Лекция 4 логика и методология науки

- Макаров В.В.

$A, B, C, \ldots$ пропозициональные буквы

$\neg, \to$ примитивные связки

(а) Пропозициональные буквы — формулы

(в) $\mathcal{A}$ и $\mathcal{B}$ — формулы $\Rightarrow$

$\neg\mathcal{A}$, $\mathcal{A} \to \mathcal{B}$ — формулы

(A1) $A \to (B \to A)$

(A2) $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$

(A3) $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$

Здесь A, B, C — формулы

Modus Ponens (MP)

$$A, A \to B \vdash B$$

Теорема 1. $\vdash (A \to A)$

1. (A2) $(A \to ((A \to A) \to A)) \to ((A \to (A \to A)) \to (A \to A))$
2. (A1) $A \to ((A \to A) \to A)$
3. 1. 2. (MP) $(A \to (A \to A)) \to (A \to A)$
4. (A1) $A \to (A \to A)$
5. 3. 4. (MP) $\vdash (A \to A)$

Предложение (теорема дедукции, Эрбран, 1930)

Γ – множество формул. A и B – формулы.

$\Gamma, A \vdash B \Rightarrow \Gamma \vdash A \to B$

Доказательство.

$B_1, \ldots, B_n$ – вывод из Γ, A.

$B_n = B$.

Математическая индукция по i $(1 \le i \le n)$

докажем $\Gamma \vdash (A \to B_i)$

B_1 1) $B_1 \in \Gamma$

(A1) $B_1 \to (A \to B_1)$ $\Gamma \vdash (A \to B_1)$ по MP

2) B_1 – одна из аксиом

(A1) $B_1 \to (A \to B_1)$ $\Gamma \vdash (A \to B_1)$ по MP

3) $B_1 = A$ $\vdash A \to A$ (Задача) $\Gamma \vdash (A \to B_1)$

$i = 1$ (база) – исчерпано

Пусть $\Gamma \vdash (A \to B_k)$ $k < i$

1) B_i – аксиома, 2) $B_i \in \Gamma$, 3) $B_i = A$

(A1) $B_i \to (A \to B_i)$ $\Gamma \vdash (A \to B_i)$ (MP) $\vdash A \to A$

4) B_i – (MP) по B_j, $B_m = B_j \to B_i$ $j < i$, $m < i$

Предположение индукции.

$\Gamma \vdash A \to B_j$, $\Gamma \vdash A \to (B_j \to B_i)$

(A2) $\vdash (A \to (B_j \to B_i)) \to ((A \to B_j) \to (A \to B_i))$

(MP) $\Gamma \vdash (A \to B_j) \to (A \to B_i)$

(MP) $\Gamma \vdash (A \to B_i)$

$i = n$ $\Gamma \vdash (A \to B_n)$ ∎

Теорема 2.

$A \to B, B \to C \vdash A \to C$

1. $A \to B$
2. $B \to C$
3. A – гипотеза
4. B (MP) по 1. 3.
5. C (MP) по 2. 4.

Доказано: $A \to B, B \to C, A \vdash C$

По теореме Эрбрана: $A, A \to B, B \to C \vdash C$

имеем $A \to B, B \to C \vdash A \to C$

Теорема 3.

$A \to (B \to C), B \vdash A \to C$

1. B
2. $A \to (B \to C)$
3. A – гипотеза
4. $\vdash (B \to C)$ MP 2. 3.
5. $\vdash C$ MP 1. 4.
6. Теорема дедукции:

$A, A \to (B \to C), B \vdash C \Rightarrow$

$A \to (B \to C), B \vdash (A \to C)$.

ОСНОВНАЯ ЛЕММА

(a) $\neg\neg B \to B$

(b) $B \to \neg\neg B$

(c) $\neg A \to (A \to B)$

(d) $(\neg B \to \neg A) \to (A \to B)$

(e) $(A \to B) \to (\neg B \to \neg A)$

(f) $A \to (\neg B \to \neg(A \to B))$

(g) $(A \to B) \to ((\neg A \to B) \to B)$

(2

(a) $\vdash \neg\neg B \to B$

1. (A3) $(\neg B \to \neg\neg B) \to ((\neg B \to \neg B) \to B)$
2. $\neg B \to \neg B$ T.1
3. $(\neg B \to \neg\neg B) \to B$ T.3
4. (A1) $\neg\neg B \to (\neg B \to \neg\neg B)$
5. $\neg\neg B \to B$ T.2 3. 4.

(B) $\vdash B \to \neg\neg B$ (3

1. (A3) $(\neg\neg\neg B \to \neg B) \to ((\neg\neg\neg B \to B) \to \neg\neg B)$

2. $\neg\neg\neg B \to \neg B$ (a)

3. $(\neg\neg\neg B \to B) \to \neg\neg B$ 1.2. MP

4. $B \to (\neg\neg\neg B \to B)$ (A1)

5. $B \to \neg\neg B$ T.2 3.4.

(c) $\vdash \neg A \to (A \to B)$ (4

Докажем: $\neg A, A \vdash B$

1. $\neg A$ гипотеза
2. A гипотеза
3. (A1) $A \to (\neg B \to A)$
4. (A1) $\neg A \to (\neg B \to \neg A)$
5. 2.3. MP $\neg B \to A$
6. 1.4. MP $\neg B \to \neg A$
7. (A3) $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$
8. 6.7. MP $(\neg B \to A) \to B$
9. 5.8. MP B

Эрбран $\neg A, A \vdash B \Rightarrow \neg A \vdash A \to B$

Эрбран $\neg A \vdash A \to B \Rightarrow \vdash \neg A \to (A \to B)$

(d) $\vdash (\neg B \to \neg A) \to (A \to B)$ 15

1. $\neg B \to \neg A$ гипотеза
2. A гипотеза
3. (A3) $(\neg B \to \neg A) \to ((\neg B \to A) \to B)$
4. (A1) $A \to (\neg B \to A)$
5. 1.3. MP $(\neg B \to A) \to B$
6. 4.5 T.2 $A \to B$
7. 2.6. MP B

Эрбран $\neg B \to \neg A, A \vdash B \Rightarrow \neg B \to \neg A \vdash A \to B$

Эрбран $\neg B \to \neg A \vdash A \to B \Rightarrow \vdash (\neg B \to \neg A) \to (A \to B)$

(e) $\vdash (A \to B) \to (\neg B \to \neg A)$

1. $A \to B$ хипотеза
2. $\neg\neg A \to A$ (a)
3. 1.2. Т.2 $\neg\neg A \to B$
4. $B \to \neg\neg B$ (в)
5. 3.4. Т.2 $\neg\neg A \to \neg\neg B$
6. $(\neg\neg A \to \neg\neg B) \to (\neg B \to \neg A)$ (d)
7. 5.6. MP $\neg B \to \neg A$

Теорема $A \to B \vdash \neg B \to \neg A \Rightarrow \vdash (A \to B) \to (\neg B \to \neg A)$

(5) $\vdash A \to (\neg B \to \neg(A \to B))$

$A, A \to B \vdash B$

и по Эрбрану $A \vdash (A \to B) \to B$

и по Эрбрану $\vdash A \to ((A \to B) \to B)$

(e) $((A \to B) \to B) \to (\neg B \to \neg(A \to B))$

T.2. $\vdash A \to (\neg B \to \neg(A \to B))$

(g) $\vdash (A \to B) \to ((\neg A \to B) \to B)$ (8

1. $A \to B$ хипотеза
2. $\neg A \to B$ хипотеза
3. $(A \to B) \to (\neg B \to \neg A)$ (e)
4. 1.3. MP $\neg B \to \neg A$
5. $(\neg A \to B) \to (\neg B \to \neg\neg A)$ (e)
6. 2.5. MP $\neg B \to \neg\neg A$
7. (A3) $(\neg B \to \neg\neg A) \to ((\neg B \to \neg A) \to B)$
8. 6.7. MP $(\neg B \to \neg A) \to B$
9. 4.8. MP B

Ердван:
$A \to B, \neg A \to B \vdash B \Rightarrow A \to B \vdash (\neg A \to B) \to B$

Ердван:
$A \to B \vdash (\neg A \to B) \to B \Rightarrow \vdash (A \to B) \to ((\neg A \to B) \to B)$

Лемма.

$\mathcal{A}$ — формула

$B_1, \dots, B_k$ — пропозициональные буквы, входящие в $\mathcal{A}$

Пусть задано распределение истинностных значений для $B_1, \dots, B_k$

$$B_i' = \begin{cases} B_i & \text{при } B_i = 1 \\ \neg B_i & \text{при } B_i = 0 \end{cases}$$

$$\mathcal{A}' = \begin{cases} \mathcal{A} & \text{если } \mathcal{A} \text{ принало } 1 \\ \neg \mathcal{A} & \text{если } \mathcal{A} \text{ принало } 0 \end{cases}$$

$$\Rightarrow \quad B_1', \dots, B_k' \vdash \mathcal{A}'$$

Пример $\quad \mathcal{A} = \neg(\neg A_2 \to A_3)$

A_2	A_3	$\neg(\neg A_2 \to A_3)$
1	1	0
0	1	0
1	0	0
0	0	1

3-я строка $\quad A_2, \neg A_3 \vdash \neg\neg(\neg A_2 \to A_3)$

Док-во леммы.

индукция по числу примитивных связок

БАЗА. $n=0$ $\mathcal{A} = B_1$ $B_1 \vdash B_1$, $\neg B_1 \vdash \neg B_1$

предположение. $j < n$

Случай 1. $\mathcal{A}$ имеет вид $\neg \mathcal{B}$.

1а. $\mathcal{B}$ принимает 1

$\mathcal{A}$ принимает 0

$\mathcal{B}' = \mathcal{B}$ (*) $\mathcal{A}' = \neg \mathcal{A}$

$B_1', \dots, B_k' \vdash \mathcal{B}$ (предп. и (*))

[Но лемма осн. (в) $\vdash B \to \neg\neg B$] [MP] $B_1', \dots, B_k' \vdash \underbrace{\neg\neg \mathcal{B}}_{\mathcal{A}'}$

1в. $\mathcal{B}$ принимает 0

$\mathcal{B}' = \neg \mathcal{B}$

$\mathcal{A}' = \mathcal{A}$

$B_1', \dots, B_k' \vdash \underbrace{\neg \mathcal{B}}_{\mathcal{A}'}$ (предп.)

Случай 2.

$\mathcal{C} = \mathcal{A} \to \mathcal{B}$

$B_1', \ldots, B_k' \vdash \mathcal{A}'$ $\quad$ $B_1', \ldots, B_k' \vdash \mathcal{B}'$

2a $\mathcal{A}$ принимает 0

$\mathcal{C}$ принимает 1

$\mathcal{A}' = \neg \mathcal{A}$ $\quad$ $\mathcal{C}' = \mathcal{C}$

$B_1', \ldots, B_k' \vdash \neg \mathcal{A}$ [Лемма (осн.)(c) $\vdash \neg A \to (A \to B)$]

[MP] $B_1', \ldots, B_k' \vdash \mathcal{A} \to \mathcal{B}$ $\quad$ $\mathcal{A} \to \mathcal{B} = \mathcal{C}'$

2b $\mathcal{B}$ принимает 1

$\mathcal{C}$ принимает 1

$\mathcal{B}' = \mathcal{B}$ $\quad$ $\mathcal{C}' = \mathcal{C}$

$B_1', \ldots, B_k' \vdash \mathcal{B}$ [(A1) $A \to (B \to A)$] [MP]

$B_1', \ldots, B_k' \vdash \mathcal{A} \to \mathcal{B}$ $\quad$ $\mathcal{A} \to \mathcal{B} = \mathcal{C}'$

2c $\mathcal{A}$ принимает 1, $\mathcal{B}$ принимает 0

$\mathcal{C}$ принимает 0

$\mathcal{C}'$ есть $\neg \mathcal{C}$

$\mathcal{A}' = \mathcal{A}$ $\quad$ $\mathcal{B}' = \neg \mathcal{B}$

$B_1', \ldots, B_k' \vdash \mathcal{A}$ $\quad$ $B_1', \ldots, B_k' \vdash \neg \mathcal{B}$

[Лемма (осн.)(f) $\vdash A \to (\neg B \to \neg (A \to B))$]

$\mathcal{A} \to (\neg \mathcal{B} \to \neg (\mathcal{A} \to \mathcal{B}))$ (MP)(MP)

$B_1', \ldots, B_k' \vdash \underbrace{\neg (\mathcal{A} \to \mathcal{B})}_{\mathcal{C}'}$

Теорема Гёделя о полноте.

Тавтология $\Rightarrow$ теорема.

Доказательство (Кальмар).

$\mathcal{A}$ – тавтология

$B_1, \ldots, B_k$

$B_1', \ldots, B_k' \vdash \mathcal{A}$

$B_1', \ldots, B_{k-1}', B_k \vdash \mathcal{A}$

$B_1', \ldots, B_{k-1}', \neg B_k \vdash \mathcal{A}$

Эрбран

$B_1', \ldots, B_{k-1}' \vdash B_k \to \mathcal{A}$

$B_1', \ldots, B_{k-1}' \vdash (\neg B_k) \to \mathcal{A}$

Лемма (осн.) (g)

$[\ \vdash (A \to B) \to ((\neg A \to B) \to B)\ ]$ (MP) (MP)

$B_1', \ldots, B_{k-1}' \vdash \mathcal{A}$

ит-д. с B_{k-1}'

$\vdash \mathcal{A}$

1. $A \to (B \to A)$
2. $(A \to (B \to C)) \to ((A \to B) \to (A \to C))$
3. $(A \& B) \to A$
4. $(A \& B) \to B$
5. $A \to (B \to (A \& B))$
6. $A \to (A \vee B)$
7. $B \to (A \vee B)$
8. $(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$
9. $(A \to B) \to ((A \to \neg B) \to \neg A)$

10. $\neg\neg A \to A$ 10.и $\neg A \to (A \to B)$

MP

$A, A \to B \vdash B$

Интуиционистская логика

$\perp_I$

Система аксиом Клини

$\to, \&, \vee, \neg$ примитивные связки

Теорема дедукции верна

$\neg$, $\rightarrow$

MP

$A, A \rightarrow B \vdash B$

$[((A \rightarrow B) \rightarrow (\neg C \rightarrow \neg D)) \rightarrow E] \rightarrow [(E \rightarrow A) \rightarrow (D \rightarrow A)]$

Система Мередита

P_{n+1} 0 — истина

$$\neg A = \begin{cases} 0, & A = n \\ n, & \text{иначе} \end{cases}$$

$A \,\&\, B = \max(A, B)$

$A \vee B = \min(A, B)$

$$A \to B = \begin{cases} 0, & A \geq B \\ B, & \text{иначе} \end{cases}$$

Все теоремы есть выделенные формулы

$A \vee (\neg A)$

не теорема

$n = 3$

$(\neg\neg A) \to A$

не теорема

$n = 3$

L_I не подходящая для всех конечнозначных логик.

Яськовский P счетнозначная

Теория защиты информации

Вспомогательные факты из теории целых чисел

Множество целых чисел $\boldsymbol{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$

Множество натуральных чисел $\boldsymbol{N} = \{1, 2, \ldots\}$

Делимость целых чисел:

m, n ($n \neq 0$) n делит нацело m (обозначение $n \mid m$) $\Leftrightarrow$ существует k: $m = nk$.

Замечание. $n \mid m$, $n \mid l \Rightarrow n \mid m \pm l$.

Д. $m = nk_1$, $l = nk_2$ ($n \neq 0$); $m \pm l = n(k_1 \pm k_2)$

Теорема о делении целых чисел с остатком.

Пусть $a \in \boldsymbol{Z}$, $b \in \boldsymbol{N}$. Тогда можно подобрать, причем единственным способом, целые числа q и r: $a = bq + r$, $0 \leq r < b$.

Задача 1. Доказать, что при любом целом n: $6 \mid n^3 - n$.

Задача 2. Число a при делении на b дает остаток r. Какой остаток при делении на b дает число $(-a)$.

Задача 3. Доказать, что $6 \mid n^3 + 3n^2 + 2n$.

Обозначения:

(a, b) – НОД a и b.

a сравнимо с b по модулю m ($m \geq 2$) [$a = b(\mathrm{mod}\ m)$]: a и b дают одинаковые остатки при делении на m.

Теорема 1. $m \geq 2$. $a = b(\mathrm{mod}\ m) \Leftrightarrow m \mid a - b$.

Доказательство. Пусть $a = b(\mathrm{mod}\ m)$:

$$a = mq + r;$$

$$b = ms + r;$$

$$a - b = m(q - s);$$

Обратно, пусть $m \mid a - b$.

$$a - b = mq \qquad (1)$$

Поделим b на m с остатком:

$$b = ms + r; \quad 0 \leq r < m. \qquad (2)$$

Сложим (1) и (2):

$$a = mq + ms + r;$$

$$a = m(q + s) + r; \quad 0 \le r < m$$

Итак, $a = b \pmod m$.

Теорема 2.

Пусть $a = b \pmod m$, $c = d \pmod m \Rightarrow$

$$a + c = b + d \pmod m$$

$$a - c = b - d \pmod m$$

$$ac = bd \pmod m$$

$$a^n = b^n \pmod m, n \ge 1.$$

Доказательство. По теореме 1: $a - b = km$, $c - d = lm$.

$$(a + c) - (b + d) = a - b + c - d = (k + l)m.$$

И опять используем теорему 1:

$$(a - c) - (b - d) = a - b - (c - d) = (k - l)m;$$

$$ac - bd = (ac - ad) + (ad - bd) = a(c - d) + d(a - b) = alm + dkm = (al + dk)m;$$

Воспользовавшись тем, что сравнения можно попарно перемножать, из сравнения $a = b \pmod m$ получим $a^n = b^n \pmod m$.

Задача. Делится ли число $222^{555} + 555^{222}$ на 7.

Решение. Найдем остаток от деления 222^{555} на 7. $222 = 7 \ 31 + 5$

Посмотрим, какие остатки дают степени 5 при делении на 7:

$$5^0 = 1 \pmod 7;$$

$$5^1 = 5 \pmod 7;$$

$$5^2 = 4 \pmod 7;$$

$$5^3 = 6 \pmod 7;$$

$$5^4 = 2 \pmod 7;$$

$$5^5 = 3 \pmod 7;$$

$$5^6 = 1 \pmod 7;$$

Далее остатки будут повторяться.

n	0	1	2	3	4	5	6	7	8	9
r	1	5	4	6	2	3	1	5	4	6

$$555 = 6\times92 + 3$$

Значит, $222^{555} = 6(\text{mod } 7)$;

Аналогично, $555^{222} = 1(\text{mod } 7)$;

Итак, $7 \mid 222^{555} + 555^{222}$.

Теорема 3.

Пусть $ax_1 = ax_2(\text{mod } m)$, $(a, m) = 1 \Rightarrow x_1 = x_2(\text{mod } m)$.

Доказательство.

$ax_1 - ax_2 = mq$; $(a, m) = 1$, значит $a \mid q$; $x_1 - x_2 = mq_1$; $x_1 = x_2(\text{mod } m)$.

Теорема 4.

$(a, m) = 1$, $(x, m) = 1$, $\Rightarrow (ax, m) = 1$. И если $ax = mq + r$, то $(r, m) = 1$.

Доказательство. Первая часть очевидна.

Пусть $ax = mq + r$. Если $p \mid m$ и $p \mid r$, то $p \mid ax$ и $p = 1$.

Докажем теперь основную для криптографических следствий теорему.

Теорема 5 (Эйлер).

Пусть $m \geq 2$. Пусть функция Эйлера $\varphi(m)$ – число чисел в ряду $1, \ldots, m$ взаимно-простых с m.

Пусть $(a, m) = 1$. Тогда $a^{\varphi(m)} = 1(\text{mod } m)$.

Доказательство.

Пусть $r_1, \ldots, r_{\varphi(m)}$ – числа в ряду $1, \ldots, m$, взаимно-простые с m.

Пусть

$$ar_1 = \rho_1(\text{mod } m);$$

$$\ldots$$

$$\mathbf{a\, r_{\varphi(m)} = \rho_{\varphi(m)} (mod\ m),}$$

и пусть $0 \leq \rho_i < m$.

$\rho_1, \ldots, \rho_{\varphi(m)}$ есть те же самые числа $r_1, \ldots, r_{\varphi(m)}$, но в другом порядке.

Имеем:

$$a^{\varphi(m)}\ r_1 \dots r_{\varphi(m)} = r_1 \dots r_{\varphi(m)} \pmod m;$$

$$a^{\varphi(m)}\ r_2 \dots r_{\varphi(m)} = r_2 \dots r_{\varphi(m)} \pmod m;$$

и т.д.

$$a^{\varphi(m)} = 1 \pmod m$$

Задача. Пусть $m = pq$, где p и q – простые числа.

Доказать, что $\varphi(m) = (p-1)(q-1)$.

Криптосистема RSA (Райвест, Шамир, Адельман)

Пусть p и q – простые числа (более, чем 50-значные).

Пусть $m = pq$.

Пусть число s такое, что

$$\begin{cases}(s, p-1) = 1\\(s, q-1) = 1\end{cases}$$

Найдем число t такое, что $st = 1 \pmod{(p-1)(q-1)}$.

Воспользуемся теоремой Эйлера.

(m, s) – сообщаем всем;
(p, q, t) – держим в тайне

Шифрование сообщения x такого, что $(x, m) = 1$.

$E(x) = x^s \pmod m$, $y = E(x)$.

Дешифровка

$D(y) = y^t \pmod m$,

$D(y) = y^t = x^{st} = x^{(p-1)(q-1)l+1} = x^{\varphi(m)l}\, x = x \pmod m$,

зависимости от реализации). Другим часто используемым значением является $e = 2^{16}+1=65537$. Это число имеет одну единицу в двоичной записи и требует при использовании описанного алгоритма 16 возведений в квадрат и одно модульное умножение. Такая экспонента имеет преимущество по сравнению с $e = 3$, поскольку в этом случае атака, описанная ранее, не осуществиться, т.к. очень мала вероятность, что одно и тоже сообщение будет послано $2^{16}+1$ абонентам.

Далее некоторые задачи на целые числа.

Контрольная работа

1. Найти остаток отделения числа 1231234155 на 8.
2. Доказать, что трехзначное число, записанное тремя одинаковыми цифрами, делится на 37.
3. Доказать, что число $37^5 + 63^5$ делится на 100.
4. Написать общий вид чисел, кратных 6 и дающих при делении на 7 остаток 5.
5. Целое число n при делении на 7 дает остаток 3. Какой остаток дает число $(-n)$ при делении на 7? Какой остаток дает число $n^2 - 5n$ при делении на 7?
6. Существует ли такое целое число, которое при делении на 20 дает остаток 13, а при делении на 35 дает остаток 4.
7. Докажите, что число $n^2 + 4n + 8$ не делится на 6 ни при каких натуральных n.
8. Доказать, что число $7^{14} + 11^{11}$ составное.
9. Решить уравнения в целых числах:
   а) $xy^2 = 5x + y^2$, б) $x^2 = 5y + 3$, в) $x(y^2 + 1) = 48$, г) $3x+2y=7$.
10. Доказать, что среди чисел, записанных с помощью только цифры 1, есть число, делящееся на 2001.
11. Доказать, что при любом натуральном n число вида $5n + 3$ не является квадратом целого числа.

12. Число оканчивается цифрой 3. Если эту цифру переставить на первое место, то получится число, вдвое большее первоначального. Найти наименьшее из таких чисел.

13. Сколько целых чисел n удовлетворяют условию

$$(n^2 - 2)(n^2 - 20) < 0 ?$$

14. Найти все пары целых чисел x и y, удовлетворяющих системе:

$$\begin{cases} x > y \\ 2x + y < 32 \\ x + 2y > 28 \end{cases}$$

15. Доказать, что при любом натуральном n число $10^n + 18n - 1$ делится на 27.

16. Доказать, что число $n^2 + 3n + 11$ не делится на 25 ни при каких натуральных n.

17. Доказать, что найдутся 1000 подряд идущих натуральных чисел среди которых ровно 3 простых.

Домашняя контрольная работа

1. Найти остаток отделения числа 78346791 на 8.
2. Доказать, что числа вида $x00x$ делятся на 13.
3. Доказать, что число $143^5 - 43^5$ делится на 100.
4. Написать общий вид чисел, кратных 6 и дающих при делении на 5 остаток 2.
5. Целое число n при делении на 6 дает остаток 5. Какой остаток дает число $n^2 + 4n$ при делении на 5?
6. Существует ли такое целое число, которое при делении на 36 дает остаток 23, а при делении на 12 дает остаток 7.
7. Докажите, что число $n^2 + 5n + 7$ не делится на 9 ни при каких натуральных n.
8. Доказать, что число $13^{14} + 7^{16}$ составное.
9. Решить уравнения в целых числах:

а) $(x + 1)(y - 2) = 2$, б) $x^2 = 7y + 5$, в) $x^2(y + 1) = 48$.

10. Доказать, что среди чисел, записанных с помощью только цифры 5, есть число, делящееся на 2003.
11. Доказать, что при любом натуральном n число вида $7n + 5$ не является квадратом целого числа.
12. Доказать, что число 919191919191 составное.
13. Сколько целых чисел n удовлетворяют условию
$(n^2 - 1)(n^2 - 11)(n^2 - 101)(n^2 - 1001) < 0$?
14. Найти все пары целых чисел x и y, удовлетворяющих системе:

$$\begin{cases} 20x < y \\ 23(x-1) \geq y \\ 21x + y = 500 \end{cases}$$

G — группа

$G, \circ, e$

1. $a \circ (b \circ c) = (a \circ b) \circ c$
2. $a \circ e = e \circ a = a$

для любого a

3. Для любого a существует a^{-1}:

$a \circ a^{-1} = a^{-1} \circ a = e$

Только 1. — полугруппа

Только 1. и 2. — моноид

Циклические группы

S_3 $\begin{pmatrix} 1 & 2 & 3 \\ i_1 & i_2 & i_3 \end{pmatrix}$

её подгруппа

$$\mathbb{Z}_3 = \left\{ \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}}_{a}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}}_{a^2}, \underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}}_{a^3 = e} \right\}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

В S_4 $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ и т.д.

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

S_3 — не абелева

S_2 — циклическая

$\mathbb{Z}_{15}^{*} = \{1, 2, 4, 7, 8, 11, 13, 14\}$

×	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Таблица КЭЛИ группы

$\varphi(15) = 8.$

$a^8 \equiv 1 \pmod{15}.$

⇓ d.s.

$a^4 \equiv 1 \pmod{15}$

$\mathbb{Z}_m^*$ циклическая в случаях:

$m = 2, 4, p^\alpha, 2p^\alpha$ $\quad p \neq 2$ p-простое

$H < G$

$gH = \{ gh : h \in H \}$

$aH = bH \iff a^{-1}b \in H$

Д. $aH = bH \Rightarrow ah_1 = bh_2$

$\Rightarrow a^{-1}b = h_1 h_2^{-1} \in H$

$a^{-1}b = h \Rightarrow b = ah$

$bH = a\underbrace{hH}_{h\,h^{-1}h'} = aH$ ∎

$a \sim b \iff a^{-1}b \in H$

1. $a \sim a \qquad a^{-1}a = e \in H$
2. $a \sim b \Rightarrow b \sim a$

$a^{-1}b = h \in H$

то и $(a^{-1}b)^{-1} = b^{-1}a$ тоже из H

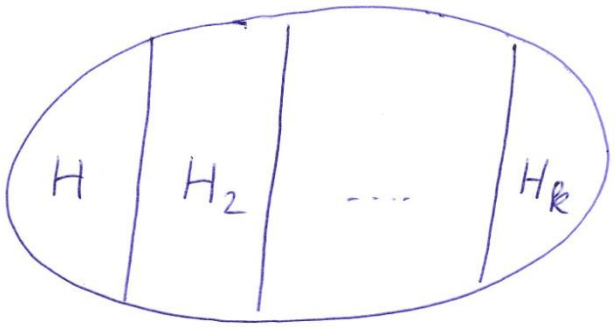
(H – подгруппа)

3. $a \sim b, b \sim c \Rightarrow a \sim c$

$a^{-1}b, b^{-1}c \in H$

$(a^{-1}b)(b^{-1}c) \in H$

$\| \; a^{-1}c$



$H \longrightarrow H_i = gH$

$h \longrightarrow gh$ биекция

$gh_1 = gh_2 \Rightarrow h_1 = h_2$

$|G| = |H| \cdot k$

Теорема Лагранжа