Филиппова Анастасия

Домашнее задание 6

(1) (a) **Решите сравнение:** $239x \equiv 228 \ mod \ 322$.

$239x + 322y = 228, (239, 322) = 1, 1|228 \Rightarrow$ уравнение имеет решение в целых числах. Найдем частное решение:

$239x + 322y = 1$

$239 \begin{pmatrix} 1 \\ 0 \end{pmatrix} 322 \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

$83 \begin{pmatrix} -1 \\ 1 \end{pmatrix} 239 \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

$73 \begin{pmatrix} 3 \\ -2 \end{pmatrix} 83 \begin{pmatrix} -1 \\ 1 \end{pmatrix}$

$10 \begin{pmatrix} -4 \\ 3 \end{pmatrix} 73 \begin{pmatrix} 3 \\ -2 \end{pmatrix}$

$3 \begin{pmatrix} 31 \\ -23 \end{pmatrix} 10 \begin{pmatrix} -4 \\ 3 \end{pmatrix}$

$1 \begin{pmatrix} -97 \\ 72 \end{pmatrix} 3 \begin{pmatrix} 31 \\ -23 \end{pmatrix}$

$x_0 = -97$

$x = -97 \cdot 228 + k \cdot 322 = 102 + 322 \cdot k$.

Ответ: $102 + 322 \cdot k, k \in Z$

(b) **Докажите, что для натурального** $a > 1$ **выполнено** $(a^k - 1, a^n - 1) = (a^{(k,n)} - 1)$**.**

Доказательство:

Пусть $(a^k - 1, a^n - 1) = d$

Не умаляя общности, скажем, что $n < k$.

По алгоритму Евклида: $d = (a^k - 1, a^n - 1) = (a^n(a^{k-n} - 1), a^n - 1) = d$.

$(a^n - 1, a^n) = 1 \Rightarrow d|(a^{k-n} - 1) \Rightarrow (a^n - 1, a^{k-n} - 1) = d$. Будем производить такие же действия на каждом шаге и ,в соответствии с алгоритмом Евклида для целых чисел, получим на последнем шаге $d = (a^{(k,n)} - 1)$. Доказано.

(2) **Являются ли следующие множества кольцами?**

(a) $T = (a + b\sqrt{(}2)|a, b \in Q)$

Множество замкнуто относительно операци сложения и умножения:

$\forall a, b, c, d \in Q \rightarrow (a + \sqrt{2}b) + (c + \sqrt{2}d) = (a + c + (b + d)\sqrt{2}) \in T; (a + \sqrt{2}b)(c + \sqrt{2}d) = (ac + 2bd + (ad + bc)\sqrt{2}) \in T$

1) Аддитивная группа: нейтральный элемент - 0, очевидно, ассоциативность выполнена, обратный к элементу a это $-a$ (очевидно $-a$ принадлежит рассматриваемому множеству).

2) Ассоциативность относительно умножения очевидна:$\forall a, b, c, d, x, y \in Q \rightarrow ((a+\sqrt{2}b)(c+\sqrt{2}d))(x+\sqrt{2}y) = (a + \sqrt{2}b)((c + \sqrt{2}d)(x + \sqrt{2}y))$

3) Дистрибутивность очевидна:$\forall a, b, c, d, x, y \in Q \Rightarrow ((a+\sqrt{2}b)+(c+\sqrt{2}d))(x+\sqrt{2}y) = (a+\sqrt{2}b)(x+\sqrt{2}y) + (c + \sqrt{2}d)(x + \sqrt{2}y))$

Следовательно, данное множество является кольцом.

(b) *** Действительные числа вида** $a + b\sqrt[3]{2}$**,** $a, b \in \mathbb{Q}$

Докажем, что $\sqrt[3]{4}$ иррациональное число. От противного, пусть $\sqrt[3]{4} = \frac{m}{n}, (m, n) = 1 \Rightarrow 4 \cdot n^3 = m^3 \Rightarrow m = 2 \cdot k, k \in \mathbb{Z} \rightarrow 4 \cdot n^3 = 8 \cdot k \Rightarrow n^3 = 2 \cdot k \Rightarrow 2|n \Rightarrow (m, n) \neq 1 \Rightarrow$ получили противоречие, следовательно, $\sqrt[3]{4}$ - иррационально.

Докажем, что множество не замкнуто относительно операции умножения, для этого покажем что $\sqrt[3]{4}$ не лежит во множестве. От противного: пусть $\sqrt[3]{4} = a + b\sqrt[3]{2} \Rightarrow \sqrt[3]{2} \cdot \sqrt[3]{2} = a + b\sqrt[3]{2}$. Домножим левую и правую части равенства на $\sqrt[3]{2} : 2 = a\sqrt[3]{2} + 2b \Rightarrow \sqrt[3]{2} = \frac{2+2b}{a} = \frac{m}{n}, (m, n) = 1$. $\sqrt[3]{2}$ - иррациональное число (доказательство аналогично приведенному выше), но представимо в виде несократимой дроби, следоваетльно, получили противоречие и $\sqrt[3]{4}$ не лежит во множестве, следовательно, не замкнуто относительно операции умножения, то есть не является кольцом.

(c) **Множество функций с положительными значениями на отрезке** $[0, 1]$ **с операциями "сложения"**$f \oplus g = f \cdot g$ **и "умножения"**$f^{\ln g}$**.**

Обозначим данное множество за S. Множество замкнуто относительно операций сложения и умножения:

$\forall f, g \in S \rightarrow f \oplus g, f^{\ln g} \in S$ - очевидно.

1) Аддитивная группа: нейтральный элемент $\exists \ e = 1 \in S : \forall \ f \in S \rightarrow e \cdot f = f \cdot e = f$, обратный элемент: $\forall \ f \in S \ \exists \ f^{-1} = 1/f \in S : f \cdot f^{-1} = f^{-1} \cdot f = e$(обратный точно найдется, так как функция f принимает только не отрицательные значения); ассоциативность: $\forall f, g, t \in S \rightarrow f \cdot (g \cdot t) = (f \cdot g) \cdot t$

2) Ассоциативность относительно умножения(обозначим оперцию умножения как $\times$): $\forall f, g, t \in S \hookrightarrow (f \times g) \times t = f^{\ln g} \times t = (f^{\ln g})^{\ln t} = f^{\ln g \cdot \ln t} = f^{\ln t \cdot \ln g} = f^{\ln(g)^{\ln t}} = f \times g^{\ln t} = f \times (g \times t)$
3) Дисстрибутивность: $\forall f, g, t \in S \hookrightarrow f \times (gt) = f^{\ln gt} = f^{\ln g + \ln t} = f^{\ln g} \cdot f^{\ln t} = (f \times g) \cdot (f \times t)$.
Следовательно, данное множество является кольцом.

(3) **Найдите НОД многочленов** $x^3 + x^2 + 1, x^2 + x + 1$
  (a) **Если это многочлены с рациональными коэфицентами.**
  Так как $(Q, +, \cdot)$ - поле, следовательно,$Q[x]$ Евклидово кольцо, следовательно определен аналог алгоритма Евклида. Найдем НОД с помощью алгоритма Евклида:
  $(x^3 + x^2 + 1, x^2 + x + 1) = (x^3 + x^2 + 1 - x^3 - x^2 - x, x^2 + x + 1) = (x^2 + x + 1, 1 - x) = (x^2 + x + 1 - (-x(1-x)), 1-x) = (1-x, 2x+1) = (2x+1-(-2(1-x)), 1-x) = (3, 1-x) \Rightarrow$так как не получили 0, НОД$(x^3 + x^2 + 1, x^2 + x + 1) = 1$.
  (b) **Если это многочлены с коэффицентами по модулю** 3**.**
  Так как на семинаре было доказано, что Z_p - поле, следовательно Z_3 - поле, то есть $Z_3[x]$ - Евклидово кольцо, то есть можем найти НОД, воспользовавшись аналогом алгоритма Евклида. Действия аналогичны первому пункту задачи: $(x^3 + x^2 + 1, x^2 + x + 1) = (3, 1 - x) = (0, 1 - x) \Rightarrow$ НОД$(x^3 + x^2 + 1, x^2 + x + 1) = 1 - x$.

(4) **Является ли кольцо** Z_{72} **кольцом главных идеалов?**
Необходимо проверить, все ли идеалы в кольце главные. Пусть I - не тривиальный идеал, $c \in I$(так как идеал - подгруппа группы кольца, следовательно $-c \in I$. Пусть $a \in I$ - наименьший элемент идеала. Пусть b - произвольный элемент, принадлежащий иделу, r - остаток от деления b на $a : b = aq + r$. $a, b \in I \Rightarrow a - qb \in I \Rightarrow r \in I$. Так как $a > r$, и a - наименьший элемент идеала, следовательно, $r = 0$. Следовательно, в идеале лежат только элементы, кратные a, и только они. То есть идеал I порожден элементом а. $I = (a) \Rightarrow I$ - главный идеал. Следовательно, Z_n - кольцо главных идеалов, то есть Z_{72} - кольцо главных идеалов.

(5) **Найти:**
  (a) $(45) + (120)$ **в** Z
  $45x + 120y = 15(3x + 8y)$
  $(3x + 8y) = c$
  Так как $(3, 8) = 1$ и $\in Z \hookrightarrow 1|c \Rightarrow \forall c \in Z\ \exists\ x, y \in Z \hookrightarrow (3x + 8y) = c$, то есть $(3x + 8y)$ принимает все возможные целые значения, следовательно: $(45) + (120) = (15)$.
  (b) $(120) + (140) + (160) + (180)$ в Z_{250}
  $(120) + (140) + (160) + (180) = 10(12x + 14y + 16z + 18c)$
  Покажем, что можем получить $10 : x = y = 1, z = c = 0-$ на таком наборе получаем 10. Следовательно, можем получить ве 10. Меньше 10 получить не можем, так как "шаг"кратен 10. Следовательно, $(120) + (140) + (160) + (180) = (10)$ в Z_{250}
  (c) $(x^{2018} - 1) + (x^{840} - 1)$
  $f(x)(x^{2018}-1)+g(x)(x^{840}-1) = (x^2-1)(f(x)(x^{2018}-1)/(x^2-1)+g(x)(x^{840}-1)/(x^2-1))$. НОД$(x^{840} - 1)/(x^2-1), (x^{2018}-1)/(x^2-1) = 1$. Следовательно,$(f(x)(x^{2018}-1)/(x^2-1)+g(x)(x^{840}-1)/(x^2-1)$ - пробегает все значения $Z_{[x]}$. То есть $(x^{2018} - 1) + (x^{840} - 1) = (x^2 - 1)$

(6) **Всегда ли гомоморфный образ идеала является идеалом?**
Контрпример: $\varphi : Z \to Z_{[x]}$. То есть элементы из кольца целых чисел переходят в многочлены нулевой степени (константы). Пусть $I = (a)$ - идеал в Z. $ax \notin \varphi(I)$. Следовательно, гомоморфный образ идеала является идеалом только при сюръективном гомоморфизме.

(7) **Является ли поле евклидовым кольцом?**
1) Так как F - поле, следовательно, нет делителей нуля.
2) $\forall\ a \in F \hookrightarrow N(a) = 1$
3) Так как F^* - группа по умножению$\Rightarrow \forall a, b \in F\ \exists\ c \in F \hookrightarrow a = bc \Rightarrow r = 0$.
Следовательно, поле - евклидово кольцо.

(8) (a) **Докажите, что кольцо чисел Эйзенштейна евклидово. Числа Эйзенштейна – это числа вида $a + b\rho$, где $a,\ b \in \mathbb{Q},\ \rho = e^{2\pi i/3}$.**

1) В кольце чисел Эйзенштейна нет делителей нуля, так как множество чисел Эйзенштейна $\subset \mathbb{C}$, а $\mathbb{C}$ - поле, то есть в $\mathbb{C}$ нет делителей нуля.

2) Определим норму для произвольного числа из множества чисел Эйзенштейна: $N(a + b\rho) = (a + b\rho)^2 = a^2 - ab + b^2$.

3)$N(ab) >= N(a), N(b)$ - следует непосредственно из пункта 2)

4) Обозначим данное множество как A. Докажем, что $\forall a, b, b \neq 0 \in A\ \exists\ q, r \in A \hookrightarrow a = bq - r$. Пусть $\frac{x}{y} = q, q \in \mathbb{C}, x, y \in A$.

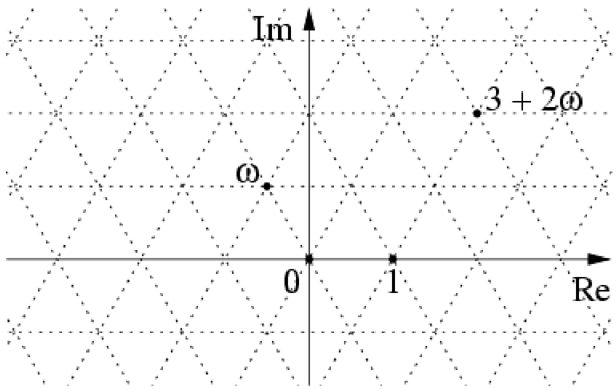

Рис. 1. Множество чисел Эйзенштейна на комплексной плоскости

Если q попадает в точку решетки, изображенной выше, то $x = yq$, то есть $r = 0$ и такое представление числа существует.

Если q не поподает в точку решетки, рассматриваем ромб, в который попало q. Найдем, вершина которая наиболее близка к q(показано на рисунке 2):

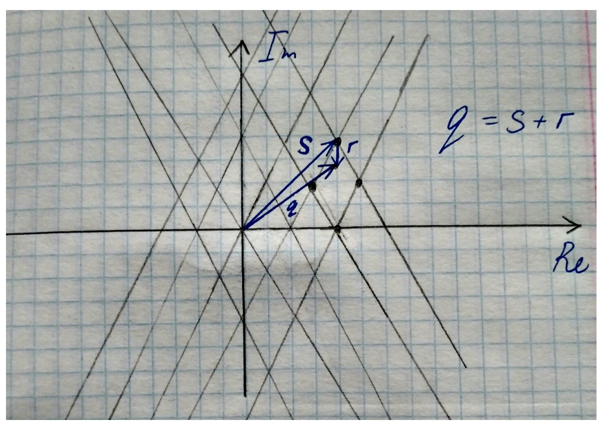

Рис. 2

$q = r + s \Rightarrow x = ys + ry \Rightarrow ry = x - ys, x, y, s \in A \Rightarrow ry \in A$. То есть это искомое представление. $\max\ N(r) = \frac{1}{\sqrt{3}}$ (из ромба) $\Rightarrow N(yr) <= N(y)$.

Получаем, что множество чисел Эйзенштейна является евклидовым кольцом.

(b) **Разложите числа 2 и 3 на простые множители в числах Гаусса и в числах Эйзенштейна.**

1) В числах Эйзенштейна:

$N(2) = 4 = N(2)N(2)$, $a^2 - ab + b^2 = 2 \Rightarrow a^2 - ab + b^2 - 2 = 0$, решим уравнение относительно a: $D = b^2 - 4b^2 + 8 = -3b^2 + 8 >= 0 \Rightarrow b^2 <= \frac{8}{3} \Rightarrow b \in [-1; 1] \subset [-\frac{2\sqrt{2}}{\sqrt{3}}, \frac{2\sqrt{2}}{\sqrt{3}}]$.

$b = 0 : a^2 = 2$ - не подходит, $b = 1 : a^2 - a - 1 = 0, D = 1 + 4 = 5 \Rightarrow a \notin \mathbb{Z}$ - не подходит, $b = -1 : D = 5$ - не подходит. Следовательно, уравнение не имеет решений в целых числах, то есть число 2 - простое в числах Эйзенштейна.

$N(3) = 9, a^2 - ab + b^2 = 3 \Rightarrow a^2 - ab + b^2 - 3 = 0, D = -3b^2 + 12 \Rightarrow b \in [-2; 2]$
$b = 2 : a^2 - 2a + 4 = 0 \Rightarrow a = 1, b = -2 : a^2 + 2a + 1 = 0 \Rightarrow a = -1$
$3 = (1 + 2\rho)(-1 - 2\rho)$. Так как уравнение симметрическое: $3 = (2 + \rho)(2 + \rho^2)$
2) В числах Гаусса:
$N(2) = 4, N(2) = a^2 + b^2 \Rightarrow a^2 + b^2 - 2 = 0, -4b^2 + 8 >= 0 \Rightarrow b \in [-1, 1], b = 1, a = 1; b = -1, a = 1 \Rightarrow 2 = (1 + i)(1 - i)$
$N(3) = 9, a^2 + b^2 - 3 = 0 \Rightarrow b = 1, b = 0, b = -1$ - не подходят, так как $a \notin \mathbb{Z}$. Следовательно, 3 - простое в числах Гаусса.

(9) (a) **Найдите все такие числа Эйзенштейна x, y такие, что $x(-1 - 2\rho) + \rho^2 y = -1 - 2\rho$.**

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + (a + b\rho) \begin{pmatrix} -1 - 2\rho \\ -\rho^2 \end{pmatrix}, \forall\ a, b \in \mathbb{Z}$$

(b) **Найдите все такие числа Гаусса x и y такие, что $x(1 + i) + y(2i) = 3 + i$.**

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 \\ -i \end{pmatrix} + (a + bi) \begin{pmatrix} 2i \\ -1 - i \end{pmatrix}, \forall\ a, b \in \mathbb{Z}$$

(c) **Найдите все такие многочлены $f(x)$, $g(x)$ над $\mathbb{Q}$ такие, что $f(x)(x^3 - 1) + g(x)(x^3 + x^2 + x) = x + 1$.**
НОД$(x^3 - 1, x^3 + x^2 + x) = (x^2 + x + 1, x^3 - 1) = (x^2 + x + 1, 0) = x^2 + x + 1, x^2 + x + 1$ не делит $x + 1$, следовательно, решений нет.

(10) **Верно ли, что множество чисел вида $a + b\sqrt{3}$ $(a, b \in \mathbb{Z})$ евклидово?**
Обозначим исходное множество $S = (a + b\sqrt{3} | a, b \in \mathbb{Z})$.
1) Так как $\mathbb{R}$ - поле, следовательно, в $\mathbb{R}$ нет делителей нуля, следовательно, в S нет делителей нуля.
2) Определим норму $\forall\ c \in S, c \neq 0$: $N : a + b\sqrt{3} \to |a^2 - 3b^2|$. Норму определяем именно таким образом, чтобы выполнялось соотношение:$N(xy) = N(x)N(y)$.
3) Из пункта 2 следует, что $N(xy) >= \max(N(x), N(y))$
4) Аналогично задаче про кольцо чисел Эйзенштейна, изобразим числа из множества S на плоскости:

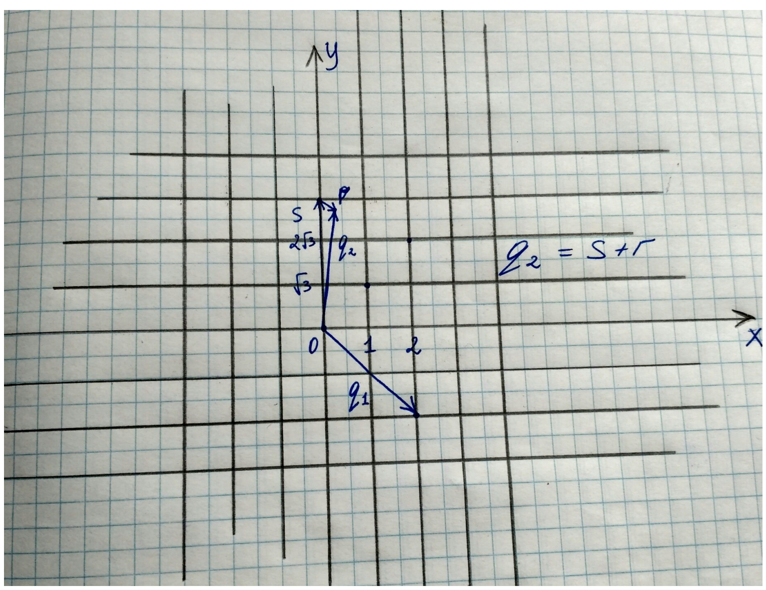

Рис. 3. Множество чисел S на плоскости

По оси Oy откладываем иррациональную часть, по оси Ox целую. Пусть $x/y = q, x, y \in S$. Если q попадает в точку решетки, следовательно, $x = yq$ - нашли искомое представление, $r = 0$.
Если q не попадает в точку решетки, рассмотрим квадрат, в который попало q и найдем наиболее близкую к q вершину (как показано на рисунке 3).
$q = s + r, x = ys + ry, ry = x - ys, x \in S, y, s \in S \Rightarrow yr \in S.$
$N(yr) <= N(y)$, так как максимально возможная норма остатка равна: max $N(r) = 1/2$. Следовательно, нашли искомое представление. То есть во множестве S можно делить числа с остатком (есть аналог алгоритма Евклида)$\Rightarrow$ данное множество является евклидовым кольцом.