9 The Fundamental Theorem of Arithmetic

Prime Factorization

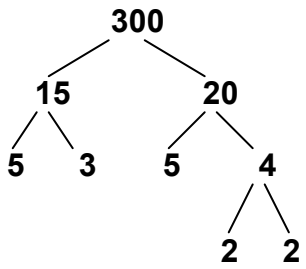
In Chapter 8 we looked for a general conjecture about the relation between $\tau(n)$ and n, and failed. Now we look for a pattern in the relation between prime numbers and composites. Finding such a pattern may illuminate our earlier problem.

Composite numbers have divisors other than themselves and 1. Some of those divisors are primes, and some may be composite. The divisors of composite divisors also may be prime or composite. But it looks as if we've got to get to prime divisors sooner or later. This leads to the conjecture:

CONJECTURE: Any composite number can be represented as a product in which all of the factors (multiplicands) are primes.

Pick a composite number such as 300. One algorithm for finding the factorization is to begin with the smallest prime divisor (2) and use it as a factor. We get $300 = 2 \cdot 150$. We look at 150 and find its smallest prime divisor. This is 2 again, so we replace 150 with $2 \cdot 75$ and write $300 = 2 \cdot 2 \cdot 75$. 75 is not prime. We find its smallest prime divisor (3), replace 75 with $3 \cdot 25$, giving $300 = 2 \cdot 2 \cdot 3 \cdot 25$. The smallest prime divisor of 25 is 5, so we get $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$. Since 5 is prime, we are done.

Another algorithm for finding the prime factorization of a number is called the "branching method."[1] Select any two numbers whose product is the number to be factored. If the factors are not prime numbers, then continue factoring until all factors are prime. The branching that leads to the prime factorization of 300 (shown at right) gives $300 = 5 \cdot 3 \cdot 5 \cdot 2 \cdot 2$. The convention is to write the primes in ascending order, so we should say $300 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5$.



Exercise. Write 57, 117, and 1728 as the products of primes.

By either method, any composite number can be represented as the product of primes. This leads to the following proof.

---

1 Angel & Porter, *A Survey of Mathematics with Applications, 4th Ed.* (Reading, Mass.: Addison-Wesley, 1993), pp. 173-5

Proof: Take any natural number **n**. If **n** is composite, it can be written as the product of two smaller natural numbers. If those two natural numbers are both prime, the conjecture is true. If either of the two is composite, it is in turn the product of smaller natural numbers. Continuing this process until we meet only primes, we eventually have **n** written as the product of primes.■

Many composite numbers can be factored in more than one way. For example, $\mathbf{12 = 2 \cdot 6 = 3 \cdot 4 = 1 \cdot 12}$. But every number I've tried seemed to have only one prime factorization. Is that the case for all composite numbers?

Suppose I decide to factor some huge number **N**. I opt to use the first algorithm, above, and, after much computer time, I get a list of **n** primes $\mathbf{p_1, p_2, p_3, \ldots,}$ and $\mathbf{p_n}$. I confirm that the $\mathbf{p_i}$s really are all prime numbers. I multiply them all together and get the product $\mathbf{p_1p_2p_3 \ldots p_n = N}$. Suppose someone else factors the same number **N**. She uses a different algorithm, running on a different kind of computer. She discovers a list of **m** prime divisors $\mathbf{q_1, q_2, q_3, \ldots,}$ and $\mathbf{q_m}$. Every one of her $\mathbf{q_i}$s is prime, and their product $\mathbf{q_1q_2q_3 \ldots q_m = N}$. Is it possible that **n** is not equal to **m** and/or that at least one of my **p**s is different from at least one of her **q**s? In how many ways can a composite number be written as the product of primes? Or is there a unique factorization of any composite number into primes?

What happens if a number you're trying to factor is prime? How many divisors do you have to try before you can be sure that the number you're trying to factor is prime?

There are some simple tests that permit quick recognition that a number is not prime. There is no need to test even numbers, because every even number is divisible by 2. Any number ending in a 5 or a 0 will be divisible by 5. We can see that a number like 5,106,843 is divisible by 3 by adding its digits (27) and then adding the digits in the result (9) until we get a single digit. If that digit is divisible by 3 (it is), the original number was divisible by 3. Other tests can be performed by converting the original number to a base other than 10. When the easy tests fail, we just have to try dividing the number by one prime after another.

If we have tried all the primes smaller than some prime **p**, and if $\mathbf{p^2 > N}$ (where **N** is the number we are trying to factor), then we can stop. **N** must be prime. (Don't just accept this claim. Satisfy yourself that it is true by figuring out why it must be so.) If **N** is a 100-digit number, **p** could be a 49- or 50-digit number. That means we'd have to try every prime less than some 49- or 50-digit number. How many primes would that be? It has been proved that the number of primes less than **N** is approximately $\frac{\mathbf{N}}{\mathbf{\ln(N)}}$.[2] We'd have to check about 10^{46} primes. If our computer could try a million primes a second, it would take about 3×10^{24} years (that's 3 followed by 24 zeroes, or 3 million

---

2 By ln(**N**) I mean the natural logarithm of **N**.

billion billion years) to finish the test. Even if a 100-digit number is composite, it might take a very long time to find its prime factors.

It is conceivable, until we can **prove** otherwise, that the prime factorization of some really big number using two different methods might yield two sets of prime factors that are not identical.

The **conjecture** is that there is one and only one prime factorization of any composite number. The conjecture has been proved. It is a theorem. Specifically, it is **the Fundamental Theorem of Arithmetic**.[3]

THE FUNDAMENTAL THEOREM OF ARITHMETIC. If (1) $p_1, p_2, p_3, \ldots, p_n$ and $q_1, q_2, q_3, \ldots, q_m$ are primes (both groups written in order of increasing size) and if (2) $p_1p_2p_3\ldots p_n = q_1q_2q_3\ldots q_m$, then $p_1 = q_1, p_2 = q_2, \ldots, p_n = q_m$ and hence $m = n$.

The Fundamental Theorem of Arithmetic

Outline of the Proof

It would be reasonable to prove first that $p_1 = q_1$. Now p_1 is a divisor of the product of all the **p**s (call it **N**) so it must be a divisor of the product of all the **q**s (which is also **N**). ***If we knew that this forces p_1 to divide at least one of the qs***, we could then reason like this: Since p_1 divides one of the **q**s, and since the **q**s are prime, so p_1 must **equal** the **q** that it divides. q_1 is the smallest of the **q**s, so $p_1 \geq q_1$. Identical reasoning about q_1 shows that $q_1 \geq p_1$. Thus $p_1 = q_1$. So, replacing q_1 with p_1 in $q_1q_2q_3\ldots q_m$, we get $p_1p_2p_3\ldots p_n = p_1q_2q_3\ldots q_m$. Dividing both sides by p_1 we get $p_2p_3\ldots p_n = q_2q_3\ldots q_m$. This new equation has one less prime on each side. The same kind of reasoning that proved $p_1 = q_1$ also shows that $p_2 = q_2$. Step by step we peel away the primes from each side, establishing that $p_k = q_k$ for all values of **k**. Since every **p** pairs off with one **q** and vice versa, we see that $m = n$ (the number of **p**s = the number of **q**s).

> A mathematical demonstration [proof] is not a simple juxtaposition of syllogisms, it is syllogisms *placed in a certain order*, and the order in which these elements are placed is much more important than the elements themselves. If I have the feeling, the intuition, so to speak, of this order, so as to perceive at a glance the reasoning as a whole, I need no longer fear lest I forget one of the elements, for each of them will take its allotted place in the array, and that without any effort of memory on my part.[4]

The problem is that we don't know that whenever a prime divides the product of several natural numbers it must divide at least one of them.

---

3 The Fundamental Theorem of Arithmetic is also called the "unique factorization theorem."

4 Henri Poincaré, in an address to the psychological society in Paris on the psychology of mathematicians, reprinted as an essay in Volume 4 of *The World of Mathematics* by J.R. Newman (New York: Simon and Schuster, 1956) pp. 2041-2050.

Special Numbers

Consider numbers (prime or composite) that **do** have the special property that, whenever they divide a product of two multiplicands, they divide at least one of the multiplicands. Stein calls them "special numbers."[5]

DEFINITION: A natural number greater than 1 is special if and only if, whenever it divides the product of two natural numbers, it divides at least one of them. Symbolically, **x** is special ≡ **((x|(a·b)) ⊃ (x|a ∨ x|b))**.

If all primes are special, the proof-strategy outlined above will work, because we would know "that this forces $\mathbf{p_1}$ to divide at least one of the **q**s." Before we try to prove that all primes are special, we should assure ourselves that at least some primes are special.

CONJECTURE: 2 is special.

PROOF: The conjecture is that whenever 2 divides a number **a·b** (i.e., when **2 | (a·b)**), 2 must divide **a** or **b** or both. We use an indirect proof. Suppose that 2 divides **a·b** but that 2 does not divide either **a** or **b**. If 2 does not divide **a** or **b** then both **a** and **b** are odd. If they are odd, **a** can be written as **2d+1** for some whole number **d**, and **b** can be written as **2e+1** for some whole number **e**. Using these forms of **a** and **b**, the product **a·b** can be written: **(2d+1)(2e+1) = 4de+2d+2e+1**. Clearly, **4de+2d+2e** is an even number. So **4de+2d+2e+1** (one more than an even number) must be odd. So **a·b** must be odd. But since 2 divides **a·b**, we have a contradiction (**a·b** is odd and **a·b** is not odd). Either **a** or **b** must be even. Either 2 must divide **a** or 2 must divide **b**. Therefore 2 is special.■

Try to prove that 3 and 5 are special.

You might conjecture that any natural number is special. However, that conjecture is easily disproved by the fact that 6 divides 12 (= **3·4**), but it divides neither 3 nor 4, so 6 is not special. That 6 (a composite number) is not special suggests the conjecture that no composite number is special. We can re-state this conjecture in the form of its contrapositive,[6] as

CONJECTURE: Every special number is prime.

PROOF: We prove this conjecture by proving that no composite number is special. Let **n** be a composite number. Then **n** is the product of two smaller natural

---

5 Sherman K. Stein, *Mathematics: the Man-Made Universe, 2nd Ed.* (San Francisco: W.H. Freeman and Company, 1969).

6 The contrapositive of **∀x(Cx ⊃ ~Sx)** (no composite number is special) is **∀x(~~Sx ⊃ ~Cx)**. Getting rid of the double-negation and because **~Cx** (**x** is not composite) is (for **x > 1**) equivalent to **Px** (**x** is prime), this is **∀x(Sx ⊃ Px)** (every special number is prime).

numbers, **a** and **b**, which are both greater than 1. Thus **n** divides the product of **a** and **b**, because every number divides itself. Because **a** and **b** are smaller than **n**, **n** cannot divide either **a** or **b**. Thus **n** is not special. Since the only thing we assumed about **n** was that it was composite, we have proved that no composite number can be special, from which it follows that every special number is prime.■

So, $\forall x(Sx \supset Px)$ – every special number is prime. As you should remember, this does not establish the converse, that every prime is special. To prove the Fundamental Theorem of Arithmetic we need to prove that every prime is special.

As we saw, **if every prime is special, then factorization into primes is unique** (in symbols, $S \supset U$, where **S** is the statement that all primes are special, and **U** is the statement that factorization into primes is unique). To prove $S \supset U$, we assumed something that we did not know. We said "*If we knew that this forces* p_1 *to divide at least one of the* **q***s*, …" and proved the Fundamental Theorem. That is a Conditional Proof step. We assume **S** and tried to prove **U**. If we succeed it follows that $S \supset U$.

Look back to what led us to define "special numbers" and remind yourself that the issue then was the question "If a prime divides the product of several natural numbers, must it divide at least one of them?" We can prove the theorem:

THEOREM 1: If a special number divides the product of several natural numbers, then it divides at least one of them.

PROOF: We make the argument for the case in which a special number **s** divides the product of three natural numbers **a**, **b**, and **c**. We have to prove that **s** divides at least one of **a**, **b**, and **c**.

Our assumed premise is that **s** is a special number which divides the product **abc**. Now **bc** (the product of two natural numbers) is a natural number. So **abc** is the product of two natural numbers – **a** and **bc**. Then **s** must divide either **a** or **bc**. If **s** divides **a**, we have shown that it divides at least one of **a**, **b**, and **c**. If **s** does not divide **a**, it must divide **bc**. If **s** divides **bc**, it must divide either **b** or **c**. So whenever (if) a special number divides a product of three natural numbers, it must divide at least one of them. Using mathematical induction, we could show that when a special number divides the product of any number of natural numbers, it divides at least one of them.■

Euclid's Algorithm

A number that is a divisor of two integers **a** and **b** is called a **common divisor** of **a** and **b**. A pair of numbers may have several common divisors (every pair of integers not both equal to 0 has at least one common divisor, since 1 divides every integer).

The **greatest common divisor** of two integers **a** and **b** – symbolized as **(a, b)** – is the largest integer that divides both **a** and **b**.

(0, 0) does not exist, since there is no largest divisor of 0. By the definition of "divides" every number divides 0, as $\forall x(x \cdot 0 = 0)$.

LEMMA 1: For any natural number **a**, **(a, 0) = a**.

PROOF: Every natural number **d** is a divisor of **0**, since $0 = 0 \cdot d$. Thus, the largest common divisor of **a** and **0** is simply the largest divisor of **a**, namely **a** itself.■

LEMMA 2: If **p** is prime and **p** does not divide **a**, then **(p, a) = 1**.

PROOF: The only divisors of **p** are **1** and **p**. Since **p** does not divide **a**, it follows that the **only** common divisor of both **p** and **a** is **1**. Thus **1** is the **greatest** common divisor of **p** and **a**.■

LEMMA 3: Let **a** and **b** be natural numbers (so **a** is not **0**). When we divide **a** into **b** we obtain a quotient **q** and a remainder **r**, so $b = qa + r$.[7] Then **(b, a) = (a, r)** (the greatest common divisor of **b** and **a** is the greatest common divisor of **a** and **r**).

To see what this means, look at the example where **a = 12** and **b = 57**. Since **12** "goes into" **57** four times with nine "left over," we have quotient **q = 4** and remainder **r = 9**. That is, $57 = 4 \cdot 12 + 9$. Lemma 3 says that **(57, 12) = (12, 9)**. Is that true? In general, since **r** is less than **a**, the computation of **(a, r)** will be easier than **(b, a)**.

We can prove more than just that the greatest common divisor of **a** and **b** is the same as the greatest common divisor of **a** and **r**. We'll prove that the list of all the common divisors of **a** and **b** is the same as the list of all common divisors of **a** and **r**. From this, Lemma 3 follows easily.

PROOF: Let **d** be any natural number dividing both **a** and **r**. Since **d** divides **a** it must divide **qa**. Hence it must also divide the sum $qa + r$, which is **b**.[8] Thus **d** divides **b**. So any common divisor of **a** and **r** is a common divisor of **b** and **a**.

Now we have to prove the converse – that every common divisor of **b** and **a** is a common divisor of **a** and **r**. Let **d** be any natural number that divides both **b** and **a**. Then **d** divides **qa**, and hence also the difference $b - qa$,[8] which is **r**. Thus **d** divides **a** and **r**. So any common divisor of **b** and **a** is a common divisor of **a** and **r**.

We have shown that the list of common divisors of **b** and **a** is the same as the list of common divisors of **a** and **r**. In particular, the greatest common divisor of **b** and **a** must be the same as the greatest common divisor of **a** and **r**. So **(b, a) = (a, r)**.■

One way to find the greatest common divisor of two large numbers is to list all the divisors of each number and find the largest number on both lists. Lemma 3 shows an

---

7 Either **q** or **r** (but not both) could be **0**, and $r < a$.

8 From the lemma before Theorem 1 in Chapter 8.

easier way to calculate the greatest common divisor of two natural numbers. The method is called **Euclid's algorithm**. To find the greatest common divisor of the numbers 72 and 20 (i.e., **(72, 20)**), we first divide 72 by 20. We get **72 = 3·20+12**. The remainder is 12. By Lemma 3, **(72, 20) = (20, 12)**. Divide 12 into 20 and find the remainder. **20 = 1·12+8** (the remainder is 8), so by Lemma 3, **(20, 12) = (12, 8)**. Divide 8 into 12. **12 = 1·8+4**, so **(12, 8) = (8, 4)**. Divide 4 into 8 and find the remainder. **8 = 2·4+0** (the remainder is 0). By Lemma 3, **(8, 4) = (4, 0)**. But Lemma 1 asserts that **(4, 0) = 4**. Combining all the steps, we get **(72, 20) = 4**.

We repeatedly divide and find remainders until we find a remainder of 0. At each step the remainder is smaller than the remainder from the previous step. Eventually we must obtain a remainder of 0. The remainder before 0 is the greatest common divisor.

Exercise on Euclid's Algorithm

1. Use Euclid's Algorithm to find the greatest common divisor of (a) 117 and 51. (b) of 252 and 147. (c) of 176 and 105. (d) of 600 and 398. (e) of 6447 and 5767.
2. Find **(433, 144)**, **(164, 72)**, **(91, 39)**, **(6463, 5773)**, **(1468823, 1456813)**.

Last Steps in the Proof

LEMMA 4: For any whole numbers **a** and **b** (not both 0) there are integers **m** and **n** such that **(a, b) = ma+nb**.

PROOF: Lemma 4 is related to the potato-weighing questions discussed in Chapter 8. Lemma 4 says that **a**- and **b**-gram weights can weigh a number of grams as small as the greatest common divisor of **a** and **b**. We can use the Euclidean Algorithm to find the greatest common divisor of any pair of weights and answer questions we posed (but did not answer) in the discussion of weights and measures.

In order to find **m** and **n**, we "unwind" the Euclidean Algorithm. An example should make this clearer.

Say **a = 945** and **b = 219**. We will find **(a, b)** by the Euclidean Algorithm and then find integers **m** and **n** such that **(a, b) = ma+nb**. The computations for finding **(945, 219)** appear on the left, below; the underline identifies the successive **a** and **b** in the relation **b = qa+r** at each stage. On the right are equations for the remainders at each stage; these equations will be used for finding **m** and **n**.

Euclidean Algorithm	Equations for finding **m** and **n**
945 = (4·219)+69	**69 = (1·945)−(4·219)**
219 = (3·69)+12	**12 = (1·219)−(3·69)**
69 = (5·12)+9	**9 = (1·69)−(5·12)**
12 = (1·9)+3	**3 = (1·12)−(1·9)**
9 = (3·3)+0	

Remember what we're trying to do. We want an equation like **(a, b) = ma+nb**, where **a = 945**, **b = 219**. The Euclidean Algorithm shows that **(945, 219)** is **3**. We want to find **m** and **n** that satisfy the equation **3 = 945·m+219·n**. We use the right column, starting at the bottom and working up (equivalent to finding a way to weigh a 3-gram potato with 945- and 219-gram weights).

The bottom equation on the right (**3 = (1·12)− (1·9)**) expresses 3 in terms of 9's and 12's. We want to express it in terms of 945's and 219's. The next equation above it expresses 9 in terms of 69's and 12's (**9 = (1·69)−(5·12)**). Substituting that expression for 9 in **3 = (1·12)−(1·9)**, we get **3=(1·12)−(1·((1·69)−(5·12)))** which can be re-written as **3 = (1·12)−(1·69)+(5·12)**, or **3 = (6·12)−(1·69)**, an equation for 3 in terms of 12's and 69's. To remove the 12, we use **12 = (1·219)−(3·69)**. We re-write **3 = (6·12)−(1·69)** as **3 = 6·((1·219)−(3·69))−(1·69)**. Reduce it to **3 = (6·219)−(18·69)−(1·69)**, or **3 = (6·219)−(19·69)**. This expresses 3 in terms of 69's and 219's. To get rid of the 69's, we look at the top equation on the right column of our table, above, and find **69 = (1·945)−(4·219)**. Substituting for 69 in the equation **3 = (6·219)−(19·69)**, we get **3 = (6·219)−(19·((1·945)−(4·219))**, simplified to **3 = (82·219)−(19·945)**. Thus, **3 = (82·219)+ ((−19)·945)**. We have found **m = −19** and **n = 82** that express **(945, 219)** in the form **m·945+n·219**.

Since this technique can be applied to any **(a, b)**, we have proved the lemma.■

THEOREM 2: Every prime is special.

PROOF: Let **a** and **b** be natural numbers, and let **p** be a prime that divides their product **ab**. We wish to prove that **p** must divide at least one of **a** and **b**. To do this, we prove that if **p** does not divide **a**, it must divide **b**.

If **p** does not divide **a**, we have, by Lemma 2, **(p, a) = 1**. Lemma 4 then promises that there are integers **m** and **n** such that **1 = mp+na**. If we multiply both sides of this equation by **b**, we obtain **b = mpb+nab**. **p** divides **mpb**. Since **p** divides **ab**, it also divides **nab**. Hence, **p** divides the sum **mpb+nab**. That sum is just **b**. Therefore **p** divides **b**. So **p** is special. Since this proof made no assumptions about **p** except that it was prime, we have shown that every prime is special.■

THEOREM 3: If a prime **p** divides a product $q_1q_2q_3\ldots q_m$ it divides at least one of the **q**s.

PROOF: Use mathematical induction. If there is only one **q** (so **m = 1**) then **p** divides it. Assume (as an **AP**) that the theorem is true for **m = n**, so whenever **p** divides a product $N = q_1q_2q_3\ldots q_n$ it divides at least one of the **q**s. Now look at the case when **m = n+1** (the product contains one more multiplicand). $q_1q_2q_3\ldots q_nq_{n+1}$ is the product of two numbers, **N** and q_{n+1}. By theorem 2, whenever a prime divides the product of two natural numbers, it divides one of them. So either **p** divides **N** or **p** divides q_{n+1}. If **p** divides **N**, then (since **N** contains only **n** factors), the assumed

premise states that **p** must divide at least one of them. If **p** does not divide **N**, then it must divide q_{n+1}. So if the theorem is true for $m = n$, it must be true for $m = n+1$. Therefore the theorem is true for any **m**.■

THE FUNDAMENTAL THEOREM OF ARITHMETIC: **Every composite natural number is the product of primes in exactly one way.**

PROOF: Suppose that two prime factorizations of some number **N** are $p_1, p_2, \ldots, p_n$ and $q_1, q_2, \ldots, q_m$. Then $N = p_1p_2\ldots p_n = q_1q_2\ldots q_m$. Since p_1 divides **N**, therefore p_1 divides $q_1q_2\ldots q_m$. By theorem 3, p_1 must divide at least one of the factors q_k. But every q_k is prime, so $p_1 = q_k$. Cancelling these factors from the equation $p_1p_2\ldots p_n = q_1q_2\ldots q_m$, it follows that p_2 must divide at least one of the remaining factors q_i, and hence must be equal to it. Cancelling these equal factors from the two sides of the equation, we continue the process with $p_3,\ldots, p_n$. After all of the **p**s have been cancelled, the left side of the equation will be equal to 1. Since all the **q**s are prime, they are all greater than 1, so there can be no **q**s left on the right side of the equation. Hence every **p** will have been paired off with one **q**, so there must have been equal numbers of both ($m = n$).■

Euclid went on to show that **if factorization into primes is unique, then every prime is special**. You should recognize that we could symbolize this as $U \supset S$. Once we have proved $U \supset S$, we can put it together with the previously proved $S \supset U$ to get $S \equiv U$. That is, the Fundamental Theorem of Arithmetic **U** is equivalent to the statement **S** ("every prime is special").

To prove $U \supset S$, we use Conditional Proof again. We assume (**U**) that factorization into primes is unique (i.e., that the Fundamental Theorem is true) and prove that every prime is special (**S**). Then we can say, "**if** the Fundamental Theorem is true **then** every prime is special" ($U \supset S$).

CONJECTURE: If the Fundamental Theorem is true (factorization into primes is unique) then every prime is special.

PROOF: Consider two natural numbers **a** and **b** and a prime **p** that divides the product $a \cdot b$. We want to prove that **p** divides either **a** or **b** or both. Now, since **p** divides $a \cdot b$, there must be a natural number **q** such that $a \cdot b = p \cdot q$ (from the definition of "divides"). We can express **q**, **a**, and **b** as the products of primes, as:

$$q = r_1r_2\ldots r_s, \qquad a = s_1s_2\ldots s_n, \qquad b = t_1t_2\ldots t_m$$

It's possible that one or more of **q**, **a**, and **b** is/are prime. If that were so, then we'd have $q = r_1$ or $a = d_1$ or $b = t_1$.

Since $a \cdot b = p \cdot q$, so $p \cdot q = a \cdot b$, and we have

$$p \cdot r_1r_2\ldots r_s = s_1s_2\ldots s_n \cdot t_1t_2\ldots t_m.$$

On the assumption that factorization into primes is unique (this is the assumed premise for the Conditional Proof), *the prime* **p** *must occur among the* **s***s or among the* **t***s*. If **p**

occurs among the **s**s, then **p** divides **a**. If **p** is among the **t**s, then **p** divides **b**. This shows that **p** is special.■

So the Fundamental Theorem of Arithmetic is equivalent to the statement "every prime is special."

Exercise on the Fundamental Theorem of Arithmetic

1. Define in your own words "prime number" and "special number." Which is easier: showing that a number is prime or showing that it is special? Why? Is it easier to show that every special number is prime or that every prime number is special? Why? Is "prime" a synonym for "special" in ordinary arithmetic?
2. List all the divisors of $2^3 \cdot 5^4$. How can one use the Fundamental Theorem in answering this question?
3. Let $a = 3^3 \cdot 7^2$ and $b = 3 \cdot 5 \cdot 7^3$. Use the Fundamental Theorem to show that $(a, b) = 3 \cdot 7^2$. Explain how you used the Fundamental Theorem of Arithmetic.
4. Find $(144, 96)$ in three ways. (a) List all the divisors of 96 and of 144 and find which is the greatest common divisor. (b) Use the Euclidean Algorithm. (c) Express 96 and 144 as the product of primes and use the Fundamental Theorem of Arithmetic.
5. Find the largest number that divides both $2^5 \cdot 7$ and $2^6 \cdot 5$.

The Fundamental Theorem and Irrational Numbers

In Chapter 7 we proved that there is no rational number whose square is **2**. The fundamental theorem allows us to prove that there are infinitely many irrational numbers.

Imagine a rational number $\frac{a}{b}$ whose square is **2**, where **a** and **b** are coprime. Two natural numbers whose greatest common divisor is 1 are said to be **relatively prime** or **coprime**. Let the number of primes in the prime factorization of **a** be **m**, and the number of primes in the prime factorization of **b** be **n**.[9] From $\frac{a^2}{b^2} = 2$, we get $a^2 = 2b^2$. Since **a** is the product of **m** primes, then a^2 will be the product of $2 \cdot m$ primes.[10] Similarly, b^2 will be the product of $2 \cdot n$ primes. But then $2b^2$ will be the product of $(2 \cdot n)+1$ primes (Why?). So the number of primes in the prime factorization of a^2 is even, and the number of primes in the prime factorization of $2b^2$ is odd. But a^2 is equal to $2b^2$. If $a^2 = 2b^2$, then the same number has two different prime factorizations (one with an odd, one with an even number of primes). This is impossible, according

---

9 **m** and/or **n** could be **1** if one or both of **a** and **b** is/are prime.

10 Figure it out. If $a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m$, then $a \cdot a = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m \cdot p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_m$, so every one of the **m** primes occurs twice in a^2, so we have $2 \cdot m$ primes.

to the Fundamental Theorem of Arithmetic. So there is no rational number whose square is two.■

Any number whose square root is rational must contain an even number of every prime in its prime factorization. Thus, $8 = 2 \cdot 2 \cdot 2$, so the square root of 8 is irrational. $16 = 2 \cdot 2 \cdot 2 \cdot 2$, so the square root of 16 is rational. Cube roots of numbers whose prime factorizations don't contain a multiple of 3 of every prime factor are also irrational. And so on.

Generalizing this further, we can prove

Theorem: If a is an integer, then the n^{th} root of a ($\sqrt[n]{a}$) is either an integer or an irrational number.

Proof: Using fractional powers, $\sqrt[n]{a}$ is just another way to write $a^{1/n}$. If $\sqrt[n]{a}$ is rational then there are some integers u and v such that $\sqrt[n]{a} = \frac{u}{v}$, with u and v relatively prime. Then $(\sqrt[n]{a})^n = (\frac{u}{v})^n$, giving $(a^{1/n})^n = a = \frac{u^n}{v^n}$. Multiplying both sides by v^n, we get $v^n a = u^n$. By the fundamental theorem of arithmetic, every prime factor of $v^n a$ must be a prime factor of u^n. The prime factors of u^n are just the prime factors of u repeated n times, so the prime factors of $v^n a$ must be prime factors of u.

By definition, if a special number divides the product of two natural numbers, then it divides at least one of them. Every prime is special. So every prime factor of u must divide either v^n or a. But u and v are relatively prime. None of the factors of u can divide v or any power of v. So every prime factor of u must be a factor of a. Every prime factor of u^n is a prime factor of u, so every prime factor of u^n is a prime factor of a. But $u^n = v^n a$. So every prime factor of $v^n a$ is a prime factor of a.

Since every prime factor of $v^n a$ is a prime factor of a, so there are <u>no</u> prime factors of v^n. So $v^n = v = 1$. So $\frac{u}{v} = u$, and $a = u^n$. Every prime factor of a must appear n times in the prime factorization of u^n. Thus, every prime factor of a must occur n times in the prime factorization of a. Then a is an n^{th} power, and so $\sqrt[n]{a}$ is an integer. So, if $\sqrt[n]{a}$ is rational, then $\sqrt[n]{a}$ is an integer. Either $\sqrt[n]{a}$ is an integer or it is irrational.■

n and Tau of n (again)

In Chapter 10 we tried to find a pattern in the relations between a number n and the number of its divisors $\tau(n)$. Knowing that each natural number has a unique prime