1 \cdot x = x$;

**Определение 1.5.** *Алгеброй над полем* $K$ *называется множество* $A$ *с операция сложения,умножения и умножения на элементы поля* $K$,*обладающими следующими свойствами:*

1. *Относительно умножения и сложения на элементы поля,*$A$ *есть векторное пространство;*

2. *Относительно сложения и умножения* $A$ *есть кольцо;*

3. $(\gamma a)b = a(\gamma b) = \gamma(ab)$ *для любых* $\gamma \in K, a, b \in A$;

**Определение 1.6.** *Непустое подмножество* $I$ *кольца* $R$ *называется идеалом кольца* $R$, *если выполняются следующие условия:*

1. $I$ *подгруппа аддитивной группы кольца* $(R, +)$ $(i_1, i_2 \in I \Rightarrow i_1 + i_2 \in I; 0 \in I)$;

2. *Для любого* $i \in I$ *выполняется* $ir, ri \in I$.

Примеры идеалов:

- В поле нет нетривиальных (т.е. отличных от нуля всего поля) идеалов.

- Всякая аддитивная подгруппа кольца $Z$ является идеалом и имеет вид $nZ$,где $n \in Z_+$.

**Определение 1.7.** *Классом смежности элемента* $a$ *кольца* $R$ *по модулю* $I$ *называется множество элементов из кольца* $R$: $[a] = \{a+I | a \in R\}$.

**Определение 1.8.** *Факторкольцом* $R/I$ *кольца* $R$ *по идеалу* $I$ *называется множество классов смежности кольца* $R$ *по идеалу* $I$: $R/I = \{[a] | a \in R\}$, *на котором определены операции,сложения и умножения,определенных согласно следующему правилу:*

1. $(a+I)(a^{'}+I)=aa^{'}+I;$
2. $(a+I)+(a^{'}+I)=a+a^{'}+I;$

Примеры факторколец:

1. Пусть дано кольцо: $G=\{m+ni|m,n\in Z\}$ и дан идеал: $I=5G$,найдем количество классов смежности в этом факторкольце $G/I$: $G/I=m+ni+I$,где $0\leq a\leq 4, 0\leq b\leq 4$ Предположительно 25 классов,проверим если ли одинаковые среди них: $\overline{a+bi}=\overline{a'+b'i}$ тогда должно $5/(a-a^{'})$ и $5/(b-b^{'})$,что выполняется только в том случае,когда: $a=a^{'}, b=b^{'}$ получаем,что классов будет 25.

2. Теперь пусть дано фактор кольцо $Z/nZ$.По определению можно записать данное фактор кольцо в виде $\overline{0},\overline{1}\cdots\overline{n-1}$

   И для любого $m\in Z/nZ$ выполняется равенство

   $\overline{m}=\overline{nq+r}=\overline{nq}+\overline{r}=\overline{0}+\overline{r}=\overline{r};(r\in\overline{0,n-1})$

   Для любых $m_1,m_2\in Z/nZ$ умножение осуществляется согласно следующему правилу:

   $$\overline{m_1m_2}=\overline{m_1m_2}=\{m_1m_2=nq+r\}=\overline{r}.$$

   Операция сложения определена следующим образом:

   $$\overline{m_1}+\overline{m_2}=\overline{m_1+m_2}=\{m_1+m_2=n'q'+r'\}=\overline{r'}.$$

   Такое фактор кольцо называют кольцом вычетов.

3. $Z[i]=\{m+ni|m,n\in Z\}$ - кольцо целых гауссовых чисел.

   Покажем,что $Z[i]/<2>\cong Z_4$

   $\overline{m+ni}=m+ni+<2>$ Или $\overline{m}+\overline{ni}=a+bi(a,b=\overline{0},\overline{1});$

   Получаем 4 класса смежности:

   $$\overline{0};\overline{i};\overline{1+i};\overline{1}.$$

   Выполним проверку на то,что среди них(классов смежности) нет одинаковых,от противного:

   $\overline{a}+\overline{bi}=\overline{a'}+\overline{b'i};$

$\overline{a} - \overline{a'} + (\overline{b} - \overline{b'})i = \overline{0}$;

$2|(a - a')$; $2|(b - b')$. так как $\overline{a}, \overline{b} \in \{\overline{0}, \overline{1}\}$ Тогда $a = a'$ и $b = b'$

Т.е. в единственном случае 2 делит $(a - a')$ тогда когда $a = a'$

4. Покажем,что выполняется изоморфизм:

   $Z[i]/ < 1 + i >= \{\overline{0}, \overline{1}\} \cong Z_2$

   $\overline{1 + i} = \overline{0}$; $\overline{1} = -\overline{i}; \overline{i} = \overline{1}$; Здесь умножили на $i$ оба члена равенства.

   $\overline{0} = (\overline{1} + \overline{i})^2 = \overline{2i}$ Домножим обе части равенства на $-i$,получим:

   $\overline{0} = \overline{2} = \overline{1} + \overline{1}$; $\overline{i} = \overline{1} = \overline{-1}$; Тогда $\overline{a + bi} = \overline{a + b} = \overline{0}, \overline{1}$ где $\overline{a}, \overline{b} = \overline{0}, \overline{1}$

5. Покажем,что выполняется изоморфизм:

   $Z[i]/ < 1 + 2i > \cong Z_5$

   $\overline{1 + 2i} = \overline{0}$; $\overline{-2i} = \overline{1}$; $\overline{1} = \overline{-4}$; $\overline{5} = \overline{0}$; $\overline{m + ni} = a + bi(a, b = (\overline{0, 4}))$;

   Далее умножим на $i$ на идеал,по которому мы факторизуем.

   Получаем: $\overline{i} = \overline{2}$;

   Покажем,что среди смежных классов нет одинаковых: $i, j = (\overline{0, 4})$ Пусть есть одинаковые.Тогда $(1 + 2i)|(i - j)$ делит только в том случае,когда $i = j$,покажем это:

   $g(1 + 2i)(1 - 2i) = (i - j)$;

   $g5 = (i - j)$ Равенство в том случае,когда: $i = j$.

6. Покажем,что выполняется изоморфизм:

   $Z[\sqrt{3}]/ < 1 + 2\sqrt{3} > \cong Z_{11}$;

   Кольцо имеет вид: $Z[\sqrt{3}] = \{m + n\sqrt{3} | m, n \in Z\}$;

   Тогда $\overline{1 + 2\sqrt{3}} = \overline{0}$ и $\overline{2\sqrt{3}} = \overline{-1}$.

   Домножим на сопряженное,получаем $\overline{11} = \overline{0}$;

   Далее умножим на $\sqrt{3}$ на идеал,по которому мы факторизуем: $\overline{\sqrt{3}} + \overline{6} = \overline{0}$; Получаем $\overline{\sqrt{3}} = \overline{5}$.

   Тогда

   $\overline{m + n\sqrt{3}} = \overline{m} + \overline{5n} = \overline{0, 10}$;

7. Покажем,что выполняется изоморфизм:

   $Z[\sqrt{3}i]/ < 1+\sqrt{3}i > \cong Z_4$

   По определению фактор кольца: $\overline{1+\sqrt{3}i} = \overline{0}$; $\overline{\sqrt{3}i} = \overline{-1}$; $\overline{4} = \overline{0}$.

   Получаем $\overline{m+n\sqrt{3}i} = \overline{m-n} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

## 1.2 Кольца главных идеалов.Евклидовы кольца.

**Определение 1.9.** *Коммутативное ассоциативное кольцо с единицей и без делителей нуля называется целостным кольцом(или областью целостности).*

**Определение 1.10.** *Идеал порожденный одним элементом и называется главным.*

**Определение 1.11.** *Целостное кольцо,в котором всякий идеал является главным,называется кольцом главных идеалов.*

**Определение 1.12.** *Элемент $a$ из целостного кольца $R$ называется неразложимым,если он необратим и из равенства: $a = bc$ следует либо $b$ либо с обратимы(но не одновременно).*

**Определение 1.13.** *$a \in R$ называется простым,если он необратим и из условия $a|bc \Rightarrow$ либо $a|c$ либо $a|b$.*

**Теорема 1.1.** $\forall$ *простой элемент из целостного кольца является неразложимым.*

**Определение 1.14.** *Целостное кольцо $A$ называется евклидовым,если существует функция:*

$$N : A/\{0\} \to Z_+$$

*(называемая нормой),удовлетворяющая следующим условиям:*

1. *$N(ab) \geq N(a)$, причем равенство имеет место тогда,когда элемент $b$ обратим;*

2. *для любых $a, b \in A$, где $b \neq 0$, существуют такие $q, r \in A$, что $a = qb + r$ и либо $r = 0$, либо $N(r) < N(b)$.*

**Теорема 1.2.** *В кольце целых чисел всякий идеал - главный.*

Доказательство. Для нулевого идеала теорема выполняется.Рассмотрим при $A \neq (0)$.Обозначим через $d$ наименьшее по абсолютной величины число из $A$ и разделим произвольное число $a \in A$ на $d$:

$$a = dq + r, |r| < |d|.$$

Так как $a$ и $dq$ принадлежит $A$,то их разность $r = a - dq$ также принадлежит $A$.Отсюда следует,что $r = 0$; в противном случае $d$ не было бы наименьшим по абсолютной величине среди отличных от нуля чисел идеала $A$; Следовательно $r = 0$ и $a$ делится на $d$. Итак,идеал $A$ есть главный идеал $(d)$. (Деление с остатком) если $a$ и $b \neq 0$ - два целых гауссовых числа,то всегда можно подобрать такую пару целых гауссовых чисел $v$ и $p$,частное и остаток,что:

$$a = bv + p,$$

причем

$$N(p) < N(b).$$

**Теорема 1.3.** *Пусть $R$ - кольцо главных идеалов и $a, b \in R$.Тогда следующие условия эквивалентны:*

1. $(a, b) = 1$
2. $aR + bR = R$

Доказательство. 2) $\Rightarrow$ 1) Очевидно.
1) $\Rightarrow$ 2) Имеет место следующее равенство $aR + bR = dR$. Тогда $d|a; d|b$. Следовательно, $d \in U(R) \Rightarrow aR + bR = R$

**Теорема 1.4.** *Пусть $R$ - кольцо главных идеалов и $a \in R$.Тогда следующие условия равносильны:*

1. *$a$ - простое элемент в $R$;*
2. *$R/aR$ - поле.*

Доказательство.
Имеют место эквивалентности
$a$ - простое $\Leftrightarrow$ любое $b \notin aR$.
$(a, b) = 1 \Leftrightarrow$ любое $b \notin aR$.
$aR + bR = 1 \Leftrightarrow$ любое $b \notin aR$.
$b + aR$ - обратимо в $R/aR \Leftrightarrow aR$ - поле.

**Теорема 1.5.** *Пусть $R$ - кольцо главных идеалов,$a, b \in R$.Следующие условия эквивалентны:*

1. $aR + bR = R; (a, b) = 1.$
2. $b + aR \in U(R/aR).$

## 1.3 Кольца вычетов.

Напомним,что для любого натурального числа $m$ через $\phi(m)$ обозначается количество натуральных чисел,не превосходящих $m$ и взаимно простых с $m$.Функция $\phi$,называемая функцией Эйлера,обладает следующими свойствами: если $m_1$ и $m_2$ - взаимно простые натуральные числа,то:

$$\phi(m_1 m_2) = \phi(m_1)\phi(m_2).$$

Если $m = p$ - простое число,то $\phi(m) = p - 1$; если $m = p^n$, то $\phi(m) = p^n - p^{(n-1)}$.

**Определение 1.15.** *Факторкольцо кольца целых чисел $Z$ по идеалу $nZ(n \in N)$ называется кольцо вычетом по модулю $n$ и обозначается $Z_n$.*

**Теорема 1.6.** *(Теорема Эйлера) Для всякого целого $a$,взаимно простого с $m$ выполняется сравнение:*

$$a^{\phi(m)} = 1(mod\ m)$$

Доказательство.

Рассмотрим кольцо $Z_m$ вычетов по модулю $m$.Вычет целого числа $a$ будем обозначать через $\overline{a}$.Обратимые элементы кольца $Z_m$ образуют группу относительно умножения.Как известно,элемент $\overline{a}$ обратим в $Z_m$ тогда и только тогда,когда число $a$ взаимно просто с $m$.Значит,порядок группы обратимых элементов равен $\phi(m)$.Отсюда следует:

$$a^{\phi(m)} = 1(mod\ m)$$

.

**Теорема 1.7.** *(Малая теорема Ферма.)*

*Если $p$ - простое натуральное число,то для $\forall$ натурального $a$ разность $a^p - a$ делится на $p$ или если натуральное число $a$ не делится на натуральное простое $p$,то $a^{p-1} - 1$ делится на $p$.*

Доказательство. Напомним,что порядком конечной группы $G$ называется число ее элементов,а порядком элемента $g \in G$ - наименьший показатель его степени,равной единичному элементу $e$ группы $G$.

Пусть $G$ - конечная группа порядка $n$.Из того,что порядок элемента $g \in G$ делит $n$,следует,что $g^n = e$.

Рассмотрим поле $Z_p$ вычетов по модулю $p$.Вычет целого числа $a$ будем обозначать через $\overline{a}$.Ненулевые элементы поля $Z_p$ образуют группу относительно умножения.Порядок этой группы,очевидно,равен $p-1$.Ее единичным элементом является $\overline{1}$.Следовательно,для любого целого числа $a$,не делящегося на $p$, $\overline{a}^{p-1} = \overline{1}$,но это как раз и означает сравнение $a^{p-1} = 1 \mod p$

**Определение 1.16.** *Факториальное кольцо - это целостное кольцо,в котором каждый ненулевой элемент обратим,либо однозначно представляется в виде произведения неприводимых элементов: $x = p_1\dot{p}_2 \dots p_n$, с точностью до перестановки сомножителей и умножения на обратимый элемент.*

**Теорема 1.8.** *В евклидовом кольце всякий необратимый ненулевой элемент может быть разложен на простые множители,причем это разложение единственно с точностью до перестановки множителей и умножения их на обратимые элементы.*

Доказательство.

Назовем необратимый ненулевой элемент $a \in A$ хорошим,если он может быть разложен на простые множители.Предположим,что существуют плохие элементы.Выберем из них элемент с наименьшей нормой.Пусть это будет элемент $a$.Он не может быть простым.Следовательно, $a = bc$, где $b$ и $c$ - необратимые элементы.Имеем $N(b) < N(a)$ и $N(c) < N(a)$ и,значит, $b$ и $c$ - хорошие элементы; но тогда,очевидно,и $a$ - хороший элемент,что противоречит нашему предположению.Таким образом,всякий необратимый ненулевой элемент кольца $A$ может быть разложен на простые множители.

Докажем теперь индукцией по $n$,что если

$$a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m,$$

где $p_i, q_j$ - простые элементы,то $m = n$,и,после подходящей перенумерации множителей,$p_i$ $q_j$ при $i = 1, 2, \dots, n$.

При $n = 1$ это утверждение очевидно.При $n > 1$ имеем $p_1|q_1q_2\dots q_m$ и по лемме 1 существует такой номер $i$,что $p_1|q_i$.

Тогда $p_1$ $q_i$.Можно считать,что $i = 1$ и $p_1 = q_1$.Сокращая равенство на $p_1$,получаем:

$$p_2\dots p_n = q_2\dots q_m.$$

По предположению индукции отсюда следует,что $m = n$ и, после подходящей перенумерации,$p_i$ $q_i$,при $i = 2,\dots,n$.Тем самым утверждение доказано.□

**Теорема 1.9.** *Если p-простое число,то группа $U(Z_p)$-циклическая,т.е. существует первообразный корень по mod p.*

Примеры.

- $p = 5, U(Z_5) = \{\overline{1},\overline{2},\overline{3},\overline{4}\}.\overline{2}^2 = \overline{4},\overline{2}^3 = \overline{3},\overline{2}^4 = \overline{1}$, т.е. $U(Z_5) = \{\overline{1},\overline{2},\overline{2^2},\overline{2^3}\} =< \overline{2} >$ .
- $m = 12, U(Z_{12}) = \{\overline{1},\overline{5},\overline{7},\overline{11}\}.\overline{5}^2 = \overline{1},\overline{7}^2 = \overline{1},\overline{11}^2 = \overline{1}$, т.е. $U(Z_5)$-не является циклической группой.
- $m = 9, U(Z_9) = \{\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}\}.\overline{2}^2 = \overline{4},\overline{2}^3 = \overline{8},\overline{2}^4 = \overline{7},\overline{2}^5 = \overline{5},\overline{2}^6 = \overline{1}$ т.е. $U(Z_9) =< \overline{2} >$ .

**Теорема 1.10.** *Если $p > 2$ - простое,то группа $U(Z_{p^n})$-циклическая,т.е. существует первообразный корень по* $\mod\ p^n$.

Пример.

Найти образующий элемент группы $U(Z_9)$.

Группа $U(Z_3) = \{\overline{1},\overline{2}\}$-циклическая группа с образующим $\overline{2}$. Тогда $a_0 = 2^3 = 2^{p-1}, p = 3, n = 2, \overline{1+p} = \overline{1+3} = \overline{4} \in Z_9$, причем $|\overline{4}| = 3$. Искомый элемент $\overline{a_0}\cdot\overline{1+p} = \overline{8}\cdots\overline{4} = \overline{32} = \overline{5}$. Действительно: $\overline{5^1} = \overline{5},\overline{5^2} = \overline{7},\overline{5^3} = \overline{8},\overline{5^4} = \overline{4},\overline{5^5} = \overline{2},\overline{5^6} = \overline{1},\phi(9) = 6$.

**Теорема 1.11.** *Группа $U(Z_{2^m})$-циклическая при $m = 1, 2$ и является прямым произведением циклической группы порядка 2 и циклической группы порядка $2^{m-2}$ при $m \geq 3$.*

**Теорема 1.12.** *Пусть $n = 2^a p_1^{a_1} p_2^{a_2}\dots p_m^{a_m}$ - разложение числа n на простые множители.Тогда*

$$U(Z/nZ) \approx U(Z/2^aZ) \times U(Z/p_1^{a_1}Z) \times \cdots \times U(Z/p_m^{a_m}Z).$$

*Группа* $U(Z/p_i^{a_i}Z)$ *- циклическая группа порядка* $p_i^{a_i-1}(p_i-1)$,*а группа* $U(Z/2^aZ)$ *- циклическая группа порядка* 1 *или* 2 *при* $a=1$ *или* 2 *соответственно.Если* $a \geq 3$,*то она будет прямым произведением двух циклических групп,одной порядка* 2,*другой порядка* $2^{a-2}$.

# 2 Теорема Вильсона и её обобщение.

## 2.1 Теорема Вильсона

**Теорема 2.1.** *(Теорема Вильсона) Если* $p$ *- простое натуральное число,то* $(p-1)!+1$ *делится на* $p$.

Доказательство.

Утверждение можно переписать как

$$(p-1)! = -1 \text{ в } Z_p$$

где $Z_p = \{1, \ldots, p-1\}$

Элементы $a \in Z_p$ мультипликативной группы поля $Z_p$ обратимы и $a \neq a^{-1}$ за исключение двух случаев,когда $a = \{1, p-1 = -1\}$ Поэтому произведение элементов $Z_p$ равно

$$(p-1)! = \prod_{a=a^{-1}} a \cdot \prod_{a \neq a^{-1}} a = \prod_{a=a^{-1}} a = 1 \cdot (-1) = -1.$$

**Пример.**

Доказать,что в поле целых чисел $Z_p$ выполняется равенство:

$$1^k + \cdots + (p-1)^k = 0, \text{ при } p-1|k$$

и

$$1^k + \cdots + (p-1)^k = 1, \text{ если } p-1 \not| k$$

Решение:

Запишем сумму в ином виде

$1^k + \cdots + (p-1)^k = g^k + \cdots + g^{k(p-1)}$ где $g$ порождающий элемент группы $U(Z_p)$. Далее получаем два случая: $1-g^k \neq 0$ и $1-g^k = 0$

Если $1-g^k = 0$,то $p-1|k$ и

$$g^k + \cdots + g^{k(p-1)} = 1 + \cdots + 1 = p-1 = -1$$

Если $1 - g^k \neq 0$,то $p - 1 \not| k$ и используя формулу суммы геометрической прогрессии,получаем:

$$g^k + \cdots + g^{k(p-1)} = \frac{1 - (g^k)^p}{1 - g^k} - 1 = \frac{1 - g^k}{1 - g^k} - 1 = 0$$

## 2.2 Групповой аналог теоремы Вильсона.

**Лемма 2.2.**

1. *Если $F_2^n$ - арифметическое вещественное пространство над полем $F_2$ и $n > 1$, то*
$$\sum_{\overline{x} \in F_2^n} \overline{x} = 0$$

2. *Если $(G, +)$ - группа у которой элементы имеют порядок не больше 2 и $|G| > 2$,тогда:*
$$\sum_{g \in G} g = 0$$

Доказательство.

1)Для каждого $i$ количества элементов из $F_2^n$,у которых на $i$-ом месте стоит соответственно 0 и 1 совпадают.Таким образом для любого $i$-места количество элементов, у которых на $i$-месте стоит 1 равно $2^{n-1}$ и делится на 2.Следовательно $i$ компонента элемента $\sum\limits_{\overline{x} \in F_2^n} \overline{x}$ равна нулю.Следовательно, $\sum\limits_{\overline{x} \in F_2^n} \overline{x} = 0$ равно нулю.

2) Посколько группа $G$ коммутативна,то бинарную операцию в этой группе будем обозначать через $+$.На $G$ можно ввести операцию умножения на элементы из $Z_2$ согласно следующему правилу:

$$\overline{n}g = ng.$$

Тогда G является векторным пространством над полем $Z_2$.Поскольку $|G| > 2$,то из первого пункта следует равенство:

$$\sum_{g \in G} g = 0$$

**Лемма 2.3.** *Всякая группа четного порядка содержит элемент второго порядка.*

Доказательство.

Предположим,что группа не содержит элемент второго порядка $a^2 = e$ и $a \neq e$,тогда она имеет вид: $G = \{e; a_1; a_1^{-1}; a_2; a_2^{-1}; \cdots ; a_k; a_k^{-1}\}$ тогда $a^{-1} = a$, домножим на $a$ слева,следует: $a^2 = e$ получаем противоречие.

**Теорема 2.4.** *(Теорема Вильсона). Пусть $(G, +)$ - конечная абелева группа,то следующие утверждения верны:*

1. *если $G$ - группа нечетного порядка,то $\sum_{g \in G} g = 0$;*
2. *если $G$ - группа четного порядка и содержит более одного элемента второго порядка,то $\sum_{g \in G} g = 0$;*
3. *если $G$ - группа четного порядка и содержит единственный элемент второго порядка $i$,то $\sum_{g \in G} g = i$;*

Доказательство:

1. Так как группа $G$ нечетного порядка,то в ней отсутствуют элементы 2-ого порядка. Тогда для любого $g \in G$ и $g \neq 0$ существует $-g \in G$ и $-g \neq g$.Следовательно, $\sum_{g \in G} g = 0$;
2. Так как группа $G$ четного порядка,то она содержит элементы 2-ого порядка.Группа $G$ имеет вид: $G = 0, a_1, -a_1, \cdots , a_k, -a_k; i_1, \cdots , i_n$, где $i$-элементы 2-ого порядка,$a_i$ - элементы нечетного порядка.Как было показано в предыдущем пункте: $\sum a_i = 0$.И используя лемму 2.2,показываем,что выполняется равенство: $\sum_{g \in G} g = 0$;
3. Если группа $G$ четного порядка и содержит единственный элемент второго порядка $i$,то $i = -i$.Тогда группу $G = \{e, g_1, -g_1, \ldots , g_n, -g_n, i\}$ где $g_j \neq -g_j, j = \overline{1, n}$. Следовательно $\sum_{g \in G} g = i$;

## 2.3 Теорема Гаусса.

Из основной теоремы предыдущего пункта следуют утверждения.

**Теорема 2.5.** *Пусть $R$ - коммутативное конечное кольцо.Тогда*

1. $\prod_{r\in U(R)} r = 1$ *тогда и только тогда,когда подгруппа* $H = \{r \in U(R) | o(r) = 2^n, n \in N\}$ *не является циклической.*

2. $\prod_{r\in U(R)} r = -1$ *тогда и только тогда,когда подгруппа* $H = \{r \in U(R) | o(r) = 2^n\}$ *является циклической.*

**Теорема 2.6.** *(Теорема Гаусса) Введем следующее множество натуральных чисел:* $M = \{2, 4, p^k, 2p^k | p -$ *нечетное простое число* $, k \in N\}$.

*Пусть* $n \in N$*.Тогда имеют место следующие утверждения:*

1. $\prod_{\overline{m}\in U(Z_n)} \overline{m} = 1$ *тогда и только тогда,когда* $n \notin M$*.*

2. $\prod_{\overline{m}\in U(Z_n)} \overline{m} = -1$ *тогда и только тогда,когда* $n \in M$*.*

Примеры.

- Возьмем группу $U(Z_9) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Сосчитаем произведение её элементов,получаем: $\overline{1} \cdot \overline{2} \cdot \overline{4} \cdot \overline{5} \cdot \overline{7} \cdot \overline{8} = -1$ Так как $9 \in M$.

- Возьмем группу $U(Z_{12}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$. Сосчитаем произведение её элементов,получаем: $\overline{1} \cdot \overline{5} \cdot \overline{7} \cdot \overline{11} = 1$ Так как $12 \notin M$.

# 3 Целые Гауссовые числа.

## 3.1 Неразложимые элементы в кольце целых Гауссовых чисел.

**Определение 3.1.** *Гауссовы целые числа - это комплексные числа,у которых вещественная и мнимая части - целые числа.*

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

*Они образуют подкольцо в* $C$ *и обозначаются* $\mathbb{Z}[i]$*.Кольцо* $\mathbb{Z}[i]$ *является евклидовым относительно нормы:*

$$N(c) = |c|^2 = a^2 + b^2$$

**Теорема 3.1.** *Всякий идеал в кольце целых гауссовых чисел является главным.*

Доказательство. Для нулевого идеала теорема очевидна.Рассмотрим,когда идеал $A \neq (0)$и выберем число с наименьшей нормой; обозначим его через $q$ и разделим произвольное число $a \in A$ на $q$:

$$a = q \cdot v + p, N(p) < N(q)$$

Отсюда видим,что $p$ равен нулю;Таким образом идеал $A$ есть главный идеал $(q)$.

**Теорема 3.2.** *Других единиц,кроме* $\pm 1; \pm i$*,в кольце целых гауссовых чисел не существует.*

Доказательство.

Если $e$ - единица,то $N(e) = 1$. Отсюда полагая $e = x + iy$, получаем такое уравнение:

$$x^2 + y^2 = 1.$$

Это уравнение имеет следующие целые решения: $a)x = 0, y = 1; b)x = 0, y = -1;$

$c)x = 1, y = 0; d)x = -1, y = 0;$

В соответствии с этим для $e$ получаются четыре значения $i, -i, 1, -1$, и легко проверить.

**Теорема 3.3.** *В кольце целых гауссовых чисел число* 2 *разложимо: оно ассоциировано с квадратом* $1 + i$*. При этом* $1 + i$ *уже неразложимо.*

Доказательство.

В самом деле, нетрудно проверить,что

$$2 = -i(1 + i)^2.$$

Двойка, таким образом, ассоциирована с $(1+i)^2$. Остается убедиться, что $1 + i$ неразложимо. Находим, чему равна норма $1 + i$:

$$N(1 + i) = 1^2 + 1^2 = 2.$$

Пусть $\delta$ — какой-нибудь делитель $1+i$. В силу свойства делимости норма $N(1+i) = 2$ должна делиться на норму $N(\delta)$.Отсюда для $N(\delta)$ представляются только две возможности: либо $N(\delta) = 1$, либо $N(\delta) = 2$. В первом случае $\delta$ есть единица. Во втором случае:

$$N(\frac{1 + i}{\delta}) = \frac{N(1 + i)}{N(\delta)} = \frac{2}{2} = 1,$$

т.е.$\frac{1+i}{\delta} = e$, где  — одна из единиц $\pm 1, \pm i$. Иными словами,$\delta$ ассоциировано с $1+i$. Итак,$1+i$ имеет только тривиальные делители,а потому $1+i$ является неразложимым.

**Теорема 3.4.** *Натуральные простые числа  вида $4n+3$ в кольце целых гауссовых чисел неразложимы.*

Доказательство. Пусть $\delta = x + iy$ — какой-нибудь делитель . Как и выше, приходим к заключению, что норма $N(p) = p^2$ должна делиться на $N(\delta)$, вследствие чего для $N(\delta)$ представляются только три возможности:

1. $N(\delta) = 1$
2. $N(\delta) = p^2$
3. $N(\delta) = p$

В первом случае $\delta$ есть единица. Во втором случае $\delta$ ассоциировано с . В самом деле,

$$N\left(\frac{p}{\delta}\right) = \frac{N(p)}{N(\delta)} = \frac{p^2}{p^2} = 1,$$

т.е. $\frac{p}{\delta} = e$,где $e$ — одна из единиц $\pm 1, \pm i$.

Третий случай исключается.В этом можно убедиться следующим образом. Если $N(\delta) = p$, то по определению нормы:

$$x^2 + y^2 = p.$$

Так как  нечетно, то одно из слагаемых, например $x^2$, должно быть четным, а другое нечетным. Значит $x = 2k_1, y = 2k_2 + 1$. Отсюда получается,что

$$4k_1^2 + (2k_2 + 1)^2 = p,$$

или

$$p = 4m + 1,$$

где $m = k_1^2 + k_2^2 + k_2$. Мы пришли к абсурду: натуральное простое число $p$ вида $4n+3$ в то же время имеет вид

$$4m + 1.$$

Итак, $p$ имеет тривиальные делители, т. е. $p$ неразложимо в кольце целых гауссовых чисел.

**Теорема 3.5.** *Натуральное простое число $p$ вида $4n+1$ в кольце целых гауссовых чисел разложимо, оно равно произведению двух неразложимых сомножителей.*

Доказательство.

Обозначим для краткости $\frac{p-1}{2}!$ через $a$. Согласно следствию из теоремы Вильсона $a^2+1$ делится на $p$. Если бы число $p$ было неразложимо в кольце целых гауссовых чисел, то один из сомножителей $a+i$ или $a-i$ произведения $(a+i)(a-i) == a^2+1$ делился бы на $p$. Но последнее невозможно: при делении $a+i$ и $a-i$ на  получаются заведомо дробные комплексные числа $\frac{a}{p}+\frac{1}{p}i, \frac{a}{p}-\frac{1}{p}i$

Остается показать, что $p$ равно произведению двух неразложимых сомножителей. Обозначим через $\delta$ какой- нибудь неразложимый делитель $p$. Норма $N(p)=p^2$, очевидно, должна делиться на норму $N(\delta)$. Поэтому для $N(\delta)$ представляются только такие возможности:

1. $N(\delta)=1$,
2. $N(\delta)=p^2$,
3. $N(\delta)=p$.

Так как $\delta$ в силу своей неразложимости не может равняться единице или быть ассоциированным с $p$, то первые две возможности отпадают. Остается третья возможность:

$$N(\delta)=\delta\overline{\delta}=p.$$

Посмотрим, будет ли $\overline{\delta}$ разложимым. Пусть $\overline{\delta}=ab$,где $a,b$ отличны от единиц. Тогда

$$N(\overline{\delta})=N(a)N(b)=(a\overline{a})(b\overline{b})=(ab)(\overline{a}\overline{b})=\delta\overline{a}\overline{b},$$

или,принимая в расчет соотношение $N(\overline{\delta})=\delta\overline{\delta}$: $\delta\overline{\delta}=\overline{\delta}\overline{a}\overline{b}$. Сокращая это равенство на $\overline{\delta}$, получаем невозможный результат:

$$\delta=\overline{a}\overline{b}$$

невозможный, так как, по предположению,$\delta$ неразложимо. Итак $p$ равно произведению двух неразложимых множителей $\delta$ и $\overline{\delta}$. Теорема, таким образом, полностью доказана.

Примеры неразложимых целых гауссовых чисел.

- $1+i$ - единственное неразложимое,лежащее над $p$, с точностью до ассоциированности,причем $N(1+i)=2$.
- Все простые числа вида $p=4k+3$,где $k \in Z$.

## 3.2 Фактор-кольца колец целых Гауссовых чисел

**Теорема 3.6.** *Имеют место следующие утверждения:*

1. $Z[i]/<1+i> \cong Z_2$;
2. *$p$ - простое и $p=4k+3$, то $Z[i]/<p> \cong F_{p^2}$ - поле состоит из $p^2$ - элементов.* $F_{p^2}=\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a,b \in Z_p\}$
3. *Если $a+bi \in Z[i]$ и $(a+bi)(a-bi)=a^2+b^2=4k+1=p$ - простое целое число,то:* $Z[i]/<a+bi> \cong Z_p$

Доказательство.

1. Третьи пример в параграфе 1.2.
2. Начнем с того,что: $Z[i]/<p>$ - является полем,т.к. $p$ неразложимо в $Z[i]$ и используя тот факт,что кольцо целых гауссовых чисел $a+bi$ изоморфно множеству матриц вида $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ где $a,b \in Z$

   Так как мы факторизуем по идеалу порожденному $p$,то в этом поле $p=0$.Тогда
   $$Z[i]/<p> \cong \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$
   где $a,b \in Z_p$
3. $\overline{a+bi}=\overline{0}$ в $Z[i]/<a+ib>$

   $\overline{(a-bi)(a+bi)}=\overline{a^2+b^2}=\overline{p}=\overline{0}$

   Ясно,что $a$ и $b$ не делятся на $p$.Тогда для некоторых $b$ и $b'$ имеем:

   $1=bb'+pb' \Rightarrow \overline{1}=\overline{bb'}$,

   Тогда

   $\overline{a}+\overline{bi}=\overline{0}$.

$\overline{a}b' + \overline{bb'i} = \overline{0}\ \overline{i} = -\overline{ab'}$.

Тогда для произвольного элемента $\overline{m+ni} \in Z[i]/ < a+ib >$ имеем:
$\overline{m+ni} = \overline{m} + \overline{ni} = \overline{m} + \overline{n}(-\overline{ab'} = \overline{m-nab'} \in \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$

Покажем,что выполняется: $\overline{a} = \overline{b}(0 \leq a, b \leq p-1)$,то $a = b$.

Если $\overline{a} = \overline{b}$,то $\overline{a-b} = \overline{0}$,и $a \neq b$

$a + bi | a - b$

$(a+bi)(c+di) = a - b$

$(a-bi)(c-di) = a - b$ Получим,что: $p \cdot (c^2 + d^2) = (a-b)^2$ Из этого следует,что: $p$ должно делить:$(a-b)^2$,а делит в том случае, когда $a = b$.Противоречие.

## 3.3 Теорема Эйлера для кольца целых гауссовых чисел.

**Определение 3.2.** *Пусть $G$ - кольцо целых Гауссовых чисел. На множестве $G \setminus \{0\}$ определена функция $\phi_G : G \setminus \{0\} \to N$,тогда*

$$\phi_G(m+ni) = |U(G/m+ni)|$$

*Эта функция аналог функции Эйлера для целых Гауссовых чисел.*

**Лемма 3.7.** *Пусть $z$ - простое целое Гауссово число.Тогда*

$$\phi_G(z^n) = |G/ < z > |^n - |G/ < z > |^{n-1}.$$

**Лемма 3.8.** *Пусть выполняются равенства*

$$m + ni = z_1 z_2 \ u\ z_1 G + z_2 G = G,\ \ m.e.\ (z_1, z_2) = 1$$

*где $n, m \in Z; z_1, z_2 \in G \setminus \{0\}$. Тогда $\phi_G(z_1 z_2) = \phi_G(z_1)\phi_G(z_2)$.*

Доказательство. Справедлива следующая цепочка изоморфизмов:

$$G/ < z_1 z_2 > \cong G/ < z_1 > \cap < z_2 > \cong G/ < z_1 > \times G/ < z_2 >$$

Тогда,также справедлив и этот изоморфизм:

$$U(G/ < z_1 z_2 >) \cong U(G/ < z_1 >) \times U(G/ < z_2 >)$$

следовательно

$|U(G/ < z_1 z_2 >)| = |U(G/ < z_1 >)| \cdot |U(G/ < z_2 >)|$, т.е.$\phi_G(z_1 z_2) = \phi_G(z_1)\phi_G(z_2)$.

**Теорема 3.9.** *(Теорема Эйлера для колец целых Гауссовых чисел.)*
*Пусть* $a = m + ni, b = m' + n'i$ *- целые Гауссовые числа.*
*Если* $(a, b) = 1$,*то* $a^{\phi(b)} = 1 \mod b$

Доказательство. Так как $a + bR \in U(R/bR)$,то
$(a + b)^{\phi(b)} = 1 + bR$, т.е. $a^{\phi(b)} + b = 1 + bR$.
Следовательно $a^{\phi(b)} = 1 \mod b$.

**Следствие**(аналог малой теоремы Ферма).

1. Пусть $p = 4k + 1$ - простое число.Если $a \in G$ и $(a, p) = 1$, то
$$a^{(p-1)(p-1)} = 1 \mod p.$$
2. Пусть $p = 4k + 3$ - простое число.Если $a \in G$ и $(a, p) = 1$, то
$$a^{(p^2-1)} = 1 \mod p.$$
3. Если $a \in G$ и $(a, p) = 1$, то
$$a^2 = 1 \mod 2.$$
4. Если $m + ni$ - целое Гауссовое число, $m^2 + n^2 = 4k + 1$ - простое число и $(a, m + ni) = 1$, то
$$a^{p-1} = 1 \mod m + ni$$

# 4 Матричный аналог малой теоремы Ферма.

## 4.1 Матричный аналог малой теоремы Ферма

**Лемма 4.1.** *Собственные значения целочисленной матрицы являются целыми алгебраическими числами.*

Доказательство. Действительно,собственное значение матрицы $A$ есть корень характеристического многочлена $det(XE-A)$,который в случае целочисленной матрицы имеет целые коэффициенты.

**Лемма 4.2.** *Если $a_1, a_2, \ldots, a_r$ - целые алгебраические числа,то для любого простого $p$ имеет место равенство*

$$(a_1 + a_2 + \cdots + a_r)^p = a_1^p + a_2^p + \cdots + a_r^p + pb,$$

*где $b$ есть целое алгебраическое число,являющееся суммой произведений чисел $a_j$ с некоторыми целыми коэффициентами.*

Доказательство. Лемма доказывается индукцией по числу $r$ слагаемых,используя делимость биномиальных коэффициентов $\begin{pmatrix} p & d \end{pmatrix}$ на $p$ для $1 < d < p$ и тот факт,что целые алгебраические числа образуют кольцо.

**Теорема 4.3.** *Если собственные значения матрицы $A$ являются целыми алгебраическими,то для любого простого $p$ имеет место равенство*

$$(TrA)^p = (TrA^p) + pb,$$

*где $b$ есть целое алгебраическое число.*

Доказательство. Обозначим через $\lambda_1, \lambda_2, \ldots, \lambda_n$ все собственные значения целочисленной $(n \times n)$-матрицы $A$.Тогда

$$TrA = \sum_{i=1}^{n} \lambda_i, TrA^p = \sum_{i=1}^{n} \lambda_i^p.$$

Поэтому в силу предыдущих лемм имеет место равенство

$$(TrA)^p = TrA^p + pb,$$

где $b$ есть некоторое алгебраическое число.

**Следствие**.Для любой целочисленной матрицы $A$ и любого простого числа $p$ имеет место сравнение

$$TrA^p = (TrA)^p \mod p.$$

**Теорема 4.4.** *Пусть $a_1, \ldots, a_d$ - корни нормированного многочлена $f \in Z[x]$ степени $d$ и $p$ - простое число. Тогда*

$$a_1^p + \cdots + a_d^p = a_1 + \cdots + a_d \mod p.$$

Доказательство. Индукцией по числу переменных,исходя из сравнения

$$(x+y) = x^p + y^p \mod p$$

получаем сравнение

$$(x_1 + \cdots + x_d)^p = x_1^p + \cdots + x_d^p \mod p$$

в кольце $Z[x_1, \ldots, x_d]$. Подставляя $x_1 = a_1, \ldots, x_d = a_d$ и используя малую теорему Ферма в обычном варианте,получаем

$$a_1^p + \cdots + a_d^p = (a_1 + \cdots + a_d)^p = a_1 + \cdots + a_d \mod p,$$

что и требовалось доказать.

Пример.

Рассмотрим кубический трехчлен $f = x^3 - 9x^2 - 46x + 120 = 0$. Его корни: $a_1 = 12, a_2 = -5, a_3 = 2$. При $p = 17$ получаем

$$a_1^{17} + a_2^{17} + a_3^{17} = 2218610343801114939 = 9 = a_1 + a_2 + a_3 \mod 17.$$

# Список литературы

[1] Л.Я. Окунев, *Целые комплексные числа*, Учпедгиз, 1941.

[2] Э. Б. Винберг, *Малая теорема Ферма и ее обобщения*, Матем.просв., 2008.

[3] Э. Б. Винберг, *Курс алгебры*, Московский центр непрерывного математического образования (МЦНМО), 2013.

[4] А. В. Зарелуа, *О матричных аналогах малой теоремы Ферма* Матем. заметки, 2006.