PROOF In part (i), the product on the right hand side divides both a and b, and is the largest such integer, by Proposition 12.1. And in part (ii), the product on the right hand side is a multiple of both a and b, and is the smallest such positive integer, again by Proposition 12.1. Finally, if we take the product of the right hand sides in (i) and (ii), we get

$$p_1^{\min(r_1,s_1)+\max(r_1,s_1)} \dots p_m^{\min(r_m,s_m)+\max(r_m,s_m)},$$

which is equal to ab since $\min(r_i,s_i) + \max(r_i,s_i) = r_i + s_i$. ∎

Here is our next application of the Fundamental Theorem of Arithmetic.

PROPOSITION 12.3

Let n be a positive integer. Then $\sqrt{n}$ is rational if and only if n is a perfect square (i.e., $n = m^2$ for some integer m).

PROOF The right-to-left implication is obvious: if $n = m^2$ with $m \in \mathbb{Z}$, then $\sqrt{n} = |m| \in \mathbb{Z}$ is certainly rational.

The left-to-right implication is much less clear. Suppose $\sqrt{n}$ is rational, say

$$\sqrt{n} = \frac{r}{s}$$

where $r,s \in \mathbb{Z}$. Squaring, we get $ns^2 = r^2$. Now consider prime factorizations. Each prime in the factorization of r^2 appears to an even power (since if $r = p_1^{a_1} \dots p_k^{a_k}$ then $r^2 = p_1^{2a_1} \dots p_k^{2a_k}$). The same holds for the primes in the factorization of s^2. Hence, by the Fundamental Theorem, each prime factor of n must also occur to an even power — say $n = q_1^{2b_1} \dots q_l^{2b_l}$. Then $n = m^2$, where $m = q_1^{b_1} \dots q_l^{b_l} \in \mathbb{Z}$. ∎

A similar argument applies to the rationality of cube roots, and more generally, n^{th} roots (see Exercise 5 at the end of the chapter).

Now for our final consequence of the Fundamental Theorem 12.1. Again it looks rather innocent, but in the example following the proposition we shall give a striking application of it.

In the statement, when we say a positive integer is a square (or an n^{th} power), we mean that it is the square of an integer (or the n^{th} power of an integer).

PROPOSITION 12.4

Let a and b be positive integers that are coprime to each other.

(a) *If ab is a square, then both a and b are also squares.*

(b) *More generally, if ab is an n^{th} power (for some positive integer n), then both a and b are also n^{th} powers.*

PROOF (a) Let the prime factorizations of a,b be

$$a = p_1^{d_1} \dots p_k^{d_k},\ b = q_1^{e_1} \dots q_l^{e_l}$$

(where $p_1 < \dots < p_k$ and $q_1 < \dots < q_l$). If ab is a square, then $ab = c^2$ for some integer c; let c have prime factorization $c = r_1^{f_1} \dots r_m^{f_m}$. Then $ab = c^2$ gives the equation

$$p_1^{d_1} \dots p_k^{d_k} q_1^{e_1} \dots q_l^{e_l} = r_1^{2f_1} \dots r_m^{2f_m}.$$

Since a and b are coprime to each other, none of the p_is are equal to any of the q_is. Hence, the Fundamental Theorem 12.1 implies that each p_i is equal to some r_j, and the corresponding powers d_i and $2f_j$ are equal; and likewise for the q_is and their powers.

We conclude that all the powers d_i, e_i are even numbers — say $d_i = 2d_i', e_i = 2e_i'$. This means that

$$a = \left(p_1^{d_1'} \dots p_k^{d_k'}\right)^2,\ b = \left(q_1^{e_1'} \dots q_l^{e_l'}\right)^2,$$

so a and b are squares.

(b) The argument for (b) is the same as for (a): an equation $ab = c^n$ gives an equality

$$p_1^{d_1} \dots p_k^{d_k} q_1^{e_1} \dots q_l^{e_l} = r_1^{nf_1} \dots r_m^{nf_m}.$$

The Fundamental Theorem implies that each power d_i, e_i is a multiple of n, and hence a,b are both n^{th} powers. ∎

Example 12.1

Here is an innocent little question about the integers:

Can a non-zero even square exceed a cube by 1?

(The non-zero even squares are of course the integers $4, 16, 64, 100, 144, \dots$ and the cubes are $\dots, -8, -1, 0, 1, 8, 27, \dots$.)

In other words, we are asking whether the equation

$$4x^2 = y^3 + 1 \tag{12.1}$$

has any solutions with x, y both non-zero integers. This is an example of a *Diophantine equation*. In general, a Diophantine equation is an equation for which the solutions are required to be integers. Most Diophantine