

basic properties of the integers

1

axiomatic definition on \mathbb{N} :

the smallest set M , together with a special element $zero$ and an injective mapping (the *successor* function) $s : M \rightarrow M$ such that $zero \notin s(M)$

this set M is unique “up to isomorphism” and looks like

$$M = \{zero, one, two, three, four, \dots\}$$

where

$$one = s(zero)$$

$$two = s(one) = s(s(zero))$$

$$three = s(two) = s(s(one)) = s(s(s(zero)))$$

etc

2

definition of the arithmetic operations by primitive recursion

- addition $add : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$$add(m, zero) := m$$

$$add(m, s(n)) := s(add(m, n))$$

- multiplication $mult : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$$mult(m, zero) := zero$$

$$mult(m, s(n)) := add(mult(m, n), m)$$

- exponentiation $exp : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$

$$exp(m, zero) := s(zero)$$

$$exp(m, s(n)) := mult(exp(m, n), m)$$

3

- order relation on \mathbb{N}

$$m \leq n := \exists a \in \mathbb{N} \text{ add}(m, a) = n$$

properties of \mathbb{N} like

- addition is associative, commutative, cancellative, has $zero$ as neutral element
- multiplication is associative, commutative, cancellative on \mathbb{N}_+ , has one as neutral element and $zero$ as absorbing element
- usual properties of exponentiation
- \leq is a well-ordering of \mathbb{N}

are independent of any concrete realization on \mathbb{N}

4

there are many different realizations of \mathbb{N} and its operations (“numbering systems”) — the most frequent ones are “positional numbering systems”, in particular systems with a fixed base (“radix”)

Theorem: let β be a positive integer > 1 (the base), $\Delta_\beta = \{0, 1, 2, \dots, \beta - 1\}$ the set of base- β -digits.

For each $k \in \mathbb{N}_+$ the mapping

$$\langle a_{k-1}, \dots, a_1, a_0 \rangle \mapsto \underbrace{a_0 + a_1\beta + \dots + a_{k-1}\beta^{k-1}}_{\langle a_{k-1}, \dots, a_0 \rangle_\beta} = \sum_{j=0}^{k-1} a_j \beta^j$$

is an order-preserving bijection between Δ_β^k and $\{0, 1, 2, \dots, \beta^k - 1\}$

5

Corollary: Each positive integer $a \in \mathbb{N}_+$ has a unique base- β -representation

$$a = \langle a_{k-1} \dots a_1 a_0 \rangle_\beta$$

where $a_{k-1} \neq 0$ ($\Leftrightarrow \beta^{k-1} \leq a < \beta^k$)

The base- β -representation of 0 is $\langle 0 \rangle$

This is a canonical representation for natural numbers

Often “leading zeros” are tolerable

6

representation of negative integers

– the signature of an integer is

$$\text{sgn}(a) := \begin{cases} 1 & \text{if } a > 0 \\ 0 & \text{if } a = 0 \\ -1 & \text{if } a < 0 \end{cases}$$

so that $a \in \mathbb{Z}$ can be uniquely represented in base- β by

$$\langle \text{sgn}(a), a_{k-1} \dots a_0 \rangle$$

where $|a| = \langle a_{k-1} \dots a_0 \rangle_\beta$.

– as an alternative, one may use positive and negative digits in a positional representation

7

the following “division property” is the most important property of the integers

Theorem: given integers a, b , where $b \geq 2$, there exist uniquely determined integers q, r such that

$$a = b \cdot q + r \quad \text{and} \quad 0 \leq r < b$$

q is the *quotient* and r is the *remainder* of the division of a by b

notation: $q = a \text{ div } b = \text{iquo}(a, b)$, $r = a \text{ mod } b = \text{irem}(a, b)$

obviously (for positive a):

$$a = \langle a_{k-1} \dots a_1 a_0 \rangle_b \Leftrightarrow q = \langle a_{k-1} \dots a_1 \rangle_b, r = a_0$$

8

divisibility and primes

- divisibility in a ring R

$$\text{for } a, b \in R : b|a \text{ ("}a \text{ divides } b\text{")} \Leftrightarrow \exists c \in R : b \cdot c = a$$

- divisibility in \mathbb{Z}

$$b|a \Leftrightarrow a \bmod b = 0$$

- primes

$$p \in \text{PRIM} \stackrel{\text{df}}{\Leftrightarrow} p \geq 2 \wedge (a|p \Rightarrow a = \pm 1 \vee a = \pm p)$$

- there are infinitely many primes (EUCLID)

$$\text{PRIM} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \dots\}$$

9

consequences of the division property of \mathbb{Z}

- \mathbb{Z} is a principal ideal domain:

- if H is any subgroup (an ideal) of the group (the ring) \mathbb{Z} , then there exists a $d \in \mathbb{N}$ such that

$$H = d \cdot \mathbb{Z} = \{d \cdot n ; n \in \mathbb{Z}\}$$

i.e., the sets $d \cdot \mathbb{Z}$ with $d \in \mathbb{N}$ are precisely the subgroups (ideals) of the additive group (ring) \mathbb{Z}

- the quotient rings $\mathbb{Z}_d := \mathbb{Z}/(d \cdot \mathbb{Z})$ for $n \in \mathbb{Z}$ are (up to isomorphism) the only homomorphic images of the ring \mathbb{Z}

10

- gcd's and lcm's

possible definition for the greatest common divisor $d = \gcd(a, b)$ of two integers a, b (not both equal to 0):

- $d = \max\{n \in \mathbb{Z}; n|a \wedge n|b\}$
- $d > 0, d|a, d|b$ and $c|a \wedge c|b \Rightarrow c|d$
- $d = \min\{a \cdot s + b \cdot t > 0; s, t \in \mathbb{Z}\}$
- $d > 0$ and $d \cdot \mathbb{Z} = \{a \cdot s + b \cdot t; s, t \in \mathbb{Z}\} = a \cdot \mathbb{Z} + b \cdot \mathbb{Z}$

notation: $a \perp b \stackrel{\text{df}}{\Leftrightarrow} \gcd(a, b) = 1$ (a and b are "relatively prime")

definition of least common multiple

$$a \cdot \mathbb{Z} \cap b \cdot \mathbb{Z} = \text{lcm}(a, b) \cdot \mathbb{Z}$$

11

properties of the gcd

$$\begin{aligned} \gcd(a, b) &= \gcd(b, a) & \gcd(a, \gcd(b, c)) &= \gcd(\gcd(a, b), c) \\ \gcd(a, b) &= a \Leftrightarrow a|b & \gcd(a, 0) &= a \\ a/\gcd(a, b) \perp b/\gcd(a, b) & & \gcd(m \cdot a, m \cdot b) &= m \cdot \gcd(a, b) \\ \gcd(a, b) &= \gcd(b, a - b \cdot q) & & \end{aligned}$$

properties of gcd related to relative primeness

$$\begin{aligned} a \perp b \Rightarrow \gcd(a, b \cdot c) &= \gcd(a, c) & a \perp b, a|b \cdot c &\Rightarrow a|c \\ a \perp b, a \perp c &\Rightarrow a \perp b \cdot c & a \perp b, a|c, b|c &\Rightarrow a \cdot b|c \\ a \perp b \Rightarrow a^n \perp b^m & (n, m \geq 1) & a \perp b &\Rightarrow (a^m|b \cdot c \Leftrightarrow a^m|c) \end{aligned}$$

12

definition of multiplicities for $a \geq 2$:

$$\nu_a(n) := \max \{ m \in \mathbb{N}; a^m | n \}$$

$$p \in \text{PRIM}, p | b \cdot c, p \nmid b \Rightarrow p | c$$

$$a \perp b \Rightarrow \nu_a(b \cdot c) = \nu_a(c)$$

$$p \in \text{PRIM}, a = p^m \cdot b : m = \nu_p(a) \Leftrightarrow p \perp b$$

$$p \in \text{PRIM} \Rightarrow (\nu_p(b \cdot c) = \nu_p(b) + \nu_p(c))$$

properties of *lcm* follow from

$$\gcd(a, b) \cdot \text{lcm}(a, b) = a \cdot b$$

13

- solvability of linear diophantine equations —Bézout's identity for $a, b, c \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$ it holds that

$$\exists u, v \in \mathbb{Z} : a \cdot u + b \cdot v = c \Leftrightarrow \gcd(a, b) | c$$

and if the condition is satisfied, then all integer solutions of

$$a \cdot x + b \cdot y = c$$

are given by

$$\frac{c}{d} \cdot (s, t) + \frac{k}{d} \cdot (-b, a) \quad (k \in \mathbb{Z})$$

where s, t are Bézout coefficients for (a, b) and $d = \gcd(a, b)$, i.e., $a \cdot s + b \cdot t = d$

14

- \mathbb{Z} is a factorial ring (or *unique factorization domain*) (existence and uniqueness of prime factorization)

– existence:

$$n = \prod_{p \in \text{PRIM}} p^{\nu_p(n)}$$

– uniqueness:

$$n = \prod_{p \in \text{PRIM}} p^{\alpha_p} \Rightarrow \forall p \in \text{PRIM} : \alpha_p = \nu_p(n)$$

– canonical factorization for $n \in \mathbb{N}_+$

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}$$

where $p_1 < p_2 < \dots < p_m$ are primes and $\alpha_1, \dots, \alpha_m \in \mathbb{N}_+$

15

- prime factorization and gcd/lcm

For

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_m^{\alpha_m}, \quad b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_m^{\beta_m}$$

with primes $p_1 < p_2 < \dots < p_m$ and exponents $\alpha_i, \beta_j \geq 0$, one has

$$\begin{aligned} a | b &\Leftrightarrow \forall i : \alpha_i \leq \beta_i \\ \gcd(a, b) &= p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_m^{\min(\alpha_m, \beta_m)} \\ \text{lcm}(a, b) &= p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_m^{\max(\alpha_m, \beta_m)} \end{aligned}$$

16