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 done, then a different proof of Euclid's lemma would be called for, i.e., one that did *not* rely on the fundamental theorem.)

The following proof of Euclid's lemma, while slightly more complicated than the aforementioned proof, is instructive in its own way—despite the fact that it continues to rely on the fundamental theorem.

a) Let $n_1 = \mu_1 p + \nu_1$, where $\mu_1 \geq 0$ and $0 \leq \nu_1 < p$. Similarly, let $n_2 = \mu_2 p + \nu_2$, with $\mu_2 \geq 0$ and $0 \leq \nu_2 < p$. Here, the parameters $\mu_1, \nu_1, \mu_2, \nu_2$ are integers. We will have

$$n_1 n_2 = \mu_1 \mu_2 p^2 + (\mu_1 \nu_2 + \mu_2 \nu_1) p + \nu_1 \nu_2.$$

Since, by assumption, $n_1 n_2$ is divisible by p, the product $\nu_1 \nu_2$ is either zero or is itself divisible by p. If $\nu_1 \nu_2$ happens to be zero, then $\nu_1 = 0$, in which case n_1 is divisible by p, or $\nu_2 = 0$, in which case n_2 is divisible by p, or $\nu_1 = \nu_2 = 0$, in which case both n_1 and n_2 are divisible by p. However, if it turns out that $\nu_1 \nu_2 \neq 0$, then, given that ν_1 is less than p, its decomposition into a product of prime factors cannot contain p. Similarly, the decomposition of ν_2 cannot contain p as a prime factor. Consequently, the fundamental theorem of arithmetic informs us that $\nu_1 \nu_2$ cannot contain p in its prime decomposition, which means that $\nu_1 \nu_2$ is not divisible by p, thus contradicting the initial assumption that $n_1 n_2$ is divisible by p.

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.