Алгебра, семинар 9–13 ноября: кольцо $\mathbb{Z}/k\mathbb{Z}$

1. (повторение) Найдите НОД чисел **a)** 7777 и 7777777, **b)** 2^m-1 и 2^n-1.

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

Кольцо $\mathbb{Z}/k\mathbb{Z}$ – это фактормножество $\mathbb{Z}$ по отношению эквивалентности

$$a \equiv b \mod k \;\Leftrightarrow\; k \text{ делит } a-b$$

с операциями $[a]+[b]=[a+b]$ и $[a]\cdot[b]=[ab]$ (через $[a]\in\mathbb{Z}/k\mathbb{Z}$ обозначается класс эквивалентности числа $a\in\mathbb{Z}$, называемый также его *вычетом* по модулю k).

3. Найдите все $x\in\mathbb{Z}$, удовлетворяющие условиям
a) $\begin{cases} x \equiv 1 \mod 7 \\ x \equiv 0 \mod 8 \end{cases}$ **b)** $\begin{cases} x \equiv 0 \mod 7 \\ x \equiv 1 \mod 8 \end{cases}$ **c)** $\begin{cases} x \equiv 2 \mod 7 \\ x \equiv 7 \mod 8 \end{cases}$

4. Произведением колец A и B называется кольцо $A\times B$, элементами которого являются пары $(a,\,b)$, $a\in A$, $b\in B$, а операции определяются покомпонентно: $(a_1,b_1)+(a_2,b_2)=(a_1+a_2,\,b_1+b_2)$, $\quad(a_1,b_1)\cdot(a_2,b_2)=(a_1a_2,\,b_1b_2)$.
a) Китайская теорема об остатках. Докажите, что для взаимно простых m и n естественное отображение $\mathbb{Z}/mn\mathbb{Z}\to(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$, отправляющее вычет числа x по модулю mn в пару (вычет x по модулю m, вычет x по модулю n), является изоморфизмом колец.
b) Докажите, что при этом изоморфизме в пары $(1,0)$ и $(0,1)$ переходят вычеты чисел an и bm, таких что $an+bm=1$.

5. Найдите все $x\in\mathbb{Z}$, удовлетворяющие условиям
a) $\begin{cases} x \equiv 1 \mod 50 \\ x \equiv 0 \mod 61 \end{cases}$ **b)** $\begin{cases} x \equiv 0 \mod 50 \\ x \equiv 1 \mod 61 \end{cases}$ **c)** $\begin{cases} x \equiv 15 \mod 50 \\ x \equiv 2 \mod 61 \end{cases}$ **d)** $\begin{cases} x \equiv 1 \mod 5 \\ x \equiv 3 \mod 6 \\ x \equiv 6 \mod 7 \end{cases}$
e) $\begin{cases} x \equiv 1 \mod 8 \\ x \equiv 9 \mod 10 \end{cases}$

6. Через $(\mathbb{Z}/k\mathbb{Z})^\times$ обозначается множество всех обратимых элементов в кольце $\mathbb{Z}/k\mathbb{Z}$, а через $\varphi(k)$ – число его элементов. Функция $\varphi:\mathbb{N}\to\mathbb{N}$ называется *функцией Эйлера*.
a) Докажите, что для взаимно простых m и n изоморфизм $\mathbb{Z}/mn\mathbb{Z}\to(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/n\mathbb{Z})$ дает взаимно однозначное соответствие $(\mathbb{Z}/mn\mathbb{Z})^\times\to(\mathbb{Z}/m\mathbb{Z})^\times\times(\mathbb{Z}/n\mathbb{Z})^\times$, т.е. $\varphi(mn)=\varphi(m)\varphi(n)$.
b) Докажите, что $\varphi(p^k)=(p-1)p^{k-1}$ для простого числа p. **c)** Вычислите $\varphi(144)$ и $\varphi(1000)$.
d) найдите все $k\in\mathbb{N}$ с $\varphi(k)=10$.

Теорема Эйлера (см. листок 3): если a взаимно просто с k, то $a^{\varphi(k)}\equiv 1 \mod k$.

7. Найдите последние три цифры чисел **a)** 7^{404}, **b)** 5^{404}, **c)** 15^{404}, **d)** 2^{404}.

8. Верно ли, что **a)** $7|a^2+b^2 \;\Rightarrow\; 7|a$ и $7|b$? **b)** $7|a^3+b^3+c^3 \;\Rightarrow\; 7|abc$?

9. Решите уравнения **a)** $x^2\equiv 1 \mod 360$, **b)** $x^3\equiv 1 \mod 360$, **c)** $x^2\equiv 49 \mod 360$.