Math 55 Lecture 7 §4.3, start 4.4

Def: A positive integer p greater than 1 is **prime** if

Recall: (★) If $a|b$ and $a|c$ then

Theorem: There are infinitely many primes.

Proof:
Assume there are only finitely many primes

Consider the pos. number

Def: Let $a, b \in \mathbb{Z}$. The largest integer d s.t. $d|a$ and $d|b$ is called the

Ex:

Def: Integers a, b are relatively prime if

Def: Integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if

To calculate gcd of a and b,

Q:

Algorithm: If $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ are prime factorizations, then
$\gcd(a, b) =$

Def: The least common multiple $\operatorname{lcm}(a, b)$ of pos. integers a and b is the

Algo: If $a = p_1^{a_1} \cdots p_n^{a_n}$ and $b = p_1^{b_1} \cdots p_n^{b_n}$ as before,
$\operatorname{lcm}(a,b) =$

Ex:

Exercise: Let $a, b \in \mathbb{Z}^+$. Then
$ab =$

Euclidean algo: Divide larger # by smaller, then smaller by remainder, then

Example:

Euclidean algo works because of

Lemma: Let $a = bq + r$ where $a, b, q, r \in \mathbb{Z}^+$. Then

Pf: Enough to show that every common factor of a and b is

Suppose d divides a and b. Then

Suppose d divides b and r. Then

$\therefore$ a and b have the same common factors that

Bezout's Theorem: If $a, b \in \mathbb{Z}^+$, there exist $s, t \in \mathbb{Z}$ s.t.

To find s and t, go backwards through Euclidean algo:

Ex:

Euclid. algo: ①
②
③
④

Step ③ $\Rightarrow$
Step ② $\Rightarrow$
Step ① $\Rightarrow$

Lemma 1: If $a, b, c \in \mathbb{Z}^+$ s.t. $\gcd(a,b) = 1$ and $a \mid bc$, then

Pf: Since $\gcd(a,b) = 1$, Bezout $\Rightarrow$

Cor: If p prime, and $p \mid a_1 a_2 \ldots a_n$ (where $a_i \in \mathbb{Z}$) then

Fund Thm of Arithmetic: Each $n \in \mathbb{Z}^+$ can be written uniquely as
$n =$

We'll prove that each n has at most one such expression. (rest of proof - later)

Pf: (Contradiction)
Suppose n can be written

§4.4 Inverses

Def: If $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, we say x is

Notation for 'inverse':

Thm: If $\gcd(a, m) = 1$, $m \in \mathbb{Z}^+$, then

Furthermore, it is

Pf: