# Divisibility and the Division Algorithm

MTH 350 -- Module 2A

# Today

- Review: Definition of “divides”, statement of the Division Algorithm
- Proving the Division Algorithm
- Recap and feedback

# Suppose that $x|10$. Then we can conclude:

$10|x$

There exists an integer $y$ such that $y = 10x$

There exists an integer $y$ such that $x = 10y$

There exists an integer $y$ such that $10 = xy$

To 0

There is no such thing as integer division, but we can say when one integer divides another.

# True or false: 0 divides 0.

True

False

Tc 0

# Consider the integers $a = 12$ and $b = 90125$. According to the Division Algorithm,

$12 | 90125$

There exist integers $q, r$ with $90125 = 12q + r$ and $0 \leq r < 90125$, and those integers are unique.

There exist integers $q, r$ with $12 = 90125q + r$ and $0 \leq r < 12$, and those integers are unique.

There exist integers $q, r$ with $90125 = 12q + r$ and $0 \leq r < 12$, and those integers are unique.

There exist integers $q, r$ with $12 = 90125q + r$ and $0 \leq r < 90125$, and those integers are unique.

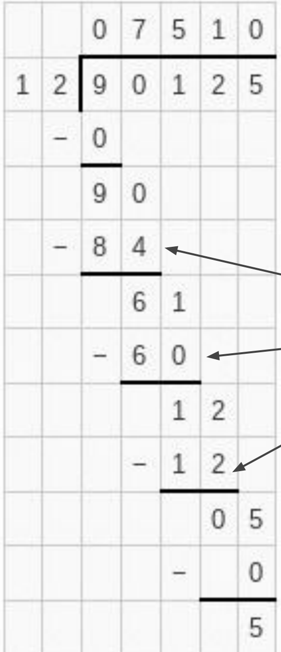
To 0

**The Division Algorithm.** *Let $a$ and $b$ be integers, with $a > 0$. Then there exist unique integers $q$ and $r$ such that*

$$b = aq + r \ \text{ and } \ 0 \le r < a.$$

**Example: If a = 12 and b = 90125, then q = 7510 and r = 5.**

**90125 = (12)(7510) + 5**




This "algorithm" works by ***subtracting off multiples of the divisor*** until we hit the ***smallest quantity possible without going negative*** on the next step. That "smallest quantity" is the remainder.

The Division Algorithm is a top-5 math result in terms of importance. Let’s prove it!

**The Division Algorithm.** *Let $a$ and $b$ be integers, with $a > 0$. Then there exist unique integers $q$ and $r$ such that*

$$b = aq + r \ \ \textit{and} \ \ 0 \leq r < a.$$

Start by assuming a,b are integers and a > 0.

We need to prove:

1. The EXISTENCE of integers q and r that satisfy BOTH b = aq + r, AND 0 ≤ r < a; and
2. The UNIQUENESS of those integers. (Which means…?)

# Consider the set $\{12q+3 \ : \ q \in \mathbb{N}\}$. According to the Well Ordering Principle,

- This set is infinite
- This set is nonempty
- This set has a smallest element
- This set can be written in numerical order
- (Trick question -- the Well Ordering Principle alone doesn't tell us anything about this set)

To 0

# In your groups:

Look at the set: $S = \{x \in \mathbb{Z} : x \geq 0 \text{ and } x = 1000 - 22m$

$\text{for some } m \in \mathbb{Z}\}$

Example: 956 is an element of S, because 956 is an integer, and 956 = 1000 - 22(2).

- Does S have a smallest element? If so, what is it, and what is the value of "m" that will produce it?
- Long-divide 1000 by 22 and note the quotient and remainder. Notice anything?

# Proving the existence part of the Division Algorithm

# Existence of q, r

Let a, b be integers with a > 0. We want to show that there exist integers q, r such that b = aq + r and 0 ≤ r < a.

Define the set S: $S = \{x \in \mathbb{Z} : x \geq 0 \text{ and } x = b - am \text{ for some } m \in \mathbb{Z}\}$

The set S is a subset of the integers by definition, but in fact it is a subset of the *whole numbers* because….

We will now show that S is always nonempty regardless of the choice of a and b. Consider two cases: b ≥ 0, and b < 0.

If b ≥ 0, then S is nonempty because ____ is an element of S by setting m = 0.
If b < 0, then -b ___ 0. Since a > 0 and a is an integer, a ≥ ___. Multiply both sides of this inequality to get -ab ≥ ___. This is equivalent to _______ ≥ 0. By setting m = ____ we now see that the nonnegative integer ______ belongs to S, so S is nonempty in this case too.

Because S is a nonempty subset of the whole numbers, S _____________________________________.

# Existence of q, r continued

$$S = \{x \in \mathbb{Z} \,:\, x \geq 0 \text{ and } x = b - am \text{ for some } m \in \mathbb{Z}\}$$

Let *r* denote the smallest element of S. Since *r* is an element of S, there is an integer q such that r = ___ - _____. This is equivalent to ____ = ______+ ____.

Thus we have found integers q, r such that….

Next we need to show that……

We'll do this by contradiction. Assume to the contrary that….

If that's the case, then r - a ≥ ___. However note that r - a = (________) - a = ___ - a(___________) . Since r ≥ ___ and there exists an integer m (namely m = ____________) with r - a = b - am, this means that….

Hence r-a is an element of ___. But r-a is _______ _____ r, which is a contradiction because….

# What about uniqueness?

**Generally speaking:** When we have proven that “X” is **unique** with respect to some property or characteristic, we mean that “X” is **the only object of its kind** that has that property or characteristic.

**Strategy for proving uniqueness:** Suppose “X” and “Y” are two objects that have the property or characteristic. Show that $X = Y$.

**In the Division Algorithm:** We’ve shown the *existence* of q and r that satisfy both the equation $b = aq + r$ and the inequality $0 \leq r < a$. Now suppose q’ and r’ are two other integers with $b = aq' + r'$ and the inequality $0 \leq r' < a$. **Show that $q = q'$ and $r = r'$**

# Recap

- **Definition of “divides”:** Does not involve or introduce division! Is really a statement about multiplication.
- **Division Algorithm:** Is neither an algorithm nor a statement about division! Not every pair of integers will divide each other, but you will always be able to find a quotient and a remainder, and the result is unique.
- **Proof of the DA:** Involves subtracting multiples of the divisor off of the dividend and recording the results in a set, which must have a least element.

NEXT UP: Integer congruence

Feedback:

**http://gvsu.edu/s/1zN**