Week 1

This week we discussed proof by induction. We began with the following:

Theorem 0.1. *Let R be a commutative ring, $a, b \in R$. Then $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$.*

We then noted that all we really needed was that $ab = ba$, and proceeded to do the proof.

Proof. We proceed by induction.

Base case: $n = 1$. Then $(a+b)^1 = a + b$ by definition, and so the base case works, as $1 = \binom{1}{0} = \binom{1}{1}$.

Induction step: we assume that the result holds for $k = 1, \ldots, n$ and want to prove it for the case $k = n+1$. We note that $(a+b)^{n+1} = (a+b)^n(a+b)$. We know that $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$. Thus, $(a+b)^{n+1} = (a+b)\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} = a\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} + b\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$. Finally, this gives us

$$(a+b)^{n+1} = \sum_{i=0}^{n} \binom{n}{i} a^{i+1} b^{n-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i}.$$

Next, we reindex, taking $j = i + 1$ in the first sum. That is, $i = j - 1$. This changes that sum to $\sum_{j=1}^{n+1} \binom{n}{j-1} a^{j-1+1} b^{n-j+1} = \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n+1-j}$. Now, it doesn't matter what we call the index of summation, so we're free to call it i again. Thus

$$(a+b)^{n+1} = \sum_{i=1}^{n+1} \binom{n}{i-1} a^i b^{n+1-i} + \sum_{i=0}^{n} \binom{n}{i} a^i b^{n+1-i}.$$

This is then equal to

$$a^{n+1} + b^{n+1} + \sum_{i=1}^{n} \left(\binom{n}{i-1} + \binom{n}{i} \right) a^i b^{n+1-i}.$$

All that remains is to show that $\binom{n}{i-1} + \binom{n}{i} = \binom{n+1}{i}$, and the result must hold.

To see this, we make a counting argument. The number $\binom{n}{i}$ is just the number of ways to choose i objects from a collection of n objects. So now, say we are given $n + 1$ objects and want to select i of them. That is, we want to write down an expression for $\binom{n+1}{i}$. If we fix one of the objects, then every way

to do this either contains it or doesn't. If it doesn't, then we're choosing i from the other n, and if it does then we're choosing $i-1$ from the other n. The way to do these are, respectively, $\binom{n}{i}$ and $\binom{n}{i-1}$, so $\binom{n+1}{i} = \binom{n}{i} + \binom{n}{i-1}$, which is exactly what we wanted. □

Next up, a non-proof (due to Polya). We claim that all horses are the same color.

Base case: one horse is the same color as itself, so the base case holds.

Induction step: assume you have $n+1$ horses, and any n of them are the same color. Then look at $\{1, \ldots, n\}$ and $\{2, \ldots, n+1\}$. These two sets consist entirely of horses of one color each. There is overlap between them, so all horses must be the same color.

The flaw in this proof is that for $n = 2$, there is not, in fact, an overlap. So the proof breaks down at $n = 2$. You must always check that the implication always holds, for all numbers greater than your base case.

The following are problems that were assigned in class and presented, along with my solutions to them. These we will come back to later once we've discussed modular arithmetic, because they clarify the problems and make the solutions much easier.

Proposition 0.2. *If n is odd, then 8 divides $n^2 - 1$.*

Proof. Base case: if $n = 1$, then 8 needs to divide zero, which it does.

Induction step: Assume that for n, we have $8|n^2 - 1$. Then we must show it for $n+2$, the next odd number. $(n+2)^2 - 1 = n^2 + 4n + 4 - 1 = n^2 - 1 + 4n + 4$. We already know that 8 divides $n^2 - 1$, so we must merely show that it divides $4n+4$, which is $4(n+1)$. As n is odd, $n+1$ is even, and so we get the additional factor of two that we need. □

Proposition 0.3. *If n is odd and not divisible by 3, then $6|n^2 - 1$.*

Proof. The base case is again $n = 1$, which is trivial.

For the induction step, we will break the problem into two cases.

First we look at the case where the odd number $n+2$ is not divisible by three. Then we need to show that $(n+2)^2 - 1$ is divisble by six. This is $n^2 + 4n + 4 - 1 = n^2 - 1 + 4(n+1)$. We know that six divides $n^2 - 1$, so we just need that it divides $4(n+1)$. As $2|4$, we just need to check that $3|n+1$. Now, n and $n+2$ aren't divisible by three, so $n+1$ must be, and this case is done.

Now, we look at the case where $3|n+2$. Then the next number is $n+4$. So we look at $(n+4)^2 - 1$ and get $n^2 + 8n + 16 - 1 = n^2 - 1 + 8(n+2)$. By induction hypothesis, $n^2 - 1$ is divisible by six. Now, $8(n+2)$ is divisible by 2, and $n+2$ is divisible by 3, because that's the case that we're in. Thus, $6|(n+4)^2 - 1$.

Combined, this gives us the full induction, as the sequence of numbers not divisible by two or three alternates between the two cases. □

Proposition 0.4. *For all n, $30|n^5 - n$.*

Proof. This one we had trouble with in class. We break it up into three parts. For 30 to divide $n^5 - n$, we need to show that 2, 3 and 5 all divide it.

We don't need induction for the first two parts. We will just factor $n^5 - n$. It is $n(n^4-1) = n(n^2+1)(n^2-1) = n(n-1)(n+1)(n^2+1)$. Now, one of n and $n+1$ must be even, so there is a factor of two. Additionally, one of $n-1, n, n+1$ must be divisible by 3. This leaves divisibility by 5 to check. For this, we do induction.

Base case: $n = 1$, we have $5|1^5 - 1 = 0$, which works out.

Now we assume that $5|n^5 - n$. Look at $(n+1)^5 - (n+1)$. This is just $n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 - n - 1 = n^5 - n + 5n^4 + 10n^3 + 10n^2 + 5n$. We have that $5|n^5 - n$, so we just need five to divide $5n^4 + 10n^3 + 10n^2 + 5n$, which is obvious. □

The above divisibility problems will be done again once we've covered modular arithmetic, because that tool makes them much easier to prove.

For more practice on induction, prove the following (these will not be collected):

Exercise 0.1. *Every natural number is a product of prime numbers.*

Exercise 0.2. *Prove* $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Exercise 0.3. *Show that if* $f_1, \ldots, f_n$ *are differentiable, then* $(f_1 \ldots f_n)' = f_1' f_2 \ldots f_n + \ldots + f_1 \ldots f_n'$. *You may assume theorems from calculus.*