Занятие 9

Напомним, что множество $f \subseteq A \times B$ называется — относительно некоторых *фиксированных* множеств A и B:

функциональным, если для всех $a \in A$ и $b, b' \in B$ из $(a, b) \in f$ и $(a, b') \in f$ следует $b = b'$;

тотальным, если для каждого $a \in A$ найдется $b \in B$, т. ч. $(a, b) \in f$;

инъективным, если для всех $a, a' \in A$ и $b \in B$ из $(a, b) \in f$ и $(a', b) \in f$ следует $a = a'$;

сюръективным, если для каждого $b \in B$ найдется $a \in A$, т. ч. $(a, b) \in f$.

Если множество f функционально для данных A и B, оно называется *функцией из A в B*. Функция f из A в B называется *всюду определенной* или, *тотальной*, если множество f тотально для A и B. Тогда пишут $f\colon A \to B$. Также, всюду определенную функцию f из A в B мы будем называть *отображением из A в B*.

Функция f из A в B называется *инъективной (сюръективной) функцией*, если множество f инъективно (сюръективно) для данных A и B. Инъективное (сюръективное) отображение $f\colon A \to B$ называется *инъекцией (сюръекцией) из A в B*. Отображение $f\colon A \to B$, являющееся вместе инъекцией и сюръекцией из A в B, называется *биекцией из A в B*.

Пусть f есть функция из A в B. По определению функции, для каждого $a \in A$ существует не более одного элемента $b \in B$, т. ч. $(a, b) \in f$. Если таковой b найдется, говорят, что функция f *определена* на элементе a, и обозначают этот единственный элемент b, называемый *значением* функции f на элементе a, символом $f(a)$. Заметим, что если f не определена на a, выражение $f(a)$ не обозначает никакого элемента множества B; как иногда говорят, это выражение «не имеет смысла».

Областью определения функции f из A в B называется множество

$$\operatorname{dom} f = \{a \in A \mid \text{существует } b \in B, \text{ т. ч. } (a, b) \in f\}.$$

Очевидно, функция f из A в B будет всюду определенной тогда и только тогда, когда $\operatorname{dom} f = A$. *Образом множества $X \subseteq A$ под действием функции f* из A в B называется множество

$$f(X) = \{b \in B \mid \text{существует } a \in X, \text{ т. ч. } (a, b) \in f\}.$$

Несколько менее аккуратно можно написать:

$$f(X) = \{f(a) \mid a \in X\}.$$

Обратите внимание, что символ $f()$ употребляется нами в разных, хотя и связанных, смыслах. *(Полным) прообразом множества* $Y \subseteq B$ *под действием функции* $f\colon A \to B$ называется множество

$$f^{-1}(Y) = \{a \in A \mid \text{существует } b \in Y, \text{ т. ч. } (a, b) \in f\}.$$

Заметим, что $f^{-1}(B) = \operatorname{dom} f$.

Задача 9.1. Функция g из множества положительных целых чисел в множество положительных целых чисел сопоставляет числу x наибольший простой делитель x.

a) Какова область определения g?

b) Верно ли, что если X — конечное, то и $g^{-1}(X)$ конечное?

Решение. **a)** У каждого положительного целого число лишь конечное множество простых делителей, причем это множество пусто только у единицы. Значит, всякое целое число, большее единицы, имеет наибольший простой делитель. Таким образом, $\operatorname{dom} g = \{n \in \mathbb{N} \mid n > 1\}$.

b) Неверно. Рассмотрим бесконечное множество $Y = \{2^m \mid m \in \mathbb{N}\} = \{2, 2^2, 2^3, \ldots\}$. Для каждого из $n \in Y$ имеем $g(n) = 2$, а значит, $Y \subseteq g^{-1}(\{2\})$, хотя множество $X = \{2\}$ конечно. Легко также заметить, что $Y = g^{-1}(X)$, поскольку если 2 наибольший простой делитель числа, то число это не имеет иных простых делителей и, следовательно, является натуральной степенью двойки. □

Напомним, что символом $\cup_{i \in I} A_i$ обозначается объединение всех множеств A_i из семейства (множества) $\{A_i \mid i \in I\}$, как говорят, «индексированного множеством I». Точнее,

$$\cup_{i \in I} A_i = \cup\{A_i \mid i \in I\} = \{x \mid \text{существует } i \in I, \text{ т. ч. } x \in A_i\}.$$

(Чтобы быть еще более аккуратными, мы должны рассматривать A_i как значение некоторой тотальной функции $\mathcal{F}\colon I \to U$ на элементе $i \in I$, где U есть некоторое множество множеств.[1] Тогда получится, что $\cup_{i \in I} A_i = \cup \mathcal{F}(I)$.) Со столь абстрактными объектами лучше работать с помощью формальных аксиом; существование объединения произвольного множества множеств тогда приходится постулировать.

Аналогично, для $I \neq \varnothing$, можно определить множество

$$\cap_{i \in I} A_i = \cap\{A_i \mid i \in I\} = \{x \mid \text{для всех } i \in I \text{ верно } x \in A_i\}.$$

В чем трудность с $I = \varnothing$? По законам логики, в этом случае оказывается, что множеству

$$\cap_{i \in \varnothing} A_i = \{x \mid \text{для всех } i, \text{ если } i \in \varnothing, \text{ то } x \in A_i\}$$

[1] В стандартной формальной теории множеств, так называемой ZFC, единственным рассматриваемыми объекатми являются множества, так что уточнение «множество *множеств*» излишне. Например, натуральные числа можно *определить* как множества: $0 = \varnothing$, $1 = \{\varnothing\}$, $2 = \{\varnothing, \{\varnothing\}\}$, $\ldots$, $n + 1 = n \cup \{n\}$, $\ldots$

принадлежит «все что угодно» — во всяком случае, каждое множество. Предположение о существовании таких «больших» множеств приводит к противоречию.[2] Напротив, когда $I \neq \varnothing$, существует какое-то A_{i_0} и оказывается, что $\cap_{i\in I} A_i \subseteq A_{i_0}$, т. е. множество $\cap_{i\in I} A_i$ включено в какое-то существующее множество и не является «большим».

Задача 9.2. Сравните множества:

a) $(\cup_{i\in I} A_i) \times (\cup_{j\in J} B_j)$ и $\cup_{i\in I, j\in J}(A_i \times B_j)$;

b) $(\cap_{i\in I} A_i) \times (\cap_{j\in J} B_j)$ и $\cap_{i\in I, j\in J}(A_i \times B_j)$.

Решение. Прежде всего заметим, что символ $\cup_{i\in I, j\in J}$ мы, чтобы оставаться в области действия уже данного определения, можем понимать как $\cup_{(i,j)\in I\times J}$. Аналогично для $\cap_{i\in I, j\in J}$.

a) Данные множества равны. Установим включение слева направо. Пусть $x \in (\cup_{i\in I} A_i) \times (\cup_{j\in J} B_j)$. Это означает, как мы знаем из Лекций, что найдутся единственные такие $a \in \cup_{i\in I} A_i$ и $b \in \cup_{j\in J} B_j$, что $(a, b) = x$. Далее, существует $i_0 \in I$, для которого $a \in A_{i_0}$, и существует $j_0 \in J$, для которого $b \in B_{j_0}$. Но тогда $(a, b) \in A_{i_0} \times B_{j_0}$, причем $(i_0, j_0) \in I \times J$. Значит, $x = (a, b) \in \cup_{(i,j)\in I\times J}(A_i \times B_j)$.

Установим обратное включение. Пусть $x \in \cup_{(i,j)\in I\times J}(A_i \times B_j)$. Тогда найдется пара $(i_0, j_0) \in I \times J$, т. е. найдутся $i_0 \in I$ и $j_0 \in J$, со свойством $x \in A_{i_0} \times A_{j_0}$. Значит, $x = (a, b)$ для некоторых $a \in A_{i_0}$ и $b \in B_{j_0}$. Отсюда $a \in \cup_{i\in I} A_i$ и $b \in \cup_{j\in J} B_j$ и, следовательно, $x = (a, b) \in (\cup_{i\in I} A_i) \times (\cup_{j\in J} B_j)$.

b) Данные множества равны. Напомним, что определены они лишь при $I, J \neq \varnothing$.

Допустим $x \in (\cap_{i\in I} A_i) \times (\cap_{j\in J} B_j)$. Тогда $x = (a, b)$, причем $a \in A_i$ для всех $i \in I$ и $b \in B_j$ для всех $j \in J$. Значит, для всех $i \in I$ и всех $j \in J$ верно $(a, b) \in A_i \times B_j$. Далее, для всех $(i, j) \in I \times J$ верно $(a, b) \in A_i \times B_j$, откуда $x = (a, b) \in \cap_{(i,j)\in I\times J}(A_i \times B_j)$.

Обратно, пусть $x \in \cap_{(i,j)\in I\times J}(A_i \times B_j)$. Тогда для всех $(i, j) \in I \times J$, т. е. для всех $i \in I$ и для всех $j \in J$, верно $x \in A_i \times A_j$. Поскольку $I, J \neq \varnothing$, существуют $i_0 \in I$ и $j_0 \in J$, т. ч. $x \in A_{i_0} \times A_{j_0}$. Но тогда $x = (a, b)$ для некоторых a и b, причем для всех $i \in I$ верно $(a, b) \in A_i \times A_{j_0}$ и тем более $a \in A_i$.[3]

Аналогично получаем $b \in A_j$ для всех $j \in J$. Имеем $a \in \cap_{i\in I} A_i$ и $b \in \cap_{j\in J} B_j$ и, окончательно, $x = (a, b) \in (\cap_{i\in I} A_i) \times (\cap_{j\in J} B_j)$. □

Задача 9.3. Пусть f — функция из множества A в множество B, $X, Y \subseteq A$ и $U, V \subseteq B$. Верны ли для любых множеств f, A, B, X, Y, U, V следующие утверждения:

[2] Пусть множеству V принадлежат все множества. Разумно считать («аксиома выделения»), что существуют любые его подмножества, заданные некоторым условием. В частности, существует множество $V' = \{x \in V \mid x \notin x\}$. Раз V «большое», $V' \in V$. Если $V' \in V'$, то $V' \notin V'$. Противоречие. Значит, $V' \notin V'$. Но тогда $V' \in V'$. Противоречие.

[3] Для логически настроенного читателя особо отметим, что из $\forall i \in I\, \forall j \in J\, (a \in A_i)$ мы, вообще говоря, не можем заключить $\forall i \in I\, a \in A_i$ из-за возможности пустого J. В самом деле, приведенное утверждение логически эквивалентно $\forall i\, (i \in I \Rightarrow \forall j\, (j \in J \Rightarrow a \in A_i))$, что эквивалентно $\forall i\, (i \in I \Rightarrow (\exists j\, (j \in J) \Rightarrow a \in A_i))$. Таким образом, просто так убрать квантор по j, хотя утверждение $a \in A_i$ ничего про j не говорит, не удается.

c) $f(X \cup Y) = f(X) \cup f(Y)$;
d) из равенства $f(X) = f(Y)$ следует $X \cap Y \neq \varnothing$;
e) $f^{-1}(U \cap V) = f^{-1}(U) \cap f^{-1}(V)$;
f) из равенства $f^{-1}(U) = f^{-1}(V)$ следует $U = V$.

Решение. **a)** Утверждение верно. Установим включение слева направо. Пусть $b \in f(X \cup Y)$. Это значит, что найдется $a \in X \cup Y$, т. ч. $f(a) = b$. Имеем, однако, $a \in X$ или $a \in Y$. В первом случае $b \in f(X)$, а во втором — $b \in f(Y)$; очевидно, в обоих случаях $b \in f(X) \cup f(Y)$.

Проверим обратное включение. Если $b \in f(X) \cup f(Y)$, то $b \in f(X)$ или $f(Y)$. В первом случае найдется $a \in X \subseteq X \cup Y$, т. ч. $f(a) = b$. Имеем $b \in f(X \cup Y)$. Аналогично во втором случае.

b) Утверждение верно не для любых множеств. Рассмотрим двухэлементное множество $A = \{x, y\}$ и множество $B = \{1\}$. Положим

$$f = \{(x, 1), (y, 1)\}.$$

Ясно, что f есть функция из A в B. Положим также $X = \{x\}$ и $Y = \{y\}$. Имеем $f(X) = \{1\} = f(Y)$, хотя $X \cap Y = \varnothing$.

c) Утверждение верно. Установим включение слева направо. Пусть $a \in f^{-1}(U \cap V)$. Тогда найдется $b \in U \cap V$, т. ч. $(a, b) \in f$. Однако для этого b верно $b \in U$ и $b \in V$, так что $a \in f^{-1}(U)$ и $a \in f^{-1}(V)$, откуда $a \in f^{-1}(U) \cap f^{-1}(V)$.

Проверим обратное включение. Пусть $a \in f^{-1}(U) \cap f^{-1}(V)$, т. е. $a \in f^{-1}(U)$ и $a \in f^{-1}(V)$. Первое из этих условий означает, что найдется $b \in U$, для которого $(a, b) \in f$. Аналогично, найдется $b' \in V$ со свойством $(a, b') \in f$. В силу функциональности f, имеем $b = b'$, а значит, $b \in U \cap V$. Следовательно, $a \in f^{-1}(U \cap V)$.

d) Утверждение верно не для любых множеств. Рассмотрим множество $A = \{1\}$ и двухэлементное множество $B = \{x, y\}$. Положим

$$f = \{(1, x)\}.$$

Ясно, что f есть функция из A в B. Положим также $U = \{x\}$ и $V = \{x, y\}$. Имеем $f^{-1}(U) = \{1\} = f^{-1}(V)$, хотя $U \neq V$. □

Задача 9.4. Функция f определена на множестве X и принимает значения во множестве Y, при этом $B \subseteq Y$. Какой знак сравнения множеств можно поставить вместо ?, чтобы утверждение $f(f^{-1}(B))$? B стало верным?

Решение. Докажем, что можно поставить знак $\subseteq$. Действительно, допустим, $y \in f(f^{-1}(B))$. Это значит, что найдется $x \in f^{-1}(B)$, т. ч. $(x, y) \in f$. С другой стороны, из $x \in f^{-1}(B)$ следует существование $y' \in B$ со свойством $(x, y') \in f$. В силу функциональности f, $y = y'$ и, следовательно, $y \in B$.

Отметим, что знак $=$, вообще говоря, поставить нельзя. В самом деле, пусть $X = \{1\}$, $Y = \{a, b\}$, причем $a \neq b$, и $f = \{(1, a)\}$. Полагая $B = \{a, b\}$, имеем $f^{-1}(B) = \{1\}$, но $f(\{1\}) = \{a\} \neq B$. □

Задача 9.5. Постройте биекцию между конечными подмножествами множества положительных целых чисел и конечными строго возрастающими последовательностями положительных целых чисел.

Решение. Каждому конечному подмножеству, включая пустое, поставим в соответствие последовательность всех его элементов (быть может, пустую), упорядоченных по возрастанию. Ясно, что это всюду определенная функция: каждое подмножество можно упорядочить по возрастанию, причем единственным способом.

Проверим инъективность. Допустим, что подмножества A и B различны. Тогда существует число a, принадлежащее только одному из них. Пусть, без ограничения общности, это число принадлежит только a. Тогда оно стоит на каком-то месте в последовательности для A, но не встречается в последовательности для B. Следовательно, эти последовательности различны.

Проверим сюръективность. Для каждой последовательности можно рассмотреть множество чисел, которые в ней встречаются. Ясно, что этому множеству соответствует именно данная последовательность. □

Задача 9.6. Приведите пример сюръекции множества положительных целых чисел на себя, для которой прообраз любого одноэлементного множества бесконечен.

Решение. За основу конструкции можно взять функцию g из задачи 9.1. Ясно, что множество $g^{-1}(\{p\}) \supseteq \{p, p^2, \ldots, p^m, \ldots\}$ бесконечно для каждого *простого* p. Однако, функция g не сюръективна.

По счастью, нетрудно сделать ее таковой. Как известно читателю, существует бесконечно много различных простых чисел.[4] Пусть p_n означает n-ое по возрастанию простое число. Например, $p_1 = 2$ и $p_2 = 3$. Положим

$$h(x) \quad = \quad \begin{cases} 1, \text{ если } x = 1; \\ n, \text{ если } p_n \text{ есть наибольший простой делитель числа } x. \end{cases}$$

Нетрудно видеть, что h есть всюду определенная функция из множества натуральных чисел в себя. Действительно, если $x \neq 1$, у x есть единственный наибольший простой делитель q, причем существует единственное n, т. ч. $q = p_n$.

Также ясно, что $h^{-1}(\{n\}) \supseteq \{p_n, p_n^2, \ldots, p_n^m, \ldots\}$ для каждого натурального n (в частности, видно, что функция h сюръективна). □

Пусть натуральные числа $m_1, \ldots, m_k$ попарно взаимно просты и пусть $(a_1, \ldots, a_k)$ есть набор вычетов по модулям $m_1, \ldots, m_k$, т. е. $0 \leqslant a_i < m_i$ для всех i. Очевидно, различных таких наборов имеется ровно $M = m_1 \cdot \ldots \cdot m_k$. С другой стороны, вычетов по модулю M имеется тоже ровно M. Каждому из этих вычетов a поставим в соответствие набор $g(a) = (a_1, \ldots, a_k)$, где a_i есть остаток от деления a на m_i.

[4] Предположим противное: *все* простые числа суть $p_1, p_2, \ldots, p_k$. Рассмотрим $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. Ясно, что $N \equiv 1 \pmod{p_i}$ для всех p_i, т. е. $p_i \nmid N$. Также ясно, что $N > 1$. С другой стороны, из «основной теоремы арифметики» следует, что каждое натуральное число, отличное от единицы, кратно некоторому простому.

Мы утверждаем, что функция g инъективна, т. е. если $a_i = b_i$ для всех i, то и $a = b$. Действительно, мы получаем, что $a \equiv b \pmod{m_i}$, а значит, $m_i \,|\, (a - b)$ для всех i.

Лемма 1. *Если $a \,|\, bc$ и числа a и b взаимно просты, то $a \,|\, c$.*

Доказательство. Из НОД$(a, b) = 1$, в силу соотношения Безу, следует, что $1 = au + bv$ для некоторых целых u и v. Тогда $c = acu + bcv$. Но $a \,|\, bc$, а значит, $a \,|\, c$. □

Лемма 2. *Если $a \,|\, c$ и $b \,|\, c$, причем числа a и b взаимно просты, то $ab \,|\, c$.*

Доказательство. Имеем $c = ak$ для некоторого целого k. По предыдущей лемме, из $b \,|\, ak$ заключаем $b \,|\, k$, т. е. $k = bl$ для некоторого целого l. Следовательно, $c = ak = abl$, откуда $ab \,|\, c$. □

Лемма 3. *Если число a взаимно просто с b и взаимно просто с c, то числа a и bc взаимно просты.*

Доказательство. Соотношение Безу дает

$$\begin{aligned} au + bv &= 1 \\ au' + cv' &= 1 \end{aligned}$$

для некоторых целых u, v, u', v'. Перемножая эти равенства, получаем

$$a(auu' + ucv' + u'bv) + bcvv' = 1.$$

Значит, любой общий делитель чисел a и bc делит 1, т. е. эти числа взаимно просты. □

Приведенные леммы позволяют легко заключить, что $M \,|\, (a - b)$ (напомним, $M = m_1 \cdot \ldots \cdot m_k$). Тогда из $0 \leqslant a, b < M$ следует, что $a = b$, как и требовалось. Итак, g есть всюду определенная инъекция из множества вычетов по модулю M во множество наборов вычетов по модулям $m_1, \ldots, m_k$.

Лемма 4. *Пусть множества A и B конечны, причем $|A| = |B| = n$, и $f \colon A \to B$ есть инъекция. Тогда f есть сюръекция из A в B.*

Доказательство. Индукция по n. Если $n = 0$, то $A = B = \varnothing$ и $f = \varnothing$. Легко проверить, что множество $\varnothing$ есть биекция из $\varnothing$ в $\varnothing$. Пусть требуемое верно для всех множеств мощности n и пусть $|A| = |B| = n + 1$. Выберем произвольный $a \in A$ и положим $A' = A \setminus \{a\}$, $B' = B \setminus \{f(a)\}$ и $f' = f \setminus \{(a, f(a))\}$.

Ясно, что f' есть всюду определенная инъекция из A' в B': в самом деле, все элементы A' функция f отображает, в силу инъективности, в элементы B, отличные от $f(a)$, т. е. в элементы множества B'. Однако, $|A'| = |B'| = n$ и, по предположению индукции, f' есть сюръекция из A' в B'. Но тогда $f = f' \cup \{(a, f(a))\}$ есть сюръекция из $A = A' \cup \{a\}$ в $B = B' \cup \{f(a)\}$. □

По доказанной лемме, функция g является сюръекцией, т. е. для каждого набора вычетов $(a_1, \ldots, a_k)$ по модулям $m_1, \ldots, m_k$ найдется вычет a по модулю M, — и притом только один в силу инъективности — такой что a дает остаток a_i при делении на m_i для каждого i. Это утверждение можно несколько переформулировать:

Теорема 5 (китайская теорема об остатках)**.** *Пусть натуральные числа $m_1, \ldots, m_k$ попарно взаимно просты и пусть $M = m_1 \cdot \ldots \cdot m_k$. Тогда для любых целых $a_1, \ldots, a_k$ существует ровно одно число x_0, т. ч. $0 \leqslant x_0 < M$ и x_0 удовлетворяет системе:*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_k \pmod{m_k}. \end{cases} \tag{1}$$

Более того, данной системе удовлетворяют все числа вида $x_0 + kM$, где k целое, и только они.

Доказательство. Большая часть работы нами уже сделана. Прежде всего заметим, что любые a_i можно заменить на их остатки по модулям m_i, так что полученная система будет равносильна исходной. Далее, ясно, что число $x_0 + kM \equiv x_0 \equiv a_i \pmod{m_i}$ для всех i. Наконец, допустим, что некоторый x удовлетворяет системе. Тогда $m_i \,|(x - x_0)$ для всех i, откуда $M \,|(x - x_0)$, а значит, $x = x_0 + kM$. □

Задача 9.7. Решите систему сравнений

$$\begin{cases} x \equiv 3 \pmod{13} \\ x \equiv 4 \pmod{14} \\ x \equiv 5 \pmod{15}. \end{cases}$$

Решение. Числа $13, 14, 15$ попарно взаимно просты, так что применима китайская теорема об остатках. Можно догадаться, что подходит число $x = -10$. Значит, все решения системы суть, в точности, числа $-10 + 13 \cdot 14 \cdot 15k$ при всевозможных целых k. □

Укажем систематический способ нахождения частного решения системы (1). Именно, положим $M_i = \frac{M}{m_i}$ и обозначим M_i' любое такое число, что

$$M_i M_i' \equiv 1 \pmod{m_i}.$$

Очевидно, такое M_i' существует, поскольку M_i и m_i взаимно просты, причем мы умеем находить такое число с помощью алгоритма Евклида. Положим, наконец,

$$x' = a_1 M_1 M_1' + a_2 M_2 M_2' + \ldots + a_k M_k M_k'.$$

Поскольку $m_i \,|\, M_j$ для всех $j \neq i$, имеем

$$x' \equiv a_i M_i M_i' \equiv a_i \cdot 1 \equiv a_i \pmod{m_i},$$

т. е. число x' удовлетворяет системе (1). Чтобы найти x_0, достаточно рассмотреть остаток от деления x' на M.