▷ Запись $a \equiv b \pmod n$, если $a - b \vdots n$. Говорят, что a *сравнимо с* b *по модулю* n. Например, $11 \equiv -3 \pmod 7$; $x \equiv 7x \pmod 3$. ◁

▷ Множество всех остатков по модулю n обозначают $\mathbb{Z}/n\mathbb{Z} := \{0, 1, ..., n-1\}$ ◁

Задача 1. Прочитайте определение и покажите, что $a \equiv b (mod\, n)$, если и только если у a и b одинаковые остатки от деления на n.

Задача 2. Могут ли среди k последовательных чисел найтись 2 с одинаковым остатков от деления на k?

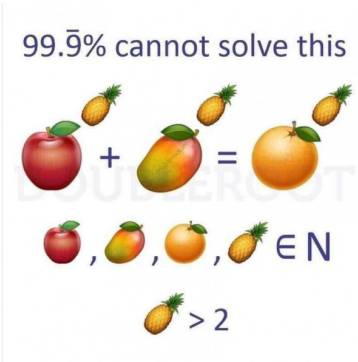
Задача 3. Пусть $a \equiv b \pmod n$, $e \equiv f \pmod n$. Докажите, что **а)** остатки можно складывать и вычитать: $a + e \equiv b + f \pmod n$; **б)** остатки можно умножать $ae \equiv bf \pmod n$; **в)** можно возводить в степень $a^m \equiv b^m \pmod n$.
Во что превратятся сравнения при $e = f$?

Задача 4. Пусть p – простое, a – ненулевой остаток по модулю p. **а)** Докажите, что если умножить a на все остатки по модулю p, снова получатся все остатки. **б)** (*Малая теорема Ферма*) Докажите, что $a^{p-1} \equiv 1 \pmod p$). (1)

Задача 5. **а)** Найдите два ненулевых остатка, произведение которых – нулевой остаток. Такие остатки называют *делителями нуля*. **б)** Докажите, что натуральное число n простое, если и только если в $\mathbb{Z}/n\mathbb{Z}$ нет делителей нуля.

▷ Остаток b называется *обратным* к остатку a $(a, b \in \mathbb{Z}/n\mathbb{Z})$, если $a \cdot b \equiv 1 \pmod n$. Если к классу есть обратный, он называется *обратимым*. Например, $2 \cdot 3 \equiv 1 \pmod 5$. ◁

Задача 6. Найдите все обратимые и обратные к ним остатки по модулю 6,7,8.



Задача 7. **а)** Докажите, что каждый ненулевой остаток либо является делителем нуля, либо обратим. Выведите отсюда, что в $\mathbb{Z}/p\mathbb{Z}$ у каждого ненулевого остатка есть обратный. **б)** Докажите, что обратный остаток единственен.

Задача 8. Докажите, что остаток от деления простого числа на 30 есть простое число или 1.

(1) *Указание.* Перемножьте ненулевые элементы $\mathbb{Z}/p\mathbb{Z}$.

Дополнительные задачи

Задача 9. **а)** Найдите все остатки a в $\mathbb{Z}/p\mathbb{Z}$, такие что $a^2 \equiv 1 \pmod{p}$.
б) Докажите, что остальные ненулевые остатки разбиваются на пары взаимно-обратных. **в)** Чему равно произведение всех ненулевых остатков в $\mathbb{Z}/p\mathbb{Z}$?
г) (*Критерий Вильсона*) Докажите, что натуральное число n простое, если и только если $(m-1)! + 1 \equiv 0 \pmod{n}$.

Задача 10. 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 $(a+b)^p = a^p + b^p$.
в) Выведите из пункта б) малую теорему Ферма.

Задача 11*. (*Теорема Эйлера*) Пусть $a, n \in \mathbb{N}$, $(a, n) = 1$, $\varphi(n)$ – количество натуральных чисел, не превосходящих n и взаимно простых с n (функция Эйлера). Докажите, что $a^{\varphi(n)} \equiv 1 \pmod{n}$.