Алгебра, семинар 1–4 декабря: квадраты

1. Решите в кольце $\mathbb{Z}/360\mathbb{Z}$ уравнения **a)** $x^2 = 1$, **b)**$^{\text{x}}$ $x^3 = 1$, **c)**$^{\text{x}}$ $x^2 = 49$.
d)$^{\text{x}}$ Сколько решений имеет уравнение $x^2 + 1 = 0$ в $\mathbb{Z}/2^k\mathbb{Z}$ для каждого $k \in \mathbb{N}$?

2. **a)** Докажите, что в кольце $\mathbb{F}_p$ ровно $\frac{p-1}{2}$ полных квадратов.
b) Докажие, что они являются корнями многочлена $x^{\frac{p-1}{2}} - 1 = 0$.
c) Докажите, что $a^{\frac{p-1}{2}} = 1$, если a – полный квадрат в $\mathbb{F}_p$, и $a^{\frac{p-1}{2}} = -1$ иначе.
Число $a^{\frac{p-1}{2}}$ называется символом Лежандра и обозначается $\left(\frac{a}{p}\right)$.

3. **a)** Докажите следующие эквивалентности для каждого простого числа p:

число p не представимо в виде суммы квадратов двух целых чисел $\Leftrightarrow$
число p просто в кольце $\mathbb{Z}[i]$ $\Leftrightarrow$
кольцо $\mathbb{F}_p[x]/(x^2+1)$ является полем $\Leftrightarrow$
число p имеет вид $4k+3$.

число p представимо в виде суммы квадратов двух целых чисел $\Leftrightarrow$
число p разлагается в произведение $q\bar{q}$, где q – простое гауссово число $\Leftrightarrow$
кольцо $\mathbb{F}_p[x]/(x^2+1)$ изоморфно $\mathbb{F}_p \oplus \mathbb{F}_p$ $\Leftrightarrow$
число p имеет вид $4k+1$.
b)$^{\text{x}}$ Выясните, какие простые числа представимы в форме $x^2 - xy + y^2$ для целых x и y, используя вместо гауссовых чисел числа Эйзенштейна $\mathbb{Z}[\sqrt[3]{1}]$.

4. **a)** Докажите, что для любого кольца R матрицы вида $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$, $x, y \in R$, образуют кольцо. Что это за кольца при $\mathbb{K} = \mathbb{Z}, \mathbb{R}$ и $\mathbb{C}$?
b) Докажите, что для любого кольца R матрицы вида $\begin{pmatrix} x & y \\ 0 & x \end{pmatrix}$, $x, y \in R$, образуют кольцо, изоморфное $R[x]/(x^2)$.
c) Докажите, что матрицы вида $\begin{pmatrix} x & -y \\ \bar{y} & \bar{x} \end{pmatrix}$, $x, y \in \mathbb{C}$, образуют кольцо, в котором каждый ненулевой элемент обратим (*тело кватернионов*).
d) Придумайте в кольце вещественных матриц размера 4 подкольцо, изоморфное телу кватернионов.