Алгебра, семинар 2–6 ноября: делимость

Разделить многочлен P на многочлен Q с остатком – значит найти такие многочлены S и R, $\deg R < \deg Q$, что $P = SQ + R$.

1. Разделите с остатком **a)** $x^5+2x^4+3x^3+4x^2+5x+6$ на x^3+x^2+x+1, **b)** x^{10} на $(x+1)(x+2)$, **c)** x^{10} на x^2-2x+2, **d)** x^{10} на $(x+1)^2$.

Гауссово число – комплексное число вида $a+ib$, $a,b \in \mathbb{Z}$. Его норма – $|a+ib| = a^2+b^2$. Разделить гауссово число p на гауссово число q с остатком – значит найти такие гауссовы числа s и r, $|r| < |q|$, что $p = sq + r$.

2. Разделите с остатком всеми возможными способами **a)** 3 на $1+i$, **b)** 8 на $1+3i$.

3. Гауссово число называется обратимым, если дает 1 в произведении с другим гауссовым числом. Найдите все обратимые гауссовы числа.

4. Гауссово число называется приводимым, если представляется в виде произведения двух необратимых гауссовых чисел. Разложите в произведение неприводимых гауссовых чисел **a)** 3, **b)** 2, **c)** 5, **d)** 7, **e)** 10.

5. Разложите в произведение неприводимых многочленов с целыми коэффициентами **a)** x^3-1, **b)** x^6-1, **c)** $x^3+2x^2-14x+5$, **d)** x^4-7x^2+1, **e)** x^4+x+1, **f)** x^6+x^3+1.

Определение. Множество с двумя операциями, удовлетворяющими всем аксиомам поля, кроме существования обратного, называется *коммутативным кольцом*. Говорят, что элемент a кольца R делит $b \in R$, если $b = ac$ для некоторого $c \in R$.
Примеры колец: целые числа, многочлены, гауссовы числа.

Определение. Пусть каждому элементу $a \neq 0$ кольца R сопоставлено целое число $n(a) \geqslant 0$, так что (1) $n(a) \leqslant n(ab)$ для любых ненулевых a и $b \in R$, и (2) можно делить с остатком: для любых a и $b \in R$ есть q и r, такие что $a = bq + r$, причем $n(r) < n(b)$ или $r = 0$. Тогда функция $n : R \to \mathbb{Z}$ называется *евклидовой нормой*.
Примеры евклидовых норм: модуль целого числа, степень многочлена с коэффициентами в поле, норма гауссового числа.

Определение. НОД (наибольший общий делитель) элементов a и b кольца R – это такой их общий делитель $c \neq 0$, который делится на все остальные общие делители.
Замечание. Если на кольце есть евклидова норма, то у любых элементов a_1 и a_2 существует НОД, который можно найти посредством всем известного алгоритма Евклида: это последний ненулевой элемент последовательности $a_i = (\text{остаток от деления } a_{i-2} \text{ на } a_{i-1})$ при $i = 3, 4, \ldots$

6. Найдите НОД чисел **a)** 7777 и 7777777, **b)** 2^m-1 и 2^n-1. Найдите НОД многочленов **c)** x^3-6x^2+x+4 и x^5-6x+1, **d)** x^m-1 и x^n-1.

7. Найдите НОД **a)** $11+7i$ и $18-i$, **b)** $41+23i$ и $19+5i$.

8. Решите в целых числах уравнение **a)** $13x+20y=1$, **b)** $12x+20y+15z=1$.

9. Найдите многочлены P и $Q \in \mathbb{Z}[x]$, такие что **a)** $(x-1)^3P(x)+(x+1)^3Q(x)=1$, **b)** $(x^3-1)P(x)+(x^5-1)Q(x)=x-1$.

10. Сколько существует неприводимых многочленов степени **a)** 2, **b)** 3 с коэффициентами в поле из q элементов? **c)** Неприводимых многочленов степени 5 в $\mathbb{F}_2[x]$?