MATH 145

Jason Bell

Fall 2020

Welcome

For most of you, this will be your first experience doing rigorous proofs. It can take a bit of time before you feel comfortable writing careful mathematical arguments. The important things for you to succeed are:

- work hard;
- do lots of problems;
- do not give up.

As we look at proofs, consider the following questions.

- What is the overall strategy in the proof?
- What are the hypotheses or assumptions?
- What definitions do I need?
- Are the hypotheses needed?
- Are there counterexamples to the theorem if they are removed or relaxed?

LaTeX

One thing you'll thank me for is if you learn how to use LaTeX.

I recommend doing your assignments in LaTeX, and I will provide the .tex file for each assignment so that you can use it to make your assignments. To use LaTeX, you will need some sort of application to run it. I use TeX shop, but there are others you can use.

I’ve provided you with a sample .tex file in Learn. The basic things to know are that a .tex file has two parts: a preamble, where one puts macros and packages one will use, and a body.

A crash course on proofs

The simplest types or results we'll need to prove are statements of the form "if p then q," where p and q are themselves statements that can assume the values 'true' or 'false.' Some examples of statements of this form are:

- if Anna lives in France then Anna lives in Europe;
- if n is an even integer, then $n + 1$ is an odd integer;
- if a human is a fish then a dog is a cat;
- if I roll two dice and one die has the value six, then the total is at least seven;
- if n is even, then $n + 1$ is a multiple of three.

For a statement of the form “if p then q” to be true we require q must also be true **whenever p is true.**

If p is false then the statement *if* p *then* q is vacuously true.

We can record this in the following table:

p	q	if p then q
True	True	True
True	False	False
False	True	True
False	False	True

If Anna lives in France then Anna lives in Europe.

Since France is a part of Europe it is true that if a person lives in France then this person also lives in Europe. In this case p is the statement *Anna lives in France* and q is the statement *Anna lives in Europe*.

if n is even, then $n+1$ is odd.

To give a formal mathematical proof one must use the definitions of *even* and *odd*.

Definition. Let n be an integer. We say that n is *even* if there is an integer m such that $n = 2m$; we say that n is *odd* if there is an integer m such that $n = 2m + 1$.

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

Proof.

Suppose that n is even. Then there is some integer m such that $n = 2m$. It follows that $n + 1 = 2m + 1$, and since $n + 1$ is of the form $2m + 1$, we see that $n + 1$ is odd, by definition. $\square$

If a human is a fish then a dog is a cat.

It’s true!

If I roll two dice and one die has the value six, then the total is at least seven.

In this case, p is the statement that I roll two dice and one of the two dice has a value of six and q is the statement that the total value of the two dice is at least seven.

$$(1,6),(2,6),(3,6),(4,6),(5,6),(6,6),(6,5),(6,4),(6,3),(6,2),(6,1).$$

We see that q is true whenever p is true, by looking at all of the ways in which p can possibly be true.

A more succinct proof!

Theorem. If two dice are rolled and one of dice is a six, then the total is at least seven.

Proof.

Let a and b be the values of the two dice. Suppose that one of a or b is equal to six. We may assume without loss of generality that $a = 6$, in fact. Since a die has the values $1, 2, 3, \ldots, 6$, b must be at least one. Thus the total of the two dice is $a + b$ and $a + b = 6 + b \geq 6 + 1 = 7$. The result follows. $\square$

"if n is even, then $n + 1$ is a multiple of three."

We know this is false, but showing something is false still requires an argument.

We must show that it is possible for the statement "$n + 1$ is a multiple of three" to be false when the statement "n is even" is true.

If we have a statement P of the form "if p then q", it is also sometimes interesting to consider the statement "if q then p." This statement is called the *converse* of P. Sometimes both the statement "if p then q" and its converse are true. In this case, we write "p if and only if q" or "p iff q."

Example: "an integer n is even if and only if $n + 1$ is odd."

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

Proof.

We must show that if n is even then $n + 1$ is odd and that if $n + 1$ is odd then n is even. We proved the first direction earlier, and so it suffices to prove that if $n + 1$ is odd then n is even. So suppose that $n + 1$ is odd. By our definition, there is some integer m such that $n + 1 = 2m + 1$. It follows that $n = 2m$ and so n is even by definition. $\square$

Negation

If p and q are statements that can be either true or false, one can make statements “not p” and “not q”.

The statement “not p” is true if p is false and it is false if p is true. In other words,

“p is true if and only if not p is false”.

Sometimes one has to prove statements of the form

"if not p then not q",

"if not p then q",

"if p then not q".

Contraposition

Given a statement P: “if p then q”, we can form a statement “if not q then not p”.

This statement is called the *contrapositive* of P.

Theorem. Let p and q be true/false statements. "If p then q" is true if and only if the statement "if not q then not p" is true.

Proof.

Since this is an if and only if proof, we must prove two directions. First suppose that "if p then q" is true. Then q is true whenever p is true. It follows that if q is false then p is false. In other words, "not p" is true whenever "not q" is true and so the statement "if not q then not p is true. This completes the first direction.

For the second direction, suppose that the statement "if not q then not p" is true. Then "not p" must be true whenever "not q" is true. In other words, p is false whenever q is false. It follows that if p is true then q must be true and so q is true whenever p is true. Thus "if p then q" is true. □

Theorem. Let α be a real number. If α^2 is irrational then α is irrational.

Proof.

By taking the contrapositive, it suffices to prove that if α is rational then α^2 is rational. Suppose that α is rational. Then there are integers a, b with $b > 0$ such that $\alpha = a/b$. Then $\alpha^2 = a^2/b^2$. Since a^2 and b^2 are integers and $b^2 > 0$, we see that α^2 is rational by definition. The result follows. $\square$

Proof by contradiction

his is a very useful proof technique wherein one assumes that the statement one wants to prove is not true. One then shows that this results in a contradiction. This contradiction implies that our original assumption must be false and so the statement we want to prove must be true.

Theorem. The real number $\sqrt{2}$ is irrational.

Proof.

Suppose toward a contradiction that this statement is not true. Then $\sqrt{2}$ is rational and so we may write it as $\sqrt{2} = a/b$ with a and b positive integers sharing no common integer factor greater than 1. Then $a = \sqrt{2}b$. Squaring both sides, gives $a^2 = 2b^2$. Since the right side of this equation is even, we see a^2 is even and so a is also even. Thus we may write $a = 2m$ for some integer m. But now $a^2 = (2m)^2 = 4m^2$ and so we have $4m^2 = 2b^2$, which gives $2m^2 = b^2$. It follows that b^2 is even and so b is also even. But this gives that a and b both share the factor 2, which is a contradiction, and so we see that our assumption that $\sqrt{2}$ is rational must be false. Thus $\sqrt{2}$ is irrational. □

The Integers

We'll use the notation $\mathbb{Z}$ to denote the set of integers. This is just the collection

$$\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

The reason we use the letter 'Z' to denote this set, comes from the German word *Zahlen* for numbers.

An important subset of the integers is the subset of natural numbers

$$\mathbb{N} := \{1, 2, \ldots\}.$$

The integers is the first example we'll see of a mathematical object called a *ring*.

Binary operations

The integers have two binary operations $+$ and $\cdot$. Here, $+$ is the operation that takes as input an ordered pair of integers (m, n) and outputs $m + n$ and $\cdot$ is the operation that gives the product, $m \cdot n$, of m and n as output. We'll often omit the $\cdot$ in a product and write mn for $m \cdot n$

Both of these operations are *commutative*. So in the case of addition and multiplication, we have $m + n = n + m$ and $m \cdot n = n \cdot m$, and we see that the order of the two inputs doesn't matter when we perform the operations.

The Axioms: Addition

After playing around with the integers for a bit, you've probably discovered the following axioms.

A1: Commutativity of addition:

$$a + b = b + a$$

for all $a, b \in \mathbb{Z}$.

A2: Associativity of addition:

What is

$$2 + 3 + 6?$$

$$(a + b) + c = a + (b + c)$$

for all $a, b, c \in \mathbb{Z}$.

A3: Additive identity.

We have a special element 0:

$$a + 0 = 0 + a = a$$

for every $a \in Z$.

A4: Additive inverses

You might recall every integer a has a negative counterpart $-a$.
So for every $a \in \mathbb{Z}$ there is an integer $-a$ such that

$$a + (-a) = (-a) + a = 0$$

The Axioms: Multiplication

We also have axioms for our multiplication operation $\cdot$.

M1: Commutativity of multiplication:

$$a \cdot b = b \cdot a$$

for all $a, b \in \mathbb{Z}$.

M2: Associativity of multiplication:

What is

$$2 \cdot 3 \cdot 6?$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

for all $a, b, c \in \mathbb{Z}$.

M3: Multiplicative identity.

We have a special element 1:

$$a \cdot 1 = 1 \cdot a = a$$

for every $a \in Z$, and that's it for multiplication. But we're not done!

D1: Distributive laws

For every $a, b, c \in \mathbb{Z}$ we have

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

and

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

And now we're done!

Summary

(A1) $a + b = b + a$ for all $a, b \in \mathbb{Z}$.

(A2) $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$.

(A3) There is an element $0 \in \mathbb{Z}$ such that $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}$.

(A4) For every $a \in \mathbb{Z}$ there is an element $-a \in \mathbb{Z}$ with $a + (-a) = -a + a = 0$.

(M1) $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{Z}$.

(M2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{Z}$.

(M3) There is an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}$.

(D1) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in \mathbb{Z}$.

Last time we saw that the integers is a set $\mathbb{Z}$ with two binary operations, $+$ and $\cdot$, which have the following properties:

(A1) $a + b = b + a$ for all $a, b \in \mathbb{Z}$.

(A2) $(a + b) + c = a + (b + c)$ for all $a, b, c \in \mathbb{Z}$.

(A3) There is an element $0 \in \mathbb{Z}$ such that $a + 0 = 0 + a = a$ for all $a \in \mathbb{Z}$.

(A4) For every $a \in \mathbb{Z}$ there is an element $-a \in \mathbb{Z}$ with $a + (-a) = -a + a = 0$.

(M1) $a \cdot b = b \cdot a$ for all $a, b \in \mathbb{Z}$.

(M2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{Z}$.

(M3) There is an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}$.

(D1) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in \mathbb{Z}$.

This is saying that $\mathbb{Z}$ is a commutative ring.

A ring is a set R with two binary operations $+$ and $\cdot$ such that the following axioms:

(A1) $a + b = b + a$ for all $a, b \in R$.

(A2) $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.

(A3) There is an element $0 \in R$ such that $a + 0 = 0 + a = a$ for all $a \in R$.

(A4) For every $a \in R$ there is an element $-a \in R$ with $a + (-a) = -a + a = 0$.

(M2) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in \mathbb{Z}$.

(M3) There is an element 1 such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$.

(D1) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

If, in addition, $a \cdot b = b \cdot a$ for all $a, b \in R$ then R is a *commutative* ring.

You have encountered several examples of commutative rings already in addition to the integers. Examples:

- $\mathbb{R}$ has binary operations $+$ and $\cdot$ and elements 0 and 1.
- $\mathbb{Q}$, the set of rational numbers, is also a commutative ring.
- The complex numbers.

A new example

Let

$$R := \mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} \colon a, b \in \mathbb{Z}\}.$$

Then R is a subset of the real numbers and observe that ordinary addition and multiplication in $\mathbb{R}$ give us addition and multiplication in R as follows:

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2}$$

and

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (cd + ad)\sqrt{2}$$

for $a, b, c, d \in \mathbb{Z}$. Then R is a commutative ring.

This observation gives us an important way of constructing new rings from a given one.

Proposition. Let R be a ring with binary operations $+$ and $\cdot$, and suppose that $S \subseteq R$ is a subset with the following properties:

(i) $0, 1, -1 \in S$;

(ii) if $a, b \in S$ then $a + b \in S$;

(iii) if $a, b \in S$ then $a \cdot b \in S$.

Then S is also a ring.

This is saying $S \subseteq R$ is *closed* under addition and multiplication.

Before we do the proof, notice that $-s = (-1) \cdot s \in S$ for $s \in S$. (Exercise!)

Proof.

Notice (ii) and (iii) give that addition and multiplication restrict to binary operations on S. Then since $0 \in S$ and (A1)–(A3) hold inside R, they must also hold in S since $-1 \in S$, by the above, we have $-s \in S$. Similarly, since $1 \in S$, (M1) and (M3) hold in S. Finally (D1) holds for S for the same reason. Thus S is a ring. □

Notice that if (M2) holds in R then it also holds in S, so if R is a commutative ring, and (i)—(iii) hold for S, then S is also a commutative ring.

A noncommutative ring

Let

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

Then we have binary operations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Units

Definition. Let R be a ring. We call an element a of R a *unit* if there is an element $b \in R$ such that $a \cdot b = b \cdot a = 1$. We call b the *multiplicative inverse* of a.

Example. The element $\sqrt{2} - 1$ is a unit of R, as $(\sqrt{2} - 1)(\sqrt{2} + 1) = 2 - 1 = 1$.

Show that if u and v are units in a ring R then so is $u \cdot v$. Show that if u is a unit then so is its multiplicative inverse.

Zero divisors

In a commutative ring R an element $a \in R$ is called a *zero divisor* if there is some $b \neq 0$ such that $a \cdot b = 0$.

Notice that in some commutative rings the only zero divisors are 0. These rings are called *integral domains*:
$a \cdot b = 0 \implies a = 0$ or $b = 0$.

Example

Let $R = \{(a, b) : a, b \in \mathbb{Z}\} = \mathbb{Z} \times \mathbb{Z}$. Then R has binary operations $+$ and $\cdot$ given by $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \cdot (c, d) = (a \cdot c, b \cdot d)$, where we use ordinary addition and multiplication in $\mathbb{Z}$ to compute sums and products inside the coordinates. Show that R is a commutative ring. What are the units of R? What are the zero divisors of R?

Order and Induction

These are really the key properties of the integers, but there's one other fact that is often useful: the integers are *ordered*. Notice we have a total ordering $\leq$ on the integers, which is expressed via the inequalities

$$\cdots < -2 < -1 < 0 < 1 < 2 < \cdots .$$

If $a \not\geq b$ then $a < b$. The important properties of this order are:

- if $a > b$ then $a + c > b + c$ for each integer c;
- if $a > b$ and $a \cdot c > b \cdot c$ when $c > 0$ and $a \cdot c < b \cdot c$ when $c < 0$.

The well-ordering axiom

We have the following equivalent forms:

- Every non-empty subset of $\mathbb{N}$ has a smallest element;
- There does not exist a strictly decreasing infinite chain of natural numbers

$$n_1 > n_2 > n_3 > \cdots .$$

The principle of mathematical induction

Theorem (The Principle of Mathematical Induction) Suppose we have true/false statements $P(0), P(1), P(2), \ldots, P(n), \ldots$ for each natural number and suppose that the following hold:

1. (base case) $P(0)$ is true;
2. (induction step) if $P(m)$ is true then $P(m+1)$ is true for $m \in \mathbb{N}$.

Then $P(n)$ is true for every $n \in \mathbb{N}$.

We'll see how we can prove this using the well-ordering axiom.

Proof of the principle of induction

Proof.

1. Suppose there is some n such that $P(n)$ is not true. (Argument by contradiction)
2. Let S denote the collection of $n \in N$ for which $P(n)$ is false.
3. Then S is a non-empty subset of $\mathbb{N}$ and so there is some smallest element $n_0 \in \mathbb{N}$. (well-ordering axiom)
4. Since $P(0)$ is true, $0 \notin S$ and so $n_0 \geq 1$.
5. Then $n_0 - 1 \in \mathbb{N}$ and by minimality of n_0 we see that $n_0 - 1 \notin S$.
6. So $P(n_0 - 1)$ is true. But since $P(n_0 - 1)$ is true, we also have $P(n_0 - 1 + 1) = P(n_0)$ is true, contradicting the fact that $n_0 \in S$.

□

Important variations

Sometimes instead of showing if $P(m)$ is true then $P(m+1)$ is true, we show that if $P(i)$ is true for $i = 0, 1, \ldots, m$ then $P(m+1)$ is true. This is strong induction.

Sometimes we might want to have a base case that is larger than zero.

Sometimes we might need more than one base case.

$1 + 2 + \cdots + n = n(n+1)/2$ for $n \geq 1$

Our base case is $n = 1$. Here the left side is 1 and the right side is $1 \cdot 2/2 = 1$, so the case when $n = 1$ is OK.

For the induction step, we assume that $1 + 2 + \cdots + m = m(m+1)/2$ where $m \geq 1$ (induction hypothesis). We'll consider the case when $n = m + 1$ on the next slide.

Assumption: $1 + 2 + \cdots + m = m(m+1)/2$

Our goal is to show that $1 + 2 + \cdots + m + (m+1) = (m+1)(m+2)/2$. (When $n = m + 1$, $n(n+1)/2 = (m+1)(m+2)/2$.)

Notice that the left side is

$$1 + 2 + \cdots + m + (m+1) = m(m+1)/2 + (m+1)$$

by the induction hypothesis. But let's simplify $m(m+1)/2 + (m+1)$. This is equal to

$$(m+1)(m/2+1) = (m+1)(m+2)/2.$$

Thus we see that if $P(n)$ is the statement $1 + 2 + \cdots + n = n(n+1)/2$ then $P(1)$ is true and if $P(m)$ is true then $P(m+1)$ is true, and so the principle of mathematical induction gives the result.

The Fibonacci numbers

Let $f_0 = 0$, $f_1 = 1$, and $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$. Show that

$$f_n = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

We'll use the fact that $(1 \pm \sqrt{5})/2$ are the two roots of $x^2 - x - 1 = 0$ so $x^2 = x + 1$ for these numbers.

This one we actually need two base cases $n = 0$ and $n = 1$.

When $n = 0$, the left side and right side are both zero. When $n = 1$, the left side is 1 and the right side is

$$(1/\sqrt{5}) \cdot \sqrt{5} = 1.$$

Induction hypothesis: suppose that $m \geq 2$ and that the claim is true for all $i < m$. We'll show the claim for $n = m$.

Goal: To show

$$f_m = \frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^m - \left(\frac{1-\sqrt{5}}{2} \right)^m \right).$$

Since $m \geq 2$, the left side is

$$f_m = f_{m-1} + f_{m-2}.$$

We can then use the induction hypothesis and write this as

$$\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{m-1} - \left(\frac{1-\sqrt{5}}{2} \right)^{m-1} \right)$$

$$+\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{m-2} - \left(\frac{1-\sqrt{5}}{2} \right)^{m-2} \right).$$

$$\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{m-1} - \left(\frac{1-\sqrt{5}}{2} \right)^{m-1} \right)$$

$$+\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{m-2} - \left(\frac{1-\sqrt{5}}{2} \right)^{m-2} \right)$$

is equal to

$$\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2} \right)^{m-1} + \left(\frac{1+\sqrt{5}}{2} \right)^{m-2} \right)$$

$$-\frac{1}{\sqrt{5}} \cdot \left(\left(\frac{1-\sqrt{5}}{2} \right)^{m-1} + \left(\frac{1-\sqrt{5}}{2} \right)^{m-2} \right) .$$

We'll rewrite this as

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^{m-2}}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2}\right)+1\right)$$

$$-\frac{\left(\frac{1-\sqrt{5}}{2}\right)^{m-2}}{\sqrt{5}} \cdot \left(\left(\frac{1-\sqrt{5}}{2}\right)+1\right)$$

Now we recall that this is just

$$\frac{\left(\frac{1+\sqrt{5}}{2}\right)^{m-2}}{\sqrt{5}} \cdot \left(\left(\frac{1+\sqrt{5}}{2}\right)^{2}\right)$$

$$-\frac{\left(\frac{1-\sqrt{5}}{2}\right)^{m-2}}{\sqrt{5}} \cdot \left(\left(\frac{1-\sqrt{5}}{2}\right)^{2}\right).$$

Simplifying gives the result.

Let $n \geq 1$, In every group of n people, all people in the group have the same hair colour.

"Proof". Base case: $n = 1$. Immediate.

Suppose it's true for every group of size $< m$ with $m \geq 2$ and consider a group of m people. Then by the induction hypothesis, the first $m - 1$ people have the same hair colour and the last $m - 1$ people have the same hair colour. Since every person is in one of these two groups, they all have the same hair colour.

What's wrong with this?

Binomial coefficients and the Binomial Theorem

We recall that for a nonnegative integer n, $n!$ is defined to be the product of the positive integers from 1 to n; that is,

$$n! = 1 \cdot 2 \cdot 3 \cdots n. \tag{1}$$

We take

$$0! = 1, \tag{2}$$

which is justified by the general idea that an empty product should be equal to one, while an empty sum should be equal to zero.

We define

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{3}$$

for nonnegative integers n and k with $n \geq k$. We define $\binom{n}{k}$ to be zero when $k > n$, so, for example,

$$\binom{0}{3} = \binom{2}{5} = 0.$$

We read $\binom{n}{k}$ as "n choose k."

The reason we say "n choose k" comes from the following result.

theorem Let n and k be nonnegative integers. Then $\binom{n}{k}$ is the equal to the number of k-element subsets of a set of size n.

E.g., $\{a, b, c, d\}$ pick two different elements where the order doesn't matter

$$ab, ac, ad$$

$$ba, bc, bd$$

$$ca, cb, cd$$

$$da, db, dc$$

Proof.

It is enough to prove the result for k-element subsets of the set $S = \{1, 2, \ldots, n\}$. If $k > n$ then there are no k-element subsets of S. If $k = 0$, there is precisely one k-element subset of S, namely the empty set, so the result holds when $k = 0$. Now let's look at selecting a k-elements of S, where we care about the order. So for example, if we were picking three elements from the set $\{1, 2, 3, 4, 5\}$ we would count $2, 3, 5$ as being different from $3, 5, 2$, because although the elements we select are the same, we selected them in different orders.

We have n choices for the first element; having selected this element, we have $n-1$ elements left to choose from, so we have $n-1$ choices for the second element. In general, we have $n-i+1$ possible choices for the i-th element for $i = 1, 2, \ldots, k$. This shows that we have $n(n-1)(n-2)\cdots(n-k+1)$ ways of selecting k-elements from S if we care about the order. Notice that for each set of k elements, there are $k!$ ways of ordering them and so each k-element subset of S gives rise to exactly $k!$ ways of selecting those k elements in some order. We thus see that the number of k-element subsets of S is equal to

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

The result follows.

Corollary.

Let n and k be nonnegative integers. Then $\binom{n}{k}$ is an integer.

Let $m, j \geq 1$. Then

$$\binom{m}{j-1} + \binom{m}{j} = \binom{m+1}{j}.$$

Combinatorial proof. Think of picking a j-element subset of $\{1, 2, \ldots, m+1\}$. Let A be all such subsets which don't contain $m+1$ and let B be all such subsets which do contain $m+1$. Then $|A| = \binom{m}{j}$ and $|B| = \binom{m}{j-1}$. And $A \cup B$ is all sets so $|A| + |B| = \binom{m+1}{j}$.

Computational proof

$$\binom{m}{j-1} + \binom{m}{j} = m!/(j-1)!(m-j+1)! + m!/j!(m-j)!.$$

Factor out $m!/(j-1)!(m-j)!$ from the right side:

$$m!/(j-1)!(m-j)!\,(1/(m-j+1) + 1/j)$$

$$= m!/(j-1)!(m-j)!\,((m+1)/j(m-j+1))\,.$$

Now simplify!

The binomial theorem

Now we come to one of the more important results of the course.

Theorem. Let R be a commutative ring and let x and y be elements of R. Then for $n \in \mathbb{N}$ we have

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}.$$

E.g.,

$$(x+y)^3 = \binom{3}{0} x^3 y^0 + \binom{3}{1} x^2 y^1 + \binom{3}{2} x^1 y^2 + \binom{3}{3} x^0 y^3.$$

Proof by induction on n.

We first establish the base case. When $n = 1$, the left side is $(x + y)^1 = x + y$, while the right side is

$$\binom{1}{0} x^0 y^1 + \binom{1}{1} x^1 y^0 = y + x$$

and so the two sides agree.

Next we have an induction hypothesis. So suppose that the result holds when $n = m$, where m is a positive integer. We'll show that it then holds when $n = m + 1$.

$$
\begin{aligned}
(x+y)^{m+1} &= (x+y)\cdot(x+y)^m \\
&= (x+y)\left(\sum_{i=0}^{m}\binom{m}{i}x^i y^{m-i}\right) \\
&= \sum_{i=0}^{m}\binom{m}{i}x^{i+1}y^{m-i} + \sum_{i=0}^{m}\binom{m}{i}x^i y^{m-i+1} \\
&= \sum_{j=1}^{m+1}\binom{m}{j-1}x^j y^{m+1-j} + \sum_{i=0}^{m}\binom{m}{i}x^i y^{m-i+1} \\
&= \binom{m}{0}y^{m+1} + \left(\sum_{j=1}^{m}\left(\binom{m}{j-1}+\binom{m}{j}\right)x^j y^{m+1-j}\right) \\
&+ \binom{m}{m}x^{m+1} \\
&= y^{m+1} + \sum_{j=1}^{m}\binom{m+1}{j}x^j y^{m+1-j} + x^{m+1}
\end{aligned}
$$

Thus we've shown that if the result holds when $n = m + 1$ under the assumption that it holds when $n = m$. It follows by the Principle of Mathematical Induction that the result holds for all $n \geq 1$.

After you were first introduced to multiplication for integers, you're were soon introduced to the related concept of *division*. Since $6 \cdot 2 = 12$, we can also say that $12/6 = 2$ (read as "12 divided by 6 is equal to 2"). One way, of saying this is that 12 is a multiple of 6 or, equivalently, that 6 is a *divisor* of 12. We'll explore the divisors of integers a bit more in this section. Let's recall that one of the key differences between the operations $+$ and $\cdot$ on the integers is that every integer has an additive inverse, while most integers do not have a multiplicative inverse.

When one talks about division, one always makes implicit assumptions about where the division is being performed. For example, 5 is not a divisor of 9 in the integers, but it is a divisor if we work in the rational numbers, since there we have $9 = 5 \cdot (9/5)$.

Every number has itself as a divisor; it also has the units 1 and -1 as divisor, but some numbers have more divisors. A number $n \in \mathbb{Z}$ is *composite* if we can write $n = a \cdot b$ where neither a nor b is equal to 1 or -1. A number that is not composite and that is not a unit is called *prime*. Under this definition, numbers like $2, 3, 5, \ldots$ are prime, but so are numbers like $-2, -3, -5, \ldots$. Often one only worries about the positive integers when one speaks of primes.

Euclid's famous proof

Let's show there are infinitely many prime numbers. **Theorem.** There are infinitely many prime numbers.

Proof.

Suppose that this is not true. Then there are only finitely many primes, $p_1, \ldots, p_n$. Let $N = p_1 \cdots p_n + 1$. Observe that N is not divisible by any of the primes $p_1, \ldots, p_n$.

Then either N is a new prime not in the set $\{p_1, \ldots, p_n\}$ or N has a smaller prime factor that is not one of $p_1, \ldots, p_n$. In either case we obtain a contradiction and so we conclude there are infinitely many primes. $\square$

Given two numbers m and n, we can talk about common divisors. A number d is a common divisor of m and n if $d|m$ and $d|n$.

Notice that if we let S denote the set of all common divisors of m and n, then it has a unique largest element. We call this the *greatest common divisor* of m and n and write $\gcd(m, n)$.

E.g., $\gcd(6, 15) = 3$, $\gcd(2, 7) = 1$.

The Euclidean Algorithm

The Euclidean algorithm goes back over 2000 years. It's an algorithm that takes a pair of positive integers (m, n) as input and outputs the biggest positive integer d that divides both m and n. This number d is called the *greatest common divisor* of m and n and we write $d = \gcd(m, n)$. For example, the greatest common divisor of 35 and 15 is 5 and $\gcd(12, 17) = 1$. To employ the Euclidean algorithm, we must make use of the related division algorithm. This is something most of us learn before we are twelve, although we don't usually give it such a fancy name at that time.

The division algorithm

Let m and n be positive integers with $m < n$. Then there exists a unique positive integer q and a nonnegative integer $r \in \{0, 1, \ldots, m-1\}$ such that

$$n = qm + r.$$

Intuitively, we can m divides into n q times and the remainder is r. The remainder is always nonnegative and strictly smaller than the number we are dividing by.

Proof.

Let X denote the set of positive integers j such that $m \cdot j \leq n$. Observe that X is non-empty since $1 \in X$. Also X is bounded above, because if $k > n$ then $m \cdot k \geq k > n$ and thus all elements of X are less than or equal to n. It follows that X has some largest element and we let q denote this largest element. In particular, $q + 1$ is not in X and so we have $(q + 1) \cdot m > n$. We now let $r = n - q \cdot m$. Then since $q \in X$, we see that $r \geq 0$. On the other hand, $(q + 1) \cdot m > n$ and so $m > n - q \cdot m = r$. This gives the desired inequality. $\square$

The reason this is typically called an algorithm rather than a theorem is that there is in fact an algorithm for producing the integers q and r when dividing n by m. I'll assume you learned stuff like

There's a more naive algorithm too: We begin with n and repeatedly subtract m, keeping track of the total number of times we subtract; there is then some last point where the result of the subtraction remains nonnegative—this value is r, and q is the number of times we subtracted m from n.

We'll give an extended version of this algorithm.

Input: Positive integers m and n with $m < n$.

Output: The greatest common divisor d of m and n and integers a and b such that $d = a \cdot n + b \cdot m$. Let's describe the algorithm. We'll then give some examples and show that the algorithm always eventually terminates and does what is claimed.

The steps

Step 1. Let $r_0 = n$, $a_0 = 1$, and $b_0 = 0$. Similarly, we let $r_1 = m$, $a_1 = 0$, and $b_1 = 1$. Notice that $r_j = a_j \cdot n + b_j \cdot m$ for $j = 1, 2$. Let $v_0 = (r_0, a_0, b_0)$ and let $v_1 = (r_1, a_1, b_1)$. Let $i = 1$ and go to Step 2.

Step 2. Apply the division algorithm to r_i and r_{i-1} to find a positive integer q_{i+1} and an integer $r_{i+1} \in \{0, 1, \ldots, r_i - 1\}$ such that $r_{i-1} = q_{i+1} \cdot r_i + r_{i+1}$. We let $a_{i+1} = a_{i-1} - q_{i+1} \cdot a_i$ and $b_{i+1} = b_{i-1} - q_{i+1} \cdot b_i$ and let $v_{i+1} = (r_{i+1}, a_{i+1}, b_{i+1})$. If r_{i+1} is equal to zero then go to Step 4; otherwise, we increment i by one and return to Step 2.

Step 3. We return the integers $d = r_i$, $a = a_i$, and $b = b_i$ as output. Then d is the greatest common divisor of m and n and $d = a \cdot n + b \cdot m$. The algorithm terminates.

Theorem. The extended Euclidean algorithm terminates and produces and the output d, a, b satisfy $d = an + bm$.

To do this proof, we must carefully analyze the algorithm. We first claim that for each applicable integer $j \geq 0$, we have $r_j = a_j \cdot n + b_j \cdot m$. We'll prove this by induction on j. When $j = 0$ and $j = 1$, this is shown in Step 1 of the algorithm, and so we have proven the base cases. Suppose now that the claim holds whenever $j \leq i$ with $i \geq 1$ and consider the case when $j = i + 1$. If $r_i = 0$, then the algorithm terminates and we do not produce r_{i+1}. Thus we may assume that $r_i > 0$. Then there is an integer q_{i+1} such that

$$r_{i-1} = q_{i+1} \cdot r_i + r_{i+1},$$

and $0 \leq r_{i+1} < r_i$. We also have $a_{i+1} = a_{i-1} - q_{i+1} \cdot a_i$ and $b_{i+1} = b_{i-1} - q_{i+1} \cdot b_i$.

Then

$$\begin{aligned} a_{i+1} \cdot n + b_{i+1} \cdot m &= (a_{i-1} - q_{i+1} \cdot a_i) \cdot n + (b_{i-1} - q_{i+1} \cdot b_i) \cdot m \\ &= (a_{i-1} \cdot n + b_{i-1} \cdot m) - q_{i+1} \cdot (a_i \cdot n + b_i \cdot m) \\ &= r_{i-1} - q_{i+1} r_i \\ &= r_{i+1}. \end{aligned}$$

It follows by induction that $r_j = a_j \cdot n + b_j \cdot m$ for each applicable nonnegative integer j.

Termination

Next let's show explain why the algorithm terminates. The algorithm terminates as soon as $r_{i+1} = 0$. Notice that the algorithm produces nonnegative integers $r_0, r_1, r_2, \ldots$ and by the construction in the algorithm we have the inequalities $r_0 > r_1 > r_2 > \cdots$. By the well-ordering principle we cannot have an infinite strictly descending chain of elements in $\mathbb{N}$ and so we see that the chain must terminate at some point and so there is some $i + 1$ such that $r_{i+1} = 0$.

Producing the gcd

The only thing that remains to show is that if $r_{i+1} = 0$ then $d := r_i$ is the greatest common divisor of m and n. Suppose first that ℓ divides both m and n. Then ℓ divides $a_i \cdot n + b_i \cdot m = d$ and so ℓ divides d. Thus every positive integer that divides both m and n necessarily divides d and so to show that d is the greatest common divisor of m and n, it suffices to show that d divides them both.

We do this by induction. Notice that $r_{j-1} = q_{j+1} \cdot r_j + r_{j+1}$, and so if r_i divides r_{j+1} and r_j then it divides r_{j-1}. In particular, d divides $r_0 = n$ and $r_1 = m$ and so it divides the both. This completes the proof.

Theorem. Let p be a prime number, and let a and b be integers. If $p|ab$ then either $p|a$ or $p|b$.

Proof.

Notice p divides an integer n if and only if it divides $-n$; moreover, the result holds if either a or b is equal to zero. Thus we may assume without loss of generality that a and b are nonzero and we may replace a by $-a$ if necessary and b by $-b$ if necessary and we may further assume that a and b are positive. If p doesn't divide a then since the only divisors of p are 1 and p, $\gcd(p, a) = 1$ and so there are integers c and d such that $1 = c \cdot p + d \cdot a$. Hence

$$b = (b \cdot c) \cdot p + d \cdot (a \cdot b).$$

Since p divides both $a \cdot b$ and p, we see it divides $(b \cdot c) \cdot p + d \cdot (a \cdot b)$, and so it divides b. The result follows. □

More general version (prove by induction):

If $p|a_1 \cdots a_m$ then $p|a_i$ for some i.

Given a finite collection of positive integers $n_1, n_2, \ldots, n_s$, it still makes sense to talk about the greatest common divisor of these numbers. This is the unique positive integer d with the property that d divides each of $n_1, \ldots, n_s$ and such that there is no larger positive integer with this property. As before, we write $d = \gcd(n_1, \ldots, n_s)$ to express the fact that d is the greatest common divisor of $n_1, \ldots, n_s$.

Theorem.

Let $s \geq 2$ and let $n_1, \ldots, n_s$ be positive integers. Then there exist integers $a_1, \ldots, a_s$ such that

$$\gcd(n_1, \ldots, n_s) = a_1 \cdot n_1 + \cdots + a_s \cdot n_s.$$

Proof

We prove this by induction on s. When $s = 2$, this follows from the Extended Euclidean Algorithm. Suppose next that the result holds when $s \leq k$ with $k \geq 2$ and consider the case when $s = k + 1$. We let $d' = \gcd(n_1, \ldots, n_k)$. Then by the induction hypothesis there are integers $b_1, \ldots, b_k$ such that

$$d' = b_1 n_1 + \cdots + b_k n_k.$$

We claim that $d = \gcd(d', n_{k+1})$. Once we have the claim, observe that we are done as the Extended Euclidean Algorithm guarantees the existence of integers a and b such that

$$d = ad' + bn_{k+1}.$$

So we have

$$d = (ab_1)n_1 + \cdots + (ab_k)n_k + bn_{k+1},$$

giving the desired result. Thus it suffices to show that $d = \gcd(d', n_{k+1})$. Notice that $\gcd(d', n_{k+1})$ divides both d' and n_{k+1} and since d' divides each of $n_1, \ldots, n_k$ we then have $d = \gcd(d', n_{k+1})$ divides each of $n_1, \ldots, n_{k+1}$. On the other hand, if e divides all of $n_1, \ldots, n_{k+1}$ then it divides

$$d = ad' + bn_{k+1}.$$

So d is the gcd of $n_1, \ldots, n_{k+1}$.

Unique factorization

Theorem Let n be a positive integer. Then n has at least one factorization into primes.

Proof.

Suppose that this is not the case. Then let S denote the collection of positive integers which cannot be written as a (possibly empty) finite product of prime numbers. Then by assumption S is non-empty and hence S has some smallest element n_0. Notice that $n_0 \neq 1$ since 1 is by convention an empty product of prime numbers. If n_0 is prime then n_0 is a product of one prime, namely itself. Thus we may assume that $n_0 > 1$ and that n_0 is not prime. Thus n_0 is composite and so $n_0 = ab$ with $a, b > 1$ and $a, b < n_0$. □

Now we'll see that every positive integer factors *uniquely* into primes. That means that if $n = p_1 \cdots p_s = q_1 \cdots q_t$ are two factorizations of n into (not necessarily distinct) primes then $s = t$ and the p_i are a permutation of the q_j.

This is not easy!