

# MATH 216 BY THE BOOK

MARK REEDER

Boston College

May 2002

## 0. BASICS

### Logical Notation —

$\exists$	there exists
$\forall$	for all
$\Rightarrow$	left side implies right side
$\Leftarrow$	right side implies left side
$\Leftrightarrow$	if and only if (each side implies the other)

**Sets** — A collection of objects is called a **set**. A set is denoted  $\{\dots\}$  with the objects inside the brackets. A set of objects with conditions is denoted  $\{\dots : \text{---}\}$ , where the  $\dots$  are the objects, and the  $\text{---}$  are the conditions. The colon is interpreted as “such that” in this notation.

For some reason, objects in a set  $S$  are not called objects, they are called **elements** of  $S$ . The notation  $a \in S$  means that  $a$  is an element of  $S$ . If  $S$  has finitely many elements, then  $|S|$  denotes the number of elements in  $S$ .

If we have two sets  $S$  and  $T$ , and every element of  $S$  is also an element of  $T$ , then  $S$  is called a **subset** of  $T$ , and we write  $S \subset T$ . Using logical notation, this is expressed as

$$S \subset T \Leftrightarrow (a \in S \Rightarrow a \in T).$$

Two sets are equal exactly when each is a subset of the other.

If  $S$  and  $T$  are two sets, their **union** is the set  $S \cup T$  consisting of element which are either in  $S$  or in  $T$ . Their **intersection** is the set  $S \cap T$  consisting of elements which are in both  $S$  and in  $T$ .

The **direct product**  $S \times T$  of two sets  $S, T$  is the set of all ordered pairs  $(s, t)$ , with  $s \in S$  and  $t \in T$ . In our set theoretic notation, this is written

$$S \times T = \{(s, t) : s \in S, t \in T\}.$$

## Various kinds of numbers —

$$\mathbb{Z} = \{0, 1, -1, 2, -2, \dots\} \quad (\text{Integers}),$$

$$\mathbb{N} = \{n \in \mathbb{Z} : n \geq 1\} = \{1, 2, 3, \dots\} \quad (\text{Natural Numbers}),$$

$$\mathbb{Q} = \left\{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \right\} \quad (\text{Rational Numbers}),$$

$$\mathbb{R} = \text{The set of all decimals.} \quad (\text{Real Numbers}),$$

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\} \quad (\text{Complex Numbers}).$$

We think of real numbers as decimals, without further comment. In general, we assume elementary school arithmetic, high school algebra and trigonometry, and basic calculus.

**Integers** — Let  $a, b \in \mathbb{Z}$ . We say that  $a$  **divides**  $b$ , and write  $a \mid b$ , if  $ak = b$  for some integer  $k$ . Any proof involving divisibility must use this definition. Here is our first proof. We will prove a Lemma, which means it is something to be proved en route to a more important result. The end of the proof will be denoted  $\square$ .

**0.1 Lemma.** *If  $a \mid b$  and  $a \mid c$ , then  $a \mid b + c$ .*

*Proof.* We write down the hypotheses. Since  $a \mid b$ , we have  $ak = b$  for some  $k \in \mathbb{Z}$ . Since  $a \mid c$ , we have  $a\ell = c$  for some  $\ell \in \mathbb{Z}$ . The conclusion of the Lemma involves  $b + c$ , so we write that down next:

$$b + c = ak + a\ell = a(k + \ell).$$

Since  $k + \ell \in \mathbb{Z}$ , we see that  $a \mid b + c$ .  $\square$

If  $a$  and  $b$  are integers,  $n$  is an integer  $> 1$ , and  $n \mid (a - b)$ , then we say

$$a \equiv b \pmod{n}.$$

This is pronounced “ $a$  is congruent to  $b$  mod  $n$ ”. To say that  $a \equiv b \pmod{n}$  is to say that  $a = b + nk$  for some integer  $k$ . That is, if we put on glasses that filter out multiples of  $n$ , then  $a$  and  $b$  look the same. In particular, to say  $a \equiv 0 \pmod{d}$  is to say that  $n \mid a$ .

For example, if  $n = 2$ , then  $a \equiv 0 \pmod{2}$  if  $a$  is even, and  $a \equiv 1 \pmod{2}$  if  $a$  is odd.

**0.2 Lemma.** *If  $a \equiv b \pmod{n}$  and  $c \equiv d \pmod{n}$  then  $a + c \equiv b + d \pmod{n}$  and  $ac \equiv bd \pmod{n}$ .*

*Proof.* The hypotheses say that  $n \mid a - b$ , and  $n \mid c - d$ . By (0.1), we have  $n \mid (a - b) + (c - d) = (a + c) - (b + d)$ . Hence  $a + c \equiv b + d$ .

For the multiplicative version, we write our hypotheses in the form  $a = b + kn$ ,  $c = d + \ell n$  for some integers  $k, \ell$ . Then

$$ac = (b + kn)(d + \ell n) = bd + n(kd + \ell b + k\ell n).$$

since  $kd + \ell b + k\ell n \in \mathbb{Z}$ , this shows that  $ac \equiv bd \pmod{n}$ .  $\square$

**Induction** — This is a very common style of proof that is used to prove a sequence of results for all integers  $n$  beyond a certain point, say  $n \geq n_0$ , for some  $n_0$ . The most obvious situation of this kind is formulas involving  $n$ , such as the following, where we explain the method of induction by example.

**0.3 Lemma.** For all  $n \geq 1$  we have

$$1 + 2 + 3 + \cdots + n = \frac{1}{2}n(n + 1).$$

*Proof.* There are two steps. The first step is to prove it in the minimal case  $n = n_0$ , where  $n_0 = 1$  here. This is always easy, but let us be careful anyway. Start with one side, say the right side (RHS), of the equation to be proved, and work on it until you arrive the other side (LHS, in this case). Usually you start with the most complicated side, because there are fewer choices for simplifying than complexifying.

$$\text{RHS} = \frac{1}{2} \cdot 1 \cdot (1 + 1) = 1 = \text{LHS}.$$

So the result is true for  $n = 1$ .

Now for the second step, *assume* the result is true for  $n - 1$ , and use this assumption to derive the formula for  $n$ . This assumption is called the **induction hypothesis**, and we will abbreviate it by IH. To write the IH, replace every occurrence of  $n$  by  $n - 1$ , and simplify if you wish. We get

$$1 + 2 + 3 + \cdots + n - 1 = \frac{1}{2}(n - 1)(n - 1 + 1) = \frac{1}{2}n(n - 1). \quad (\text{IH})$$

Now consider the formula for  $n$ . The left side seems more complicated, because of the  $\cdots$ , so we start there. We put IH under the  $=$  sign, when we use it.

$$\begin{aligned} \text{LHS} &= 1 + 2 + 3 + \cdots + n \\ &= [1 + 2 + \cdots + (n - 1)] + n \\ &= \frac{1}{2}n(n - 1) + n \quad \text{IH} \\ &= \frac{1}{2}n(n + 1) \\ &= \text{RHS} \end{aligned}$$

That completes the proof.  $\square$

By proving the minimal case  $n = n_0$ , and then proving that you can get from any case already established to the next case, you have proved the result for  $n_0 + 1$ ,  $n_0 + 2$ ,  $n_0 + 3$ , and so on, hence for all  $n \geq n_0$ .

We'll do another example. First, define the **factorial function**, for  $n \geq 1$  to be

$$n! = n(n - 1)(n - 2) \cdots 2 \cdot 1,$$

and define also

$$0! = 1.$$

Now we will use induction to prove

$$\int_0^\infty x^n e^{-x} dx = n!, \text{ for all } n \geq 0.$$

The first step is to prove it for  $n = 0$ . We start with the LHS.

$$\text{LHS} = \int_0^{\infty} x^0 e^{-x} dx = -e^{-x} \Big|_0^{\infty} = 1 = 0! = \text{RHS}.$$

Now we assume the formula for  $n - 1$ .

$$\int_0^{\infty} x^{n-1} e^{-x} dx = (n-1)! \quad (\text{IH})$$

and try to prove the formula for  $n$ . We integrate by parts.

$$\begin{aligned} \text{LHS} &= \int_0^{\infty} x^n e^{-x} dx \\ &= -x^n e^{-x} \Big|_0^{\infty} - n \int_0^{\infty} x^{n-1} (-e^{-x}) dx \\ &= n \int_0^{\infty} x^{n-1} e^{-x} dx \\ &= n \cdot (n-1)! \quad \text{IH} \\ &= n! \\ &= \text{RHS}. \end{aligned}$$

**Binomial Coefficients** — For integers  $n \geq k \geq 0$ , the binomial coefficient is defined by

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

It is pronounced “ $n$  choose  $k$ ”. When  $k > 0$ , we have some cancellations, which give the alternate expression

$$\binom{n}{k} = \frac{1}{k!} n(n-1)(n-2) \cdots (n-k+1).$$

For example,

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{2} = \frac{1}{2}n(n-1), \quad \binom{n}{3} = \frac{1}{6}n(n-1)(n-2), \dots$$

The values for  $k$  near  $n$  are found from the symmetry

$$\binom{n}{k} = \binom{n}{n-k}.$$

#### (0.4) Properties of Binomial coefficients.

(1)

$$\binom{n-1}{k-1} + \binom{n-1}{k} = \binom{n}{k}, \quad \text{for } 1 < k < n$$

(2)

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}, \quad \text{for } n \geq 0.$$

(3)  $\binom{n}{k}$  is the number of  $k$ -element subsets of an  $n$ -element set.

*Proof.* The first property is the key to everything else. It is proved directly, using the definition of  $\binom{n}{k}$ . Property (2) is proved by induction, using (1). You can prove (3) this way too, but here is a different proof, using (2) instead. Consider the product

$$(x_1 + 1)(x_2 + 1) \cdots (x_n + 1).$$

when we multiply this out, we get one term for every subset  $S \subset \{1, 2, \dots, n\}$ . The number of  $x_i$ 's in such a term is  $|S|$ . So the number of subsets with  $k$  elements is the number of terms with  $k$   $x_i$ 's. If we make each  $x_i = x$ , then each such term becomes  $x^k$ . And the product becomes  $(x + 1)^n$ . So the number of  $k$  element subsets is the coefficient of  $x^k$  in  $(x + 1)^n$ , which is  $\binom{n}{k}$ , by (2).  $\square$

Property (2) is called the **binomial expansion**, because it involves two variables  $x, y$ . Hence the term “binomial coefficients”.

**0.5 Corollary.** *The number of subsets of an  $n$ -element set is  $2^n$ .*

*Proof.* By (3), the number of subsets of an  $n$ -element set is

$$\sum_{k=0}^n \binom{n}{k}.$$

We evaluate this sum by setting  $x = y = 1$  in (2), and get  $(1 + 1)^n = 2^n$ .  $\square$