Module 1. Integers, Induction, and Recurrences

This module will look at

- The integers and the natural numbers.
- Division and divisors, greatest common divisors
- Methods of reasoning including proof by contradiction and proof by induction.
- The solution to certain recursively defined sequences

Since discrete math deals with discrete entities, we can count them and so the counting numbers play an important role.

Reading: Gossett Ch 3.1, 3.2, 3.3, 3.4 (optional), 3.6.

Integers and Natural Numbers

Recall:

- The integers $\mathbb{Z} = \{0, 1, -1, 2, -2, ...\}$
- and the natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$

These are important sets. We will study them for their own sake and use them as a source of examples of general proof techniques that apply throughout math.

Axiom: **The well ordering principle (WOP)**. In any nonempty set of natural numbers, there is a unique smallest member.

Starting point.

- Besides the WOP, we'll assume that the basic facts of addition, subtraction, multiplication, and comparison are all understood for the integers and the natural numbers.
- For example, I'll use the inference for natural numbers
$$a \cdot b < c \cdot b \Rightarrow a < c$$
without stopping to justify it.
- Aside: It would be possible to start instead with just 0 and function succ and prec as "undefined terms" and a small number of axioms (called the Peano postulates) about them and define addition, subtraction, multiplication, and comparison in terms of these undefined terms. (The functions turn out to be such that $\mathrm{succ}(a) = a+1$ and $\mathrm{prec}(b) = b-1$.) However, such an exercise would take a while and not add much to your practical understanding of the integers.
- Therefore we next look at *division* of integers.

Division

Lemma: “The Euclidean lemma” For any $a, b \in \mathbb{N}$, with $b \neq 0$, there exists a pair of natural numbers (q, r) such that $a = qb + r$ and $r < b$.

Aside: We can express this theorem more concisely as

$$\forall a, b \in \mathbb{N}, [b \neq 0 \to \exists q, r \in \mathbb{N}, (a = qb + r \wedge r < b)]$$

Proof

Aside on reasoning techniques used

This single proof illustrates several important proof techniques.

Direct proof of “for all”

To prove that all members of a set V have some property P:

$$\forall x \in V, P(x)$$

Pick a name x for an arbitrary member of the set, then show that $P(x)$ is true.

We wrote:

- Suppose that a, b are any natural numbers at all.
- *The rest of the proof shows that*

$$b \neq 0 \to \exists q, r \in \mathbb{N}, (a = qb + r \wedge r < b)$$

Direct proof of implication

To prove an implication $P \to Q$: Suppose that P is true, show that Q is also true.

We wrote:

- Suppose that $b \neq 0$.
- *The rest of the proof shows*
$$\exists q, r \in \mathbb{N}, (a = qb + r \wedge r < b)$$

Likewise, to show $P \vee Q$: Suppose that $\neg P$ is true and show that Q must then be true.

This is because $P \vee Q \Leftrightarrow \neg P \rightarrow Q$.

Constructive proof of existence

To show that $\exists x \in V, P(x)$: Find an example $x_0 \in V$ and then show that $P(x_0)$ is true.

We constructed numbers r_0 and q_0 and then showed that $a = q_0 b + r_0 \wedge r_0 < b$

Proof of a conjunction

To show $P \wedge Q$: Prove P and then prove Q. (Actually, when proving Q we may assume P, since it has already been proved, or, to put it another way, because $P \wedge Q \Leftrightarrow P \wedge (P \rightarrow Q)$.)

To prove $a = q_0 b + r_0 \wedge r_0 < b$ we first proved $a = q_0 b + r_0$ and then proved $r_0 < b$.

Proof by contradiction

To show P: Assume $\neg P$ and then prove something that is false.

We wanted to show $r_0 < b$, so we assumed that $r_0 \geq b$ and then showed that this implied that r_0 is not the smallest member of S, when in fact, by definition, it is.

- Suppose (falsely, it will turn out) $r_0 \geq b$
  - $*$ *This part of the proof shows a contradiction.*
- Thus, in fact, $r_0 < b$

Justifying existence

If you introduce a name for an object that has certain properties, then you must be able to justify that such an object actually exists.

In the example,

- we justified the existence of a the smallest member of S by appealing to the WOP and
- we justified the existence of a q_0 such that $r_0 = a - q_0 b$ by the fact that $r_0 \in S$ and by defining property of the set S.

Back to division

We can extend the above lemma in two ways. First we extend it from the natural numbers to the integers. Second, we show that the pair is unique.

Notn: The absolute value of an integer b is the natural number $|b|$ such that $|b| = b \vee |b| = -b$.

Theorem: "The Euclidean Division Algorithm" [Note this is not really an algorithm, It is an existence theorem.]

For any $a, b \in \mathbb{Z}$ with $b \neq 0$, there exists a unique pair of integers (q, r) such that $a = qb + r$ and $0 \leq r < |b|$

Proof of existence.

- Let a and b be any members of $\mathbb{Z}$ with $b \neq 0$.
- Case: $a, b \in \mathbb{N}$
  - ∗ Our Euclidean lemma already proves the existence of (q, r)
- Case $a \in \mathbb{N}$ and $-b \in \mathbb{N}$
  - ∗ Let (q_1, r_1) be such that $-bq_1 + r_1 = a$ and $0 \leq r_1 < -b$. (Such a pair must exist by the Euclidean lemma)
  - ∗ Let $q_0 = -q_1$ and $r_0 = r_1$

  - $*$ The pair (q_0, r_0) satisfies the constraints $a = q_0 b + r_0$ and $0 \leq r_0 < |b|$

- Case $-a \in \mathbb{N}$ and $b \in \mathbb{N}$
  - $*$ Let (q_1, r_1) be such that $bq_1 + r_1 = -a$ and $0 \leq r_1 < b$. (Such a pair must exist by the Euclidean lemma)
  - $*$ Case $r_1 > 0$

$$\begin{aligned} a &= -bq_1 - r_1 \\ &= -b(q_1 + 1 - 1) - r_1 \\ &= -b(q_1 + 1) + b - r_1 \end{aligned}$$

    - · Let $q_0 = -(q_1 + 1)$ and $r_0 = b - r_1$
    - · Note that since $0 < r_1 < b$ we have $0 < r_0 < b$
    - · The pair (q_0, r_0) satisfies the constraints $a = q_0 b + r_0$ and $0 \leq r_0 < |b|$
  - $*$ Case $r_1 = 0$
    - · $a = -bq_1$
    - · Let $q_0 = -q_1$ and $r_0 = 0$
    - · The pair (q_0, r_0) satisfies the constraints $a = q_0 b + r_0$ and $0 \leq r_0 < |b|$

- Case $-a \in \mathbb{N}$ and $-b \in \mathbb{N}$
  - $*$ Let (q_1, r_1) be such that $-bq_1 + r_1 = -a$ and

$0 \leq r_1 < -b$. (Such a pair must exist by the Euclidean lemma)

- $*$ Case $r_1 > 0$

$$\begin{aligned} a &= bq_1 - r_1 \\ &= b(q_1 + 1 - 1) - r_1 \\ &= b(q_1 + 1) - b - r_1 \\ &= b(q_1 + 1) + (-b - r_1) \end{aligned}$$

  - $\cdot$ Let $q_0 = (q_1 + 1)$ and $r_0 = (-b - r_1)$.
  - $\cdot$ Note that since $0 < r_1 < -b$ we have $0 < r_0 < -b$
  - $\cdot$ The pair (q_0, r_0) satisfies the constraints $a = q_0 b + r_0$ and $0 \leq r_0 < |b|$

- $*$ Case $r_1 = 0$
  - $\cdot$ $a = bq_1$
  - $\cdot$ Let $q_0 = q_1$ and $r_0 = 0$
  - $\cdot$ The pair (q_0, r_0) satisfies the constraints $a = q_0 b + r_0$ and $0 \leq r_0 < |b|$

□

By the way, Gossett presents a much more elegant existence proof by generalizing the construction we used to prove the lemma. For this reason he does not need and does not present the lemma.

Aside

This proof illustrates two more useful proof techniques

Proof by cases.

We want to prove P . First assume A_0 and prove P under that assumption. Then assume A_1 and prove P under that assumption. As long as $A_0 \vee A_1$ is clearly true, then we have proved P.

The idea extends to any number of cases.

Using previously proved theorems and lemmata

In the above proof we appealed a number of times to the lemma proved earlier.

It makes sense to decompose complicated arguments into a number of theorems, just as one would decompose a complex algorithm into a number of subroutines.

Back to the Euclidean Algorithm

The Euclidean Algorithm asserts also that the pair (q, r) is unique.

Proof of uniqueness.

Aside on the proof technique

This proof illustrates a common method of proving uniqueness (nonduplication)

To show that no more than 1 thing has property P:

- Let x and y be any two things.
- Assume $P(x)$ and $P(y)$.
- Show $x = y$ under these assumptions.

Underlying this proof technique is the following fact about sets

$$(\exists x, y \in S, x \neq y) \Leftrightarrow |S| > 1$$

or equivalently (negating both sides & using De Morgan)

$$(\forall x, y \in S, x = y) \Leftrightarrow |S| \leq 1$$

which might be worth a moment's thought.

Back to division again

If (q, r) satisfy the conditions set out

- we call q the quotient of a divided by b and
- we call r the remainder of a divided by b.

Notation

div We write $a \operatorname{div} b$ to mean the quotient, when a is divided by b.

mod We write $a \operatorname{mod} b$ to mean the remainder when a is divided by b.

Thus, when $b \neq 0$, $b(a \operatorname{div} b) + a \operatorname{mod} b = a$ and $0 \leq a \operatorname{mod} b < |b|$

Examples

- $9 \operatorname{div} 3 = \square$ while $9 \operatorname{mod} 3 = \square$
- $10 \operatorname{div} 3 = \square$ while $10 \operatorname{mod} 3 = \square$
- $11 \operatorname{div} 3 = \square$ while $11 \operatorname{mod} 3 = \square$
- $-9 \operatorname{div} 3 = \square$ while $-9 \operatorname{mod} 3 = \square$
- $-10 \operatorname{div} 3 = \square$ while $-10 \operatorname{mod} 3 = \square$
- $-11 \operatorname{div} 3 = \square$ while $-11 \operatorname{mod} 3 = \square$
- $10 \operatorname{div} -3 = \square$ while $10 \operatorname{mod} -3 = \square$
- $-10 \operatorname{div} -3 = \square$ while $-10 \operatorname{mod} -3 = \square$

If x is a real number then

- “floor” $\lfloor x \rfloor$ is the largest integer not larger than x

- “ceiling” $\lceil x \rceil$ is the smallest integer not smaller than x

Note that

- $a \operatorname{div} b = \left\lfloor \frac{a}{b} \right\rfloor$, if $b > 0$
- $a \operatorname{div} b = \left\lceil \frac{a}{b} \right\rceil$, if $b < 0$
- $a \operatorname{div} b = \frac{a}{b}$ iff $a \bmod b = 0$
- $a \bmod b = a - b(a \operatorname{div} b)$

Divisibility

Divisibility: For $a, b \in \mathbb{Z}$, we say that $b \mid a$ (b **divides** a) iff there exists an integer q such that $a = bq$.

When $b \neq 0$, this is to say $a \bmod b = 0$ or that $a \operatorname{div} b = \frac{a}{b}$

True or false?

- $6 \mid 12$, $6 \mid 6$, $6 \mid 0$, $6 \mid -6$ □
- $6 \mid 11$□
- $0 \mid 0$□

Theorem: If $a \mid b$ and $a \mid c$ then

- $a \mid b + c$
- $a \mid k \cdot b$, for any $k \in \mathbb{Z}$.
- $a \mid b - c$

Theorem: For all $a, b, c \in \mathbb{N}$

- Reflexivity: $a \mid a$
- Antisymmetry: If $a \mid b$ and $b \mid a$ then $a = b$
- Transitivity: If $a \mid b$ and $b \mid c$ then $a \mid c$.

This is to say divisibility is a **partial order** on the naturals.

(For the integers, divisibility is reflexive and transitive, but not antisymmetric. Why?)

Divisors. We say that the divisors of an integer a is the set of integers b such that $b|a$.

Congruence. If integers a, b, and m are such that $m \mid (a - b)$ then we say that a and b are congruent mod. m.

Thus for each integer m there is a different binary relation of congruence.

Notn. We write $a \equiv b \pmod m$ to mean that a and b are congruent mod m.

Aside: Note that the use of the symbol mod here is quite different from our earlier use of mod as a binary operator. Here we are using mod in a parenthetical remark that indicates which relation of congruence we are dealing with at the moment.

Theorem. If $a \equiv b \,(\mathrm{mod}\, m)$ and $c \equiv d \pmod m$ then

- $a + c \equiv b + d \,(\mathrm{mod}\, m)$
- $ka \equiv kb \pmod m$
- $ac \equiv bd \pmod m$

Proof

Theorem. For all $a, b, c, m \in \mathbb{Z}$ and $m \neq 0$

- Reflexivity: $a \equiv a \pmod{m}$
- Symmetry: $a \equiv b \pmod{m}$ iff $b \equiv a \pmod{m}$
- Transitivity: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.

This is to say that congruence mod m is an **equivalence relation.**

GCD: The greatest common divisor of two integers (not both 0) is the largest integer that divides both.

I.e. $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$ and for all c if $c \mid a$ and $c \mid b$ then $c \leq \gcd(a, b)$.

E.g.

- $\gcd(12, 8)$ is what?
- $\gcd(9, 3)$ is what?
- $\gcd(0, 20)$ is what?
- $\gcd(10, 21)$ is what?

If $\gcd(a, b) = 1$, what does that say about a and b?

Theorem

- $\gcd(0, b) = b$, if b is a positive integer
- $\gcd(a, b) = \gcd(b, a)$, if either $a \neq 0$ or $b \neq 0$
- If $b \neq 0$, then $\gcd(a, b) = \gcd(a \bmod b, b)$

Proof of last part

Let $r = a \bmod b$ and $q = a \operatorname{div} b$. Then $a = qb + r$.

- Let $g_0 = \gcd(a, b)$ and $g_1 = \gcd(r, b)$
- Since $g_1 \mid r$ and $g_1 \mid b$, we have $g_1 \mid qb + r$, and thus $g_1 \mid a$
- Also $g_1 \mid b$ and so g_1 is a divisor of both a and b. Thus $g_1 \leq g_0$ (by definition of GCD)
- Since $g_0 \mid b$ we have $g_0 \mid qb$.
- Since $g_0 \mid a$ and $g_0 \mid qb$ we have $g_0 \mid a - qb$ and thus

$g_0 \mid r$.

- Since g_0 divides both r and b we have $g_0 \leq g1$ (by the definition of GCD)
- Since $g_1 \leq g_0$ and $g_0 \leq g_1$ we have $g_0 = g_1$. □

Using this theorem we can see that the following algorithm computes the $\gcd(A, B)$ for natural A and B where $A \neq 0$ or $B \neq 0$

```
{ // Euclidean algorithm for GCD in C/Java notation.
        int a = A, b = B ;
        // Loop invariant: gcd(A,B) == gcd(a,b)
        //                    && (a !=0 || b !=0)
        while( b != 0 ) {
                int r = a  % b ;
                a = b ;
                b = r ; }
        gcd = a ; }
```

Aside: What is a loop invariant?

- A loop invariant is a statement about the state of the program that is true just before the evaluation of a loop's guard expression (in this case $b \neq 0$ is the guard expression).

- In our example, the invariant is trivially true at the start of the first iteration because a and b are initialized to A and B respectively.
- In our example, the invariant is true at the end of each iteration because it was true at the start of the iteration.
  - $*$ To see this, let a and b be the values of 'a' and 'b' at the start of an iteration and let a' and b' be the values of 'a' and 'b' at the end of the iteration:

    $$a' = b \text{ and } b' = a \bmod b$$

  - $*$ We have

$$\begin{aligned} \gcd(A, B) &= \gcd(a, b) \text{ Assuming the invariant holds at start} \\ &= \gcd(b, a \bmod b) \text{ Latest theorem} \\ &= \gcd(a', b') \text{ From the loop body} \end{aligned}$$

  - $*$ From the loop guard we have $b \neq 0$ so $a' \neq 0$.
  - $*$ Thus $\gcd(A, B) = \gcd(a', b') \wedge (b' \neq 0 \vee a' \neq 0)$
- When the loop is exited, the invariant $\gcd(A, B) = \gcd(a, b)$ will be true and so will $b = 0$. Thus, when the loop is exited, $\gcd(A, B) = a$.