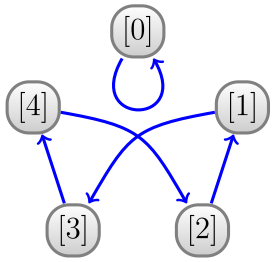
Определение 1. Пусть $m \in \mathbb{N}$. Для каждого целого r множество целых чисел, сравнимых с r по модулю m, называется *классом (вычетов) по модулю* m и обозначается через $[r]_m$ (или просто $[r]$, если понятно, о каком m идёт речь). Множество всех классов вычетов по модулю m обозначается $\mathbb{Z}_m$. Класс $[0]_m$ называется *нулевым*.

Задача 1. **а)** Докажите, что $[r]_m = \{mq + r \mid q \in \mathbb{Z}\}$. **б)** Сколько элементов в множестве $\mathbb{Z}_m$?

Определение 2. Для любых классов вычетов $[r]$ и $[s]$ по модулю m определим их *сумму* и *произведение*, положив $[r] + [s] = [r + s]$ и $[r] \cdot [s] = [r \cdot s]$.

Задача 2. Докажите, что сложение и умножение в $\mathbb{Z}_m$ определены корректно.

Замечание. Можно представлять себе $\mathbb{Z}_m$ как множество чисел $0, 1, 2, \ldots, m-1$, которые складываются и умножаются «по модулю m» (как остатки от деления на m).



Задача 3. **а)** Составьте таблицы сложения и умножения в $\mathbb{Z}_2$, $\mathbb{Z}_3$ и $\mathbb{Z}_4$.
б) Найдите сумму всех элементов $\mathbb{Z}_m$.

Задача 4. Изобразим элементы $\mathbb{Z}_m$ точками, зафиксируем $\alpha \in \mathbb{Z}_m$ и из каждой точки $\omega \in \mathbb{Z}_m$ проведём стрелку в точку $\alpha \cdot \omega$. Нарисуйте такие картинки для каждого $\alpha \in \mathbb{Z}_m$ при $m = 6$ и $m = 7$. (На рисунке дан пример для $\mathbb{Z}_5$ при $\alpha = [3]$.)

Задача 5. Приведите пример, когда произведение двух ненулевых классов вычетов по модулю m является нулевым классом. Такие классы называют *делителями нуля* в $\mathbb{Z}_m$.

Задача 6. Докажите, что натуральное число m простое если и только если в $\mathbb{Z}_m$ нет делителей нуля.

Определение 3. Класс $\beta \in \mathbb{Z}_m$ называется *обратным* (по умножению) к классу $\alpha \in \mathbb{Z}_m$, если $\alpha \cdot \beta = [1]$. Класс, к которому имеется обратный, называется *обратимым* (по умножению).

Замечание. Чтобы не писать всюду числа в квадратных скобках, можно заменять классы на их представителей (числа без скобок), но тогда равенства для классов надо заменять на соответствующие сравнения для их представителей: например, равенство $[r]_m \cdot [s]_m = [1]_m$ эквивалентно сравнению $r \cdot s \equiv 1 \pmod{m}$.

Задача 7. Докажите, что ненулевой класс не является делителем нуля если и только если он обратим.

Задача 8. **а)** Докажите, что целое $m > 1$ простое если и только если для любого ненулевого класса в $\mathbb{Z}_m$ найдётся обратный к нему класс из $\mathbb{Z}_m$. **б)** Докажите, что обратный класс единствен.

Задача 9. Пусть p — простое число.
а) Найдите все такие α из $\mathbb{Z}_p$, что $\alpha^2 = [1]$ (то есть α обратен (по умножению) сам себе).
б) Чему равно произведение всех ненулевых элементов $\mathbb{Z}_p$?

Задача 10. *(Критерий Вильсона)* Докажите, что целое число $m > 1$ простое тогда и только тогда, когда $(m-1)! + 1 \equiv 0 \pmod{m}$.

Задача 11. Пусть p — простое, $\alpha \in \mathbb{Z}_p$, $\alpha \neq [0]$.
а) Домножим все элементы $\mathbb{Z}_p$ на α. Докажите, что снова получатся все элементы $\mathbb{Z}_p$.
б) Выведите из пункта а) *малую теорему Ферма*: $\alpha^{p-1} = [1]$.

Задача 12. **а)** Пусть p простое и имеет вид $4k + 3$. Найдется ли такое целое x, что $x^2 \equiv -1 \pmod{p}$?
б) Докажите, что если $x^2 + 1$ делится на нечётное простое число p, то p имеет вид $4k + 1$.
в) Докажите, что простых чисел вида $4k + 1$ бесконечно много.
г)* Пусть p простое и имеет вид $4k + 1$. Найдите такое целое x, что $x^2 \equiv -1 \pmod{p}$.

Задача 13. Пусть p — простое число. Докажите, что
а) C_p^k делится на p при всех таких целых k, что $1 < k < p$;
б) в $\mathbb{Z}_p$ выполнено тождество $(\alpha + \beta)^p = \alpha^p + \beta^p$.

Задача 14. Изобразим элементы $\mathbb{Z}_m$ точками, зафиксируем *обратимый (по умножению)* элемент $\alpha \in \mathbb{Z}_m$ и из каждой точки $\omega \in \mathbb{Z}_m$ проведём стрелку в точку $\alpha \cdot \omega$. Докажите, что на этой картинке
а) движение по стрелкам распадается на непересекающиеся циклы;
б) каждый цикл, содержащий хоть один обратимый класс, весь состоит из обратимых классов;
в) циклы, состоящие из обратимых классов, имеют одинаковую длину.

Задача 15. *(Теорема Эйлера)* Пусть $m \in \mathbb{N}$, $\varphi(m)$ — количество натуральных чисел, не превосходящих m и взаимно простых с m. Докажите, что $a^{\varphi(m)} \equiv 1 \pmod{m}$, если $a \in \mathbb{Z}$ и $(a, m) = 1$.

Задача 16. Найдётся ли **а)** 3^k, оканчивающееся на 0001; **б)** $2^k - 1$, делящееся на данное нечётное x?

1 а	1 б	2	3 а	3 б	4	5	6	7	8 а	8 б	9 а	9 б	10	11 а	11 б	12 а	12 б	12 в	12 г	13 а	13 б	14 а	14 б	14 в	15	16 а	16 б