Theorems (NIB) 1, 2, and 3 (to be inserted in Section 4.3 of the textbook)

Theorem (NIB) 1: For all integers $n > 1$ and for all prime numbers p, p is a divisor of n if, and only if, p appears as a prime factor in the Unique Prime Factorization of n (from the Unique Factorization Theorem, Theorem 4.3.5).

Proof: Let n be any integer such that $n > 1$ and suppose p is any prime number.

[We first prove that if p is a divisor of n, then p appears as a prime factor in the Unique Prime Factorization of n.]

Suppose that p is a divisor of n.

Then, by definition of "divisor", there exists an integer l such that $n = p\,l$.

If $l = 1$, then $n = p$, and so, "$n = p^1$" is the Unique Prime Factorization of n, so p is a factor in the Unique Prime Factorization of n.

Assume, then, that $l \neq 1$ and since n and p are both positive, $l > 1$.

By the UFT, (i.e., by Theorem 4.3.5), l has a Unique Prime Factorization, i.e., there is some positive integer k and prime numbers $p_1, p_2, p_3, \ldots, p_k$ and positive exponents $e_1, e_2, e_3, \ldots, e_k$ such that

$l = p_1^{e_1}\, p_2^{e_2}\, p_3^{e_3} \ldots p_k^{e_k}$ and any other factorization of l into prime factors simply rearranges these factors in some other order.

Now, since $n = p\,l$, $n = p\,(p_1^{e_1}\, p_2^{e_2}\, p_3^{e_3} \ldots p_k^{e_k})$, which is a factorization of n into prime factors and, as such, is a simple rearrangement of the prime factors which appear in the Unique Prime Factorization of n. Since p is one of these factors, we conclude that p appears in the Unique Prime Factorization of n.

$\therefore$ If p is a divisor of n, then p appears as a factor in the Unique Prime Factorization of n.

[We next prove that if p appears as a prime factor in the Unique Prime Factorization of n, then p is a divisor of n.]

Suppose p appears as a factor in the Unique Prime Factorization of n.

By the UFT, (i.e., by Theorem 4.3.5), n has a Unique Prime Factorization, i.e., there is some positive integer k and prime numbers $p_1, p_2, p_3, \ldots, p_k$ and positive exponents $e_1, e_2, e_3, \ldots, e_k$ such that

$$n = p_1^{e_1}\, p_2^{e_2}\, p_3^{e_3} \ldots p_k^{e_k} \ .$$

Since p appears as a prime factor in this factorization of n, $p = p_i$ for some integer i and we may renumber these prime factors so that $i = 1$ and $p = p_1$.

Let $l = p_1^{(e_1 - 1)}\, p_2^{e_2}\, p_3^{e_3} \ldots p_k^{e_k}$

Since the exponent $e_1 > 0$, $(e_1 - 1) \geq 0$, l is an integer. Also, $n = p\,l$.

$\therefore p$ is a divisor of n.

$\therefore$ If p appears as a factor in the Unique Prime Factorization of n, then p is a divisor of n.

Q E D

Lemma (NIB) 1: For all integers a and b, $a \mid b$ if and only if $a \mid (-1)\,b$ if and only if a divides $|b|$.

Proof: The proof is left as an exercise.

Theorem (NIB) 2:

For all integers a and b, and for all prime numbers p,

if p divides ab, then p divides a or p divides b.

Proof: Let a and b be any integers and suppose p is any prime number such that p divides ab.

[We need to show that p | a or p | b.]

[We first prove that we can assume that $a > 1$ and $b > 1$.]

Suppose $ab = 0$. Then, by the Zero Product Property, $a = 0$ or $b = 0$.

Therefore, since $p \mid 0$, $p \mid a$ or $p \mid b$.

Therefore, we can assume that $ab \neq 0$. Thus, by the Zero Product Property, $a \neq 0$ and $b \neq 0$.

Without loss of generality, we can assume that $a > 0$ and $b > 0$ because, if the theorem is true for $|a|$ and $|b|$, then the theorem is true for a and b, by Lemma (NIB) 1,.

Now, suppose $a = 1$ or $b = 1$. Therefore, $ab = b$ or $ab = a$.

Since p divides ab, $p \mid b$ or $p \mid a$, which is to say that $p \mid a$ or $p \mid b$.

Therefore, we can assume that $a \neq 1$ and $b \neq 1$.

Therefore, $a > 1$ and $b > 1$

By the UFT (Theorem 4.3.5), there is some positive integer k and prime numbers $p_1, p_2, p_3, \ldots, p_k$ and positive exponents $e_1, e_2, e_3, \ldots, e_k$ such that

$$a = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$$

and there is some positive integer s and prime numbers $q_1, q_2, q_3, \ldots, q_s$ and positive exponents $f_1, f_2, f_3, \ldots, f_s$ such that

$$b = q_1^{f_1} q_2^{f_2} q_3^{f_3} \ldots q_s^{f_s}$$

By the uniqueness of prime factorizations, the Unique Prime Factorization of ab is a rearrangement of the prime factors in the following prime factorization:

$$ab = \left(p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}\right)\left(q_1^{f_1} q_2^{f_2} q_3^{f_3} \ldots q_s^{f_s}\right).$$

Since p divides ab and by Theorem (NIB) 1, p appears as one of the prime factors in this prime factorization of ab, that is, $p = p_i$ for one of the prime factors of a or $p = q_j$ for one of the prime factors of b. If $p = p_i$ for one of the prime factors of a, then p divides a. If $p = q_j$ for one of the prime factors of b, then p divides b. Therefore, p divides a or p divides b. QED

Theorem (NIB) 3: For any integer n, and for any prime number p,

if $p \mid n^2$, then $p \mid n$.

Proof: Suppose n is any integer and suppose that p is a prime number such that p divides n^2.

Let $a = n$ and let $b = n$. Then, $ab = n^2$, so p divides ab, by substitution. By Theorem (NIB) 2, $p \mid a$ or $p \mid b$. Thus, $p \mid n$ or $p \mid n$. In either case, $p \mid n$. Q E D