Алгебра — I

Листок 5

Внимание! Срок сдачи 11 декабря.

1. Назовем два отрезка соизмеримыми, если существует третий, который укладывается в каждом из них целое число раз.

   (a) Верно ли, что два отрезка соизмеримы тогда и только тогда, когда найдется третий, в котором каждый из них укладывается целое число раз?

   (b) От прямоугольника со сторонами a и b отрезают (пока это возможно) квадраты со стороной, равной меньшей из сторон прямоугольника (назовем эту операцию операцией Евклида). К полученному прямоугольнику применим снова операцию Евклида, и т.д.

   Докажите, что a и b соизмеримы тогда и только тогда, когда прямоугольник разрежут на конечное количество квадратов, причем сторона наименьшего квадрата является их общей мерой.

   Верно ли, что сторона наименьшего квадрата является наибольшей общей мерой?

2. Докажите, что в конечной абелевой группе порядка n для любого $d \mid n$ существует хотя бы одна подгруппа порядка d.

3. Сколько попарно неизоморфных групп здесь выписано: $\mathbb{Z}_{24}$, $\mathbb{Z}_{12} \oplus \mathbb{Z}_2$, $\mathbb{Z}_8 \oplus \mathbb{Z}_3$, $\mathbb{Z}_6 \oplus \mathbb{Z}_4$, $\mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2$, $\mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$?

4. (a) Найдите все такие $x \in \mathbb{Z}_p$ (p — простое), что $x^2 = 1$.

   (b) Чему равно произведение всех ненулевых элементов $\mathbb{Z}_p$ (p — простое)?

   (c) Докажите терему Вильсона: Число p является простым тогда и только тогда, когда $(p-1)!+1 \equiv 0 \pmod{p}$.

5. Докажите, что ровно половина элементов $\mathbb{Z}_p^*$ является квадратами (p — простое, $p > 2$, $\mathbb{Z}_p^* = \{x \in \mathbb{Z}_p \mid x \neq 0\}$).

6. Обозначим через $\varphi(m)$ число обратимых элементов в кольце $\mathbb{Z}_m$ (то есть количество натуральных чисел, меньших m и взаимно простых с m). Эта функция называется функцией Эйлера. Докажите теорему Эйлера:

   Если класс вычетов $[a]_m$ обратим, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.