MAT 160, PROBLEM SEMINAR, WEEK OF 3/8/99

PROBLEM SET 7: INTEGERS AND DIVISIBILITY

You need to know the following facts for this set of problems. In what follows, by an *integer* we mean an element of the set $\{0, 1, 2, 3, \dots\}$.

• We say that an integer n *divides* an integer m, or that m is *divisible by* n, if $m = nk$ for some integer k. In this case we write $n|m$. n is also called a *divisor* of m. For example, $3|12$, $5|235$, $n|0$ and $n|n$ for all integers n.

• An integer $p \geq 2$ is called a *prime* if p and 1 are the only divisors of p. For example, 2, 11, 37 are primes while 35 is not, since both 5 and 7 divide 35. Note that 2 is the only even integer which is also prime.

• **Fundamental Theorem of Arithmetic.** Every integer $n \geq 2$ is either a prime or else can be written as a product of (not necessarily distinct) primes. Modulo the order in which the primes appear, there is exactly one way to decompose an integer into primes.

For example, $24 = 2 \times 2 \times 2 \times 3$, $3381 = 3 \times 7 \times 7 \times 23$.

In a fancier language, the theorem says: Every integer $n \geq 2$ can be written as

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where $p_1 < p_2 < \cdots < p_k$ are primes, each power a_j is at least 1, and $k \geq 1$. This decomposition is unique in the sense that if we have another decomposition

$$n = q_1^{b_1} q_2^{b_2} \cdots q_m^{b_m}$$

into primes $q_1 < q_2 < \cdots < q_m$, then $k = m$, $p_j = q_j$ and $a_j = b_j$ for all $j = 1, 2, \dots, k$.

• **Division Algorithm.** Given integers n, k, you can divide n by k to get a *quotient* q and a *remainder* r:

$$n = qk + r, \qquad 0 \leq r < k.$$

q are r are uniquely determined by n and k. It is easy to see that n is divisible by k if and only if the remainder r is zero.

• For integers n, m, k, we say that n *is congruent to* m *modulo* k if n and m have the same remainder when we divide them by k. In this case we write $n \equiv m \pmod{k}$. For example, $16 \equiv 0 \pmod{4}$, $22 \equiv 4 \pmod{6}$, and $51 \equiv 2 \pmod{7}$.

An equivalent definition is the following (which is often easier to apply): $n \equiv m \pmod{k}$ if and only if k divides the difference $n - m$. This relation $\equiv$ has the following property: If $n \equiv m \pmod{k}$ and $n' \equiv m' \pmod{k}$, then

$$n + n' \equiv m + m' \pmod{k}$$

and also

$$nn' \equiv mm' \pmod{k}$$

Problem 43. (a) If an integer n is not divisible by 3, is it possible that $2n$ be divisible by 3?
(b) If the number $15n$ is divisible by 6, must n be divisible by 6?

Problem 44. Let p and q be distinct primes. The number pq has 4 divisors: $1, p, q, pq$. Similarly, p^2q has 6 divisors: $1, p, p^2, q, pq, p^2q$. Generalizing this, can you find the number of divisors for $p^n q^m$, where $n \geq 1, m \geq 1$? Can you find the number of divisors for $p^n q^m h^k$, where now p, q, h are distinct primes? Can you guess an algorithm for finding the number of divisors of *any* integer? (*Hint*: For the last part, use the Fundamental Theorem of Arithmetic.)

Problem 45. Find all integers n, m which satisfy $n^2 - m^2 = 37$. (*Hint*: Note that $n^2 - m^2 = (n+m)(n-m)$.)

Problem 46. For any integer n, prove that $n(n+1)(n+2)$ is divisible by 6. (*Hint*: Of course you can use induction on n. But it is also possible to show directly that $n(n+1)(n+2)$ is divisible by both 2 and 3.)

Problem 47. What is the rightmost decimal digit of the number 7^{45}? (*Hint*: The rightmost decimal digit of an integer is the remainder that you get when you divide the integer by 10. Use congruences modulo 10 to determine this remainder.)

Problem 48. Prove that for any integer n, the number $n^3 + 2n$ is always divisible by 3. (*Hint*: Again, you could use induction on n, but better consider the remainder of n by 3 and use congruences modulo 3.)

Problem 49. Let n be an integer which is not divisible by any of the integers between 2 and $\sqrt{n}$ (inclusive). Prove that n must be a prime.