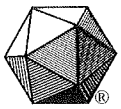
Number Theory Through Inquiry

David C. Marshall
Monmouth University

Edward Odell
The University of Texas at Austin

Michael Starbird
The University of Texas at Austin



Published and Distributed by
The Mathematical Association of America

CLASSROOM RESOURCE MATERIALS

Classroom Resource Materials is intended to provide supplementary classroom material for students—laboratory exercises, projects, historical information, textbooks with unusual approaches for presenting mathematical ideas, career information, etc.

101 Careers in Mathematics, 2nd edition edited by Andrew Sterrett

Archimedes: What Did He Do Besides Cry Eureka?, Sherman Stein

Calculus Mysteries and Thrillers, R. Grant Woods

Combinatorics: A Problem Oriented Approach, Daniel A. Marcus

Conjecture and Proof, Miklós Laczkovich

A Course in Mathematical Modeling, Douglas Mooney and Randall Swift

Creative Mathematics, H. S. Wall

Cryptological Mathematics, Robert Edward Lewand

Differential Geometry and its Applications, John Oprea

Elementary Mathematical Models, Dan Kalman

Environmental Mathematics in the Classroom, edited by B. A. Fusaro and P. C. Kenschaft

Essentials of Mathematics, Margie Hale

Exploratory Examples for Real Analysis, Joanne E. Snow and Kirk E. Weller

Fourier Series, Rajendra Bhatia

Geometry From Africa: Mathematical and Educational Explorations, Paulus Gerdes

Historical Modules for the Teaching and Learning of Mathematics (CD), edited by Victor Katz and Karen Dee Michalowicz

Identification Numbers and Check Digit Schemes, Joseph Kirtland

Interdisciplinary Lively Application Projects, edited by Chris Arney

Inverse Problems: Activities for Undergraduates, Charles W. Groetsch

Laboratory Experiences in Group Theory, Ellen Maycock Parker

Learn from the Masters, Frank Swetz, John Fauvel, Otto Bekken, Bengt Johansson, and Victor Katz

Mathematical Connections: A Companion for Teachers and Others, Al Cuoco

Mathematical Evolutions, edited by Abe Shenitzer and John Stillwell

Mathematical Modeling in the Environment, Charles Hadlock

Mathematics for Business Decisions Part 1: Probability and Simulation (electronic textbook), Richard B. Thompson and Christopher G. Lamoureux

Mathematics for Business Decisions Part 2: Calculus and Optimization (electronic textbook), Richard B. Thompson and Christopher G. Lamoureux

Math Made Visual: Creating Images for Understanding Mathematics, Claudi Alsina and Roger B. Nelsen

Number Theory Through Inquiry, David C. Marshall, Edward Odell, and Michael Starbird

Ordinary Differential Equations: A Brief Eclectic Tour, David A. Sánchez

Oval Track and Other Permutation Puzzles, John O. Kiltinen

A Primer of Abstract Mathematics, Robert B. Ash

Proofs Without Words, Roger B. Nelsen

Proofs Without Words II, Roger B. Nelsen

A Radical Approach to Real Analysis, 2nd edition, David M. Bressoud

Real Infinite Series, Daniel D. Bonar and Michael Khoury, Jr.

She Does Math!, edited by Marla Parker

Solve This: Math Activities for Students and Clubs, James S. Tanton

Student Manual for Mathematics for Business Decisions Part 1: Probability and Simulation, David Williamson, Marilou Mendel, Julie Tarr, and Deborah Yoklic

Student Manual for Mathematics for Business Decisions Part 2: Calculus and Optimization, David Williamson, Marilou Mendel, Julie Tarr, and Deborah Yoklic

Teaching Statistics Using Baseball, Jim Albert

Topology Now!, Robert Messer and Philip Straffin

Understanding our Quantitative World, Janet Andersen and Todd Swanson

Writing Projects for Mathematics Courses: Crushed Clowns, Cars, and Coffee to Go, Annalisa Crannell, Gavin LaRose, Thomas Ratliff, Elyn Rykken

MAA Service Center
P.O. Box 91112
Washington, DC 20090-1112
1-800-331-1MAA FAX: 1-301-206-9789

2

Prime Time

The Prime Numbers

One of the principal strategies by which we come to understand our physical or conceptual world is to break things down into pieces, describe the most basic pieces, and then describe how those pieces are assembled to create the whole. Our goal is to understand the natural numbers, so here we adopt that reductionist strategy and think about breaking natural numbers into pieces.

We begin by thinking about how natural numbers can be combined to create other natural numbers. The most basic method is through addition. So let's think about breaking natural numbers into their most basic pieces from the point of view of addition. What are the 'elements' so to speak with respect to addition of natural numbers? The answer is that there is only one element, the number 1. Every other natural number can be further broken down into smaller natural numbers that add together to create the number we started with. Every natural number is simply the sum of $1 + 1 + 1 + \cdots + 1$. Of course, this insight isn't too illuminating since every natural number looks very much like any other from this point of view. However, it does underscore the most basic property of the natural numbers, namely, that they all arise from the process of just adding 1 some number of times. In fact, this property of natural numbers lies at the heart of inductive processes both for constructing the natural numbers and often for proving theorems about them.

A more interesting way of constructing larger natural numbers from smaller ones is to use multiplication. Let's think about what the elementary particles, so to speak, are of the natural numbers with respect to multipli-

cation. That is, what are the natural numbers that cannot be broken down into smaller natural numbers through multiplication. What natural numbers are not the product of smaller natural numbers? The answer, of course, is the prime numbers.

The study of primes is one of the main focuses of number theory. As we shall prove, every natural number greater than 1 is either prime or it can be expressed as a product of primes. Primes are the multiplicative building blocks of all the natural numbers.

The prime numbers give us a world of questions to explore. People have been exploring primes for literally thousands of years, and many questions about primes are still unanswered. We will prove that there are infinitely many primes, but how are they distributed among the natural numbers? How many primes are there less than a natural number n? How can we find them? How can we use them? These questions and others have been among the driving questions of number theory for centuries and have led to an incredible amount of beautiful mathematics.

New concepts in mathematics open frontiers of new questions and uncharted paths of inquiry. When we think of an idea, like the idea of prime numbers, we can pose questions about them to integrate the new idea with our already established web of knowledge. New mathematical concepts then arise by making observations, seeing connections, clarifying our ideas by making definitions, and then making generalizations or abstractions of what we have observed.

When we have isolated a concept sufficiently to make a definition, then we can state new theorems. We will see not only new theorems, but also new types of proof.

All proofs are simply sequences of statements that follow logically from one another, but one structure of proof that you will develop and use in this chapter and future chapters is proof by induction. You will naturally come up with inductive styles of proving theorems on your own. In fact you may already have used this kind of argument in the last chapter, for example, in proving that the Euclidean Algorithm works. Inductive styles of proof are so useful that it is worthwhile to reflect on the logic involved. We have included an appendix that describes this technique of proof, and this may be a good time to work through that appendix.

Fundamental Theorem of Arithmetic

The role of definitions in mathematics cannot be overemphasized. They allow us to be precise in our language and reasoning. When a new definition

is introduced, you should take some time to familiarize yourself with its details. Try to get comfortable with its meaning. Look at examples. Memorize it.

Definition. A natural number $p > 1$ is *prime* if and only if p is not the product of natural numbers less than p.

Definition. A natural number n is *composite* if and only if n is a product of natural numbers less than n.

The following theorem tells us that every natural number larger than 1 has at least one prime factor.

2.1 Theorem. *If n is a natural number greater than 1, then there exists a prime p such that $p|n$.*

To get accustomed to primes, it's a good idea to find some.

2.2 Exercise. *Write down the primes less than 100 without the aid of a calculator or a table of primes and think about how you decide whether each number you select is prime or not.*

You probably identified the primes in the previous exercise by trial division. For example, to determine whether or not 91 was prime, you might have first tried dividing it by 2. Once convinced that 2 does not divide 91, you probably moved on to 3; then 4; then 5; then 6. Finally, you reached 7 and discovered that in fact 91 is not a prime. You were probably relieved, as you might have secretly feared that you would have to continue the daunting task of trial division 91 times! The following theorem tells us that you need not have been too concerned.

2.3 Theorem. *A natural number $n > 1$ is prime if and only if for all primes $p \leq \sqrt{n}$, p does not divide n.*

2.4 Exercise. *Use the preceding theorem to verify that 101 is prime.*

The search for prime numbers has a long and fascinating history that continues to unfold today. Recently the search for primes has taken on practical significance because primes are used everyday in making internet communications secure, for example. Later, we will investigate ways that primes are used in cryptography. And we'll see some modern techniques of identifying primes. But let's begin with an ancient method for finding

primes. The following exercise introduces a very early method of identifying primes attributed to the scholar Eratosthenes (276–194 BC).

2.5 Exercise (Sieve of Eratosthenes). *Write down all the natural numbers from* 1 *to* 100, *perhaps on a* 10×10 *array. Circle the number* 2, *the smallest prime. Cross off all numbers divisible by* 2. *Circle* 3, *the next number that is not crossed out. Cross off all larger numbers that are divisible by* 3. *Continue to circle the smallest number that is not crossed out and cross out its multiples. Repeat. Why are the circled numbers all the primes less than* 100?

With our list of primes, we can begin to investigate how many primes there are and what proportion of natural numbers are prime.

2.6 Exercise. *For each natural number* n, *define* $\pi(n)$ *to be the number of primes less than or equal to* n.

1. *Graph* $\pi(n)$ *for* $n = 1, 2, \ldots, 100$.

2. *Make a guess about approximately how large* $\pi(n)$ *is relative to* n. *In particular, do you suspect that* $\frac{\pi(n)}{n}$ *is generally an increasing function or a decreasing function? Do you suspect that it approaches some specific number (as a limit) as* n *goes to infinity? Make a conjecture and try to prove it. Proving your conjecture is a difficult challenge. You might use a computer to extend your list of primes to a much larger number and see whether your conjecture seems to be holding up.*

Mathematicians do not give out the title of "Fundamental Theorem" too often. In fact, you may have only come across one or two in your lifetime (the Fundamental Theorem of Algebra and the Fundamental Theorem of Calculus come to mind). We might think of such theorems as somehow very important. If so, we would be correct. What makes a theorem important? One answer might be that it captures a basic relationship and that it is widely applicable to explaining a broad range of mathematics. We will see that the Fundamental Theorem of Arithmetic certainly possesses these qualities.

We will write the Fundamental Theorem of Arithmetic in two parts: the Existence part and the Uniqueness part. The Existence part says that every natural number bigger than 1 can be written as the product of primes and the Uniqueness part says basically that there is only one way to do so. For example, $24 = 2^3 \cdot 3 = 3 \cdot 2^3$.

2.7 Theorem (Fundamental Theorem of Arithmetic—Existence Part). *Every natural number greater than* 1 *is either a prime number or it can be expressed as a finite product of prime numbers. That is, for every natural number* n *greater than* 1, *there exist distinct primes* $p_1, p_2, \ldots, p_m$ *and natural numbers* $r_1, r_2, \ldots, r_m$ *such that*

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}.$$

The following lemma might be helpful in proving the Uniqueness part of the Fundamental Theorem of Arithmetic. A lemma is actually a theorem, but it is designed to be a step towards the proof of a more important theorem.

2.8 Lemma. *Let* p *and* $q_1, q_2, \ldots, q_n$ *all be primes and let* k *be a natural number such that* $pk = q_1 q_2 \cdots q_n$. *Then* $p = q_i$ *for some* i.

2.9 Theorem (Fundamental Theorem of Arithmetic—Uniqueness part). *Let* n *be a natural number. Let* $\{p_1, p_2, \ldots, p_m\}$ *and* $\{q_1, q_2, \ldots, q_s\}$ *be sets of primes with* $p_i \neq p_j$ *if* $i \neq j$ *and* $q_i \neq q_j$ *if* $i \neq j$. *Let* $\{r_1, r_2, \ldots, r_m\}$ *and* $\{t_1, t_2, \ldots, t_s\}$ *be sets of natural numbers such that*

$$\begin{aligned} n &= p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m} \\ &= q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}. \end{aligned}$$

Then $m = s$ *and* $\{p_1, p_2, \ldots, p_m\} = \{q_1, q_2, \ldots, q_s\}$. *That is, the sets of primes are equal but their elements are not necessarily listed in the same order; that is,* p_i *may or may not equal* q_i. *Moreover, if* $p_i = q_j$ *then* $r_i = t_j$. *In other words, if we express the same natural number as a product of powers of distinct primes, then the expressions are identical except for the ordering of the factors.*

Putting the existence and uniqueness parts together, we get the whole formulation of the Fundamental Theorem of Arithmetic:

Theorem (Fundamental Theorem of Arithmetic). *Every natural number greater than* 1 *is either a prime number or it can be expressed as a finite product of prime numbers where the expression is unique up to the order of the factors.*

Let's take a moment to think through a little issue about our definition of "prime." Humans make decisions about what definitions to make. Let's think about the choices we made in defining "prime." One notion of "prime" is the inability to further decompose. Surely 1 meets this criterion. Yet our

choice of definition of prime omits 1. What is the advantage to not choosing to include 1 among the prime numbers? If 1 were called a prime, why would the Fundamental Theorem of Arithmetic no longer be true?

The Fundamental Theorem of Arithmetic tells us that every natural number bigger than 1 is a product of primes. Here are some exercises that help to show what that means in some specific cases.

2.10 Exercise. *Express $n = 12!$ as a product of primes.*

2.11 Exercise. *Determine the number of zeroes at the end of* $25!$.

The Fundamental Theorem of Arithmetic says that for any natural number $n > 1$ there exist distinct primes $\{p_1, p_2, \ldots, p_m\}$ and natural numbers $\{r_1, r_2, \ldots, r_m\}$ such that

$$n = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$$

and moreover, the factorization is unique up to order. When the p_i are ordered so that $p_1 < p_2 < \cdots < p_m$ we will say that $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ is the *unique prime factorization of* n.

Applications of the Fundamental Theorem of Arithmetic

One application of the Fundamental Theorem of Arithmetic is that if we know the prime factorizations of two natural numbers, it is a simple matter to determine whether one divides the other. The following is a characterization of divisibility in terms of primes. There are lots of letters and lots of subscripts, but once understood, this theorem makes sense.

2.12 Theorem. *Let a and b be natural numbers greater than 1 and let $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ be the unique prime factorization of a and let $q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}$ be the unique prime factorization of b. Then $a|b$ if and only if for all $i \leq m$ there exists a $j \leq s$ such that $p_i = q_j$ and $r_i \leq t_j$.*

Prime factorizations make it easy to prove some assertions that might otherwise be more difficult.

2.13 Theorem. *If a and b are natural numbers and $a^2|b^2$, then $a|b$.*

Prime factorizations can help us to find the greatest common divisor and least common multiple of two natural numbers. Here are some examples.

2.14 Exercise. *Find* $(3^{14} \cdot 7^{22} \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17)$.

2.15 Exercise. *Find* $\text{lcm}(3^{14} \cdot 7^{22} \cdot 11^5 \cdot 17^3, 5^2 \cdot 11^4 \cdot 13^8 \cdot 17)$.

After doing some examples, we instinctively seek the general pattern. That is, we seek to make a general statement that captures the reason that the method we used in the specific examples works.

2.16 Exercise. *Make a conjecture that generalizes the ideas you used to solve the two previous exercises.*

2.17 Question. *Do you think this method is always better, always worse, or sometimes better and sometimes worse than using the Euclidean Algorithm to find* (a, b)*? Why?*

The following theorem requires a clever use of the Fundamental Theorem of Arithmetic.

2.18 Theorem. *Given* $n+1$ *natural numbers, say* $a_1, a_2, \ldots, a_{n+1}$*, all less than or equal to* $2n$*, then there exists a pair, say* a_i *and* a_j *with* $i \neq j$*, such that* $a_i | a_j$.

The Fundamental Theorem of Arithmetic can be used to prove that certain equations do not have integer solutions.

2.19 Theorem. *There do not exist natural numbers* m *and* n *such that* $7m^2 = n^2$.

2.20 Theorem. *There do not exist natural numbers* m *and* n *such that* $24m^3 = n^3$.

Up to this point we have been talking exclusively about natural numbers and integers. Our insights into natural numbers and integers can actually help us to understand more general kinds of numbers such as rational numbers and irrational numbers.

Definition. A *rational number* is a real number that can be written as $\frac{a}{b}$ where a and b are integers and $b \neq 0$.

Definition. A real number that is not rational is *irrational*.

The next theorems ask you to prove that certain specific numbers are irrational.

2.21 Exercise. *Show that* $\sqrt{7}$ *is irrational. That is, there do not exist natural numbers* n *and* m *such that* $\sqrt{7} = \frac{n}{m}$.

2.22 Exercise. *Show that* $\sqrt{12}$ *is irrational.*

2.23 Exercise. *Show that* $7^{\frac{1}{3}}$ *is irrational.*

Having proved some specific numbers are irrational we take the usual step of generalizing our insights as far as possible.

2.24 Question. *What other numbers can you show to be irrational? Make and prove the most general conjecture you can.*

Let's now return to the world of integers. The following was a theorem we first proved in Chapter 1. Here we repeat the theorem with the idea that the Fundamental Theorem of Arithmetic might help to provide an alternative proof.

2.25 Theorem. *Let* a, b, *and* n *be integers. If* $a|n$, $b|n$, *and* $(a,b) = 1$, *then* $ab|n$.

Integers are either divisible by a prime p or are relatively prime to p.

2.26 Theorem. *Let* p *be a prime and let* a *be an integer. Then* p *does not divide* a *if and only if* $(a, p) = 1$.

Notice that $9|(6 \cdot 12)$ and yet 9 does not divide either 6 or 12. However, if a prime divides a product of two integers, then it must divide one or the other.

2.27 Theorem. *Let* p *be a prime and let* a *and* b *be integers. If* $p|ab$, *then* $p|a$ *or* $p|b$.

The following theorems explore the relationships among the greatest common divisor and various arithmetic operations. You might consider proving them in at least two ways, one using the Fundamental Theorem of Arithmetic and one using the techniques from Chapter 1.

2.28 Theorem. *Let* a, b, *and* c *be integers. If* $(b,c) = 1$, *then* $(a,bc) = (a,b) \cdot (a,c)$.

2.29 Theorem. *Let* a, b, *and* c *be integers. If* $(a,b) = 1$ *and* $(a,c) = 1$, *then* $(a,bc) = 1$.

2.30 Theorem. *Let* a *and* b *be integers. If* $(a,b) = d$, *then* $(\frac{a}{d}, \frac{b}{d}) = 1$.

2.31 Theorem. *Let a, b, u, and v be integers. If $(a,b) = 1$ and $u|a$ and $v|b$, then $(u,v) = 1$.*

The infinitude of primes

One of the most basic questions we can ask about prime numbers is, "How many are there?" In this section, we will prove that there are infinitely many. To prove that there are infinitely many primes, we need to show that there are large natural numbers that are not the product of smaller natural numbers. Our first observation points out that consecutive natural numbers cannot share common divisors greater than 1.

2.32 Theorem. *For all natural numbers n, $(n, n+1) = 1$.*

Can you think of a natural number that is divisible by 2, 3, 4, and 5? Can you think of a natural number that has a remainder of 1 when divided by 2, 3, 4, and 5? If you think of systematic ways to answer these questions, you will be well on your way to proving the following theorem.

2.33 Theorem. *Let k be a natural number. Then there exists a natural number n (which will be much larger than k) such that no natural number less than k and greater than 1 divides n.*

The previous theorem shows us how to produce natural numbers that are specifically not divisible by certain natural numbers. This insight helps us to find natural numbers that are not divisible by any natural numbers other than themselves and 1, in other words, primes.

2.34 Theorem. *Let k be a natural number. Then there exists a prime larger than k.*

The Infinitude of Primes Theorem is one of the basic results of mathematics. It was proved in ancient times and is recognized as one of the foundational theorems about numbers. At first you might think, "Of course, there must be infinitely many primes. How could there not be infinitely many primes since there are infinitely many natural numbers?" But remember that the same prime can be used many times. For example, we can construct arbitrarily large natural numbers just by raising 2 to large powers. So it is conceivable that some finite number of primes would suffice to produce all natural numbers. However, in fact there are infinitely many primes, as you will now prove.

2.35 Theorem (Infinitude of Primes Theorem). *There are infinitely many prime numbers.*

After you have devised a proof or proofs or learned a proof, it is satisfying to reflect on the logic of the argument and celebrate and appreciate the beauty or cleverness of the reasoning.

2.36 Question. *What were the most clever or most difficult parts in your proof of the Infinitude of Primes Theorem?*

One of the principal ways that new mathematics is created is to take one result and see whether it can be extended or variations of it can be proved. In the case of the Infinitude of Primes, we can ask whether there are infinitely many primes of a certain type. We begin by making an observation about numbers congruent to 1 modulo 4, which then will help us to prove that there are infinitely many primes of the form $4k + 3$.

2.37 Theorem. *If $r_1, r_2, \ldots, r_m$ are natural numbers and each one is congruent to* 1 *modulo* 4, *then the product $r_1 r_2 \cdots r_m$ is also congruent to* 1 *modulo* 4.

To prove the following theorem, remember the proof of the Infinitude of Primes Theorem and see how the strategy of that proof might be adapted to prove the following harder theorem.

2.38 Theorem (Infinitude of $4k + 3$ Primes Theorem). *There are infinitely many prime numbers that are congruent to* 3 *modulo* 4.

When you have proved the previous theorem, you will have forced yourself to understand a technique of proving theorems about the existence of infinitely many primes of a certain type. Now is the time to see how far that technique can be pushed. In other words ask yourself how many theorems like the preceding one are provable using a similar idea.

2.39 Question. *Are there other theorems like the previous one that you can prove?*

In fact, the following much more general theorem is true. Its proof in its full generality, however, is quite difficult and we will not attempt it in this course.

Theorem (Infinitude of $ak + b$ Primes Theorem). *If a and b are relatively*

prime natural numbers, then there are infinitely many natural numbers k for which $ak + b$ is prime.

The previous theorem is often called *Dirichlet's Theorem on primes in an arithmetic progression* and is due to Lejeune Dirichlet (1805–1859). An arithmetic progression is a sequence of numbers of the form $ak + b$, $k = 0, 1, 2, \ldots$, where b is any integer and a is a natural number. It is a sequence of numbers all of which are congruent to b modulo a. The study of primes in arithmetic progressions is still an active field today. Consider the following recent result due to Ben Green and Terence Tao.

Theorem (Green and Tao, 2005). *There are arbitrarily long arithmetic progressions of primes.*

This means that for any natural number n there exists a prime p and a natural number a such that p, $p + a$, $p + 2a$, $p + 3a$, ..., $p + na$ are all prime. As an example, an arithmetic progression of primes of length five is found by choosing $p = 5$ and $a = 6$, which yields the sequence $5, 11, 17, 23, 29$. The longest known arithmetic progression of primes as of July of 2004 has length 23 and is given by

$$56211383760397 + k\,44546738095860,\ k = 0, \ldots, 22.$$

Terence Tao was awarded a Fields medal in part for his work related to this result. Fields medals, the mathematical equivalent of the Nobel prize, are awarded once every four years to outstanding mathematicians under the age of 40.

2.40 Exercise. *Find the current record for the longest arithmetic progression of primes.*

Primes of special form

The largest known prime is of a special type known as a Mersenne prime, which is a prime of the form $2^n - 1$. The theorems here show some features of Mersenne primes and related primes.

2.41 Exercise. *Use polynomial long division to compute* $(x^m - 1) \div (x - 1)$.

2.42 Theorem. *If n is a natural number and $2^n - 1$ is prime, then n must be prime.*

2.43 Theorem. *If n is a natural number and $2^n + 1$ is prime, then n must be a power of 2.*

Definition. A *Mersenne prime* is a prime of the form $2^p - 1$, where p is a prime. A prime of the form $2^{2^k} + 1$ is called a *Fermat prime.*

2.44 Exercise. *Find the first few Mersenne primes and Fermat primes.*

2.45 Exercise. *For an A in the class and a Ph.D. in mathematics, prove that there are infinitely many Mersenne primes (or Fermat primes) or prove that there aren't (your choice).*

The distribution of primes

We now know that there are infinitely many primes, but in a sense that information is a rather crude measure of how the primes appear among the natural numbers. We could ask other questions such as roughly what fraction of the natural numbers are prime? And we might wonder whether the primes occur in some sort of pattern. To investigate how the primes are distributed among the natural numbers, let's begin by looking at some ranges of natural numbers with the primes printed in bold:

1, **2**, **3**, 4, **5**, 6, **7**, 8, 9, 10, **11**, 12, **13**, 14, 15, 16, **17**, 18, **19**, 20, 21,

22, **23**, 24, . . . , 300, 301, 302, 303, 304, 305, 306, **307**, 308, 309,

310, **311**, 312, **313**, 314, 315, 316, . . . , 2025, 2026, **2027**, 2028,

2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, . . .

What observations can we make? First, we may notice that the proportion of bold numbers occurring seems to be getting smaller. That is, primes tend to be more sparse as we move further out into the sequence of natural numbers. We tend to see longer and longer runs of consecutive composite numbers. In fact, there is no limit to the length of strings of composite numbers.

2.46 Theorem. *There exist arbitrarily long strings of consecutive composite numbers. That is, for any natural number n there is a string of more than n consecutive composite numbers.*

On the other hand, we still observe pairs of primes separated by just one even number, such as 311 and 313, or 2027 and 2029. One of the

most famous unanswered questions in number theory asks whether or not this behavior continues indefinitely. If you have already settled the previous question about Mersenne primes, then solving the following question will give you another Ph.D.

2.47 Question (The Twin Primes Question). *Are there infinitely many pairs of prime numbers that differ from one another by two? (The pairs* 11 *and* 13, 29 *and* 31, 41 *and* 43 *are examples of such twin primes.)*

Out of the first 24 natural numbers, 9 of them are primes—that's just a little over one third. We saw how this fraction changes as n increases in the Sieve of Eratosthenes exercise.

Suppose someone asked you to write down all the primes less than 100 million without the aid of a calculator or a computer. With a pencil and paper, you would find that task to be tedious and prone to error; however, that was the challenge facing mathematicians before the advent of modern computing machinery. Surely one of the most amazing feats of prime-finding before computers was completed in about 1863, when J.P. Kulik finished his 20-year project of finding the least prime factor of every natural number up to 100 million. Our sadness in losing the volume of Kulik's work that contained the natural numbers between 12,642,600 and 22,852,800 is somewhat lessened by the fact that his work was full of errors and that a modern computer could reproduce the whole work in a matter of seconds.

The significance of computing lists of primes before the invention of computers and even before Kulik's work is that those lists allowed mathematicians to gain some intuition about the distribution of primes.

As we observed above, the *proportion* of primes seems to slowly go downward. That is, the *percentage* of numbers less than a million that are prime is smaller than the *percentage* of numbers less than a thousand that are prime. The primes, in some sense, get sparser and sparser among the bigger numbers. That observation was greatly refined in the 1790s by Carl Friedrich Gauss (1777–1855), known by many as the Prince of Mathematics, and Adrien-Marie Legendre (1752–1833). They conjectured that the number of primes less than the natural number n, which is denoted by $\pi(n)$, is approximated by n divided by the *natural logarithm* of n. Using computers, we can produce evidence that the proportion of primes less than n becomes increasingly smaller as n increases. Table 1 also shows that the ratio between $\pi(n)$ and the fraction $\frac{n}{\ln(n)}$ gets increasingly closer to 1.

n	$\pi(n)$	$\frac{\pi(n)}{n}$	$\frac{n}{\ln(n)}$	$\frac{\pi(n)}{n/\ln(n)}$
10	4	.4	4.3...	0.92104...
10^2	25	.25	21.7...	1.15133...
10^3	168	.168	144.7...	1.16054...
10^4	1229	.1229	1085.7...	1.13199...
10^5	9592	.09592	8685.8...	1.10443...
10^6	78498	.078498	72382.4...	1.08452...
10^7	664579	.0664579	620420.7...	1.07121...
10^8	5761455	.05761455	5428681.0...	1.06144...
10^9	50847534	.050847534	48254942.4...	1.05385...

Table 1. Prime Proportions

The formal statement of these observations is called The Prime Number Theorem. We state it here, but the proofs of this theorem are difficult, and beyond the scope of this book.

Theorem (The Prime Number Theorem). *As n approaches infinity, the number of primes less than n, $\pi(n)$, approaches $\frac{n}{\ln(n)}$, that is,*

$$\lim_{n\to\infty}\left(\frac{\pi(n)}{n/\ln(n)}\right) = 1.$$

Finally, we mention here one more famous open question concerning prime numbers.

2.48 Exercise. *Express each of the first 20 even numbers greater than 2 as a sum of two primes. (For example: $8 = 5 + 3$.)*

In a letter to Euler, dated June 7, 1742, Christian Goldbach (1690–1764) claimed that every natural number greater than 2 was the sum of three primes. It was convention at the time to include the number 1 as being among the primes. The conjecture was re-expressed by Euler as follows.

Conjecture (The Goldbach Conjecture). *Every positive, even number greater than 2 can be written as the sum of two primes.*

The Goldbach Conjecture has been verified by computer, as of June of 2006, for all even numbers up to 400,000,000,000,000,000. As the even numbers get larger, there seem to be more ways to write them as a sum of two primes. For example, the number 100,000,000 can be written as the

sum of two primes in 219,400 different ways. But no one knows how to prove that in general all even natural numbers are the sum of two primes. Perhaps some even number with 10 trillion digits is not the sum of two primes. Until we have a general method of proof that will apply to all even numbers, we will not know whether such a natural number exists or not.

2.49 Blank Paper Exercise. *After not looking at the material in this chapter for a day or two, take a blank piece of paper and outline the development of that material in as much detail as you can without referring to the text or to notes. Places where you get stuck or can't remember highlight areas that may call for further study.*

From Antiquity to the Internet

Interest in the multiplicative properties of the natural numbers surely predated the works of Euclid (*Elements*, Books VII, VIII, IX), but it is here that we find the first written study. For example, Proposition 20 of Book IX gives the first known proof of the infinitude of primes. The ancient Greeks' interest in the primes may have been further spawned by the connection they shared with *perfect numbers*. A natural number is said to be *perfect* if it is equal to the sum of its proper divisors. For example, the smallest perfect number is 6, since 6=1+2+3. We list the first four perfect numbers.

$$6 = 2^{2-1}(2^2 - 1) = 1 + 2 + 3$$
$$28 = 2^{3-1}(2^3 - 1) = 1 + 2 + 4 + 7 + 14$$
$$496 = 2^{5-1}(2^5 - 1) = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$$
$$8128 = 2^{7-1}(2^7 - 1) = 1 + 2 + 4 + 8 + 16 + \cdots + 2032 + 4064$$

In Book IX of his *Elements* Euclid proved the following: if for some n, $2^n - 1$ is prime, then $2^{n-1}(2^n - 1)$ is perfect. This established the link between perfect numbers and primes of the form $2^n - 1$.

The serious study of perfect numbers and primes of special forms was picked up again in the seventeenth century by the likes of Rene Descartes (1596–1650), Pierre de Fermat (1601–1665), and Marin Mersenne (1588–1648). In a 1638 letter to Mersenne, Descartes stated that he thought he could prove that every even perfect number was of the form given by Euclid's theorem, but no proof was given. Also in a letter to Mersenne, dated 1640, Fermat indicated he had proved the following: if n is composite, then $2^n - 1$ is composite; but if n is prime, then $2^n - 1$ need not be prime, with two examples being $2^{11} - 1 = 23 \cdot 89$, and $2^{23} - 1 = 47 \cdot 178481$.

In 1647 Mersenne gave the following list of 11 primes p for which he believed $2^p - 1$ was prime as well: 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. He erred only by including 67 (and excluding 61, 89 and 107). To this day primes of the form $2^p - 1$ are called Mersenne primes, and it is still unknown whether infinitely many exist. In a posthumously published paper, Euler finally succeeded in proving that all even perfect numbers are of Euclid's type, giving a one-to-one correspondence between Mersenne primes and even perfect numbers. Curiously, it is not known if any odd perfect numbers exist.

The search for new Mersenne primes continues to this day. In fact, anyone with a home computer and an internet connection can join the *Great Internet Mersenne Prime Search* (GIMPS). Mersenne's list has only been increased to contain 44 examples as of September, 2006, with the largest having over 9.8 million digits.

2.50 Exercise. *Find the current record for the largest known Mersenne prime.*

There is a monetary award of $100,000 for the first person (or group) to find a Mersenne prime with at least 10 million digits. So happy hunting.

8

Pythagorean Triples, Sums of Squares, and Fermat's Last Theorem

Congruences to Equations

The Law of Quadratic Reciprocity gives us a neat view of which numbers are squares modulo a prime p. Information about squares modulo p can help us to understand actual numbers and equations in addition to modular numbers and congruences. In this chapter and the next we turn from quadratic congruences to quadratic (and higher order) Diophantine equations. We start with a quadratic equation we should all have some familiarity with from its connections to right triangles and the Pythagorean Theorem. Some of the questions will lead us to ask which numbers can be written as sums of squares, and the Law of Quadratic Reciprocity will help us find an answer. Finally, we turn to one of the most famous recent results of number theory, Fermat's Last Theorem.

Pythagorean triples

The Pythagorean Theorem asserts that the sum of the squares on the legs of a right triangle equals the square on the hypotenuse. Said another way, the lengths of the sides of a right triangle always provide a solution to the equation

$$x^2 + y^2 = z^2$$

by substituting the lengths of the legs for x and y and the length of the hypotenuse for z. In this section we consider the above quadratic as a Diophantine equation, that is, we consider only its integer solutions.

Definition. A triple of three positive integers (a, b, c) satisfying $a^2 + b^2 = c^2$ is called a *Pythagorean triple.*

Due to the close relationship with right triangles, the values a and b in a Pythagorean triple will sometimes be referred to as the *legs*, and the value c as the *hypotenuse.*

There are no Pythagorean triples in which both legs are odd.

8.1 Theorem. *If (a, b, c) is a Pythagorean triple, then at least one of a or b is even.*

The most famous Pythagorean triples are $(3, 4, 5)$ and $(5, 12, 13)$, but there are infinitely many. Let's begin by just finding a few.

8.2 Exercise. *Find at least seven different Pythagorean triples. Make a note of your methods.*

You may have discovered how to generate new Pythagorean triples from old ones through multiplication. Namely, if (a, b, c) is any Pythagorean triple and d is any natural number, then (da, db, dc) is also a Pythagorean triple. Pythagorean triples that are not simply multiples of smaller Pythagorean triples have a special designation.

Definition. A Pythagorean triple (a, b, c) is said to be *primitive* if a, b, and c have no common factor.

There are infinitely many primitive Pythagorean triples, so let's start by finding a few.

8.3 Exercise. *Find at least five primitive Pythagorean triples.*

We saw earlier that no Pythagorean triple has both legs odd, but for primitive Pythagorean triples, the legs cannot both be even either.

8.4 Theorem. *In any primitive Pythagorean triple, one leg is odd, one leg is even, and the hypotenuse is odd.*

It turns out that there is a method for generating infinitely many Pythagorean Triples in an easy way. It comes from looking at some simple algebra from high school. Remember that

$$(x + y)^2 = x^2 + 2xy + y^2$$

and

$$(x - y)^2 = x^2 - 2xy + y^2.$$

The difference between the two is $4xy$. So we have a relationship that looks almost like a Pythagorean triple, namely, one square $(x+y)^2$ equals another square $(x-y)^2$ plus something that we wish were a square, namely $4xy$. How could we ensure that $4xy$ is a square? Simple, just choose x and y to be squares. This kind of analysis leads to the following theorem.

8.5 Theorem. *Let s and t be any two different natural numbers with $s > t$. Then*

$$(2st, (s^2 - t^2), (s^2 + t^2))$$

is a Pythagorean triple.

The preceding theorem lets us easily generate infinitely many Pythagorean triples, but, in fact, every primitive Pythagorean triple can be generated by choosing appropriate natural numbers s and t and making the Pythagorean triple as described in the preceding theorem. As a hint to the proof, we make a little observation.

8.6 Lemma. *Let (a, b, c) be a primitive Pythagorean triple where a is the even number. Then $\frac{c+b}{2}$ and $\frac{c-b}{2}$ are perfect squares, say, s^2 and t^2, respectively; and s and t are relatively prime.*

So now we can completely characterize all primitive Pythagorean triples.

8.7 Theorem (Pythagorean Triple Theorem)**.** *Let (a, b, c) be a triple of natural numbers with a even, b odd, and c odd. Then (a, b, c) is a primitive Pythagorean triple if and only if there exist relatively prime positive integers s and t, one even and one odd, such that $a = 2st$, $b = (s^2 - t^2)$, and $c = (s^2 + t^2)$.*

The formulas given in the Pythagorean Triple Theorem allow us to investigate the types of numbers that can occur in Pythagorean triples. Let's start our investigation by looking at examples.

8.8 Exercise. *Using the above formulas make a lengthy list of primitive Pythagorean triples.*

We'll begin by looking at the legs and then think about the hypotenuse later.

8.9 Exercise. *Make a conjecture that describes those natural numbers that can appear as legs in a primitive Pythagorean triple.*

You might have come up with the following theorem.

8.10 Theorem. *In every primitive Pythagorean triple, one leg is an odd integer greater than* 1 *and the other is a positive multiple of* 4.

This observation does not tell us which odd numbers are allowable or which multiples of 4 occur, but in fact every odd number and every multiple of 4 occurs as a leg in a Pythagorean triple.

8.11 Theorem. *Any odd number greater than* 1 *can occur as a leg in a primitive Pythagorean triple.*

8.12 Theorem. *Any positive multiple of* 4 *can occur as a leg in a primitive Pythagorean triple.*

To analyze what numbers can occur as the hypotenuse of a primitive Pythagorean triple is a bit trickier. It amounts to investigating the general problem of representing numbers as sums of two squares.

Sums of squares

The question we seek to answer is, for which numbers n does the Diophantine equation

$$x^2 + y^2 = n$$

have a solution? As usual we will first investigate the case of primes.

8.13 Question. *Make a list of the first fifteen primes and write each as the sum of as few squares of natural numbers as possible. Which ones can be written as the sum of two squares? Make a conjecture about which primes can be written as the sum of two squares of natural numbers.*

Your conjecture likely singles out those primes that are congruent to 1 modulo 4.

Theorem. *Let p be a prime. Then p can be written as the sum of two squares of natural numbers if and only if $p = 2$ or $p \equiv 1 \pmod 4$.*

There are really two theorems here and we will state them separately below. The first is a much simpler theorem to prove than the second.

8.14 Theorem. *Let p be a prime such that $p = a^2 + b^2$ for some natural numbers a and b. Then either $p = 2$ or $p \equiv 1 \pmod 4$.*

The fact that every prime congruent to 1 modulo 4 is expressible as the sum of two squares is more challenging to prove. As you work to prove this result in the next few theorems it is worthwhile to recall another theorem you recently proved about primes that are congruent to 1 modulo 4. For primes congruent to 1 modulo 4, -1 is a quadratic residue; that is, for any prime p that is congruent to 1 modulo 4, there is some natural number a such that a^2 is congruent to -1 modulo p. To prove the second theorem, try applying the following lemma to a square root of -1 modulo p.

8.15 Lemma. *Let p be a prime and let a be a natural number not divisible by p. Then there exist integers x and y such that $ax \equiv y \pmod{p}$ with $0 < |x|, |y| < \sqrt{p}$.*

8.16 Theorem. *Let p be a prime such that $p \equiv 1 \pmod{4}$. Then p is equal to the sum of two squares of natural numbers.*

(Hint: Try applying the previous lemma to a square root of -1 modulo p.)

Knowing which primes can be written as the sum of two squares is a great start, but that does not yet answer the question as to which numbers can occur as the hypotenuse of a primitive Pythagorean triple. We need a strategy for moving from primes to products of primes.

8.17 Exercise. *Check the following identity:*

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (bc - ad)^2.$$

The preceding exercise tells us that the products of sums of two squares are themselves sums of two squares.

8.18 Theorem. *If an integer x can be written as the sum of two squares of natural numbers and an integer y can be written as the sum of two squares of natural numbers, then xy can be written as the sum of two squares of natural numbers.*

Let's try writing a few numbers as sums of squares of natural numbers.

8.19 Exercise. *For each of the following numbers, (i) determine the number's prime factorization and (ii) write the number as the sum of two squares of natural numbers.*

1. 205
2. 6409

3. 722

4. 11745

8.20 Question. *Which natural numbers can be written as the sum of two squares of natural numbers? State and prove the most general theorem possible about which natural numbers can be written as the sum of two squares of natural numbers, and prove it.*

We give the most general result next.

8.21 Theorem. *A natural number n can be written as a sum of two squares of natural numbers if and only if every prime congruent to 3 modulo 4 in the unique prime factorization of n occurs to an even power.*

Pythagorean triples revisited

We are now in a position to describe the possible values for the hypotenuse in a primitive Pythagorean triple.

8.22 Theorem. *If (a, b, c) is a primitive Pythagorean triple, then c is a product of primes each of which is congruent to 1 modulo 4.*

8.23 Theorem. *If the natural number c is a product of primes each of which is congruent to 1 modulo 4, then there exist integers a and b such that (a, b, c) is a primitive Pythagorean triple.*

Having satisfactorily analyzed the question of which squares are the sum of two smaller squares, it is natural to ask the analogous question for higher powers, and Pierre de Fermat did ask that question in what became known as Fermat's Last Theorem.

Fermat's Last Theorem

There are infinitely many Pythagorean triples of natural numbers (a, b, c) such that $a^2+b^2 = c^2$. A natural question arises if we replace the exponent 2 with larger numbers. In other words, can we find triples of natural numbers (a, b, c) such that $a^3+b^3 = c^3$ or $a^4+b^4 = c^4$, or, in general, $a^n+b^n = c^n$ for $n \geq 3$? In 1637, Fermat claimed to be able to prove that no triple of natural numbers (a, b, c) exists that satisfies the equation $a^n + b^n = c^n$ for any natural number $n \geq 3$. During his lifetime, Fermat probably realized his "proof" was inadequate, but the question tantalized mathematicians for

hundreds of years. Incremental progress was made. By 1992 it was known that the equations $a^n + b^n = c^n$ had no natural number solutions for $3 \leq n \leq 4,000,000$ (as well as many other special cases). But there are infinitely many possible exponents larger than $4,000,000$, so Fermat's Last Theorem was far from being resolved. But all the remaining exponents were taken care of by the groundbreaking work of Andrew Wiles, which took place some 350 years after Fermat first considered the question.

Theorem (Fermat's Last Theorem, proved by Andrew Wiles in 1994). *For natural numbers $n \geq 3$, there are no natural numbers x, y, z such that $x^n + y^n = z^n$.*

We probably won't find a proof of this theorem ourselves since it took many high-powered mathematicians 350 years to do so. Instead, let's look at one case of this theorem which can be proved using a strategy known as *Fermat's method of descent*. The method involves showing how a given solution in natural numbers can be used to produce a "smaller" natural number solution. That new solution would imply the existence of a yet smaller solution, and so on. Since any decreasing sequence of natural numbers must be finite in length, the method of descent implies that there could not be a solution to begin with. Let's see how this strategy can be used to prove the case of Fermat's Last Theorem when the exponent is 4.

In fact, notice that the following statement is a little stronger than what is called for in Fermat's Last Theorem since the z is squared rather than raised to the fourth power.

8.24 Theorem. *There are no natural numbers x, y, and z such that $x^4 + y^4 = z^2$.*

(Hint: Note that if there were a solution $x = a$, $y = b$, and $z = c$, then (a^2, b^2, c) would be a Pythagorean triple, which we could assume to be a primitive Pythagorean triple by removing common factors. Can you use the characterization of Pythagorean triples to find other natural numbers d, e, f such that $d^4 + e^4 = f^2$ where f is less than c? If you can do that, how can you complete your proof?)

8.25 Blank Paper Exercise. *After not looking at the material in this chapter for a day or two, take a blank piece of paper and outline the development of that material in as much detail as you can without referring to the text or to notes. Places where you get stuck or can't remember highlight areas that may call for further study.*

Who's Represented?

Representing numbers as the sum of two squares had immediate practical relevance to the description of Pythagorean triples. But it is also a problem that lends itself well to many different possible directions of generalization. For example,

1. Which numbers can be represented as the sum of three squares; sum of four squares; etc.?

2. Which numbers can be represented as the sum of two cubes; sum of two fourth powers; etc.?

Mathematicians have given much attention to all of these questions. This is another one of the many instances of simple sounding questions leading to deep and important mathematics.

Sums of squares

Albert Girard (1595–1632) appeared to know as early as 1625 which numbers could be written as the sum of two squares, although a proof due to Girard is lacking. Descartes proved in a 1638 letter to Mersenne that primes of the form $4n + 3$ could not be represented as a sum of two squares. Fermat stated in a letter to Blaise Pascal (1623–1662) in 1654 that he had a proof of the fact that primes of the form $4n + 1$ were always the sum of two squares. But a proof of Girard's complete (and correct) observation would have to wait for Euler, who gave a complete proof in two letters to Goldbach dated 1747 and 1749.

What about representing numbers as the sum of three squares? In a letter to Mersenne dated 1636, Fermat stated (again without proof!) that no integer of the form $8n+7$ could be expressed as the sum of three squares. Mersenne communicated the claim to Descartes who provided a proof in 1638. The complete characterization is given here.

Theorem. *A natural number can be expressed as the sum of three squares of natural numbers if and only if it is not of the form* $4^n(8k + 7)$ *for non-negative integers* n *and* k.

The proof of this theorem is due in large part to Legendre, but a key step also requires Dirichlet's work on primes in arithmetic progressions.

What about sums of four squares? Fermat stated that he had a proof of the fact that every number is either a square or the sum of two, three,

or four squares, although, as we now expect when dealing with Fermat, no proof was communicated. Building on the work of Fermat and Euler, it was Lagrange in 1770 who finally provided the proof of the following theorem.

Theorem (Four Squares Theorem). *Every natural number is the sum of at most four squares of natural numbers.*

A key identity needed for Lagrange's proof was due to Euler, who spent more than 40 years trying to establish the Four Squares Theorem. Euler established an amazing identity showing that the product of two numbers, each of which can be expressed as the sum of four squares, is also a sum of four squares, namely,

$$\begin{aligned}(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)&\\ &= (a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2\\ &\quad + (a_1b_2-a_2b_1+a_3b_4-a_4b_3)^2\\ &\quad + (a_1b_3-a_2b_4-a_3b_1+a_4b_2)^2\\ &\quad + (a_1b_4+a_2b_3-a_3b_2-a_4b_1)^2.\end{aligned}$$

Sums of cubes, taxicabs, and Fermat's Last Theorem

Euler, in 1770, provided us with a proof of the first case of Fermat's Last Theorem by establishing that no cube is the sum of two cubes. Of the numbers which *can* be expressed as the sum of two cubes, perhaps 1729 is the most famous.

Suffering from tuberculosis and lying in a hospital bed in London, the young Indian mathematician Ramanujan (1887–1920) was paid a visit by his friend and mentor G. H. Hardy (1877–1947). Hardy remarked that he had arrived in a taxicab numbered 1729, which he considered a rather dull number. Ramanujan responded that 1729 is not dull at all. It is, in fact, the smallest number that can be expressed as the sum of two cubes in two essentially distinct ways,

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

Said another way, there are (at least) four distinct integer points, namely $(1, 12)$, $(12, 1)$, $(9, 10)$, and $(10, 9)$, on the cubic plane curve

$$x^3 + y^3 = 1729.$$

Taking statements about numbers and transforming them into statements about points on curves (or surfaces, etc.) is now a fairly common practice

in the field of *arithmetical geometry*. For example, in studying whether the number m is expressible as a sum of two cubes, the corresponding plane curve is given by

$$x^3 + y^3 = m.$$

This is another example of what is known as an *elliptic curve*. While naturally arising when looking at the problem of expressing a number as the sum of two cubes, elliptic curves have also played a much more central role in the modern development of number theory. They are the central objects under study in Andrew Wiles' proof of Fermat's Last Theorem.

In 1990 it was known that if (a, b, c) were a triple of natural numbers satisfying an equation of the form

$$a^p + b^p = c^p,$$

where p is a prime greater than 2 (i.e., if the triple (a, b, c) provided a counterexample to Fermat's Last Theorem), then the curve

$$y^2 = x(x - a^p)(x + b^p)$$

would be an elliptic curve with some very strange properties. The precise statement is that the curve would be *semistable* but not *modular*, although the exact meanings of these words is beyond the scope of this book. Such a curve was believed not to exist. More precisely, it was believed by many (and was the content of the Shimura-Taniyama Conjecture) that *all* elliptic curves were modular. This conjecture is now known to be true. The first major contribution to the proof of the Shimura-Taniyama Conjecture was due to Wiles with the help of his student Richard Taylor. Wiles and Taylor proved in 1994 that *all semistable elliptic curves are modular*, once and for all confirming the truth of Fermat's Last Theorem.