Math 412. Adventure sheet on the Division Algorithm

Let $\mathbb{Z}$ denote the set of all integers. There are at least a couple of related things that we mean by *divides / division* in $\mathbb{Z}$.

Division Algorithm Theorem: Let $n, d \in \mathbb{Z}$ with $d > 0$. There exists *unique* $q, r \in \mathbb{Z}$ such that

$$n = qd + r \qquad \text{and} \qquad 0 \leqslant r < d.$$

DEFINITION: Let $a, b \in \mathbb{Z}$. We say a *divides* b if there exists $q \in \mathbb{Z}$ such that $b = aq$. Equivalently, in this case, we say a is a *divisor* or *factor* of b, or that b *is divisible by* a, and write $a|b$.

A. DIVISION ALGORITHM WARM UP:

(1) Discuss with your team: *You have known the division algorithm since Grade 3. Explain. What did the uniqueness part mean in third grade? What words are used in third grade for q and r?*
(2) Drop the phrase "$0 \leqslant r < d$" from the statement of the theorem. Is it still true? Prove it or find a counterexample.
(3) Discuss with your team: Describe the main scaffolding (outline) of the proof of the Division Algorithm. What are the two main things to show?

B. DIVISOR WARM UP. True or False. Justify.

(1) The integer -4 is a factor of both 24 and 100.
(2) The integer 1 has exactly two divisors.
(3) The integer 0 has exactly one divisor.
(4) The integer 3 is a divisor of 4.
(5) If $n \in \mathbb{Z}$, then 5 divides $5n$.
(6) If $n \in \mathbb{R}$, then 5 divides $5n$.
(7) If a, b, c are integers, $a|b$, and $b|c$, then $a|c$.

C. THE CONNECTION BETWEEN "DIVIDES" AND "DIVISION ALGORITHM:" Let n, d be positive integers, and (using the division algorithm) write $n = qd + r$ where $0 \leqslant r < d$. Then d divides n if and only if $r = 0$.

D. DIVISION ALGORITHM PROOF: EXISTENCE. Let n, d be integers with d positive. Define the set $\mathcal{S}$ as follows:

$$\mathcal{S} := \{n - dx \mid x \in \mathbb{Z} \text{ and } n - dx \geq 0\}.$$

(1) In the special case $n = 17, d = 5$, write out some explicit elements of $\mathcal{S}$. Ditto for $n = -33$ and $d = 8$.
(2) Prove that $\mathcal{S}$ is non-empty.[1]
(3) Explain why $\mathcal{S}$ has a **smallest element.**[2]
(4) Ler r be the smallest element of $\mathcal{S}$. Prove that $r < d$.
(5) Prove the **existence** part of the Division algorithm.

[1]Often, the easiest way to show a set is non-empty is to exhibit an element in it. Also, you can consider the case where $n \geq 0$ and $n < 0$ separately.]

[2]This follows from the obvious but fancy-sounding **Well-Ordering Principle**: every non-empty subset of integers which is bounded below has a minimal element. Like most axioms, this is formalized "common sense."

E. DIVISION ALGORITHM PROOF: UNIQUENESS. Let n, d be integers with d positive. Suppose that $n = qd + r$ and $n = q'd + r'$, where $q, r, q', r' \in \mathbb{Z}$ and $0 \leqslant r, r' < d$.

(1) Show that $d|(r - r')$.
(2) Show that $|r - r'| < d$. [Hint: Start by observing that, without loss of generality, you can assume that $r' \leqslant r$.]
(3) Show that $|d(q - q')| < d$. [Hint: Substitute.]
(4) Show that $|(q - q')| < 1$.
(5) Show that $q = q'$.
(6) Show that $r = r'$.
(7) Explain how Problem D above and your steps here complete the proof of the Division Algorithm.