MATH 25 CLASS 2 NOTES, 9/24/2010

1. Logical statements

Math is primarily about determining the truth value of various statements. For example, a statement like "The number 3 is even" is obviously false, while the statement "The area of a circle of radius r is πr^2" is true, but substantially harder to prove. In what follows, P and Q will be generic statements which are either true or false.

The language of mathematics is packed with statements of the form 'If P, then Q', where P, Q might be statements which can be either true or false. For example, the statement 'If S is a square, then S is a rectangle' is a true statement, while the statement 'If $f : \mathbb{R} \to \mathbb{R}$ is integrable, then f is continuous' is a false statement. Notice that to disprove this statement, we need only exhibit one counterexample; for instance, any piecewise continuous function (which itself is not continuous) will do. We write $\sim P$ for the *negation* of P. This is the statement which is false exactly when P is true, and can be obtained from P by adding the word 'not'. For example, if P is the statement 'S is a square', then $\sim P$ is the statement 'S is not a square'.

We bring all this up because the statement 'If P, then Q', can be expressed in several other ways. The mathematical shorthand for this statement is $P \implies Q$, which we sometimes read 'P implies Q'. Two other forms this statement might take are 'P is a sufficient condition for Q', or 'Q is a necessary condition for P'. The first statement says that as long as P is true, then Q is true, which is exactly what the original statement says, and the latter statement says that Q must be true if P is true: that is, if P is true, then Q is also true. Another way of saying 'If P, then Q' is by saying 'P is true only if Q is true', or more succinctly, 'P only if Q'. (The word 'only' is of critical importance, since omitting it completely changes the logical content of the statement.)

An important logical point is that the statement $P \implies Q$ **IS NOT ALWAYS EQUIVALENT** to the statement $Q \implies P$. We say two statements are equivalent if one is true exactly when the other is true. For example, consider the statement 'If S is a square, then S is a rectangle'. In this statement, P is 'S is a square', while Q is 'S is a rectangle'. Then it is obvious that $Q \implies P$ is false, since the statement 'If S is a rectangle, then S is a square' is clearly not true. The statement $Q \implies P$ is sometimes called the *converse* of $P \implies Q$.

On the other hand, $P \implies Q$ is logically equivalent to the statement $\sim Q \implies \sim P$, which is sometimes called the *contrapositive* of $P \implies Q$. This might not be obvious, but a careful consideration of what it means for $P \implies Q$ to be true, or consideration of a few examples, will explain why this statement is true.

Finally, the *inverse* of $P \implies Q$ is the statement $\sim P \implies \sim Q$. This is the contrapositive of the converse, so while the inverse and converse are logically equivalent to each other, whether the inverse and converse are true is independent of whether the original statement $P \implies Q$ is true.

Example. Let n be an integer, and let P be the statement "n ends in the digit 0", and Q the statement "n is even". Then $P \implies Q$ is evidently true, since any number which ends in 0 must be even. The converse is the statement "If n is even, then n ends in the digit 0", which is clearly false (n ending in $2, 4, 6, 8$ are all counterexamples), while the contrapositive is the statement "If n is not even, then n does not end in the digit 0". Finally, the inverse is the statement "If n does not end in the digit 0, then n is not even", which obviously is false, for the same reasons the converse is false.

2. Proof by induction

Often, a mathematical statement will make an assertion about positive integers. For example, there is a story about the young C. F. Gauss. One day, when he was ten years old, his teacher, who apparently was not very creative, told his students to sum all the numbers from 1 to 100 before they could go to recess (or something like that). While his classmates were furiously adding $1 + 2 + 3 + \ldots$, Gauss reflected for a few seconds, wrote a number down on his board, and then turned it in. Of course, he was right, and the number he wrote down was 5050.

Gauss realized that $1 + 2 + \ldots + n = n(n + 1)/2$. Before describing how he did it, let's talk about how one uses induction to prove this formula. First, notice that this formula is a statement about all positive integers n. Let $P(n)$ be this statement for the particular value of n; for instance, $P(2)$ is the claim that $1+2 = 3$, while $P(4)$ is the claim $1+2+3+4 = 10$. Notice that simple calculation shows that both are true.

If we want to prove $P(n)$ is true for all positive n, we obviously can't use brute force. Induction is a general strategy for proving that a statement is true for all positive integers n. It consists of two steps:

- Prove $P(1)$ is true (this is usually easy), and
- Prove that, for any positive n, if $P(n)$ is true, then $P(n + 1)$ is also true.

Why does this work? Suppose we've proven both statements true. In particular, we know $P(1)$ is true. But then the second statement tells us that $P(2)$ is true, which in turn tells us that $P(3)$ is true, ad infinitum. So we've proven that $P(n)$ is true for every positive integer n. A way to visualize the induction strategy is to think about setting up an infinite chain of dominos. If $P(n)$ corresponds to toppling the nth domino over, then the first step corresponds to knocking the first domino in the chain over, and the second step corresponds to setting up the dominos in such a way so that if the nth domino falls, then the $n + 1$th domino does as well.

Let's use this strategy to prove the formula for the sum of the first n positive integers. First, verifying $P(1)$ is trivial; it's just the statement $1 = 1$. Next, suppose $P(n)$ is true. We write out what this means:

$$1 + 2 + \ldots + n = \frac{n(n + 1)}{2}.$$

We want to show that $P(n+1)$ is true. This is a statement about $1 + 2 + \ldots + n + (n + 1)$, so it makes sense to add $n + 1$ to both sides of the equation above. This gives

$$1 + 2 + \ldots + n + (n + 1) = \frac{n(n + 1)}{2} + (n + 1).$$

Remember, we're trying to prove the statement $P(n + 1)$, which is the equation

$$1 + 2 + \ldots + n + (n + 1) = \frac{(n + 1)(n + 2)}{2}.$$

The LHS (left hand side) of these two equations are equal. One easily checks that the RHS are equal as well. So we've proven that if $P(n)$ is true, then $P(n+1)$ is true as well. Then induction tells us that $P(n)$ must be true for all n, as desired.

Of course, one could cosmetically modify induction by not starting with $P(1)$; for instance, one might only want to prove $P(n)$ is true for all $n \geq 3$, in which case one starts by proving $P(3)$ instead of $P(1)$. But the general idea is the same.

Incidentally, this isn't the way Gauss discovered the formula $P(n)$. He realized that if you sum the first and last terms in $1+2+\ldots+n$, you get $n+1$. If you sum the second and second to last terms, you also get $n+1$. One continually pairs the integers in this way to get some number of pairs summing to $n+1$. If n is even, there are exactly $n/2$ such pairs, while if n is odd, there are $(n-1)/2$ pairs, with the middle number of $(n+1)/2$ by itself. In both cases, adding up these terms gives $n(n+1)/2$.

3. Divisibility

Let's start with some number theory proper. Let a and b be two integers (not necessarily positive, although most cases we consider will be positive integers).

Definition 1. *We say that b **divides** a if there exists an integer q such that $a = qb$. We sometimes write this as $b|a$. If b does not divide a, then we sometimes write $b \nmid a$. If b divides a, we sometimes say that b is a **divisor** of a.*

Let's look at some basic examples and prove some basic facts about divisibility.

Examples.

- One has $3|12$, say, while $2 \nmid 5$, because $12 = 3 * 4$, while $5 = 2 * (2.5)$, and 2.5 is not an integer. Notice that $b|a$ is the same thing as saying that a is a multiple of b.
- Let's prove a few facts from Exercise 1.3 of the book. First, we'll prove that if $a|b$ and $b|c$, then $a|c$.

  Proof. Since $a|b$ and $b|c$, we can find integers q_1, q_2 such that $b = q_1a, c = q_2b$. Substitute the first equation for b into the second; we get $c = q_2q_1a$. Since q_2q_1 is an integer, $a|c$, as desired. □

  (What's that box for at the end? It signifies that we've finished our proof, and is meant as a way to organize our writing.)
- Another fact is that if $a|b$ and $b|a$, then $a = \pm b$.

  Proof. Write $b = q_1a, a = q_2b$. Again, substituting the first into the second equation, we get $a = q_1q_2a$. At this point, we want to cancel a from both sides. However, we can only do this if $a \neq 0$. So let's first analyze what happens if $a = 0$. If $a = 0$, then the equation $b = q_1a = 0$ tells us $b = 0$ as well, so $a = \pm b$ is definitely true in this case. So now that we've handled what happens if $a = 0$, we can go back to $a \neq 0$ case. We can cancel a from both sides of $a = q_1q_2a$, which gives $q_1q_2 = 1$. However, the only way two integers multiply to 1 is if they are both equal to 1 or ± 1. This implies that $b = \pm a$, as desired. □
- Here is a useful fact (Theorem 1.3a of the text). If $c|a_1, a_2, \ldots, a_k$, then $c|(a_1u_1 + \ldots + a_ku_k)$ for any integers $u_1, \ldots, u_k$.

  Proof. Since $c|a_i$ for all i, we have $a_i = cq_i$ for some integer q_i. Then $a_1u_1 + \ldots + a_ku_k = c(q_1u_1 + \ldots + q_ku_k)$. Since $q_1u_1 + \ldots + q_ku_k$ is an integer, this implies that $c|(a_1u_1 + \ldots + a_ku_k)$, as desired. □
- As an illustration of this fact, we know that $3|6, 15$, say. Then this fact tells us that $3|(6x + 15y)$, for any integers x, y.

In one of the proofs above we see that there are occasions where we might need to do a *case-by-case* analysis. Always be wary when you divide an equation by a number, for example, because it is illegal to divide by 0 and you may need to separately analyze what happens if that number is equal to 0.

Sample Question 1. *You should consult Exercise 1.3 of the text for more basic properties. Let's look at a few of them now. Suppose $d|a$. Is it necessarily true that $|d| \leq |a|$? Why or why not? If not, how might you slightly modify this statement to make it true?*

4. Euclidean division

A concept related to the notion of divisibility is *Euclidean division.* How does this differ from ordinary division? Euclidean division is simply the name we give to the elementary school calculation of division with remainder. For example, suppose we want to divide 13 by 5. On the one hand, the answer is 13/5, but it is also 2 with a remainder of 3, because $13 = 2(5) + 3$. The following theorem tells us that this remainder is unique.

Theorem 1 (Theorem 1.1 of text)**.** *Let a, b be integers, with $b > 0$. Then there exists a unique integer r such that $0 \leq r < b$, with*

$$a = qb + r$$

for some unique integer q. We call r the remainder *of a divided by b.*

Proof. Let's prove this theorem. First, let's show that we can find some q, r satisfying the above, and take care of the uniqueness later. Consider the set of integers $S = \{a - qb | q \in \mathbb{Z}, a - qb \geq 0\}$. This is the set of integers which differ from a by a multiple of b, and such that the difference $a - qb$ is non-negative. This set consists solely of non-negative integers, and is non-empty. To see why this is non-empty, all we need to do is choose q sufficiently negative to ensure that $a - qb > 0$. It is a fact (actually, an axiom, in the sense that we can't prove it from simpler statements) that any non-empty set of positive integers (or non-negative integers) has a least element. This is called the *well-ordering principle.* It seems obvious; however, note that this is false if we replace $\mathbb{N}$ with $\mathbb{Z}, \mathbb{Q}$, or $\mathbb{R}$. In any case, we know that S has a least element by this principle. Call this least element r. Then obviously $r = a - qb$ for some integer q. How do we know that $0 \leq r < b$? First, we know that $0 \leq r$, by the fact that $r \in S$ and S consists only of positive integers. To show that $r < b$, we will use a proof by contradiction. If $r \geq b$, then $a - (q+1)b = r - b \geq 0$. However, this means that $(r - b) \in S$, and $r - b < r$, which contradicts the fact that r is the least element in S. Therefore, we must have $r < b$.

So we've shown the existence of integers q, r such that $a = qb + r$ and $0 \leq r < b$. Now let's show that they're unique. Suppose that there are two pairs q_1, r_1, q_2, r_2 satisfying the above. Then equating the two equations, we get

$$q_1 b + r_1 = a = q_2 b + r_2.$$

This is equivalent to

$$(r_1 - r_2) = b(q_2 - q_1).$$

However, notice that because $0 \leq r_1, r_2 < b$, we must have $-b < r_1 - r_2 < b$. On the other hand, the right hand side is a multiple of b; that is, $b|(r_1 - r_2)$. But the only way this is possible (recall the question earlier in today's class!) is if $r_1 - r_2 = 0$, or $r_1 = r_2$. This immediately tells us that $q_1 = q_2$ as well. So the pair (q, r) must be unique. □

Examples.

- We saw earlier that 13 divided by 5 with remainder gives $q = 2, r = 3$.
- Let $a = -7, b = 4$. Then -7 divided by 4 with remainder gives $q = -2, r = 1$, since $-7 = (-2) * 4 + 1$. Notice that q is allowed to be negative, but the remainder never is.
- (Example 1.2 of the text) We can use division with remainder to determine all possible remainders of x^2 when divided by 4. Before working out this example, list the first few squares $(0, 1, 4, 9, \ldots)$, and find their remainders when you divide by 4.

What do you notice? Let's prove this observation. For any x, we can find q, r such that $x = 4q + r$, with $0 \leq r < 4$. Then $x^2 = (4q + r)^2 = 16q^2 + 8rq + r^2$. When we divide this by 4, notice that because $4|16q^2, 8qr$, the remainder when we divide x^2 by 4 is the same as when we divide r^2 by 4. But since $r = 0, 1, 2, 3$, we need only check that $0, 1, 4, 9$ leave remainders of $0, 1, 0, 1$, respectively. So the only possible remainders for squares when divided by 4 are 0 and 1. We'll come back to many calculations like this later in the class.