Topic 10:

Integers

Background

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

We already know at least two ways in which to categorize integers:

Prime Numbers

Definition: Factor

Definition: Prime

Definition: Composite

Example(s):

From the 'Is This a Great Name or What?' Dept.

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.

Example(s):

Definition: Prime Factorization

. . . .

Another Prime/Composite Theorem (1 / 2)

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

Another Prime/Composite Theorem (2 / 2)

Extra room for the proof:

Example(s):

Dear Euclid: How Many Primes Exist? (1 / 2)

Theorem: **There are infinitely many prime integers.**

Dear Euclid: How Many Primes Exist? (2 / 2)

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

Extra room for the proof:

Mersenne Numbers (1 / 2)

- The n^{th} Mersenne Number is $2^n - 1$ (1, 3, 7, 15, ...).
- If n is composite, $2^n - 1$ can't be prime.
  - Why not? As $n = ab$, $2^n - 1 = 2^{ab} - 1$, which is a binomial number and so it has $2^a - 1$ as a factor.
- If n is prime, $2^n - 1$ might be prime. $(2^{11} - 1 = 23 \cdot 89)$
  - If so, it's called a *Mersenne Prime*.
  - Only a few dozen such primes have been found.

So ... what's the big deal?

Mersenne Numbers (2 / 2)

- There exist efficient tests for the primality of Mersenne numbers (e.g., the Lucas–Lehmer test).
- The GIMPS project uses spare CPU cycles to find Mersenne primes.
  - Curious? Visit: www.mersenne.org

Division

Name the parts!

$$\begin{array}{r} 2 \\ 8 \,\big/\, \overline{21} \\ 16 \\ \hline 5 \end{array}$$

Too Bad This Isn’t Really An Algorithm

Definition: Division ‘Algorithm’

Example(s):

Greatest Common Divisor (GCD) (1 / 2)

Definition: Greatest Common Divisor

Example(s):

Definition: Relatively Prime

Greatest Common Divisor (GCD) (2 / 2)

Definition: Pairwise Relatively Prime

Example(s):

Least Common Multiple (LCM) (1 / 2)

Definition: Least Common Multiple

. . . .

. . . .

Example(s):

Least Common Multiple (LCM) (2 / 2)

Example(s):

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 five days. Yesterday, all three occurred on the same day. How often does that happen?

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 GCD terms is the product of all terms in the prime factorizations.

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

Congruences (1 / 3)

It is pitch black. You are likely to be eaten by a . . .

Congruences (2 / 3)

(Review from Topic 1.)

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(s):

Congruences (3 / 3)

Example(s):