Induction and Recursion 1

Today:

- ☐ Mathematical induction
- ☐ Examples

1 Mathematical Induction

Like set theory, number theory can be understood as the consequences of a set of axioms. Number theory is only a bit less spare than set theory. As a matter of syntax, we have only

- One constant symbol: 0
- One predicate symbol: $<$
- Three function symbols, say:
  - S, the successor function, a unary function
  - $+$, for addition, a binary function
  - $\cdot$, for multiplication, a binary function (can be defined from above).

As usual, we also include equality.

While this may seem small, it's plenty powerful to say hard things about numbers. For example, one can define an define an exponentiation operator E and then, from that, state "Fermat's Last Theorem." That result (proven by Andrew Wiles in 1993) says that there are are positive numbers a, b, c, and $n > 2$ such that $a^n + b^n = c^n$:

$$(\forall a)(\forall b)(\forall c)(\forall n)(S(S(0)) < n \to \neg(aEn + bEn = cEn)).$$

The axioms that traditionally *define* number theory are called the axioms of *Peano arithmetic*, named for Giuseppe Peanno (1989).

1. $(\forall x)(S(x) \neq 0)$
2. $(\forall x)(\forall y)(S(x) = S(y) \to x = y)$

3. $(\forall x)(x + 0 = x)$
4. $(\forall x)(\forall y)(x + S(y) = S(x + y))$
5. $(\forall x)(x \cdot 0 = 0)$
6. $(\forall x)(\forall y)(x \cdot S(y) = x \cdot y + x)$
7. $(\forall P)(P(0) \wedge (\forall n)(P(n) \rightarrow P(n + 1))) \rightarrow (\forall n)P(n)$

The last is not a "first-order" property in logic, as we are quantifying over all predicates P, not all points in the underlying universe $\mathcal{U}$.

You can think of this last property like a *ladder*: if you can get to the bottommost rung, and you can always move up one rung, then you can get to an arbitrarily high rung of the ladder.

We can't *prove* the principle of induction. Rather, it is something that we assume in our basic definition about what numbers *are*.

Here is is without the symbols, and in a way that is more prescriptive:

> **Principle of mathematical induction, 1.** To prove a proposition $P(n)$ for all numbers n:
>
> - Prove $P(0)$. "The basis"
> - Prove that $P(n) \rightarrow P(n + 1)$ for all n. "The inductive step"

When you're carrying out step (2), the assumption $P(n)$ is referred to as the "inductive assumption."

Sometimes, when applying this principle, it's useful to start at a number $n_0 > 0$. We can recast induction to allow this:

> **Principle of mathematical induction, 2.** To prove a proposition $P(n)$ for all numbers $n \geq n_0$:
>
> - Prove $P(n_0)$.
> - Prove that $P(n) \rightarrow P(n + 1)$ for all $n \geq n_0$.

This isn't actually a strengthening. All you have to do to get the second form from the first is to "shift" the predicate P you are thinking about, so that it adds n_0 to the prior value of n.

Finally, it is sometimes nice to strengthen the inductive assumption so that we have more to work with.

> **Principle of mathematical induction, 3.** To prove a proposition $P(n)$ for all numbers $n \geq n_0$:
>
> - Prove $P(n_0)$.
> - Prove that $P(n_0) \wedge P(n_0 + 1) \wedge \cdots \wedge P(n) \rightarrow P(n+1)$ for all $n \geq n_0$.

Folks call this "strong" induction. Again, it isn't a significant change we have made, in some sense, as we have just redefined our predicate.

Note: an alternative to assuming $P(n)$ and proving $P(n+1)$ is assuming $P(n-1)$ and proving $P(n)$. It amounts to the same.

2 Example 1: Sum of first n numbers

Let's start to use this thing, repeating a proof that we've already seen two proofs of: $1 + 2 + \cdots + n = n(n+1)/2$.

Do the proof in class.

3 Example 2: Sum of first n odd numbers

Similarly, we can reprove the simple result that $1 + 3 + \cdots + (2n-1) = n^2$.

Do the proof in class.

4 Example 3: Sum of first n squares

We already argued that the sum of the first n squares is $O(n^3)$, and even that it's about $n^3/3$. Let's show, more precisely, that

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n.$$

Do the proof in class.

5 Example 4: Divisibility

How about proving that $n^2 + n$ is always even. Again, there are non-inductive approaches. The most obvious is a case analysis: if n is even than we are adding the square of an even number, which is even, to an even number, and the sum of two even numbers is even.

Alternatively, if n is odd, we are adding the square of an odd number, which is odd, to an odd number, making an even sum. But induction works perfectly well, too, so let's see it that way.

Do the proof in class.

6 Example 5: Dispensing envelopes

Sam's Department Store sells envelopes in packages of 5 and 12. Prove that, for any $n \geq 44$, the store can sell you exactly n envelopes.

Basis: $44 = 2 \cdot 12 + 4 \cdot 5$.

Inductive step: Suppose it is possible to buy $n \geq 44$ envelopes. Show that it is possible to buy $n+1$ envelopes.o So $n+1 \geq 45$.

Consider your way of buying n envelopes.

(a) Suppose it entailed buying at least 7 packets of 5. Then trade in the 7 packets of 5 for 3 packets of 12.

(b) Alternatively, it entailed buying at most 6 packets of 5. So you bought at most 30 envelopes in packets of 5. So you bought at least 14 envelopes in packets of 12. Which means you bought at least 2 packets of 12, obtaining at least 24 envelopes. So take those 2 packets of 12 and trade them in for 5 packets of 5. You will again have bought one more packet of envelopes. $\diamondsuit$

Can you figure out a more efficient way to solve the problem? Where you can map $n \geq 44$ to its solution quickly and easily?

7 Example 6: Triominoes

Show that you can tile any "punctured" $2^n \times 2^n$ grid by *triominoes* A triominoe looks like:

```
#
##
```

Triominoes may be rotated. A punctured grid is a grid has one cell value "removed."

Do the proof in class.