§3.1: Direct Proofs

►. Section 3.1 (Direct Proofs) is a reinforcement of Section 1.2 (Constructing Direct Proof).
§1.2 introduced direct proof using the concepts of even and odd integers.
§3.1 reinforces direct proofs by using concepts (probably know from high school) other than just even/odd.

Def. A nonzero integer n **divides** an integer b, denoted $n|b$, provided that $(\exists k \in \mathbb{Z})\ [nk = b]$. p82

Rmk. The integer 0 does not divide any integer.

Defs. Let $n \in \mathbb{Z} \setminus \{0\}$ and $b \in \mathbb{Z}$. Then the following are equivalent (i.e., TFAE).

- $n|b$
- n **divides** b
- n is a **divisor** of b
- n is a **factor** of b ◦ b is a **multiple** of n

Do NOT express $n|b$ as $\frac{b}{n}$. Why? p82

Thm. Let a, b, and c be integers with $a \neq 0$ and $b \neq 0$. If $a|b$ and $b|c$, then $a|c$. I.e., "divides" is *transitive*. Thm3.1 p88

★. At end of §3.1's summary, see: Recall some Definitions used in ER's. ⟨prime, composite, irrational⟩

Division Algorithm (DA) Revisited

Recall. **Thm. DA**. For all $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, there exist unique integers q and r s.t. §3.5 p143

$$a = nq + r \qquad \text{and} \qquad 0 \leq r < n\ . \tag{1}$$

We says: "when we divide the integer a by the natural number n, the **quotient** is q and the **remainder** is r."

Rmk. The equality in (1) can be written as $\frac{a}{n} = q + \frac{r}{n}$ ⟨but we do not write like this in our proofs⟩. §3.5 p144

▷. DA symbolically: $(\forall n \in \mathbb{N})\ (\forall a \in \mathbb{Z})\ (\exists! q \in \mathbb{Z})\ (\exists! r \in \mathbb{Z})\ [\ a = nq + r \quad \wedge \quad 0 \leq r < n\ ]$.

???. What happens in the DA if instead of starting the remainder r at $s = 0$ we start r at some other $s \in \mathbb{Z}$?

Cor. **Thm. DA$^+$**. Fix $s \in \mathbb{Z}$. For all $n \in \mathbb{N}$ and $a \in \mathbb{Z}$, there exist unique integers q_s and r_s s.t. not in book

$$a = nq_s + r_s \qquad \text{and} \qquad s \leq r_s < s + n\ . \tag{2}$$

▷. DA$^+$ symbolically: $(\forall n \in \mathbb{N})\ (\forall a \in \mathbb{Z})\ (\forall s \in \mathbb{Z})\ (\exists! q_s \in \mathbb{Z})\ (\exists! r_s \in \mathbb{Z})\ [\ a = nq_s + r_s \wedge s \leq r_s < s + n\ ]$.

Lemma. Lemma DA$^+$ uniqueness part. Let $s \in \mathbb{Z}$. ⟨s is the *starting* number for the remainder in DA$^+$.⟩ not in book
Let $n \in \mathbb{N}$ and $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ such that $nq_1 + r_1 = nq_2 + r_2$ with $s \leq r_1 < s+n$ and $s \leq r_2 < s+n$.
Then $q_1 = q_2$ and $r_1 = r_2$.

why?. Let the given hold. ⟨We WTS $q_1 = q_2$ and $r_1 = r_2$. So it is E$_{\text{nuf}}$TS: $q_1 - q_2 = 0$ and $r_2 - r_1 = 0$.⟩
⟨What can we say about $r_2 - r_1$?⟩ Since $s \leq r_2 < s + n$ and $-s - n < -r_1 \leq -s$ we get

$$-n < r_2 - r_1 < n. \tag{3}$$

⟨What can we say about $q_1 - q_2$?⟩ Since $nq_1 + r_1 = nq_2 + r_2$ we get

$$n(q_1 - q_2) = r_2 - r_1. \tag{4}$$

Combining (3) and (4) gives

$$-n < n(q_1 - q_2) < n.$$

Since $n \neq 0$ ⟨so can divide thru by n⟩ we get $-1 < q_1 - q_2 < 1$. Since $q_1 - q_2 \in \mathbb{Z}$ and $-1 < q_1 - q_2 < 1$, we get $q_1 - q_2 = 0$. So $r_2 - r_1 \underset{(4)}{\overset{\text{by}}{=}} n(q_1 - q_2) \underset{q_1 - q_2 = 0}{\overset{\text{know}}{=}} n(0) = 0$.

Divides and Congruent

Def. A nonzero integer n **divides** an integer b, denoted $n|b$, provided that $(\exists k \in \mathbb{Z})\ [nk = b]$. p82

Def. Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. p92
Then a **is congruent to** b **modulo** n, denoted $a \equiv b \pmod{n}$, provided n divides $a - b$.

Rmk. Let $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$. The following are equivalent (TFAE).

(1) a is congruent to b modulo n
(2) $a \equiv b \pmod{n}$
(3) n divides $a - b$, i.e., $n|(a-b)$
(4) $(\exists k \in \mathbb{Z})\,[a - b = nk]$
(5) $(\exists k \in \mathbb{Z})\,[a = nk + b]$

to see (4)$\Leftrightarrow$(4′) $\Longleftrightarrow$ take $j = -k$

(1′) b is congruent to a modulo n
(2′) $b \equiv a$ (mod n)
(3′) n divides $b - a$, i.e., $n|(b-a)$
(4′) $(\exists j \in \mathbb{Z})\,[b - a = nj]$
(5′) $(\exists j \in \mathbb{Z})\,[b = nj + a]$

Note (1) $\overset{\text{notation}}{\Longleftrightarrow}$ (2) $\underset{\text{congruence}}{\overset{\text{def. of}}{\Longleftrightarrow}}$ (3) $\underset{\text{divides}}{\overset{\text{def. of}}{\Longleftrightarrow}}$ (4) $\overset{\text{algebra}}{\Longleftrightarrow}$ (5). Similiarly, (1′) $\Leftrightarrow$ (2′) $\Leftrightarrow$ (3′) $\Leftrightarrow$ (4′) $\Leftrightarrow$ (5′).

$\triangleright$. As def. of $a \equiv b \pmod{n}$ we can use (unless otherwise indicated) any of the above equivalent formations: (3), (4), (5), (3′), (4′), (5′).

Thm. Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$ ER 11 p98

(1) $a \equiv a$ (mod n) (reflexive)
(2) If $a \equiv b$ (mod n), then $b \equiv a$ (mod n). (symmetric)
(3) If $a \equiv b$ (mod n) and $b \equiv c$ (mod n), then $a \equiv c$ (mod n). (transitive)

Thm. **Thm. 3.30**. Congruence modulo n is an **equivalence relation**. p148

Def. Congruent is a **relation** means that $a \equiv b$ (mod n) is either true or false, but not both.
The adjective **equivalence** means the relation is: reflexive, symmetric, and transitive. < rst>

Thm. **Modulo Arithmetic**. Let $n \in \mathbb{N}$ and $a_1, a_2, b_1, b_2 \in Z$. ER 12 p98
Let the congruences in (5) and (6) hold.

$$a_1 \equiv a_2 \text{ (mod n)} \tag{5}$$
$$b_1 \equiv b_2 \text{ (mod n)} \tag{6}$$

Then the congruences in (7) and (8) hold.

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n} \tag{7}$$
$$a_1 b_1 \equiv a_2 b_2 \pmod{n} \tag{8}$$

★. **ER 3.5.5a**. Fix $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then $a \equiv 0 \pmod{n}$ if and only if $n|a$. p153

why?. Note: $a \equiv 0 \pmod{n} \underset{\text{mod congr.}}{\overset{\text{def.}}{\Longleftrightarrow}} n|\,(a-0) \overset{\text{algrebra}}{\Longleftrightarrow} n|a.$

Thm. **Thm. 3.31**$^+$. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ and $r \in \mathbb{Z}$. ⟨think DA$^+$⟩ p150
Then $a = nq + r$ for some $q \in \mathbb{Z}$ if and only if $a \equiv r$ (mod n).

why?. $(\exists q \in \mathbb{Z})\,[a = nq + r] \overset{\text{algebra}}{\Longleftrightarrow} (\exists q \in \mathbb{Z})\,[a - r = nq] \underset{\text{divides}}{\overset{\text{def.}}{\Longleftrightarrow}} n|\,(a-r) \underset{\text{mod congr.}}{\overset{\text{def.}}{\Longleftrightarrow}} a \equiv r \pmod{n}$.

Rmk. So $a \in \mathbb{Z}$ is congruent modulo n to the remainder obtained when a is divided by $n \in \mathbb{N}$ in DA.

Cor. **Cor. 3.32**. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then there exists a unique $r \in \mathbb{Z}$ such that p150

$$a \equiv r \pmod{n} \qquad \text{and} \qquad 0 \le r < n\ .$$

Cor. **Cor 3.32**$^+$. Fix $s \in \mathbb{Z}$. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then there exists a unique $r \in \mathbb{Z}$ such that not in book

$$a \equiv r \pmod{n} \qquad \text{and} \qquad s \le r < s + n\ .$$

why?. Fix $s \in \mathbb{Z}$ (for Cor. 3.32 take $s = 0$). Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. First apply Thm. DA$^+$ to express $a = nq + r$ for a unique $q \in \mathbb{Z}$ and unique $r \in \mathbb{Z}$ with $s \le r < s + n$. Then use Thm. 3.31$^+$.

Recall some Definitions
used in ER's

Def. A $p \in \mathbb{N}$ is **prime** provided $p \neq 1$ and the only natural numbers that are factors of p are: 1 and p. p78

Def. A $c \in \mathbb{N}$ is **composite** provided $c \neq 1$ and c is not a prime number. p78

▷. The number 1 is neither prime nor composite. In Math 546 you will learn 1 is a unit.

So. A $p \in \mathbb{N}$ is a **prime number** provided $(p \neq 1) \wedge (\forall d \in \mathbb{N}) \left[\, d|p \Rightarrow (d = 1 \ \vee \ d = p) \,\right]$
A $c \in \mathbb{N}$ is a **composite number** provided $(c \neq 1) \wedge (c \text{ is not a prime number})$.

Def. A real number x is a rational number provided that $(\exists\, (a,b) \in \mathbb{Z}^2) \left[\, x = \frac{a}{b} \ \wedge \ b \neq 0 \,\right]$. p122
, or equivalently, provided that $(\exists\, (a,b) \in \mathbb{Z} \times \mathbb{N}) \left[\, x = \frac{a}{b} \,\right]$.
A real number that is not a rational number is called an irrational number.

Rmk. The rational numbers are denoted by $\mathbb{Q}$. Thus the irrational numbers are $\mathbb{R} \setminus \mathbb{Q}$.

§3.2 More Methods of Proofs

►. More (other than direct) methods of proof:

contrapositive, biconditional, other logical equivalency, constructive/nonconstructive proofs .

Often, these new methods reduces the problem down to a direct proof (or to several direct proofs).

Def. A **constructive proof** is a proof where we construct the desired object we want to show exists. p88
E.g. Theorem. There exists a real number x such that $x^2 - 9 = 0$.
Proof. Let $x = 3$. Then $x \in \mathbb{R}$ and $x^2 - 9 = 3^2 - 9 = 0$. When have just ⟨constructively⟩ proved that there exists a real number x such that $x^2 - 9 = 0$. □

►. The below facts are used often in the homework problems.

- **Thm 3.10**. $(\forall n \in \mathbb{Z})$ [n is even $\Leftrightarrow$ n^2 is even]. p108
- **Cor 3.10**. $(\forall n \in \mathbb{Z})$ [n is odd $\Leftrightarrow$ n^2 is odd]. not in book
- **ER 3.2.1c**. $(\forall n \in \mathbb{Z})$ [n is even $\Leftrightarrow$ n^3 is even]. p112
- **ER 3.2.1d**. $(\forall n \in \mathbb{Z})$ [n is odd $\Leftrightarrow$ n^3 is odd]. p112

§3.3 Proof by Contradiction

►. To proof Thm. 1 ⟨is true⟩ by contradiction , assume that Thm. 1 is false. Then logically argue that the assumption ⟨that Thm. 1 is false⟩ leads to a contradction (e.g. $0 = 1$). Thus Thm. 1 must be true.

★. See this summary's Section on Prime Factorization.

§3.4 Using Cases in Proofs

►. A proof by cases (also called proof by exhaustion) is a proof consisting of examining every possible case.

Rmk. Often, proof by cases is not the first choice of proof method.

Rmk. Natural concepts that lead to r a proof by cases are: DA, DA$^+$, and Modulo Congrence ⟨even PR⟩.
E.g., Cor. 3.32$^+$ can be used set up a proof by cases. The $n \in \mathbb{N}$ and $a \in \mathbb{Z}$ are given in the theorem's statement. Pick $s \in \mathbb{Z}$ ⟨pick s to make the arithmetic easy⟩. Then the integer a is congruent modulo n to precisely one of the integer in the set $\{s, s+1, s+2, \ \ldots \ , s+n-1\}$, which contains n elements. So we can consider these n cases for a.

§3.5 Division Algorithm/Congruence

Thm. **Thm. 3.28**. Let $n \in \mathbb{N}$ and $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. If $a_1 \equiv a_2 \pmod{n}$ and $b_1 \equiv b_2 \pmod{n}$, then p147

(1) $(a_1 + b_1) \equiv (a_2 + b_2) \pmod{n}$
(2) $(a_1 \cdot b_1) \equiv (a_2 \cdot b_2) \pmod{n}$
(3) $(a_1)^m \equiv (a_2)^m \pmod{n}$ for each $m \in \mathbb{N}$.

Prime Factorization (PF)

Note. Since 75 factors as $75 = (3)\,(25) = (3)\,(5^2)$, the prime factorization of 75 is: $75 = (3^1)\,(5^2)$.

Each $n \in \mathbb{N} \setminus \{1\}$ has a unique prime factorization.

Thm. Prime Factorization (Fundamental Theorem of Arithmetic) Thm8.15 p432 p427

For each $n \in \mathbb{N} \setminus \{1\}$ there exists unique

(1) $m \in \mathbb{N}$ $\langle m$ is the number of primes in the prime factorization of $n\rangle$

(2) prime numbers $p_1, p_2, \ldots, p_m$

(3) natural numbers $k_1, k_2, \ldots, k_m$

such that

$$n = \prod_{i=1}^{m} (p_i)^{k_i}$$

and $p_1 < p_2 < \ldots < p_{m-1} < p_m$. (We often say: the prime factorization of n is "unique up to ordering")

▷. Corollaries to Prime Factorization Theorem:

Cor 1. In the prime factorization of $n \in \mathbb{N}^{>1}$, the total numbers of factors of a prime is a nonnegative integer.

why?. Let q be a prime and consider the prime factorization $n = \prod_{i=1}^{m} (p_i)^{k_i}$.
If q is one of the p_i's, then the PF of n has $k_i \in \mathbb{N}$ factors of q.
If q is not one of the p_i's, then the PF of n has 0 factors of q.

Cor 2. Let $n \in \mathbb{N} \setminus \{1\}$ have a prime factorization $n = \prod_{i=1}^{m} (p_i)^{k_i}$ where each p_i is a prime number and each $k_i \in \mathbb{N}$. Then

(1) n is even if and only if $2 \in \{p_1, \ldots, p_m\}$

(2) n is odd if and only if $2 \notin \{p_1, \ldots, p_m\}$.

why?. Note: n even $\overset{\text{def.}}{\underset{\text{even}}{\Longleftrightarrow}} (\exists k \in \mathbb{Z})[n = 2k] \overset{\text{def.}}{\underset{\text{factor}}{\Longleftrightarrow}}$ 2 is a factor of $n \overset{\text{PF}}{\underset{\text{of } N}{\Longleftrightarrow}} 2 \in \{p_1, \ldots, p_m\}$.
Note: (2) follows from (1) by contrapostive (twice). $[R \Leftrightarrow S] \equiv [\sim R \Leftrightarrow \sim S]$

Cor 3. Let $n \in \mathbb{N}$ and p be a prime number. If the total number of factors of p in n is $k \in \mathbb{Z}^{\geq 0}$,

then the total number of factors of p in n^2 is $2k \in \mathbb{Z}^{\geq 0}$.

Thus the total number of factors of a prime in the square of a natural number is a even integer.

why?. Let p be prime.
First: let $n \in \mathbb{N}^{>1}$. For n and n^2, consider their prime factorizations:

$$n = \prod_{i=1}^{m} (p_i)^{k_i} \overset{\text{algebra}}{\Longleftrightarrow} n^2 = \prod_{i=1}^{m} (p_i)^{2k_i}.$$

So if $p = p_i$ for some i, then n has k_i factors of p_i while n^2 has $2k_i$ factors of p_i.
And if p is not one of the p_i's then both n and n^2 have 0 factors of p $\langle$and $0 = 2\,(0)\rangle$.
Second: let $n = 1$. Then $n^2 = 1$ so both n and n^2 have 0 factors of p.