Билеты по алгебре, 2 модуль

Таисия Чегодаева, ПАДИИ, 1 курс

25 October 2023

1 Кольцо формальных степенных рядов.

Определение: Многочлен - выражение вида $a_0 + a_1 \cdot x + a_2 \cdot x^2 + ... + a_n \cdot x^n$.

Определение: Пусть R - коммутативное кольцо с 1. Тогда кольцо формальных степенных рядов $R[[x]]$ - множество отображений $f : \mathbb{Z}_{\geq 0} \longrightarrow R$ с заданными операциями:
1. Сложение: $(f_1, f_2, f_3, ...) + (g_1, g_2, g_3, ...) = (f_1 + g_1, f_2 + g_2, f_3 + g_3, ...)$.
2. Умножение: $(a_i) \cdot (b_i) = \sum_{i=0}^{n} a_i \cdot b_{n-i}$ - правило свертки.

Утверждение: Кольцо $R[[x]]$ действительно коммутативное кольцо.

Доказательство: Очевидно все, кроме ассоциативности по умножению:
$(a_i \cdot b_i) \cdot (c_i) = \sum_{i+j=n} (a_i \cdot b_i) \cdot c_j = \sum_{i+j=n} (\sum_{r+s=i} a_r \cdot b_s) \cdot c_j = \sum_{i+j=n} \sum_{r+s=i} a_r \cdot b_s \cdot c_j = \sum_{r+s+j=n} a_r \cdot b_s \cdot c_j$.
$(a_i) \cdot (b_i \cdot c_i) = \sum_{r+i=n} a_r \cdot (b_i \cdot c_i) = \sum_{r+i=n} a_r \cdot (\sum_{j+s=i} b_s \cdot c_j) = \sum_{r+i=n} \sum_{j+s=i} a_r \cdot b_s \cdot c_j = \sum_{r+s+j=n} a_r \cdot b_s \cdot c_j$.

Определение: $x = (0, 1, 0, 0, ...)$.

Утверждение: $x^k = (0, 0, 0, ..., 0, 1, 0, 0, 0, ...)$, 1 стоит на k-той позиции.

Доказательство:

Лемма: $f : R \longrightarrow R[[x]]$, a сопоставляется ряду $(a, 0, 0, ...)$. Тогда f - инъективный гомоморфизм.

Доказательство:

Следствие: $\forall k \in \mathbb{Z}_{\geq 0}$ $\forall a_0, a_1, ..., a_k \in R$ $a_0 + a_1 x + a_2 x^2 + ... + a_k x^k = (a_0, a_1, a_2, ..., a_k, 0, 0, ...)$.

Теорема: $f \in R[[x]]$ обратим $\Leftrightarrow a_0 \neq 0$.

Доказательство:

2 Определение кольца многочленов. Степень многочлена и её свойства. Когда кольцо многочленов - область целостности.

Определение: R - коммутативное кольцо, кольцо многочленов над R ($R[x]$) $= \{f \in R : \exists N : \forall n > N \ a_n = 0$ и $f = a_n\}$.

Утверждение: $R[x]$ действительно коммутативное кольцо.

Доказательство:

Определение: $f \in R[x], \ f = \sum_{i=0}^{l} a_i \cdot x^i$. Тогда степень f $(deg(f)) = maxj :$ $(a_j \neq 0)$.

Свойства степени многочлена:
1. $deg(f + g) \leq max(f, g)$.
2. $deg(f \cdot g) \leq deg(f) + deg(g)$.

Доказательство:

3 Теорема о делении с остатком (существование и единственность).

Теорема: K - поле. Тогда $\forall f, g \in K[x] \ \exists! q, r \in K[x] \ : f = g \cdot q + r, \ deg(r) < deg(q)$.

Доказательство:

4 Теорема Безу, теорема о количестве корней многочлена и контрпримеры к ней.

Теорема (теорема Безу): Пусть K - поле, $a \in K$. Тогда остаток от деления f на $x - a = f(a)$.

Доказательство:

Следствие: $f(a) = 0 \Leftrightarrow f$ делится на $x - a$, т.е. a - корень многочлена f.

Следствие: K - поле, $f \in K[x], \ deg(f) = n \geq 0, \ f \neq 0$. Тогда у f не более чем $deg(f)$ корней.

Доказательство:

5 Формальное и функциональное равенство, полиномиальные функции в поле вычетов.

Теорема (о формальном и функциональном равенстве многочленов):
1. K - поле. $f, g \in K[x]$, $max(deg(f), deg(g)) < |K|$. Если $f(a) = g(a)$, то f и g формально равны.
2. K - бесконечное поле. Тогда формально равенство равно функциональному.

Доказательство:

6 Интерполяционная задача, единственность и многочлен Лагранжа.

Интерполяционная задача: Пусть K - поле. $x_1, x_2, ..., x_n \in K$, $\forall i, j\ x_i \neq x_j$ - узлы интерполяции; $y_1, y_2, ..., y_n \in K$. Тогда задача - построить многочлен $f \in K[x] :\ f(x_i) = y_i\ \forall\ i = 1...n$.

Теорема:
1. Любая интерполяционная задача имеет ровно 1 решение среди $f \in K[x]\ :\ deg(f) \leq n - 1$.
2. Всего решений ∞. Если f_0 - решение, то любое решение имеет вид $f = f_0 + (x - x_1) \cdot (x - x_2) \cdot (x - x_n) \cdot g$, где $g \in K[x]$.

Доказательство:

Интерполяционная формула Лагранжа:

$$f = \sum_{i=1}^{n} y_i \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}$$

Утверждение: Любой $f \in K[x]$ однозначно раскладывается на неразложимые слагаемые.

7 Идеалы и главные идеалы в кольцах, Евклидовы кольца и ОГИ – примеры и контрпримеры.

Определение: Пусть R - область целостности. R называется Евклидовым кольцом, если $\exists\ \phi : R$
$\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$, что $\forall f, g\ \exists! q, r :\ \ f = g \cdot q + r$, где $r = 0$ или $\phi(r) < \phi(q)$. ϕ -

евклидова норма.

Определение: R - коммутативное кольцо. $I \subset R$ - идеал, если:
1. $I \neq 0$.
2. $a, b \in I \Longrightarrow a + b \in I$.
3. $a \in I,\ k \in R \Longrightarrow a \cdot k \in I$.

Главный идеал $< a >= Ra = \{ka | k \in R\} = \{x | x \vdots a\}$.
R - кольцо главных идеалов, если в нем все идеалы главные.

Определение: Область главных идеалов - область целостности, где все идеалы главные.

Пример: $\mathbb{Z}$ - область главных идеалов.
$\mathbb{Z}[x]$ - не область главных идеалов.

8 Евклидовы кольца – ОГИ. Существование НОД в ОГИ.

Теорема: Если R - евклидово кольцо, то R - область главных идеалов.

Доказательство:

9 Определение и основные свойства делимости в кольцах. Отношение ассоциированности, равносильные определения.

Определение: R - область целостности, $a, b \in R$. a и b называются ассоциированными, если выполнено хотя бы одно из следующих утверждений:
1. $< a >=< b >$ (множества кратных a и b равны).
2. Множество делителей a совпадает с множеством делителей b.
3. $a \vdots b,\ b \vdots a$.
4. $a = e \cdot \epsilon,\ \epsilon \in R*$.

Доказательство:

Определение: Пусть R - область целостности. Тогда $(a, b) = x$, такой что $a \vdots x$ и $b \vdots x$ и если $a \vdots y, b \vdots y$, то $x \vdots y$.

Теорема: R - область главных идеалов. Тогда $\forall a, b \in R\ \exists (a, b) = x$ и $\exists y, z$, такие что $x = ay + bz$.

Доказательство:

10 Неразложимые элементы и простые элементы, их совпадение в ОГИ, контрпример.

Определение: R - область целостности, $a \in R$. a является неразложимым, если a не обратим и из равенства $a = bc$ следует, что либо b обратим, либо c обратим.

Определение: R - область целостности, $a \in R$. a является простым, когда $bc \,\vdots\, a$, если $b \,\vdots\, a$ или $c \,\vdots\, a$.

Утверждение: Любой простой элемент всегда неразложим.

Доказательство:

Утверждение: В области главных идеалов любой неразложимый элемент является простым.

Доказательство:

11 Основная теорема арифметики в ОГИ.

Теорема: R - область главных идеалов. Тогда любой $b \in R\{$
$0\}$ представим в виде $b = p_1 \cdot p_2 \cdot ... \cdot p_n$, где p_i неразложимы однозначно с точностью до перестановки сомножителей и ассоциированности.

Доказательство:

12 Производная многочлена: "правильное"определение, вывод из него "вычислительного". Линейность и лейбницевость.

Определение: K - поле, $f \in K[x]$. Тогда производной f называется $f' = \frac{f(x)-f(y)}{(}x - y)$ при $x \longrightarrow y$.

Лемма:
1. $(f + g)' = f' + g'$.
2. $(k \cdot f)' = k \cdot f'$, $k \in K$.
3. $(f \cdot g)' = f' \cdot g + f \cdot g'$.

Доказательство:

Утверждение:

$$(a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + ... + a_1 \cdot x + a_0)' = \sum_{i=1}^{n} a_i \cdot i \cdot x^{i-1}$$

Определение: $f \in K[x], a \in K.a$ - корень кратности k, если f делится на $(x-a)^k$, но не делится на $(x-a)^{k+1}$.

Теорема:
1. Если a - корень f кратности k, то a - корень f' кратности $\geq k-1$.
2. Если в $K 1+1+...+1 \neq 0$, то a - корень f' кратности $k-1$.

Доказательство:

13 Характеристика поля и чему она может быть равна. Теорема о кратности корня.

Определение: K - поле. Характеристика K - $char\ K = min(n \in \mathbb{N} | \underbrace{1+1+1+...+1}_{n} = 0)$. Если такого n нет, то $char\ K = 0$.

Пример: $char\ \mathbb{R} = 0$.
$char\ \mathbb{Z}/_{n\mathbb{Z}} = n$.

Теорема:

Доказательство:

14 Формула Тейлора.

Теорема: $f \in K[x],\ deg(f) = n,\ char\ K > n$ или $char\ K = 0$. Тогда

$$f = \sum_{k=0}^{n} \frac{f^{(k)}(a)}{k!} \cdot (x-a)^k$$

Доказательство:

15 Кольца вычетов многочленов, построение, явное описание элементов.

Определение: $h \in K[x],\ K$ - поле. $f \equiv g \mod h$, если $(f-g) \vdots h$.

Утверждение:
1. Сравнимость - отношение эквивалентности на $K[x]$.
2. Операции сложения и умножения корректны и задают структуру кольца на фактор-множестве.
3. h неразложим $\Longleftrightarrow K$ - поле.

Доказательство:

16 Когда кольцо вычетов – поле. Примеры и контрпримеры (для многочленов степени 1 и 2), связь с интерполяцией.

Определение: $K = \mathbb{R},\ f \in K[x],\ f = x^2+1$ - неразложимый. По предыдущей теореме $\mathbb{R}[x]/f$ - поле. Оно называется полем комплексных чисел $\mathbb{C}$.

17 Построение поля комплексных чисел, вещественная и мнимая часть. Модуль и сопряжение, их свойства.

Построение поля $\mathbb{C}$*:*
$\forall f \in K[x]\ f = (x^2+1)\cdot q(x) + ax + b;\ a, b \in \mathbb{R}$.

$\overline{f} = \overline{ax+b},\ \overline{x^2+1} = 0$.

$\mathbb{C} = \{\overline{ax+b} \mid a, b \in \mathbb{R}\}$ - поле.

$\overline{x} = i \Longrightarrow i^2 = (\overline{x})^2 = \overline{x^2} = \overline{x^2+1-1} = \overline{x^2+1} - \overline{1} \Longrightarrow i^2 = -1$.

Алгебраическая форма записи комплексного числа: $z = a + bx = a + bi;\ a = Re(z), b = Im(z)$.

Обратный элемент: $\frac{1}{a+bi} = \frac{a-bi}{(a+bi)(a-bi)} = \frac{a-bi}{a^2+b^2}$.

Определение: $z = a + bi \in \mathbb{C}$. Сопряженный к $z = \overline{z} = a - bi$.

Свойства:
1. $z = \overline{z}$, если $z \in \mathbb{R}$.
2. $\overline{x} : \mathbb{C} \longrightarrow \mathbb{C}$ - изоморфизм поля $\mathbb{C}$ на себя (автоморфизм).
3. $\overline{\overline{z}} = z$: сопряжение - инволюция.
4. $z + \overline{z},\ z \cdot \overline{z} \in \mathbb{R}$.

Доказательство:

Замечание: $z, \overline{z}$ - корни $x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$.

Определение: $|z| = \sqrt{a^2 + b^2}$ - модуль комплексного числа.

Свойства:
1. $|z| \in \mathbb{R}_{\geq 0}$.
2. $|z_1 \cdot z_2| = \sqrt{(z_1 \cdot z_2) \cdot \overline{(z_1 \cdot z_2)}} = \sqrt{z_1 \cdot \overline{z_1}} \cdot \sqrt{z_2 \cdot \overline{z_2}} = |z_1| \cdot |z_2|$

18 Геометрическое изображение, умножение единичных векторов. Аргумент комплексного числа, группа углов, тригогонометрическая форма.

$z = a + bi \longrightarrow (a, b) \in \mathbb{R} \times \mathbb{R}$ - точка на декартовой плоскости.

При сложении векторов их координаты складываются $\Longleftrightarrow$ при сложении комплексных чисел их части складываются.

Сопряжение - симметричное отражение.

$f(z) = z + a$ - параллельный перенос на вектор a.

Любое комплексное число может быть записано единственным образом в виде $z = |z| \cdot (\cos \alpha + i \cdot \sin \alpha)$.

При перемножении комплексных чисел их модули перемножаются, а углы складываются: $z_1 \cdot z_2 = |z_1| \cdot (\cos \alpha + i \cdot \sin \alpha) \cdot |z_2| \cdot (\cos \beta + i \cdot \sin \beta) = |z_1| \cdot |z_2| \cdot (\cos \alpha \cdot \cos \beta + \cos \alpha \cdot i \cdot \sin \beta + \cos \beta \cdot i \cdot \sin \alpha - \sin \alpha \cdot \sin \beta) = |z_1| \cdot |z_2| \cdot (\cos (\alpha + \beta) + i \cdot \sin (\alpha + \beta))$.

α - аргумент z (или угол, который образует комплексное число с осью OX).

Определение: Группа углов - $G(\mathbb{R}, +)$ с заданным отношением: $a \equiv b \mod 2\pi$, если $(a - b) = 2\pi \cdot k,\ k \in \mathbb{Z}$. Тогда это отношение эквивалентности.

Внимание: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ некорректно.

Экспоненциальная запись комплексного числа: $z = |z| \cdot e^{i\varphi}$

19 Формулы для поворотных гомотетий и симметрий в комплексных числах, преобразования подобия. Любая линейная функция — поворотная гомотетия. Композиция поворотных гомотетий.

$f : \mathbb{C} \longrightarrow \mathbb{C}$

$f(z) = z + a$ - параллельный перенос на вектор a.

$f(z) = kz,\ k \in \mathbb{R}_+$ - гомотетия (коэффицент k растяжения).

$f(z) = kz,\ k = -1$ - центральная симметрия в 0.

$f(z) = kz,\ k = e^{i\varphi}$ - поворот на угол φ.

Утверждение: Любая линейная функция - поворотная гомотетия или перенос.

Доказательство:

Следствие: Композиция поворотных гомотетий - поворотная гомотетия или перенос.

Доказательство:

Определение: $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ - преобразование подобия, если f - биекция и $\forall x, y, z, f \in \mathbb{R}^2 \left|\frac{f(x)f(y)}{f(z)f(t)}\right| = \left|\frac{xy}{zt}\right| = const = k$, k - коэффицент подобия.

f - движение, если $\forall x, y \in \mathbb{R}^2\ |f(x)f(y)| = |xy|$.

В данном случае буквы означают начало и конец отрезков.

Упражнение: Любое преобразование подобия - композиция гомотетии и движения.

Теорема Шаля: Любое движение плоскости - или параллельный перенос, или поворот (центральная симметрия), или осевая симметрия (т.е. меняем ориентацию).

Осевая симметрия - относительно $OX : f(z) = \overline{z}$, относительно $b : z = p{\cdot}\overline{z}{+}q$.

Сохраняющее ориентацию преобразование подобия - множество линейных функций.

Преобразование подобия = линейная функция.

20 Формула Муавра, многочлены Чебышёва. Вычисление тригонометрической суммы (ядро Дирихле).

Формула Муавра: $(r \cdot e^{i\varphi})^n = r^n \cdot e^{ni\varphi} = r^n \cdot (\cos(n\varphi) + i \cdot \sin(n\varphi))$.

Применение:
1. Многочлены Чебышева.

$$\cos(n\varphi) = Re(\cos\varphi + i \cdot \sin\varphi)^n$$

$$\cos(n\varphi) = \sum_{k=0}^{\frac{n}{2}} (-1)^k \cdot \binom{n}{2k} \cdot (\cos\varphi)^{n-2k} \cdot (\sin\varphi)^{2k}$$

$$\cos(n\varphi) = \sum_{k=0}^{\frac{n}{2}} (-1)^k \cdot \binom{n}{2k} \cdot (\cos\varphi)^{n-2k} \cdot (1-\cos^2\varphi)^k = T_n(\cos\varphi)$$

$T_1(x) = x,\ T_2(x) = 2x^2 - 1$ - многочлен Чебышева.

2. Ядро Дирихле.

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = Re(e^{i\varphi}) + Re(e^{2i\varphi}) + ... + Re(e^{ni\varphi})$$

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = Re(1 + z + z^2 + ... + z^n)$$

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = Re(\frac{z^{n+1}-1}{z-1})$$

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = Re\left(\frac{e^{i(n+1)\varphi}-1}{e^{i\varphi}-1}\right)$$

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = Re\left(\frac{e^{\frac{i(n+1)\varphi}{2}}(e^{\frac{i(n+1)\varphi}{2}} - e^{\frac{-i(n+1)\varphi}{2}})}{e^{\frac{i\varphi}{2}}(e^{\frac{i\varphi}{2}} - e^{\frac{-i\varphi}{2}})}\right)$$

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = Re\left(e^{\frac{in\varphi}{2}} \cdot \frac{2i \cdot \sin(\frac{n+1}{2}\varphi)}{2i \cdot \sin(\frac{\varphi}{2})}\right)$$

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = Re\left(\cos\frac{n\varphi}{2} + i \cdot \sin\frac{n\varphi}{2}\right) \cdot \frac{\sin\frac{(n+1)\varphi}{2}}{\sin\frac{\varphi}{2}}$$

$$1 + \cos\varphi + \cos(2\varphi) + ... + \cos(n\varphi) = \cos\frac{n\varphi}{2} \cdot \frac{\sin\frac{(n+1)\varphi}{2}}{\sin\frac{\varphi}{2}}$$

21 Извлечение корней из комплексных чисел. Группа корней из 1, её цикличность.

$z_0 \in \mathbb{C},\ z^n = z_0$ - хотим все решения.

1. $z^n = 0 \Longrightarrow z_0 = 0$.

2. $z_0 \in \mathbb{C}* \Longrightarrow z_0 = r \cdot (\cos\varphi + i \cdot \sin\varphi)$. Тогда пусть $z = s \cdot (\cos\psi + i \cdot \sin\psi)$.

По т. Муавра $z^n = s^n \cdot (\cos n\psi + i \cdot \sin n\psi) = r \cdot (\cos\varphi + i \cdot \sin\varphi)$.

$$\begin{cases} s^n = r \\ n\overline{\psi} = \overline{\varphi} \end{cases}$$

$$\begin{cases} s = \sqrt[n]{r} \\ n\overline{\psi} \equiv \overline{\varphi} \mod 2\pi \end{cases}$$

$$\begin{cases} s = \sqrt[n]{r} \\ \psi_k = \frac{\varphi}{n} + \frac{2k\pi}{n} \end{cases}$$

Т.е. $z = \sqrt[n]{r} \cdot (\cos\frac{\varphi}{n} + \frac{2k\pi}{n} + i \cdot \sin\frac{\varphi}{n} + \frac{2k\pi}{n})$

$\sqrt[n]{r} -$ n$-$0.

Утверждение:$\psi_{k_1} = \psi_{k_2} \Longleftrightarrow \frac{\varphi}{n} + \frac{2k_1\pi}{n} = \frac{\varphi}{n} + \frac{2k_2\pi}{n} + 2k\pi \Longleftrightarrow k_1 - k_2 \vdots n \Longleftrightarrow k_1 \equiv k_2 \mod n$, т.е. $k \in \{0, ..., n-1\}$.

$$\sqrt[n]{1} = \left\{ \cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n} \mid k \in \{0, ..., n-1\} \right\}$$

Определение: K - поле. $\mu_n(K) = \{a \in K \mid a^n = 1\}$. $\mu_n(K)$ - группа по умножению.

Лемма: Если K - поле, то $\mu_n(K)$ - циклическая группа.

$\mu_n = \left\{ (e^{\frac{2i\pi}{n}})^k \mid k = \{0, ..., n-1\} \right\} = \left\{ \varepsilon^k \mid k = \{0, ..., n-1\} \right\}$.

Доказательство:

22 Первообразные корни. Лемма о суммах степеней корней из 1.

Определение: Пусть $a \in \mu_n$, т.е. $a^n = 1$. Тогда a - первообразный корень из 1, если:
1. $< a >= \mu_n$.
2. Не существует $k < n,\ k \in \mathbb{N} : a^k = 1$.
3. $a = \cos\frac{2k\pi}{n} + i \cdot \sin\frac{2k\pi}{n},\ gcd(k, n) = 1$.

Доказательство равносильности:

Лемма: $k, n \in \mathbb{N}$.

$$\sum_{\varepsilon \in \mu_n} \varepsilon^k \begin{cases} 0, & k \neq n \cdot l \\ n, & k \,\vdots\, n \end{cases}$$

Доказательство:

23 Дискретное преобразование Фурье. Формула для обратного перобразования.

$f \in \mathbb{C}[x],\ \deg(f) < n$

$\mu_n = \{1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}\}$

$f = \sum_0^{n-1} a_i \cdot x^i$.

$f(\epsilon^k) = b_k,\ 0 \leq k < n$

Дискретное преобразование Фурье:

$$b_i = \sum_{j=0}^{n-1} a_j \cdot \varepsilon^{ij}$$

Теорема:

$$a_i = \frac{1}{n} \sum_{j=0}^{n-1} b_j \cdot \varepsilon^{-ij}$$

Доказательство:

Применение:
1. Перемножение многочленов.

24 Основная теорема алгебры.

Теорема (основная теорема алгебры): $f \in \mathbb{C}[x],\ deg(f) > 0$. Тогда f имеет комплексный корень.

Следствие: $\forall f \in \mathbb{C}[x]\ f = a_0 \cdot (x - x_1) \cdot (x - x_2) \cdot ... \cdot (x - x_n)$ - ровно n корней с учетом кратности.

Доказательство:

Лемма: $f \in \mathbb{C}[x],\ z \in \mathbb{C} : f(z) = 0$. Тогда $f(\overline{z}) = 0$.

Доказательство:

Теорема: $f \in \mathbb{R}[x]$. Тогда $f = a_0 \cdot \prod_i (x - a_i) \cdot \prod_i (x^2 - p_i x + q_i)$, где $D_i = p_i^2 - 4q_i < 0$.

Доказательство:

25 Разложение $x^n - 1$ над $\mathbb{Q}$, $\mathbb{R}$, определение и целочисленность круговых многочленов.

Пример:
$x^n - 1$ раскладывается на n множителей в $\mathbb{C}$.

$x^n - 1$ раскладывается на $(x-1)\prod_{k=1}^{\frac{n-1}{2}}(x^2 - 2\cos\frac{kx\pi}{n} + 1)$ в $\mathbb{R}$, если n нечетное.

$x^n - 1$ раскладывается на $\tau(n)$ (число делителей) множителей в $\mathbb{Q}$.

26 Кольцо гауссовых чисел, его евклидовость.

Определение: Кольцо гауссовых чисел $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

Утверждение: Это действительно кольцо.

Теорема: $\mathbb{Z}[i]$ - евклидово кольцо.

Доказательство:

Следствие: В $\mathbb{Z}[i]$ выполнена основная теорема арифметики и другие свойства из теории чисел.

27 Простота чисел вида 4k + 1 в Гауссовом кольце и Рождественская теорема Ферма.

Теорема (рождественская теорема Ферма): p - простое, $p = 4k + 1$. Тогда $\exists x, y \in \mathbb{Z} \ : \ p = x^2 + y^2$.

Доказательство: