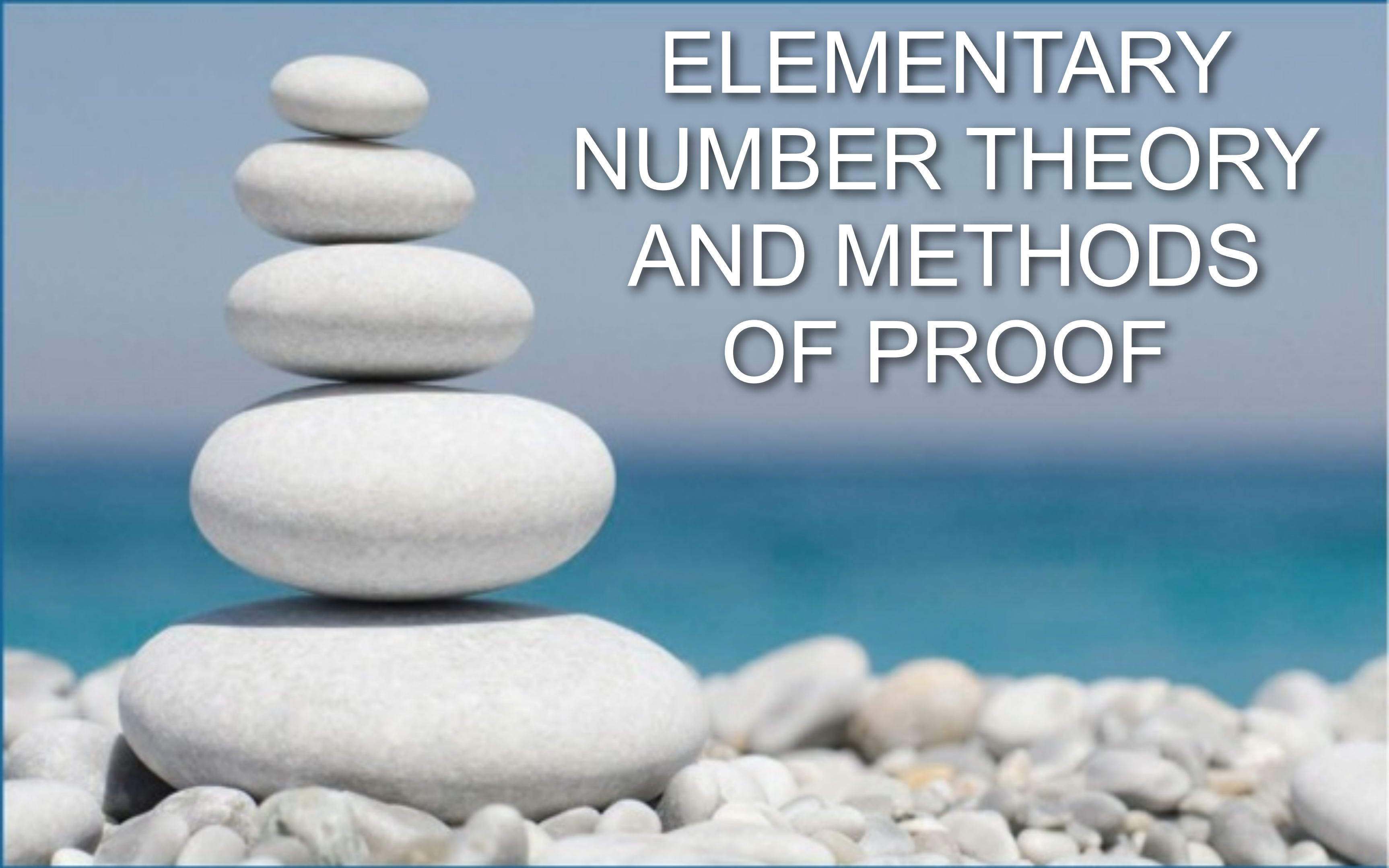
CHAPTER 4

ELEMENTARY NUMBER THEORY AND METHODS OF PROOF



SECTION 4.7

Indirect Argument: Two Classical Theorems

Indirect Argument: Two Classical Theorems

This section contains proofs of two of the most famous theorems in mathematics: that $\sqrt{2}$ is irrational and that there are infinitely many prime numbers.

Both proofs are examples of indirect arguments and were well known more than 2,000 years ago, but they remain exemplary models of mathematical argument to this day.

The Irrationality of $\sqrt{2}$

The Irrationality of $\sqrt{2}$

When mathematics flourished at the time of the ancient Greeks, mathematicians believed that given any two line segments, say *A*: ____ and *B*: ________, a certain unit of length could be found so that segment *A* was exactly *a* units long and segment *B* was exactly *b* units long.

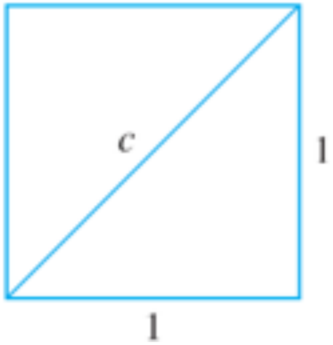
(The segments were said to be *commensurable* with respect to this special unit of length.)

Then the ratio of the lengths of *A* and *B* would be in the same proportion as the ratio of the integers *a* and *b*. Symbolically:

$$\frac{\text{length } A}{\text{length } B} = \frac{a}{b}.$$

The Irrationality of $\sqrt{2}$

Now it is easy to find a line segment of length $\sqrt{2}$; just take the diagonal of the unit square:



By the Pythagorean theorem, $c^2 = 1^2 + 1^2 = 2$, and so $c = \sqrt{2}$. If the belief of the ancient Greeks were correct, there would be integers *a* and *b* such that

$$\frac{\text{length (diagonal)}}{\text{length (side)}} = \frac{a}{b}.$$

The Irrationality of $\sqrt{2}$

And this would imply that

$$\frac{c}{1} = \frac{\sqrt{2}}{1} = \sqrt{2} = \frac{a}{b}.$$

But then $\sqrt{2}$ would be a ratio of two integers, or, in other words, $\sqrt{2}$ would be rational.

The proof begins by supposing the negation: $\sqrt{2}$ is rational. This means that there exist integers *m* and *n* such that $\sqrt{2} = m/n$.

The Irrationality of $\sqrt{2}$

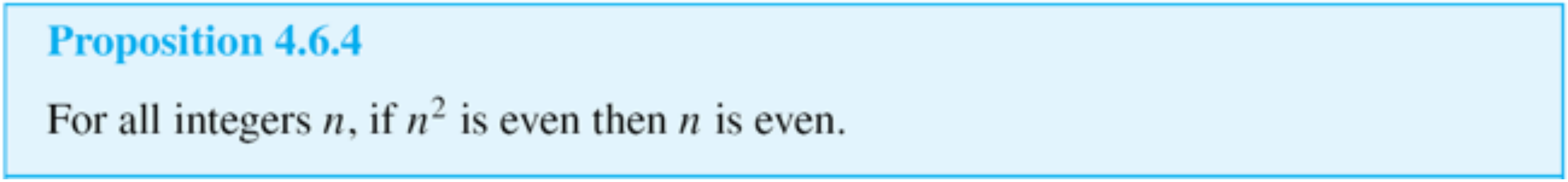
Now if *m* and *n* have any common factors, these may be factored out to obtain a new fraction, equal to *m*/*n*, in which the numerator and denominator have no common factors. (For example, $18/12 = (6 \cdot 3)/(6 \cdot 2) = 3/2$, which is a fraction whose numerator and denominator have no common factors.)

Thus, without loss of generality, we may assume that *m* and *n* had no common factors in the first place.

We will then derive the contradiction that *m* and *n* *do* have a common factor of 2.

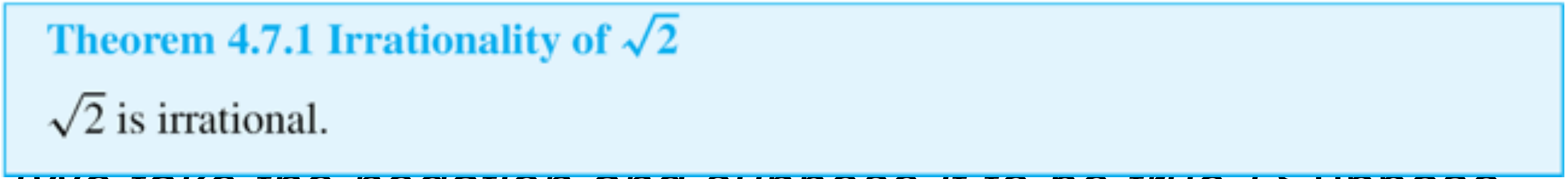
The Irrationality of $\sqrt{2}$

The argument makes use of Proposition 4.6.4. If the square of an integer is even, then that integer is even.



Proposition 4.6.4

For all integers n, if n^2 is even then n is even.



Theorem 4.7.1 Irrationality of $\sqrt{2}$

$\sqrt{2}$ is irrational.

[We take the negation and suppose it to be true.] Suppose not. That is, suppose   is rational.

$\sqrt{2}$

The Irrationality of $\sqrt{2}$

Then there are integers *m* and *n* with no common factors such that

$$\sqrt{2} = \frac{m}{n} \qquad 4.7.1$$

[by dividing m and n by any common factors if necessary]. [We must derive a contradiction.]

Squaring both sides of equation (4.7.1) gives

$$2 = \frac{m^2}{n^2}.$$

Or, equivalently,

$$m^2 = 2n^2. \qquad 4.7.2$$

The Irrationality of $\sqrt{2}$

Note that equation (4.7.2) implies that $m^2$is even (by definition of even). It follows that *m* is even (by Proposition 4.6.4). We file this fact away for future reference and also deduce (by definition of even) that

$$m = 2k \quad \text{for some integer } k. \qquad 4.7.3$$

Substituting equation (4.7.3) into equation (4.7.2), we see that

$$m^2 = (2k)^2 = 4k^2 = 2n^2.$$

Dividing both sides of the right-most equation by 2 gives

$$n^2 = 2k^2.$$

The Irrationality of $\sqrt{2}$

Consequently, n^2 s even, and so *n* is even (by Proposition 4.6.4). But we also know that *m* is even. *[This is the fact we filed away.] Hence both m* and *n* have a common factor of 2. But this contradicts the supposition that *m* and *n* have no common factors. *[Hence the supposition is false and so the theorem is true.]*

Are There Infinitely Many Prime Numbers?

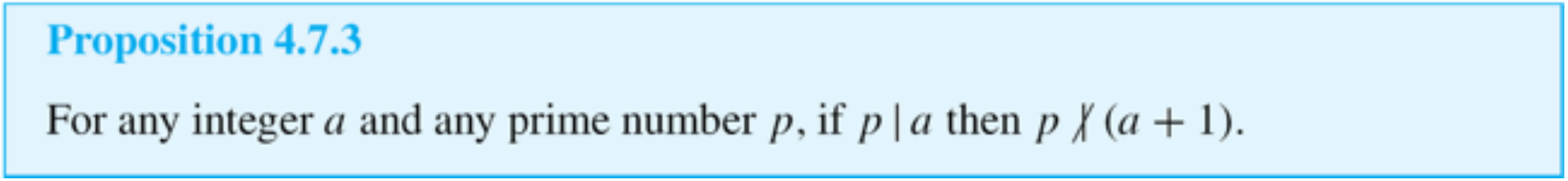
Are There Infinitely Many Prime Numbers?

You know that a prime number is a positive integer that cannot be factored as a product of two smaller positive integers.

Is the set of all such numbers infinite, or is there a largest prime number?

Are There Infinitely Many Prime Numbers?

Euclid’s proof requires one additional fact we have not yet established: If a prime number divides an integer, then it does not divide the next successive integer.



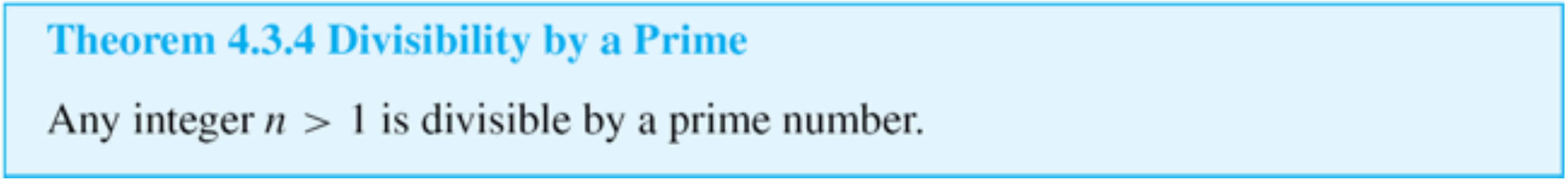
Proposition 4.7.3

For any integer a and any prime number p, if $p \mid a$ then $p \nmid (a+1)$.

The idea of Euclid’s proof is this: Suppose the set of prime numbers were finite. Then you could take the product of all the prime numbers and add one.

Are There Infinitely Many Prime Numbers?

By Theorem 4.3.4 this number must be divisible by some prime number.



Theorem 4.3.4 Divisibility by a Prime

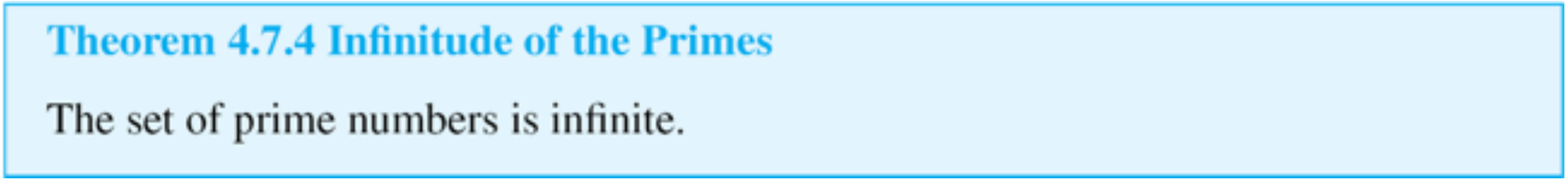
Any integer $n > 1$ is divisible by a prime number.

But by Proposition 4.7.3, this number is not divisible by any of the prime numbers in the set.

Are There Infinitely Many Prime Numbers?

Hence there must be a prime number that is not in the set of all prime numbers, which is impossible.

The following formal proof fills in the details of this outline.



Theorem 4.7.4 Infinitude of the Primes

The set of prime numbers is infinite.

Proof (by contradiction):

Suppose not. That is, suppose the set of prime numbers is finite. *[We must deduce a contradiction.]*

Are There Infinitely Many Prime Numbers?

Then some prime number *p* is the largest of all the prime numbers, and hence we can list the prime numbers in ascending order:

$$2,\ 3,\ 5,\ 7, 11, \ldots, p.$$

Let *N* be the product of all the prime numbers plus 1:

$$N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$$

Then *N* > 1, and so, by Theorem 4.3.4, *N* is divisible by some prime number *q*. Because *q* is prime, *q* must equal one of the prime numbers $2,\ 3,\ 5,\ 7, 11, \ldots, p.$

Are There Infinitely Many Prime Numbers?

Thus, by definition of divisibility, *q* divides

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p,$$

and so, by Proposition 4.7.3, *q* does not divide

$$(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1, \text{ which equals } N.$$

Hence *N* is divisible by *q* and *N* is not divisible by *q*, and we have reached a contradiction. *[Therefore, the supposition is false and the theorem is true.]*

When to Use Indirect Proof

When to Use Indirect Proof

Many theorems can be proved either way. Usually, however, when both types of proof are possible, indirect proof is clumsier than direct proof.

In the absence of obvious clues suggesting indirect argument, try first to prove a statement directly. Then, if that does not succeed, look for a counterexample.

If the search for a counterexample is unsuccessful, look for a proof by contradiction or contraposition.

Open Questions in Number Theory

Open Questions in Number Theory

In this section we proved that there are infinitely many prime numbers. There is no known formula for obtaining primes, but a few formulas have been found to be more successful at producing them than other formulas.

One such is due to Marin Mersenne, a French monk who lived from 1588–1648. *Mersenne primes* have the form $2^p - 1$, where p is prime.

Not all numbers of this form are prime, but because Mersenne primes are easier to test for primality than are other numbers, most of the largest known prime numbers are Mersenne primes.

Open Questions in Number Theory

An interesting question is whether there are infinitely many Mersenne primes. As of the date of publication of this book, the answer is not known, but new mathematical discoveries are being made every day and by the time you read this someone may have discovered the answer.

Another formula that seems to produce a relatively large number of prime numbers is due to Fermat.

Fermat primes are prime numbers of the form $2^{2^n} + 1$, where *n* is a positive integer. Are there infinitely many Fermat primes?

Open Questions in Number Theory

Again, as of now, no one knows. Similarly unknown are whether there are infinitely many primes of the form $n^2 + 1$, where n is a positive integer, and whether there is always a prime number between integers n^2 and $(n + 1)^2$.

Another famous open question involving primes is the *twin primes conjecture*, which states that there are infinitely many pairs of prime numbers of the form p and $p + 2$.

Open Questions in Number Theory

As with other well-known problems in number theory, this conjecture has withstood computer testing up to extremely large numbers, and some progress has been made toward a proof.

In 2004, Ben Green and Terence Tao showed that for any integer *m* > 1, there is a sequence of *m* equally spaced integers all of which are prime.

In other words, there are positive integers *n* and *k* so that the following numbers are all prime:

$$n, n+k,\ n+2k,\ n+3k,\ \ldots,\ n+(m-1)k.$$

Open Questions in Number Theory

Related to the twin primes conjecture is a conjecture made by Sophie Germain, a French mathematician born in 1776, who made significant progress toward a proof of Fermat’s Last Theorem.

Germain conjectured that there are infinitely many prime number pairs of the form p and $2p + 1$.

Initial values of p with this property are 2, 3, 5, 11, 23, 29, 41, and 53, and computer testing has verified the conjecture for many additional values.

Open Questions in Number Theory

In fact, as of the writing of this book, the largest prime p for which $2p$ + 1 is also known to be prime is $183027 \cdot 2^{265440} - 1$.

This is a number with 79911 decimal digits! But compared with infinity, any number, no matter how large, is less than a drop in the bucket.

In 1844, the Belgian mathematician Eugène Catalan conjectured that the only solutions to the equation $x^n - y^m = 1$, where x, y, n, and m are all integers greater than 1, is $3^2 - 2^3 = 1$.

This conjecture also remains unresolved to this day.

Open Questions in Number Theory

In 1993, while trying to prove Fermat’s last theorem, an amateur number theorist, Andrew Beal, became intrigued by the equation $x^m + y^n = z^k$, where no two of x, y, or z have any common factor other than ±1.

When diligent effort, first by hand and then by computer, failed to reveal any solutions, Beal conjectured that no solutions exist.

His conjecture has become known as *Beal’s conjecture*, and he has offered a prize of $100,000 to anyone who can either prove or disprove it.

Open Questions in Number Theory

These are just a few of a large number of open questions in number theory.

Many people believe that mathematics is a fixed subject that changes very little from one century to the next.

In fact, more mathematical questions are being raised and more results are being discovered now than ever before in history.