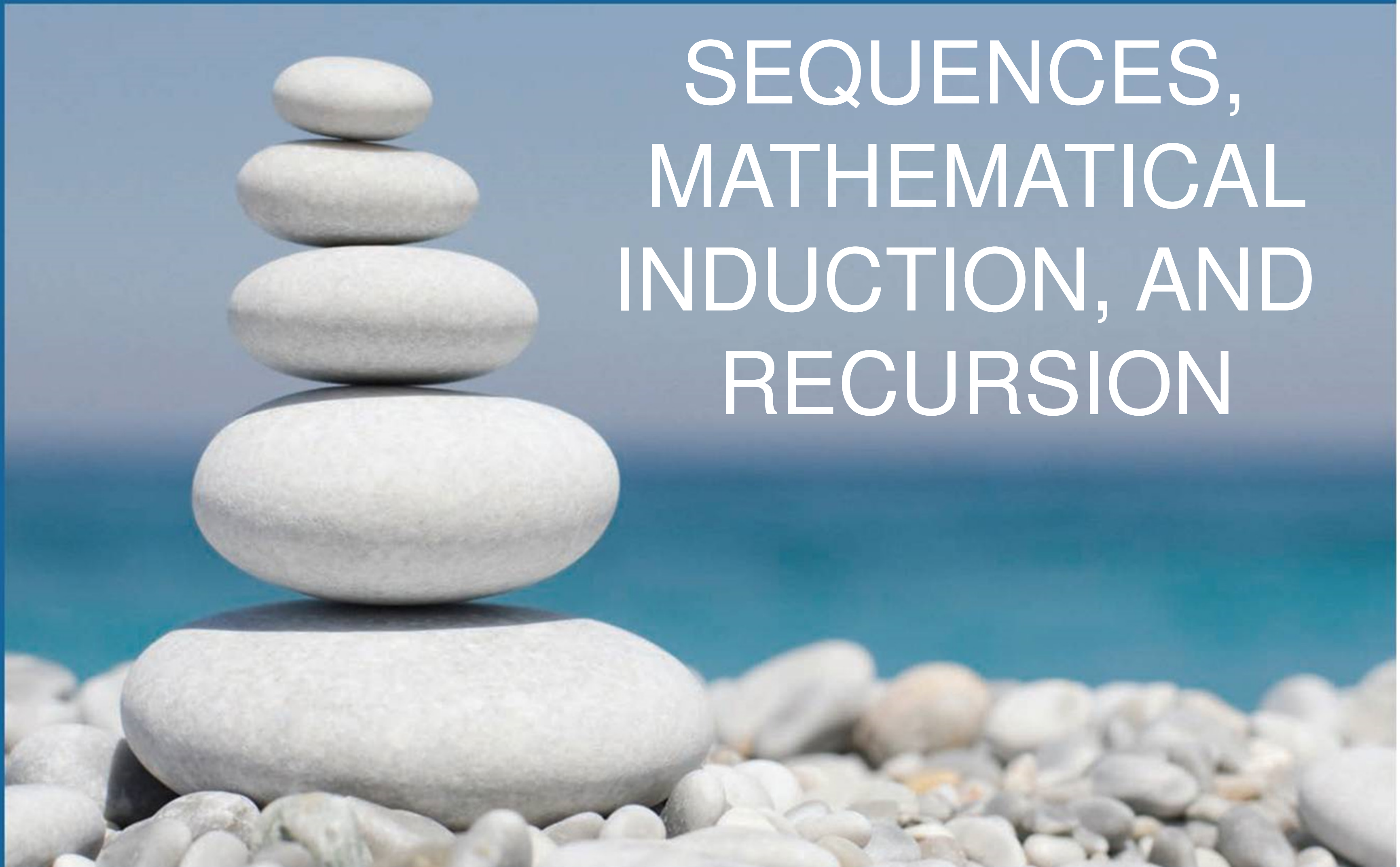
CHAPTER 5

SEQUENCES, MATHEMATICAL INDUCTION, AND RECURSION



SECTION 5.4

Strong Mathematical Induction and the Well-Ordering Principle for the Integers

Strong mathematical induction is similar to ordinary mathematical induction in that it is a technique for establishing the truth of a sequence of statements about integers.

Also, a proof by strong mathematical induction consists of a basis step and an inductive step.

However, the basis step may contain proofs for several initial values, and in the inductive step the truth of the predicate $P(n)$ is assumed not just for one value of n but for all values through k, and then the truth of $P(k + 1)$ is proved.

Principle of Strong Mathematical Induction

Let $P(n)$ be a property that is defined for integers n, and let a and b be fixed integers with $a \leq b$. Suppose the following two statements are true:

1. $P(a)$, $P(a+1)$, . . . , and $P(b)$ are all true. **(basis step)**
2. For any integer $k \geq b$, if $P(i)$ is true for all integers i from a through k, then $P(k+1)$ is true. **(inductive step)**

Then the statement

$$\text{for all integers } n \geq a,\ P(n)$$

is true. (The supposition that $P(i)$ is true for all integers i from a through k is called the **inductive hypothesis.** Another way to state the inductive hypothesis is to say that $P(a)$, $P(a+1)$, . . . , $P(k)$ are all true.)

Any statement that can be proved with ordinary mathematical induction can be proved with strong mathematical induction.

The reason is that given any integer $k \geq b$, if the truth of $P(k)$ alone implies the truth of $P(k + 1)$, then certainly the truth of $P(a)$, $P(a + 1)$, . . . , and $P(k)$ implies the truth of $P(k + 1)$.

It is also the case that any statement that can be proved with strong mathematical induction can be proved with ordinary mathematical induction.

The principle of strong mathematical induction is known under a variety of different names including the *second principle of induction*, *the second principle of finite induction*, and the *principle of complete induction*.

Applying Strong Mathematical Induction

Applying Strong Mathematical Induction

The divisibility-by-a-prime theorem states that any integer greater than 1 is divisible by a prime number.

We prove this theorem using strong mathematical induction.

Example 1 – *Divisibility by a Prime*

Prove: Any integer greater than 1 is divisible by a prime number.

Solution:

The idea for the inductive step is this: If a given integer greater than 1 is not itself prime, then it is a product of two smaller positive integers, each of which is greater than 1.

Since you are assuming that each of these smaller integers is divisible by a prime number, by transitivity of divisibility, those prime numbers also divide the integer you started with.

Example 1 – *Solution*

cont'd

Proof (by strong mathematical induction):

Let the property $P(n)$ be the sentence

n is divisible by a prime number. $\leftarrow P(n)$

Show that $P(2)$ is true:

To establish $P(2)$, we must show that

2 is divisible by a prime number. $\leftarrow P(2)$

But this is true because 2 is divisible by 2 and 2 is a prime number.

Example 1 – *Solution*

cont'd

Show that for all integers $k \geq 2$, if $P(i)$ is true for all integers i from 2 through k, then $P(k + 1)$ is also true:

Let k be any integer with $k \geq 2$ and suppose that

i is divisible by a prime number for all integers i from 2 through k. ← inductive hypothesis

We must show that

$k + 1$ is divisible by a prime number. ← $P(k + 1)$

Example 1 – *Solution*

cont'd

Case 1 (k + 1 is prime): In this case $k + 1$ is divisible by a prime number, namely itself.

Case 2 (k + 1 is not prime): In this case $k + 1 = ab$ where a and b are integers with $1 < a < k + 1$ and $1 < b < k + 1$.

Thus, in particular, $2 \leq a \leq k$, and so by inductive hypothesis, a is divisible by a prime number p.

In addition because $k + 1 = ab$, we have that $k + 1$ is divisible by a.

Example 1 – *Solution*

cont'd

Hence, since $k + 1$ is divisible by a and a is divisible by p, by transitivity of divisibility, $k + 1$ is divisible by the prime number p.

Therefore, regardless of whether $k + 1$ is prime or not, it is divisible by a prime number *[as was to be shown]*.

[Since we have proved both the basis and the inductive step of the strong mathematical induction, *we conclude that the given statement is true*.*]*

Applying Strong Mathematical Induction

Strong mathematical induction makes possible a proof of the fact used frequently in computer science that every positive integer n has a unique binary integer representation.

The proof looks complicated because of all the notation needed to write down the various steps. But the idea of the proof is simple.

It is that if smaller integers than n have unique representations as sums of powers of 2, then the unique representation for n as a sum of powers of 2 can be found by taking the representation for $n/2$ (or for $(n - 1)/2$ if n is odd) and multiplying it by 2.

Applying Strong Mathematical Induction

Theorem 5.4.1 Existence and Uniqueness of Binary Integer Representations

Given any positive integer n, n has a unique representation in the form

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

where r is a nonnegative integer, $c_r = 1$, and $c_j = 1$ or 0 for all $j = 0, 1, 2, \ldots, r-1$.

The Well-Ordering Principle for the Integers

The Well-Ordering Principle for the Integers

The well-ordering principle for the integers looks very different from both the ordinary and the strong principles of mathematical induction, but it can be shown that all three principles are equivalent.

That is, if any one of the three is true, then so are both of the others.

Well-Ordering Principle for the Integers

Let S be a set of integers containing one or more integers all of which are greater than some fixed integer. Then S has a least element.

Example 4 – *Finding Least Elements*

In each case, if the set has a least element, state what it is. If not, explain why the well-ordering principle is not violated.

a. The set of all positive real numbers.

b. The set of all nonnegative integers n such that $n^2 < n$.

c. The set of all nonnegative integers of the form $46 - 7k$, where k is an integer.

Solution:

a. There is no least positive real number. For if x is any positive real number, then $x/2$ is a positive real number that is less than x.

Example 4 – *Solution*

cont'd

No violation of the well-ordering principle occurs because the well-ordering principle refers only to sets of integers, and this set is not a set of integers.

b. There is no *least* nonnegative integer n such that $n^2 < n$ because there is *no* nonnegative integer that satisfies this inequality.

The well-ordering principle is not violated because the well-ordering principle refers only to sets that contain at least one element.

Example 4 – *Solution*

cont'd

c. The following table shows values of $46 - 7k$ for various values of k.

k	0	1	2	3	4	5	6	7	...	−1	−2	−3	...
$46 - 7k$	46	39	32	25	18	11	4	−3	...	53	60	67	...

The table suggests, and you can easily confirm, that $46 - 7k < 0$ for $k \geq 7$ and that $46 - 7k \geq 46$ for $k \leq 0$.

Therefore, from the other values in the table it is clear that 4 is the least nonnegative integer of the form $46 - 7k$. This corresponds to $k = 6$.

The Well-Ordering Principle for the Integers

Another way to look at the analysis of Example 4(c) is to observe that subtracting six 7's from 46 leaves 4 left over and this is the least nonnegative integer obtained by repeated subtraction of 7's from 46.

In other words, 6 is the quotient and 4 is the remainder for the division of 46 by 7.

More generally, in the division of any integer n by any positive integer d, the remainder r is the least nonnegative integer of the form $n - dk$.

The Well-Ordering Principle for the Integers

This is the heart of the following proof of the existence part of the quotient-remainder theorem.

Quotient-Remainder Theorem (Existence Part)

Given any integer n and any positive integer d, there exist integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

Proof:

Let *S* be the set of all nonnegative integers of the form

$$n - dk,$$

where *k* is an integer.

The Well-Ordering Principle for the Integers

This set has at least one element. *[For if n is nonnegative, then*

$$n - 0 \cdot d = n \geq 0,$$

and so n – 0·d is in S. And if n is negative, then

$$n - nd = \underset{<0}{n}\underbrace{(1 - d)}_{\leq 0 \text{ since } d \text{ is a positive integer}} \geq 0,$$

and so n – nd is in S.] It follows by the well-ordering principle for the integers that *S* contains a least element *r*. Then, for some specific integer *k* = *q*,

$$n - dq = r$$

[because every integer in S can be written in this form].

The Well-Ordering Principle for the Integers

Adding dq to both sides gives

$$n = dq + r.$$

Furthermore, $r < d$. *[For suppose $r \geq d$.*

Then

$$n - d(q + 1) = n - dq - d = r - d \geq 0,$$

and so $n - d(q + 1)$ would be a nonnegative integer in S that would be smaller than r. But r is the smallest integer in S. This contradiction shows that the supposition $r \geq d$ must be false.]

The Well-Ordering Principle for the Integers

The preceding arguments prove that there exist integers *r* and *q* for which

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

[This is what was to be shown.]

Another consequence of the well-ordering principle is the fact that any strictly decreasing sequence of nonnegative integers is finite.

That is, if $r_1, r_2, r_3, \ldots$ is a sequence of nonnegative integers satisfying

$$r_i > r_{i+1}$$

for all $i \geq 1$, then $r_1, r_2, r_3, \ldots$ is a finite sequence.

The Well-Ordering Principle for the Integers

[For by the well-ordering principle such a sequence would have to have a least element r_k*. It follows that* r_k *must be the final term of the sequence because if there were a term* r_{k+1}*, then since the sequence is strictly decreasing,* $r_{k+1} < r_k$*, which would be a contradiction.]*

This fact is frequently used in computer science to prove that algorithms terminate after a finite number of steps.