ТАБЛИЦА УМНОЖЕНИЯ ПО ПРОИЗВОЛЬНОМУ МОДУЛЮ

На прошлом уроке мы доказали, что таблица умножения по простому модулю не содержит нулей. Рассмотрим теперь таблицу умножения по произвольному модулю m, а в ней — любую строку a.

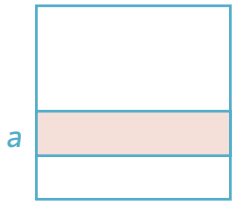


Таблица умножения по произвольному модулю m

Следующие три утверждения эквивалентны:

1. В строке a нет нулей;
2. В строке a есть 1;
3. В строке a все остатки разные.

ДОКАЗАТЕЛЬСТВО

3 ⇒ 2) очевидно: т.к. в $m - 1$ ячеек помещены различные числа от 1 до $m - 1$, по **принципу Дирихле** среди них обязательно будет 1.

2 ⇒ 1) Пусть в строке a на пересечении со столбцом x стоит 1. Тогда для некоторого целого $k \cdot a \cdot x = 1 + m \cdot k$. Предположим, что в строке a есть 0 на пересечении со столбцом y. Это означает, что $a \cdot y$ делится на m. Тогда $x \cdot a \cdot y$ должно делиться на m.

$$x \cdot a \cdot y = (1 + m \cdot k) \cdot y = y + m \cdot k \cdot m \Rightarrow \text{ не делится на } m.$$

не может делиться на m, т.к. $y < m$ | делится на m

Значит, в строке a нет нулей. Доказано.

1 ⇒ 3) От противного. Пусть в строке a есть два одинаковых остатка l на пересечении со столбцами x и y.

НАИБОЛЬШИЙ ОБЩИЙ ДЕЛИТЕЛЬ

Тогда $a \cdot x = a \cdot y$ по модулю m.
$\Rightarrow$ $a \cdot y - a \cdot x = a \cdot (y - x)$ делится на m. Тогда в строке a на пересечении со столбцом $y - x$ должен стоять 0. Противоречие. Доказано.

3 ⇒ 1) очевидно: если в $m - 1$ ячейках стоят все числа от 1 до $m - 1$, то нулей там нет.

Итак, мы доказали, что утверждения 1) – 3) эквивалентны между собой (каждое следует из каждого). Докажем теперь, что они эквивалентны следующему утверждению:

4) НОД$(a, m) = 1$.

ДОКАЗАТЕЛЬСТВО

ОПРЕДЕЛЕНИЕ

Наибольший общий делитель чисел a и m(d = НОД(a, m)) — это такое число, что:
1. a делится на d, и m делится на d;
2. $d \geqslant l$ для любого l — общего делителя a и m.

Достаточно доказать, что из любого из утверждений 1) – 3) следует утверждение 4), а из утверждения 4) следует любое из утверждений 1) – 3), так как утверждения 1) – 3) эквивалентны между собой.

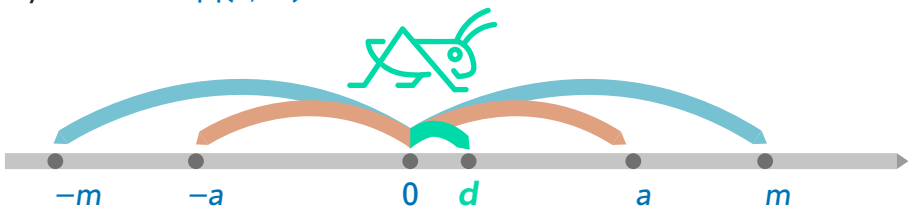
1 ⇒ 4) Докажем, что если $d > 1$, то в строке a есть нули. Существует остаток, равный $m : d$, и на пересечении строки a со столбцом с таким номером стоит $a \cdot m : d = (a : d) \cdot m$, а это равно 0 по модулю m.

4 ⇒ 2) Докажем, что если $d = 1$, то в строке a есть 1.

Проект реализуется при поддержке Фонда президентских грантов

НОД(a, m) = 1 ⇒ ⇒ ТРИ УТВЕРЖДЕНИЯ ВЕРНЫ

Пусть d = НОД(a, m).



ТЕОРЕМА

Кузнечик вида [a, m] (который может совершать по числовой прямой прыжки длины a и m) попадает во все точки, кратные d, и только в них.

ДОКАЗАТЕЛЬСТВО

Пусть $\tilde{d}$ — ближайшая к 0 точка, в которую может попасть кузнечик. Мы доказывали ранее, что тогда он может попасть во все точки, кратные $\tilde{d}$.
Т.к. кузнечик попадает в точки a и m, то числа a и m должны быть кратны $\tilde{d}$, т.е. $\tilde{d}$ — их общий делитель.
Докажем, что он и есть наибольший.

Пусть l и k — такие числа, что следующая комбинация приводит кузнечика в точку $\tilde{d}$:

$$\tilde{d} = l \cdot a + k \cdot m$$

Если c — любой другой общий делитель a и m, то $\tilde{d}$ делится на c, т.к. является суммой кратных с чисел.

Таким образом, $\tilde{d}$ = НОД(a, m) и совпадает с d.

ТЕОРЕМА ДОКАЗАНА

Таким образом, если НОД(a, m) = 1, то по теореме кузнечик может попадать в точку 1, а значит, в строке a есть 1.

Итак, мы доказали, что все четыре утверждения для строки a таблицы по произвольному модулю m эквивалентны между собой:

1. В строке a нет нулей;
2. В строке a есть 1;
3. В строке a все остатки разные;
4. НОД(a, m) = 1

Проект реализуется при поддержке Фонда президентских грантов

3 ВАЖНОЕ УТВЕРЖДЕНИЕ

Утверждение, на котором строится основная теорема арифметики:

Пусть p — простое число. Тогда:
$a, b \not\vdots p \Rightarrow a \cdot b \not\vdots p$.

ДОКАЗАТЕЛЬСТВО

Разделим a и b с остатком на p:

$$a = p \cdot \alpha + \tilde{a}$$
$$b = p \cdot \beta + \tilde{b}$$

где $\tilde{a}, \tilde{b}$ — некоторые ненулевые остатки.

Мы знаем, что $\tilde{a} \cdot \tilde{b} \not\vdots p$ т.к. в таблице по модулю p нет нулей.

$$a \cdot b = (p \cdot \alpha + \tilde{a})(p \cdot \beta + \tilde{b}) = p^2\alpha\beta + p\alpha\tilde{b} + p\beta\tilde{a} + \tilde{a} \cdot \tilde{b}$$

В этом выражении три первые слагаемые делятся на p, а последнее — не делится, следовательно, сумма не делится на p.

ЧТО И ТРЕБОВАЛОСЬ ДОКАЗАТЬ.

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ

Пусть n — целое число, $n \geqslant 2$.Тогда существует представление числа n в виде произведения простых сомножителей. Это разложение единственно с точностью до порядка сомножителей.

ДОКАЗАТЕЛЬСТВО

Пусть для числа n есть два совершенно различных разложения на простые множители:

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k = q_1 \cdot q_2 \cdot \ldots \cdot q_l$$

Возьмем простое число p_1 из первого разложения.
Ни одно из $q_1, q_2, \ldots, q_l$ не делится на p_1, т.к. они тоже простые.
По доказанному только что утверждению их произведение тоже не делится на p_1. Это значит, что число n не делится на p_1. Противоречие. Следовательно, представление числа n в виде произведения простых множителей единственно (с точностью до их порядка).

ОСНОВНАЯ ТЕОРЕМА АРИФМЕТИКИ ДОКАЗАНА.

Проект реализуется при поддержке Фонда президентских грантов