§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.

Some Math Terninology

p85-86

1. A **proof** in mathematics is a convincing argument that some mathematical statement is true. §1.2 p22
⟨Proof is a noun while prove is a verb. So we prove a true stament by providing a proof of the statement.⟩
2. A **definition** is simply an agreement as to the meaning of a particular term. ⟨e.g., even integer⟩
3. There are **undefined terms** in math. <Simply put, we must start somewhere. E.g., in Euclidean Geometry: point&line.>
4. An **axiom** is a mathematical statement that is accepted without proof.
5. A **lemma** is a true statement that was proven mainly to help in the proof of some theorem.
6. A **theorem** is a true mathematical statement for which we have a proof. ⟨*Theorem* is abbreviated by *Thm.*.⟩
7. A **proposition** is a *small theorem*. ⟨this def. of proposition is more common than using prop. to mean statement⟩
8. A **corollary** is a (small) thm. that is easily proven once some other (bigger) thm. has been proven.
9. A **conjecture** is a statement that we believe is plausible (but we do not have a proof for it ... yet).
<To show a conjecture is true, we prove the conjecture.
To show a conjecture is false, you can find a counterexample to the conjecture.>

Def. A **constructive proof** is a proof where we use your *givens* to construct the desired object that 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 $x^2 - 9 = 0$. □

Definitions used in HW

Def. A natural number p is a **prime number** provided $p \neq 1$ and the only natural numbers that are factors of p are: 1 and p. A natural number c is a **composite number** provided $c \neq 1$ and c is not a prime number. ⟨The number 1 is neither prime nor composite. In Math 546 you will learn 1 is a unit.⟩ p78

So. A $p \in \mathbb{N}$ is a **prime number** provided $(p \neq 1) \wedge (\forall d \in \mathbb{N})\,[\, d|p \Rightarrow (d = 1 \ \vee \ d = p)\,]$
A $c \in \mathbb{N}$ is a **composite number** provided $(c \neq 1) \wedge (c \text{ is not a prime number})$.
The number 1 is neither prime nor composite.

Division Algorithm (DA) Revisited

Lemma. **Lemma DA**. Fix $s \in \mathbb{Z}$. ⟨s is the *starting* number for the ramainder. In DA, remainder $r \in \{0, 1, \ldots, n-1\}$ so $s = 0$.⟩ 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 $s \le r_1 < s+n$ and $s \le r_2 < s+n$. Then $q_1 = q_2$ and $r_1 = r_2$.

Why? Let the given hold. Note $-n < r_2 - r_1 < n$ since $s \le r_2 < s + n$ and $-s - n < -r_1 \le -s$.
Since $nq_1 + r_1 = nq_2 + r_2$ get $n(q_1 - q_2) = r_2 - r_1$. So $-n < n(q_1 - q_2) < n$. Since $n \neq 0$ get $-1 < q_1 - q_2 < 1$.
Since $q_1 - q_2 \in \mathbb{Z}$, get $q_1 - q_2 = 0$. So $q_1 = q_2$. Since $nq_1 + r_1 = nq_2 + r_2$ we get $r_1 = r_2$.

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

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

Why? The existence part is beyond the scope of this class. For the uniqueness part, let $a = nq_1 + r_1$ and $a = nq_2 + r_2$ for some $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \le r_1 < n$ and $0 \le r_2 < n$. Apply above Lemma DA (with $s = 0$) to get $q_1 = q_2$ and $r_1 = r_2$.

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

Rmk. The equality in (1) can be thought of as $\frac{a}{n} = q + \frac{r}{n}$ (but we do not write like this in our proofs) and so we say: when we divide the a by n, the **quotient** is q and the **remainder** is r. p144

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

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

Why? The existence part follows from Thm. DA. The uniqueness part follows from Lemma DA.

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

Rmk. The integer 0 does not divide any integer. For $n \in \mathbb{Z} \setminus \{0\}$ and $b \in \mathbb{Z}$, 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

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) $(\exists k \in \mathbb{Z})\ [a = b + nk]$

to see (4)⇔(4′) take $j = -k$

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

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′) ⇔ (2′) ⇔ (3′) ⇔ (4′) ⇔ (5′).

▷. You can use (on HW& exams, unless otherwise indicated) any of the above equivalent formations as the definition of $a \equiv b \pmod{n}$.

Thm. Let $n \in \mathbb{N}$ and $a, b, c \in \mathbb{Z}$ ER 11 p98
(1) $a \equiv a \pmod{n}$ (reflexive)
(2) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$. (symmetric)
(3) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$. (transitive)

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

Def. Congruent is a **relation** means that $a \equiv b \pmod{n}$ 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 (3) and (4) hold.

$$a_1 \equiv a_2 \pmod{n} \quad (3)$$
$$b_1 \equiv b_2 \pmod{n} \quad (4)$$

Then the congruences in (5) and (6) hold.

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{n} \quad (5)$$
$$a_1 b_1 \equiv a_2 b_2 \pmod{n} \quad (6)$$

§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.

▷. The below Theorem and Corollary are used often in the homework problems (and you can quote them).

Thm. $(\forall n \in \mathbb{Z})$ [n is even $\Leftrightarrow$ n^2 is even]. Thm3.10 p108

Cor. $(\forall n \in \mathbb{Z})$ [n is odd $\Leftrightarrow$ n^2 is odd]. not in book

§3.3 Proof by Contradiction

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 $\mathbb{R} \setminus \mathbb{Q}$.

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. **Theorem 8.15 (The Fundamental Theorem of Arithmetic/Prime Factorization)** p432
For each $n \in \mathbb{N} \setminus \{1\}$ there exists unique $m \in \mathbb{N}$ ⟨m is the number of primes in the prime factorization⟩ p427
and prime numbers $p_1, p_2, \ldots, p_m$ and 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")

§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. 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

- n is even if and only if $2 \in \{p_1, \ldots, p_m\}$
- n is odd if and only if $2 \notin \{p_1, \ldots, p_m\}$.

Def. For $x \in \mathbb{R}$, the absolute value of x, denoted $|x|$, is p135

$$|x| = \begin{cases} x, & \text{if } x \geq 0 \\ -x, & \text{if } x < 0 \,. \end{cases}$$

§3.5 Division Algorithm/Congruence

Thm. **Thm. 3.31$^+$**. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. p150
There exists $q, r \in \mathbb{Z}$ such that $a = nq + r$ if and only if $a \equiv r \pmod{n}$.
Thinking Land of Proof: $a = nq + r \;\Leftrightarrow\; a - r = nq \;\Leftrightarrow\; n \mid (a - r) \;\Leftrightarrow\; a \equiv r \pmod{n}$.

Rmk. An $a \in \mathbb{Z}^{\geq 0}$ is congruent (modulo n) to the remainder obtained when a is divided by $n \in \mathbb{N}$.

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

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

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

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

TL of Proof: Fix $s \in \mathbb{Z}$. Let $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Apply Thm. DA$^+$ to express $a = nq + r$ for a unique $q \in \mathbb{Z}$ and unique $r \in \mathbb{Z}$ with $s \leq r < s + n$. Then use Thm. 3.31$^+$.

Question: Why is Cor. 3.32$^+$ a corollary to Theorem 3.31$^+$?

Rmk. 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.

Rmk. **Exercise 3.5.5a**. Fix $n \in \mathbb{N}$ and $a \in \mathbb{Z}$. Then $n|a$ if and only if $a \equiv 0 \pmod{n}$. p153
Why? $a \equiv 0 \pmod{n} \;\Leftrightarrow\; n \mid (a - 0) \;\Leftrightarrow\; n|a$.

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 $m \in \mathbb{N}$.

Thinking Lands Rough Outlines

►. Let $P(x)$, $Q(x$, and $R(x)$ be open sentences in the variable x.

$(\forall x \in U)\ [R(x)]$

►. Direct proof §3.1

TL. Let $x \in U$.
We shall show $R(x)$.
⟨Start arguing that $R(x)$ holds.⟩

►. Proof by Contradiction (BWOC stands for by way of contradiction) §3.3

TL. Viewpoint 1.
Fix/let $x \in U$.
We shall show $R(x)$ by contradiction.
BWOC, **assume** $\sim R(x)$.
⟨Start looking for a contradiction.⟩

TL. Viewpoint 2.
We shall show $(\forall x \in U)\ [R(x)]$ by contradiction.
BWOC, **assume** $\sim (\forall x \in U)\ [R(x)]$.
So assume $(\exists x \in U)\ [\sim R(x)]$.
So assume there exists $x \in U$ such that $\sim R(x)$.
⟨Start looking for a contradiction.⟩

▷ Compare Viewpoints 1 and 2. Do you see both viewpoints lead to the same place/assumption?

$(\forall x \in U)\ [P(x) \Rightarrow Q(x)]$

►. Direct proof §3.1

TL. Let $x \in U$.
Let $P(x)$ hold/be-true.
We shall show $Q(x)$ holds/is-true ⟨Start arguing that $Q(x)$ holds.⟩

►. Proof by contrapostive §3.2

TL. Let $x \in U$.
We shall show $P(x) \Rightarrow Q(x)$ by contrapositive.
Thus, we shall show ⟨, usually by direct proof,⟩ that

$$\sim Q(x) \Rightarrow \sim P(x).$$

Let

$$\sim Q(x) \text{ hold/be-true.} \tag{$*$}$$

⟨Start arguing that $\sim P(x)$ holds/is-true.⟩

►. Proof by contradiction §3.3

TL. ⟨Let's use the above Viewpoint 1 from Proof by Contradiction for $(\forall x \in U)\ [R(x)]$, with $R(x)$ being $P(x) \Rightarrow Q(x)$.⟩
Fix/let $x \in U$.
We shall show $P(x) \Rightarrow Q(x)$ by contradiction.
BWOC, **assume** $\sim [P(x) \Rightarrow Q(x)]$ and WantToFind a contradiction.
⟨Think of $\sim [P \Rightarrow Q]$ as a broken promise so $\sim [P \Rightarrow Q] \equiv [P \wedge \sim Q]$.⟩
So we shall **assume** that

$$\sim Q(x) \tag{$*$}$$

AND

$$P(x). \tag{$**$}$$

⟨Now we WantToFind a contradiction.⟩

▷ For $(\forall x \in U)\ [P(x) \Rightarrow Q(x)]$, note similarity in logic between proof by contrapostive & contradiction.