Math 330: Intro to Higher Math, Section 1, Spring 2009 — Homework # 13, due March 25

Definition. Let n be an integer greater than 1, i.e., $n \in \mathbb{Z}$ and $n > 1$. We say that n *is prime* (or equivalently that n *is a prime number*) if n is only divisible by 1, -1, n, and $-n$.

Lemma 1. *Let $n \in \mathbb{Z}$ and $n > 1$. If n is not prime then there exist $x, y \in \mathbb{N}$ such that $1 < x < n$, $1 < y < n$, and $n = xy$.*

Proposition 2. *Every integer greater than 1 is either a prime or a product of primes.*

Hint. Use strong induction and lemma 1. □

Theorem 3. *There are infinitely many prime numbers.*

Hint. If there were only finitely many prime numbers, say $p_1, p_2, \ldots, p_s$, then $n = p_1 p_2 \cdots p_s + 1$ would contradict proposition 2. □

Problem 4. *Given any finite set of primes, the proof of theorem 3 provides a method for finding primes that do not belong to the given set.*

(1) *Use this method to find a prime different from 2, 3, 5, and 7.*
(2) *Use this method to find a prime different from 2, 5, and 11.*

Proposition 5. *For every $m, n \in \mathbb{N}$ there exists $d \in \mathbb{N}$ such that:*

(1) *d divides m and d divides n;*
(2) *for all $c \in \mathbb{Z}$, if c divides m and c divides n, then c divides d and $c \leq d$.*

The natural number d is called the *greatest common divisor* of m and n and is denoted $\gcd(m, n)$.

Hint. Consider $A = \{\, a \in \mathbb{N} \mid \exists\, x, y \in \mathbb{Z} \text{ s.t. } a = mx + ny \,\}$. Verify that A is not empty. So, by the well-ordering principle, A has a least element. Define d to be the least element of A.

In order to prove that d divides m, apply the division theorem to get $m = dq + r$ with $0 \leq r < d$; now use the fact that d is the least element of A to conclude that $r = 0$, i.e., that d divides m. □

Theorem 6 (Euclid's Lemma)**.** *Let m and n be natural numbers and p be a prime. If p divides mn then p divides m or p divides n.*

Hint. Apply proposition 5 to m and p, and consider $d = \gcd(m, p)$. Given that p is prime, what can d possibly be? □

Corollary 7. *Let $s \in \mathbb{N}$, and let $n_1, n_2, \ldots, n_s$ be natural numbers and p be a prime. If p divides $n_1 n_2 \cdots n_s$ then p divides n_i for some i with $1 \leq i \leq s$.*

Hint. Use induction on s and theorem 6. □

Proposition 8. *Let $s, t \in \mathbb{N}$, and let $p_1, p_2, \ldots, p_s$ and $q_1, q_2, \ldots, q_t$ be primes such that $p_1 \leq p_2 \leq \ldots \leq p_s$ and $q_1 \leq q_2 \leq \ldots \leq q_t$. If $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$ then $s = t$ and for all i with $1 \leq i \leq s = t$ we have $p_i = q_i$.*

Notice that in particular proposition 8 implies that the factorization in proposition 2 is unique.

Hint. Use induction on either s or t and corollary 7. □

Lemma 9. *Let p be a prime and j be an integer such that $0 < j < p$. Then p divides $\binom{p}{j}$.*

Hint. Use corollary 7. □

Theorem 10 (Fermat's Little Theorem)**.** *For every prime p and every natural number n, p divides $n^p - n$.*

Hint. Fix p and use induction on n, the binomial theorem, and lemma 9. □

Problem 11. *Show that the conclusion of theorem 10 is false if p is not a prime.*

Corollary 12. *For every prime p and every natural number n, if $\gcd(p, n) = 1$ then p divides $n^{p-1} - 1$.*

Problem 13. *Show that the conclusion of corollary 12 is false if $\gcd(p, n) \neq 1$.*