ТАБЛИЦЫ УМНОЖЕНИЯ ПО ПРОСТОМУ МОДУЛЮ

На прошлом уроке мы убедились методом экспериментальной математики, что:

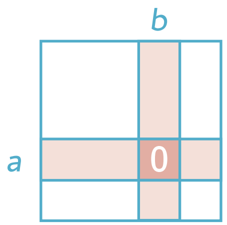
таблицы умножения* по модулю n

не содержат нулей, если n — простое	**содержат нули, если n — не простое**

Докажем это строго для произвольного модуля.

ДОКАЗАТЕЛЬСТВО

Если n — не простое, то $n = a \cdot b$, и в таблице остатков на пересечении строки a и столбца b стоит 0.

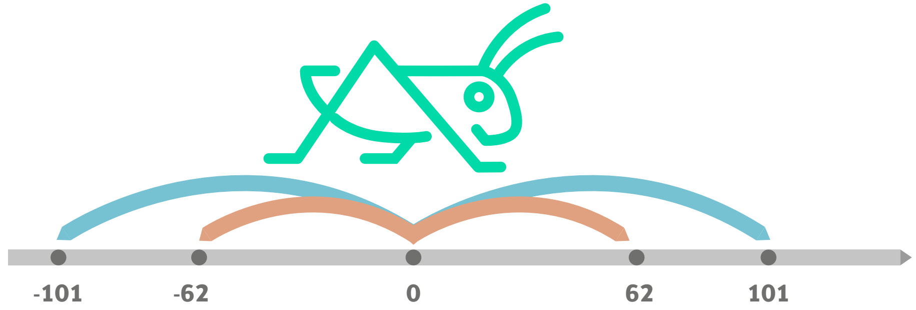


Если $n = p$ — простой модуль, то в таблице умножения по модулю p нет нулей.

Докажем сначала для $p = 101$, а затем обобщим.
Пусть на числовой прямой есть кузнечик, который совершает по ней прыжки длины 101 или 62, стартуя из нуля.

Примечание * здесь и далее под таблицей умножения понимаем ее ненулевую часть (за вычетом нулевой строки и нулевого столбца)

МОЖЕТ ЛИ КУЗНЕЧИК ПОПАСТЬ В ТОЧКУ 1?



Произвольная последовательность его прыжков задается формулой $101n + 62l$, где n и l — любые целые числа.

Если кузнечик может оказаться в точке X, то он может попасть в любую точку, кратную X, кратно повторив ту же последовательность прыжков.

Докажем, что кузнечик может попасть в точку 1:

$$0 \xrightarrow{+101} 101 \xrightarrow{-62} 39 \xrightarrow{\times 2} 78 \xrightarrow{-101} -23 \xrightarrow{+39}$$

$$16 \xrightarrow{\times 6} 96 \xrightarrow{-101} -5 \xrightarrow{\times 20} -100 \xrightarrow{+101} 1$$

Значит, существуют такие целые n и l, что $101n + 62l = 1$.

Проект реализуется при поддержке Фонда президентских грантов

2 ЕСЛИ В СТРОКЕ ЕСТЬ 1, ТО НЕТ 0

Сначала убедимся, что в таблице умножения остатков по модулю 101 в строке 62 есть 1.

Если l — остаток, то
$101n + 62l = 1 \Rightarrow$
$62l = 1 \bmod 101 \Rightarrow$
в строке 62 на пересечении со столбцом l стоит 1.

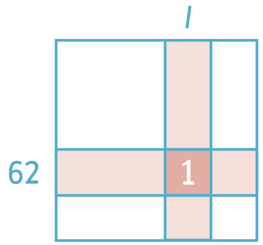


Таблица умножения по модулю 101

Если $l > 101$ или $l < 0$, то разделим l на $101 : l = 101k + m$, где m — остаток.

Тогда $101n + 62 \cdot 101k + 62m = 1 \Rightarrow 62m = 1 \bmod 101 \Rightarrow$ в строке 62 на пересечении со столбцом m стоит 1.

Докажем, что если в строке есть 1, то нет 0 **методом от противного**:

- предположим **обратное** нашему утверждению;
- проведем логическую цепочку, ведущую к **противоречию**.

Если бы в строке 62 стоял 0, то для некоторого остатка r было бы выполнено $62m \cdot r = 0 \bmod 101$.

Тогда $62m \cdot r = 0 \bmod 101$.

Но $62m \cdot r = 1 \bmod 101$, значит, $r = 0 \bmod 101$.

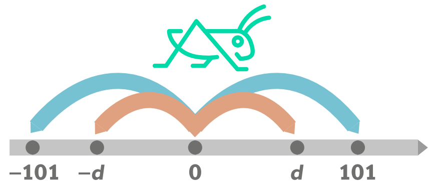
Но r не может делиться на 101, т.к. r — остаток $\Rightarrow$ **противоречие.**

ЧТО И ТРЕБОВАЛОСЬ ДОКАЗАТЬ.

ПРОИЗВОЛЬНАЯ СТРОКА

Пусть теперь d — произвольная строка в таблице умножения остатков по модулю 101.

По доказанному ранее, если мы убедимся, что в строке d есть 1, то в ней не будет 0.



Пусть на числовой прямой есть кузнечик, который совершает по ней прыжки длины 101 или d, стартуя из нуля.

Докажем, что этот кузнечик тоже может попасть в точку 1, а значит, во все целые числа.

Доказательство снова проведем методом от противного.

Пусть кузнечик не может попасть в точку 1, и точка k $(k > 1)$ — ближайшая к нулю, куда он может попасть.

Тогда следующая точка, куда может попасть кузнечик, это $2k$, потому что k по определению есть длина минимального интервала между позициями кузнечика, которой можно добиться при любых комбинациях прыжков длины 101 или d.

Таким образом, кузнечик попадает только в точки, кратные k.

Значит, и точка 101 — одна из таких точек, и для некоторого числа ρ $101 = k \cdot \rho$.
Но 101 — простое число $\Rightarrow$ противоречие.

Значит, $k = 1$, и кузнечик может попасть в точку 1.

Проект реализуется при поддержке Фонда президентских грантов

3 ПРОИЗВОЛЬНЫЙ ПРОСТОЙ МОДУЛЬ

Таким образом, мы доказали, что в таблице умножения по модулю 101 в каждой строке есть 1, а следовательно, нет нулей.

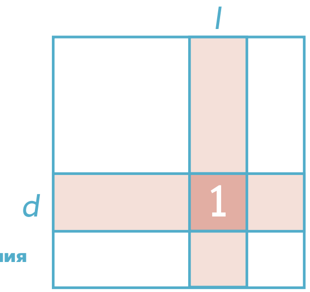
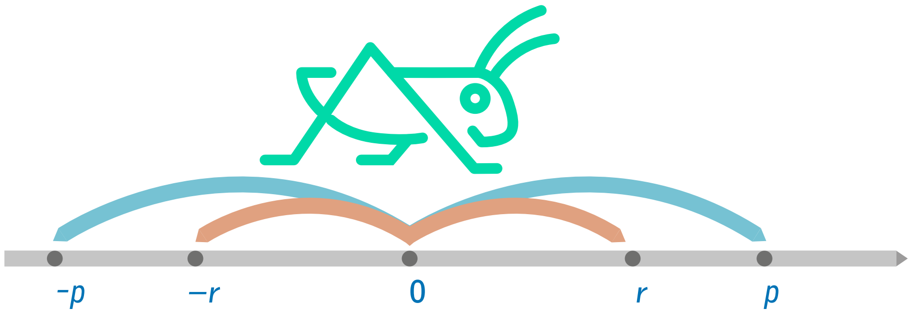


Таблица умножения по модулю 101

Осталось сделать последнее обобщение:

Пусть p — произвольный простой модуль. Тогда таблица умножения по модулю p не содержит нулей.

Пусть на числовой прямой есть кузнечик, который совершает по ней прыжки длины p или $r (r < p)$, стартуя из нуля.



Докажем, что этот кузнечик тоже может попасть в точку 1, а значит, во все целые числа.

Снова предположим, что k — ближайшая точка, в которую может попасть кузнечик из точки 0, и $k > 1$.

Повторим те же шаги доказательства от противного, что и для $p = 101$. Они приведут нас к противоречию с тем, что p — простое число.

Значит, $k = 1$, и кузнечик может попасть в точку 1.

Следовательно, существует такой остаток l, что на пересечении строки r и столбца l в таблице умножения по простому модулю p стоит 1, а значит, в строке r нет нулей.

Проект реализуется при поддержке Фонда президентских грантов