Announcements

- Homework #3 due tomorrow
- Midterm #1 is on March 12^{th} (Two weeks.)

Recall: Fundamental Theorem of Arithmetic (Unique Prime Factorization Theorem)

Theorem: For any $n \in \mathbb{N}$, n can be expressed as the product of primes in a **unique** way.

In proofs, we will write:

$$n = p_1^{e1} \times p_2^{e2} \times p_3^{e3} \times \ldots \times p_k^{ek}$$

Examples

Proofs using the F.T.O.A.

- Claim: $(\forall a \in \mathbb{N}^{+})(\forall q \in \mathbb{N}^{prime})$ [$q|a^2 \rightarrow q|a$]
- Claim: $\sqrt{3} \notin Q$

Modular Congruence

- "a *mod* n" represents the remainder when *a* is divided by *n*
  (Similar to Java: a%n, but different when *a* is negative)

- a = b (*mod* n)   means: a *mod* d = b *mod* n

- Better notation:
  $a \equiv_n b$

- We say "a is congruent to b mod n"

- Examples.

Equivalently…

Claim: For all a, b$\in \mathbb{N}$, the following are equivalent:

1. $a \equiv_n b$
2. $n|(a - b)$
3. $(\exists k \in \mathbf{Z})\ [a = b + kn]$

(We will prove this later, but let's talk about it…)

Modular Arithmetic Theorem

Theorem: Let a, b, c, d, n $\in$ Z, and n > 1. Suppose a $\equiv_n$ c and b $\equiv_n$ d. Then:

1. $(a + b) \equiv_n (c + d)$
2. $(a - b) \equiv_n (c - d)$
3. $ab \equiv_n cd$
4. $a^m \equiv_n c^m$ for all integers m

Using the Modular Arithmetic Theorem

- Examples.

- Claim: For all natural numbers, n: n is divisible by 3 if and only if the sum of the digits of n is divisible by 3.