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 $\mathbb{Z}_m$?

Задача 2. Для любых классов вычетов $[r]$ и $[s]$ по модулю m определим их *сумму* и *произведение*, положив $[r] + [s] = [r + s]$ и $[r] \cdot [s] = [r \cdot s]$. Докажите, что сложение и умножение в $\mathbb{Z}_m$ определены корректно.

Замечание. Можно представлять себе $\mathbb{Z}_m$ как множество чисел 0, 1, 2, ..., $m - 1$, 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. Пусть p — простое число. Докажите, что в $\mathbb{Z}_p$ выполнено тождество $([a] + [b])^p = [a]^p + [b]^p$.

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.

Задача 7. Докажите, что целое $m > 1$ простое если и только если для любого ненулевого класса $[a]_m$ найдётся такой класс $[b]_m$, что $[a]_m \cdot [b]_m = [1]_m$ (при этом $[b]$ называется *обратным* (по умножению) к $[a]$).

Задача 8. Пусть p — простое число. **а)** Найдите все такие $[a]$ из $\mathbb{Z}_p$, что $[a]^2 = 1$ (то есть $[a]$ обратен (по умножению) сам себе). **б)** Чему равно произведение всех ненулевых элементов $\mathbb{Z}_p$?

Задача 9. *(Теорема Вильсона)* Докажите, что целое $m > 1$ простое если и только если $(m-1)! + 1 \equiv 0 \pmod{m}$.

Задача 10. Пусть p — простое, $a \in \mathbb{Z}_p$, $a \neq 0$. **а)** Домножим все элементы $\mathbb{Z}_p$ на a. Докажите, что снова получатся все элементы $\mathbb{Z}_p$. **б)** Выведите из пункта а) малую теорему Ферма: $a^{p-1} \equiv 1 \pmod{p}$.

Задача 11. **а)** Пусть простое p имеет вид $4k + 3$. Найдется ли такое целое число 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.

Представимость чисел в виде суммы двух квадратов

Задача 12. Пусть p — простое вида $4k + 1$, и пусть $x = (2k)!$. Докажите, что $x^2 \equiv -1 \pmod{p}$.

Задача 13. Пусть p — простое вида $4k+1$, и пусть x удовлетворяет сравнению $x^2 \equiv -1 \pmod{p}$. Докажите, что
а) $(a + xb)(a - xb) \equiv a^2 + b^2 \pmod{p}$ при $a, b \in \mathbb{Z}$;
б) среди чисел вида $m + xn$, где $m, n \in \mathbb{Z}$, $0 \leqslant m, n \leqslant [\sqrt{p}]$, найдутся два с равными остатками от деления на p;
в) найдётся ненулевое число вида $a + bx$, делящееся на p, где $a, b \in \mathbb{Z}$, причем $|a| < \sqrt{p}$ и $|b| < \sqrt{p}$;
г) p представимо в виде суммы двух квадратов целых чисел.

Задача 14. Пусть p — простое число вида $4k + 3$, числа a и b целые и $a^2 + b^2$ делится на p. Докажите, что a делится на p и b делится на p. *Указание:* воспользуйтесь задачей 11, а).

Задача 15. Докажите, что произведение чисел, представимых в виде суммы двух квадратов целых чисел, само представимо в виде суммы двух квадратов целых чисел.

Задача 16. Сформулируйте и докажите теорему о том, как по разложению числа на простые множители узнать, представимо ли это число в виде суммы двух квадратов целых чисел.

Теорема Эйлера и китайская теорема об остатках

Задача 17. Изобразим элементы $\mathbb{Z}_n$ точками, зафиксируем остаток $a \in \mathbb{Z}_n$, и из каждой точки $x \in \mathbb{Z}_n$ проведём стрелку в точку $a \cdot x$. Докажите, что если a обратим (по умножению), то на этой картинке движение по стрелкам распадается на непересекающиеся циклы, причём каждый цикл, содержащий хоть одно обратимое число, весь состоит из обратимых чисел, и циклы, состоящие из обратимых чисел, имеют одинаковую длину.

Задача 18. *(Теорема Эйлера)* Пусть $m \in \mathbb{N}$, $\varphi(m)$ — количество натуральных чисел, меньших 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 19. Существует ли **а)** 3^k, заканчивающееся на 0001; **б)** $2^n - 1$, делящееся на данное нечётное m?

Задача 20. **а)** Найдите $\varphi(p^\alpha)$, где p простое, $\alpha \in \mathbb{N}$. **б)** Докажите, что $\varphi(ab) = \varphi(a)\varphi(b)$, если $(a, b) = 1$.

Задача 21. (*Китайская теорема об остатках*) **а)** Пусть натуральные $m_1, \ldots, m_k$ попарно взаимно просты. Докажите, что для любых целых $b_1, \ldots, b_k$ существует такое целое x, что $x \equiv b_1 \pmod{m_1}$, ..., $x \equiv b_k \pmod{m_k}$, и это x можно выбрать так, что $0 \leqslant x < m_1 \cdot m_2 \cdot \ldots \cdot m_k$. **б)** С помощью задачи 18 явно укажите такое x.

Задача 22. Найдите такое целое $a > 0$, что $a/2$ — точный квадрат, $a/3$ — точный куб, $a/5$ — точная 5-я степень.

Задача 23*. Существует ли **а)** сколь угодно длинная; **б)** бесконечная арифметическая прогрессия, каждый член которой — степень натурального числа с целым показателем, большим 1?