NOTES FOR PROOF TEXTBOOK

1 Chapter 1 **2**

1.1 Notes . . . 2

1.2 Excercises . . . 2

2 Chapter 2 **6**

2.1 Notes . . . 6

2.1.1 The structure of direct proofs . . . 9

2.1.2 Divisibility . . . 10

2.1.3 Greatest Common Divisors . . . 11

2.2 Main Exercises . . . 17

3 Chapter 3: Sets **24**

3.1 Notes . . . 24

3.1.1 Proving $A \subseteq B$ . . . 26

3.1.2 Set Operations . . . 28

3.1.3 Power Sets and Cardinality . . . 29

3.2 Main Exercises . . . 31

4 Chapter 4 : Induction **37**

4.1 Notes . . . 37

4.1.1 General Inductive Proofs . . . 38

4.1.2 Strong Induction . . . 42

5 5 **45**

CHAPTER 1

CHAPTER 1

Here is the general link to all the solutions

1.1 Notes

Definition of Relatively Prime numbers

Two integers m and n are said to be relatively prime if there is no integrer larger than 1 which divides both m and n.

1.2 Excercises

Exercise 1.4

Suppose that there are m and n are positive odd integers.

a.) Does there exist a perfect cover of the $m \times n$ chessboard?

b.) If I remove 1 square from the $m \times n$ chessboard, will it have a perfect cover?

1.4a)

If there are an odd number of squares, there will be a parity :

Looking at a simple case of a 3×3 chess board

In this case, there are 4 black squares and 5 white squares. We know that a piece can "cover" 1 White and 1 Black square. This is because all squares are surrounded orthagonally by squares of the opposite color. Therefore it would be impossible for 1×2 rectanges to perfectly cover these types of chessboards. □

1.4b)

If you remove one of the squares, there is no longer a parity of 1. This means that it would now be possible to create a perfect solution. Since each of the rectangles is able to erase 2 squares of different colors, the new even count of colored squares would allow for full coverage.

Excercise 1.5

If I remove two squares of different colors from an 8×8 chessboard, must the result have a perfect cover?

Yes, since there is an even number of squares belonging to each color, you would be able to cover every square using the 1×2 rectangles.

Excercise 1.6

If I remove four squares - two black, two white - from an 8×8 chessboard, must the result have a perfect cover?

I believe that in this case there will still always be a possible covering arrangement of the squares on the board. This is largely because of the continued even-ness of the number of colored squares. Since we have proved above that perfect coverings exist in the case there is an even number of squares of each color, this would still apply her

Excercise 1.7

The game tetris is played with five different shapes formed by 4 unit squares.
a.) Is it possible to perfectly cover a 4×5 chessboard using each of these shapes exactly once? Prove either case.
b.) Is it possible to perfectly cover an 8×5 chessboard using each of these shapes exactly twice? Prove either case.

1.7a)

The first thing I'll try is counting the number of squares, since the chessboard is 20 squares and the 5 shapes each consisting of 4 unit squares has a total size of 20 squares means this is alright and the sizes match.

Since that didn't prove anything, I'll now try an approach revolving around the even - odd parity of the chessboard. Looking at a chessboard of this size I'll look for a pattern in smaller chessboards.

So this is just a smaller version of the proposed 4×5 chessboard, you can see that the pattern where when dealing with odd rows, there are an uneven number of colored squares.

But when there are an even number of rows, there is an even total number of squares of each color. This means that the 4×5 chessboard will have an even number of squares of each color. So we now can make sure that the net of the 5 pieces will cover a net neutral of squares.

The I piece will cover an even number of squares

The Square piece will cover an even number of squares

The L piece will cover an even number of colored squares

The offset square will cover an even number of each color

The "branch" piece will over an uneven number of colors of square.

Because there is an uneven number of net squares being covered, no this arrangement is not possible largely because of the "branch" (or middle most) piece covering one square of 1 color, then 3 squares of the other color. So there is no arrangement that is possible in this case.

□

1.7b)

Now we can pretty much do the same thing as before, since the arragnement of squares has not changed in evenness, there hasn't been any introduced parity, atleast in the chessboard.

Now in terms of the pieces, we can do the same thing as with part a.)

Because we know that an even times an even will create an even, the first 4 pieces will not have a change in parity. However, there will be a change in parity with the middle most "Branch" piece.

Since the "branch" piece covers 1 square of 1 color and then 3 of the other, you could arrange the 2 branch pieces to be "centerd" on different colors. Therefore, they would have a net neutral in terms of covering colored pieces. So we can conclude that the parity from earlier has been solved.

We can say that for the case of the 8×5 chessboard with 2 pieces each, this is entirely possible.

□

Excercise 1.8

Prove that if one chooses $n + 1$ numbers from $\{1, 2, 3, \ldots, 2n\}$ it is guaranteed that two of the numbers they choose are consecutive.

If you are to select $n + 1$ numbers from the set, you would have to pick atleast one set of consecutive numbers. This problem can be easily viewed as a pigeonhole issue with even and odd numbers. Because of the pattern of even and odd numbers, one can say that an even and odd number will always be consecutive. Because there will be $2n$ total numbers, that means there will be at most n odd or even numbers (depending on evenness of the first element). Because you have to select $n + 1$ numbers though, you will be forced to have atleast 1 even number and atleast 1 odd number. Meaning that there must be atleast one consecutive pair of numbers.

Excercise 1.10

Assume that n is a positive integer. Prove that if one selects any $n + 1$ numbers from the set $\{1, 2, 3, \ldots, 2n\}$, then two of the selected numbers will sum to $2n + 1$.

This is another example of a problem approachable with the pigeonhole principle. Consecutive numbers can be written $\{n, n+1\}$ this is quite intuitive. The sum of these numbers will be $n+n+1 = 2n+1$. So this problem is essentially just stating that if you select $n+1$ numbers from a set of $2n$ numbers, then two will be consecutive. Which is what we proved in 1.8.

□

Since relatively prime essentially means that the two numbers don't share any factors other than 1, two even numbers cannot be coprime. This is because by being even, they are by definition evenly divisble by 2. This means that the numbers chosen from the set have to be odd, with the inclusion of at most one even number if relatively prime numbers are intended to be chosen. Given that our set ranges from 1 to 60, that means that there are * * * * * * * * * *

CHAPTER 2

CHAPTER 2

2.1 Notes

Fact 2.1

The sum of integers is an integer, the different of integers is an integerr,and the product of integers is an integer.

This leads us to the conclusion that

Definiton of even and odd

An integer n is even if $n = 2k$ for some integer k
An integer n is odd if $n = 2k + 1$ for some integer k

For example

$$6 = 2 \cdot 3 \rightarrow n = 2k, n = 6, k = 3$$

$$9 = 2 \cdot 4 + 1 \rightarrow n = 2k + 1, n = 9, k = 2$$

$$0 = 2 \cdot 0 \rightarrow n = 2k, n = 0, k = 0$$

$$-15 = 2 \cdot (-8) + 1, n = 2k + 1, n = -15, k = 0$$

Worked Proof

Prove that the sum of two even integers is even.

Ths is quite easily proved.

We can say that integers n_1, n_2 are both even. This means they can both be represented as :

$$n_1 = 2k_1 || n_2 = 2k_2$$

This means that the sum can be written as

$$n_1 + n_2 = 2k_1 + 2k_2 \rightarrow 2(k_1 + k_2)$$

And we know from the defintion of even numbers :

$$n_{\text{sum}} = 2 \cdot (k_1 + k_2)$$

So n_{sum} has to be even.

□

Worked Proof Again

Prove that the sum of two odd integers is even.

Let n and m be two arbitrary odd integers.

This means we can represent the integers as

$$n = 2k_1 + 1 || m = 2k_2 + 1$$

We can then sum the integers :

$$n + m = 2k_1 + 1 + 2k_2 + 1 = 2 + 2k_1 + 2k_2$$

This simplies to :

$$2(1 + k_1 + k_2) = n_{\text{sum}}$$

Substituting : $a = 1 + k_1 + k_2$

$$n_{\text{sum}} = 2(a)$$

This is the form of an even number. Therefore, this means that the sum of two odd numbers is even.

□

Worked Proof Again Again

Prove that if n is an odd integer, then n^2 is an odd integer.

We know that we can represent an odd integer as :

$$n = 2k + 1$$

So we can square this algebraic form :

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1$$

We can factor this :

$$n^2 = 2(2k^2 + 2k) + 1$$

Which easily follows the form of an odd number.

□

So generally when writing proofs, if then is a very useful thing to use. You can say that if something is true, then something else also MUST be true. It is also represnted symbolically by $\implies$. It can also be called implies.

If you live in LA then you live in California.
You live in LA $\implies$ you live in California.
For math we can say
m and n being even implies $m + n$ is even
m and n are both even $\implies$ $m + n$ is even
So the general form :

$$P \implies Q$$

Where P and Q are both statements.

2.1.1 The structure of direct proofs

A direct proof involves starting at a proposition $P \implies Q$ by starting at P and working towards Q

So this style of proof will generally follow the form :

Proposition. $P \implies Q$
Proof. Assume P.

$\ll$ An explanation of P. $\gg$
$\vdots$ apply algebra,
$\vdots$ logic, techs
Now we can see what Q means.

Proposition

If n is an integer, then $n^2 + n + 6$ is even.

There are two possible cases, the case where n is even and the case where n is odd. Because all integers are either even or odd.

We will consider the two cases :

Case 1: n is even

This means that $n = 2a$ for some integer a.

Substituting this into the main term, $n^2 + n + 6$ gives us :

$$(2a)^2 + 2a + 6 \implies 4a^2 + 2a + 6$$

We can then use algebraic manipulation :

$$4a^2 + 2a + 6 \implies 2(2a^2 + a + 3)$$

Since we know that $2a^2 + a + 3$ is an integer by the closedness of integers under addition, we can conclude that $n^2 + n + 6 = 2k$ where $k = 2a^2 + a + 3$.

Case 2: n is odd

This means that $n = 2a + 1$ for some integer a.

Substituting this into the main term, $n^2 + n + 6$ gives us :

$$
\begin{aligned}
n^2+n+6 &= (2a+1)^2+(2a+1)+6 \\
&= 4a^2+4a+1+2a+1+6 \\
&= 4a^2+6a+8 \\
&= 2(2a^2+3a+4)
\end{aligned}
$$

We know that due to the closedness of integers under addition, that $2a^2+3a+4$ is an integer. So we can say that $n^2+n+6=2k$ if $k=2a^2+3a+4$. This means that n^2+n+6 is even.

Since we have proven that in the case of even and odd numbers n^2+n+6 is even. Therefore, for all integers, n^2+n+6 is even. □

Proof by cases ultimately makes it much more convient for you to deal with

2.1.2 Divisibility

How can we define if something "divides" something else? Well normally you'd say that if the division results in an integer :

"a divides b" if $\frac{b}{a}$ if an integer "a divides b" if $\frac{b}{a}=k$, where k is an integer "a divides b" if $b=ka$, where k is an integer.

Definition of Divisible

An integer a is said to *divide* an integer b if $b \equiv ak$. When a does divide b, we write "$a|b$" and when a does not divide b we write "$a \nmid b$""

The $b=0$ case: $a|0$ for every integer a, because $0=a\cdot 0$ for every such a.

The $a=0$ case: $0 \nmid b$ for every integer b, because for any such b, we have $b \neq 0\cdot k$ for any integer k.

The $a|b$ term is a boolean, either true or false. Remember that for example $4|8$ does not equal 2, rather it is true.

Propositione

Let a,b,c all be integers. If $a|b$ and $b|c$ then $a|c$.

Assume a,b and c are all integers, $a|b$ and $b|c$. Then by definition of divisibilty, $b=ka$ for some integer k and that $c=sb$ for some integer s. Therefore we can say, *Proof.*

$$\begin{aligned} c &= sb \\ &= s(ka) \\ &= a(ks) \end{aligned}$$

Since we have established that s and k are integers, so is ks. So it is indeed true that $c = a(ks)$. This means that $a|c$. □

THeorem

For all integers a and m with $m > 0$. There exist unique integers q and r such that

$$a = mq + r$$

Where $0 \leq r < m$.

This is cool! Because all numbers can be represented by this. For example :

- If $a = 18$ and $m = 7$, then $18 = 7 \cdot 2 + 4$
- If $a = 3$ and $m = 13$, then $13 = 3 \cdot 4 + 1$
- If $a = 35$ and $m = 5$. then $35 = 5 \cdot 7 + 0$

2.1.3 Greatest Common Divisors

Definition

Let a and b be integers. If $c|a$ & $c|b$, then c is said to be a common divisor of a and b The greatest common divisor of a and b is the largest integer d such that $d|a$ and $d|b$. This number is denoted $\text{ged}(a, b)$

Time to try a challenging proof, proving Bezout's identity.

Theorem

If a and b are positive integers, then there exist integers k and l such that

$$\text{ged}(a, b) = ak + bl$$

Using the equation given :

$$\text{qed} = d = ak + bl$$

We want to prove that d is a common divisor of a and b. Looking at the equation for the division algorithm :

$$a = dq + r$$

We want to find values of d where r is equal to 0. So we can set up the equation :
With $0 \leq r \leq d$

$$\begin{aligned} r &= -dq + a \\ &= -(ak + bl)q + a \\ &= -qak - qbl + a \\ &= a(1 - qk) + b(-lq) \end{aligned}$$

We know that these valuas of $(1 - qk)$ and $-lq$ must be integers because integers are closed under addition and multiplication. Remember that d was chosen as the smallest value that can be written like this, and since r has to be less than d, it is intuitive that $r = 0$ because of the sandwich between d and 0. So since $r = 0$, we can conclude that $a = dq$ which means that d is a factor of a. We can do the same with b and conclude confidently that $d|a\&\&d|b$.

Now we will prove that d is the greatest common divisor of a and b.
We will do this by assigning d' as an integer that is a different divisor of a and b
So we know based on the definition of divisibility :

$$a = d'm \quad b = d'n$$

We are also given :

$$d = ak + bl$$

Now we can do some algebra :

$$\begin{aligned} d &= ak + bl \\ &= (d'm)k + (d'n)k \\ &= d'(mk + nk) \end{aligned}$$

So here we have the concluding expression :

$$d = d'(mk + nk)$$

This intuitively means that d must be larger than d'. Because $mk + nk$ is an integer, and since d cannot be negative, this would mean that $mk + nk$ would have to be positive integer. This means that d has to be largest of any other potential divisors of both a and b. Therefor we can say :

$$\text{qed}(a, b) = d = ak + bl$$

□

Since we just proved Bezont's identity, we can now use it to prove other results. Like this one :

$$\text{qed}(ma, mb) = m \cdot \text{QED}(a, b)$$

Modular Arithmetic

When dividing an integer a by an integer m, the relationship between a and its remainder is surprisingly important. a is called congruent to it's remainder.

Definition

For integers a and m, a is congruent to r modulo m and can write $a \equiv r \pmod{m}$ if $m|(a - r)$

For example

- $35 \equiv 0$ (mod5)
- $-3 \equiv 2$ (mod5)

Let's see what we can prove :

Proposition

Assume that a, b, c, d and m are all integers, $a \equiv b \bmod m$ and $c \equiv d \mod m$. It follows that

1. $a + c \equiv b + d \mod m$
2. $a + c \equiv b - d \mod m$
3. $a \cdot c \equiv b \cdot d \mod m$

Let's try and prove 1. This makes intuitive sense, all it's saying is that when added, the remainders from $a + b \mod m$ are added together. Which seems fine. So we can prove this by applying the modulo operator to both a and b then doing some factoring (most likely)

Proof. Assume $a \equiv b \mod m$ and $c \equiv d \mod m$. It follows that

$$m|(a-b) \quad \text{and} \quad m|(c-d) \text{ thus,}$$
$$a - b = mk \quad \text{and} \quad c - d = mf \text{ for some integers } k, t$$

$$\begin{aligned} a - b + c - d &= ml + mk \\ a - b + c - d &= m(l + k) \\ (a + c) - (b + d) &= m(l + k) \\ (a + c) - (b + d) &= mt \end{aligned}$$

□

Since we know that $l + k$ is an integer (which we will represent as t), we can then conclude

$$m|[(a+c) - (b+d)]$$

We can then apply the definition from earlier :

$$a + c \equiv b + d \mod (m)$$

Proposition

Assume that x and y are positive numbers. If $x \geq y$, then $\sqrt{x} \leq \sqrt{y}$

Scratch work : This is a little weird but we can do some algebra to get this solution quite simply :

$$x \geq y$$

Subtracting :

$$x - y \geq 0$$

Now you can actually rewrite this in an interesting way :

$$\sqrt{x}^2 - \sqrt{y}^2 \geq 0$$

Now we can factor by difference of squares :

$$(\sqrt{x} + \sqrt{y})(\sqrt{x} - \sqrt{y}) \geq 0$$

Since we know that x and y are both positive integers, we know that the term $(\sqrt{x}+\sqrt{y})$ has to be just a positive value that scales the other term. So we can easily divide both sides of the equation by it.

$$(\sqrt{x} - \sqrt{y}) \geq 0$$

This implies that $\sqrt{x} \geq \sqrt{y}$

Theorem

AM-GM inequality. If x and y are positive integers, then $\sqrt{xy} \leq \frac{x+y}{2}$

Scratch work :

Because this is a little confusing we can start by proving $Q \implies P$, while this isn't exactly incredibly important, it still gives us decent ideas for future proofs.

$$\begin{aligned}
\sqrt{xy} &\leq \frac{x+y}{2} \\
2\sqrt{xy} &\leq x+y \\
4xy &\leq x^2+2xy+y^2 \\
0 &\leq x^2-2xy+y^2 \\
0 &\leq (x-y)^2
\end{aligned}$$

We know this has to be true because a squared value has to be greater than 0. So we can essentially start at this conclusion, work backwards, and get our proof.

Proof. Let x and y be positive integers. Observe that $0 \leq (x-y)^2$, because the square of a real number is always negative.

$$\begin{aligned}
0 &\leq (x-y)^2 \\
0 &\leq x^2-2xy+y^2 \\
4xy &\leq x^2+2xy+y^2 \\
4xy &\leq (x+y)^2 \\
2\sqrt{xy} &\leq x+y \\
\sqrt{xy} &\leq \frac{x+y}{2}
\end{aligned}$$

So we can see here that there that the geometric mean has to be less than or equal to the arithmetic mean. □

Important to note that you CANNOT start a proof at the conclusion then work backwards. $P \implies Q \neq Q \implies P$

Theorem

Fermat's little theorem. If a is an integer and p is a prime number which does not divide a then :

$$a^{p-1} \equiv 1 \mod p$$

2.2 Main Exercises

Question 1

Prove that the product of two odd integers is odd.

Proof. n and m are two odd integers. Because of this we can represent n and m as $2(k)+1$ and $2(t)+1$ representatively, where k, l are both integers.

$$\begin{aligned} m \cdot n &= (2(k)+1)(2(t)+1) \\ &= 4kt + 2k + 2t + 1 \quad a = 2kt + k + t \\ &= 2(a) + 1 \end{aligned}$$

Because we know that all the values used in this proof are integers, we can say that $2kt + k + t$ is an integer, so by substituting, we can pretty easily see this equation follows the form of an odd number. □

Question 2

Suppose that n is an integer. Prove that if n is odd, then $n^2 + 6n + 5$ is even.

Proof. Since n is odd, we can say that it is equivalent to $2(k)+1$ where k is some arbitrary integer.

$$\begin{aligned} n^2 + 6n + 5 &= (2k+1)^2 + 6(2k+1) + 5 \\ &= (4k^2 + 4k + 1) + (12k + 6) + 5 \\ &= 4k^2 + 16k + 12 \quad a = 2k^2 + 8k + 6 \\ &= 2(a) \end{aligned}$$

Since we know that l and k are both integers, we are able to conclude that $2k^2 + 8k + 6$ would also be an integer, we can call this quantity a, making this substitution we could clearly see that $n^2 + 6n + 5 = 2(a)$. Which follows the form of an even number. □

Question 3

Give an example of the following property. Then prove that it is true.

- If n is an integer, then $5n^2 + n + 3$ is odd.

For an example : $n = 5$

$$5n^2 + n + 3 \implies 5(5)^2 + 5 + 3 \implies 133$$

And since we want to prove that 133 is odd :

$$133 = 2(x) + 1$$

$$132 = 2x$$

$$66 = x$$

And since 66 is an integer, this works out and this case works.

Proof. We will have to solve for 2 cases, the case where the n is an odd value, and the case where n is an even value. For the case where n is odd, it can be represented by $2(a) + 1$, by definition of odd numbers. For the case where n is even, it can be represented by $2(a)$, by definition of even numbers. In both cases a is an arbitrary integer.

Case 1: n is odd

$$\begin{aligned} 5n^2 + n + 3 &= 5(2a+1)^2 + (2a+1) + 3 \\ &= 5(4a^2 + 4a + 1) + (2a + 1) + 3 \\ &= 20a^2 + 20a + 5 + 2a + 4 \\ &= 20a^2 + 22a + 9 \quad k = (10a^2 + 11a + 4) \\ &= 2(k) + 1 \end{aligned}$$

In this case we have only used addition and multiplication with integers, so we can conclude that $10a^2 + 11a + 4$ is an integer. Therefor we can conclude that from the form $2(k) + 1$, that in the case of an odd integer the outcome of $5n^2 + n + 3$ will be odd.

Case 2: n is even

$$\begin{aligned} 5n^2 + n + 3 &= 5(2a)^2 + 2a + 3 \\ &= 5(4a^2) + 2a + 3 \\ &= 20a^2 + 2a + 3 \quad k = 10a^2 + a + 1 \\ &= 2k + 1 \end{aligned}$$

In this case we only used addition and multiplication with integers, so we can conclude that $10a^2+a+1$ is an integer, which makes our substitution valid. Since the form $2k+1$ can be reached again, this means that in the case of an even integer the outcome of $5n^2+n+3$ will be odd. □

Question 4

Prove the following for each, m, n and t are integers.

1. If $m|n$, then $m^2|n^2$.
2. If $m|n$ and $m|t$, then $m|(n+t)$

1. *Proof.* $m|n$ means that $n = km$ where k is some integer. We can use this to deduce that $m^2|n^2$

$$\begin{aligned} m|n &\equiv n = km \\ n^2 &= (km)^2 \\ n^2 &= k^2m^2 \end{aligned}$$

   Since k is just a normal integer, we can deduce that k^2 would also just be a standard integer. This means that $m^2|n^2$. □

2. *Proof.* $m|n$ means that $n = km$ where k is some integer. $m|t$ means that $t = am$ where a is some integer. So we have to combine this. We can do this pretty easily by adding the equations.

$$t + n = am + km \implies m(a+k)$$

   We know that $a+k$ is an integer, this means that $t+n = mb$ where b is an integer. So therefor, by definition of divisibility, $m|(t+n)$ □

Question 5

1. Prove that if n is a positive integer, then 4 divides $1+(-1)^n(2n-1)$
2. Prove that every multiple of 4 is equal to $1+(-1)^n(2n-1)$ for some positive integer n.

Proof.

We want to prove the divisibility of $1+(-1)^n(2n-1)$ by 4. Since we are testing every positive integer, we might as well break the proof into two cases. One where n is even, meaning it can be represented as $2k$ where k is an integer, and one where n is odd, meaning it can be represented as $2k+1$ where k is an integer.

Case 1: n is even

$$\begin{aligned}
1+(-1)^n(2n-1) &= 1+(-1)^{-2k}(2(2k)-1) \\
&= 1+1(4k-1) \\
&= 1+4k-1 \\
&= 4k
\end{aligned}$$

In this case, the expression simplifies down to $4k$, through the definition of divisibility, $4|4a$. Therefor, we can say that in the case where n is even, $4|(1+(-1)^n(2n-1))$

Case 2: n is odd

$$\begin{aligned}
1+(-1)^n(2n-1) &= 1+(-1)^{2k+1}(2(2k+1)-1) \\
&= 1+(-1)^{2k+1}(4k+2-1) \\
&= 1-(4k+1) \\
&= 1-4k-1 \\
&= -4k
\end{aligned}$$

In this case, the expression simplified down to $-4k$, and by definition of divisibility $4|-4k$ because k was defined as an integer. This means that we can say in the case where n is odd, $4|(1+(-1)^n(2n-1))$ □

We can conclude this proof with the fact that all numbers are either odd or even. This means that since we have proven that $4|(1+(-1)^n(2n-1))$ for both when numbers are odd and when numbers are even, we have proven it for all numbers.

Question 6

For each pair of integers, find the unique quotient and remainder when a is divided by q.

1. $a = 13, m = 5$
2. $a = 5, m = 17$
3. $a = -10, m = 3$

1. To find this we can cite the divisibility equation :

Question 7

Determine $4^{301} \equiv n \mod 17$

$$4^{301} = 4^{300} \times 4$$

$$4^{300} = \underbrace{4^2 \times 4^2 \times \ldots \times 4^4}_{150}$$

Now this may not seem very useful, however, all you need to do is see that

$$4^2 = 16 \equiv -1 \mod 17$$

This means that we can then deduce :

$$4^{300} \equiv 1 \mod 17$$

This then means :

$$4^{301} \equiv 4^{300} \times 4 \mod 17 \; \boxed{4^{301} \equiv 4 \mod 17}$$

Question 8

Assume that a is an integer and p and q are distinct primes. Prove that if $p|a$ and $q|a$, then $pq|a$.

Since the two values are distinctly prime this means gcd(pq) = 1
If $p|a$ this implies that $a = pk$ for some integer k.
If $q|a$ and $a = pk$, this means that $q|pk$.

Since we know that gcd(pg)=1 we can say that $q|k$. This means that $k = nq$ for some integer n.

We can then actually concatenate this :

$$a = pk = p(nq)$$

Which means that by divisibility, $pq|a$ with the integer term being n.

Question 9

Prove that for every integer n, either $n^2 \equiv 0 \mod 4$ or $n^2 \equiv 1 \mod 4$

So this is a case where it is easiest to break tested values into even and odd integers. Even integers being able to be represented as $n = 2k$ for some integer k. While odd integers are able to be represented as $n = 2k + 1$ for some integer k.

Case 1 : n is even

$$n^2 = (2k)^2 = 4k^2$$

Since we know that k^2 is an integer, we can say that :

$$n^2 = 4a$$

Where a is an integer, this means that $4|n^2$,

Since 4 goes into n^2, we can say :

$$n^2 \equiv 0 \mod 4$$

When n is even.

Case 2: n is odd

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$$

Since we know that $k^2 + k$ is just an integer, we can say that

$$n^2 - 1 = 4(a)$$

Where a is an integer, this means that $4|n^2 - 1$

Since 4 goes into $n^2 - 1$, we can say :

$$n^2 \equiv 1 \mod 4$$

.

When n is odd.

You can combine these two cases to cover all integers. This essentially results by saying that for all integers the proposed solutions occur.

YAY DONE WITH THIS CHAPTER!!!

CHAPTER 3

CHAPTER 3: SETS

3.1 Notes

So what is a set ?

Definitions

- A set is an unordered collection of distinct objects called elements.
- $x \in S$ means x is an element of S, it's read "x in S."

Sets are very frequently represented by a bunch of curly braces displaying elements : $\{12, potato, \pi, \sin(15)\}$. Anything can be in a set.

Definitions

- The set of *natural numbers*, denoted $\mathbb{N}$, is the set $\{1, 2, 3, \ldots\}$
- The set of *integers*, denoted $\mathbb{Z}$, is the set $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$
- The *empty set*, denoted $\emptyset$ or $\{\}$ has no elements.
- The set of *rational numbers*, denoted by $\mathbb{Q}$, follows a more complex definition

So very cool, we can define sets and there are a bunch of different sets we frequently use for a whole variety of places. However it is very inconvenient to need to try and write out all the elements, and the $\ldots$ is not rigorous. So instead we use set builder notation.

$$\{\text{Elements} \in S : \text{Conditions used to generate elements}\}$$

S being a larger set from which elements are taken

It is worth noting that it is optional to include $\in S$ if you are not necessarily pulling from a larger set. Generally one side of the set will have this.

Examples :

$$\begin{aligned} \{n^2 : n \in \mathbb{N}\} &= \{1, 4, 9, 16, \} \\ \{|n|\} &= \{0, 1, 2, 3, \ldots\} \end{aligned}$$

Very cool, you see above where it says $N \in \mathbb{N}$, that's essentially saying you take values from $\mathbb{N}$ and place them into the modifier.

You can also write these in the "opposite" way where the source of the elements and the "sorting algorithm" is on the right :

$$\begin{aligned} \{n \in \mathbb{Z} : n \text{is even}\} &= \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\} \\ \{n \in N : 6|n\} &= \{6, 12, 18, 24, \ldots\} \end{aligned}$$

So this is cool too! Either way it works. It doesn't matter what goes on what side.

Definition

The set of *rational numbers* is referred to as $\mathbb{Q}$. It's definition using set builder notation is :

$$\mathbb{Q} = \left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$$

So this is interesting we can now define most "things" using set builder notation for example all 2x2 matrices can be written as :

$$\left\{\begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in R\right\}$$

The $xy-$plane of all ordered pairs of real numbers :

$$\mathbb{R}^2 = \{(x, y) : x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$$

While the unit circle can be written as :

$$S^1 = \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$$

The open interval (a,b) can be written as :

$$(a,b) = \{x \in \mathbb{R} : a < x < b\}$$

3.1.1 Proving $A \subseteq B$

Defintion of $\subseteq$

Suppose A and B are sets. If every element in A is also an element of B, then A is a *subset* of B, which can be written $A \subseteq B$.

Some examples :

- $\{1, 3.5\} \subseteq \{1,2,3,4,5,6,7,8\}$
- $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$
- $\{a,b,c\} \nsubseteq \{a,b,e,f,g\}$

So when writing $A \subseteq B$, generally this means that A only has elements that are in B or $A = B$. In the case where $A \subseteq B$ but $A \neq B$ this called a *proper subset* of B. The correct notation for this is $A \subset B$

So let's try and prove this in a few example problems! Generally the key here is to find your commonality between the two sets you're discussing.

Example 1:

Proposition

Prove that

$$\{n \in \mathbb{Z} : 12|n\} \subseteq \{n \in \mathbb{Z} : 3|n\}$$

Ok so let's get too it! Generally the way I'd approach this is looking at the things we are testing and where the elements are being taken from in each set. The set on the left has integers divisible by 12 while the set on the left has integers divisible than 3. This proposition is intuitively obviously true. However we can prove it rigorously as well.

Proof. Assume $x \in \{n \in \mathbb{Z} : 12|n\}$ this means that $x \in \mathbb{Z}$ and $12|x$. We know through the definition of divisibility this means $x = 12k$ with $k \in \mathbb{Z}$. However we can then say :

$$x = 3(4k)$$

Because we know that $k \in \mathbb{Z}$, we know that $4k \in \mathbb{Z}$, which by extension means that

$$3|x$$

Since $x \in \{n \in \mathbb{Z} : 12|n\}$ also implies $x \in \{n \in \mathbb{Z} : 3|n\}$ it is easily seen that $\{n \in \mathbb{Z} : 12|n\} \subseteq \{n \in \mathbb{Z} : 3|n\}$ □

So generally, when trying to prove that $A \subseteq B$, we pick an arbitrary $x \in A$ and prove that $x \in B$. We should never pick a specific element and we should never assume anything about the element other than it's definition in set A.

If something applies to an arbitrary element of a set, it will apply to every element in the set.

So now let's do that exact thing we're not supposed to do :

Proposition

Let $A = \{-1, 3\}$ and $B = \{x \in \mathbb{R} : x^3 - 3x^2 - x + 3 = 0\}$ then $A \subseteq B$.

This one is actually quite funny, so rather than ignoring the specific examples, the easiest way of doing this problem is just breaking it into 2 cases for each of the integers in A.

Proof. Assume $x \in A$. Then either $x = -1$ or $x = 3$. Consider the cases separately.

Case 1: x = -1

$$(-1)^3 - 3(-1)^2 - (-1) + 3 = 0$$

This is congruent with the definition of B, implying that $x \in B$

Case 2: x = 3

$$(3)^3 - 3(3)^2 - 3 + 3 = 0$$

This is congruent with the definition of B, implying that $x \in B$ Since $x \in A$ implies that $x \in B$, it's evident that $A \subseteq B$ □

Proving that a set $A \subseteq B$ is called *proving subset inclusion.*

Proving A = B

When proving $A = B$, you have to prove that both sets are subsets of each other, essentially saying that : $A \subseteq B$ and $B \subseteq A$. So it's just double the work.

3.1.2 Set Operations

Defintions

- The *union* of sets A and B is the set $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- the *intersection* of sets A and B is the set $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- If $A_1, A_2, A_3, \ldots, A_n$ are all sets, then the union of all of them is denoted :

$$\bigcup_{i=1}^{n} A_i$$

- If $A_1, A_2, A_3, \ldots, A_n$ are all sets, then the intersection of all of them is denoted :

$$\bigcap_{i=1}^{n} A_i$$

The easiest way of thinking about this is that the union operation is like dropping the contents of each of the sets into one larger "box" and removing any duplicates. While the intersection is like dropping all of the objects from each set into one box, then removing one of each object so that only objects shared between the sets are left in the larger box.

Subtraction and Complements

Defintion

Assume A and B are sets and $x \notin B$ means that x is not an element of B.

- The *subtraction* of B from A is $A \backslash B = \{x : x \in A \text{ and } x \notin B\}$
- If $A \subseteq U$, then U is called a *universal* set of A. The *complement* of A in U is $A^c = U \backslash A$

This is quite intuitive, $A \backslash B$ basically just means "all elements in A not in B". When you look at the complement A^C this is also understood as everything *not* in A.

Note that : $A \cup B = B \cup A$ and $A \cap B = B \cap A$ are always true. But there are very rare cases where $A \setminus B = B \backslash \} A$ only in the case where both sets are identical.

3.1.3 Power Sets and Cardinality

Definitions

The *power set* of a set A is $\mathcal{P}(A) = \{X : X \subseteq A\}$
THe *cardinality* of a set A is the number of elements in the set, it's denoted $|A|$

The powerset is essentially just a list of all possible subsets of a set. This is best viewed in an example

- The power set of $\{1, 2, 3\}$ is

$$\mathcal{P}(\{1,2,3\}) = \{\{1,2,3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1\}, \{2\}, \{3\}, \{\emptyset\}\}$$

- The power set of $\mathbb{N}$ can be viewed as the set of all possible sets containing only natural numbers.

Cardinality is much easier to understand, just being the number of elements in a set.

Cartesian Products

Definition

Assuming A and B are sets :
The *Cartesian product* of A and B is $A \times B = \{(a, b) : a \in A \text{ and } b \in B\}$

This is a way to multiply sets by each other. They essentially just pair all the possible combinations of elements with each other in an ordered pair.

$$\{1,2,3\} \times \{a, b\} = \{(1,a), (1,b), (2,a), (2,b), (3,a), (3,b)\}$$

The name Cartesian product is used because think of the cartesian plane, this plane is actually a large number of points that are all $\mathbb{R} \times \mathbb{R}$.

So let's write a proof :

Prove that if A and B are both sets, then $A \subseteq B$ assuming $\mathcal{P} \subseteq \mathcal{P}(B)$

Proof. We know from the definition of a power series :

$$A \in \mathcal{P}(A)$$

Since we had assumed that $\mathcal{P}(A) \in \mathcal{P}(B)$, we can say

$$A \in \mathcal{P}(B)$$

Through the definition of a power set, we know that if A is an element of the power set, then A is one of the subsets of B. Which means we can conclude:

$$A \subseteq B$$

□

Theorem

De Morgan's Law : Suppose A and B are subsets of a universal set U. Then,

$$(A \cup B)^c \subseteq A^c \cap B^c \quad \text{and} \quad (A \cap B)^c \subseteq A^c \cup B^c$$

Or more concisely :

$$(A \cup B)^c = A^c \cap B^c$$

Let's prove this theorem. However, rather than manually working through the set operations, I realized this is much easier to prove using set builder notation to build sets that match these parameters :

Proof.

$$\begin{aligned}
(A \cup B)^c &= \{x \in U : x \in A^c \text{ and } x \in B^c\} \\
&= \{x \in U : x \notin A \text{ and } x \notin B\} && \text{Applying definition of converse} \\
&= \{x \in U : x \notin (A \cup B)\} && \text{Union definition} \\
&= (A \cap B)^c && \text{Definition of complment}
\end{aligned}$$

□

Fun Sample Exercise

Prove this : Given any $A \subseteq \{1, 2, 3, \ldots, 100\}$ for which $|A| = 10$, there exist two different subsets $X \subseteq A$ and $Y \subseteq A$ for which the sum of the elements in X is equal to the sum of the elements in Y.

Proof. The best way of approaching this problem would be to establish pigeonholes. Which seems to be a great way of approaching these combinatoric problems.

Because we know there will be 10 elements in our sets A, we know that there are 2^{10} possible variations.

Since we know that $A \subseteq \{1, 2, 3, \ldots, 100\}$ and we have $|A| = 10$, we can say that the smallest possible value for a subset A would be the set :

$$\{1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 + 10 = 55\}$$

Conversely, we can say the largest possible subset A would be the set :

$$\{100 + 99 + 98 + 97 + 96 + 95 + 94 + 93 + 92 + 91 = 955\}$$

Because we know the largest possible subset value would be 955 and 55, we can conclude that there are 945 different values possible for the value of the sum of elements from A. However, we have deduced earlier that there are actually 1024 possible different combinations of element sums. So because there are only 945 different total sums with 1024 possible 3 □

3.2 Main Exercises

Question 1

Rewrite each of the following sets by listing their elements between braces.

1. (a) $\{n \in \mathbb{N} : -7 \leq n < 6\}$ (b) $\{\frac{m}{n} \in \mathbb{Q} : |\frac{m}{k}| < 1 \text{ and } 1 \leq n \leq 4\}$
2. (a) $\{4n : n \in \mathbb{Z} \text{ and } |2n| < 7\}$ (b) $x \in \mathbb{R} : x^2 - 1 = 0$

1.

$$\{-, 7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6\}$$

2.

$$\left\{0, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{2}{3}, \frac{2}{4}, \frac{3}{4}\right\}$$

3.

$$4\,\{-3, -2, -1, 0, 1, 2, 3\}$$

$$\{-12, -8, -4, 0, 4, 8, 12\}$$

4.
$$\{-1, 1\}$$

Question 2

Write these sets in set builder notation.

1. (a) $\{2, 5, 8, 11, 14\}$ (b) $\{-4, -3, -2, -1, 0, 1\}$
2. (a) $\left\{\ldots, -\frac{3\pi}{2}, -\pi, -\frac{\pi}{2}, 0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}, \ldots\right\}$ (b) $\left\{\ldots, -\frac{3125}{243}, -\frac{125}{27}, -\frac{5}{3}, 1, \frac{25}{9}, \frac{625}{81}\right\}$

1.
$$\{2n + 3 : n \in \mathbb{N} \text{ and } 2n + 3 < 17\}$$

2.
$$\{n \in \mathbb{Z} : -4 \leq n \leq 1\}$$

3.
$$\left\{\frac{n\pi}{2} : n \in \mathbb{Z}\right\}$$

4. This is easiest done with some reordering :

$$\left\{1, -\frac{5}{3}, \frac{25}{9}, -\frac{125}{27}, \frac{625}{81}, -\frac{3125}{243}\right\}$$

$$\left\{(-1)^n \left(\frac{5}{3}\right)^n : n \in \mathbb{Z}\right\}$$

Question 3

The set $\{71 + 2b : a, b \in \mathbb{Z}\}$ is equal to a familiar set. By examining which elements are possible, determine the familiar set.

Since we see that $71 + 2b$ has no influence from variable a,we can determine that the set : $\{71 + 2b : b \in \mathbb{Z}\}$ is equivalent to the set in question. So by looking at this set, we can use the definition of an odd number, where $a = 2k + 1$ where k is any given integer to solve for b.

$$\begin{aligned} 71 + 2b &= 2k + 1 \\ 2b &= 2k - 70 \\ b &= k - 35 \end{aligned}$$

We know that both b and k are integers. So we can conclude that it's essentially evident that $71 + 2b$ is essentially just another way of rewriting the odd integers.

Question 4

Suppose A and B are sets. Prove that

$$\mathcal{P}(A) \cup \mathcal{P}(B) \subset \mathcal{P}(A \cup B)$$

So we want to prove that any element that is found in the union of the power sets of both A and B will also be found in the $\mathcal{P}$ of the union of sets A and B.

$$x \in \mathcal{P}(A) \cup \mathcal{P}(B)$$

By definition of union, we know that x is an element from both $\mathcal{P}(A)$ and $\mathcal{P}(B)$. So without loss of generality we can say that $x \in \mathcal{P}(A)$, as the future argument will be identical if $x \in \mathcal{P}(B)$.

If $x \in \mathcal{P}(A)$, then we have to say that $x \subseteq A$.

So we can then say intuitively that $x \subseteq A \subseteq A \cup B$. This means that $x \subseteq A \cup B$. So since this is true, we can then say $x \in \mathcal{P}(A \cup B)$

This allows us to draw the conclusion that

$$\boxed{\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)}$$

Question 5

Prove that

$$\{n \in \mathbb{Z} : n \equiv 1 \mod 4\} \not\subseteq \{n \in \mathbb{Z} : n \equiv 1 \mod 8\}$$

In order for $A \subseteq B$, all elements in A must be found in B. So for our purposes we can disprove this above statement by finding one counterexample for an element in the first statement that is not present in the second set.

Using the definition of mod we can rewrite the two sets in this way :

For set 1 :

$$n = 4k + 1$$

For set 2:

$$n = 8k + 1$$

Where k and n must be integers.

Now we can test different n values to find a counterexample.

n=5

For set 1:

$$5 = 4k + 1$$
$$k = 1$$

This is a valid expression as k is an integer.

For set 2:

$$5 = 8k + 1$$
$$4 = 8k$$
$$\frac{1}{2} = k$$

This expression is not valid as $\frac{1}{2}$ is not an integer. So we can conclude that

$$\boxed{\{n \in \mathbb{Z} : n \equiv 1 \mod 4\} \not\subseteq \{n \in \mathbb{Z} : n \equiv 1 \mod 8\}}$$

Question 6

Suppose someone conjectured that, for any sets A and B which contain finitely many elements, we have

$$|A \cup B| = |A| + |B|$$

Prove or disprove it.

We know that in a set elements cannot be repeated and this property is the primary flaw with this conjecture. I'll disprove by counterexample :

$$A = \{1, 2, 3, 4\} \quad |A| = 4$$

$$B = \{4, 5, 6, 7\} \quad |B| = 4$$

So we know intuitively that $|A| + |B| = 8$

However, when dealing with the cardinality of the union of the sets, it is easily seen that the cardinality will be different :

$$A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$$

So $|A \cup B| = 7$. This makes intuitive sense as the two sets have one overlapping element, therefor a copy of this element will be deleted upon the union of the two sets.

Question 7

Suppose A, B and C are sets. Prove that

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Since we want to prove equivalence we will be using the definition of equivalence of sets, this being that both sets are subsets of each other.

Proof. There are two cases we have to prove. That $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ and $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$

Proving $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ **:**
$x \in A \cup (B \cap C)$ by definition of the union we know this means that $x \in A$ or $x \in (B \cap C)$. So lets test these two cases.

Case 1: $x \in A$
Since we have the intersection of $A \cup B$ and $A \cup C$, we know that A is a commonality between both unions. Therefore A must be included in the intersection. This intuitively means that

$$x \in A, \text{ then } x \in (A \cup B) \text{ and } x \in (A \cup C)$$

$$x \in (A \cup B) \cap (A \cup C)$$

Case 2: $x \in B \cap C$
Since we have $x \in B \cup C$, we can say $x \in B$ or $x \in C$. We can then conclude that $x \in A \cup B$ and $x \in A \cup C$. So we can then conclude that $B \cap C \subseteq (A \cup B) \cap (A \cup C)$.

This allows us to finally conclude that $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. Now for the second primary case.

Proving $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$ **:**
$x \in (A \cup B) \cap (A \cup C)$ through definition of the intersection means that $x \in (A \cup B)$ and

$x \in (A \cup C)$. So there are two pretty clear cases. The case where $x \in A$ and $x \notin A$.

Case 1: $x \in A$

This is a rather moot point and is quite obvious. If $x \in A$, then obviously $x \in A \cup (B \cap C)$ by definition of union.

Case 2: $x \notin A$

Since we know that $x \in (A \cup B) \cap (A \cup C)$, we can say that both, $x \in B$ and $x \in C$. This means that $x \in B \cap C$. This means that $x \in A \cup (B \cap C)$ by definition of union.

We can now confidently conclude that $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Since we proved that both sets are subsets of each other we can finally conclude that both sets are equivalent. Allowing us to conclude

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

□

Question 8

Let C be any set. Prove that there is a unique set $A \in \mathcal{P}(C)$ such that for every $B \in P(C)$ we have $A \cup B = B$

There is only one set that likely applies to this case, $\emptyset$. We know that if $A = \emptyset$, then $A \cup B = B$ for all $B \in \mathcal{P}(C)$

So in order to prove this case is unique we can assume the opposite and prove by contradiction. Let A and A' be the two sets that satisfy this property, A, being the set $\{\emptyset\}$. Since we know that $A \cup B = B$, we can say that $A \cup A' = A$ if we say that $B = A'$. This means that there is only one set that fits this property. Ultimately meaning that $\{\emptyset\}$ is the only possible set that has this property. □

CHAPTER 4

CHAPTER 4 : INDUCTION

4.1 Notes

Induction allows us to apply proofs to infinite series type proofs. This is done by proving a statement for one (generally trivial) case, then showing that if this statement is true for any of the cases, then the subsequent cases would be true as well.

Induction Definiton

Consider a sequence of matehmatical statements, $S_1, S_2, S_3, \ldots$.

- Suppose S_1 is true, and
- Suppose, for each $k \in \mathbb{N}$, if S_k is true, then $S_\mathrm{k+q}$ is true.

Then, S_n is true for every $n \in \mathbb{N}$

This implies there is a usual form that these inductive proofs take :

Inductive Proof Format

Proposition : $S_1, S_2, S_3, \ldots$ are all true.

Proof. $\ll$ General setup or assumptions $\gg$

Base Case - Proving that S_1 is true

Inductive Hypothesis - Assuming that S_{k} is true

Inductive Step - Proving that S_k implies S_{k+1}

Conclusion - Therefor, by induction all the S_n are true.

□

4.1.1 General Inductive Proofs

Examples :

This is a little complicated so we can try and just make some simple examples :

Induction Example with Triangular numbers.

For any $n \in \mathbb{N}$,

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

Proof. : We will perform this proof via induction.

Base Case

The base case is defined as when $n = 1$, therefor

$$1 = \frac{1(1+1)}{2}$$

Which is valid.

Inductive Hypothesis

Let $k \in \mathbb{N}$, and we can assume :

$$1 + 2 + 3 + \ldots + k = \frac{k(k+1)}{2}$$

Inductive Step

So we now want to prove that this result will hold for $k + 1$. Meaning that we want to prove that

$$1+2+3+\ldots+(k+1)=\frac{(k+1)((k+1)+1)}{2}$$

Rewritten :

$$1+2+3+\ldots+k+(k+1)=\frac{(k+1)(k+2)}{2}$$

Since we have an inductive hypothesis, we are able to apply it to this situation :

$$1+2+3+\ldots+k+(k+1)=\frac{k(k+1)}{2}+(k+1)$$

We can now work on simplifying the right side :

$$\begin{aligned}&=\frac{k(k+1)}{2}+k+1\\&=\frac{k(k+1)}{2}+\frac{2(k+1)}{2}\\&=\frac{k^2+3k+2}{2}\\&=\frac{(k+1)(k+2)}{2}\\&=\frac{(k+1)((k+1)+1)}{2}\end{aligned}$$

Which aligns perfectly with our prediction.

Conclusion

Therefore, by induction we can conclude that $1+2+3+\ldots+n=\frac{n(n+1)}{2}$ for all $n\in\mathbb{N}$ □

Proposition

Let S_n be the sum of the first n natural numbers. Then for any $n\in\mathbb{N}$,

$$S_{\mathrm{n}}+S_{\mathrm{n+1}}=(n+1)^2$$

So there are two primary ways this is easily proven. A direct proof and a inductive proof. First the direct proof will be done then the inductive, I'll be trying these without using the textbook!

Direct Proof

It has been proven that $S_n=\frac{n(n+1)}{2}$ and that $S_{n+1}=\frac{(n+1)(n+2)}{2}$

We are now able to prove that these forms can be rewritten as $(n+1)^2$

$$\begin{aligned} S_n + S_{n+1} &= \frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} \\ &= \frac{n^2 + n + n^2 + 3n + 2}{2} \\ &= \frac{2n^2 + 4n + 2}{2} \\ &= n^2 + 2n + 1 \\ &= (n+1)^2 \end{aligned}$$

□

That was quite easy! And it worked quite well. But this can also be done in an inductive way.

Inductive Proof

So we have to establish the Base case, Inductive hypothesis, Inductive step, and then our Conclusion.

Base Case : $n = 1$

$$S_n + S_{n+1} = 1 + 3 = 4, \text{ and } (1+1)^2$$

Inductive hypothesis if we assume $k \in \mathbb{N}$:

$$S_k + S_{k+1} = (k+1)^2$$

Inductive step

So we want to prove that our hypothesis will hold for $k+1$,

$$S_{k+1} + S_{k+2} = (k+2)^2$$

$$S_{k+1} = 1 + 2 + 3 + \ldots + k + (k+1)$$

$$S_{k+1} = S_k + (k+1)$$

Following the same logic :

$$S_{k+2} = S_{k+1} + (k+1)$$

So we can use this :

$$\begin{aligned} S_{k+1} + S_{k+2} &= S_k + (k+1) + S_{k+1} + (k+2) \\ &= (k+1)^2 + 2k + 3 \\ &= k^2 + 2k + 1 + 2k + 3 \\ &= k^2 + 4k + 3 \\ &= (k+2)^2 \end{aligned}$$

Conclusion: By induction we can conclude that this proposition holds for $n \in \mathbb{N}$. □.
Another example :

Proposition

For every $n \in \mathbb{N}$, the product of the first n odd natural numbers equals $\frac{(2n)!}{2^n n!}$. That is :

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2n-1) = \frac{(2n)!}{2^n n!}$$

We will proceed with this proof via induction.
Base Case:
$n = 1$

$$1 = \frac{(2n)!}{2^1(1!)}$$

$$1 = \frac{2}{2}$$

$$1 = 1$$

Inductive Hypothesis:
Assuming $k \in \mathbb{N}$

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1) = \frac{(2k)!}{2^k k!}$$

Induction Step:
We aim to prove this result holds for $k+1$.
This meaning :

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2(k+1)-1) = \frac{(2(k+1))!}{2^{k+1}(k+1)!}$$

Trying to simplify, since it can be helpful to write out the penultimate step :

$$1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1) \cdot (2k+1)$$

Based on the definition of our inductive hypothesis we can then rewrite this series as :

$$\frac{(2k)!}{2^k k!} \cdot (2k+1) = \frac{(2k+2)!}{2^{k+1}(k+1)!}$$

We know that $(2k)! = 2k \cdot 2(k-1) \cdot 2(k-2) \ldots (2)$ so we can say that $(2k)! \cdot (2k+1) = (2k+1)!$ So we can perform some algebra :

$$\begin{aligned} 1 \cdot 3 \cdot 5 \cdot \ldots \cdot (2k-1) \cdot (2k+1) &= \frac{(2k)!}{2^k(k)!} \cdot (2k+1) \\ &= \frac{(2k+1)!}{2^k(k)!} \\ &= \frac{(2k+1)! \cdot (2k+2)}{2^k k! \cdot (2k+2)} \\ &= \frac{(2k+2)!}{2^{k+1}(k+1)!} \end{aligned}$$

Conclusion: We have proven by induction that

$$1 \cdot 3 \cdot 4 \cdot (2n-1) = \frac{(2n)!}{2^n n!}$$

For all $n \in \mathbb{N}$.

4.1.2 Strong Induction

Strong Induction Definition.

Consider a sequence of matematical statements $S_1, S_2, S_3, \ldots$

- Suppose s_1 is true, and
- Suppose, for any $k \in \mathbb{N}$, if $S_1, S_2, \ldots S_k$ are all true, then S_{k+1} is true.

Them S_n is true for every $n \in \mathbb{N}$.

In regular induction, you use S_1 to prove S_2, and then S_2 to prove S_3.
But in strong induction, you use S_1 to prove S_2, and then S_1 and S_2 to prove S_3.
This is the primary template for a Strong inductive proof.

Strong Inductive Proof Format

Proposition : $S_1, S_2, S_3, \ldots$ are all true.

Proof. ≪ General setup or assumptions ≫

Base Case - Proving that S_1 is true

Inductive Hypothesis - Assuming that S_{k} is true

Inductive Step - Proving that $(S_1, S_2, \ldots, S_k)$ implies S_{k+1}

Conclusion - Therefor, by induction all the S_n are true.

□

This is best shown through examples :

We have said before that all integers larger than 2 are either prime or a product of primes.

Theorem

Every integer $n \geq 2$ is either prime or a product of primes.

Proof. We proceed with strong induction.

Base Case: Our base case is the case where $n = 2$, this is trivial as 2 is clearly defined as prime.

Inductive Hypothesis: Let k be a natural number such that $k \geq 2$, and assume that each of the integers $2, 3, 4, \ldots, k$ is either prime or a product of primes.

Inductive Step: We have to prove that $k + 1$ is either prime or composite. Since we know that $k + 1$ is obviously larger than 1, it has to either be prime or composite. So we can consider these two cases

Case 1, k+1 is prime : This case is obivious since we want to prove that $k+1$ is either prime or composite, so if $k + 1$ is prime then it's prime.

Case 2, $k + 1$ is composite : This is to say, that $k + 1$ has factors other than 1 and itself. Meaning we could say that $k + 1 = st$ where s, t are positive integers.

$$1 < s < k + 1 \quad \text{and} \quad 1 < t < k + 1$$

By inductive hypothesis, we can say that s and t should be able to be written as a product of primes.

$$s = p_1 \cdot p_2 \cdot$$

Conclusion: All $\mathbb{Z} > 2$, are either prime or multiples of primes.

□

Strong induction proof for multiple base cases :

Proposition

For every $n \in \mathbb{N}$ with $n \geq 11$ can be written as $2a + 5b$ for some natural numbers a and b.

Proof. We proceed with induction

Base Case: There are two primary base cases in this situation, the case where $n = 11$ and when $n = 12$.

$$n = 11, 2(3) + 5(1) \therefore a = 3, b = 1$$

$$n = 12, 2(1) + 5(2) \therefore a = 1, b = 2$$

Inductive Hypothesis: Let k be a natural number such that $k \geq 13$, we will assume that the $2a + 5b$ property will hold for

$$n = 11, 12, 13, \ldots, k$$

Inductive Step: We want a proof for $k + 1$, we know that :

$$k - 1 = 2a + 5b$$

This is equivalent to $n = 2a + 5b$, which is said in our inductive hypothesis.

Conclusion: □

CHAPTER 5

5