Tuesday, September 17

- Homework #0 due Thursday
- After class, I'll post solutions to today's group work, as well as Homework #1 (due next Tuesday)

Fundamental Theorem of Arithmetic: Every integer $n \geq 2$ can be written as a product of (one or more) primes; moreover, this factorization is unique up to reordering the primes.

Proof: Existence – use strong induction on n. Base case $n=2$: 2 is prime, so done.

Inductive step: Suppose $n > 2$. If n is prime, then we're done. Otherwise n is composite; then we can write $n = ab$ with $1 < a, b < n$. By induction hypothesis, $a = p_1 p_2 \cdots p_k$ and $b = q_1 q_2 \cdots q_\ell$ where p_i, q_j are prime. Then

$$n = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_\ell$$ is a product of primes.

Proof of uniqueness: By contradiction.

If not, let n be the smallest integer ≥ 2 with non-unique factorization.

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l.$$

Note $p_1 \mid n \Rightarrow p_1 \mid q_1 q_2 \cdots q_l$.

By Euclid's lemma (extended via induction to l factors), $p_1 \mid q_j$ for some $1 \leq j \leq l$. Without loss of generality, $p_1 \mid q_1 \Rightarrow p_1 = q_1$.

Then $m = p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l$ is a smaller integer with non-unique factorization, which is a contradiction. //

Theorem: There are infinitely many primes.

Proof: We'll show that any finite set of primes excludes some prime. Let $\{p_1, p_2, \ldots, p_k\}$ be primes, and set

$$N = p_1 p_2 \cdots p_k + 1.$$

$N \geq 2 \Rightarrow N$ is divisible by some prime p. (by Fund. Thm. of Arith.) Note: division algorithm with N and p_1 yields

$$N = p_1 (p_2 \cdots p_k) + 1$$

$\Rightarrow p_1 \nmid N$.

Similarly $p_2, p_3, \ldots, p_k \nmid N$.

Thus $p \neq p_1, \ldots, p \neq p_k$. //