Problem 11) This problem is easily solved by invoking the fundamental theorem of arithmetic at the outset. Since any integer can be decomposed into a unique product of its prime factors, if the product $n_1 n_2 \cdots n_k$ contains the prime number p (or an integer power of p) in its decomposition, then p must belong to at least one of the constituents $n_1, n_2, \cdots, n_k$ of the product. This completes the proof of Euclid's lemma. Note that our proof of the fundamental theorem given in Problem 10 in no way depends on the present problem. Of course, if one were to invoke Euclid's lemma in proving the fundamental theorem, as is often the case, then a different proof of Euclid's lemma would be called for, i.e., one that did *not* rely on the fundamental theorem.

a) We prove a generalized version of Euclid's lemma without invoking the fundamental theorem. In this version, the product of two positive integers n_1 and n_2 is assumed to be divisible by a positive integer n; that is, $n_1 n_2 = mn$, where m is a positive integer. Assuming that n shares no common factors with n_1, the lemma states that n must divide n_2.

Proof: Suppose the lemma holds for all integers up to $n_1 n_2$. In other words, let $n_1 n_2$ be the smallest integer for which the lemma fails for at least one allowed combination of the involved integers n, n_1, n_2.

Case i) If $n < n_1$, subtracting nn_2 from both sides of the equation $n_1 n_2 = mn$ yields

$$n_1 n_2 - nn_2 = mn - nn_2 \quad \rightarrow \quad (n_1 - n)n_2 = (m - n_2)n. \tag{1}$$

Clearly, $0 < (n_1 - n)n_2 < n_1 n_2$ and n does not share a common factor with $n_1 - n$ (because, otherwise, that common factor would have to be shared with n_1 as well). Therefore, by the assumption that $n_1 n_2$ is the *smallest* integer for which the lemma fails, n must divide n_2.

Case ii) If $n > n_1$, subtracting mn_1 from both sides of the equation $n_1 n_2 = mn$ yields

$$n_1 n_2 - mn_1 = mn - mn_1 \quad \rightarrow \quad n_1(n_2 - m) = m(n - n_1). \tag{2}$$

Clearly, $0 < n_1(n_2 - m) < n_1 n_2$ and $n - n_1$ does not share a common factor with n_1 (because, otherwise, that common factor would have to be shared with n as well). Consequently, by the assumption that $n_1 n_2$ is the *smallest* integer for which the lemma fails, $n - n_1$ must divide $n_2 - m$; that is, $n_2 - m = \nu(n - n_1)$, where ν is a positive integer. Multiplying both sides of this equation by n_1 and comparing the result with Eq.(2), we find that $m = \nu n_1$. Substituting for m into the equation $n_1 n_2 = mn$, we finally arrive at $n_2 = \nu n$, confirming that indeed n divides n_2.

In the special case when n is a prime number p, the assertion that n and n_1 share no common factors is equivalent to stating that p does *not* divide n_1. Therefore, if $n_1 n_2$ happens to be divisible by p while n_1 is not, then p must be a divisor of n_2.

b) Since $n_1 n_2 \cdots n_k$ is divisible by p, the proof in part (a) ensures that if n_1 is not divisible by p then the product $n_2 n_3 \cdots n_k$ must be a multiple of p. In the latter case, if n_2 is not a multiple of p, then the product $n_3 \cdots n_k$ must be a multiple of p. Continuing in this way, we see that at least one of the integers $n_1, n_2, \cdots, n_k$ must be divisible by p.