MATH/COMP61-03 Spring 2014 Notes: January 16th

Andrew Winslow

1 Definitions

Definitions are the starting point for all mathematical reasoning. Here is a defintion:

Definition. *An integer n is* even *provided n it is divisible by 2.*

This defintion uses other terms that are ambiguous. What is an *integer*? What does it mean to be *divisible*?

Definition. *An* integer *is a number in the infinite set $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.*

Now we have more problems. What is a *set*? What does it mean for something to be *infinite*? What does $\ldots$ mean? These are complex issues we will consider now. Instead, we simply say "integers are whole numbers" and rely on common sense. For instance, 5 is an integer, -57 is an integer, 0 is an integer. But $\frac{3}{4}$ is not, nor is $\sqrt{2}$, π, etc.

On the other hand, *divisible* isn't so intuitive, and needs a definition:

Definition. *An integer n is* divisible *by an integer a provided there is an integer b such that $ab = n$.*

For instance, 12 is divisible by 4 since $4 \cdot 3 = 12$, i.e. $n = 12$, $a = 4$, and $b = 3$. On the other hand, 12 is not divisible by 5, since there is no integer b such that $5b = 12$. We use the notation $a \mid n$ to mean "n is divisible by a", and $a \nmid n$ to mean "n is not divisible by a".

Often times there are multiple defintions surrounding the same idea. In this case we can define these addition terms using previously definitions:

Definition. *An integer a is said to be a* divisor *or* factor *of n if n is divisible by a.*

Now let's build some more interesting definitions that we can use later to say interesting things about integers.

Definition. *An integer n is* odd *provided there is an integer a such that $n = 2a + 1$.*

Definition. *An integer n is* composite *provided that $n > 1$ and there is some integer a with $1 < a < n$ such that $a \mid n$.*

Is 9 composite? $9 > 1$ and $a = 3$ is a number with $1 < a < 9$ such that $a \mid 9$. So 9 is composite. On the other hand, 5 is not composite, since for all potential values of a with $1 < a < 5$, namely 2, 3, and 4, it is not the case that $a \mid 5$. To complement the definition of composite numbers, we introduce a name for integers larger than 1 that are not composite:

Definition. *An integer n is* prime *provided that $n > 1$ and for each integer a with $1 < a < n$, $a \nmid n$.*

Is 3 prime? $3 > 1$ and for the only integer a with $1 < a < 3$, namely 2, $a \nmid 3$. So yes, 3 is prime. Is 10 prime? $10 > 1$, but there is an integer $a = 5$ with $1 < a < 10$ such that it is not the case that $a \nmid 10$. So 10 is not prime. Is 2 prime? $2 > 1$, but there is no integer a with $1 < a < 2$. So it is the case that for each integer b with $1 < a < 2$, $b \nmid x$.

Does this last result seem weird? The statement "for each integer a with $1 < a < 2$, $a \nmid 2$" is true because there is no such a. Lame. We call such a statement *vacuously true*. Here's another vacuously true statement: all negative prime numbers are even. No prime numbers are negative, so all the negative ones are even – although it may seem like a silly statement, it is a true statement.

2 Theorems

We just talked about a few statements regarding objects we defined, like divisibility and what it means for an integer to be prime. In mathematics, such statements that are true are called *theorems*. Here's a theorem:

Theorem. *If an integer n is even, then $n + 1$ is odd.*

Theorems usually have the *if-then form*: "If A, then B.", where A and B are called the *hypothesis* and *conclusion*, respectively. For the previous theorem, $A =$ "an integer n is even" and $B =$ "$n + 1$ is odd". As shorthand, we denote theorems of this form as $A \Rightarrow B$. The "If A, then B." statement can also be written as "A only if B" and "A implies B".

If we have a theorem $A \Rightarrow B$ that is true, what does this mean? It means that if A is true, then B is true. For instance, if $n = 2$, then the previous theorem says that $n + 1 = 3$ is odd. But if $n = 3$ (and thus x is not even), then the theorem says nothing.

Consider the four combinations of truth values for A and B:

A	B	Possible if $A \Rightarrow B$
True (n is even)	True ($n + 1$ is odd)	Yes
True (n is even)	False ($n + 1$ is not odd)	No
False (n is not even)	True ($n + 1$ is odd)	Yes
False (n is not even)	False ($n + 1$ is not odd)	Yes

If the hypothesis A is always false (e.g. $A =$ "n is a negative prime.") then only the last two combinations occur. In this is the case we call the theorem *vacuous*. All vacuous theorems are true.

The A and B statements can be simple, but may also be composed of combinations of smaller statements conjoined with "and" or "or". For instance:

Theorem. *If an integer n is prime and odd, then $n \geq 3$.*

In this case, the theorem still has the if-then form with $A \Rightarrow B$, but $A = C$ and D, where $C =$ "n is prime" and $D =$ "n is odd". In other words, the theorem is C and D $\Rightarrow$ B. An and-statement is defined to be true if both halves are true, and false otherwise:

A	B	A and B
True	True	True
True	False	False
False	True	False
False	True	False

An or-statement is similar:

Theorem. *If an integer n is prime or composite, then $n > 1$.*

Unlike some usages in English, an or-statement even if both halves are true:

A	B	A or B
True	True	True
True	False	True
False	True	True
False	True	False

A statement can also be negated using "not", like in English:

Theorem. *If an integer n is not even, then n is odd.*

A	not A
True	False
False	True

Finally, we consider a special case of composing two if-then statements. It may seem strange to compose if-then statements, but they are statements like any other and can be used as hypotheses and conclusions in theorems. Consider two closely related theorems:

Theorem. *If an integer n is even, then $n + 1$ is odd.*

Theorem. *If an integer $n + 1$ is odd, then n is even.*

The first theorem is "If A, then B." ($A \Rightarrow B$) and the second theorem is "If B, then A." ($B \Rightarrow A$). Suppose we wanted to have a theorem that combined these theorems, i.e. "If A then B, and if B then A":

Theorem. *If an integer n is even, then $n+1$ is odd, and if $n+1$ is odd, then n is even.*

This is legit, but a little hard to read. It turns out theorems of this form are very common; so common that we have a special *if-and-only-if form* for them: "A if and only if B":

Theorem. *An integer n is even if and only if $n+1$ is odd.*

Just like if-then theorems were written as $A \Rightarrow B$, if-and-only-if theorems are written as $A \Leftrightarrow B$, where $A \Leftrightarrow B$ is defined as $A \Rightarrow B$ and $\mathrm{B} \Rightarrow \mathrm{A}$. Sometimes the English "if and only if" is shortened to "iff", e.g. "an integer n is even iff $n+1$ is odd. Compare $A \Rightarrow B$ to $A \Leftrightarrow B$:

A	B	Possible if $A \Rightarrow B$	Possible if $A \Leftrightarrow B$
True	True	Yes	Yes
True	False	No	No
False	True	Yes	No
False	False	Yes	Yes

So proving $A \Leftrightarrow B$ says more than $A \Rightarrow B$, since it forbids the situation where A is false and B is true.

3 Proofs

A convincing argument as to why a theorem is true is known as a *proof*. Theorems and proofs usually come in pairs, with the theorem first and the proof following. Like so:

Theorem. *If an integer n is even, then $n+1$ is odd.*

Proof. *Let n be an even integer. If n is even, then by the definition of* even*, $2 \mid n$. If $2 \mid n$, then by the definition of* divisible*, there exists an integer a such that $n = 2a$. So $n+1 = 2a+1$ for some integer. So by the definition of* odd*, $n+1$ is odd.* □

Notice how each step of the proof follows from previous statements and definitions. Here are the steps of the proof:

1. Let n be an even integer. (by hypothesis)
2. If n is even, then $2 \mid n$. (by definition of *even*)
3. If $2 \mid n$, then there exists an integer a such that $n = 2a$. (by definition of *divisible*)
4. If $n = 2a$, then $n+1 = 2a+1$. (by algebra)
5. If $n+1 = 2a+1$, then $n+1$ is odd. (by definition of *odd*)

Each step of the proof is small step that follows easily from previous steps. This gives a growing set of true statements, moving towards the statement of the theorem we wish to prove. Proofs don't need to follow this form, but many do, and one can think of a proof of this form as a path through "truthland" from the hypothesis to the conclusion. The proof acts as tour guide, making small steps to lead the tourist along the path. Here's another theorem-proof pair:

Theorem. *If an integer n is odd, then $n-1$ is even.*

Proof. *Let n be an odd integer. If n is odd, then by the definition of* odd*, $n = 2a+1$ for some integer a. So $n-1 = 2 \cdot a$ for some integer a and so $2 \mid n-1$. So $n-1$ is even.* □

Now we can use this and the prior theorem in the proof of a new theorem:

Theorem. *An integer n is even if and only if $n+1$ is odd.*

Proof. *Let n be an even integer. Then by the previous theorem, $n+1$ is odd. So if n is even, then $n+1$ is odd. Now let $n+1$ be an odd integer. By the previous theorem, $(n+1)-1 = n$ is even. So if $n+1$ is odd, then n is even. So n is even if and only if $n+1$ is odd.* □

Many times the path is not so clear. Consider this interesting theorem:

Theorem. *The integer n^2-1 is composite for any integer $n \geq 3$.*

This theorem isn't in if-then form. What is the hypothesis and what is the conclusion? Let's start by identifying some statements. Let $A =$ "$n \geq 3$ is an integer" and $B =$ "n^2-1 is composite". Then we can restate the theorem as $A \Rightarrow B$:

Theorem. *If $n \geq 3$ is an integer, then n^2-1 is composite.*

The first and last few steps of the proof follow from the definitions of the hypothesis and conclusion:

1. Let $n \geq 3$ be an integer.
2. So n^2-1 is an integer.
3. ...
4. ... then $n^2-1 > 1$.
5. ... there exists an integer a with $1 < a < n^2-1$ and $a \mid n^2-1$.
6. So n^2-1 is composite.

When starting a proof, the first step is to fill in the first and last few steps of the proof by "unravelling" the definitions in the hypothesis and conclusion. But what about the in-between? Notice $3^2-1 = 2 \cdot 4$, $4^2-1 = 3 \cdot 5$, $5^2-1 = 4 \cdot 6$, etc. The pattern $n^2-1 = (n-1) \cdot (n+1)$ emerges. We can use $n-1$ as the integer a needed to show a^2-1 is composite. This is enough to complete the missing middle of the proof:

Theorem. *If $n \geq 3$ is an integer, then n^2-1 is composite.*

Proof. *Let $n \geq 3$ be an integer. If $n \geq 3$, then $2 \leq n-1 < (n-1) \cdot (n+1) = n^2-1$. If $2 \leq n-1 < (n-1) \cdot (n+1) = n^2-1$, then $n^2-1 > 1$. Moreover, $1 < n-1 < n^2-1$ and $n-1 \mid n^2-1$. So there exists an integer $a = x-1$ with $1 < a < n^2-1$ and $a \mid n^2-1$. So n^2-1 is composite.* □

In this case, trying a few examples of hypothesis and conclusion pairs was enough to see the connection. In general, finding proofs can be very difficult; persistence and the willingness to try new ideas is key.