CHAPTER 4: THE INTEGERS

Section 4.1: Mathematical Induction

The Principle of Mathematical Induction

Mathematical induction is a method for proving a statement of the form $(\forall n \geq n_0)\, P(n)$, where n_0 is a specific integer, n is an arbitrary integer with $n \geq n_0$, and $P(n)$ is an open statement that contains the variable n.

To illustrate, in Example 1 below we will prove, by induction on n, that 13 divides $18^n - 5^n$ for all integers $n \geq 1$. Thus, if we let $P(n)$ denote the statement "13 divides $18^n - 5^n$", then we will prove $(\forall n \geq 1)\, P(n)$.

Theorem 1: (The Principle of Mathematical Induction) Let S be a set of integers that satisfies the following two properties:

- $n_0 \in S$.
- For all $n \geq n_0$, if $n_0, \ldots, n \in S$ then $n + 1 \in S$.

Then $\{\, n \in \mathbf{Z} \,|\, n \geq n_0 \,\} \subseteq S$.

We will not prove Theorem 1, but the following discussion should provide some intuition.

- We are given that $n_0 \in S$.
- Since both statements, $n_0 \in S$ and $(n_0 \in S) \rightarrow (n_0 + 1 \in S)$ are true, it follows that $n_0 + 1 \in S$.
- We now have $n_0, n_0 + 1 \in S$ and we know that $(n_0, n_0 + 1 \in S) \rightarrow (n_0 + 2 \in S)$. It follows that $n_0 + 2 \in S$.
- We now have $n_0, n_0 + 1, n_0 + 2 \in S$ and we know that $(n_0, n_0 + 1, n_0 + 2 \in S) \rightarrow (n_0 + 3 \in S)$. It follows that $n_0 + 3 \in S$. And the process continues.

Indeed, the value of induction is that it permits a rigorous argument without having to say "and the process continues."

The Form of an Induction Proof (with commentary):

To Prove: $(\forall n \geq n_0)\, P(n)$.

Outline of Proof:

- State the proof is by induction on n.
- Prove that $P(n_0)$ is true. (*This is called the* **base case**.)

Comment: *In the next three steps below we are proving*

$$(**) \quad (\forall n \geq n_0)\,[\Big(\, P(n_0) \wedge \cdots \wedge P(n) \,\Big) \rightarrow P(n+1)].$$

Note that statement $(**)$ *has general form* $(\forall x \in U)\,\Big(P(x) \rightarrow Q(x)\Big)$. *We will follow the form for proving such a statement.*

- Let $n \in \mathbf{Z}$ with $n \geq n_0$. Assume that $P(k)$ is true for every integer k such that $n_0 \leq k \leq n$. (*In this step we state the* **Inductive Assumption**.)

If it's helpful (and it often is), expand on the inductive assumption.

Comment: *To prove an implication,* $(\forall x)(P(x) \rightarrow Q(x))$, *we begin with: "Let* $x \in U_x$ *and suppose that* $P(x)$ *is true." In the case of a proof by induction, this becomes: "Let* $n \geq n_0$ *and suppose that* $P(n_0) \wedge \cdots \wedge P(n)$ *is true." As noted above, we call this the* **inductive assumption**.

Note that we are not asserting that $P(n_0) \wedge \cdots \wedge P(n)$ *is indeed true. We just wish to show that whenever it is true, then* $P(n+1)$ *is also true.*

- Give a valid argument that leads from the assumption that $P(n_0) \wedge \cdots \wedge P(n)$ is true to the conclusion that $P(n+1)$ must ,then, also be true. (*That is,* **prove the "$n+1$" case**.)

- State that, by the Principle of Induction, $P(n)$ is true for all $n \geq n_0$.

Comment: *Let* S *denote the truth set of* $P(n)$. *In Step 2 of the outline above we prove that* $P(n_0)$ *is true; that is, we prove that* $n_0 \in S$.

In Steps 3 and 4 we prove $(**)$. *In doing so, we have proved that* $(\forall n \geq n_0)\,[(n_0, \ldots, n \in S) \rightarrow n+1 \in S]$.

By the Principle of Induction, $\{\, n \in \mathbf{Z} \,|\, n \geq n_0 \,\} \subseteq S$. *But* S *is the truth set for* $P(n)$, *so* $P(n)$ *is true for* $n \geq n_0$.

We now give a brief and stripped down outline for a proof by induction.

The Brief Form of an Induction Proof:

To Prove: $(\forall n \geq n_0)\,P(n)$.

Outline of Proof:

- State the proof is by induction on n.
- Prove the **base case**.
- State the **Inductive Assumption**.
- Prove the **"$n+1$" case**.
- State that, by the Principle of Induction, $P(n)$ is true for all $n \geq n_0$.

Example 1: Prove by induction on n that for every integer $n \geq 1$, 13 divides $18^n - 5^n$.

Outline of Proof:

- State the proof is by induction on n.
- **Prove the base case**. That is, prove that $P(1)$ is true.
- **State the inductive assumption**: Let $n \in \mathbf{Z}$ with $n \geq 1$. Assume that $P(k)$ is true for every integer k such that $1 \leq k \leq n$; that is, assume that 13 divides $18^k - 5^k$ for $1 \leq k \leq n$.

If it's helpful, expand on the inductive assumption.

- **Prove the** "$n + 1$" **case**. That is, give a valid argument that leads from the inductive assumption above to the conclusion that 13 divides $18^{n+1} - 5^{n+1}$.
- State that, by the Principle of Induction that 13 divides $18^n - 5^n$ for all $n \geq 1$.

Proof: The proof is by induction on n. For $n = 1$ we have $18^1 - 5^1 = 13$, so $18^1 - 5^1$ is clearly divisible by 13.

Now let n be an integer with $n \geq 1$. Assume that 13 divides $18^k - 5^k$ for all integers k, where $1 \leq k \leq n$. Thus for each k, $1 \leq k \leq n$, we are assuming that there is an integer m_k such that $18^k - 5^k = 13m_k$. Now $18^{n+1} - 5^{n+1} = 18^n 18 - 5^n 5$. If we add 0 to the last expression, it remains unchanged. But we add 0 in the form $-18^n 5 + 18^n 5$. (This "trick" is often referred to as "put and take.") Therefore, $18^{n+1} - 5^{n+1} = 18^n 18 - 18^n 5 + 18^n 5 - 5^n 5 = 18^n(18 - 5) + (18^n - 5^n)5 = 18^n 13 + 13m_n 5 = 13(18^n + m_n 5)$. This shows that 13 divides $18^{n+1} - 5^{n+1}$. By the Principle of Induction, 13 divides $18^n - 5^n$ for every integer $n \geq 1$.

An Intuitive View: Let $P(n)$ denote the statement that 13 divides $18^n - 5^n$. Then we have proved

- $P(1)$ is true, and
- $(\forall n \geq 1)\left[\Big(P(1) \wedge \cdots \wedge P(n)\Big) \rightarrow P(n+1)\right]$.

Therefore

- $P(1)$ and $P(1) \rightarrow P(2)$ are both true. It follows that $P(2)$ is true.
- $P(1) \wedge P(2)$ and $\Big(P(1) \wedge P(2)\Big) \rightarrow P(3)$ are both true. It follows that $P(3)$ is true.
- $P(1) \wedge P(2) \wedge P(3)$ and $\Big(P(1) \wedge P(2) \wedge P(3)\Big) \rightarrow P(4)$ are both true. It follows that $P(4)$ is true. And so forth.

Exercise 1: Prove by induction on n that for every integer $n \geq 1$, 5 divides $2^{2n-1} + 3^{2n-1}$.

In the next example, the base case is $n_0 = 2$.

Example 2: Prove that for every natural number $n \geq 2$, $n^3 + 1 > n^2 + n$.

Proof: The proof is by induction on n. For $n = 2$ we have $n^3 + 1 = 2^3 + 1 = 9$ and $n^2 + n = 2^2 + 2 = 6$. Clearly, $9 > 6$.

Now let n be an integer, $n \geq 2$, and assume that $k^3 + 1 > k^2 + k$ for every integer k such that $2 \leq k \leq n$. Then $(n+1)^3 + 1 = (n^3 + 3n^2 + 3n + 1) + 1 = (n^3 + 1) + 3n^2 + 3n + 1$. By assumption, $n^3 + 1 > n^2 + n$, so
$(n+1)^3 + 1 = (n^3 + 1) + 3n^2 + 3n + 1 > (n^2 + n) + 3n^2 + 3n + 1 = 4n^2 + 4n + 1 =$
$(n^2 + 2n + 1) + 2n + 3n^2 = (n+1)^2 + 2n + 3n^2 > (n+1)^2 + 2n > (n+1)^2 + (n+1)$.
This proves that $(n+1)^3 + 1 > (n+1)^2 + (n+1)$. By the Principle of Induction,
$n^3 + 1 \geq n^2 + n$ for every integer $n \geq 2$.

Exercise 2: Prove that $2^{n+1} < 3^n$ for every integer $n \geq 2$.

Recursively Defined Sequences

We say that a sequence, $\{ a_n \}_{n=1}^{\infty}$, is defined by a **recurrence relation** provided that from some n on, a_n is expressed as a function of the preceding terms in the sequence. The first few terms are explicitly defined via the **initial conditions** of the recurrence relation. For example:

The sequence $\{ f_n \}_{n=1}^{\infty}$ of **Fibonacci numbers** is defined by

- (*The initial conditions*) $f_1 = f_2 = 1$, and
- (*The recurrence relation*) $f_n = f_{n-1} + f_{n-2}$ for $n \geq 3$.

Thus, from f_3 on, each Fibonacci number is the sum of the two preceding Fibonacci numbers.

The first few Fibonacci numbers are:
$f_1 = 1$, $f_2 = 1$, $f_3 = 2$, $f_4 = 3$, $f_5 = 5$, $f_6 = 8$, $f_7 = 13$, $f_8 = 21$, and $f_9 = 34$.

Exercise 3: Let $\{ f_n \}_{n=1}^{\infty}$ be the sequence of Fibonacci numbers. Prove that for every integer $n \geq 2$, $f_1 + \cdots + f_{n-1} = f_{n+1} - 1$.

Example 3: Define a sequence $\{ a_n \}_{n=1}^{\infty}$ as follows:

- Let $a_1 = a_2 = a_3 = 1$.
- For $n \geq 4$, set $a_n = a_{n-1} + a_{n-2} + a_{n-3}$.

Prove that $a_n \leq 2^{n-2}$ for every integer $n \geq 2$.

COMMENTS: Note that the formula to be proved, $a_n \leq 2^{n-2}$, is false for $n = 1$. Thus, for our base case, n_0, it is necessary that $n_0 \geq 2$. This will actually be our first example in which we will need to prove more that one step in the base case. The sort of reasoning below illustrates the type of analysis that leads us to a base case with more than a single step.

First, after we have stated the inductive hypothesis and are ready to prove the "$n+1$" case, it will be convenient to to define a_{n+1} via the given recurrence relation. That is, we will wish to write $a_{n+1} = a_n + a_{n-1} + a_{n-2}$. Since the recurrence relation applies only to the 4th and later terms, this requires $n+1 \geq 4$, or $n \geq 3$. But to suppose that $n \geq 3$ in the inductive assumption requires that we have proved the cases $n = 2$ and $n = 3$ in the base case.

Further, to use the recurrence formula $a_{n+1} = a_n + a_{n-1} + a_{n-2}$ to prove the "$n+1$" case (that is, to prove that $a_{n+1} \leq 2^{n-1}$), we will wish to apply the inductive assumption to each of the three preceding terms that define a_{n+1}. That is, we want to assume that we already know that $a_n \leq 2^{n-2}$, $a_{n-1} \leq 2^{n-3}$, and $a_{n-2} \leq 2^{n-4}$. This means that we need $n-2 \geq 2$ or $n \geq 4$. But to suppose that $n \geq 4$ in the inductive assumption requires that we have proved the cases $n = 2$ and $n = 3$, and $n = 4$ in the base case.

The second analysis above trumps the first, so in our base case we will need to prove the first three cases, $n = 2, 3, 4$.

Proof: The proof is by induction on n.

The base cases: If $n = 2$ then $a_n = a_2 = 1$ and $2^{n-2} = 2^0 = 1$. since $1 \leq 1$ we have $a_n \leq 2^{n-2}$.
If $n = 3$ then $a_n = a_3 = 1$ and $2^{n-2} = 2^1 = 2$. since $1 \leq 2$ we again have $a_n \leq 2^{n-2}$.
If $n = 4$ then $a_n = a_4 = a_3 + a_2 + a_1 = 1 + 1 + 1 = 3$ and $2^{n-2} = 2^2 = 4$. since $3 \leq 4$ we have $a_n \leq 2^{n-2}$.

The Inductive Assumption: Let n be an arbitrary integer such that $n \geq 4$. Assume that $a_k \leq 2^{k-2}$ for every integer k such that $2 \leq k \leq n$.

Proof of the "$n+1$" case: Since we are assuming that $n \geq 4$, we have $n+1 \geq 5$ so a_{n+1} is defined by the recurrence relation, that is, $a_{n+1} = a_n + a_{n-1} + a_{n-2}$. Also, $n \geq 4$ means that $n-2 \geq 2$, so the inductive assumption applies to each of the terms a_n, a_{n-1}, and a_{n-2}. Thus, by assumption, $a_n \leq 2^{n-2}$, $a_{n-1} \leq 2^{n-3}$, and $a_{n-2} \leq 2^{n-4}$. Therefore, $a_{n+1} = a_n + a_{n-1} + a_{n-2} \leq 2^{n-2} + 2^{n-3} + 2^{n-4} \leq 2^{n-2} + 2^{n-3} + 2^{n-3} = 2^{n-2} + 2^{n-3}2 = 2^{n-2} + 2^{n-2} = 2^{n-2}2 = 2^{n-1}$. This proves that $a_{n+1} \leq 2^{n-1} = 2^{(n+1)-2}$.

By the Principle of Induction, $a_n \leq 2^{n-2}$ for every integer $n \geq 2$.

More on The Inductive Hypothesis

In a genuine proof by induction, the proof of the "$n+1$" case always requires that the inductive assumption be applied to an earlier case or cases. Given this pivotal role, it is essential that the inductive assumption be stated accurately and completely.
Suppose we wish to prove $(\forall n \geq n_0)P(n)$ by induction on n. As we have seen in the example above, the base case may involve proving $P(n_0), \ldots, P(m)$, for some $m \geq n_0$. The inductive assumption then has the form:

Form of the Inductive Assumption: Let $n \geq m$ and assume that $P(k)$ is true for every integer k, where $n_0 \leq k \leq n$.

(**NOTE**: In your written proof, never use the symbolic representation, $P(n)$, for a statement. Always give the statement in complete written form.)

To illustrate, let's revisit Example 3 above. We were to prove: For all $n \geq 2$, $a_n \leq 2^{n-2}$. The base cases were $n = 2$, $n = 3$, and $n = 4$. Thus, following the form above, the inductive assumption is:

Let $n \geq 4$ and assume that $a_k \leq 2^{k-2}$ for every integer k, where $2 \leq k \leq n$.

Exercise 4: Let $\{ a_n \}_{n=1}^{\infty}$ be the sequence defined in Example 3. The object of this exercise is to prove that $a_n < 2a_{n-1}$ for every integer $n \geq 5$.

(a) Determine the number of steps that need to be proved as base cases and prove them.

HINTS: In proving the "$n + 1$" case, we will want a_{n+1} to be defined by the recurrence relation; that is, we need $n + 1 \geq 4$. But since the problem stipulates that $n \geq 5$, we actually have $n + 1 \geq 6$.

When we use the recurrence relation to write $a_{n+1} = a_n + a_{n-1} + a_{n-2}$, we will wish to apply the inductive assumption to each of the terms a_n, a_{n-1}, and a_{n-2}. Thus, what is the minimum value for $n - 2$? for n?

(b) State the inductive assumption.

(c) Prove the "$n + 1$" case.

An Important Theorem

Theorem: For every integer $n \geq 2$ either n is a prime or n can be expressed as a product of two or more primes.

Proof: The proof is by induction on n.

The Base Case

If $n = 2$, then n is a prime so we are done.

The Inductive Assumption

Let n be an arbitrary integer with $n \geq 2$. For every integer k such that $2 \leq k \leq n$, suppose that either k is prime or k can be expressed as a product of two or more primes.

Proof of the "$n + 1$" Case

Consider the integer $n + 1$. If $n + 1$ is prime then we are done, so assume that $n + 1$ is not prime. Then there exist integers a and b such that $2 \leq a \leq n$, $2 \leq b \leq n$ and $n + 1 = ab$. By our inductive assumption, each of a and b is either a prime or can be expressed as a product of two or more primes. It follows that $n + 1$ can be expressed as a product of two or more primes.

By the Principle of Induction, for every integer $n \geq 2$ either n is a prime or n can be expressed as a product of two or more primes.

Exercise 5:

Background: For an integer $n \geq 2$ define $f(n)$ to be the number of (not necessarily distinct) prime factors of n. For example, $f(5) = 1$, $f(6) = 2$, $f(8) = 3$, and $f(9) = 2$. You are given that $f(ab) = f(a) + f(b)$ for all positive integers a and b, where $a \geq 2$ and $b \geq 2$.

Exercise: Prove by induction on n that for every integer $n \geq 2$, $f(n) < 2 \ln n$.

HINT: After you have stated the inductive assumption, consider two cases:

Case 1: $n + 1$ is prime.

Case 2: $n + 1$ is not prime. Then $n + 1$ is a composite. What does that mean? Apply the inductive assumption to the factors.

Section 4.1. EXERCISES

4.1.1. Prove by induction on n that 6 divides $n(n+1)(n+2)$ for every integer $n \geq 1$.

4.1.2. Prove by induction on n that for every integer $n \geq 6$ there exists integers r and s such that $r \geq 0$, $s \geq 0$ and $n = 2r + 5s$. (Thus, if $n \geq 6$, n can be expressed as a sum of 2's and 5's.)

HINT: Based on the induction hypothesis you can argue that there are integers r and s such that $r \geq 0$, $s \geq 0$ and $n = 2r + 5s$. Consequently, $n + 1 = 2r + 5s + 1$. Consider the following two cases:

Case 1: $s \geq 1$. Now get $n + 1 = 2r + 5(s - 1) + 6$.

Case 2: $s = 0$. Then $n + 1 = 2r + 1$. Argue that $r \geq 3$, so $n + 1 = 2(r - 2) + 5$.

4.1.3. Prove by induction on n that $(1 + \frac{1}{n})^n < n$ for every integer $n \geq 3$.

4.1.4. Suppose that you are presented with a sequence of closed doors numbered 1 to m and behind these doors are the unknown real numbers x_1, x_2, ..., x_{m-1}, x_m, respectively. You are given that $x_1 < x_2 < \cdots < x_{m-1} < x_m$. Further, you are given a number y such that $y = x_i$ for some i. The object is to find where y is located by opening as few doors as possible. The actual number of doors that need to be opened will vary depending on the location of y and the strategy employed. In this problem we will determine a value, $N(m)$, such that y can be located by opening at most $N(m)$ doors.

(a) (An Example – Not to turn in.) Conjecture a value for $N(15)$. (One strategy is given below, but find your own before looking.)

A Strategy: First open door 8. If $y = x_8$ we are done. Otherwise, either $y < x_8$ and is behind one of the first 7 doors, or $y > x_8$ so is located behind one of the doors $9 - 15$. The cases are similar, so we consider the case where $y < x_8$.

Now open door 4. As above, if $y = x_4$ we are done in two steps. Otherwise, either $y < x_4$ so is behind one of the first 3 doors, or $y > x_4$ so is located behind one of the doors $5 - 7$. Again the cases are similar, so assume $y < x_4$.

Finally, open door 2. If $y = x_2$ we are done. If $y < x_2$, then y is behind door 1. If $y > x_2$, then y is behind door 3.

This shows that if y is hidden behind one of 15 doors, we need to open at most 3 doors to locate y. Thus, we can take $N(15) = 3$.

(b) (Not to turn in): Conjecture a value (based on some strategy similar to that above) for $N(2)$ and $N(3)$.

Repeat for $N(4)$, $N(5)$, $N(6)$, and $N(7)$.

(c) Prove by induction on n that if $n \geq 0$ and $m < 2^{n+1}$ then $N(m) \leq n$; that is, we can locate a value y, hidden behind one of m, doors by opening no more that n doors.

(**NOTES**: When proving the "$n+1$" case you will assume that $m < 2^{n+2}$. Consider two cases. If, actually, $m < 2^{n+1}$ your inductive assumption already applies. If $m \geq 2^{n+1}$ use one move to open the door numbered 2^{n+1}. If y is not behind that door, what is the maximum number of doors to either side. Apply the inductive assumption to those sets of doors.)

4.1.5. Let $\{ f_n \}_{n=1}^{\infty}$ be the sequence of Fibonacci numbers. Prove that for every integer $n \geq 1$, $f_1^2 + \cdots + f_n^2 = f_n f_{n+1}$.

4.1.6. Let Let m be a given positive integer with $m \geq 2$. (So m remains constant throughout the problem.) Let $\{ f_n \}_{n=1}^{\infty}$ be the sequence of Fibonacci numbers. Prove that for every integer $n \geq 1$, $f_{m+n} = f_m f_{n+1} + f_{m-1} f_n$.

[**Caution**: I want you to include exactly the correct number of steps in your base case. You may need to work through your argument first to see how many steps are needed. See, as an illustration, the comments following Example 3.]

4.1.7. Prove by induction on n that for every integer $n \geq 1$, there exists integers t_1, t_2, ..., t_m such that

$$t_1 > t_2 > \cdots > t_m \geq 0 \text{ and } n = 2^{t_1} + 2^{t_2} + \cdots + 2^{t_m}.$$

Some Examples: $1 = 2^0$, $4 = 2^2$, $13 = 2^3 + 2^2 + 2^0$, $35 = 2^5 + 2^1 + 2^0$.

HINT: When proving the "$n+1$" case, note that $n+1$ is either even or odd. Thus, there is an integer l such that either $n+1 = 2l$ or $n+1 = 2l+1$. In either case, note that $1 \leq l \leq n$ and apply the inductive assumption to k.

4.1.8. First, a description of the game:

You are given a row of boxes, each containing a 0 or a 1.

A permissible move consists of removing a 0 from one and only one box then changing the values in the neighboring boxes; that is, a neighboring 0 becomes 1 and a neighboring 1 becomes 0. (Thus, if no zero's are present, the game is over.)

The object of the game is to empty all the boxes, if possible.

An Example:

The given boxes:

1	0	1	0	0

Remove the leftmost 0 to obtain:

0		0	0	0

Remove the leftmost 0 to obtain:

		0	0	0

Remove the leftmost 0 to obtain:

			1	0

Remove the leftmost 0 to obtain:

			0	

Remove the remaining 0 to obtain:

Thus, in this example, the boxes were successfully emptied.

Exercise: Let S denote a given string of n boxes containing zero's and one's. We will call n the **length** of S and write $L(S) = n$. Let $z(S)$ denote the number of zero's present in the string S. (So if $L(S) = n$, $z(S)$ could have any integer value from 0 to n.)

Prove, by induction on n, that for every integer $n \geq 1$, a given string S, with $L(S) = n$, can be emptied if $z(S)$ is odd but cannot be emptied if $z(S)$ is even.

Comments: Include both the even and odd cases at each step of the proof. For instance, if $L(S) = 1$ then either $z(S) = 0$, which is even, or $z(S) = 1$.

For the "$n + 1$" case, assume that S is a string of zero's and one's with $L(S) = n + 1$. First suppose that $z(S)$ is odd. (So at least one zero is present.) Remove the leftmost zero and don't forget to change the entries in the neighboring boxes.

If the leftmost zero is at either end of S, after removing it we have created a string, S' such that $L(S') = n$. Argue that $z(S')$ is still odd and apply the inductive assumption.

If the leftmost zero is not at either end, we have separated our given string S into two strings, S_1 and S_2, of zero's and one's. If $L(S_1) = q$ and $L(S_2) = r$, argue that $q \leq n$, $r \leq n$. Also argure that both $z(S_1)$ and $z(S_2)$ are odd. Apply the inductive hypothesis to each of the strings S_1 and S_2.

Next, assume that $z(S)$ is even. What if $z(S) = 0$? If $z(S) > 0$, remove any zero from S and change the neighboring entries. Proceed with a strategy similar to the odd case.

4.1.9. This game requires two players. You are given an $n \times n$ square partitioned into n^2 subquares that are each 1×1. (Like an $n \times n$ checkerboard without colors.) On the first move, player 1 may claim (mark with a X) any square in the right most column. (Player two can claim squares with O's.) After the first move, players take turns according to the following rule:

Rule: After an opposing player has claimed a square, you may then claim a square either in the same column but anywhere below the opponent's last square, or in the same row but anywhere to the left of the opponent's last square. (So play must move down or left.)

The winner is the player who claims the square in the lower left corner.

Examples: Following are two examples in a 6×6 grid. In both examples, player 2 won.

					X
	O		X		O
O	X				

				O	X
X	O			X	
O					

Exercise: Prove, by induction on n, that for every integer $n \geq 1$, player 1 can always win the above game played on an $n \times n$ grid.

Some Notation: Count the rows of the grid from the bottom and count the columns from the left. Now let S_{ij} denote the square in the ith row and jth column. For example, S_{11} is the square in the lower left corner, S_{nn} is the square in upper right corner and S_{23} is the square on the 2nd row from the bottom and the third column from the left.

Comments: In the base case, $n = 1$, player 1 wins on the first move – player 2 never gets a move. Thus, the base case is not helpful.

Your proof of the "$n + 1$" case will necessarily include the winning strategy for player 1, so first play the game enough to find and understand such a strategy.

In proving the "$n + 1$" case, describe play through the second move for player 1. At that point you should be able to apply your inductive assumption to a smaller grid.

Section 4.2: The Division Algorithm and Greatest Common Divisors

The Division Algorithm

The Division Algorithm is merely long division restated as an equation. For example, the division

$$\begin{array}{r} 29 \quad r.\,20 \\ 32\overline{)\,948} \end{array}$$

can be rewritten in equation form as $948 = 32(29) + 20$.

More generally, if m (the dividend) and d (the divisor) are positive integers then division of m by d yields quotient q and remainder r as follows:

$$(**) \qquad \begin{array}{r} q \quad rem\ r \\ d\overline{)\,m} \end{array}$$

Furthermore, we know that $0 \leq r < d$.

We can express $(**)$ in equation form as:

$$m = dq + r \text{ where } \ 0 \leq r < d.$$

Theorem 1 (The Division Algorithm for Integers): Let m be any integer and let d be a positive integer. Then there exist unique integers q and r such that $0 \leq r < d$ and $m = dq + r$.

Comment: Note that in the Division Algorithm, m, the dividend, is an arbitrary integer. From long division, we are familiar only with the case where $m \geq d$. The other cases are easily handled as follows.

Case 1: Assume $0 \leq m < d$. Then set $q = 0$ and $r = m$; that is, $m = d(0) + m$.

Case 2: Assume the dividend is $-m$, where m is positive. Since m is positive, we can use long division to find integers q and r such that $m = dq + r$. Then
$-m = d(-q) - r = d(-q - 1) + (d - r)$. Since $0 \leq r < d$, it follows that $0 \leq d - r < d$.

Exercise 1: In each of (a) – (d) you are given values for m and d. In each case find (using the notation of the Division Algorithm) the quotient q and the remainder r.

(a) $m = 6$, $d = 10$ (b) $m = -6$, $d = 10$

(c) $m = 15153$, $d = 83$ (d) $m = -15153$, $d = 83$

Greatest Common Divisors

Definition 1: Let a and b be integers. A positive integer d is called the **greatest common divisor of a and b**, written $d = \gcd(a, b)$, provided:

(a) d divides a and d divides b; and

(b) if c is an integer such that c divides a and c divides b, then c divides d.

Comment: In words, the definition states that $d = \gcd(a, b)$ provided d is a **common divisor** of a and b and d is divisible by all other common divisors of a and b.

Example 1: The common divisors of 18 and 30 are ± 1, ± 2, ± 3, and ± 6. Clearly, $6 = \gcd(18, 30)$ and note that all other common divisors of 18 and 30 divide 6.

Uniqueness of the GCD

Lemma 1: Let d_1 and d_2 be positive integers such that d_1 divides d_2 and d_2 divides d_1. Then $d_1 = d_2$.

Proof: Let d_1 and d_2 be positive integers such that d_1 divides d_2 and d_2 divides d_1. Then there exist positive integers q_1 and q_2 such that $d_1 = q_1 d_2$ and $d_2 = q_2 d_1$. Thus,

$$d_1 = q_1 d_2 = q_1(q_2 d_1) = (q_1 q_2) d_1.$$

Since $d_1 = (q_1 q_2) d_1$, it follows that $1 = q_1 q_2$. Recall that q_1 and q_2 are both positive, so it follows that $q_1 = q_2 = 1$. (The only other possibility, $q_1 = q_2 = -1$, is eliminated.) Thus, $d_1 = q_1 d_2 = d_2$.

Theorem 2: Let a and b be integers. If $\gcd(a, b)$ exists, it is unique.

Proof: Let a and b be integers and assume that $\gcd(a, b)$ exists. Suppose that $d_1 = \gcd(a, b)$ and suppose also that $d_2 = \gcd(a, b)$. Let's first view d_1 as $\gcd(a, b)$. Since d_2 is, by (a) of Definition 1, a common divisor of a and b, it follows from (b) of Definition 1 that d_2 divides d_1. Similarly, viewing d_2 as $\gcd(a, b)$, we see that d_1 divides d_2. It now follows from Lemma 1 that $d_1 = d_2$, so $\gcd(a, b)$ is unique when it exists.

Existence of the GCD

Special Cases: Let a and b be integers.

- $\gcd(0,0)$ does not exist.
- If $a \neq 0$ then $\gcd(a,0) = |a|$.
- If a divides b then $\gcd(a,b) = |a|$.
- If $a \neq 0$ and $b \neq 0$ then $\gcd(a,b) = \gcd(|a|,|b|)$.

Thus, in the algorithm given as the proof of Theorem 3 below, we may always assume that a and b are positive integers.

The next Lemma gives an essential "reduction step" for calculating $\gcd(a,b)$.

Lemma 2: Let a, b, q, and r be integers such that $a = qb + r$. (cf. The Division Algorithm) Then $\gcd(a,b) = \gcd(b,r)$.

Proof: The proof of Lemma 2 is Exercise 4.2.3.

Theorem 3: If a and b are integers, not both zero, then $\gcd(a,b)$ exists.

Proof: The special cases were considered above. We give here an algorithm for finding $\gcd(a,b)$ when $a \geq b > 0$.

Apply the Division Algorithm, with b as the divisor, to obtain

$$a = q_1 b + r_1 \text{ where } 0 \leq r_1 < b.$$

If $r_1 \neq 0$, apply the Division Algorithm to b and r_1, with r_1 as the divisor, to obtain

$$b = q_2 r_1 + r_2 \text{ where } 0 \leq r_2 < r_1.$$

If $r_2 \neq 0$, apply the Division Algorithm to r_1 and r_2, with r_2 as the divisor, to obtain

$$r_1 = q_3 r_2 + r_3 \text{ where } 0 \leq r_2 < r_1.$$

Since the remainders r_1, r_2, r_3, etc. form a sequence of positive integers with $r_1 > r_2 > r_3 \cdots \geq 0$. It follows that there is an integer k such that $r_k \neq 0$ but $r_{k+1} = 0$.

Following is the algorithm for calculating $\gcd(a,b)$:

Algorithm 1: Finding the GCD:

$$a = q_1 b + r_1 \text{ where } 0 \leq r_1 < b$$
$$b = q_2 r_1 + r_2 \text{ where } 0 \leq r_2 < r_1$$
$$r_1 = q_3 r_2 + r_3 \text{ where } 0 \leq r_2 < r_1$$
$$\vdots$$
$$r_{k-3} = q_{k-1} r_{k-2} + r_{k-1} \text{ where } 0 \leq r_{k-1} < r_{k-2}$$
$$r_{k-2} = q_k r_{k-1} + r_k \text{ where } 0 \leq r_k < r_{k-1}$$
$$r_{k-1} = q_{k+1} r_k$$

Then $r_k = \gcd(a, b)$.

To see that $r_k = \gcd(a, b)$, repeatedly apply Lemma 2 to get
$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{k-1}, r_k)$. But, by the last equation in Algorithm 1, r_k divides r_{k-1}. Thus, $r_k = \gcd(r_{k-1}, r_k) = \gcd(a, b)$.

Example 2: Find $\gcd(216, 80)$.

Solution: Repeated use of long division gives:

$$\begin{array}{r} 2 \\ 80\overline{)216} \end{array} \quad r.\,56 \qquad \begin{array}{r} 1 \\ 56\overline{)80} \end{array} \quad r.\,24 \qquad \begin{array}{r} 2 \\ 24\overline{)56} \end{array} \quad r.\,8 \qquad \begin{array}{r} 3 \\ 8\overline{)24} \end{array} \quad r.\,0$$

or, in equation form:

$$216 = (2)80 + 56 \qquad 80 = (1)56 + 24 \qquad 56 = (2)24 + 8 \qquad 24 = (3)8.$$

Therefore, $8 = \gcd(216, 80)$.

Exercise 2: In each of (a) – (d), find $\gcd(a, b)$.

(a) $a = -44$, $b = 0$ (b) $a = -22$, $b = 660$

(c) $a = 715$, $b = 208$ (d) $a = 715$, $b = -208$

Further Theorems

Theorem 4: Let a and b be integers and suppose $d = \gcd(a, b)$. Then there exist integers m and n such that $d = ma + nb$.

Comment: Note that $6 = \gcd(18, 30)$ and we may write
$6 = (2)18 + (-1)30 = (-3)18 + (2)30 = (7)18 + (-4)30$, so, in the notation of Theorem 4, m and n are not unique.

The following algorithm for finding one choice for m and n is a continuation of Algorithm 1 for find $\gcd(a, b)$.

Algorithm 2: Writing gcd$(a, b) = ma + nb$

Beginning with the second to last equation of Algorithm 1 and working up, we solve each equation for the remainder. This gives:

$$r_k = r_{k-2} - q_k r_{k-1}$$
$$r_{k-1} = r_{k-3} - q_{k-1} r_{k-2}$$
$$\vdots$$
$$r_3 = r_1 - q_3 r_2$$
$$r_2 = b - q_2 r_1$$
$$r_1 = a - q_1 b$$

Recall that $r_k = \gcd(a, b)$.

In the equation for r_k, substitute for r_{k-1}, using the second equation. This gives

$$r_k = r_{k-2} - q_k r_{k-1} = r_{k-2} - q_k(r_{k-3} - q_{k-1} r_{k-2}) = (1 + q_{k-1}) r_{k-2} + (-q_k) r_{k-3}.$$

In the resulting equation, we next substitute for r_{k-2} and simplify. Then substitute for r_{k-3} and simplify. Continuing, we eventually substitute for r_1 and simplify. This will yield $r_k = ma + nb$.

Example 3: We have seen in Example 2 that $8 = \gcd(216, 80)$. Find integers m and n such that $8 = 216m + 80n$.

Solution: In the solution to Example 3 we obtained several equations representing the repeated applications of the Division Algorithm. In reverse order, we solve each those equations for the remainder. This gives:

$$8 = 56 - (2)24 \qquad 24 = 80 - (1)56 \qquad 56 = 216 - (2)80.$$

Now in $8 = \underline{56} - (2)\underline{24}$ substitute $\underline{24} = \underline{80} - (1)\underline{56}$ to obtain

$$8 = \underline{56} - 2\Big(\underline{80} - (1)\underline{56}\Big) = (-2)\underline{80} + (3)\underline{56}.$$

Next, substitute $\underline{56} = \underline{216} - (2)\underline{80}$ to obtain:

$$8 = (-2)\underline{80} + (3)\underline{56} = (-2)\underline{80} + 3\Big(\underline{216} - (2)\underline{80}\Big) = (3)\underline{216} - (8)\underline{80}.$$

Thus, $8 = (3)\underline{216} - (8)\underline{80}$.

Exercise 3: Find $d = gcd(4977, 405)$ and find integers m and n such that $d = 4977m + 405n$.

Theorem 5: Let a, and b be integers, where a and b are not both zero. Then $\gcd(a, b)$ exists so let $d = \gcd(a, b)$. For an integer c there exist integers m and n such that $c = ma + nb$ if and only if c is a multiple of d.

Proof: Note that this is an equivalence, so two proofs are required.

First, let c be an integer and assume that there exist integers m and n such that $c = ma + nb$. Let $d = \gcd(a, b)$. Then d divides both a and b, so there exist integers a_1 and b_1 such that $a = a_1 d$ and $b = b_1 d$. Thus, $c = ma + nb = ma_1 d + nb_1 d = (ma_1 + nb_1)d$. Consequently, $c = qd$, where $q = ma_1 + nb_1$, and so d divides c.

In the opposite direction, set $d = \gcd(a, b)$, let c be an integer, and assume that d divides c. Then there exists an integer k such that $c = kd$. By Theorem 4, there exist integers m_1 and n_1 such that $d = m_1 a + n_1 b$. Therefore, $c = kd = k(m_1 a + n_1 b) = km_1 a + kn_1 b$. Thus, $c = ma + nb$, where $m = km_1$ and $n = kn_1$.

Exercise 4: Suppose $11 = ma + nb$, where a, b, m, and n are integers. List all possible choices for $d = gcd(a, b)$.

Section 4.2. EXERCISES

4.2.1. In each of (a) – (e) you are given integers m and n, where n is positive. In each case, find integers q and r such that $m = qn + r$ and $0 \leq r < n$.

(a) $m = 2$, $n = 5$ (b) $m = -2$, $n = 5$ (c) $m = 30$, $n = 6$
(d) $m = 4129$, $n = 232$ (e) $m = -4129$, $n = 232$.

4.2.2. In each of (a) – (c) below you are given integers a and b. In each case use the Division Algorithm to find $\gcd(a, b)$ and to find integers m and n such that $\gcd(a, b) = ma + nb$

(a) $a = 899$, $b = 29$ (b) $a = 224$, $b = 98$ (c) $a = 963$, $b = 177$

4.2.3. Let a, b, q, and r be integers such that $a = bq + r$. Prove that $\gcd(a, b) = \gcd(b, r)$.

HINT: Let $d_1 = \gcd(a, b)$ and let $d_2 = \gcd(b, r)$. Use part (b) of the definition of greatest common divisor to argue that d_1 divides d_2 and d_2 divides d_1.

4.2.4. Let a, b, c, and d be integers such that a divides bc and $d = \gcd(a, b)$. Prove that a divides cd.

HINT: Apply Theorem 4 and multiply the resulting equation by c.

4.2.5. Let a and b be integers and let $d = \gcd(a, b)$. If k is a positive integer, prove that $kd = \gcd(ka, kb)$.

HINT: Set $d_1 = \gcd(ka, kb)$. Argue that kd is a common divisor of ka and kb, so kd divides d_1. Next, apply Theorem 5 to argue that d_1 divides kd.

Section 4.3: Relatively Prime Integers

Let a and b be integers, not both zero (so $\gcd(a, b)$ exists). Let $d = \gcd(a, b)$ and let

$$S = \{\, c \in \mathbf{Z} \,|\, \text{there exist integers } m \text{ and } n \text{ such that } c = ma + nb \,\}.$$

We have seen, in Theorem 5 of Section 4.2, that $c \in S$ if and only if d divides c; that is, S consists of all integer multiples of d. Thus, an alternate description of S is

$$S = \{\, md \,|\, m \in \mathbf{Z} \,\}.$$

The following theorem is an immediate consequence of this observation.

Theorem 1: Let a and b be integers, not both zero. Let $d = \gcd(a, b)$ and let

$$S = \{\, c \in \mathbf{Z} \,|\, \text{there exist integers } m \text{ and } n \text{ such that } c = ma + nb \,\}.$$

Then d is the smallest positive integer in S.

Example 1: Let a and b be integers, not both zero. Suppose there exist integers m and n such that $15 = ma + nb$. What are the possibilities for $\gcd(a, b)$.

Solution: If $d = \gcd(a, b)$ then, by Theorem 5 of Section 4.2, d is a positive divisor of 15. Thus, the choices for d are 1, 3, 5, and 15.

Exercise 1: Let a and b be integers, not both zero. Suppose $\gcd(a, b) < 10$ and there exist integers m and n such that $17 = ma + nb$. What are the possibilities for $\gcd(a, b)$.

Definition 1: Let a and b be integers, not both zero. Then a and b are **relatively prime** provided $1 = \gcd(a, b)$.

Example 2: The integers 15 and 22 are relatively prime and $1 = (-2)22 + (3)15$.

Theorem 2: Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers m and n such that $1 = ma + nb$.

Proof: Note that Theorem 2 is an equivalence, so two proofs are required.

First, let a and b be integers, not both zero, and suppose a and b are relatively prime. Then $1 = \gcd(a, b)$ so, by Theorem 4 of Section 4.2, there exist integers m and n such that $1 = ma + nb$.

In the other direction, let a and b be integers, not both zero, and suppose there exist integers m and n such that $1 = ma + nb$. If
$S = \{ c \in \mathbf{Z} \,|\, \text{there exist integers } m \text{ and } n \text{ such that } c = ma + nb \}$ then we are assuming that $1 \in S$. Let $d = \gcd(a, b)$. By Theorem 1, d is the smallest positive integer in S. Clearly 1 is the smallest positive integer there is. Since $1 \in S$ and d is the smallest positive integer in S, it follows that $d = 1$.

Exercise 2: Determine whether the following statement is true or false:

For all integers a, b, and c, if a divides bc then either a divides b or a divides c.

Theorem 3: For all integers a, b, and c, if a divides bc and $\gcd(a, b) = 1$, then a divides c.

Proof: Let a, b, and c be integers. Suppose that a divides bc and $\gcd(a, b) = 1$. Since a divides bc, there exists an integer k such that $bc = ak$. Since $\gcd(a, b) = 1$, by Theorem 2 (or by Theorem 4 of Section 4.2), there exist integers m and n such that $1 = ma + nb$. Multiplying by c gives $c = mac + nbc$. This gives

$$c = mac + nbc = mac + nak = (mc + nk)a; \text{ that is, } c = qa \text{ where } q = mc + nk.$$

This proves that a divides c.

Example 3: Let k be an integer such that 12 divides $35k$. Since 12 and 35 are relatively prime, it follows from Theorem 3 that 12 divides k.

Exercise 3: Let a be an integer and let p be a prime integer. List all possibilites for $\gcd(a, p)$.

Theorem 4: Let a be an integer and let p be a prime integer. Then either p divides a and $p = \gcd(a, p)$ or a and p are relatively prime.

Proof: Let a be an integer and let p be a prime integer. Set $d = \gcd(a, p)$. Then d is a positive integer divisor of p so either $d = p$ or $d = 1$. If $d = p$ then it follows that p divides a (since d divides a). If $d = 1$ then a and p are relatively prime.

Exercise 4: Let n be a positive integer such that 7 divides $3n$ and $25 \leq 3n \leq 60$. Determine the value of $3n$.

Theorem 5: Let a and b be integers. If p is a prime integer such that p divides ab, then either p divides a or p divides b.

Proof: We will prove the equivalent formulation:

If p is a prime integer such that p divides ab and p does not divide a, then p divides b.

Thus, assume that p divides ab and p does not divide a. By Theorem 4, a and p are relatively prime. By Theorem 3, p divides b.

Exercise 5: Let p and q be distinct prime integers such that $15p = 35q$. Find values for p and q and prove that those are the only values possible.

Section 4.3. EXERCISES

4.3.1. Let a and b be integers, not both 0, and let d be a positive integer that divides both a and b. Then there exists integers a_1 and b_1 such that $a = a_1 d$ and $b = b_1 d$.

Prove that $d = \gcd(a, b)$ if and only if $1 = \gcd(a_1, b_1)$.

NOTE: This is an equivalence, so requires two proofs.

HINT: In one direction, Exercise 4.2.5 should be quite helpful.

4.3.2. Let a, b, and n be integers such that $1 = \gcd(a, n)$ and $1 = \gcd(b, n)$. Prove that $1 = \gcd(ab, n)$.

HINT: Theorem 2 of Section 4.3 should prove quite useful.

4.3.3. Let p be a prime integer. Prove by induction that for every integer $n \geq 2$, if a_1, a_2, $\ldots$, a_n are integers such that p divides the product $a_1 a_2 \cdots a_n$ then there exists an integer i such that $1 \leq i \leq n$ and p divides a_i.

HINT: For the base case cf. Theorem 5 of Section 4.3.
After you have stated the induction hypothesis, suppose p divides $a_1 a_2 \cdots a_n a_{n+1}$ and set $b = a_1 a_2 \cdots a_n$. Then p divides $b a_{n+1}$.