Листок №23

Классы вычетов

19.09 – 30.09.2018
33/28/23 з. на 5/4/3

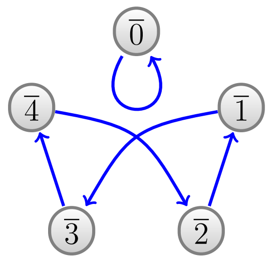
Определение 1. Пусть $m \in \mathbb{N}$. Рассмотрим отношение эквивалентности «разность делится на m» на множестве целых чисел (см. задачу 6, е листка 22), обозначение: $\equiv$. Класс эквивалентности числа r называют *классом (вычетов) по модулю* m и обозначают $\overline{r}_m$ (или просто $\overline{r}$, если понятно, о каком m идёт речь). Множество всех классов вычетов по модулю m обозначают $\mathbb{Z}/m\mathbb{Z}$. Класс $\overline{0}_m$ называют *нулевым.*

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

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

Задача 2. Докажите, что сложение и умножение в $\mathbb{Z}/m\mathbb{Z}$ не зависит от выбора представителей классов эквивалентности (то есть сложение и умножение *согласованы* с отношением эквивалентности).

Замечание. Можно представлять себе $\mathbb{Z}/m\mathbb{Z}$ 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 $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ и $\mathbb{Z}/4\mathbb{Z}$. **б)** Найдите сумму всех элементов $\mathbb{Z}/m\mathbb{Z}$.

Задача 4✎. Изобразим элементы $\mathbb{Z}/m\mathbb{Z}$ точками, зафиксируем $\alpha \in \mathbb{Z}/m\mathbb{Z}$ и из каждой точки ω проведём стрелку в точку $\alpha \cdot \omega$. Нарисуйте такие картинки для каждого $\alpha \in \mathbb{Z}/m\mathbb{Z}$ при $m = 6$ и $m = 7$. (На рисунке — пример для $\mathbb{Z}/5\mathbb{Z}$, $\alpha = \overline{3}$.)

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

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

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

Замечание. Чтобы не писать всюду числа с чертой сверху, можно заменять классы на их представителей (числа без черты), но тогда равенства для классов надо заменять на соответствующие сравнения для их представителей: например, равенство $\overline{r}_m \cdot \overline{s}_m = \overline{1}_m$ эквивалентно сравнению $r \cdot s \equiv 1 \pmod{m}$.

Задача 7✎. Выпишите все обратимые элементы и найдите к ним обратные в $\mathbb{Z}/m\mathbb{Z}$ для $m = 5, 6, 7, 8$.

Задача 8. Докажите, что ненулевой класс не является делителем нуля если и только если он обратим.

Задача 9✎. **а)** Докажите, что целое $m > 1$ простое если и только если для любого ненулевого класса в $\mathbb{Z}/m\mathbb{Z}$ найдётся обратный к нему класс из $\mathbb{Z}/m\mathbb{Z}$. **б)** Докажите, что обратный класс единствен.

Задача 10✎. Решите уравнения **а)** $8x = 3$ в $\mathbb{Z}/13\mathbb{Z}$; **б)** $7x = 2$ в $\mathbb{Z}/11\mathbb{Z}$; **в)** $x^2 = 1$ в $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$.

Задача 11. Для каких $\overline{a}$ из $\mathbb{Z}/m\mathbb{Z}$ равенство $\overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{y}$ при «сокращении» на $\overline{a}$ остаётся верным?

Задача 12. Пусть p — простое. **а)** Найдите все такие α из $\mathbb{Z}/p\mathbb{Z}$, что $\alpha^2 = \overline{1}$ (то есть α обратен (по умножению) сам себе). **б)** Докажите, что остальные элементы разбиваются на пары взаимнообратных. **в)** Чему равно произведение всех ненулевых элементов $\mathbb{Z}/p\mathbb{Z}$? **г)** (*Критерий Вильсона*) Докажите, что целое число $m > 1$ простое тогда и только тогда, когда $(m-1)! + 1 \equiv 0 \pmod{m}$.

Задача 13. Пусть p — простое, $\alpha \in \mathbb{Z}/p\mathbb{Z}$, $\alpha \neq \overline{0}$. **а)** Домножим все элементы $\mathbb{Z}/p\mathbb{Z}$ на α. Докажите, что снова получатся все элементы $\mathbb{Z}/p\mathbb{Z}$. **б)** Выведите из пункта а) *малую теорему Ферма*: $\alpha^{p-1} = \overline{1}$.

Задача 14✎. **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 $x^2 \equiv -1 \pmod{p}$.
Указание. Воспользуйтесь задачей 12в).

Задача 15. Пусть p — простое. Докажите, что **а)** C_p^k делится на p при всех таких целых k, что $1 < k < p$; **б)** в $\mathbb{Z}/p\mathbb{Z}$ выполнено тождество $(\alpha + \beta)^p = \alpha^p + \beta^p$. **в)** Выведите из пункта б) малую теорему Ферма.

Задача 16✎. Изобразим элементы $\mathbb{Z}/m\mathbb{Z}$ точками, зафиксируем *обратимый (по умножению)* элемент $\alpha \in \mathbb{Z}/m\mathbb{Z}$ и из каждой точки $\omega \in \mathbb{Z}/m\mathbb{Z}$ 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 17. *(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 18. 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	9 а	9 б	10 а	10 б	10 в	11	12 а	12 б	12 в	12 г	13 а	13 б	14 а	14 б	14 в	14 г	15 а	15 б	15 в	16 а	16 б	16 в	17	18 а	18 б