Без ограничения общности (б.о.о.) — это означает, что мы рассматриваем один из многих возможных случаев, но при этом уверены, что об оставшихся случаях можно сказать ровно то же.

1. Истинность, ложность и высказывания

A	B	не A	A и B	A или B	если A то B	A тогда и только тогда, когда B
0	0	1	0	0	1	1
0	1	1	0	1	1	0
1	0	0	0	1	0	0
1	1	0	1	1	1	1

Связка	*отрицание*	*конъюнкция*	*дизъюнкция*
В логике	не A	A и B	A или B
Символьно	$\neg A$, $\bar{A}$	$A \wedge B$, $A \mathbin{\&} B$	$A \vee B$
В русском языке	неправда, что A; A неверно	и A, и B; A, но B; A несмотря на B	либо A, либо B; A и/или B; A, B или и то, и то

Связка	*импликация*	*эквивалентность*
В логике	если A то B	A тогда и только тогда, когда B
Символьно	$A \to B$, $A \Rightarrow B$	$A \leftrightarrow B$, $A \Leftrightarrow B$
В русском языке	B если A; B когда A; A только когда B; A только если B; из A следует B; B при условии, что A; в случае A, B; A достаточно для B; B необходимо для A	A равнозначно B; если A, то B, и наоборот; A необходимо и достаточно для B

D/Д – предметная область предикатов

Конъюнкция и дизъюнкция имеют меньший ***приоритет***, чем отрицание, но больший, чем импликация.

Высказывания F и G (логически) **эквивалентны** тогда (и только тогда), когда они оба истинны либо оба ложны, в зависимости от истинностных значений высказываний $A1, \dots, An$.

Мы будем обозначать данное отношение как $F \equiv G$.

Высказывание F, состоящее из высказываний $A1, \dots, An$ мы называем **тавтологией** если оно (всегда) истинно при любых значениях высказываний $A1, \dots, An$.

Чтобы доказать тавтологичность формулы, достаточно предположить, что она ложна и прийти к противоречию.

Рассуждение **корректно** тогда и только тогда, когда вывод истинен при истинности посылок.

2. Язык математики

Квантор	*существования*	*всеобщности*
В логике	существует некоторый x такой, что A	для любого x верно A
В символах	$\exists x\, A(x)$; $\exists x\, A$	$\forall x\, A(x)$; $\forall x\, A$
На русском	для некоторого x, $A(x)$; для какого-то x, $A(x)$; что-то A; кто-то A; хотя бы один A; для хотя бы одного x, $A(x)$; есть x такой, что $A(x)$	для всех x, $A(x)$; для любого x, $A(x)$; для произвольного x, $A(x)$; каким бы x ни был, $A(x)$; $A(x)$ всегда верно; всё A; все A

$\neg\neg A \equiv A$ $A \vee B \equiv B \vee A$ (аналог. с $\wedge$)

$\neg(A \wedge B) \equiv \neg A \wedge \neg B$ $\neg(A \vee B) \equiv \neg A \vee \neg B$

$\mathbf{A \to B \equiv \neg A \vee B}$ $\mathbf{\neg(A \to B) \equiv A \wedge \neg B}$ $A \to B \equiv \neg B \to \neg A$

$\mathbf{A \to (B \to C) \equiv (A \wedge B) \to C}$

$\exists x\, A(x) \equiv \neg\forall x\, \neg A(x)$ $\forall x\, A(x) \equiv \neg\exists x\, \neg A(x)$

$\neg\forall x\, (P1(x) \to P2(x)) \equiv \exists x\, (P1(x) \wedge \neg P2(x))$

Связывание квантора сильнее (имеет большийприоритет), чем любая логическая связка, так что область действия квантора заканчивается на первой бинарной логической связке справа от него. Чтобы включить связку в область действия квантора, необходимы скобки: например, в $\forall x\, (A(x) \to B(x))$. С другой стороны, в формуле $\forall x\, A(x) \to B(x)$, никакое вхождение x в B(x) не связано первым квантором. То есть любое такое вхождение свободно для подстановки вместо него значения (если не связано каким-либо квантором внутри B(x)).

Vacuous truth (пустая истина). Пример: Сегодняшний король Франции лысый. $\forall x(K(x) \to B(x))$ – всегда истина, так как посылка всегда ложна.

Стандартный алгоритм доказательства утверждения «не существует такого x, что A(x)»: рассмотрим произвольный x такой, что A(x) истинно, и докажем, что какое-то известно ложное высказывание логически следует из A(x). Следовательно, если бы x с истинным A(x) существовал, то заведомо ложное высказывание было бы истинным, что невозможно. Таким образом, такого x не существует.

3. Строки/Списки

Правила образования списков под алфавитом A:

(П1) [ ] — строка над A; **[ ] ∈ S(A);**

(П2) если s′ — строка над A, а x — символ из A, тогда x : s′ — тоже строка над A, $\mathbf{\forall s' \forall x\, ((s' \in S(A) \wedge x \in A) \to x : s' \in S(A))}$

(A1) **[ ] ≠ x : s** для всех x и s.

(A2) $\mathbf{x : s = y : t \iff (x = y \wedge s = t)}$ для всех $x, y \in A$ и $s, t \in S(A)$, т.е. две строки, составленные с помощью оператора конкатенации **:** равны тогда и только тогда, когда соответствующие их головы и хвосты равны.

Принцип индукции (ПИ) для строк: Для любого унарного предиката P над S(A), если P([ ]) и $\forall s \forall x\, (P(s) \to P(x : s))$, то $\forall s\, P(s)$.

Утверждение P([ ]) называется базой индукции, $\forall s \forall x\, (P(s) \to P(x : s))$ — индукционным переходом, а P(s) — предположением индукции.

Рекурсивные функции для строк:

ln(s) – ***длина строки.*** Определим ln следующими двумя правилами:

ln([ ]) = 0;   ln(x : s) = 1 + ln(s) для всех x и s.

app(s1, s2) – *конкатенация/склеивание*. Определение:

app([ ], t) = t для любого t;   app(x : s, t) = x : app(s, t) для любых x, s, и t.

rev(s) – *обращение/инверсия строки*. Определение:

rev([ ]) = [ ];   rev(x : s) = app(rev(s), [x]) для всех x и s.

init(s) – *удаление последнего символа строки*. Определение:

init([ ]) = [ ];   init(x:[ ]) = [ ] для любого x из алфавита A

init(s≠[ ] → init (x:s) = x:init(s)) для любого символа x из алфавита A и любой строки s, состоящей из символов алфавита A

Леммы для строк:

1) Для любых s ∈ S(A), app(s, [ ]) = s.
2) Для любых s, t, r ∈ S(A), app(s, app(t, r)) = app(app(s, t), r).
3) Для любых s, t, r ∈ S(A), если app(s, t) = app(s, r), то t = r.
4) Для любых s, t ∈ S(A), если app(s, t) = [ ], то s = [ ] и t = [ ].

4. Индукция: $\forall\varphi$ (φ в определениях фиксирован)

ПМИ: $\mathbf{\varphi(0) \wedge \forall n \in N\, (\varphi(n) \to \varphi(n + 1)) \to \forall n \in N\, \varphi(n)}$. ($\varphi$ фиксирован)

Для произвольного предиката φ, если выполнено φ(0) и для каждого n ∈ N φ(n) влечёт φ(n + 1), то φ(n) выполнено для всех n ∈ N.

Утверждение φ(0) называется *базой индукции*, $\forall n \in N\, (\varphi(n) \to \varphi(n + 1))$ - *шаг индукции*, а утверждение φ(n) для каждого n - *предположение индукции*.

ПСИ: $\mathbf{\forall n\, (\forall m{<}n\, \varphi(m) \to \varphi(n)) \to \forall n\, \varphi(n)}$ или $\mathbf{Prog(\varphi) \to \forall n\, \varphi(n)}$

Для произвольного предиката φ, если верно φ(0) и для каждого n ∈ N φ(n + 1) выполнено, когда выполнены φ(0), φ(1). . . , φ(n), то φ(n) верно для любого n ∈ N.

Он позволяет нам использовать в качестве индукционного предположения не одно лишь φ(n), а все утверждения φ(0), φ(1), . . . , φ(n) вместе.

ПНЧ: $\mathbf{\exists n\, \varphi(n) \to \exists n\, (\varphi(n) \wedge \forall m{<}n\, \neg\varphi(m))}$

Если существует хотя бы одно натуральное число (n), для которого выполняется (φ(n)), то существует наименьшее такое число (n), для которого выполняется (φ(n)), и для всех чисел, меньших (n), утверждение (φ(m)) не выполняется.

5. Делимость и деление (подразумеваем ***целые*** числа)

Делимость: число а делит число b, если существует k ∈ Z такое, что **b = ak**. В свою очередь, число b делится на число (или числом) а. Также мы называем a делителем числа b, а b — кратным числу a. Мы будем писать **a | b**, если a делит b.

Пример: 1; −2 | 6 т.к. 6 = (−2) · (−3);

Леммы для делимости:

1) ±1 | a (a=±1*a) 2) 0 | a (0=a*0)
3) a|1 => a=±1   a|-1 => a=±1   4) a | a;
5) если a | b и b | c, то a | c; 6) если a | b и b | a, то a = ±b.
7) если a | b и a | c, то a |(b + c) и a |(b − c)

Следствие Л7: если a |(b + c) или a |(b − c) и a | b, то a | c.

Деление: Для любых натуральных чисел a и b ≠ 0, существует уникальная пара $(q, r) \in N^2$ такая, что $a = bq + r$ и $0 \le r < b$.

Такое число q называется *неполным частным*, а r — *остатком от деления* a на b.

Следствие. Для всех чисел a и b≠ 0, существует уникальная пара

$(q, r) \in Z \times N$ такая, что $a = bq + r$ и $0 \le r < |b|$.

Модульная арифметика. Положим m - положительное число. Тогда

a сравнимо с b по модулю m, если m |(a − b). Мы записываем это как

a ≡ b (mod m) или **a ≡ b (m)** и называем m ***модулем***.

m > 1 (т.к. любое число делится на 1)

<u>Лемма</u>: Для любых a, b, m, верно, что a ≡ b (mod m) тогда и только тогда, когда <u>a и b дают одинаковый остаток при делении на m</u>.

Следствия:

1) Никакие два числа из 0, 1, . . . , m − 1 не сравнимы по модулю m.
2) Предположим r — остаток при делении a на m. Тогда a ≡ r (mod m).
3) Для любых a, b, m верно следующее:
   - a ≡ a (mod m);
   - если a ≡ b (mod m), то b ≡ a (mod m);
   - если a ≡ b (mod m) и b ≡ c (mod m), то a ≡ c (mod m).

Положим a ≡ b (mod m) и c ≡ d (mod m). Тогда верно следующее:

1. a + c ≡ b + d (mod m);
2. ac ≡ bd (mod m);
3. a^n ≡ b^n(mod m) для всех n ∈ N.

<u>Простые числа и разложение на множители</u>. Число p > 1называется **простым**, если оно делится на ±1, на ±p и ни на что больше. В противном случае, число больше 1 зовется **составным**.

Отрицательные числа, 0 и 1 не являются ни простыми, ни составными.

Представление вида $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ для числа $n > 1$, где p_i — попарно отличные простые, а $a_i \in \mathbb{N}$, называется *разложением числа n на (простые) множители*. Естественным образом может возникнуть предположение, что в разложении числа n на множители участвует *каждое* простое число p, но только конечное количество простых чисел имеют ненулевые степени a. Возможно также разложить на множители число 1, но в таком случае каждое простое число в разложении будет иметь степень 0. Два разложения на множители *различны*, если и только если хотя бы одно простое число в их разложениях имеет различные степени.

Основная теорема арифметики: Для любого числа n > 1 существует уникальное его разложение на простые множители.

Теорема. Существует бесконечно много простых чисел.

<u>Признак делимости.</u>

Лемма 6.20 (Признак делимости). *Для любых ненулевых a и b, a делит b тогда и только тогда, когда $\alpha_i \le \beta_i$ для всех простых p_i, где α_i (или β_i) — степень простого p_i в разложении a (и, соответственно, b).*

1. Формализуйте следующее рассуждение, и выясните, корректно ли оно: Существуют куздры. Следовательно, есть такая куздра, что если она глокая, то и все вообще куздры глокие.

Решение:
пусть K это множество куздр,
$x \in K - x$ это куздра (можно так же использовать обозначение $K(x)$)
$G(x) - x$ глокая
Теперь формализуем рассуждение:
$\exists x \in K \Rightarrow (\exists x \in K : G(x) \Rightarrow \forall y \in \ : G(y))$
Заметим, что это выражение может быть ложно, например: $K = \{a, b\}$, G(a), $\neg G(b)$
$\exists x \in K$ – верно $\exists x \in K : G(x)$ – верно $\forall y \in K : G(y)$ – неверно
$1 \to (1 \to 0) = 1 \to 0 = 0$

2. Докажите, что n! $> 2^n$ при всех натуральных n > 3

Доказательство:
Докажем по индукции
База: $4! > 2^4$ - верно
Пусть верно для n, рассмотрим это неравенство для $n+1$: $(n+1)! = (n+1) \cdot n! > 2 \cdot 2^n = 2^{n+1}$, так как $n! > 2^n$ по предположению $\Rightarrow$ по ПМИ неравенсто верно $\forall n \in \mathbb{N}$

3. Существует ли такая логическая формула X = X(A, B, C), что формулы F = (A ∨¬B) → (C ∨ X)и G = (¬X ∧ ¬A) → (B → C) логически эквивалентны?

Решение:
Заметим, что если X - истина, то F = (A $\vee \neg B) \to (C \vee 1) = (A \vee \neg B) \to 1 \equiv 1$, а $G = (0 \wedge \neg A) \to (B \to C) = (0) \to (B \to C) \equiv 1$
Получим, что если взять X тавтологией (например, $\neg A \vee A \vee C \vee B$), то F и G тоже будут тавтологиями

4. Обязательно ли следующее утверждение о натуральных числах верно? Если не все числа голубые, но число 0 голубое, то найдется такое голубое число, что следующее за ним число не голубое.

Решение: Да, это верно. Доказательство:
Утверждение является имликацией: (не все числа голубые, но число 0 голубое) → (найдется такое голубое число, что следующее за ним число не голубое)
Допустим, что не все числа голубые, но 0 — голубое. По ПМИ для свойства голубизны имеем ¬(голубое(0) ∧ ∀ x: (голубое(x) → голубое(x + 1))) - ложная конъюнкция. голубое(0) = 1, значит, ∀ x: (голубое(x) → голубое(x + 1)) = 0 ⟺ ∃ x: (голубое(x)∧ ¬голубое(x + 1)) . Получим, что обязательно найдется такое голубое число, что следующее за ним число не голубое.

5. Докажите, что число 1203. . .308, содержащее ровно n троек, делится на 19 при всех натуральных n

Доказательство:
Докажем по индукции:
База: n = 0: 12008 = 19 * 632
Шаг: пусть a_k — число с k тройками — делится на 19. Тогда $a_{k+1} = (\frac{(a_k - 8)}{10} + 3) \cdot 100 + 8 = 10 \cdot a_k + 228$. Так как 228 = 19 ·12, в силу предположения индукции получаем, что a_{k+1} делится на 19, следовательно это верно $\forall n \in \mathbb{N}$

6. Докажите, что $\boldsymbol{app}(s, \boldsymbol{app}(t, r)) = \boldsymbol{app}(\boldsymbol{app}(s, t), r)$ для всех $s, t, r \in S(A)$

Доказательство: по определению, $\forall s \forall t \forall a\ app(a : s, t) = a : app(s, t)$ и $\forall t\ app([], t) = t$
Проведем индукцию по s:
База: $s = []$: $app([], app(t, r)) = app(t, r) = app(app([], t), r)$
Шаг: пусть для s равенство верно, тогда для $a : s$ имеем $app(a : s, app(t, r)) = a : app(s, app(t, r)) = a : app(app(s, t), r)$ (по предположению индукции) $= app(a : app(s, t), r) = app(app(a : s, t), r)$, чтд.

Задача 6. Простое число p поделили на $n!$ (где $n \in \mathbb{N}$) и получили остаток r, причём оказалось, что $1 < r < n^2$. Докажите, что r — всегда простое число.

Решение:

Рассмотрим деление простого числа p на $n!$:

$$p = q \cdot n! + r,$$

где q — целое число, а r — остаток, такой что $0 \le r < n!$.

По условию задачи, $1 < r < n^2$, значит $r \ne 0$ и $r \ne 1$.

Предположим, что r не является простым числом. Тогда r можно разложить на произведение $r = a \cdot b$, где $1 < a, b < r$.

Рассмотрим факториал $n!$. Он содержит в качестве множителей все целые числа от 1 до n, и следовательно $n!$ делится на a и b для всех $1 < a, b \le n$.

Так как $1 < a, b < n^2$ и по условию $r < n^2$, то a и b меньше n. Следовательно, a и b делят $n!$.

Таким образом, если r не является простым и делится на a и b, то r должно делить и p (так как $p = q \cdot n! + r$). Но p — простое число, и это возможно только если r равно либо 1, либо самому p. Однако, по условию $1 < r < n^2 < p$, следовательно, наше предположение о том, что r не является простым числом, неверно.

Таким образом, r должно быть простым числом.

Ответ: Остаток r всегда является простым числом при $1 < r < n^2$.

1. Математическая индукция

Задача: Доказать, что сумма первых n натуральных чисел равна $\frac{n(n+1)}{2}$.

- **База индукции**: Для $n = 1$: $\frac{1(1+1)}{2} = 1$ (истина).
- **Шаг индукции**: Пусть утверждение верно для $n = k$: $1 + 2 + \ldots + k = \frac{k(k+1)}{2}$. Нужно доказать для $n = k+1$: $1 + 2 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{k(k+1)+2(k+1)}{2} = \frac{(k+1)(k+2)}{2}$. Утверждение верно для $n = k+1$. Индукция завершена.

Если существует некоторое не голубое число, то перед ним должно быть голубое.

Исключение: Если 0 – не голубое число, то перед ним нет голубых.

Так как 0 – наименьшее натуральное число. По условию, данное исключение не исполняется – следовательно, любое число, не равное 0, не обладающее свойством голубизны, имеет голубое число перед ним.

По ПНЧ.

Докажите, что число 1203. . .308, содержащее ровно n троек, делится на 19 при всех натуральных n.

База: при n = 0 - докажем, что число 1203308 делится на 19. (63332)
Шаг: при n = n + 1, умножим число на 10, прибавим 300 и отнимем 80 и прибавим 8.

Посчитаем разницу между шагом: при умножении на 10 не сменяется кол-во десятков, следовательно свойство делимости сохраняется, а разница между шагом и исходным числам равна 300 – 80 + 8 = 228 : 19 = 12.

Следовательно, для любых натуральных n выполняется.

Задача: Найдите все натуральные n, при которых число $2n^3+3n+10^n$ делится на 11.

Решение:

Нам нужно найти такие n, при которых:

$$2n^3 + 3n + 10^n \equiv 0 \pmod{11}.$$

Рассмотрим выражение по модулю 11.

1. **Анализ степени** $10^n \mod 11$:

   Так как $10 \equiv -1 \pmod{11}$, то $10^n \equiv (-1)^n \pmod{11}$. Это дает нам:

   $$10^n \equiv \begin{cases} 1 \pmod{11}, & \text{если } n \text{ чётное,} \\ -1 \pmod{11}, & \text{если } n \text{ нечётное.} \end{cases}$$

2. **Рассмотрим выражение** $2n^3 + 3n + 10^n$ **по модулю 11**:

   Подставим выражение $10^n \equiv (-1)^n$ в наше равенство:

   $$2n^3 + 3n + (-1)^n \equiv 0 \pmod{11}.$$

   Теперь рассмотрим два случая: n чётное и n нечётное.

3. **Случай 1:** n **чётное.**

   Если n чётное, то $(-1)^n \equiv 1 \pmod{11}$, и наше выражение принимает вид:

   $$2n^3 + 3n + 1 \equiv 0 \pmod{11}.$$

   Проверим возможные чётные значения n:

   - $n = 2$:

     $$2 \cdot 2^3 + 3 \cdot 2 + 1 = 2 \cdot 8 + 6 + 1 = 21 \equiv 10 \pmod{11}.$$

     Не делится на 11.

   - $n = 4$:

     $$2 \cdot 4^3 + 3 \cdot 4 + 1 = 2 \cdot 64 + 12 + 1 = 141 \equiv 9 \pmod{11}.$$

     Не делится на 11.

   - $n = 6$:

     $$2 \cdot 6^3 + 3 \cdot 6 + 1 = 2 \cdot 216 + 18 + 1 = 451 \equiv 0 \pmod{11}.$$

     Делится на 11.

   Таким образом, $n = 6$ является решением в случае чётных n.

4. **Случай 2:** n **нечётное.**

   Если n нечётное, то $(-1)^n \equiv -1 \pmod{11}$, и наше выражение принимает вид:

   $$2n^3 + 3n - 1 \equiv 0 \pmod{11}.$$

   Проверим возможные нечётные значения n:

   - $n = 1$:

     $$2 \cdot 1^3 + 3 \cdot 1 - 1 = 2 + 3 - 1 = 4 \not\equiv 0 \pmod{11}.$$

     Не делится на 11.

   - $n = 3$:

     $$2 \cdot 3^3 + 3 \cdot 3 - 1 = 2 \cdot 27 + 9 - 1 = 62 \equiv 7 \pmod{11}.$$

     Не делится на 11.

   - $n = 5$:

     $$2 \cdot 5^3 + 3 \cdot 5 - 1 = 2 \cdot 125 + 15 - 1 = 264 \equiv 0 \pmod{11}.$$

     Делится на 11.

   Таким образом, $n = 5$ является решением в случае нечётных n.

Ответ: Натуральные числа n, при которых $2n^3 + 3n + 10^n$ делится на 11, это $n = 5$ и $n = 6$.