Lecture 1: Integers (1.1 – 1.3)

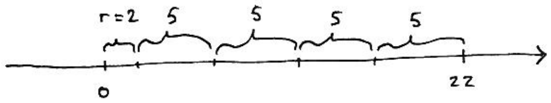
Integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$ with the usual operations $+, \cdot$ and order relation $<$.

> **Well-ordering axiom:** Every nonempty subset of $\mathbb{N} = \{0, 1, 2, 3, \dots\}$ has a smallest element.

Note: Is equivalent to the induction principle (App. C)

> **Division algorithm:** Let $a, b \in \mathbb{Z}$ and $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$, $0 \le r < b$, such that
> $$a = bq + r.$$

Ex: $22 = 5 \cdot 4 + 2 \qquad (0 \le 2 < 5)$



Proof: (for the case $a \ge 0$). Consider the set
$$S = \{a - xb \mid x \in \mathbb{Z},\ a - xb \ge 0\}.$$
We see that $S \subseteq \mathbb{N}$ and that $S \ne \emptyset$ (since $a - 0 \cdot b \in S$). According to the w.o.-axiom S has a smallest element $r = a - qb$.

We get $a = bq + r$ and it remains to show

that $0 \le r < b$: We know by construction that $r \ge 0$, and if $r \ge b$ it follows that $r - b \ge 0$ and
$$r - b = a - qb - b = a - (q+1)b \in S,$$
contradicting the minimality of r.

Uniqueness: Assume $a = bq_1 + r_1 = bq_2 + r_2$, $0 \le r_1, r_2 < b$, and show that $q_1 = q_2$, $r_1 = r_2$ (see book). □

. . . .

Def: $a, b \in \mathbb{Z}$, $b \ne 0$. We say that b divides a, and write $b \mid a$, if there exists $c \in \mathbb{Z}$ s.t. $a = bc$.

Ex: $2 \mid 6$ since $6 = 2 \cdot 3$, but $4 \nmid 6$.

Ex: 6 has the divisors $\pm 1, \pm 2, \pm 3, \pm 6$.

Ex: $b \mid 0$ for all $b \ne 0$, since $0 = b \cdot 0$

$1 \mid a$ for all a, since $a = 1 \cdot a$

$a \mid a$ for all $a \ne 0$, since $a = a \cdot 1$.

Exercise: A) $\left.\begin{matrix} a \mid b \\ b \mid a \end{matrix}\right\} \Rightarrow b = \pm a$

B) $\left.\begin{matrix} a \mid b \\ b \mid c \end{matrix}\right\} \Rightarrow a \mid c$

C) $\left.\begin{matrix} c \mid a \\ c \mid b \end{matrix}\right\} \Rightarrow c \mid xa + yb$ for all $x, y \in \mathbb{Z}$.

Def: Let $a, b \in \mathbb{Z}$ (not both zero). The greatest common divisor $d \in \mathbb{Z}$ of a, b is the integer that satisfies

1. $d \mid a$ and $d \mid b$ (common divisor)
2. if $c \mid a$ and $c \mid b$, then $c \le d$ (greatest).

We write $d = (a, b)$.

Ex: 6 has divisors $\pm 1, \pm 2, \pm 3, \pm 6$

10 — " — $\pm 1, \pm 2, \pm 5, \pm 10$

Common divisors are $\pm 1, \pm 2$

$\Rightarrow (6, 10) = 2.$

Ex: $(7, 12) = 1$, relatively prime.

> **Theorem:** If $d = (a, b)$ then there exist $u, v \in \mathbb{Z}$ such that
> $$d = ua + vb.$$

Proof: Let $S = \{xa + yb \mid x, y \in \mathbb{Z},\ xa + yb > 0\}$.

By construction $S \subseteq \mathbb{N}$ and $S \ne \emptyset$ since $a \cdot a + b \cdot b = a^2 + b^2 > 0$. By the w.o.-axiom S has a smallest member $t = ua + vb$. We want to show that $t = d$:

$t \mid a$ and $t \mid b$: $a = qt + r$, $0 \le r < t \Rightarrow$
$$r = a - qt = a - q(ua + vb) = (1 - qu)a + (-qv)b$$
If $r > 0$ then it follows that $r \in S$, and conseq. this contradicts the minimality of t.

Thus $r = 0$ and $a = qt \Rightarrow t \mid a$.

Analogously we get $t \mid b$

t greatest: Assume $c \mid a$ and $c \mid b$. Then
$$c \mid ua + vb = t \Rightarrow c \le t.$$
□

Note: $d = (a, b)$ is the smallest positive integer of the form $ua + vb$.

Alternative def. of gcd:

1. $d \mid a$ and $d \mid b$
2. if $c \mid a$ and $c \mid b$, then $c \mid d$

> **Theorem:** If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Proof: $1 = ua + vb$ for some $u, v \Rightarrow$
$$c = cua + cvb = (cu)a + v(bc)$$
Since $a \mid a$ and $a \mid bc$, it follows that
$$a \mid (cu)a + v(bc), \text{ i.e. } a \mid c$$
□

Euclidean algorithm

A way to compute (a,b).

Ex: $a = 228$, $b = 186$.

Div. alg.

$$228 = 186 \cdot 1 + 42$$
$$186 = 42 \cdot 4 + 18$$
$$42 = 18 \cdot 2 + 6$$
$$18 = 6 \cdot 3 + \underline{0}$$

The last nonzero remainder is gcd,

so $(228,186) = \underline{6}$.

Based on the following lemma:

Lemma: If $a = bq + r$, then $(a,b) = (b,r)$.

Proof. Left as exercise (see book).

Note: $(228,186) = (186,42) = (42,18) = (18,6) = 6$.

Note: We can also use E.A. backwards:

$$\underline{6} = 42 - 18 \cdot 2 = 42 - (186 - 42 \cdot 4) \cdot 2 =$$
$$= 9 \cdot 42 - 2 \cdot 186 = 9(228 - 186 \cdot 1) - 2 \cdot 186 =$$
$$= \underline{9 \cdot 228 + (-11) \cdot 186}.$$

We obtain (a,b) as a linear combination of of a and b, i.e. $(a,b) = ua + vb$.

. . . .

Def: $p \in \mathbb{Z}$ is prime if $p \neq 0, \pm 1$ and the only divisors are ± 1 and $\pm p$.

Ex: $\pm 2, \pm 3, \pm 5, \pm 7, \ldots$ are primes

Theorem: $\left.\begin{array}{l} p \text{ prime} \\ p \mid ab \end{array}\right\} \Rightarrow p \mid a$ or $p \mid b$.

Proof: Assume $p \nmid a$. Then $(p,a) = 1$ and $p \mid b$ by th. above. □

Corollary: $\left.\begin{array}{l} p \text{ prime} \\ p \mid a_1 a_2 \cdots a_n \end{array}\right\} \Rightarrow p \mid a_i$ for some i.

Proof: Use th. above repeatedly. □

Theorem: Every $n \neq 0, \pm 1$ is a product of primes.

Proof: Sufficient to consider $n \geq 2$.

Consider the set $S = \{ n \in \mathbb{Z} \mid n \geq 2, n \text{ not product of primes} \}$.

We want to show that $S = \emptyset$.

Assume the contrary, i.e that $S \neq \emptyset$. By the w.o.-axiom. S then contains a smallest element m. Since m cannot be prime we have $m = ab$ with $1 < a,b < m$. Since $a,b \notin S$ (m is minimal) these are products of primes, i.e. $a = p_1 p_2 \cdots p_k$, $b = q_1 q_2 \cdots q_l$

$\Rightarrow$ $m = ab = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$ is a product of primes $\Rightarrow m \notin S$. Contradiction! □

Fundamental theorem of arithmetic: Every integer $\neq 0, \pm 1$ is a product of primes, unique up to the ordering (and the sign) of the factors.

Proof: See book. □

Note: Prime factoring is a hard problem. Basis for coding theory (e.g. RSA).

. . . .

Congruence in $\mathbb{Z}$ (2.1-2.2):

Def: Let $a,b \in \mathbb{Z}$ (and let $n \geq 2$). If

$$n \mid b - a,$$

then we say that a is congruent to b modulo n, and write $a \equiv b \pmod{n}$.

I.e. $a \equiv b \pmod{n} \Leftrightarrow b = a + kn$ for some $k \in \mathbb{Z}$

Theorem:
1. $a \equiv a \pmod{n}$ (reflexive)
2. $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ (symmetric)
3. $\left.\begin{array}{l} a \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\} \Rightarrow a \equiv c \pmod{n}$ (transitive)

Proof: ①: $n \mid a - a = 0$

②: $n \mid b - a \Leftrightarrow n \mid a - b$

③: $\left.\begin{array}{l} n \mid b - a \\ n \mid c - b \end{array}\right\} \Rightarrow n \mid (b-a) + (c-b) = c - a$ □

A relation that is reflexive, symmetric and transitive is called an equivalence relation.

We then define the congruence classes

$$[a] = \{ b \in \mathbb{Z} \mid b \equiv a \pmod{n} \}$$

Ex: $n = 3$ $[7] = \{ \ldots, 7-3, 7, 7+3, 7+2 \cdot 3, \ldots \}$
$$= \{ \ldots, 4, 7, 10, 13, \ldots \}$$

Theorem: ① $a \equiv b \pmod{n} \Leftrightarrow [a] = [b]$

② For $a, b \in \mathbb{Z}$ either $[a] = [b]$ (equal)

or $[a] \cap [b] = \emptyset$ (disjoint)

Proof: See book. □

Since congruence classes are disjoint and every $a \in \mathbb{Z}$ belongs to one congruence class ($a \in [a]$, since $a \equiv a \pmod{n}$) the congruence classes constitute a partition of $\mathbb{Z}$.

Def: The set of all congruence classes mod n is denoted $\mathbb{Z}_n$.

Div. alg.: $a = nq + r$, $0 \le r < n$.

We get $a \equiv r \pmod{n}$ and

$$\mathbb{Z}_n = \{[0], [1], [2], \dots, [n-1]\}$$

Arithmetic in $\mathbb{Z}_n$:

We define
$$[a] \oplus [b] = [a+b]$$
$$[a] \odot [b] = [ab].$$

Ex: $\mathbb{Z}_5$: $[3] \oplus [4] = [7] = [2]$

$[3] \odot [4] = [12] = [2]$

Note! Only meaningful if $\oplus$ and $\odot$ are well-defined, i.e if

$$\left.\begin{matrix} [a] = [c] \\ [b] = [d] \end{matrix}\right\} \Rightarrow \begin{matrix} [a+b] = [c+d] \\ [ab] = [cd] \end{matrix}$$

or alternatively

$$\left.\begin{matrix} a \equiv c \pmod{n} \\ b \equiv d \pmod{n} \end{matrix}\right\} \Rightarrow \begin{matrix} a+b \equiv c+d \pmod{n} \\ ab \equiv cd \pmod{n} \end{matrix}$$

Check yourself (or see book).

Th. 2.7, properties of $\oplus$ and $\odot$ in $\mathbb{Z}_n$, follows from corr. properties of $\mathbb{Z}$.