Содержание

1 Операции над высказываниями. Логические законы.

Высказывание —это утверждение. Оно может быть истинным или ложным. Над высказываниями определены следующие операции:

Отрицание: Если A — высказывание, то $\neg A$ — отрицание A ("не"A; $\bar{A}$). $\neg A$ истино, если A ложно.

Пример 1. $A: \ x = y; \ \neg A: \ x \neq y.$

Конъюнкция: Высказывание, которое истино, если высказывания A и B истины ("и"). $A \wedge B$, $A\&B$, AB.

Пример 2.
$A:$ *данный четырехугольник — ромб;*
$B:$ *данный четырехугольник — прямоугольник;*
$A \wedge B:$ *данный четырехугольник — квадрат.*

Дизъюнкция: Высказывание, которое истино, когда хотя бы одно из A и B истино ("или"в соединительном смысле). $A \vee B$.

Импликация: $A \Rightarrow B$. Если A, то B. A влечет B. $A \Rightarrow B$ ложно, если A — истино, а B — ложно. Принцип ложности посылки: Выражение $A \Rightarrow B$ (где A — посылка, B — заключение) истино, когда A ложно, независимо от B.

Эквиваленция: $A \Leftrightarrow B$. Высказывание, которое истино, если $A \wedge B$ истино или $A \wedge B$ ложно.

Существуют некоторые логические законы:

1. Коммутативность, ассоциативность для "не", "и" и "или".
2. $A \wedge A = A$
3. $A \vee A = A$
4. $A \wedge \neg A \equiv Ложь$
5. $A \vee \neg A \equiv Истина$
6. $\neg\neg A = A$

Математические высказывания можно представить в виде таблиц истинности.

A	B	$A \wedge B$	$A \vee B$	$A \Rightarrow B$	$A \Leftrightarrow B$
Истина	*Истина*	*Истина*	*Истина*	*Истина*	*Истина*
Истина	*Ложь*	*Ложь*	*Истина*	*Ложь*	*Ложь*
Ложь	*Истина*	*Ложь*	*Истина*	*Истина*	*Ложь*
Ложь	*Ложь*	*Ложь*	*Ложь*	*Истина*	*Истина*

Другие логические законы и теоремы (доказываются с помощью таблиц истинности):

1. $(A \vee B)\, C = AC \vee BC$, — дистрибутивность.
2. $(AB) \vee C = (A \vee C)\,(B \vee C)$
3. Законы Деморгана:
   $\neg\,(A \wedge B) = \neg A \vee \neg B$, $\neg\,(A \vee B) = \neg A \wedge \neg B$.
4. $A \Rightarrow B = \neg A \vee B$
5. $A \Rightarrow B = \neg B \Rightarrow \neg A$, — закон контрпозиции.
6. Импликация не обладает коммутативностью и ассоциативностью.
7. Эквиваленция обладает коммутативностью, но не ассоциативностью.

2 Принцип математической индукции

Определение. *Дедукция* — переход от общего к частному.

Определение. *Индукция* — переход от частного к общему.

Пусть $A(n)$ — высказывание, зависящее от $n \in \mathbb{N}$.
Пусть выполнены условия:

1. $A(1) = И_{стина}$
   (базис индукции)
2. $\underbrace{(\forall k \in \mathbb{N}, A(k) = И_{стина})}_{\text{Предположение}} \Rightarrow \underbrace{(A(k+1) = И_{стина})}_{\text{Заключение}}$
   (индукционный переход)

Тогда $A(n) = И_{стина}, \forall n \in \mathbb{N}$.
Суммарно: $\Big((A(1) = И_{стина}) \wedge ((\forall k \in \mathbb{N}, A(k) = И_{стина}) \Rightarrow (A(k+1) = И_{стина}))\Big) \Rightarrow$
$\Rightarrow \Big(A(n) = И_{стина}, \forall n \in \mathbb{N}\Big)$ В различных модификациях ММИ можно брать не $n = 1$, а другое n.
Также есть усиленный принцип индукции, который следует из ММИ. То есть:

1. $A(1) = И_{стина}$
2. $\forall k \in \mathbb{N} \mid A(1), A(2), \ldots, A(k) = И_{стина} \mid\Rightarrow A(k+1) = И_{стина}$
3. $\Rightarrow A(n) = И_{стина}, \forall n \in \mathbb{N}$

Докажем, что ММИ $\Leftrightarrow$ УПИ. При доказательстве того, что УПИ $\Rightarrow$ ММИ дано: $A(1) = И_{стина}$, $A(k) = И_{стина} \Rightarrow A(k+1) = И_{стина}$. Также известно, что УПИ верен. Доказательство очевидно. Докажем, что ММИ $\Rightarrow$ УПИ.

Доказательство. Дано $A(1) = И_{стина}$ и $A(1) \wedge \cdots \wedge A(k) = И_{стина} \Rightarrow A(k+1) = И_{стина}$. Известно, что ММИ верен. Возьмем такое $B(k)$, что:

$$B(k) = \bigcup_{i=1}^{n} A(i)$$

Пусть $B(k)$ — истино. Тогда надо доказать, что $B(k+1) = И_{стина}$. Т. к. $B(k) = И_{стина}$, то $A(1), A(2), \ldots, A(k)$ — истино. Следовательно, $A(k+1) = И_{стина}$. Тогда $(B(k) \Rightarrow B(k+1)) = И_{стина}$. Тогда $A(n) = И_{стина}, \forall n \in \mathbb{N}$. □

3 Неравенство Бернулли

$$(1+x)^n \geq 1 + nx,\ x \geq -1,\ n \in \mathbb{N}$$

ММИ. Рассмотрим выражение для $n = 1$:

$$1 + x \geq 1 + x$$

Пусть для $n = k$ выражение верно. Т. е.:

$$(1+x)^k \geq 1 + kx$$

Рассмотрим выражение для $n = k + 1$:

$$(1+x)^{k+1} \geq 1 + kx + x$$

$$(1+x)\times\underbrace{(1+x)^k}_{\geq 1+kx}\geq 1+kx+x$$

$$(1+x)\times(1+kx)\geq 1+kx+x$$

$$1+kx+x+\underbrace{kx^2}_{\geq 0}\geq 1+kx+x$$

Т. к. импликация верна, то неравенство доказано. □

4 Неравенство Коши

$$\frac{\sum_{i=1}^{n} x_i}{n}\geq \sqrt[n]{\prod_{i=1}^{n} x_i}$$

Замечание. *Если* $\exists\, i \mid x_i = 0 \Rightarrow const \geq 0$. *Далее будем считать, что* $\forall x_i > 0$.

Замечание. *Неравенство однородное. Т. е. если* $\exists\,(x_1, x_2, \ldots, x_n)$, *удволетворяющая неравенству, то* $\exists\,(\lambda x_1, \lambda x_2, \ldots, \lambda x_n)$ — *верно. Тогда можно считать, что* $\prod_{i=1}^{n} x_i = 1$ *(тогда* $\lambda = \sqrt[n]{\frac{1}{\prod_{i=1}^{n} x_i}}$*).*

Следовательно, надо доказать:

$$\left(\prod_{i=1}^{n} x_i = 1\right)\Rightarrow\left(\sum_{i=1}^{n} x_i \geq n\right)$$

Доказательство. Докажем индукцией по n. Для $n = 1$ неравенство верно. Рассмотрим выражение для n членов. Обязательно $\exists x_i \geq 1$ и $\exists x_j \leq 1$ (если надо — перенумеровать). Пусть $x_{n-1} \leq 1$ и $x_n \geq 1$. Предположим, что для $n-1$ элементов неравенство верно. Возьмем такой элемент $a = x_{n-1} \times x_n$. Тогда верны следующие равенства:

$$\underbrace{x_1 \times x_2 \times \cdots \times x_{n-2} \times a}_{n-1 \text{ элементов}} = 1$$

$$x_1 + x_2 + \cdots + x_{n-2} + a \geq n - 1$$

Рассмотрим неравенство для n членов. Надо доказать, что $x_1 + \cdots + x_n \geq n$, если $\prod_{i=1}^{n} x_i = 1$. Прибавим и отнимим a в левой части:

$$\underbrace{x_1 + x_2 + \cdots + x_{n-2} + a}_{\geq n-1} + x_{n-1} + x_n - a \geq n(\text{надо доказать})$$

$$(n-1) + x_{n-1} + x_n + \underbrace{(x_{n-1} \times x_n)}_{a} \geq n$$

$$n + (x_n - 1) - ((x_{n-1} \times x_n) + x_{n-1}) \geq n$$

$$\underbrace{n + \underbrace{(x_n - 1)}_{\geq 0}\underbrace{(1 - x_{n-1})}_{\geq 0}}_{\text{См. замечания}} \geq n$$

□

5 Размещения с и без повторениями. Перестановки.

5.1 Размещения без повторений

Определение. *Размещением* из n элементов по k называется упорядоченный набор из k элементов из n-элементного множесва.

$$A = \{a_1, a_2, \ldots, a_n\} \to (a_1, a_2, \ldots, a_k)$$

Обозначается как $\mathbf{A}_n^k$. Вывод:

1	2	…	i	…	k
n			$n-i+1$		

$$A = \{a_1, a_2, \ldots, a_n\}$$

Соответственно, в первую ячейку можно поместить один из n элементов, во вторую — $n-1$ и т. д. То есть в первую и вторую ячейку можно поставить элементами $n \times (n-1)$ способами. Таким образом,

$$\mathbf{A}_n^k = n \times (n-1) \times (n-2) \times \cdots \times (n-k+1) =$$
$$= \frac{n \times (n-1) \times (n-2) \times \cdots \times (n-k+1) \times (n-k) \times (n-k-1) \times \cdots \times 1}{(n-k) \times (n-k-1) \times \cdots \times 1} =$$
$$= \frac{n!}{(n-k)!}$$

5.2 Размещения с повторениями

Определение. *Размещением с повторениями* из n элементов по k называется упорядоченный набор из k элементов из n-элементного множества с возможностью повторения элементов в наборе.

Обозначается как $\tilde{\mathbf{A}}_n^k$. Вывод:

1	2	…k	
n	n	…	n

$$\tilde{\mathbf{A}}_n^k = n^k$$

5.3 Перестановки

Определение. *Перестановка* из n элементов — это упорядоченный набор элементов из n-элементного множества, в котором все элементы участвуют по одному разу.

Обозначается как $\mathbf{P}_n$.

$$\mathbf{P}_n = \mathbf{A}_n^n = \frac{n!}{(n-n)!} = \frac{n!}{0!} = n!$$

6 Сочетания с и без повторений

6.1 Сочетания без повторений

Определение. *Сочетанием* из n элементов по k называется неупорядоченный набор из k элементов из n-элементного множества.

Обозначается как $\mathbf{C}_n^k$ или $\binom{n}{k}$. Вывод: Выпишем все сочетания без повторений из n по k по одному разу:

$$\{a_{i1}, a_{i2}, \ldots, a_{ik}\}$$
$$\{a_{j1}, a_{j2}, \ldots, a_{jk}\}$$
$$\ldots$$
$$\underbrace{\{a_{s1}, a_{s2}, \ldots, a_{sk}\}}_{k \text{ элементов}}$$

Всего таких сочетаний $\mathbf{C}_n^k$, каждое из них образует $\mathbf{P}_k$ размещений. Таким образом в каждом из $\mathbf{C}_n^k$ сочетаний находится $\mathbf{P}_k$ размещений. Это будут все размещения, каждое по одному разу, без повторений. Таким образом:

$$\mathbf{A}_n^k = \mathbf{C}_n^k \times \mathbf{P}_k$$

$$\mathbf{C}_n^k = \frac{\mathbf{A}_n^k}{\mathbf{P}_k} = \frac{n!}{k!\,(n-k)!}$$

6.2 Сочетания с повторениями

Определение. *Сочетанием с повторениями* из n элементов по k называется неупорядоченный набор из k элементов из n-элементного множества с возможностью повторения элементов в наборе.

Обозначается как $\tilde{\mathbf{C}}_n^k$. Вывод: Пусть дано n-элементное множество $A = \{a_1, a_2, \dots, a_n\}$. Возьмем какое-либо сочетние с повторениями и упорядочим элементы в нем. Например: $(a_1, a_1, a_1, a_2, a_3, a_6, a_6, \dots)$. Обозначим каждый элемент как точку, а на месте смены индекса элемента поставим палочку.

Пример 3. *Из множества* $\{a_1, a_2, a_3, a_4, a_5\}$*:*

$$(a_1, a_1, a_3, a_5) \to \boxdot\boxdot \,||\, \boxdot \,||\, \boxdot$$

$$(a_3, a_3, a_3, a_4) \to||\, \boxdot\,\boxdot\,\boxdot \,|\, \boxdot \,|$$

$$(a_2, a_2, a_4, a_4) \to|\, \boxdot\boxdot \,||\, \boxdot\boxdot \,|$$

$$(a_1, a_2, a_5, a_5) \to \boxdot \,|\, \boxdot \,|||\, \boxdot\boxdot$$

$$(a_1, a_2, a_4, a_4) \to \boxdot \,|\, \boxdot \,||\, \boxdot\boxdot \,|$$

Таким образом можно однозначно сопоставить неупорядоченный набор с последовательностью точек и единиц. Тогда для задания неупорядоченного набора из k элементов из n-элементного множества необходимо выбрать k точек из $n + k - 1$ ячеек.

$$\tilde{\mathbf{C}}_n^k = \mathbf{C}_{n+k-1}^k$$

7 Бином Ньютона

$(a+b)^1 = a + b$
$(a+b)^2 = a^2 + 2ab + b^2$
$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$
$\dots$
$(a+b)^n = \underbrace{(a+b) \times (a+b) \times \dots \times (a+b)}_{n \text{ раз}} =$
$= \underbrace{a^n + na^{n-1}b + \dots + \mathbf{C}_n^k a^{n-k}b^k + \dots + nab^{n-1} + b^n}_{2^n \text{ неприведенных слагаемых}}$
Таким образом,

$$(a+b)^n = \sum_{k=0}^{n} \mathbf{C}_n^k \times a^{n-k} \times b^k$$

$$\underbrace{T_{k+1}}_{k+1\text{-ое слагаемое}} = \mathbf{C}_n^k \times a^{n-k} \times b^k$$

8 Свойства биномиальных коэффициентов. Треугольник Паскаля.

1. $\mathbf{C}_n^0 = 1, \forall n \in \mathbb{N}$
2. $\mathbf{C}_n^n = 1, \forall n \in \mathbb{N}$
3. $\mathbf{C}_n^k + \mathbf{C}_n^{k-1} = \mathbf{C}_{n+1}^k$

   Доказательство.

$$\frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!} = \frac{n!}{k!\,(n-k)!} + \frac{n! \times k}{k!\,(n-k)!\,(n-k+1)} =$$

$$= \frac{n!\,(n-k+1) + n! \times k}{k!\,(n-k)!\,(n-k+1)} = \frac{n!\,(n+1)}{k!\,(n-k)!\,(n-k+1)} =$$

$$= \frac{(n+1)!}{k!\,(n+1-k)!} = \mathbf{C}_{n+1}^k$$

   □

4. $\sum_{k=0}^{n} (-1)^k \times \mathbf{C}_n^k = 0$

   Доказательство. Докажем индукцией по n. Проверим для $n = 1$:

$$\mathbf{C}_1^0 - \mathbf{C}_1^1 = 1 - 1 = 0$$

   Предположим, что для $n = m, m \in \mathbb{N}$ выражение верно:

$$\mathbf{C}_m^0 - \mathbf{C}_m^1 + \cdots + (-1)^m \mathbf{C}_m^m = 0$$

   Рассмотрим выражение для $n = m + 1$:

$$\underbrace{\mathbf{C}_{m+1}^0}_{=1} - \mathbf{C}_{m+1}^1 + \cdots + (-1)^m \mathbf{C}_{m+1}^m + (-1)^{m+1} \underbrace{\mathbf{C}_{m+1}^{m+1}}_{=1} =$$

$$= 1 - \mathbf{C}_{m+1}^1 + \cdots + (-1)^m \mathbf{C}_{m+1}^m + (-1)^{m+1} =$$

$$= 1 - \left(\mathbf{C}_m^0 + \not{\mathbf{C}}_m^1\right) + \left(\not{\mathbf{C}}_m^1 + \not{\mathbf{C}}_m^2\right) - \cdots + (-1)^m \left(\not{\mathbf{C}}_m^{m-1} + \mathbf{C}_m^m\right) + (-1)^{m+1} =$$

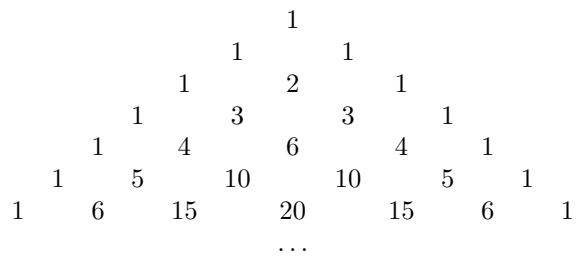
$$= 1 - \underbrace{\mathbf{C}_m^0}_{=1} + (-1)^m \underbrace{\mathbf{C}_m^m}_{=1} + (-1)^{m+1} =$$

$$= 1 - 1 + (-1)^m + (-1)^{m+1} =$$

$$= 0$$

   □

Треугольник Паскаля получается из свойства суммы биноминальных коэффициентов. Каждый ряд является рядом биномиальных коэффициентов для разложения, степень которого равна номеру ряда (начиная с нуля).



9 Полиномиальная формула

Полиномиальная формула является обобщением бинома Ньютона. Рассмотрим выражение $(a_1 + a_2 + \cdots + a_k)^n$:

$$(a_1 + \cdots + a_k)^n = \underbrace{(a_1 + \cdots + a_k) \times (a_1 + \cdots + a_k) \times \cdots \times (a_1 + \cdots + a_k)}_{n \text{ раз}} =$$

$$= a_1^n + a_2^n + \cdots + a_k^n + n \times a_1^{n-1} \times a_2 + \cdots + \boxdot \times a_1^{i_1} \times a_2^{i_2} \times \cdots \times a_k^{i_k} + \cdots =$$

$$= \sum_{\sum_{j=1}^{k} i_j = n} \left(\boxdot \times \prod_{j=1}^{k} \left(a_j^{i_j} \right) \right)$$

Числа $i_1, i_2, \ldots, i_k$ отображают, сколько чисел каждого типа будет в данном члене разложения. При этом коэффициент перед этим первым числом будет определяться как $\mathbf{C}_n^{i_1}$, перед вторым $\mathbf{C}_{n-i_1}^{i_2}$, $\ldots$, перед k-тым: $\mathbf{C}_{n-(i_1+i_2+\cdots+i_{k-1})}^{i_k}$. Соответственно, коэффициент перед членом разложения будет определяться произведением этих чисел.

$$\mathbf{C}_n^{i_1} \times \mathbf{C}_{n-i_1}^{i_2} \times \mathbf{C}_{n-(i_1+i_2)}^{i_3} \times \cdots \times \underbrace{\mathbf{C}_{n-(i_1+i_2+\cdots+i_{k-1})}^{i_k}}_{=1} =$$

$$= \frac{n!}{i_1! \times (n-i_1)!} \times \frac{(n-i_1)!}{i_2! \times (n-(i_1+i_2))!} \times \frac{(n-(i_1+i_2))!}{i_3! \times (n-(i_1+i_2+i_3))!} \times \ldots$$

$$\cdots \times \frac{(n-(i-1+\cdots+i_{k-3}))!}{i_{k-2}! \times (n-(i_1+\cdots+i_{k-2}))!} \times \frac{(n-(i_1+\cdots+i_{k-2}))!}{i_{k-1}! \times \underbrace{(n-(i_1+\cdots+i_{k-1}))!}_{i_k!}} =$$

$$= \frac{n!}{i_1! \times i_2! \times \cdots \times i_{k-1}! \times i_k!}$$

Таким образом, окончательно получаем:

$$(a_1 + \cdots + a_k)^n = \sum_{i_1+\cdots+i_k=n} \frac{n!}{i_1! \times \cdots \times i_k!} \times \left(a_1^{i_1} \times \cdots \times a_k^{i_k} \right)$$

$$\left(\sum_{j=1}^{k} a_j \right)^n = \sum_{\left(\sum_{j=1}^{k} i_j\right)=n} \left(\frac{n!}{\prod_{j=1}^{k} i_j!} \times \prod_{j=1}^{k} a_j^{i_j} \right)$$

Число неподобных членов в разложении равно $\tilde{\mathbf{C}}_k^n$ (получается, если представить n ячеек, в которые необходимо расставить с повторениями цифры от 1 до k). Сумма положительных коэффициентов при членах разложения равна k^n.

10 Сравнения

Каждое число при делении на другое дает какой-либо остаток. Говорят $a \equiv b \pmod n, n \in \mathbb{N}$, если $a - b \vdots n$ (a сравнимо с b по модулю n; т. е. $a - b$ делится на n). Свойства сравнений:

- $a \equiv a \pmod n$.

  Доказательство.

  $$a \equiv a \pmod n$$
  $$a - a \equiv 0 \pmod n$$
  $$0 \vdots n$$

  $\square$

- $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ (симметричность).

  Доказательство.

  $$a - b \vdots n \Rightarrow a - b = c \times n, c \in \mathbb{Z}$$
  $$\Rightarrow -c \times n = b - a \Rightarrow b - a \vdots n$$
  $$\Rightarrow b \equiv a \pmod{n}$$

  □

- $a \equiv b \pmod{n}, b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (транзитивность)

  Доказательство.

  $$(a - b \vdots n) \wedge (b - c \vdots n) \Rightarrow (a - c \vdots n) \Rightarrow (a \equiv c \pmod{n})$$

  □

- $a \equiv b \pmod{n} \Rightarrow a + c \equiv b + c \pmod{n}$

  Доказательство.

  $$a \equiv b \pmod{n} \Rightarrow a - b \vdots n \Rightarrow a - b = n \times d, d \in \mathbb{Z}$$
  $$a - b = n \times d \Rightarrow (a + c) - (b + c) = n \times d \Rightarrow a + c \equiv b + c \pmod{n}$$

  □

- $a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$

  Доказательство.

  $$a \equiv b \pmod{n} \Rightarrow a - b \vdots n$$
  $$(a - b) \times c \vdots n \Rightarrow ac - bc \vdots n \Rightarrow ac \equiv bc \pmod{n}$$

  □

- $(a \equiv b \pmod{n}) \wedge (c \equiv d \pmod{n}) \Rightarrow (a + c \equiv b + d \pmod{n})$

  Доказательство.

  $$(a - b = xn) \wedge (c - d = yn)$$
  $$(a - b) + (c - d) = (x + y)\, n$$
  $$(a + c) - (b + d) = (x + y)\, n$$
  $$\Rightarrow a + c \equiv b + d \pmod{n}$$

  □

- $(a \equiv b \pmod{n}) \wedge (c \equiv d \pmod{n}) \Rightarrow (ac \equiv bd \pmod{n})$

  Доказательство.

  $$a \equiv b \pmod{n} \Rightarrow ac \equiv bc \pmod{n}$$
  $$c \equiv d \pmod{n} \Rightarrow bc \equiv bd \pmod{n}$$
  $$\Rightarrow ac \equiv bd \pmod{n}$$

  □

11 Простые числа и их свойства

Определение. Пусть a — натуральное число. a называется *простым* , если $a \neq 1$ и $\forall x, y \in \mathbb{N} \mid a = xy \Rightarrow (x = a) \vee (y = a)$.

Теорема. *Если* $ab \vdots p, p$ *— простое* $\Rightarrow b \vdots c$

Доказательство. Т. к. $ab \vdots p$, p — простое, то $(a; p) = p \vee (b; p) = p. \Rightarrow (a \vee b) \vdots p.$ □

Теорема. *Существует бесконечное число простых чисел.*

Доказательство. Пусть простых чисел — конечное число. Тогда:

$$\{p_1, p_2, p_3, \ldots, p_n\}$$

Все простые числа. Возьмем число a, такое, что:

$$a = \prod_{i=1}^{n} p_i + 1$$

Тогда по основной теореме арифметики число a представимо в виде:

$$a = q_1 \times q_2 \times \ldots \times q_k \quad (\text{где } q_1, q_2, \ldots, q_k \text{ — простые числа})$$

Допустим, что $q_1 = p_j$, тогда:

$$\underbrace{q_1}_{\vdots p_j} \times q_2 \times \ldots \times q_k = p_1 \times p_2 \times \ldots \times \underbrace{p_j}_{\vdots p_j} \times \ldots \times p_n + 1$$

$\Rightarrow 1 \vdots p_j$
$\Rightarrow$ Противоречие
$\Rightarrow q_1, q_2, \ldots, q_k$ — новые простые числа. □

12 Наибольший общий делитель. Алгоритм Евклида.

$$a, b \in \mathbb{Z}$$

Определение. *НОД* — наибольшее целое число, такое, что $(a \vdots x) \wedge (b \vdots x)$.

Определение. *НОК* — наименьшее целое число, такое, что $(a \mid x) \wedge (b \mid x)$.

Для поиска НОД'а чисел используется алгоритм Евклида.

$$\begin{array}{lll} a & = b \times u_1 & +r_1, \text{ где } r_1 \leq b,\ r_1 \geq 0 \\ b & = r_1 \times u_2 & +r_2, \text{ где } r_2 \in [0; r_1] \\ r_1 & = r_2 \times u_3 & +r_3 \\ & \ldots & \\ r_{n-1} & = r_n \times u_{n+1} & +r_{n+1} \\ r_n & = r_{n+1} \times u_{n+2} & \end{array}$$

r_{n+1} — НОД $(a; b)$. Надо доказать, что $(a \vdots r_{n+1}) \wedge (b \vdots r_{n+1})$ и что r_{n+1} — наибольший делитель.

Доказательство пункта 1. Доказательство "снизу-вверх".
$(r_n = r_{n+1} \times u_{n+2}) \Rightarrow r_n \vdots r_{n+1}$
$(r_{n-1} = r_n \times u_{n+1} + r_{n+1}) \Rightarrow r_{n-1} \vdots r_{n+1}$
$\ldots$
$\Rightarrow b \vdots r_{n+1}$
$\Rightarrow a \vdots r_{n+1}$ □

Доказательство пункта 2. Иными словами, надо доказать, что r_{n+1} делится на любой делитель a и b. Доказательство "сверху-вниз".
Пусть $a, b \vdots d$. Тогда:
$(r_1 = \underline{a} - \underline{b} \times u_1) \Rightarrow r_1 \vdots d$
$\left(r_2 = \underline{b} - \underline{r_1} \times u_1\right) \Rightarrow r_2 \vdots d$
$\left(r_3 = \underline{r_1} - \underline{r_2} \times u_1\right) \Rightarrow r_2 \vdots d$
...
$\left(r_{n+1} = \underline{r_{n-1}} - \underline{r_n} \times u_{n+1}\right) \Rightarrow r_{n+1} \vdots d$ □

Следствие из алгоритма Евклида:

$$(\forall a, b \in \mathbb{Z}\, \exists\, (a; b) = d) \Rightarrow d = ax + by \mid x, y \in \mathbb{Z}$$

Доказательство.

$$d = r_{n+1} = r_{n-1} - r_n \times u_{n+1} = \cdots = \alpha \times a + \beta \times b$$

□

Теорема. $(a_1; \ldots; a_n) = d \Rightarrow \exists u_1, \ldots, u_n \in \mathbb{Z} \mid d = a_1 u_1 + \cdots + a_n u_n$

13 Основная теорема арифметики

Теорема. *Всякое натуральное число раскладывается на произведение простых чисел, и это разложение единственно (с точностью до перестановки).*

Доказательство существования разложения. Докажем усиленным принципом индукции. n — натуральное число. для $n = 1$:

$$n = \underbrace{2 \times 2 \times 2 \times 2 \times \cdots \times 2}_{0 \text{ раз}}$$

Пусть все натуральные числа, меньшие n раскладываются. Докажем, что n раскладывается на простые множители. Возможны два случая.

1. n — простое. Тогда разложение очевидно.
2. n — составное. Тогда $n = ab \mid (a < n) \wedge (b < n)$. По предположению индукции a и b раскладываются на простые числа. Тогда и n раскладывается на простые числа.

□

Доказательство единственности. n — натуральное число.

$$n = p_1 \times \cdots \times p_k$$

Пусть существует другое разложение:

$$n = q_1 \times \cdots \times q_l$$

Приравняем:

$$p_1 \times \cdots \times p_k = q_1 \times \cdots \times q_l$$

Правая часть равна n и делится на q_1. Значит левая часть тоже делится на q_1. А т. к. все p_i простые, то $\exists j \in \mathbb{N}, j \leq k \mid p_j = q_1$. Сократим и перенумеруем, начиная с двух.

$$p_2 \times \cdots \times p_k = q_2 \times \cdots \times q_l$$

Аналогично продолжаем сокращать. В какой-то момент слева или справа будет единица. Т. к. левая и правая часть определяли одну и ту же часть и сокращали на одинаковые числа, то в другой части тоже должна стоять единица. Значит $k = l$ и $\{p_i\} = \{q_j\}$. □

14 Малая теорема Ферма

Теорема. $a^p \equiv a \pmod p$, *если* p - *простое,* $a \in \mathbb{Z}$

Доказательство. 1. Если $a \vdots p$, то $0 \equiv 0 \pmod 0$.

2. Тогда можно считать, что $(a; p) = 1$. Докажем, что $a^{p-1} \equiv 1 \pmod p$.

3. Выпишем все нулевые остатки от деления на p:

$$A = \{1, 2, 3, \ldots, p-2, p-1\}$$

Причем $a \mod p \in A$.

4. Найдем все элементы A, помноженные на a:

$$\underbrace{a \times 1, a \times 2, a \times 3, \ldots, a \times (p-2), a \times (p-1)}_{\text{Все разные по модулю } p\text{, все ненулевые по модулю } p}$$

Докажем, что они все разные по модулю p.

Предположим, что $\exists\, i, j \mid a \times i \equiv a \times j \pmod p, i \neq j$.

Тогда $a \times (i - j) \vdots p$

Из этого получаем:

$$a \quad \vdots \quad p \tag{1}$$
$$i - j \quad \vdots \quad p \tag{2}$$

Должно выполняться условие 1 или 2.

Выражение 1 неверно по предположению, что $(a; p) = 1$.

Выражение 2 неверно, потому что $i, j < p \Rightarrow |i - j| < p$.

Докажем, что они все ненулевые по модулю p.

Предположим, что $\exists\, i \mid a \times i \equiv 0 \pmod p$.

Тогда $a \times i \vdots p$.

Из этого получаем:

$$a \quad \vdots \quad p \tag{3}$$
$$i \quad \vdots \quad p \tag{4}$$

Должно выполняться условие 3 или 4.

Выражение 3 неверно по предположению, что $(a; p) = 1$.

Выражение 4 неверно, потому что $i < p$.

5. Т. к. числа $1, \ldots, p-1$ — все ненулевые остатки от деления на p, а $a \times 1, \ldots, a \times (p-1)$ все разные по модулю p, то можно сопоставить: $n \equiv a \times m \pmod p \mid n, m \in \mathbb{N} \mid n, m < p$.

$$\Rightarrow (a \times 1) \times (a \times 2) \times \ldots \times (a \times (p-1)) \equiv 1 \times 2 \times \ldots \times (p-1) \pmod p$$
$$\Rightarrow \left(a^{p-1} - 1\right) \times (p-1)! \equiv 0 \pmod p$$
$$\Rightarrow \underbrace{(p-1)!}_{\not\vdots p} \times \left(a^{p-1} - 1\right) \equiv 0 \pmod p$$
$$\Rightarrow a^{p-1} - 1 \equiv 0 \pmod p$$
$$\Rightarrow a^{p-1} \equiv 1 \pmod p$$

6. Т. к. $a^{p-1} \equiv 1 \pmod p$ верно, то $a^p \equiv a \pmod p$ тоже верно.

□

15 Теорема Вильсона

Теорема. $(n-1)! \equiv -1 \pmod{n} \Leftrightarrow n$ — *простое.*

Доказательство. Пусть $(n-1)! \equiv -1 \pmod{n}$. Доказать, что n — простое. Предположим, что n — непростое. Тогда:

$$\Rightarrow (n-1)! \equiv -1 \pmod{ab} \quad | \quad a, b \in (1, n)\,,\ a, b \in \mathbb{N}$$

$$\Rightarrow \underbrace{1 \times 2 \times 3 \times \ldots \times (n-1)}_{\text{Содержит } a} = -1 + \underbrace{kn}_{\vdots a} \quad | \quad k \in \mathbb{Z}$$

$$\Rightarrow 1 \vdots a$$

Получили противоречие. Значит, n — простое. Рассмотрим $(n-1)!$.

Утверждение. $\forall\, a \in \{1, 2, \ldots, n-1\}\ \exists\, b \mid a \times b \equiv 1 \pmod{n}$

Доказательство. Т. к. n — простое, то $(a; n) = 1$. Тогда по свойству НОД'а:

$$\exists\, i, j \in \mathbb{Z} \mid a \times i + n \times j = 1$$

$$\Rightarrow a \times i \equiv 1 \pmod{n}$$

□

Утверждение. *К каждому числу из множества* $\{1, 2, \ldots, n-1\}$ *существует только одно число из этого множества, такое, что* $a \times b \equiv 1 \pmod{n}$.

Доказательство. Дано число a. Число b обратное к нему по модулю n. Предположим, что существует еще одно число b', обратное к a по модулю n.

$$a \times b \equiv 1 \pmod{n}, \quad a \times b' \equiv 1 \pmod{n}$$

$$a \times (b - b') \equiv 0 \pmod{n}$$

$$a \vdots n \quad \vee \quad b - b' \vdots n$$

Это не верно, так как $(a; n) = 1$ и $b, b' < n$. □

Утверждение. *Кроме элементов* 1 *и* $p-1$ *нету обратных самим себе по модулю* n.

Доказательство. Пусть $a \times a \equiv 1 \pmod{n}$. Тогда:

$$a^2 \equiv 1 \pmod{n}$$

$$a^2 - 1 \equiv 0 \pmod{n}$$

$$(a-1)\,(a+1) \equiv 0 \pmod{n}$$

$$\Rightarrow a - 1 \vdots p \quad \vee \quad a + 1 \vdots p$$

$$\Rightarrow a = 1 \quad \vee \quad a = p - 1$$

□

Тогда:

$$\left\{ \overbrace{1}^{\equiv 1},\ 2,\ \overbrace{\underbrace{3,\ \ldots}_{\equiv 1}}^{\equiv 1},\ \underbrace{(n-1)}_{\equiv 1} \right\}$$

$$\Rightarrow \prod_{i=1}^{n-1} i \equiv 1 \times 2 \times \ldots \times (n-1) \equiv 1 \times 1^{n-3} \times (-1) \equiv -1$$

$$\Rightarrow (n-1)! \equiv -1 \pmod{n}$$

□

16 Диофантовы уравнения

Уравнения в целых числах. Линейные диофантовы уравнения:

$$ax + by = c, \quad (\text{где } a, b, c \in \mathbb{Z},\ x, y \in \mathbb{Z})$$

Пусть $(a; b) = d$. Тогда $a = a_1 d,\ b = b_1 d$, где $(a_1; b_1) = 1$. Тогда уравнение принимает вид:

$$a_1 dx + b_1 dy = c$$

Если $c \not\vdots d$, то решений нет. Пусть $c \vdots d \Rightarrow c = c_1 d$. Уравнение примет вид:

$$a_1 dx + b_1 dy = c_1 d$$

$$a_1 x + b_1 y = c_1$$

Тогда можно считать, что $(a; b) = d$. Надо решить уравнение $ax + by = c$. Пусть $(x_0; y_0)$ — решение уравнения. Оно всегда существует. Т. к. $(a; b) = 1 \Rightarrow 1 = au + bv \Rightarrow c = a\underline{cu} + b\underline{cv}$. Тогда:

$$-\begin{cases} ax + by &= c \\ ax_0 + by_0 &= c \end{cases}$$

$$a(x - x_0) = -b(y - y_0)$$

$$\Rightarrow x - x_0 \vdots b \Rightarrow x - x_0 = bt, t \in \mathbb{Z}$$

$$\Rightarrow y - y_0 = -at$$

Итого,

$$\begin{cases} x &= x_0 + bt \\ y &= y_0 - at, t \in \mathbb{Z} \end{cases}$$

17 Теорема и функция Эйлера

17.1 Функция Эйлера

Определение. *Функция Эйлера* $(\varphi(n))$ — количество чисел, меньших n и взаимнопростых с ним.

Пример 4. $\varphi(5) = 4$ — $\{1, 2, 3, 4\}$, $\varphi(20) = 8$ — $\{1, 3, 7, 9, 11, 13, 17, 19\}$,

Если p — простое, то:

$$\varphi(p) = p - 1$$

$$\varphi\left(p^2\right) = p^2 - p$$

$$\varphi\left(p^3\right) = p^3 - p^2$$

$$\dots$$

$$\varphi\left(p^i\right) = p^i - p^{i-1}, \quad i \in \mathbb{N}$$

Также:

$$\varphi(m \times n) = \varphi(m) \times \varphi(n), \quad \text{при } (m; n) = 1$$

17.2 Теорема Эйлера

Теорема. *Если* $(a;n)=1$, *то* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Доказательство. Выпишем все числа, меньшие n и взаимно простые с ним:

$$A = \left\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{\varphi(n)}\right\}$$

Домножим каждый из элементов множества A на a:

$$A' = \left\{a \times \alpha_1, a \times \alpha_2, a \times \alpha_3, \ldots, a \times \alpha_{\varphi(n)}\right\}$$

Каждый из них не сравним с n по модулю n, взаимопрост с n и все они разные по модулю n (аналогично малой теореме Ферма (стр. 12)). Тогда:

$$(a \times \alpha_1) \times (a \times \alpha_2) \times (a \times \alpha_3) \times \ldots \times \left(a \times \alpha_{\varphi(n)}\right) \equiv \alpha_1 \times \alpha_2 \times \alpha_3 \times \ldots \times \alpha_{\varphi(n)} \pmod{n}$$

$$a^{\varphi(n)} \times \prod_{i=1}^{\varphi(n)} \alpha_i \equiv \prod_{i=1}^{\varphi(n)} \alpha_i \pmod{n}$$

$$a^{\varphi(n)} \times \prod_{i=1}^{\varphi(n)} \alpha_i - \prod_{i=1}^{\varphi(n)} \alpha_i \equiv 0 \pmod{n}$$

$$\underbrace{\left(\prod_{i=1}^{\varphi(n)} \alpha_i\right)}_{\not\vdots n \Leftarrow (\forall\, \alpha_i \in A \Rightarrow (\alpha_i; n)=1)} \times \left(a^{\varphi(n)} - 1\right) \equiv 0 \pmod{n}$$

$$\Rightarrow a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$$

$$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$$

□

18 Мультипликативность функции Эйлера

Теорема. $\varphi(mn) = \varphi(m)\,\varphi(n)$, *при* $(m;n)=1$.

Доказательство. Возьмем множество A из взаимнопростых с mn элеметнов, меньших mn. Также возьмем множества B и C, аналогичные для m и n. $A = \{a \mid (a;mn)=1\,;\ a<mn\}\,;\ |A| = \varphi(mn)$
$B = \{b \mid (b;m)=1\,;\ b<m\}\,;\ |B| = \varphi(m)$
$C = \{c \mid (c;n)=1\,;\ c<n\}\,;\ |C| = \varphi(n)$
Если мы докажем, что между множеством A и множествами B, C существует взаимнооднозначное соответствие, то мультипликативность будет доказана. При этому каждый элемент из A будет иметь образ в B и C.

$$a_n \to (b_i \in B; c_j \in C)$$

$$a_n \to (a_n \mod m; a_n \mod n)$$

Почему $a_i \mod m \in B$**?** Пусть $(a_i \mod m = x) \Rightarrow a_i \equiv x \pmod{m}$. Надо доказать, что $x \in B$, т. е. $(x;m)=1$. Предположим, что $(x \vdots p) \wedge (m \vdots p)$. $\Rightarrow a_i \mod m \vdots p$. Знаем, что $(a_i - x \vdots m) \Rightarrow (a_i = km + x, m \in \mathbb{Z})$. $m \vdots p$ и $x \vdots p$ (см. выше). Значит, $a_i \vdots p$. Тогда $(a_i; mn) \geq p \neq 1$. Противоречие.

Почему $a_i \mod n \in C$**?** Аналогично первому пункту.

Почему разные элементы из A **отображаются в разные элементы?** Предположим, что $c \mod m = c' \mod n$. Тогда $(c - c' \vdots m) \wedge (c - c' \vdots n)$. Тогда, т. к. m и n взаимнопростые, $c - c' \vdots mn$. Но этого не может быть, т. к. они $c, c' < mn$.

Почему $(b_i; c_j)$ **является образом** a_n**?** Возьмем такой $x \in \{0, 1, 2, \ldots, mn-1\}$, что

$$\begin{cases} x & \equiv b_i \pmod m \\ x & \equiv c_j \pmod n \end{cases}$$

Такой x в данном промежутке всегда можно взять (по китайской теореме об остатках). Докажем, что $x \in A$. Пусть $x \notin A$. Тогда $(x; mn) \neq 1$. Тогда $\exists p \mid (x \vdots p) \wedge (mn \vdots p) \wedge p$ — простое. Т. к. $mn \vdots p$, то $(m \vee n) \vdots p$. Также, т. к. $x \equiv b_i \pmod m$, то $x - b_i = km, k \in \mathbb{Z} \Rightarrow b_i = x - km \Rightarrow b_i \vdots p$, т. к. $x \vdots p$ и $km \vdots p$. Значит, $(b_i; m) \neq 1$. Противоречие. Значит, $x \in A$.

Таким образом, каждому элементу из A взаимно однозначно соответствует элемент из B и C. $\square$

19 Китайская теорема об остатках

Теорема. *Система сравнений*

$$\begin{cases} x & \equiv a_1 \pmod{b_1} \\ x & \equiv a_2 \pmod{b_2} \\ x & \equiv a_3 \pmod{b_3} \\ & \ldots \\ x & \equiv a_n \pmod{b_n} \end{cases}$$

имеет единтсвенное решение $x = a \pmod{b_1 b_2 b_3 \ldots b_n}$ *при попарно взаимно простых* $b_1, b_2, b_3, \ldots, b_n$.

Доказательство. Докажем индукцией по n. Для $n = 1$ очевидно. Предположим, что для $n = k$ верно (т. е. система имеет решение $x \equiv c_1 \pmod{b_1 b_2 b_3 \ldots b_k}$). Тогда надо доказать, что система

$$\begin{cases} x & \equiv c_1 \pmod{b_1 b_2 b_3 \ldots b_k} \\ x & \equiv c_2 \pmod{b_{k+1}} \end{cases}$$

всегда имеет решение. Пусть $b_1 b_2 b_3 \ldots b_k = B, b_k + 1 = b$. Тогда

$$\begin{cases} x & = uB & +c_1 \\ x & = vb & +c_2 \end{cases}$$

$$uB + c_1 = vb + c_2$$

$$uB - vb = c_2 - c_1$$

Получили диофантово уравнение относительно u и v. Оно имеет решения, т. к. B и b взаимнопростые.

$$\begin{cases} u & = u_0 + b\tau \\ v & = v_0 + B\tau \end{cases}, \tau \in \mathbb{Z}$$

$$x = B(u_0 + b\tau) + c_1$$

$$x \equiv \underbrace{Bu_0 + c_1}_{c_3} \pmod{Bb}$$

$$x \equiv c_3 \pmod{b_1 b_2 b_3 \ldots b_k b_{k+1}}$$

$\square$

20 Уравнение Пелля

Определение. *Уравнением Пелля* называется уравнение вида $x^2 - Ay^2 = 1$, где $A \geq 0 \wedge A \neq a^2, \forall a \in \mathbb{N}$.

Если $A = a^2$, то:

$$(x - ay)(x + ay) = 1$$

$$\frac{1}{x + ay} = x - ay$$

$$\Rightarrow \left[\begin{cases} x &= 1 + ay \\ x &= 1 - ay \end{cases} \right. \left. \begin{cases} x &= -1 + ay \\ x &= -1 - ay \end{cases} \right] \Rightarrow \left[\begin{cases} x &= 1 \\ y &= 0 \end{cases} \right. \left. \begin{cases} x &= -1 \\ y &= 0 \end{cases} \right]$$

Утверждение. *$\exists x_1, y_1 > 0$, удовлетворяющие равенству. Пусть $(x_1; y_1)$ — минимальное положительное решение (доказательство сложное).*

Теорема. *Если $(x_1; y_1)$ — минимальное положительное решение, то $\left(x_1 + y_1\sqrt{A}\right)^n = x_n + y_n\sqrt{A}$, где $(x_n; y_n)$ — n-ое решение. И все положительные решения уравнения совпадают с одной из пар $(x_n; y_n)$.*

Доказательство.

Утверждение. *Если $(u; v), (s; t)$ — решения уравнения и $u < s$, то $v < t$.*

Доказательство.

$$u^2 - Av^2 = 1$$
$$s^2 - At^2 = 1$$
$$\Rightarrow v^2 = \frac{u^2 - 1}{A} \wedge t^2 = \frac{s^2 - 1}{A}$$

Далее очевидно. □

Пусть $\exists (u; v)$ — положительное решение, не совпадающее ни с одной из пар $(x_n; y_n)$. Тогда можно считать, что $x_n < u < x_{n+1}$ и $y_n < v < y_{n+1}$. Имеем:

$$\begin{aligned} x_n^2 - Ay_n^2 &= 1 \\ x_{n+1}^2 - Ay_{n+1}^2 &= 1 \\ u^2 - Av^2 &= 1 \end{aligned}$$

Также известно, что $\left(x_1 + y_1\sqrt{A}\right)\left(x_n + y_n\sqrt{A}\right) = x_{n+1} + y_{n+1}\sqrt{A}$. Запишем в виде двойного неравенства положение пары $(u; v)$:

$$x_n + y_n\sqrt{A} < u + v\sqrt{A} < x_{n+1} + y_{n+1}\sqrt{A}$$

Домножим неравенство на $\left(x_n - y_n\sqrt{A}\right)$.

$$\begin{aligned} \underbrace{x_n^2 - Ay_n^2}_{=1} \quad &< \left(u + v\sqrt{A}\right)\left(x_n - y_n\sqrt{A}\right) \quad < \left(x_{n+1} + y_{n+1}\sqrt{A}\right)\left(x_n - y_n\sqrt{A}\right) \\ 1 \quad &< x_n u - y_n u\sqrt{A} + x_n v\sqrt{A} - y_n vA \quad < \frac{\left(x_1 + y_1\sqrt{A}\right)\left(x_n + y_n\sqrt{A}\right)}{\left(x_n + y_n\sqrt{A}\right)} \\ 1 \quad &< (x_n u - y_n vA) + (x_n v - y_n u)\sqrt{A} \quad < x_1 + y_1\sqrt{A} \end{aligned}$$

Надо оценить выражения, стоящие в скобках в средней части. Оценим $x_n u - y_n vA$:

$$\begin{cases} u^2 - Av^2 &= 1 \\ x_n^2 - Ay_n^2 &= 1 \end{cases} \Rightarrow \begin{cases} u &= \sqrt{1 + Av^2} \\ x_n &= \sqrt{1 + Ay_n^2} \end{cases}$$

$$\begin{array}{rcl} x_n u & \vee & y_n v A \\ \sqrt{(1+Av^2)(1+Ay_n^2)} & \vee & y_n v A \\ \sqrt{1+A(v^2+y_n^2)+\underline{y_n^2 v^2 A^2}} & \vee & y_n v A \\ \sqrt{1+A(v^2+y_n^2)+\underline{(y_n v A)}^2} & > & y_n v A \end{array}$$

$\Rightarrow (x_n u - y_n v A) > 0.$

Оценим $x_n v - y_n u$: $x_n v - y_n u = \sqrt{1+Ay_n^2}v - y_n\sqrt{1+Av^2}$.

$$\begin{array}{rcl} v\sqrt{1+Ay_n^2} & \vee & y_n\sqrt{1+Av^2} \\ v^2(1+Ay_n^2) & \vee & y_n^2(1+Av^2) \\ v^2+Ay_n^2v^2 & \vee & y_n^2+Ay_n^2v^2 \\ v^2 & \vee & y_n^2 \\ v^2 & > & y_n^2 \end{array}$$

$\Rightarrow (x_n v - y_n v) > 0.$

Таким образом, получили пару, удволетворяющую условию, но меньше минимальной $(x_1; y_1)$. Противоречие. Значит, такой пары $(u; v)$ существовать не может, а значит нет больше других положительных решений. $\square$