Integers

4.3

Background

- In this topic we'll learn/review more properties of integer values

- We already know at least two ways to categorize integers:

  1. Odd vs. Even (a partitioning!)

  2. Negative, zero, positive (another partitioning!)

Another Partitioning: Prime Numbers

Definition: *Factor*

j is a factor of i when $i \,\%\, j = 0$ (or, $j \mid i$), $i, j \in \mathbb{Z}^+$

Definition: *Prime*

p is prime if $p \geq 2$ and its factors are 1 and p.

Definition: *Composite*

p is composite if $p \geq 2$ and p is not prime.

Example:

11 - prime

89 - prime

$51 = 3 \cdot 17$ - Composite

$91 = 7 \cdot 13$ - Composite

Playposit

Which of the following are primes?

- 21
- 17
- 9
- 31
- 43

Fundamental Theorem of Arithmetic

Theorem: (The fundamental Theorem of Arithmetic)

If p is a positive integer ≥ 2, p is prime or can be expressed as the product of multiple primes.

Proof: Rosen p. 288 (contradiction) & 357 (induction)

Example:

$$36 = 2 \cdot 2 \cdot 3 \cdot 3 = 2^2 3^2$$

Definition: *Prime Factorization*

The prime factorization of a composite integer p is the expression of p as the product of 2 or more $primes$

Playposit

What is the prime factorization of 60?

A. $2 * 30$

B. $2^2 * 3 * 5$

C. $4 * 15$

D. $2^2 * 15$

Another Prime/Composite Theorem

Theorem: If n is composite, n has at least one prime factor no larger than $\sqrt{n}$

Proof (direct): Assume n is composite.

Therefore, it has two factors x and y such that $1 < x, y < n$ and $xy = n$

$n = \sqrt{n} \cdot \sqrt{n}$, meaning that $x \leq \sqrt{n}$ or $y \leq \sqrt{n}$ (or both).
WLOG, let $x \leq \sqrt{n}$

x is either prime or composite. If x is prime, x is a prime factor of n and $x \leq \sqrt{n}$, completing the proof.

(Continues…)

Another Prime/Composite Theorem

Proof (direct): (continued)

If x is composite, it is the product of primes (by the FToA) and again n has a prime factor that is $\leq \sqrt{n}$.

Therefore, if n is composite, n has at least one prime factor no larger than $\sqrt{n}$.

Example: Is 161 prime? (Does 161 have a prime factor $\leq \sqrt{161}$?)

$\sqrt{161} \approx 12.7 \Rightarrow$ We need only test 2, 3, 5, 7 & 11

161/7 = 23; Therefore 161 is not prime.

(161 is a 2-prime or semi prime - a product of just two primes)

How Many Primes Exist?

Conjecture: There are infinitely many prime integers

Proof (Contradiction):

Assume there are a finite number of primes. Label them $p_1, p_2, \ldots, p_n$.

Let $Q = \prod_{i=1}^{n} p_i + 1$. By the FToA, Q is either prime or composite.

If Q were prime, we'd have labeled it. Thus Q is composite.

As Q is composite, at least one of the primes must divide Q evenly.

Say that p_j does. That is, $p_j \mid Q$ or $p_j \mid \left(\prod_{i=1}^{n} p_i + 1 \right)$.

(Continues…)

How Many Primes Exist?

Useful fact: If $c \mid (a+b)$ **and** $c \mid a$, then $c \mid b$.

Proof (Contradiction): (continued)

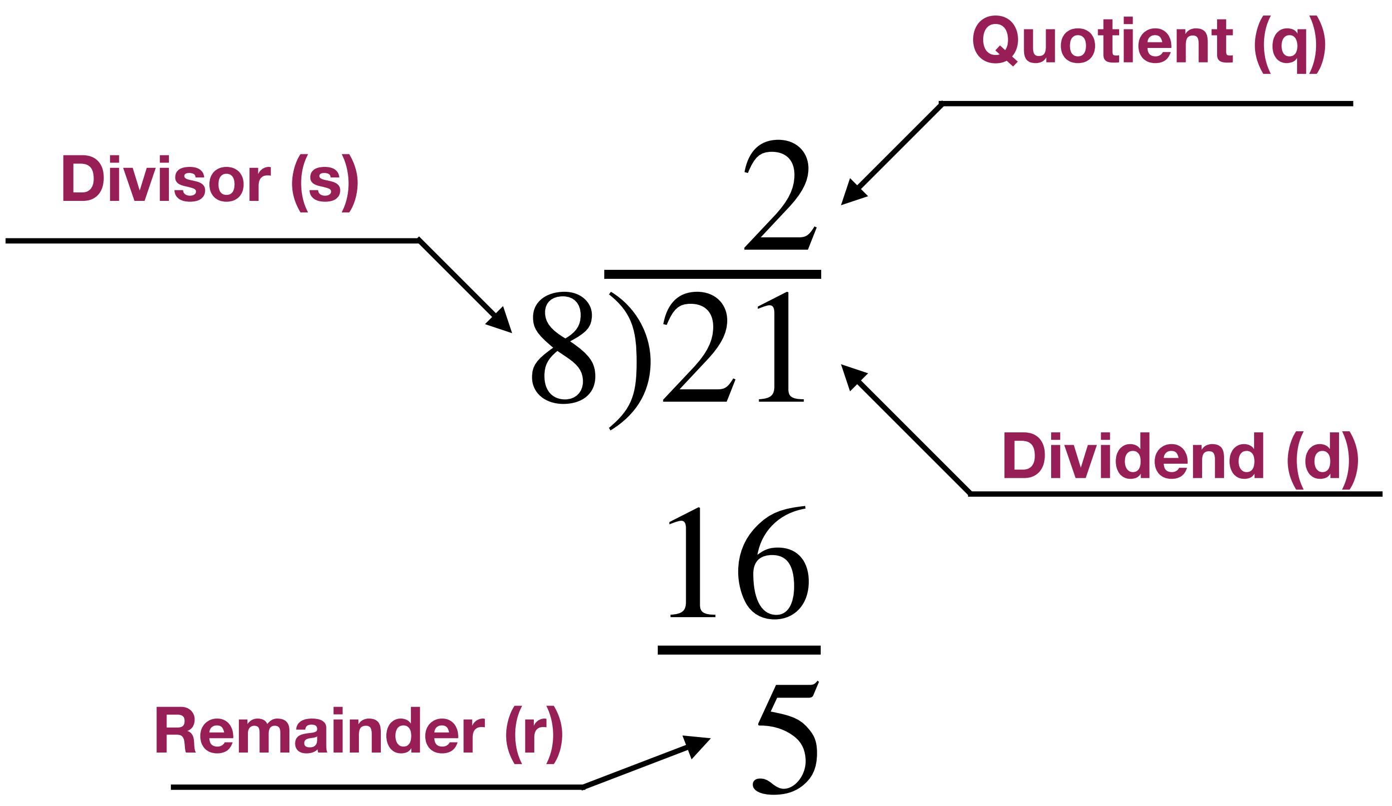
We know that $p_j \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$. It follows that $p_j \mid 1$ must be true (*) but that is impossible: $p_j > 1$!

Thus Q cannot be composite; it must be prime. This contradicts our earlier assumption that Q is composite.

Therefore, there are infinitely many prime integers.

(*) because if $c \mid (a+b)$ and $c \mid a$, then $c \mid b$.

Division



$$d = s \cdot q + r$$

Division Algorithm (not really an algorithm)

Definition: *Division 'Algorithm'* $[n = sq + r]$

If $n \in \mathbb{Z}, s \in \mathbb{Z}^+$, and $0 \leq r < s$, then q and r are unique

Example:

Find q and r when $n = -17$ and $s = 4$.

$-17 = 4(-6) + 7$ $r > s$

$-17 = 4(-5) + 3$ $0 \leq r < s$

$-17 = 4(-4) + -1$ $r < 0$

Greatest Common Divisor (GCD)

Definition: *Greatest Common Divisor* $[gcd(x, y) = i]$

Let $x, y, i \in \mathbb{Z}^+$. The GCD of x and y is the largest number i such that $i \mid x$ and $i \mid y$.

Example:

$18 = 2^1 3^2$

$60 = 2^2 3^1 5^1$

GCD(18,60) -> All shared prime factors

$GCD(18,60) = 2^1 3^1 = 6$

Definition: *Relatively Prime*

If the GCD of a and b is 1, a and b are relatively prime

Playposit

What is the greatest common divisor of 36 and 54?

A. 3
B. 2
C. 6
D. 9
E. 18

Greatest Common Divisor (GCD)

Definition: *Pairwise Relatively Prime*

When the members of a set of integers are all relatively prime to one another, they are pairwise relatively prime

Example:

Consider 31, 43, and 12.

$GCD(31,43) = 1$ 31 **- Prime**

$GCD(31,12) = 1$ 43 **- Prime**

$GCD(12,43) = 1$ $12 = 2^2 3^1$

Least Common Multiple (LCM)

Definition: *Least Common Multiple* $[lcm(x, y) = s]$

Let $x, y, s \in \mathbb{Z}^+$. The LCM of x and y is the smallest integer s such that $x \mid s$ and $y \mid s$.

Example:

$$18 = 2^1 3^2$$

LCM(18,60) -> All unshared prime factors and highest exponent of shared factors

$$60 = 2^2 3^1 5^1$$

$$LCM(18{,}60) = 2^2 3^2 5^1 = 180$$

Least Common Multiple (LCM)

Example:

At your house, the garbage is collected once a week. A new five gallon bottle of water is delivered every 10 days, and your spouse insists that you vacuum the living room every 5 days. Yesterday all three occurred on the same day.

How often does this happen?

Answer: Every $lcm(7,10,5) = 2 \cdot 5 \cdot 7 = 70$ days

Playposit

What is the least common multiple of 36 and 54?

A. 54

B. 108

C. 72

D. 1944

Another Theorem

Theorem: If $a, b \in \mathbb{Z}^+$, then $ab = gcd(a,b) \cdot lcm(a,b)$

Proof (direct): Consider the prime factorizations of a and b.

The LCM is the product of the terms with the larger exponents and all terms that aren't shared.

The GCD is the product of the remaining terms.

Thus the product of the LCM and the GCD is the product of all terms in the prime factorizations.

Therefore if $a, b \in \mathbb{Z}^+$, then $a, b = gcd(a,b) \cdot lcm(a,b)$

This theorem is useful if you need to know both the GCD and LCM of the same pair of values

Congruences

Definition: *Congruent Modulo m*

If $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, then a and b are congruent modulo m (written $a \equiv b \pmod{m}$) **iff** $a \,\%\, m = b \,\%\, m$ (or **iff** $m \mid (a - b)$)

Example:

Is 37 congruent to 21 modulo 8

$37 \,\%\, 8 = 5 \quad (37 = 8 \cdot 4 + 5)$

$21 \,\%\, 8 = 5 \quad (21 = 8 \cdot 2 + 5)$

$8 \mid (37 - 21) \Rightarrow 8 \mid 16 =$ **True**

Example

- Find 2 integers that are congruent to 11 modulo 5
- $11 \% 5 = 1$ $\qquad 11 = 5(2) + 1$
- $6 \% 5 = 1$ $\qquad 6 = 5(1) + 1$
- $21 \% 5 = 1$ $\qquad 21 = 5(4) + 1$

Congruences

Example:

1. Time: 45 minutes from 2:35 pm
   - 35+45 = 80 and 80 % 60 =20
   - Thus, the time will be 3:20 pm
   - (80 and 20 are congruent modulo 60)

---

2. Psuedo-random number generating functions
   - Ex: $x_{n+1} = (a \cdot x_n + c) \,\%\, m$ where $a \geq 2$ and $0 \leq c, x_0 < m$
   - This is a *Linear Congruential Function*

Playposit

Which of the following are congruent to 23 modulo 7?

- 30
- 15
- 54
- 72
- 34