Integers

Discrete Mathematics

Courtesy of Andrei Bulatov

Integers

"God made the integers; all else is the work of man"

Leopold Kroenecker

Division

- *Most of useful properties of integers are related to division*
- *If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c such that $b = ac$.*
- *When a divides b we say that a is a **divisor** (**factor**) of b, and that b is a **multiple** of a.*
- *The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b*
- *Example. Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?*

  The numbers in question have the form dk, where k is a positive integer and $0 < dk \le n$. Therefore, $0 < k \le n/d$. Thus the answer is $\lfloor n/d \rfloor$

Properties of Divisibility

- *Let* a, b, *and* c *be integers. Then*

  (i) *if* $a \mid b$ *and* $a \mid c$, *then* $a \mid (b + c)$;

  (ii) *if* $a \mid b$, *then* $a \mid bc$ *for all integers* c;

  (iii) *if* $a \mid b$ *and* $b \mid c$, *then* $a \mid c$.

- *Proof.*

  (i) *Suppose* $a \mid b$ *and* $a \mid c$. *This means that there are* k *and* m *such that* $b = ak$ *and* $c = am$.

  Then $b + c = ak + am = a(k + m)$, *and* a *divides* $b + c$.

Properties of Divisibility (cntd)

- *If a, b, and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.*
- *Proof.*

  By part (ii) it follows that $a \mid mb$ and $a \mid nc$.

  By part (i) it follows that $a \mid mb + nc$.

- *If $a \mid b$ and $b \mid a$, then $a = \pm b$.*
- *Proof.*

  Suppose that $a \mid b$ and $b \mid a$. Then $b = ak$ and $a = bm$ for some integers k and m.

  Therefore $a = bm = akm$, which is possible only if $k, m = \pm 1$.

Euclidean division algorithm

- **Theorem** *(Euclidean division)*

  Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$

- *d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder* q

- *Examples:*

  - $a = 101$ and $d = 11$ $\rightarrow a = d \cdot 9 + 2$

  - $a = -11$ and $d = 3$ $\rightarrow a = d \cdot (-4) + 1$

  - $a = 3$ and $d = 11$ $\rightarrow a = d \cdot 0 + 3$

Representation of Integers

- *In most cases we use decimal representation of integers. For example, 657 means*

$$6 \cdot 100 + 5 \cdot 10 + 7 = 6 \cdot 10^2 + 5 \cdot 10^1 + 7 \cdot 10^0$$

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

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

where k is a nonnegative number, $a_k, a_{k-1}, \ldots, a_1, a_0$ are nonnegative integers less than b, and $a_k \neq 0$

- *Such a representation of n is called the base b expansion of n, denoted by $(a_k a_{k-1} \ldots a_1 a_0)_b$*

Binary Expansion

$n = 2 \cdot q + a_0$

- *Important case of a base is 2. The base 2 expansion is called the binary expansion of a number*

$$n = a_k \cdot 2^k + a_{k-1} \cdot 2^{k-1} + \cdots + a_1 \cdot 2 + a_0$$

- *Find the binary expansion of 165*

Quotient	82	41	20	10	5	2	1 (a_7)
Division	2 ⟌ 165	2 ⟌ 82	2 ⟌ 41	2 ⟌ 20	2 ⟌ 10	2 ⟌ 5	2 ⟌ 2
Remainder	1	0	1	0	0	1	0
	a_0	a_1	a_2	a_3	a_4	a_5	a_6

$165 = 2 \cdot 82 + 1$

$82 = 2 \cdot 41 + 0$

$41 = 2 \cdot 20 + 1$

$20 = 2 \cdot 10 + 0$

$10 = 2 \cdot 5 + 0$

$5 = 2 \cdot 2 + 1$

$2 = 2 \cdot 1 + 0$

$1 = 2 \cdot 0 + 1$

$$165 = (10100101)_2$$

D A

Hexadecimal Expansion

1101 1010

- *Using A, B, C, D, E, F for 10, 11, 12, 13, 14, 15, respectively, find the base 16 expansion of :*

  - *174* $= 10 \cdot 16 + 14$ → AE

  - *218* –

Practice

Exercises from the Book

7th edition: 6, 8, 23 (page 244 – 245)

1ab, 3ac, 7ac (also find the decimal representation) (page 255)

8th edition: 6, 8, 29 (page 258 – 259)

1ab, 3ac, 7ac (also find the decimal representation) (page 269)