Chapter 10

The Integers

In this chapter we begin to study the most basic, and also perhaps the most fascinating, number system of all — the integers. Our first aim will be to investigate factorization properties of integers. We know already that every integer greater than 1 has a prime factorization (Proposition 8.1). This was quite easy to prove using Strong Induction. A somewhat more delicate question is whether the prime factorization of an integer is always *unique* — in other words, whether, given an integer n, one can write it as a product of primes in only one way. The answer is yes; and this is such an important result that it has acquired the grandiose title of "The Fundamental Theorem of Arithmetic." We shall prove it in the next chapter and try there to show why it is such an important result by giving some examples of its use. In this chapter we lay the groundwork for this.

We begin with a familiar definition.

DEFINITION *Let $a, b \in \mathbb{Z}$. We say a* divides *b (or a* is a factor of *b) if $b = ac$ for some integer c. When a divides b, we write $a|b$.*

Usually, of course, given two integers a, b at random, it is unlikely that a will divide b. But we can "divide a into b" and get a quotient and a remainder:

PROPOSITION 10.1
Let a be a positive integer. Then for any $b \in \mathbb{Z}$, there are integers q, r such that

$$b = qa + r \quad \textit{and} \quad 0 \leq r < a \ .$$

The integer q is called the quotient, and r is the remainder. For example, if $a = 17, b = 183$ then the equation in Proposition 10.1 is $183 = 10 \cdot 17 + 13$, the quotient is 10 and the remainder 13.

PROOF Consider the rational number $\frac{b}{a}$. There is an integer q such

that

$$q \le \frac{b}{a} < q+1$$

(this is just saying $\frac{b}{a}$ lies between two consecutive integers). Multiplying through by the positive integer a, we obtain $qa \le b < (q+1)a$, hence $0 \le b-qa < a$.

Now put $r = b-qa$. Then $b = qa+r$ and $0 \le r < a$, as required. ∎

PROPOSITION 10.2
Let $a,b,d \in \mathbb{Z}$, and suppose that $d|a$ and $d|b$. Then $d|(ma+nb)$ for any $m,n \in \mathbb{Z}$.

PROOF Let $a = c_1 d$ and $b = c_2 d$ with $c_1, c_2 \in \mathbb{Z}$. Then for $m,n \in \mathbb{Z}$,

$$ma+nb = mc_1 d + nc_2 d = (mc_1 + nc_2)\,d\ .$$

Hence $d|(ma+nb)$. ∎

The Euclidean Algorithm

The Euclidean algorithm is a step-by-step method for calculating the common factors of two integers. First we need a definition.

DEFINITION *Let $a,b \in \mathbb{Z}$. A* common factor *of a and b is an integer that divides both a and b. The* highest common factor *of a and b, written $hcf(a,b)$, is the largest positive integer that divides both a and b.*

IB: gcd(a, b). greatest common divisor

For example, $\mathrm{hcf}(2,3) = 1$ and $\mathrm{hcf}(4,6) = 2$. But how do we go about finding the highest common factor of two large numbers, say 5817 and 1428? This is what the Euclidean algorithm does for us — in a few simple, mindless steps.

Before presenting the algorithm in all its full glory, let us do an example.

Example 10.1
Here we find $\mathrm{hcf}(5817,1428)$ in a few mindless steps, as advertised. Write $b = 5817, a = 1428$, and let $d = \mathrm{hcf}(a,b)$.

Step 1 Divide a into b and get a quotient and remainder:

$$5817 = 4 \cdot 1428 + 105\ .$$

(*Deduction*: As $d|a$ and $d|b$, d also divides $a-4b = 105$.)

Step 2 Divide 105 into 1428:

$$1428 = 13 \cdot 105 + 63\ .$$

(*Deduction*: As $d|1428$ and $d|105$, d also divides 63.)

Step 3 Divide 63 into 105:

$$105 = 1 \cdot 63 + 42\ .$$

(*Deduction*: $d|42$.)

Step 4 Divide 42 into 63:

$$63 = 1 \cdot 42 + 21\ .$$

(*Deduction*: $d|21$.)

Step 5 Divide 21 into 42:

$$42 = 2 \cdot 21 + 0\ .$$

Step 6 STOP!

We claim that $d = \mathrm{hcf}(5817,1428) = 21$, the last non-zero remainder in the above steps. We have already observed that $d|21$. To prove our claim, we work upwards from the last step to the first: namely, Step 5 shows that $21|42$; hence Step 4 shows that $21|63$; hence Step 3 shows that $21|105$; hence Step 2 shows that $21|1428$; hence Step 1 shows $21|5817$. Therefore, 21 divides both a and b, so $d \ge 21$. As $d|21$, it follows that $d = 21$, as claimed.

The general version of the Euclidean algorithm is really no more complicated than this example. Here it is.

Let a,b be integers. To calculate $\mathrm{hcf}(a,b)$, we perform (mindless) steps as in the example: first divide a into b, getting a quotient q_1 and remainder r_1; then divide r_1 into a, getting remainder $r_2 < r_1$; then divide r_2 into r_1, getting remainder $r_3 < r_2$; and carry on like this until we eventually get a remainder 0 (which we must, as the r_is are decreasing and are ≥ 0). Say the remainder 0

occurs after $n+1$ steps. Then the equations representing the steps are:

$$\begin{aligned}
&(1)\ b = q_1 a + r_1 && \text{with } 0 \le r_1 < a \\
&(2)\ a = q_2 r_1 + r_2 && \text{with } 0 \le r_2 < r_1 \\
&(3)\ r_1 = q_3 r_2 + r_3 && \text{with } 0 \le r_3 < r_2 \\
&\quad \cdot\cdot && \cdot \\
&\quad \cdot\cdot && \cdot \\
&\quad \cdot\cdot && \cdot \\
&(n-1)\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} && \text{with } 0 \le r_{n-1} < r_{n-2} \\
&\quad (n)\ r_{n-2} = q_n r_{n-1} + r_n && \text{with } 0 \le r_n < r_{n-1} \\
&(n+1)\ r_{n-1} = q_{n+1} r_n + 0
\end{aligned}$$

THEOREM 10.1

In the above, the highest common factor hcf(a,b) is equal to r_n, the last non-zero remainder.

PROOF Let $d = \text{hcf}(a,b)$. We first show that $d|r_n$ by arguing from equation (1) downwards. By Proposition 10.2, d divides $b - q_1 a$, and hence by (1), $d|r_1$. Then by (2), $d|r_2$; by (3), $d|r_3$; and so on, until by (n), $d|r_n$.

Now we show that $d \ge r_n$ by working upwards from equation $(n+1)$. By $(n+1)$, $r_n|r_{n-1}$; hence by (n), $r_n|r_{n-2}$; hence by $(n-1)$, $r_n|r_{n-3}$; and so on, until by (2), $r_n|a$ and then by (1), $r_n|b$. Thus, r_n is a common factor of a and b, and so $d \ge r_n$.

We conclude that $d = r_n$, and the proof is complete. ∎

The next result is an important consequence of the Euclidean algorithm.

PROPOSITION 10.3

If $a,b \in \mathbb{Z}$ and $d = hcf(a,b)$, then there are integers s and t such that

$$d = sa + tb \ .$$

PROOF We use Equations (1),..., (n) above. By (n),

$$d = r_n = r_{n-2} - q_n r_{n-1} \ .$$

Substituting for r_{n-1} using Equation $(n-1)$, we get

$$d = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}) = x r_{n-2} + y r_{n-3}$$

where $x,y \in \mathbb{Z}$. Using Equation $(n-2)$, we can substitute for r_{n-2} in this (specifically, $r_{n-2} = r_{n-4} - q_{n-2} r_{n-3}$), to get

$$d = x' r_{n-3} + y' r_{n-4}$$

where $x',y' \in \mathbb{Z}$. Carrying on like this, we eventually get $d = sa + tb$ with $s,t \in \mathbb{Z}$, as required. ∎

Example 10.2

We know by Example 10.1 that hcf$(5817, 1428) = 21$. So by Proposition 10.3 there are integers s,t such that

$$21 = 5817s + 1428t \ .$$

Let us find such integers s,t.

To do this, we apply the method given in the proof of Proposition 10.3, using the equations in Steps 1 through 4 of Example 10.1. By Step 4,

$$21 = 63 - 42 \ .$$

Hence by Step 3,

$$21 = 63 - (105 - 63) = -105 + 2 \cdot 63 \ .$$

Hence by Step 2,

$$21 = -105 + 2(1428 - 13 \cdot 105) = 2 \cdot 1428 - 27 \cdot 105 \ .$$

Hence by Step 1,

$$21 = 2 \cdot 1428 - 27(5817 - 4 \cdot 1428) = -27 \cdot 5817 + 110 \cdot 1428 \ .$$

Thus we have found our integers s,t: $s = -27, t = 110$ will work. (But note that there are many other values of s,t which also work; for example, $s = -27 + 1428, t = 110 - 5817$.)

Here is a consequence of Proposition 10.3.

PROPOSITION 10.4

If $a,b \in \mathbb{Z}$, then any common factor of a and b also divides hcf(a,b).

PROOF Let $d = \text{hcf}(a,b)$. By Proposition 10.3, there are integers s,t such that $d = sa + tb$. If m is a common factor of a and b, then m divides $sa + tb$ by Proposition 10.2, and hence m divides d. ∎

We are now in a position to prove a highly significant fact about prime numbers: namely, that if a prime number p divides a product ab of two integers, then p divides one of the factors a and b.

DEFINITION *If $a, b \in \mathbb{Z}$ and $hcf(a,b) = 1$, we say that a and b are* coprime *to each other.*

For example, 17 and 1024 are coprime to each other. Note that by Proposition 10.3, if a, b are coprime to each other, then there are integers s, t such that $1 = sa + tb$.

PROPOSITION 10.5
Let $a, b \in \mathbb{Z}$.
(a) *Suppose c is an integer such that a, c are coprime to each other, and $c|ab$. Then $c|b$.*
(b) *Suppose p is a prime number and $p|ab$. Then either $p|a$ or $p|b$.*

PROOF (a) By Proposition 10.3, there are integers s, t such that $1 = sa + tc$. Multiplying through by b gives

$$b = sab + tcb \ .$$

Since $c|ab$ and $c|tcb$, the right-hand side is divisible by c. Hence $c|b$.

(b) We show that if p does not divide a, then $p|b$. Suppose then that p does not divide a. As the only positive integers dividing p are 1 and p, $\text{hcf}(a,p)$ must be 1 or p. It is not p as p does not divide a; hence $\text{hcf}(a,p) = 1$. Thus a, p are coprime to each other and $p|ab$. It follows by part (a) that $p|b$, as required. ∎

Proposition 10.5(b) will be crucial in our proof of the uniqueness of prime factorization in the next chapter. To apply it there, we need to generalize it slightly to the case of a prime dividing a product of many factors, as follows.

PROPOSITION 10.6
Let $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, and let p be a prime number. If $p|a_1 a_2 \ldots a_n$, then $p|a_i$ for some i.

PROOF We prove this by induction. Let $P(n)$ be the statement of the proposition.

First, $P(1)$ says "if $p|a_1$ then $p|a_1$," which is trivially true.

Now suppose $P(n)$ is true. Let $a_1, a_2, \ldots, a_{n+1} \in \mathbb{Z}$, with $p|a_1 a_2 \ldots a_{n+1}$. We need to show that $p|a_i$ for some i.

Regard $a_1 a_2 \ldots a_{n+1}$ as a product ab, where $a = a_1 a_2 \ldots a_n$ and $b = a_{n+1}$. Then $p|ab$, so by Proposition 10.5(b), either $p|a$ or $p|b$. If $p|a$, that is to say $p|a_1 a_2, \ldots, a_n$, then by $P(n)$ we have $p|a_i$ for some i; and if $p|b$ then $p|a_{n+1}$. Thus, in either case, p divides one of the factors $a_1, a_2, \ldots, a_{n+1}$.

We have established that $P(n) \Rightarrow P(n+1)$. Hence, by induction, $P(n)$ is true for all n. ∎

Exercises for Chapter 10

1. For each of the following pairs a, b of integers, find the highest common factor $d = \text{hcf}(a,b)$, and find integers s, t such that $d = sa + tb$:
   (i) $a = 17, b = 29$
   (ii) $a = 552, b = 713$
   (iii) $a = 345, b = 299$.

2. Show that if a, b are positive integers and $d = \text{hcf}(a,b)$, then there are positive integers s, t such that $d = sa - tb$.
   Find such positive integers s, t in each of cases (i)–(iii) in Exercise 1.

3. A train leaves Moscow for St. Petersburg every 7 hours, on the hour. Show that on some days it is possible to catch this train at 9a.m.
   Whenever there is a 9a.m. train, Ivan takes it to visit his aunt Olga. How often does Olga see her nephew?
   Discuss the corresponding problem involving the train to Vladivostok, which leaves Moscow every 14 hours.

4. Show that for all positive integers n,
   $$\text{hcf}(6n+8, 4n+5) = 1 \ .$$

5. Let m, n be coprime integers, and suppose a is an integer which is divisible by both m and n. Prove that mn divides a.
   Show that the above conclusion is false if m and n are not coprime (i.e., show that if m and n are not coprime, there exists an integer a such that $m|a$ and $n|a$, but mn does not divide a).

6. Let $a, b, c \in \mathbb{Z}$. Define the highest common factor $\text{hcf}(a,b,c)$ to be the largest positive integer that divides a, b and c. Prove that there are integers s, t, u such that
   $$\text{hcf}(a,b,c) = sa + tb + uc \ .$$
   Find such integers s, t, u when $a = 91, b = 903, c = 1792$.

7. Jim plays chess every 3 days, and his friend Marmaduke eats spaghetti every 4 days. One Sunday it happens that Jim plays chess and Marmaduke eats spaghetti. How long will it be before this again happens on a Sunday?

8. Let $n \geq 2$ be an integer. Prove that n is prime if and only if for every integer a, either $\text{hcf}(a,n) = 1$ or $n|a$.

9. Let a, b be coprime positive integers. Prove that for any integer n there exist integers s, t with $s > 0$ such that $sa + tb = n$.

10. After a particularly exciting viewing of the new Danish thriller *Den hele tal*, critic Ivor Smallbrain repairs for refreshment to the prison's high-security fast-food outlet O'Duçks. He decides that he'd like to eat some delicious Chicken O'Nuggets. These are sold in packs of two sizes — one containing 4 O'Nuggets, and the other containing 9 O'Nuggets.

    Prove that for any integer $n > 23$, it is possible for Ivor to buy n O'Nuggets (assuming he has enough money).

    Perversely, however, Ivor decides that he must buy exactly 23 O'Nuggets, no more and no less. Is he able to do this?

    Generalize this question, replacing 4 and 9 by any pair a, b of coprime positive integers: find an integer N (depending on a and b), such that for any integer $n > N$ it is possible to find integers $s, t \geq 0$ satisfying $sa + tb = n$, but no such s, t exist satisfying $sa + tb = N$.

Additional.

11. a. Suppose $a, b, c, d \in \mathbb{Z}$. Prove that for $a \neq 0$:
(i) if $a|b$ then $a|(bc)$ (ii) if $a|b$ and $a|c$ then $a^2|(bc)$
(iii) if $a|b$ and $c|d$ then $(ac)|(bd)$; $c \neq 0$
(iv) if $a|b$ then $a^n | b^n$.
(b) Is the converse of a.(iv) true?

12. Let $k \in \mathbb{Z}$. Prove that one of k, $k+2$ or $k+4$ is divisible by 3.

13. Determine the truth or otherwise of the statement:
If $p|(q+r)$ then either $p|q$ or $p|r$.

14. Prove that if $\gcd(a,b) = 1$ and $c|a$ then $\gcd(c,b) = 1$.

15. Let $\gcd(a,b) = 1$. Prove that $\gcd(a^2,b) = \gcd(a,b^2) = 1$.
Hence, prove that $\gcd(a^2,b^2) = 1$.

16. Let $\gcd(a,b) = 1$. Prove that $\gcd(a+b, a-b) = 1$ or 2.

Chapter 11

Prime Factorization

We have already seen in Chapter 8 (Proposition 8.1) that every integer greater than 1 is equal to a product of prime numbers; that is, it has a prime factorization. The main result of this chapter, the Fundamental Theorem of Arithmetic, tells us that this prime factorization is unique — in other words, there is essentially only one way of writing an integer as a product of primes. (In case you think this is somehow obvious, have a look at Exercise 6 at the end of the chapter to find an example of a number system where prime factorization is *not* unique.)

The Fundamental Theorem of Arithmetic may not seem terribly thrilling to you at first sight. However, it is in fact one of the most important properties of the integers and has many consequences. I will endeavour to thrill you a little by giving a few such consequences after we have proved the theorem.

The Fundamental Theorem of Arithmetic

Without further ado then, let us state and prove the theorem.

THEOREM 11.1 (Fundamental Theorem of Arithmetic)
Let n be an integer with $n \geq 2$.

(I) *Then n is equal to a product of prime numbers: we have*

$$n = p_1 \dots p_k$$

where $p_1, \dots, p_k$ are primes and $p_1 \leq p_2 \leq \dots \leq p_k$.

(II) *This prime factorization of n is unique: in other words, if*

$$n = p_1 \dots p_k = q_1 \dots q_l$$

where the p_is and q_is are all prime, $p_1 \leq p_2 \leq \dots \leq p_k$ and $q_1 \leq q_2 \leq \dots \leq q_l$, then

$$k = l \quad \text{and} \quad p_i = q_i \quad \text{for all } i = 1, \dots, k.$$

The point about specifying that $p_1 \le p_2 \le \ldots \le p_k$ is that this condition determines the order in which we write down the primes in the factorization of n. For example, 28 can be written as a product of primes in several ways: $2\times7\times2$, $7\times2\times2$ and $2\times2\times7$. But if we specify that the prime factors have to increase or stay the same, then the only factorization is $28 = 2\times2\times7$.

PROOF Part (I) is just Proposition 8.1.

Now for the uniqueness part (II). We prove this by contradiction. So suppose there is some integer n which has two different prime factorizations, say

$$n = p_1 \ldots p_k = q_1 \ldots q_l$$

where $p_1 \le p_2 \le \ldots \le p_k$, $q_1 \le q_2 \le \ldots \le q_l$, and the list of primes $p_1, \ldots, p_k$ is not the same list as $q_1, \ldots, q_l$.

Now in the equation $p_1 \ldots p_k = q_1 \ldots q_l$, cancel any primes that are common to both sides. Since we are assuming the two factorizations are different, not all the primes cancel, and we end up with an equation

$$r_1 \ldots r_a = s_1 \ldots s_b \ ,$$

where each $r_i \in \{p_1, \ldots, p_k\}$, each $s_i \in \{q_1, \ldots, q_l\}$, and none of the r_is is equal to any of the s_is (i.e., $r_i \ne s_j$ for all i, j).

Now we obtain a contradiction. Certainly r_1 divides $r_1 \ldots r_a$, hence r_1 divides $s_1 \ldots s_b$. By Proposition 10.6, this implies that $r_1 | s_j$ for some j. However, s_j is prime, so its only divisors are 1 and s_j, and hence $r_1 = s_j$. But we know that none of the r_is is equal to any of the s_is, so this is a contradiction. This completes the proof of (II). ∎

Of course, in the prime factorization given in part (I) of Theorem 11.1, some of the p_is may be equal to each other. If we collect these up, we obtain a unique prime factorization of the form

$$n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} \ ,$$

where $p_1 < p_2 < \ldots < p_m$ and the a_is are positive integers.

Some Consequences of the Fundamental Theorem

First, here is an application of the Fundamental Theorem of Arithmetic that looks rather more obvious than it really is.

PROPOSITION 11.1

Let $n = p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m}$, where the p_is are prime, $p_1 < p_2 < \ldots < p_m$ and the a_is are positive integers. If m divides n, then

$$m = p_1^{b_1} p_2^{b_2} \ldots p_m^{b_m} \quad \textit{with} \quad 0 \le b_i \le a_i \quad \textit{for all } i \ .$$

For example, the only divisors of $2^{100}3^2$ are the numbers 2^a3^b, where $0 \le a \le 100$, $0 \le b \le 2$.

PROOF If $m|n$, then $n = mc$ for some integer c. Let $m = q_1^{c_1} \ldots q_k^{c_k}$, $c = r_1^{d_1} \ldots r_l^{d_l}$ be the prime factorizations of m, c. Then $n = mc$ gives the equation

$$p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} = q_1^{c_1} \ldots q_k^{c_k} r_1^{d_1} \ldots r_l^{d_l} \ .$$

By the Fundamental Theorem 11.1, the primes, and the powers to which they occur, must be identical on both sides. Hence, each q_i is equal to some p_j, and its power c_i is at most a_j. In other words, the conclusion of the proposition holds. ∎

We can use this to prove some further obvious-looking facts about integers. Define the *least common multiple* of two positive integers a and b, denoted by $lcm(a,b)$, to be the smallest positive integer that is divisible by both a and b. For example, $lcm(15,21) = 105$.

If $lcm(a,b) = m$ then
(i) $a|m$ and $b|m$
(ii) if $a|c$ and $b|c$ then $m \le c$ where $c > 0$.

PROPOSITION 11.2

Let $a, b \ge 2$ be integers with prime factorizations

$$a = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}, \quad b = p_1^{s_1} p_2^{s_2} \ldots p_m^{s_m}$$

where the p_i are distinct primes and all $r_i, s_i \ge 0$ (we allow some of the r_i and s_i to be 0). Then

(i) $hcf(a,b) = p_1^{\min(r_1,s_1)} \ldots p_m^{\min(r_m,s_m)}$

(ii) $lcm(a,b) = p_1^{\max(r_1,s_1)} \ldots p_m^{\max(r_m,s_m)}$

(iii) $lcm(a,b) = ab/hcf(a,b)$.

PROOF In part (i), the product on the right-hand side divides both a and b and is the largest such integer, by Proposition 11.1. 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 11.1. Finally, if we take the product of the right-hand sides in (i) and (ii), then we

Let us then go about solving Equation (11.1) for $x,y \in \mathbb{Z}$. First we rewrite it as $y^3 = 4x^2 - 1$ and then cleverly factorize the right-hand side to get

$$y^3 = (2x+1)(2x-1) .$$

The factors $2x+1, 2x-1$ are both odd integers, and their highest common factor divides their difference, which is 2. Hence

$$\text{hcf}(2x+1, 2x-1) = 1 .$$

Thus, $2x+1$ and $2x-1$ are coprime to each other, and their product is y^3, a cube. By Proposition 11.4(b), it follows that $2x+1$ and $2x-1$ are themselves both cubes. However, from the list of cubes $\ldots, -8, -1, 0, 1, 8, 27, \ldots$ it is apparent that the only two cubes that differ by 2 are $1, -1$. Therefore, $x = 0$ and we have shown that the only even square that exceeds a cube by 1 is 0. In other words, there are no non-zero such squares.

Exercises for Chapter 11

√1. Find the prime factorization of 111111.

2. (a) Which positive integers have exactly three positive divisors?

   (b) Which positive integers have exactly four positive divisors?

   (c) Suppose $n \geq 2$ is an integer with the property that whenever a prime p divides n, p^2 also divides n (i.e., all primes in the prime factorization of n appear at least to the power 2). Prove that n can be written as the product of a square and a cube.

√3. Suppose that n is a positive integer such that $p = 2^n - 1$ is prime. (The first few such primes are $3, 7, 31, \ldots$.) Define

$$N = 2^{n-1}p .$$

   List all positive integers that divide N. Prove that the sum of all these divisors, including 1 but not N itself, is equal to N.

   A positive integer that is equal to the sum of all its divisors (including 1 but not itself) is called a *perfect* number. Write down four perfect numbers.

√4. Prove that $lcm(a,b) = ab/hcf(a,b)$ for any positive integers a, b without using prime factorization.

Explore (i) a=70; b=120 (ii) a=5; b=11
(iii) a=372; b=1749

5. (a) Prove that $2^{\frac{1}{3}}$ and $3^{\frac{1}{3}}$ are irrational.

   (b) Let m and n be positive integers. Prove that $m^{\frac{1}{n}}$ is rational if and only if m is an n^{th} power (i.e., $m = c^n$ for some integer c).

6. Let E be the set of all positive even integers. We call a number e in E "prima" if e cannot be expressed as a product of two other members of E.

   (i) Show that 6 is prima but 4 is not.

   (ii) What is the general form of a prima in E?

   (iii) Prove that every element of E is equal to a product of primas.

   (iv) Give an example to show that E does not satisfy a "unique prima factorization theorem" (i.e., find an element of E that has two different factorizations as a product of primas).

√7. (a) Which pairs of positive integers m, n have $hcf(m,n) = 50$ and $lcm(m,n) = 1500$?

   (b) Show that if m, n are positive integers, then $hcf(m,n)$ divides $lcm(m,n)$. When does $hcf(m,n) = lcm(m,n)$?

   (c) Show that if m, n are positive integers, then there are coprime integers x, y such that x divides m, y divides n, and $xy = lcm(m,n)$.

√8. Find all solutions $x, y \in \mathbb{Z}$ to the following Diophantine equations:

   (a) $x^2 = y^3$

   (b) $x^2 - x = y^3$

   (c) $x^2 = y^4 - 77$

   (d) $x^3 = 4y^2 + 4y - 3$.

9. Languishing in his prison cell, critic Ivor Smallbrain is dreaming. In his dream he is on the Pacific island of Nefertiti, eating coconuts on a beach by a calm blue lagoon. Suddenly the king of Nefertiti approaches him, saying, "Your head will be chopped off unless you answer this riddle: Is it possible for the sixth power of an integer to exceed the fifth power of another integer by 16?" Feverishly, Ivor writes some calculations in the sand and eventually answers, "Oh, Great King, no it is not possible." The king rejoinders, "You are correct, but you will be beheaded anyway." The executioner's axe is just coming down when Ivor wakes up. He wonders whether his answer to the king was really correct.

   Prove that Ivor was indeed correct.

obtain

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

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 11.3

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 $r = p_1^{a_1} \ldots p_k^{a_k}$ then $r^2 = p_1^{2a_1} \ldots p_k^{2a_k}$). 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 $n = q_1^{2b_1} \ldots q_l^{2b_l}$. Then $n = m^2$, where $m = q_1^{b_1} \ldots q_l^{b_l} \in \mathbb{Z}$. ∎

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 11.1. 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 11.4

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

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

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

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

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 11.1 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

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

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

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

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 11.1

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 $4, 16, 64, 100, 144, \ldots$ and the cubes are $\ldots, -8, -1, 0, 1, 8, 27, \ldots$.)

In other words, we are asking whether the equation

$$4x^2 = y^3 + 1 \qquad (11.1)$$

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 equations are very hard, or impossible, to solve — for instance, even the equation $x^2 = y^3 + k$ has not been completely solved for all values of k. However, I have chosen a nice example, in that Equation (11.1) can be solved fairly easily (as you will see), but the solution is not totally trivial and involves use of the consequence 11.4 of the Fundamental Theorem 11.1.