Научный семинар по теории чисел, ЛНМО, 2022/2023.

Задачи и упражнения.

Элементарная теория чисел.

1. Докажите, что числа Ферма $F_n = 2^{2^n} + 1$ попарно взаимно просты.
Указание. Удобно доказать и воспользоваться рекуррентной формулой для чисел Ферма.

2. Для натурального $m > 1$ вычислите в кольце $\mathbb{Z}/m\mathbb{Z}$:

- Сумму всех элементов.
- Сумму квадратов всех элементов.
- Сумму всех попарных произведений элементов.
- Сумму всех обратимых элементов.
- Сумму квадратов всех обратимых элементов.

3. Докажите *теорему Вильсона.* Сравнение

$$(p-1)! + 1 \equiv 0 \pmod{p}$$

выполняется тогда и только тогда, когда p — простое.

4. Для каких простых чисел p разрешимо сравнение $x^2 + 3 \equiv 0 \pmod{p}$?

5. Докажите, что все решения сравнения $x^2 + 1 \equiv 0 \pmod{p}$, где $p = 4m+1, m \in \mathbb{N}$ имеют вид

$$x = \pm 1 \cdot 2 \cdot \ldots \cdot 2m \pmod{p}$$

Указание. Удобно воспользоваться теоремой Вильсона

Теория колец.

1. Является данное множество кольцом относительно обычных операций сложения и умножения?

$$\mathbb{Q}\left[\sqrt{2}\right] = \left\{ a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q} \right\}.$$

Определение. Пусть R — кольцо. Элемент $r \in R$ называется *нильпотентным*, если $\exists m \in \mathbb{N}\colon r^m = 0$. Наименьшее такое m называется степенью нильпотентности элемента r.

2. Пусть R — кольцо (не обязательно коммутативное), а $r, s \in R$ — коммутирующие нильпотентные элементы. Докажите, что элемент $r + s \in R$ — нильпотентный.

Определение. *Прямой суммой* колец R и S называется кольцо $R \oplus S$, элементами которого являются упорядоченные пары $(r, s),\ r \in R, s \in S$, а операции задаются покомпонентно, то есть

$$(r_1, s_1) +_{R\oplus S} (r_2, s_2) = (r_1 +_R r_2, s_2 +_S s_2), \qquad (r_1, s_1) \cdot_{R\oplus S} (r_2, s_2) = (r_2 \cdot_R r_2, s_1 \cdot_S s_2).$$

3. Докажите, что $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

4. Докажите, что $\mathbb{Z}$ — область главных идеалов.

5. Какой вид имеют простые идеалы в $\mathbb{Z}$?

Комментарий. Эту задачу надо решить сразу после того, как расскажут, что такое простые идеалы.