Contents

1 Section 4.1

1.1 Theorem 1

Proof:

$$a|b \implies b = a \cdot m$$
$$a|c \implies c = a \cdot n$$

For some $m, n \in \mathbb{Z} \implies m+n \in \mathbb{Z}$. Then $b+c = am+an = a(m+n) \therefore a|b+c$.

1.2 Division Algorithm

The function **div** is called the division algorithm.

$$\text{div}(a, d) = a \text{ div } d = \left\lfloor \frac{a}{d} \right\rfloor \tag{1}$$

$$\text{div} : \mathbb{Z} \times \mathbb{Z}^+ \implies \mathbb{Z} \tag{2}$$

The function receives a dividend and divisor and produces the quotient.

1.3 Modulus Algorithm

The function **mod** is called the modulus algorithm.

$$\text{mod}(a, d) = a \text{ mod } d = a - \left\lfloor \frac{a}{d} \right\rfloor \tag{3}$$

where $a = d \cdot q + r$.

$$\text{mod} : \mathbb{Z} \times \mathbb{Z}^+ \implies \mathbb{Z} \tag{4}$$

The function receives a dividend and divisor and produces the remainder.

$$a \equiv b \pmod{m} \iff m|\,(a-b) \tag{5}$$

1.4 Remarks

1.
$$\mathbb{Z}_m \,(Z \bmod m)$$
$$Z_m = \{0_m, 1_m, 2_m, \cdots, (m-1)_m\}$$

where 0_m is a set

- $r \in 0_m$ if $r \equiv 0 \pmod{m}$
- $r \in 1_m$ if $r \equiv 1 \pmod{m}$

2 Section 4.2

2.1 Theorem 1

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \tag{6}$$

where k is a nonnegative integer, $a_0, a_1, \cdots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

2.2 Example

When $b = 10, a_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$$7254887 = 7 \cdot 10^6 + 2 \cdot 10^5 + 5 \cdot 10^4 + 4 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 7 \cdot 10^0$$