Алгоритм Евклида, вычеты
Семинар 14.

Задача 1. Даны целые числа $a > b > 0$. *Алгоритм Евклида* можно описать так: делим a на b, получаем остаток $r_1 < b$, затем делим b на r_1, получаем остаток $r_2 < r_1$, делим r_1 на r_2, получаем остаток $r_3 < r_2$, и т.д. Докажите, что какой-то остаток r_{n-1} разделится нацело на r_n, и $r_n = \text{НОД}(a, b)$.

Задача 2. *Линейные диофантовы уравнения.*

(a) Докажите, что каждое из чисел $r_1, r_2, \ldots$ можно представить в виде $ax + by$, подобрав подходящие целые x и y.

(b) Как с помощью алгоритма Евклида найти такие целые числа x и y, что $ax + by = \text{НОД}(a, b)$?

(c) Докажите, что НОД двух чисел a, b является наименьшим натуральным числом, которое представляется в виде целочисленной линейной комбинации $ax + by$ чисел a и b.

(d) Опишите все решения в целых числах уравнения $ax + by = c$.

Задача 3. Будем производить с матрицей $A := \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix} \middle| \begin{smallmatrix} a \\ b \end{smallmatrix}\right)$ элементарные преобразования третьего типа, уменьшая модули правой части. То есть вычтем из первой стоки матрицы вторую строчку, умноженную на натуральное число $q_1 = [a/b]$, в полученной матрице вычтем из второй строки первую, умноженную на число $[b/r_1]$. Через конечное число шагов мы придем к матрице вида $\left(\begin{smallmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{smallmatrix} \middle| \begin{smallmatrix} r \\ 0 \end{smallmatrix}\right)$ Докажите, что решения линейного диофантового уравнения $ax + by = \text{НОД}(a, b)$ имеют вид $x = c_{11} + tc_{21}$, $y = c_{12} + tc_{22}$.

Задача 4. Вычислите

(a) $(525, 231)$; **(b)** $(7777777, 7777)$; **(c)** $(2^m - 1, 2^n - 1)$.

Задача 5. Найдите частное и общее решение линейного диофантового уравнения (в целых числах).

(a) $17x + 23y = 38$; **(b)** $nx + (2n - 1)y = 3$; **(c)** $105x + 336y = 9$.

Задача 6. Пусть $\mathbb{Z}_n$ – множество остатков по модулю n.

(a) Докажите, что это кольцо;

(b)* Сформулируйте понятие факторкольца и определите $\mathbb{Z}_n$ как факторкольцо;

(c) Докажите, что подмножество остатков, взаимно простых с n, образует группу по умножению. Данная группа обозначается $\mathbb{Z}_n^*$. Количество таких остатков обозначается $\varphi(n)$ и называется функцией Эйлера числа n.

(d) Вычислите $\varphi(p^n)$, когда p – простое.

(e) Докажите, что $\varphi(ab) = \varphi(a)\varphi(b)$, если a и b взаимно просты.

(f) Докажите, что $\forall x \in \mathbb{Z}_n^*$ выполнено $x^{\varphi(n)} \equiv 1$ по модулю n.

(g) Докажите, что мультипликативная группа кольца $\mathbb{Z}_n$ не всегда является циклической.

Указание: Рассмотрите случай $n = pq$, где p, q – различные нечетные простые.

Задача 7. Вычислите две последние цифры у чисел **(a)** 2^{2014}; **(b)** 3^{2014}.

Задача 8. Докажите, что ваше 28 -летие будет в такой же день недели, как вы родились.

Задача 9. (Китайская теорема об остатках.) Докажите, что если числа m и n взаимно просты, то кольца $\mathbb{Z}_m \times \mathbb{Z}_n$ и $\mathbb{Z}_{mn}$ изоморфны.

Задача 10. Докажите, что если в абелевой группе есть элементы порядков m и n, то есть и элемент порядка $HOK(m, n)$.

Задача 11. Докажите, что любое кольцо вида $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \ldots \times \mathbb{Z}_{n_k}$ изоморфно некоторому кольцу вида $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_l}$, где числа $m_1, m_2, \ldots, m_l$ таковы, что каждое следующее является делителем предыдущего.

Задача 12. *Нильпотентными* называются остатки, которые при возведении в некоторую степень сравнимы с нулём.

(a) При каких значениях n встречаются ненулевые нильпотентные элементы кольца $\mathbb{Z}_n$?

(b) Докажите, что сумма и произведение нильпотентных элементов – снова нильпотентный элемент.

(c) Вычислите количество нильпотентных элементов в $\mathbb{Z}_n$, используя разложение на простые множители числа n.

Задача 13*. Даны m целых чисел. За один ход разрешается прибавить по единице к любым n из них. При каких m и n всегда можно за несколько таких ходов сделать числа одинаковыми?