ДЕЛИМОСТЬ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Определение 1.1. Множество $\mathbb{N}$ *натуральных чисел* определяется с использованием *аксиом Пеано*:

1. $1 \in \mathbb{N}$ (единица — натуральное число).
2. Для любого $a \in \mathbb{N}$ существует единственное последующее $a^+ \in \mathbb{N}$.
3. Для любого $a \in \mathbb{N}$ выполняется неравенство $a^+ \neq 1$ (единица — наименьшее натуральное число).
4. Если $a^+ = b^+$, то $a = b$ (каждое последующее число обладает единственным предыдущим).
5. Если некоторое подмножество $N \subseteq \mathbb{N}$ содержит единицу и для каждого натурального числа $a \in N$ выполняется $a^+ \in N$, то $N = \mathbb{N}$ (принцип индукции).

Таким образом,

$$\mathbb{N} = \{1, 2, 3, 4, \ldots\}.$$

На основании этих аксиом строится арифметика натуральных чисел, включающая следующие операции сложения и умножения. Каждой паре натуральных чисел a, b можно единственным образом сопоставить их *сумму* — натуральное число $a + b = (\ldots(a^+)^+\ldots)^+$ (b раз) так, чтобы выполнялись условия для любых натуральных чисел a, b, c:

1) $a + 1 = a^+$;
2) ассоциативность сложения: $(a + b) + c = a + (b + c)$;
3) коммутативность сложения: $a + b = b + a$;
4) если $a + b = a + c$, то $b = c$.

Упражнение. Доказать равенства 2–4, исходя из аксиом Пеано.

Каждой паре натуральных чисел a, b можно единственным образом сопоставить их *произведение* — натуральное число

$a \cdot b = (\ldots(a + a) + \ldots + a)$ (b раз) так, чтобы выполнялись условия для любых натуральных чисел a, b, c:

1) $a \cdot 1 = a$;

2) $a \cdot b^{+} = a \cdot b + a$;

3) ассоциативность умножения: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

4) коммутативность умножения: $a \cdot b = b \cdot a$;

5) дистрибутивность умножения относительно сложения: $a \cdot (b + c) = a \cdot b + a \cdot c$, $(a + b) \cdot c = a \cdot c + b \cdot c$;

6) если $a \cdot b = a \cdot c$, то $b = c$.

Упражнение. Доказать равенства 5, 6, исходя из аксиом Пеано и свойств сложения.

Из аксиом Пеано 2–4 следует, что множество натуральных чисел *линейно упорядочено*: для любых $a, b \in \mathbb{N}$ выполняется ровно одно из трех условий:

$$a > b,\ a < b,\ a = b.$$

Отношение «<» (как и отношение «>») транзитивно, то есть из неравенств $a < b$ и $b < c$ следует, что $a < c$. Если для $a, b \in \mathbb{N}$ выполняется одно из соотношений $a > b$ или $a = b$, то записывают $a \leq b$ или $b \geq a$.

Определение 1.2. Множество $\mathbb{Z}$ *целых чисел* определим как объединение множеств натуральных чисел, отрицательных натуральных чисел и нуля: $\mathbb{Z} = \mathbb{N} \cup (-\mathbb{N}) \cup \{0\}$, таким образом

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

На множестве $\mathbb{Z}$ целых чисел операции сложения и умножения задаются теми же правилами, что и для натуральных чисел.

1.1. Делимость в кольце целых чисел

Определение 1.3. Пусть над некоторым множеством Ω произвольной природы определены операции сложения «+» и умножения «·». Множество Ω называется *кольцом*, если выполняются следующие условия:

1) сложение коммутативно: $a + b = b + a$ для любых $a, b \in \Omega$;
2) сложение ассоциативно: $(a + b) + c = a + (b + c)$ для любых a, b, $c \in \Omega$;
3) существует *нулевой* элемент $0 \in \Omega$ такой, что $a + 0 = a$ для любого $a \in \Omega$;
4) для каждого элемента $a \in \Omega$ существует *противоположный* элемент $-a \in \Omega$ такой, что $(-a) + a = 0$;
5) умножение дистрибутивно относительно сложения:

$$a \cdot (b + c) = a \cdot b + a \cdot c,\ (a + b) \cdot c = a \cdot c + b \cdot c$$

для любых $a, b, c \in \Omega$.

Если в кольце Ω умножение коммутативно: $a \cdot b = b \cdot a$ для любых $a, b \in \Omega$, то кольцо называется *коммутативным*.

Если в кольце Ω умножение ассоциативно: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ для любых $a, b, c \in \Omega$, то кольцо называется *ассоциативным*.

Если в кольце Ω существует *единичный* элемент e такой, что $a \cdot e = e \cdot a = a$ для любого $a \in \Omega$, то кольцо называется *кольцом с единицей*.

Если в ассоциативном, коммутативном кольце Ω с единицей для каждого ненулевого элемента a существует *обратный* элемент $a^{-1} \in \Omega$ такой, что $a \cdot a^{-1} = a^{-1} \cdot a = e$, то кольцо называется *полем*.

Пример 1.1. Множество $\mathbb{Z}$ целых чисел является коммутативным, ассоциативным кольцом с единицей. Нулевым элементом является число 0, единичным элементом — число 1. Для каждого целого числа a противоположным элементом является число $-a$. □

Пример 1.2. Множество $2\mathbb{Z}$ четных чисел является коммутативным, ассоциативным кольцом без единицы. □

Пример 1.3. Множество квадратных матриц, элементами которых являются рациональные числа, с обычной операцией сложения матриц и операцией йорданова умножения: $A \cdot B = \frac{1}{2}(AB + BA)$, где в скобках — обычное умножение матриц, является неассоциативным, коммутативным кольцом с единицей. □

Пример 1.4. Множество подмножеств некоторого множества с операциями симметрической разности («сложение») и пересечения («умножение») является ассоциативным, коммутативным кольцом с единицей. □

Пример 1.5. Множество $\mathbb{Q}$ рациональных чисел и множество $\mathbb{R}$ вещественных чисел являются полями. □

Определение 1.4. Говорят, что целое число a *делится* (нацело) на целое число $b > 0$ (или что целое число $b > 0$ делит целое число a), если существует такое целое число c, что $a = bc$. Число a называют *кратным* числа b, число b — *делителем* числа a, число c — *частным* от деления a на b.

Пример 1.6. $38 = 19 \cdot 2$ (38 делится на 19, 19 делит 38), $-24 = (-6) \cdot 4$ (-24 делится на -6, -6 делит -24), $0 = 5 \cdot 0$ (0 делится на 5, 5 делит 0). □

Отношение делимости обладает следующими свойствами.

1. Нуль делится на любое целое число.
2. Если a_1 делится на b, a_2 делится на b, то $a_1 \pm a_2$ делится на b.

2′. Если $a_1 \pm a_2$ делится на b и a_1 делится на b, то a_2 делится на b.

3. Если a делится на b и x — произвольное целое число, то xa делится на b.
4. Любое целое число делится на 1.
5. Если a делится на b и b делится на c, то a делится на c.
6. Если 1 делится на a, то $a = \pm 1$.

Упражнение. Доказать свойства делимости.

Определение 1.5. Пусть числа a и b целые и $b \neq 0$. *Разделить a на b с остатком* — значит представить a в виде $a = qb + r$, где $q, r \in \mathbb{Z}$ и $0 \leq r < |b|$. Число q называется *неполным частным*, число r — остатком от деления a на b.

Пример 1.7. Для $b = 15$ имеем

$$45 = 3 \cdot 15 + 0,\ 0 \leq 0 < 15;$$

$$123 = 8 \cdot 15 + 3,\ 0 \leq 3 < 15;$$

$$-105 = (-7) \cdot 15 + 0,\ 0 \leq 0 < 15;$$

$$-169 = (-12) \cdot 15 + 11,\ 0 \leq 11 < 15.$$ □

Пример 1.8. Для $b = -11$ имеем

$$44 = (-4) \cdot (-11) + 0,\ 0 \leq 0 < 11;$$

$$119 = (-10) \cdot (-11) + 9,\ 0 \leq 9 < 11;$$

$$-253 = 23 \cdot (-11) + 0,\ 0 \leq 0 < 11;$$

$$-228 = 21 \cdot (-11) + 3,\ 0 \leq 3 < 11.$$ □

Теорема 1.1 (о делении с остатком). Для любых $a, b \in \mathbb{Z}$, $b \neq 0$, существует единственная пара таких чисел $q, r \in \mathbb{Z}$, что $a = qb + r;\ 0 \leq r < |b|$.