Математические основы информатики

Теория чисел.

Сергей Леонидович Бабичев

Группы, кольца и поля.

Definition (Группа)

Множество G с операцией $\circ$ называтся *группой*, если:

1. $a \circ (b \circ c) = (a \circ b) \circ c) \forall a, b \in G$;
2. $\exists E : a \circ E = E \circ a = a \forall a \in G$;
3. $\forall a \in G \; \exists a^{-1} : a \circ a^{-1} = a^{-1} \circ a = E$.

- Если $\circ$ коммутативна, то группа *коммутативная* или *Абелева*.
- Множества $\mathbb{Z}, \mathbb{N}, \mathbb{R}$ — группы, относительно операции сложения.
- Множества $\mathbb{Q} \setminus \{0\}, \mathbb{R} \setminus \{0\}$ — группы относительно операции умножения.
- Элемент E — *нейтральный*.
- Элемент a^{-1} — *обратный* для операций типа умножения и *противоположный* для операций типа сложения.

Definition (Кольцо)

Множество K с двумя заданными на нём операциями $\circ$ и $\cdot$ есть *кольцо*, если:

1. Множество K — коммутативная группа по операции $\circ$.
2. Операция $\cdot$ ассоциативна в K:

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c) \quad \forall a, b, c \in K$$

3. Операции $\circ$ и $\cdot$ связаны дистрибутивностью слева:

$$(a \circ b) \cdot c = (a \cdot c) \circ (b \cdot c), \ \forall a, b, c \in K$$

и/или справа:

$$c \cdot (a \circ b) = (c \cdot a) \circ (c \cdot b), \ \forall a, b, c \in K$$

- Кольцо *коммутативно* по $\cdot$, если $a \cdot b = b \cdot a$.
- Если $\exists e \in K : a \cdot e = e \cdot a = a$, то K — *кольцо с единицей*.
- Множества $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ — коммутативные кольца с единицей по операциям сложения и умножения.

Варианты дистрибутивности

- **Пример.** Множество $\mathbb{R}^+$ с операциями $\circ$ умножения и $\cdot$ возведения в степень дистрибутивно справа относительно умножения и не дистрибутивно слева.
- $(a \times b)^c = a^c \times b^c$.
- $a^{b \cdot c} \neq a^c \times b^c$.

Definition (Поле)

Множество Π с операциями $\circ$ и $\cdot$ есть *поле*, если оно:

1. коммутативное кольцо с единицей и $E \neq e$;
2. $\forall a \in \Pi, a \neq E,\ \exists a^{-1} \in \Pi : a \cdot a^{-1} = e$.

Поля в арифметике

Задача. Определим на множестве $\mathbb{Z}_3 = \{0, 1, 2\}$ операции:

1. $a \circ b = (a + b) \pmod 3$;
2. $a \cdot b = (ab) \pmod 3$.

Доказать, что множество $\mathbb{Z}_3$ есть поле относительно данных операций.

Поля в арифметике

Задача. Определим на множестве $\mathbb{Z}_3 = \{0, 1, 2\}$ операции:

1. $a \circ b = (a + b) \pmod 3$;
2. $a \cdot b = (ab) \pmod 3$.

Доказать, что множество $\mathbb{Z}_3$ есть поле относительно данных операций.

- Вспомним свойства операции mod.

$$\begin{array}{llll} (a+b) & (\mathrm{mod}\ m) = (a & (\mathrm{mod}\ m) + b & (\mathrm{mod}\ m)) \quad (\mathrm{mod}\ m) \\ (a-b) & (\mathrm{mod}\ m) = (a & (\mathrm{mod}\ m) - b & (\mathrm{mod}\ m)) \quad (\mathrm{mod}\ m) \\ (a \times b) & (\mathrm{mod}\ m) = (a & (\mathrm{mod}\ m) \times b & (\mathrm{mod}\ m)) \quad (\mathrm{mod}\ m) \end{array} \tag{1}$$

- Обозначим за $a \overset{3}{+} b$ операцию $\circ = (a + b) \pmod 3$.
- Обозначим за $a \overset{3}{\times} b$ операцию $\cdot = (a * b) \pmod 3$.

Задача 1. План доказательства

Нужно доказать следующие факты:

1. Множество значений результатов операций принадлежат $\mathbb{Z}_3$.
2. Операция $\overset{3}{+}$ коммутативна на множестве $\mathbb{Z}_3$.
3. Существует единичный элемент E по операции $\overset{3}{+}$.
4. Для каждого $a \in \mathbb{Z}_3$ существует обратный элемент по операции $\overset{3}{+}$.
5. Операция $\overset{3}{+}$ ассоциативна на множестве $\mathbb{Z}_3$.
6. Операция $\overset{3}{\times}$ ассоциативна на множестве $\mathbb{Z}_3$.
7. Операции $\overset{3}{+}$ и $\overset{3}{\times}$ дистрибутивны и слева и справа.
8. Существует единица e по операции $\overset{3}{\times}$ и она не равна E.
9. Для всех $a \in \mathbb{Z}_3 \setminus E$ существует обратный элемент по операции $\overset{3}{\times}$.

Задача 1. Решение.

1. Строим таблицу операции $\overset{3}{+}$.

a \b	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

   - Множество значений результатов операций принадлежат $\mathbb{Z}_3$.

2. Операция $\overset{3}{+}$ коммутативна на множестве $\mathbb{Z}_3$.
3. Элемент $0 \in \mathbb{Z}_3$ обладает свойством единицы по операции $\overset{3}{+}$ на множестве $\mathbb{Z}_3$.
4. Элемент 0 имеет обратный (противоположный) элемент 0, элемент 1 — обратный элемент 2, элемент 2 — обратный элемент 1 по операции $\overset{3}{+}$.

Задача 1. Решение.

5.

$$
\begin{aligned}
& a \overset{3}{+} (b \overset{3}{+} c) = \\
= \quad & (a + ((b + c) \pmod 3)) \pmod 3 = \\
= \quad & (a + b + c) \pmod 3 = \\
= \quad & ((a + b) \pmod 3 + c) \pmod 3 = \\
= \quad & (a \overset{3}{+} b) \overset{3}{+} c
\end{aligned}
$$

6.,7. Аналогично для операции $\overset{3}{\times}$ и для их комбинации.

8. Элемент $1 \in \mathbb{Z}_3$ обладает свойством единицы по операции $\overset{3}{\times}$.
9. Элемент 1 имеет обратный элемент 1, элемент 2 — обратный элемент 2 по операции $\overset{3}{\times}$.

Идеалы

Definition (Идеал)

Непустое подмножество I в множестве A, произвольном коммутативном кольце, есть *идеал*, если:

1. $a_1, a_2 \in I \implies a_1 - a_2 \in I$.
2. $a \in I \implies ab \in I \; \forall b \in A$.

- Пусть имеется произвольное конечное множество $a_1, a_2, \ldots, a_s$, $a_i \in A$.
- Тогда оно определяет идеал I, который состоит из всех элементов, представимых в виде линейных комбинаций $\Sigma \lambda_i a_i$, где $\lambda_i \in A$.
- Этот идеал порождён $\{a_i\}_{i=1}^{s}$ и записывается как $I = (a_1, a_2, \ldots, a_s)$.
- *Главный идеал* — идеал порождённый одним элементом $I = (a)$.
- Любой идеал в кольце $\mathbb{Z}$ — главный.

Делимость. Простые числа.

Делимость

Definition (Делимость)

Для целых чисел a и b определяется $a \vdots b$, если $\exists c \in \mathbb{N} : a = b \cdot c$

Definition (НОД)

Наибольший общий делитель чисел $a, b \in \mathbb{N}$ есть наибольшее из всех таких чисел $c \in \mathbb{N}$, которое $a \vdots c, b \vdots c$ и обозначается $\gcd(a, b)$.

Definition (НОК)

Наименьшее общее кратное чисел $a, b \in \mathbb{N}$ есть наименьшее из всех таких чисел $c \in \mathbb{N}$, которое $c \vdots a, c \vdots b$ и обозначается $\mathrm{lcm}(a, b)$.

Алгоритм Евклида

- Операция $\gcd$ коммутативна.
- Определение Евклида:

$$\gcd(a,b) = \begin{cases} a, \text{ если } b = 0 \\ b, \text{ если } a = 0 \\ \gcd(b, a-b), \text{ если } a > b \\ \gcd(b-a, a) \text{ иначе} \end{cases}$$

Definition (Простое число)

Число $a \in \mathbb{N}, a > 1$ есть *простое* если $\nexists b \in N : (1 < b < a) \wedge (a \vdots b)$.

Theorem (Количество простых чисел)

Множество простых чисел счётно и бесконечно.

Доказательство.

Рассмотрим число $p_1 p_2 \dots p_l + 1$, где p_l — последнее простое число. □

Theorem (Теорема Дирихле)

Множество, образованное числами $b \in \mathbb{N}_0$ и числами вида $ak + b, a \in \mathbb{N}, b \in \mathbb{Z}$ содержит бесконечное множество простых чисел, если $\gcd(a, b) = 1$.

Theorem (Основная теорема арифметики)

Каждое число $n \in \mathbb{N}, n > 1$ может быть однозначно записано как

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

где $p_i \in \mathbb{P}, p_i \neq p_j$ при $i \neq j$. Такое обозначение при $p_1 < p_2 < \cdots < p_s$ называется каноническим.

Corollary (Делимость чисел)

Число

$$a = p_1^{\alpha_1} \times p_2^{\alpha 2} \times \cdots \times p_n^{\alpha_n}$$

делится на

$$b = q_1^{\beta_1} \times q_2^{\beta_2} \times \cdots \times q_m^{\beta_m}$$

в том и только в том случае, если $Q \subset P$ и каждый из коэффициентов при соответствующих показателях степеней при q меньше или равен соответствующему показателю при p.

Следствия ОТА

- Пусть $N = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_n^{\alpha_n}, \alpha_i \geqslant 0$ и $M = p_1^{\beta_1} \times p_2^{\beta_2} \times \cdots \times p_n^{\beta_n} \beta_i \geqslant 0$.

$$\gcd(M, N) = p_1^{\min(\alpha_1, \beta_1)} \times p_2^{\min(\alpha_2, \beta_2)} \times \cdots \times p_n^{\min(\alpha_n, \beta_n)}.$$

$$\operatorname{lcm}(M, N) = p_1^{\max(\alpha_1, \beta_1)} \times p_2^{\max(\alpha_2, \beta_2)} \times \cdots \times p_n^{\max(\alpha_n, \beta_n)}.$$

- Отсюда, в частности, следует формула:

$$\gcd(M, N) \times \operatorname{lcm}(M, N) = M \times N$$

.

Задача. Определить количество натуральных делителей числа x.

Задача. Определить количество натуральных делителей числа x.
Решение:

- Выпишем каноническое представление x.

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

  В каждый делитель числа в разложении может входить делитель p_i с кратностью от 0 до α_i.
- Следовательно, общее количество делителей будет

$$\prod_{i=1}^{n} \alpha_i + 1$$

Задача. Определить S — сумму всех делителей числа x.

Задача. Определить S — сумму всех делителей числа x.
Решение:

- Выпишем каноническое представление x.

$$x = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

  В каждый делитель числа в разложении может входить делитель p_i с кратностью от 0 до α_i.
- Рассмотрим простой делитель p_1. Дизъюнктивно разобьём множество всех делителей на $\alpha_1 + 1$ классов, в которых этот делитель входит в различных степенях.
- Обозначим за S_1 сумму всех делителей числа x, в которых простой делитель p_1 не входит.
- Тогда $S = p_1^0 S_1 + p_1^1 S_1 + p_1^2 S_1 + \dots + p_1^{\alpha_1} S_1 = \dfrac{p_1^{n+1} - 1}{p_1 - 1} S_1.$
- По индукции: $S = \prod_{i=1}^{n} \dfrac{p_i^{\alpha_i+1} - 1}{p_i - 1}$

Позиционные системы счисления

Theorem (Запись числа в позиционной системе счисления)

В позиционной системе счисления с основанием N число $x \in N$ записывается следующим образом:

$$x = \overline{\dots a_3 a_2 a_1 a_0} = \dots + a_3 N^3 + a_2 N^2 + a_1 N^1 + a_0 N^0$$

при этом $0 \leqslant a_i \leqslant N$.

Сравнения

Definition (Сравнимость чисел по модулю)

Числа $a, b \in \mathbb{Z}$ сравнимы по модулю $m \in \mathbb{N}$ если $(a - b) \vdots m$.
Это записывается как

$$a \equiv b \pmod{m}$$

Свойства сравнимости

- Для любых a, b условие $a \equiv b \pmod{m}$ — бинарное отношение.
- Отношение сравнимости рефлексивно, симметрично, транзитивно.
- Оно является отношением эквивалентности.
- Множество $\mathbb{Z}$ разбивается на дизъюнктивные множества классов эквивалентности чисел по модулю m.
- Каждый класс сравнимых по модулю m чисел — *класс вычетов по модулю* m — обозначается $\overline{a}_m$.
- Представитель класса — наименьший неотрицательный элемент класса — остаток от деления любого элемента класса на m.
- Класс элемента a — множество $a + m\mathbb{Z}$.
- Множество всех классов вычетов — $\mathbb{Z}_m$.
- Относительно операции сложения и умножения $\mathbb{Z}_m$ есть конечное кольцо, а для $m \in \mathbb{P}$ — конечное поле.

Свойства сравнимости:

- $a \equiv a \pmod{m}$.
- Если $a \equiv b \pmod{x}$ и $b \equiv c \pmod{x}$, то $a \equiv c \pmod{x}$
- Если $a \equiv b \pmod{x}$ и $c \equiv d \pmod{x}$ то $a + c \equiv b + d \pmod{x}$;
- Если $a \equiv b \pmod{x}$ и $c \equiv d \pmod{x}$ то $a \cdot c \equiv b \cdot d \pmod{x}$;
- Если $a \equiv b \pmod{x}$ то $a^n \equiv b^n \pmod{x}, n \in N$.

Системы вычетов

Definition (Полная система вычетов)

Полная система вычетов по модулю m — множество таких $m_i \in \mathbb{Z}$, что $m_i \not\equiv m_j$ при $i \neq j$.

- Множество $\mathbb{Z}_m$ образует полную систему вычетов по модулю m.

Теоремы Ферма и Эйлера.

Ферма

Пьер Ферма (1601-1665) — французский юрист и, заодно, великий математик, не написавший ни одной книги.
Наблюдение Ферма над степенями (1640):

- 3, 9, 27, 81, 243, 729, 2187, ...
- если простое число 13 делит число $26 = 3^3 - 1$, то оно делит и числа $726 = 3^6 - 1$, $19682 = 3^9 - 1$, ...

Сам Ферма ничего не доказал, это было доказано в 1736 году Леонардом Эйлером.

Теорема Ферма

Если p — простое число, a — целое число, то $a^p - a$ кратно p.

$$\boxed{\forall p \in \mathbb{P}, \forall a \in \mathbb{Z} : a^p - a \vdots p}$$

Теорема Ферма: как доказать?

Можно легко доказать для каких-то p:

- $p = 2$:
$$a^2 - a = a(a-1) \vdots 2$$
- $p = 3$:
$$a^3 - a = a(a^2-1) = a(a-1)(a+1) \vdots 3$$
- $p = 5$:
$$a^5 - a = a(a^4-1) = a(a-1)(a+1)(a^2+1)$$

  Как доказать, что это произведение делится на 5?

Теорема Ферма: продолжение

Посмотрим на остатки от деления на 11 чисел вида $5k$, где $k \in [1..10]$.

- $k = 1 \to 5k \pmod{11} = 5$
- $k = 2 \to 5k \pmod{11} = 10$
- $k = 3 \to 5k \pmod{11} = 4$
- $k = 4 \to 5k \pmod{11} = 9$
- $k = 5 \to 5k \pmod{11} = 3$
- $k = 6 \to 5k \pmod{11} = 8$
- $k = 7 \to 5k \pmod{11} = 2$
- $k = 8 \to 5k \pmod{11} = 7$
- $k = 9 \to 5k \pmod{11} = 1$
- $k = 10 \to 5k \pmod{11} = 6$

Теорема Ферма: продолжение

Наблюдения:

- среди остатков не может быть нуля.
  Для $p \in \mathbb{P}$ и $a, k \not\vdots p \to a \cdot k \not\vdots p$.
- все остатки разные.
  Если бы существовали такие a и b, которые давали бы одинаковые остатки при делении на p, то
  $a \cdot k - b \cdot k = (a - b) \cdot k \vdots p$.
  Но $a - b$ на p не делится.

Вывод:
Для простого p существует ровно $p - 1$ остаток, который появится в правой части и каждый остаток появится ровно один раз.

Если все значения x принадлежат полной системе вычетов по модулю p, то для любого $a : a \not\vdots p$ множество ax тоже принимает значения полной системы вычетов.

Теорема Ферма: другая формулировка

Для числа $k \in \mathbb{Z}$ и числа $p \in \mathbb{P}$ таких, что $k \not\vdots p$ верно
$k^{p-1} \pmod{p} \equiv 1$

Доказательство: так как остатки от деления на p чисел $k, 2 \cdot k, \ldots, (p-1) \cdot k$ есть перестановка чисел $1, 2, \cdot, p-1$, то

$$k \cdot 2k \cdot \ldots \cdot (p-1)k \equiv 1 \cdot 2 \cdot \ldots \cdot (p-1) \pmod{p},$$

из чего следует

$$k^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

$(p-1)!$ и p взаимно просты $\rightarrow$ можно сократить обе части на $(p-1)!$, получив искомое.

Теорема Ферма: а что, если число p — не простое?

- Среди остатков появятся нули.
- Наше доказательство не пройдёт.
- Попробуем выяснить, что будет, если p — не простое.

Таблицы умножения по модулю

Давайте составим таблицу умножения всех чисел от 1 до $p-1$ по модулю p.

- p — простое число. Пусть $p = 7$..

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

Мы уже доказали, что в каждой строке встретятся все числа от 1 до $p-1$.
Какие ещё свойства?

Таблицы умножения по модулю

- p — составное число. Пусть $p = 6$.

$\times$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

- Есть строки и столбцы, содержащие нули. Вычеркнем их.

$\times$	1	5
1	1	5
5	5	1

Таблицы умножения по модулю

- p — составное число. Пусть $p = 8$.

$\times$	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	4	6	0	2	4	6
3	3	6	1	4	7	2	5
4	4	0	4	0	4	0	4
5	5	2	7	4	1	6	3
6	6	4	2	0	6	0	2
7	7	6	5	4	3	2	1

- Вычеркнем строки и столбцы, содержащие нули.

$\times$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Таблицы умножения по модулю

- Для чего мы сокращаем таблицы?

Таблицы умножения по модулю

- Для чего мы сокращаем таблицы?
- Чтобы обобщить теорему Ферма не только на простые числа.
- Что содержится в сокращённых таблицах при составных n?

Таблицы умножения по модулю

- Для чего мы сокращаем таблицы?
- Чтобы обобщить теорему Ферма не только на простые числа.
- Что содержится в сокращённых таблицах при составных n?
- Каждая строка или столбец содержит все взаимно простые с n числа.
- Строки различаются только порядком.
- Перемножим числа в строке k.

$$ka_1ka_2 \dots ka_r \equiv a_1a_2 \dots a_r \pmod{p}$$

$$(k^r - 1)a_1a_2 \dots a_r \equiv 0 \pmod{p}$$

- Так как $(k^r - 1)a_1a_2 \dots a_r$ делится на p, а все a_i взаимно просты с p, то

$$\boxed{k^r - 1 \equiv 0 \pmod{p}}$$

Теорема Эйлера

$$k^r - 1 \equiv 0 \pmod{p}$$

- Что такое r в этой формуле?
- r — число чисел, меньших p и взаимно простых с p.
- Это — теорема Эйлера.

Функция Эйлера

Леонард Эйлер (1707-1783) — один из величайших учёных мира в истории, физик, математик, астроном, ...

- Функция Эйлера $\varphi(p)$ есть число чисел, меньших p и взаимно простых с p.
- Тогда теорему Эйлера записывают так:

> Для взаимно простых целого числа k и натурального числа p верно, что
>
> $$k^{\varphi(p)} - 1 \equiv 0 \pmod{p}$$

- Здесь p — не обязательно простое число.

Функция Эйлера

Исследуем эту замечательную функцию.

- Для p — простого числа, функция $\varphi(p) = p - 1$.
- Рассмотрим p^m, где p — простое число.
- Все числа $p, 2p, 3p, \ldots, p^m - p$ имеют с p^m общие делители. Таких чисел $p^{m-1} - 1$.
- По основной теореме арифметики (ОТА), других делителей у p^m нет.
- По ОТА все остальные числа от 1 до $p^m - 1$ — взаимно простые с p^m.
- Итого: $\varphi(p^m) = p^m - 1 - (p^{m-1} - 1) = p^m \left(1 - \frac{1}{p}\right)$.

Функция Эйлера

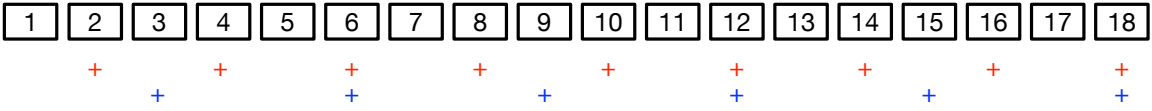
Чему равна $\varphi(18)$?

- Это — число чисел от 1 до 18, не делящихся ни на 2 ни на 3.
- На 2 делится 9 чисел.
- На 3 делится 6 чисел.
- Правда ли, что $\varphi(18) = 18 - 9 - 6 - 1$?

Функция Эйлера

Чему равна $\varphi(18)$?

- Это — число чисел от 1 до 18, не делящихся ни на 2 ни на 3.
- На 2 делится 9 чисел.
- На 3 делится 6 чисел.
- Правда ли, что $\varphi(18) = 18 - 9 - 6 - 1$?
- Нет, мы вычеркнули числа 6 и 12 дважды.
- Их надо вернуть.
- $\varphi(18) = 18 - 9 - 6 - 1 + 2 = 6$
- Это — формула включений/исключений.



Функция Эйлера

- Есть ли другой?
- Да. Используя следующую теорему:

> Функция Эйлера обладает свойством мультипликативности: для взаимно простых m и n верно:
>
> $$\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$$

Следствие из теоремы:
Если число $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, то

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \varphi(p_2^{\alpha_2}) \dots \varphi(p_k^{\alpha_k})$$

или

$$\varphi(n) = (p_1^{\alpha_1} - p_1^{\alpha_1 - 1})(p_2^{\alpha_2} - p_2^{\alpha_2 - 1}) \dots (p_k^{\alpha_k} - p_k^{\alpha_k - 1})$$

Доказательство теоремы о мультипликативности функции Эйлера

Рассмотрим все числа вида $mx + ny$, где $x \in [0, n), y \in [0, m)$ и запишем их в таблицу $n \times m$. Числа n и m взаимно просты!
Пример: $n = 5, m = 3$.

$x \backslash y$	0	1	2
0	0	5	10
1	3	8	13
2	6	11	16
3	9	14	19
4	12	17	22

Доказываем теорему

Остатки от деления на $m \times n$.

$x \backslash y$	0	1	2
0	0	5	10
1	3	8	13
2	6	11	1
3	9	14	4
4	12	2	7

Утверждение: все остатки от деления на $m \times n$ в этой таблице различны.

Доказываем утверждение: все остатки от деления на $m \times n$ в этой таблице различны.

Доказательство от противного. Пусть $\exists x_1, x_2 \in [0, n), y_1, y_2 \in [0, m)$:

$$mx_1 + ny_1 \equiv mx_2 + ny_2 \pmod{mn}.$$

Из этого следует:

$$\begin{aligned} mx_1 + ny_1 &\equiv mx_2 + ny_2 \pmod{m} \\ mx_1 + ny_1 &\equiv mx_2 + ny_2 \pmod{n} \end{aligned}$$

Далее:

$$\begin{aligned} ny_1 &\equiv ny_2 \pmod{m} \\ mx_1 &\equiv mx_2 \pmod{n} \end{aligned}$$

$gcd(m, n) = 1 \implies x_1 \equiv x_2 \pmod{n}, y_1 \equiv y_2 \pmod{m}.$

Доказываем теорему

- Все остатки в таблице — различные.
- Всего остатков в таблице — mn.
- Следовательно, для каждого остатка r существует единственная пара x, y

$$x \in [0, n), y \in [0, m),$$

что

$$r = mx + ny \pmod{mn}.$$

- Числа, взаимно простые с m находятся в $\varphi(m)$ столбцах.
- Числа, взаимно простые с n находятся в $\varphi(n)$ строках.
- Числа, взаимно простые с n и m находятся на пересечении указанных строк и столбцов и их $\varphi(m) \cdot \varphi(n)$, а это то, что мы ищем: $\varphi(mn)$.