MATHEMATICS 300 — FALL 2017

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S LECTURE NOTES

PART IV

Contents

8 Existential sentences

8.1 Existential quantifiers

- The symbol

$$\exists$$

is the ***existential quantifier symbol***.

- An ***existential quantifier*** is an expression "$(\exists x)$" or "$(\exists x \in S)$" (if S is a set). More precisely,

  "$(\exists x)$" is an ***unrestricted existential quantifier***,

  and

  "$(\exists x \in S)$" is a ***restricted existential quantifier***.

- Existential quantifiers are read as follows:

  1. "$(\exists x)$" is read as

     ∗ "there exists x such that"

     or

     ∗ "for some x"

     or

     ∗ "it is possible to pick x such that".

  2. "$(\exists x \in S)$" is read as

     ∗ "there exists x belonging to S such that"

     or

     ∗ "there exists a member x of S such that"

     or

     ∗ "for some x in S"

     or

     ∗ "it is possible to pick x in S such that" or

- ∗ "it is possible to pick a member x of S such that"

Example 28. The sentence

$$(\exists x \in \mathbb{R})x^2 = 2 \tag{8.1}$$

could be read as

> There exists an x belonging to the set of real numbers such that $x^2 = 2$.

But this is horrible! A much better way to read it is:

> There exists a real number x such that $x^2 = 2$.

An even better way is

> There exists a real number whose square is 2.

And the nicest way of all is

> 2 has a square root.

And you can also read (8.1) as:

$$\boxed{\text{It is possible to pick a real number } x \text{ such that } x^2 = 2}.$$

I recommend this reading, because when you read an existential sentence this way it becomes clear that the next thing to do is to actually pick an x, that is, to apply the rule foe using an existential sentence, i.e. Rule $\exists_{use}$ □

8.2 How do we work with existential sentences in proofs?

As you may have guessed, I am going to give you two rules, one for *proving* existential sentences, and one for *using* them. And the names of these rules are going to be—yes, you guessed it!—Rule $\exists_{prove}$ and Rule $\exists_{use}$.

8.2.1 The rule for using existential sentences (Rule $\exists_{use}$)

Rule $\exists_{use}$ says something very simple and natural: ***if you know that an object of a certain kind exists, then you can pick one and give it a name.***

Example 29. Suppose "$P(x)$" stands for "x eats grass", and C is the set of all cows. Suppose you know that

$$(\exists x \in C)P(x)\,,$$

that is, you know that there are grass-eating cows.

Then the thing you can do, according to Rule $\exists_{use}$, is pick a cow and give her a name.

So, for example, you could write

Pick a cow that eats grass and call her Suzy.

Or you could write

Let Suzy be a grass-eating cow. □

Example 30. Suppose you have a real number x and you know that

$$(\exists y \in \mathbb{R})y^5 - y^3 = x\,. \qquad (8.2)$$

Then you can say, in the next step of your proof: :

> Pick a real number that satisfies (8.2) and call it r, so $r \in \mathbb{R}$ and $r^5 - r^3 = 5$.

or you could write

> Let r be a real number such that $r^5 - r^3 = 5$.

And you could even say

> Let y be a real number such that $y^5 - y^3 = 5$.

□

Remark 13. When you pick an object, as in the previous example, you can give it any name you want: you can call it r, k, m, u, $\hat{r}$, a, α, $\diamond$, $\clubsuit$, Alice, Donald Duck, whatever.

You can even call it y, if you wish.

The key point is: ***the name you use cannot be already in use as the name of something else***.

So "y" qualifies as an acceptable name because, within the sentence "$(\exists y \in \mathbb{R})y^5 - y^3 = x$", y is a bound variable, but as soon as the sentence ends, "y" becomes a free variable, with no declared value, so you are allowed to use it.

However, I recommend that you do not use the same letter that appeared in the existential quantifier. □

There is, however, one thing that is absolutely forbidden:

You cannot give the new object that you are picking a name that is already in use as the name of another object.

The reason for this prohibition is very simple: if you could use the name r to name this new object that you are introducing, while r is already the name of some other object that was introduced before, you would be forcing these two objects to be the same. But there is no reason for them to be the same, so you cannot give them the same name.

Example 31. Suppose you know that Mr. Winthrop has been murdered. That means, if we use "$P(x)$" for the predicate "x murdered Mr. Winthrop". that you know that $(\exists x)P(x)$ (that is, somebody murdered Mr. Winthrop). Then you can introduce a new character into your discourse, and call this person "the murderer", or "the killer". (This is useful, because you want to be able to talk about that person, and say things such as "the murderer must have had a key so as to be able to get into Mr. Winthrop's apartment".) But you cannot call the murderer "Mrs. Winthrop", because if you do so you would be stipulating that it was Mrs. Winthrop that killed Mr. Winthrop, which could be true but you do not know that it is. □

And here is a precise statement[1] of Rule $\exists_{use}$:

Rule $\exists_{use}$

(I) If

1. $P(x)$ is a sentence,
2. the letter a is not in use as the name of anything,
3. you have proved $(\exists x)P(x)$,

then

* you can introduce a new object, call it a, and stipulate that $P(a)$.

(II) In addition, if S is a set, and you have proved that $(\exists x \in S)P(x)$, then you can stipulate that $a \in S$ as well.

8.2.2 The rule for proving existential sentences (Rule $\exists_{prove}$, a.k.a. the *witness rule.*)

This rule is very simple, and very easy to remember:

- ***to prove that there is money here, show me the money***;
- ***to prove that cows exist, show me a cow***;
- ***to prove that good students exist, show me a good student***,
- ***to prove that incorruptible politicians exist, show me an incorruptible politician***,
- ***to prove that prime numbers exist, show me a prime number,***

and so on.

Example 32. Suppose you want to prove that $(\exists x \in \mathbb{Z})x^2 + 3x = 10$.

[1] In this statement, we use the same convention explained earlier: $P(a)$ is the sentence obtained from $P(x)$ by substituting a for x. For example, if $P(x)$ is the sentence "x eats grass", then $P(\text{Suzy})$ is the sentence "Suzy eats grass". If $P(x)$ is the sentence "$x + 3y = x^2$", then $P(a)$ is the sentence "$a + 3y = a^2$".

You can say "Take $x = 2$. Then $x^2 + 3x = 10$, because $x^2 = 4$ and $3x = 6$, so $x^2 + 3x = 4 + 6 = 10$". Then Rule $\exists_{prove}$ allows us to go to $(\exists x)x^2 + 3 \cdot x = 10$. □

Definition 19. If $P(x)$ is a sentence, then an object a for which $P(a)$ is true is called a ***witness*** for $(\exists x)P(x)$. So, for example, any cow would be a witness for the statement "$(\exists x)x$ is a cow", and the number 2 is a witness for the statement "$(\exists x)x^2 + 3x = 10$". □

And here is a precise statement of the witness rule:

Rule $\exists_{prove}$ (the witness rule)

If:

1. $P(x)$ is a sentence,
2. a is any object,
3. you have proved $P(a)$,

then

* you can go to $(\exists x)P(x)$.

In addition, if S is a set, and you have proved that $a \in S$, then you can go to $(\exists x \in S)P(x)$.

In other words, ***Rule*** $\exists_{prove}$ ***says that you can prove the sentences*** $(\exists x)P(x)$ ***or*** $(\exists x \in S)P(x)$ ***by producing a witness.***

Remark 14. Using the "witness" terminology, we can also state Rule $\exists_{use}$: ***If you know that an existential sentence is true, then you can introduce a witness and give it a name.*** □

8.3 Examples of proofs involving existential sentences

Example 33. Let us prove that

$$(\exists x \in \mathbb{Z})(\exists y \in \mathbb{Z})x^2 - y^2 = 17\,. \tag{8.3}$$

Here is a proof:

Take $x = 9$, $y = 8$. Then $x^2 = 81$ and $y^2 = 64$. So $x^2 - y^2 = 81 - 64 = 17$. Therefore the pair $(9, 8)$ is a witness for (8.3). By the witness rule, this proves (8.3). **Q.E.D.**

Example 34. Consider the sentence

$$(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})n < m\,. \tag{8.4}$$

Is this sentence true or false? If it is true, prove it. If it is false, prove that it is false (that is, prove its negation).

SOLUTION. Sentence (8.4) is true. Here is a proof.

> Let m be an arbitrary integer.
>
> We want to prove that $(\exists n \in \mathbb{Z})n < m$.
>
> For this purpose, we produce a witness. First we say who the witness is, and then we prove it works, that is, that it really is a witness.
>
> Let $\hat{n} = m - 1$.
>
> Then $\hat{n} \in \mathbb{Z}$ and $\hat{n} < m$. So the integer $\hat{n}$ is a witness for the sentence $(\exists n \in \mathbb{Z})n < m$
>
> Therefore $(\exists n \in \mathbb{Z})n < m$. [Rule $\exists_{prove}$]

Since we have proved that $(\exists n \in \mathbb{Z})n < m$ for an arbitrary integer m, we can conclude that $(\forall m \in \mathbb{Z})(\exists n \in \mathbb{Z})n < m$. [Rule $\forall_{prove}$] **Q.E.D.**

Example 35. Consider the sentence

$$(\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z})n < m\,. \tag{8.5}$$

Is this sentence true or false? If it is true, prove it. If it is false, prove that it is false (that is, prove its negation).

SOLUTION. Sentence (8.5) is false. Here is a proof of its negation, that is, of

$$\sim (\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z})n < m\,. \tag{8.6}$$

We are going to prove (8.6) by contradiction .

Assume that

$$(\exists n \in \mathbb{Z})(\forall m \in \mathbb{Z})n < m\,. \tag{8.7}$$

Pick a witness for Statement (8.7), that is, an integer n for which the statement "$(\forall m \in \mathbb{Z})n < m$" holds, and call it n_0. [Rule $\exists_{use}$]

Then $n_0 \in \mathbb{Z}$ and $(\forall m \in \mathbb{Z})n_0 < m$.

Since $n_0 \in \mathbb{Z}$, we can conclude that $n_0 < n_0$. [Rule $\forall_{use}$, from $(\forall m \in \mathbb{Z})n_0 < m$]

Then $\sim n_0 = n_0$. [Trichotomy law]

But $n_0 = n_0$. [Equality Axiom $(\forall x)x = x$.]

So $n_0 = n_0 \wedge n_0 < n_0$. [Rule $\wedge_{prove}$]

So $n_0 = n_0 \wedge (\sim n_0 = n_0$, which is a contradiction.

So we have proved a contradiction assuming (8.7). Hence, by the proof-by-contradiction rule, (8.7) is false, that is, (8.6) is true. **Q.E.D.**

Problem 30. *For each of the following sentences,*

1. *Indicate whether the sentence is true or false.*
2. *If it is true, prove it.*
3. *If it is false, prove that it is false (that is, prove its negation).*

$$(\forall m \in \mathbb{Z})(\exists n \in \mathbb{N})n > m\,, \tag{8.8}$$
$$(\forall m \in \mathbb{N})(\exists n \in \mathbb{N})n < m\,, \tag{8.9}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{Z})n < m\,, \tag{8.10}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})n < m\,, \tag{8.11}$$
$$(\exists n \in \mathbb{N})(\forall m \in \mathbb{N})n \le m\,, \tag{8.12}$$
$$(\exists x \in \mathbb{R})(\forall m \in \mathbb{N})x < m\,. \tag{8.13}$$

8.4 Existence and uniqueness

Suppose $P(x)$ is a one-variable predicate. We write

$$(\exists! x)P(x)$$

for "there exists a unique x such that $P(x)$."

This means "there is one and only one x such that $P(x)$".

The precise meaning of this is that

1. there exists an x such that $P(x)$,

and

2. if x_1, x_2 are such that $P(x_1) \wedge P(x_2)$, then $x_1 = x_2$.

In formal language:

$$(\exists! x)P(x) \iff \Big((\exists x)P(x) \wedge (\forall x_1)(\forall x_2)(P(x_1) \wedge P(x_2)) \Longrightarrow x_1 = x_2\Big)\,.$$

It follows that, in order to prove that there exists a unique x such that $P(x)$, you must prove two things:

Existence: There exists x such that $P(x)$,

Uniqueness: Any two x's that satisfy $P(x)$ must be equal.

That is:

To prove

$$(\exists! x)P(x)$$

it suffices to prove

$$(\exists x)P(x) \tag{8.14}$$

and

$$(\forall x_1)(\forall x_2)\Big((P(x_1) \wedge P(x_2)) \Longrightarrow x_1 = x_2\Big)\,. \tag{8.15}$$

(Formula (8.14) is the <u>existence</u> assertion, and Formula (8.15) is the <u>uniqueness</u> assertion.)

Example 36. "I have one and only one mother" means:

- I have a mother,

and

- Any two people who are my mother must be the same person. (That is: if u is my mother and v is my mother than $u = v$.) □

8.4.1 An example of a proof of existence and uniqueness

Problem 31. *Prove that there exists a unique natural number n such that $n^3 = 2n - 1$.*

Solution. We want to prove that

$$(\exists! n \in \mathbb{N}) n^3 = 2n - 1\,.$$

First let us prove existence. We have to prove that $(\exists n \in \mathbb{N}) n^3 = 2n - 1$. To prove this, we exhibit a witness: we take $n = 1$. Then n is a natural number, and $n^3 = 2n - 1$. So $(\exists n \in \mathbb{N}) n^3 = 2n - 1$.

Next we prove uniqueness. We have to prove that if u, v are natural numbers such that $u^3 = 2u - 1$ and $v^3 = 2v - 1$, then it follows that $u = v$.

So let u, v be natural numbers such that $u^3 = 2u - 1$ and $v^3 = 2v - 1$. We want to prove that $u = v$.

Since $u^3 = 2u - 1$ and $v^3 = 2v - 1$, we have

$$\begin{aligned} u^3 - v^3 &= 2u - 1 - (2v - 1) \\ &= 2u - 2v \\ &= 2(u - v)\,, \end{aligned}$$

so

$$u^3 - v^3 - 2(u - v) = 0\,.$$

But it is easy to verify that

$$u^3 - v^3 = (u - v)(u^2 + uv + v^2)\,.$$

(If you do not believe this, just multiply out the right-hand side and you will find that the result equals $u^3 = v^3$.) Hence

$$\begin{aligned} 0 &= u^3 - v^3 - 2(u - v) \\ &= (u - v)(u^2 + uv + v^2) - 2(u - v) \\ &= (u - v)(u^2 + uv + v^2 - 2)\,. \end{aligned}$$

We know from a previous set of lectures that if a product of two real numbers is zero then one of the numbers must be zero. Hence

$$u - v = 0 \quad \text{or} \quad u^2 + uv + v^2 - 2\,.$$

But $u^2 + uv + v^2 - 2$ cannot be equal to zero, because u^2, uv and v^2 are natural number, so each of them is gretar than or equal to 1, and then $u^2 + uv + v^2 \geq 3$, so $u^2 + uv + v^2 - 2 \geq 1$, and then $u^2 + uv + v^2 - 2 \neq 0$. Therefore $u - v = 0$, so $u = v$, and our proof of uniqueness is complete.

Problem 32. *Prove that there exists a unique real number x such that*

$$x^7 + 3x^5 + 23x = 6\,.$$

You are allowed to use everything you know from Calculus. □

9 Some examples of wrong proofs: finding the point where the author cheated

In the following problems. you are asked to find what is wrong with a proof. In some cases, the result proved may be true, in some others it may be false, and in each case you may or may not be told if the result is true or false. But if the result is false this only telis us that the proof must be wrong somewhere, but it does not tell us where[2]. You job is to figure out exactly which step or steps are wrong. Usually, it is only one step that is wrong, but one wrong step is enough to invalidate a whole proof.

Please do not say vague generalities like "the author does not explain things clearly", or "some steps are not justified".

[2] Think of the fvollowing analogy: If you are supposed to drive from Piscataway to Boston, and end up in Baltimore, then you know for sure that you must have made a wrong turn somewhere, but this does not tell you ***where*** you made a wrong turn. I am asking you to tell me not just that you made a wrong turn somewhere, but exactly where it was that you made the wrong turn.

These are not proof mistakes, they are just imperfections of the writing.

You should show true mistakes. And be precise and specific. Say things such as, for example, "step such and such is invalid because you cannot cancel the c in '$ac = bc$' if you don't know that $c \neq 0$", or "because you cannot multiply two inequalities if you do not know that the numbers involved are positive", or "because it is not true that the sum of two irratioanal numbers is irrational."

And please don't say "the proof is wrong because the result is false". If the result is false, then that tells you that the proof must contain at least one invalid step. But the question here is not "how do you know that the proof must be wrong?", but "where did the author cheat by violating the rules?"

Problem 33. ***Determine*** *what is wrong with the following proof. (The result proved is false, So something must be worng with the proof.)*

"Theorem." If x, y are even integers, then $x + y$ is divisible by 4.

This statement is clearly false. *(To see this, just take $x = 2$ and $y = 4$. Then x and y are even, but $x + y = 6$, which is not divisible by 4.)* ***So it is not possible to prove it****, because anything that can be proved is true, provided that the proof is correct. Therefore,* ***any purported proof must be wrong.***

Here is the "proof":

Let x, y be arbitrary integers.

Assume x is even and y is even.

Then x is even, so $(\exists k \in \mathbb{Z})x = 2k$.

And y is even, so $(\exists k \in \mathbb{Z})y = 2k$.

Since $x = 2k$ and $y = 2k$, we have $x + y = 2k + 2k = 4k$.

So $x + y$ is divisible by 4. *[Definition of "divisible"]*

Q.E.D.

Problem 34. ***Determine*** *what is wrong with the following "proof".*

NOTE: This is a famous example, known as "the Peano Paradox". so named after the very important Italoian mathematician Giuseppe Peano (1858-1932).

"Theorem". 1 is the largest natural number.

Proof.

Let n *be the largest natural number.*

Then $n^2 \in \mathbb{N}$ *[Because if* $n \in \mathbb{N}$ *then* $n^2 \in \mathbb{N}$*]*

And $n^2 \leq n$ *[Because* n *is the largest natural number, so* n^2 *cannot be larger than* n*, so* $n^2 \leq n$*]*

But $n^2 \geq n$ *[Because* $n \geq 1$*, since* $n \in \mathbb{N}$*, so* $n^2 \geq n$*]*

So $n^2 = n$ *[Because* $n^2 \geq n$ *and* $n^2 \leq n$*]*

So $n^2 - n = 0$ *[adding* $-n$ *to both sides]*

But $n^2 - n = n(n-1)$ *[Trivial]*

So $n(n-1) = 0$*.*

So $n = 0 \vee n - 1 = 0$ *[Because if* $x \in \mathbb{Z}$*,* $y \in \mathbb{Z}$*, and* $xy = 0$*, them* $x = 0 \vee y = 0$*]*

So $n = 0$ *or* $n = 1$*.* *[Trivial]*

But $n \neq 0$ *[Because* $n \in \mathbb{N}$ *and* $0 \notin \mathbb{N}$*]*

So $n = 1$ *[Because* $n = 0 \vee n = 1$ *and* $n \neq 0$*]*

So 1 *is the largest natural number.*

Q.E.D.

Problem 35.

1. ***Determine*** *what is wrong with the followinf proof.*
2. ***Determine*** *if the statement of the theorem is true or false*

3. If it is true, give a correct proof.

*4. If it is false, **prove** that its is false.*

"Theorem". If n is a natural number then $n^2 + n + 41$ is a prime number.

Here is the proof:

- *For* $n = 1$, $n^2 + n + 41 = 43$, *and* 43 *is prime.*
- *For* $n = 2$, $n^2 + n + 41 = 47$, *and* 47 *is prime.*
- *For* $n = 3$, $n^2 + n + 41 = 53$, *and* 53 *is prime.*
- *For* $n = 4$, $n^2 + n + 41 = 61$, *and* 61 *is prime.*
- *For* $n = 5$, $n^2 + n + 41 = 71$, *and* 71 *is prime.*
- *For* $n = 6$, $n^2 + n + 41 = 83$, *and* 83 *is prime.*
- *For* $n = 7$, $n^2 + n + 41 = 97$, *and* 97 *is prime.*
- $\cdots$
- *Similarly, for* $n = 8, 9, 10$ *and so on,* $n^2 + n + 41$ *is prime.*

So $(\forall n \in \mathbb{N})n^2 + n + 41 \text{ is prime}$. **Q.E.D.**

Problem 36. ***Determine*** *what is wrong with the followinf proof.*

"Theorem". If n is a natural number and $p_1, p_2, \ldots, p_n$ are n distinct primes, then $\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n}$ is irrational.

In this case, the theorem is true, but the proof below is wrong. Giving a correct proof is hard.

Here is a wrong proof.
For $n = 1$, *we have to prove that if* p_1 *is a prime number then* $\sqrt{p_1}$ *is irrational.*

But this follows by the usual Euclid'a Lemma argument: suppose $\sqrt{p_1}$ *was rational. Write* $\sqrt{p_1} = \frac{m}{n}$, *where* m *and* n *are nonzero integers with no nontrivial common factors. Then* $p_1 n^2 = m^2$. *So* $p_1 | m^2$. *By Euclid's lemma,* $p_1 | m$. *Then* p_1 *must dvide* n^2, *so* p_1 *divides* m. *So* m, n *have a common factor, and this is a contradiction.*

Now let us look at the case $n = 2$. We have to prove that if p_1, p_2 are primes and $p_1 \neq p_2$, and $r = \sqrt{p_1} + \sqrt{p_2}$, then r is irrational. Suppose r was rational. Then

$$\begin{aligned} r^2 &= \left(\sqrt{p_1} + \sqrt{p_2}\right)^2 \\ &= p_1 + p_2 + 2\sqrt{p_1 p_2}\,, \end{aligned}$$

so $\sqrt{p_1 p_2} = \frac{r^2 - p_1 - p_2}{2}$, and then $\sqrt{p_1 p_2}$ is rational.

But $\sqrt{p_1 p_2}$ is irrational. (This is proved by the same Euclid lemma argument as for $\sqrt{p_1}$.)

So we reached a contradiction. So $\sqrt{p_1} + \sqrt{p_2}$ is irrational.

Similarly, $\sqrt{p_1} + \sqrt{p_2} + \sqrt{p_3}$, $\sqrt{p_1} + \sqrt{p_2} + \sqrt{p_3} + \sqrt{p_4}$, and so on, are irrational. **Q.E.D.**

10 Examples of proofs by induction

10.1 Divisibility properties of products of consecutive integers

We now discuss several theorems on divisibility of a product of consecutive integers:

1. We will look first at the case of a product $n(n + 1)$ of two consecutive integers, and prove the trivial result that such a product is divisible by 2.

2. We will then look at the product $n(n + 1)(n + 2)$ of three consecutive integers, and prove that such a product is divisible by 6.

3. Then we will look at the product $n(n + 1)(n + 2)(n + 3)$ of four consecutive integers, and prove that such a product is divisible by 24.

4. Since $2 = 2 \times 1 = 2!$, $6 = 3 \times 2 \times 1 = 3!$, and $24 = 4 \times 3 \times 2 \times 1 = 4!$, this will clearly be a good indication that there is a general pattern, namely, that for every natural number k the product of k consecutive integers is divisble by $k!$. (The ***factorial*** $m!$ of a natural number m will be defined in the next section, using the following inductive definition:

$1! = 1$ and $(n+1)! = n! \times (n+1)$ for $n \in \mathbb{N}$.) In other words, the general result should be that

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})k! \Big| n(n+1)(n+2)\cdots(n+k-1) \qquad (10.16)$$

or, using a notation without the mysterious and incomprehensible symbol "$\cdots$":

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})k! \Big| \prod_{j=1}^{k}(n+j-1) \qquad (10.17)$$

5. And we will indeed prove (10.17) eventually, but the proof will be little but harder than other proofs we have done so far, because it will use a ***double induction***: we will prove (10.17) by induction with respect to k, and for each k we will need induction with respect to n.

First let us start with the trivial result for $k = 2$:

Theorem 40. *If n is an integer, then $n(n+1)$ is even, i.e., divisible by 2. That is,*

$$(\forall n \in \mathbb{N})2|n(n+1)\,. \qquad (10.18)$$

Proof. As I said earlier, this result is trivial.

Let n be an arbitrary integer.

We know that n is either even or odd. (This follows from Theorem 26 on Part II of the notes.)

If n is even then $\boxed{n(n+1) \text{ is even}}$.

And if n is odd then $n+1$ is even so $\boxed{n(n+1) \text{ is even}}$.

So we have proved that $n(n+1)$ is even in both cases, when n is even and when n is odd. And we know that one of these two cases must occur. So $\boxed{\boxed{n(n+1) \text{ is even}}}$.

So we have proved that $n(n+1)$ is even for an arbitrary integer n.

Hence $\boxed{\boxed{\boxed{(\forall n \in \mathbb{Z})n(n+1) \text{ is even}}}}$. **Q.E.D.**

We now want to prove that the product $n(n+1)(n+2)$ of three consecutive integers is divisible by 6. And the strategy is going to be to prove the result first by induction for natural numbers n, and then use a very simple argument to derive the result for an arbitrary integer n.

So here is the result for natural numbers.

Theorem 41. *If n is a natural number, then $n(n+1)(n+2)$ is divisible by 6. That is,*

$$(\forall n \in \mathbb{N})6|n(n+1)(n+2)\,. \tag{10.19}$$

Proof. Let $P(n)$ be the statement "$6|n(n+1)(n+2)$"

We prove that $(\forall n \in \mathbb{N})P(n)$ by induction.

Basis step. If $n = 1$, then $n(n+1)(n+2) = 6$, so $P(1)$ is the statement "$6|6$", which is obviously true. So $\boxed{P(1)}$ is true.

PARENTHESES MATTER!!!

The sentence

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \qquad \text{(a)}$$

is not at all the same as the sentence

$$(\forall n \in \mathbb{N})P(n) \Longrightarrow P(n+1)\,. \qquad \text{(b)}$$

Sentence (a) says that the implication "$P(n) \Longrightarrow P(n+1)$" (that is, "$P$ is passed on from n to $n+1$") is true for every natural number n. So (a) says "every natural number passes on Property P to its successor".

Sentence (b) is totally different. It says: "if it is true that all natural numbers have P then $n+1$ has P". This is in fact meaningless, because n is an open variable.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \tag{10.20}$$

Let n be an arbitrary natural number.

We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.
Then 6 divides $n(n+1)(n+2)$.
So we may pick an integer k such that $n(n+1)(n+2) = 6k$.
And $n(n+1)$ is even. (Reason: Theorem 40.)
So we may pick an integer j such that $(n+1)(n+2) = 2j$.
Then

$$\begin{aligned}(n+1)(n+2)(n+3) &= (n+1)(n+2)\times 3 + (n+1)(n+2)\times n\\ &= 3(n+1)(n+2) + n(n+1)(n+2)\\ &= 3\times 2j + 6k\\ &= 6j + 6k\\ &= 6(j+k)\,.\end{aligned}$$

So 6 divides $(n+1)(n+2)(n+3)$.
That is, $P(n+1)$ golds.

Hence we have proved that $P(n) \Longrightarrow P(n+1)$.

Since we have proved that $P(n) \Longrightarrow P(n+1)$ for arbitrary n, we conclude that (10.20) holds.
Then it follows from the PMI that $\boxed{\text{(10.19) holds}}$. **Q.E.D.**

And now let us prove the result for all integers.

Corollary 2. *If n is an integer, then $n(n+1)(n+2)$ is divisible by 6. That is,*

$$(\forall n\in\mathbb{Z})6|n(n+1)(n+2)\,. \tag{10.21}$$

Proof. Let n be an arbitrary integer.
Then either $n \in \mathbb{N}$, or $n = 0$, or $-n \in \mathbb{N}$.
We analyze separately each of these three cases.

$\boxed{\text{If } n\in\mathbb{N}}$, then we know from Theorem 41 that $\boxed{6|n(n+1)(n+2)}$.

$\boxed{\text{If } n=0}$, then $n(n+1)(n+2) = 0$, so $\boxed{6|n(n+1)(n+2)}$.

Now suppose that $-n \in \mathbb{N}$.
Let[3] $\nu = -n-2$.

[3] Why do we introduce this ν? Just look at an example: suppose $n = -5$; then $n(n+1)(n+2) = (-5)(-4)(-3)$, so $n(n+1)(n+2) = -5\times 4\times 3$, that is, $n = -\nu(\nu+1)(\nu+2)$, if we let $\nu = 3$, that is, $\nu = -n-2$.

Then $-n = \nu + 2$, so $n = -(\nu + 2)$.
Also, $-n - 1 = \nu + 1$, so $n + 1 = -(\nu + 1)$.
And $-n - 2 = \nu$, so $n + 2 = -\nu$.
Hence $n(n+1)(n+2) = -(\nu + 2) \times \Big(-(\nu + 1)\Big) \times (-\nu)$, so

$$n(n+1)(n+2) = -(\nu + 2)(\nu + 1)\nu\,.$$

and then

$$n(n+1)(n+2) = -\nu(\nu + 1)(\nu + 2)\,. \tag{10.22}$$

Now, ν could be a natural number or not[4].
$\boxed{\text{If } \nu \text{ is a natural number}}$, then Theorem 41 tells us that $\nu(\nu+1)(\nu+2)$ is divisible by 6, and then (10.22) implies that $\boxed{6|n(n+1)(n+2)}$ as well.
What if ν is not a natural number? In any case, ν is an integer, because $\nu = -n-2$ and $n \in \mathbb{Z}$. So the only way that ν could fail to be a natural number is if $\nu \leq 0$. For this to happen, we must have $-n - 2 \leq 0$, i.e., $-n \leq 2$. So we have shown that if ν is not a natural number then the natural number $-n$ must be 1 or 2.
$\boxed{\text{If } -n = 1}$, then $n + 1 = 0$, so the product $n(n+1)(n+2)$ is equal to zero, and zero is divisbile by 6, so $\boxed{n(n+1)(n+2) \text{ is divisible by } 6}$.
If $\boxed{-n = 2}$, then $n + 2 = 0$, so the product $n(n+1)(n+2)$ is equal to zero, and zero is divisible by 6, so $\boxed{n(n+1)(n+2) \text{ is divisible by } 6}$.

Summarizing, we have shown that

- There are five possibiltiies, namely, $n \in \mathbb{N}$, $n = 0$, $-n = 1$, $-n = 2$, and $\nu \in \mathbb{N}$.
- In all five cases, $n(n+1)(n+2)$ is divisible by 6.

[4] Suppose, for example, that $n = -1$. Then $-n - 2 = 1 - 2 = -1$, so ν is not a natural number. Also, if $n = -2$, then $-n - 2 = 2 - 2 = 0$, so ν is not a natural number either. But, if $n = -3$ then $-n - 2 = 3 - 2 = 1$, ν is a natural number. And the same is true if $n = -4$, or -5, etc. So the only possible cases when ν is not a natural number are when $n = -1$ or $n = -2$.

So $\boxed{\boxed{n(n+1)(n+2) \text{ is divisible by } 6}}$. **Q.E.D.**

Similar results can be proved for the products of four and five consecutive integers.

Theorem 42. *If n is a natural number, then $n(n+1)(n+2)(n+3)$ is divisible by 24. That is,*

$$(\forall n \in \mathbb{Z}) 24 | n(n+1)(n+2)(n+3)\,. \tag{10.23}$$

Proof. **YOU DO THIS ONE.**

Corollary 3. *If n is an integer, then $n(n+1)(n+2)(n+3)$ is divisible by 24. That is,*

$$(\forall n \in \mathbb{Z}) 24 | n(n+1)(n+2)(n+3)\,. \tag{10.24}$$

Proof. **YOU DO THIS ONE.**

Problem 37. ***Prove*** *Theorem 42 and Corollary 3.* □

Theorem 43. *If n is a natural number, then $n(n+1)(n+2)(n+3)(n+4)$ is divisible by 120. That is,*

$$(\forall n \in \mathbb{Z}) 120 | n(n+1)(n+2)(n+3)(n+4)\,. \tag{10.25}$$

Proof. **YOU DO THIS ONE.**

Corollary 4. *If n is an integer, then $n(n+1)(n+2)(n+3)(n+4)$ is divisible by 120. That is,*

$$(\forall n \in \mathbb{Z}) 6 | n(n+1)(n+2)(n+3)(n+4)\,. \tag{10.26}$$

Proof. **YOU DO THIS ONE.**

Problem 38. ***Prove*** *Theorem 43 and Corollary 4.* □

10.2 Inductive definitions

In an earlier set of lectures, we defined "x^2", for a real number x, to mean "$x.x$". And we can define "x^3" to mean "$(x.x).x$", or, if you prefer, "$x^2.x$". But how can we define "x^n" for an arbitrary natural number n? One possibility would be to write something like this

$$x^n = \underbrace{x \times x \times \cdots \times x}_{n \text{ times}}$$

Similarly, we would like to define the "factorial" $n!$ of a natural number n by the formula

$$n! = 1 \times 2 \times 3 \times \cdots \times n\,.$$

And we would like to define summations such as

$$1 + 2 + 3 + \cdots + n$$

or

$$1^2 + 2^2 + 3^2 + \cdots + n^2\,,$$

or products such that

$$2 \times 4 \times 6 \times 8 \times \cdots \times 200\,.$$

With this notation, if we want to talk about the product of the first 20 prime numbers, i.e., the number

$$2\times3\times5\times7\times11\times13\times17\times19\times23\times29\times31\times37\times41\times43\times47\times53\times59\times61\times67\times71\,,$$

we could write

$$2 \times 3 \times \cdots \times 71\,. \tag{10.27}$$

But this is very unclear. I do not know what "$\cdots$" means, precisely (and if you think you do, please tell me!). For example, in the expression (10.27), how on Earth are we supposed to know which numbers should go in place of the $\cdots$? Take a simple example of a similar situation: suppose I write

$$3 \times 5 \times 7 \times \cdots \times 71\,. \tag{10.28}$$

Is this supposed to be "the product of all odd numbers from 3 to 71", or "the product of all prime numbers from 3 to 71", or "the product of all the odd numbers from 3 to 71 that do not end in a 9", or what?

Next, let us look at another example: suppose I write

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, \ldots.$$

What is the next number, after 377? Well, if you have guessed the pattern, then you will probably guess that each number, after the first two, is the sum of the two preceding ones, so what comes after 377 is $233 + 377$, that is, 610. But, why coudn't the pattern be this:

- Start with 1, and then another 1.
- Then each number is obtained by adding the two preceding ones.
- Yo go on like this until you get to 377, and then you switch to a different rule: each number is obtained by adding 100 to the previous one.

This is a perfectly legitimate rule for generating a sequence of numbers, and if you use this rule then the numbers that come after 377 are 477, 577, and so on. If you say "that's not a true pattern", then I will ask you to tell me what you mean by "a true pattern", and I will also ask "why cannot we use other patterns that aren't "true" as well as true ones?

One last example. If I write

$$27, 82, 41, 124, 61, 184, 92, 46, \cdots$$

what comes next? I'll let you think about this one.

The fact is: in general, "$\cdots$" is meaningless. So in mathematics we just do not use it.

And, in any case, once we develop fully our way of writing all of mathematics formally (that is, with formulas and no words), the symbol "$\cdots$" will not be there in the list of symbols we can use. So we do not want to use "$\cdots$" at all.

What we are going to do instead is use ***inductive definitions***.

10.2.1 The inductive definition of powers of a real number

The way to define "x^n" correctly is by means of an inductive definition: we first define x^1 to be x, and then define x^{n+1} to be $x^n.x$, for every n. That is, we write:

Definition 20. ***(Inductive definition of positive integer powers of a real number)*** For all $a \in \mathbb{R}$, we set

$$\begin{array}{rcl} a^1 & = & a\,, \\ a^{n+1} & = & a^n.a \quad \text{for } \; n \in \mathbb{N}\,. \end{array}$$

We also set $a^0 = 1$. □

Using this definition, we can write down what a^n is for any n.

Suppose, for example, that we want to know what a^5 is. By the second line of our inductive definition of a^n,

$$a^5 = a^4.a.$$

This answers our question about a^5, in terms of a^4. And what is a^4? Again, using the second line of the inductive definition, we find

$$a^4 = a^3.a.$$

So

$$a^5 = ((a^3).a).a.$$

And what is a^3? Once again, we can use the second line of the inductive definition, and find

$$a^3 = a^2.a$$

So

$$a^5 = (((a^2).a).a).a.$$

One more step yields

$$a^2 = a^1.a\,,$$

so

$$a^5 = (((a^1.a).a).a).a.$$

And, finally, the first line of the inductive definition, tells us that $a^1 = a$, so we end up with

$$a^5 = (((a.a).a).a).a.$$

Furthermore, since multiplication of real numbers has the associative property, we can omit the parentheses and just write:

$$a^5 = a.a.a.a.a.$$

10.2.2 The inductive definition of the factorial

The "factorial" of a natural number n is supposed to be the product $1 \times 2 \times 3 \times \cdots \times n$. That is, the factorial of n is the product of all the natural numbers from 1 to n. Here is the inductive definition:

Definition 21. The factorial of a natural number n is the number $n!$ given by

$$\begin{aligned} 1! &= 1\,, &(10.29)\\ (n+1)! &= n! \times (n+1) \quad \text{for } \ n \in \mathbb{N}\,. &(10.30)\end{aligned}$$

In addition, we define

$$0! = 1\,,$$

so $n!$ is defined for every nonnegative integer n. □

Example 37. Let us compute 7! using the inductive definition. Using (10.30) we get $7! = 7\times 6!$. Then using (10.30) again we get $6! = 6\times 5!$, so $7! = 7\times 6\times 5!$. Continuing in the same way we get $5! = 5\times 4!$, so $7! = 7\times 6\times 5\times 4!$, and then $4! = 4\times 3!$, so $7! = 7\times 6\times 5\times 4\times 3!$. Then $3! = 3\times 2!$, so $7! = 7\times 6\times 5\times 4\times 3\times 2!$. And $2! = 2\times 1!$, so $7! = 7\times 6\times 5\times 4\times 3\times 2\times 1!$. Finally, (10.29) tells us that $1! = 1$, so we end up with

$$7! = 7\times 6\times 5\times 4\times 3\times 2\times 1\,,$$

which is of course what 7! is supposed to be. □

10.2.3 The inductive definition of summation.

Definition 22. Suppose we have a natural number n, and a list

$$\mathbf{a} = (a_1, a_2, \ldots, a_n)$$

of n real numbers. We define the sum (or summation) of the list $\mathbf{a}$ (also called the sum of the a_j for j from 1 to n) to be the number $\sum_{j=1}^{n} a_j$ determined as follows:

$$\begin{aligned} \sum_{j=1}^{1} a_j &= a_1\,,\\ \sum_{j=1}^{n+1} a_j &= \Big(\sum_{j=1}^{n} a_j\Big) + a_{n+1} \quad \text{for} \quad n \in \mathbb{N}\,.\end{aligned}$$

And we also define $\sum_{j=1}^{0} a_j = 0$.

Example 38. Let us compute $\sum_{j=1}^{5} j^2$. We have

$$\begin{aligned}
\sum_{j=1}^{5} j^2 &= \Big(\sum_{j=1}^{4} j^2\Big) + 5^2 \\
&= \Bigg(\Big(\sum_{j=1}^{3} j^2\Big) + 4^2\Bigg) + 5^2 \\
&= \Big(\sum_{j=1}^{3} j^2\Big) + 4^2 + 5^2 \\
&= \Big(\sum_{j=1}^{2} j^2\Big) + 3^+4^2 + 5^2 \\
&= \Big(\sum_{j=1}^{1} j^2\Big) + 2^2 + 3^+4^2 + 5^2 \\
&= 1^2 + 2^2 + 3^+4^2 + 5^2 \\
&= 1 + 4 + 9 + 16 + 25 \\
&= 55\,.
\end{aligned}$$

10.2.4 Inductive definition of product.

Definition 23. For a natural number n, and a list $\mathbf{a} = (a_1, a_2, \ldots, a_n)$ of n real numbers, we define the product of the a_j for j from 1 to n to be the number $\prod_{j=1}^{n} a_j$ determined as follows:

$$\begin{aligned}
\prod_{j=1}^{1} a_j &= a_1\,, \\
\prod_{j=1}^{n+1} a_j &= \Big(\prod_{j=1}^{n} a_j\Big) \times a_{n+1} \quad \text{for} \quad n \in \mathbb{N}\,.
\end{aligned}$$

And we also define $\prod_{j=1}^{0} a_j = 1$.

Example 39. If you compare the inductive definition of a product with the inductive definition of the factorial, you can easily see that

$$n! = \prod_{j=1}^{n} j \qquad \text{for every } n \in \mathbb{N}\,.$$

10.2.5 A simple example of a proof by induction using inductive definitions

Here is a simple example of a proof of an inequality by induction. Notice how the proof uses the notion of "n-th power" of a real number exactly in the form of the inductive definition.

Proposition 1. *For all $n \in \mathbb{N}$, $n < 2^n$.*

Proof.
Let $P(n)$ be the statement "$n < 2^n$".
We are going to prove

$$(\forall n \in \mathbb{N}) P(n) \tag{10.31}$$

by induction

Basis step. $P(1)$ is the statement "$1 < 2^1$". But $2^1 = 2$ by the inductive definition, so $P(1)$ says "$1 < 2$" which is clearly true. So $\boxed{P(1)}$ is true.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \tag{10.32}$$

> Let n be an arbitrary natural number.
>
> We want to prove that $P(n) \Longrightarrow P(n+1)$.
>
> > Assume $P(n)$.
> >
> > Then $n < 2^n$.
> >
> > So $2n < 2^n \times 2 = 2^{n+1}$.
> >
> > But $1 \le n$, because n is a natural number. (Precisely: if $n = 1$ then $1 = n$, so $1 \le n$. And if $n \neq 1$ then ny Basic Fact BFZ9, $n - 1 \in \mathbb{N}$, so $1 < n$, and then $1 \le n$.)
> >
> > So $n + 1 \le n + n$, i.e., $n + 1 \le 2n$.

Therefore $n+1 < 2^{n+1}$.

So $P(n+1)$ is true.

Since we have proved $P(n+1)$ assuming $P(n)$, we can conclude that $P(n) \Longrightarrow P(n+1)$.

Since we have proved $P(n) \Longrightarrow P(n+1)$ for arbitrary n, it follows that (10.32) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (10.31 holds, that is, that $(\forall n \in \mathbb{N})n < 2^n$. **Q.E.D.**

10.2.6 Induction with a different starting point

The PMI says that, if a property is true of 1, and is passed on to the right, so each number n passes it on to its successor $n+1$, then the property will hold of all the numbers that we reach by counting starting at 1.

It is clearthat the same thing should be true if we start counting at some other integer, such as, for example, 3, or 7, or 0, or -5, or -372. The general principle is the following rather trivial theorem:

Theorem 44. *Let $P(n)$ be a sentence having n as an open variable, and let n_* be an integer. Suppose that the following are true:*

1. *$P(n_*)$ is true.*
2. *If n is an arbitrary integer such that $n \geq n_*$, then $P(n) \Longrightarrow P(n+1)$.*

Then $P(n)$ is true for all integers n such that $n \geq n_*$.

The same theorem stated in more formal language. Let $P(n)$ be a sentence having n as an open variable, and let $n_* \in \mathbb{Z}$. Suppose that the following are true:

1. $P(n_*)$.
2. $(\forall n \in \mathbb{Z})\Big(n \geq n_* \Longrightarrow \big(P(n) \Longrightarrow P(n+1)\big)\Big)$.

Then $(\forall n \in \mathbb{Z})\big(n \geq n_* \Longrightarrow P(n)\big)$.

The same theorem stated in even more formal language. Let $P(n)$ be a sentence having n as an open variable, and let $n_* \in \mathbb{Z}$. Then

$$\Bigg(P(n_*) \wedge (\forall n \in \mathbb{Z})\Big(n \geq n_* \Longrightarrow \big(P(n) \Longrightarrow P(n+1)\big)\Big)\Bigg)$$
$$\Longrightarrow (\forall n \in \mathbb{Z})\Big(n \geq n_* \Longrightarrow P(n)\Big)\,.$$

The same theorem stated in disgustingly formal language. Let $P(n)$ be a sentence having n as an open variable. Then

$$(\forall n_* \in \mathbb{Z})\Bigg[\Bigg(P(n_*) \wedge (\forall n \in \mathbb{Z})\Big(n \geq n_* \Longrightarrow \big(P(n) \Longrightarrow P(n+1)\big)\Big)\Bigg)$$
$$\Longrightarrow (\forall n \in \mathbb{Z})\Big(n \geq n_* \Longrightarrow P(n)\Big)\Bigg]\,.$$

Proof.

Let n_* be an arbitrary integer.

We want to prove that “induction startiong at n_* works”.

That is, we want to prove that if

$$P(n_*) \wedge (\forall n \in \mathbb{Z})\Big(n \geq n_* \Longrightarrow \big(P(n) \Longrightarrow P(n+1)\big)\Big) \qquad (10.33)$$

then

$$(\forall n \in \mathbb{Z})\big(n \geq n_* \Longrightarrow P(n)\big)\,. \qquad (10.34)$$

(That is: “if $P(n_*)$ is true, and each number to the right of n_* passes on P to its successor, then all the numbers to the right of n_* have P”.)

Assume that (10.33) is true.
Then in particular $P(n_*)$ is true. (That is, the starting number n_* has property P.)
And

$$(\forall n \in \mathbb{Z})\Big(n \geq n_* \Longrightarrow \big(P(n) \Longrightarrow P(n+1)\big)\Big)\,. \qquad (10.35)$$

(That is, every integer n greater than or equal to n_* passes on P to its successor.)

We want to prove that (10.34) is true.
Let $Q(n)$ be the statement[5] "$P(n_* + n - 1)$".
We are going to prove by induction that $(\forall n \in \mathbb{N})Q(n)$.

Basis step. We have to prove that $Q(1)$ is true.
But $Q(1)$ says "$P(n_*)$", and we are assuming that $P(n_*)$ is true.
So $\boxed{Q(1) \text{ is true}}$.
This completes the basis step.
Inductive step. We have to prove that

$$(\forall n \in \mathbb{N})\big(Q(n) \Longrightarrow Q(n+1)\big)\,. \tag{10.36}$$

(That is, each natural number passes on Q to its successor.)

Let n be an arbitrary natural number.

We want to prove that $Q(n) \Longrightarrow Q(n+1)$.

Assume that $Q(n)$ is true.

This means that $P(n_* + n - 1)$ is true.

Now, $n_* + n - 1$ is an integer greater than or equal to n_*, because $n \in \mathbb{N}$.

Therefore, by our assumption (10.35) (which says that every integer greater than or equal to n_* passes on P to its successor), $P(n_* + n)$ is true.

But $P(n_* + n)$ is $Q(n+1)$.

Hence $Q(n+1)$ is true.

So we have proved that $Q(n) \Longrightarrow Q(n+1)$.

Since we have proved that $Q(n) \Longrightarrow Q(n+1)$ for arbitrary n, we can conclude that $\boxed{(\forall n \in \mathbb{N})\big(Q(n) \Longrightarrow Q(n+1)\big)}$, that is, every natural number passes on Q to its successor.

This completes the inductive step.

So, by the PMI, $(\forall n \in \mathbb{N})Q(n)$.

[5] Why do we introduce this particular statement $Q(n)$? The reason is that $Q(1)$ is the same as $P(n_*)$, $Q(2)$ is the same as $P(n_*+)1$, $Q(3)$ is the same as $P(n_* + 2)$, and so on. So proving thet $P(n_*)$, $P(n_* + 1)$, $P(n_* + 2)$, and so on, are all true, amounts to proving that $Q(1)$, $Q(2)$, $Q(3)$ and so on are all true, and this is precisely what the PMI allows us to do.

In other words,

$$(\forall n \in \mathbb{N})P(n_* + n - 1)\,. \qquad (10.37)$$

Remember that what we are trying to prove is that

$$(\forall n \in \mathbb{N})\big(n \geq n_*) \Longrightarrow P(n)\big)\,. \qquad (10.38)$$

(That is, every integer to the right of n_* has P.)

Let n be an arbitrary integer such that $n \geq n_*$.

We want to prove $P(n)$.

Let m be the integer such that

$$n = n_* + m - 1\,.$$

Then

$$m = n - n_* + 1\,.$$

So m is an integer (because n and n_* are integers).

Also, $m \geq 1$ (because $n \geq n_*$).

So $m \in \mathbb{N}$.

But then (10.37) tells us that $P(n_* + m - 1$ is true.

And $n_* + m - 1$ is precisely n.

So $P(n)$ is true.

Since we have proved $P(n)$ for an arbitrary integer n such that $n \geq n_*$, we conclude that

$$(\forall n \in \mathbb{Z})\big(n \geq n_* \Longrightarrow P(n)\big)\,. \qquad (10.39)$$

We have proved that, if the assumptions of the PMI starting at n_* hold (that is, if (10.33) is true), then the conclusion of the PMI starting at n_* holds as well (that is, (10.39) is true).

This completes the proof of the PMI starting at n_*.

And n_* was an arbitrary integer.

So we have proved that

$\boxed{\textbf{\textit{the PMI starting at an arbitrary integer }} n_* \textbf{\textit{ is valid}}}$. **Q.E.D.**

10.2.7 Another simple example of a proof by induction using inductive definitions

Here is a slightly more involved example of a proof of an inequality by induction. Notice how the proof uses the notion of "n-th power" of a real number and the notion of "factorial" exactly in the form of their inductive definitions.

We would like to prove the inequality "$2^n < n!$". This, however, isn't true for every natural number n. (For example, it is not true if $n = 1$ or $n = 2$ or $n = 3$.) But it is true for $n \geq 4$.

Proposition 2. *For all $n \in \mathbb{N}$, if $n \geq 4$ then $2^n < n!$.*

Proof.
Let $P(n)$ be the statement "$2^n < n!$".
We are going to prove

$$(\forall n \in \mathbb{N})(n \geq 4 \Longrightarrow P(n)). \qquad (10.40)$$

by induction. And we will start the induction at 4 rather than 1.

Basis step. $P(4)$ is the statement "$2^4 < 4!$". But $2^4 = 16$, and $4! = 24$. So $P(1)$ says "$16 < 24$', which is clearly true. So $\boxed{P(4)}$ is true.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big). \qquad (10.41)$$

Let n be an arbitrary natural number such that $n \geq 4$..

We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.
Then $2^n < n!$.
So $2 \times 2^n < 2n!$.
But $2 \times 2^n = 2^{n+1}$.
Hence $2^{n+1} < 2n!$.
Also, $2 < n + 1$.
So $2n! < (n+1)n!$.
But $(n+1)n! = (n+1)!$ by the inductive definitionof "factorial".
Therefore $2n! < (n+1)!$.
So, finally, $2^{n+1} < (n+1)!$.
So $P(n+1)$ is true.

> Since we have proved $P(n+1)$ assuming $P(n)$, we can conclude that $P(n) \Longrightarrow P(n+1)$.

Since we have proved $P(n) \Longrightarrow P(n+1)$ for arbitrary n, it follows that (10.41) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (10.40) holds, that is, that $(\forall n \in \mathbb{N})\Big(n \geq 4 \Longrightarrow (2^n < n!)\Big)$.
Q.E.D.

10.2.8 Another simple example

Let us prove

Theorem 45. *If a, b are arbitrary integers, then for every nonnegative integer[6] n the integer $a^n - b^n$ is divisible by $a - b$.*

Example 40. Here are some examples of what the theorem says:

1. Take $a = 8$, $b = 3$. Then the theorem says that $8^n - 3^n$ is divisible by 5 for every n. (And you can check this. For example, $8^3 = 512$, and $3^3 = 27$, so $8^3 - 3^3 = 512 - 27 = 495$, which is indeed divisible by 5.

2. Take $a = 10$, $b = 1$. Then the theorem says that $10^n - 1$ is divisible by 9, and you can check this. (For example, $10^1 - 1 = 9$, $10^2 - 1 = 99$, $10^3 - 1 = 999$, $10^4 - 1 = 9,999$, and so on.)

3. Take $a = 10$, $b = -1$. Then the theorem says that $10^n - (-1)^n$ is divisible by 11. And you can check this: $10-(-1) = 11$, $10^2-(-1)^2 = 99$, $10^3 - (-1)^3 = 1,001$, $10^4 - (-1)^4 9,999$, and all these are divisible by 11. □

Proof.

Let a, b be arbitrary integers.

We will prove that

$$(\forall n \in \mathbb{N}) a - b | a^n - b^n \,, \tag{10.42}$$

and also that "$a - b | a^n - b^n$" is true for $n = 0$.

[6] Recall that the ***nonnegative integers*** are the natural numbers as well as zero.

First we prove (10.42) by induction.

Let $P(n)$ be the statement[7] "$a - b$ divides $a^n - b^n$".

Basis Step. $P(1)$ says "$a - b$ divides $a - b$", which is obviously true.

This completes the basis step.

Inductive Step. We want to rpove

Inductive step. We want to prove that

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \tag{10.43}$$

Let n be an arbitrary natural number.

We want to prove that $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$.

Then $a - b$ divides $a^n - b^n$.

So we may pick an integer k such that

$$a^n - b^n = (a-b)k\,. \tag{10.44}$$

Then

$$\begin{aligned} a^{n+1} - b^{n+1} &= a^{n+1} - ab^n + ab^n - b^{n+1} \\ &= aa^n - ab^n + ab^n - bb^n \\ &= a(a^n - b^n) + (a-b)b^n \\ &= a(a-b)k + (a-b)b^n \\ &= (a-b)\big(ak + b^n\big)\,. \end{aligned}$$

Hence $a^{n+1} - b^{n+1} = (a-b)\big(ak + b^n\big)$.

Clearly, $ak + b^n$ is an integer[8].

Therefore $a - b$ divides $a^{n+1} - b^{n+1}$.

[7] We do not have to worry about the quesion "who are a and b?", because we have fixed a and b earlier. They are fixed integers. Arbitrary, but fixed.

[8] Strictly speaking even a stupid, trivial, obvious statement like this needs proof. On the other hand, it is so obvous that nobody would actually insult the reader's intelligence by putting in the proof. On the other hand, at this point we are just getting started with proofs, so you shousl knwo how to prove this. So I am going to ask you to write down the proof, as a homework problem. ***Sorry!***.

So $P(n+1)$ is true.

Since we have proved $P(n+1)$ assuming $P(n)$, we can conclude that $P(n) \Longrightarrow P(n+1)$.

Since we have proved $P(n) \Longrightarrow P(n+1)$ for arbitrary n, it follows that (10.43) holds.

So we have completed the basis step and the inductive step, and then the PMI tells us that (10.42 holds, that is, that if n is an arbitrary natural number, then $a-b$ divides $a^n - b^n$.

This almost completes our proof. But there is a minor missing detail: we also have to prove that $a-b$ divides $a^n - b^n$ when $n = 0$.

But if $n = 0$ then $a^n - b^n$ is equal to zero, because the inductive definition of the powers tells us that $a^0 = 1$ and $b^0 = 1$.

And 0 is divisble by any integer.

So $a-b$ divides $a^n - b^n$ also when $n = 0$.

We have now proved that $a - b | a^n - b^n$ for every nonnegative integer n.

And this has been proved for arbitrary integers a, b. So our proof is complete. **Q.E.D.**

Problem 39.

1. ***Provide a detailed proof*** *of the step that we skipped in the proof of Theorem 45, namely, that* $ak + b^n$ *is an integer. (This will require proving that if* $b \in \mathbb{Z}$ *then* $b^n \in \mathbb{Z}$ *for every nonnegative integer* n*, and the only way to do that is by induction, using the inductive definition of the powers.)*

2. ***Provide an alternative proof*** *of Theorem 45, in which you do not treat separately the cases* $n \in \mathbb{N}$ *and* $n = 0$*, but do the whole thing in one swoop, using the PMI starting at* 0 *rather than at* 1.

3. ***Explain*** *how you would answer the following objection that somebody studying these notes might raise:* In the theorem, you do not assume that $a \neq b$, and you talk about "divisibility by $a-b$". But if $a = b$ then $a - b$ is zero, and we cannot divide by zero, so how come you allow a

to be equal to b? How can you say that "0 is divisble by 0", given that $\frac{0}{0}$ is not defined? □

Problem 40. *One of the consequences of Theorem 45 is that* $10^n - 1$ *is divisible by* 9 *for each nonnegative integer* n*. So, for example, if you look at the number* 4, 342, 476*, and let* $s = 4+3+4+2+4+7+6$*, so* $s = 30$*, it follows that* $4,342,476 - s$ *is divisible by* 9*, because:*

$$\begin{aligned}
&4,342,476 - s \\
&= 4\times 10^6 + 3\times 10^5 + 4\times 10^4 + 2\times 10^3 + 4\times 10^2 + 7\times 10^1 \\
&\quad +6\times 10^0 - (4+3+4+2+4+7+6) \\
&= (4\times 10^6 - 4) + (3\times 10^5 - 3) + (4\times 10^4 - 4) \\
&\quad +(2\times 10^3 - 2)(4\times 10^2 - 4) + (7\times 10^1 - 7) + (6\times 10^0 - 6) \\
&= 4\times (10^6 - 1) + 3\times (10^5 - 1) + 4\times (10^4 - 1) \\
&\quad +2\times (10^3 - 1) + 4\times (10^2 - 1) + 7\times (10^1 - 1) + 6\times (10^0 - 1)) ,
\end{aligned}$$

which is clearly divisible by 9*.*

1. ***Explain*** *how this fact leads to the following two divisibility criteria:*

> ***Criterion for divisibilitly by*** 9***:*** *A natural number* n *is divisible by* 9 *if and only if the sum of its decimal figures is divisble by* 9*. (For example:* 572, 265 *is divisible by* 9 *because* $5+7+2+2+6+5 = 27$*, which is divisble by* 9*. And* 772, 265 *is not divisible by* 9 *because* $7+7+2+2+6+5 = 29$*, which is not divisble by* 9*.)*
>
> ***Criterion for divisibilitly by*** 3***:*** *A natural number* n *is divisible by* 3 *if and only if the sum of its decimal figures is divisble by* 3*. (For example:* 572, 265 *is divisible by* 3 *because* $5+7+2+2+6+5 = 27$*, which is divisble by* 3*. And* 772, 265 *is not divisible by* 3 *because* $7+7+2+2+6+5 = 29$*, which is not divisble by* 3*.)*

2. *Explain, in a similar way, how the fact that* $10^n - (-1)^n$ *is divisible by* 11 *leads to the following divisibility criterion:*

> ***Criterion for divisibilitly by*** 11***:*** *A natural number* n *is divisible by* 11 *if and only if the alternating sum*[9] *of its decimal figures*

[9] That is, the sum with alternating signs: first figure minus second figureplus third figure minus fourth figure, etc, etc.

is divisble by 11*. (For example:* $572,275$ *is divisible by* 11 *because* $5-7+2-2+7-5=0$*, which is divisble by* 11*. And* $772,265$ *is not divisible by* 11 *because* $7-7+2-2+6-5=1$*, which is not divisble by* 11*.)* □

11 The main theorems of elementary integer arithmetic I: the division theorem

We now study the phenomena that make the natural numbers and the integers different in crucial ways from the real numbers. The root of this difference is that the division operation on $\mathbb{N}$ and $\mathbb{Z}$ is very different from division on $\mathbb{R}$.

11.1 What is the division theorem about?

The first important fact about the integers is the ***division theorem***. It deals with an issue that you know very well, namely, what happens if you have an integer a and an integer b and you want to "divide" a by b:

1. First of all: dividing by zero is never a good idea, so we have to work with integers a and b such that $b \neq 0$.

2. Dividing a by b should amount, roughly, to finding a number q, called the "quotient of a by b", such that

$$a = bq\,. \tag{11.45}$$

3. If we were dealing with real numbers rather than integers, then it is always possible[10] to find q. The real number q that satisfies (11.45) is denoted by the expression $\frac{a}{b}$, that we read as "a over b", or "a divided by b".

4. The situation is different when we are dealing with integers rather than real numbers. In this case, it is not always possible to find an integer q for which (11.45) is satisfied *exactly*. But we can come close: we can find an integer q for which (11.45) is satisfied *approximately.*

[10] Assuming, of course, that $b \neq 0$.

5. Precisely, let us rewrite (11.45) as follows:

$$a = bq + r \qquad \text{and} \quad r = 0\,. \tag{11.46}$$

Then what happens is this: we cannot satisfy (11.46), but we can satisfy

$$a = bq + r \qquad \text{and} \quad r \text{ is small}\,. \tag{11.47}$$

6. And the precise meaning of "small", if $b > 0$, is "$0 \leq r < b$". So what you will be satisfying (if $b > 0$) is

$$a = bq + r \qquad \text{and} \quad 0 \leq r < b\,. \tag{11.48}$$

7. The number q is called the ***quotient of the division of*** a ***by*** b, and the number r is called the ***remainder of the division of*** a ***by*** b.

8. The reason that r is called the "remainder" is very straightforward: suppose you have, say, 27 dollar bills, and you want to divide them equally among 5 people. Then the best you can do is give 5 dollars to each of the five people, and when you do that 2 dollars will "remain".

9. Notice that, if instead of 27 dollar bills you were dealing with, say, 27 gallons of water, then you would be able to divide the water equally, by giving 5.4 gallons to each of the five people. But with dollar bills you cannot do that. That's because ***dollar bills are countable***, whereas ***water is uncountable***. In other words,

   - You can talk about the ***amount*** of water in a tank, and ***amounts of water are measured in terms of real numbers***.
   - And you cannot talk about the ***number*** of water in a tank.
   - You can talk about the ***number*** of dollar bills in your wallet, and ***numbers of dollar bills are measured in terms of natural numbers***. (And if you want to consider negative amounts as well, e.g. to talk about debts, you would use ***integers***.)
   - And you cannot [11] talk about the ***amount*** of dollar bills in your wallet.

[11] I really mean "you shouldn't, because it's wrong". Strictly speaking, you can say anything you want, in this free counrty of ours. But there are rules of grammar, and according to those rules it is wrong to say things like "a large amount of people were at the rally", or "she has a large amount of dollar bills". But it's O.K. to ta;lk about "a large amount of money". "People", like "dollar bills", or "coins", is countable. "Water", like "money", is uncountable.

- If you have a units of a countable quantity such as dollar bills or coins, and b persons among whom you want to divide your a units equally, then the best you can do is give q units to each of the b persons, where q is the quotient of the division of a by b, and when you do that there will be a remainder of r undistributed dollar bills, where r is the remainder of the division of a by b.
- What happens if b is negative? Well, in this case you certainly cannot have $0 \leq r < b$, because if $b < 0$ this is impossible. But you can ask for a remainder r such that $0 \leq r < |b|$, where $|b|$ is the ***absolute value*** of b, that is, the number defined by

$$|x| = \begin{cases} x & \text{if} \quad x \geq 0 \\ -x & \text{if} \quad x < 0 \end{cases} . \tag{11.49}$$

- So the final condition is

$$a = bq + r \qquad \text{and} \quad 0 \leq r < |b| . \tag{11.50}$$

The division theorem says precisely that given integers a, b, there exist integers q, r such that (11.50) holds, provided, of course, that b is not equal to zero. And in addition it makes the very important and very useful assertion that q and r are ***unique***, that is, there is only one possible choice of q and r.

11.1.1 An example: even and odd integers

Example 41. Let us apply the division theorem to the case when $b = 2$. Suppose a is an integer.

What does the division theorem tell us about a?

The theorem makes two assertions, namely,

1. that the quotient and remainder exist (that's the ***existence part***),
2. that the quotient and remainder are unique (that's the ***uniqueness part***).

So let us look at each of these two parts, and see what it tells us about a.

The existence part of the theorem tells us that we can find integers q and r such that

$$a = 2q + r \text{ and } 0 \leq r < 2 .$$

Since $0 \leq r < 2$ and r is an integer, it follows that $r = 0$ or $r = 1$.

If $r = 0$ then $a = 2q$, so a is divisible by 2, that is, a is even.

If $r = 1$ then $a = 2q + 1$, so $a - 1 = 2q$, and then $a - 1$ is divisible by 2, that is, $a - 1$ is even, and, according to our definition of "odd", this implies that a is odd.

So we have shown that: either $r = 0$, in which case a is even, or $r = 1$, in which case a is odd. So ***the existence part of the division theorem tells us that a must be even or odd.***

The uniqueness part of the theorem tells us that we cannot find integers q, r such that

$$a = 2q + r \text{ and } 0 \leq r < 2\,,$$

and also find different integers q', r' such that

$$a = 2q' + r' \text{ and } 0 \leq r' < 2\,.$$

In particular, it is not possible to find integers q, q' such that

$$a = 2q \ \text{ and } \ a = 2q' + 1 \ \text{ (i.e., } \ a = 1 = 2q')\,.$$

In other words, a cannot be both even and odd. So ***the uniqueness part of the division theorem tells us that a cannot be both even and odd.***

Summarizing: ***the division theorem, for $b = 2$, tells us that an integer a has to be even or odd and cannot be both even and odd.*** And this is exactly Theorem 26, that we had to work so hard to prove!

In other words: ***The division theorem is a generalization of the theorem that says that every integer is even or odd and not both.*** □

Now that we understand what the division theorem says for $b = 2$, let us look at what it says for other values of b.

- Theorem 26 says that, when you try to divide an integer a by 2, then one and only one of two things will happen:

    1. you will be able to divide a by 2 exactly, with a remainder equal to zero, and conclude that a is even,

2. you will not be able to divide a by 2 exactly, but you will be able to do it with a remainder equal to 1, and conclude that $a-1$ is divisible by 2, so a is odd.

- The division theorem, applied with $b=2$, says exactly the same thing as Theorem 26.
- The division theorem, applied with $b=3$, says that, when you try to divide an integer a by 3, then one and only one of three things will happen:

  1. you will be able to divide a by 3 exactly, with a remainder equal to zero, and conclude that a is divisible by 3,
  2. you will not be able to divide a by 3 exactly, but you will be able to do it with a remainder equal to 1, and conclude that $a=3q+1$ for some integer q, so $a-1$ is divisible by 3.
  3. you will not be able to divide a by 3 exactly, but you will be able to do it with a remainder equal to 2, and conclude that $a=3q+2$ for some integer q, so $a-2$ is divisible by 3.

- The division theorem, applied with $b=4$, says that, when you try to divide an integer a by 4, then one and only one of four things will happen: $4|a$, $4|a-1$, $4|a-2$, $4|a-3$.
- The division theorem, applied with $b=5$, says that, when you try to divide an integer a by 5, then one and only one of five things will happen: $5|a$, $5|a-1$, $5|a-2$, $5|a-3$, $5|a-4$.
- $\cdots$
- The division theorem, applied with $b=29$, says that, when you try to divide an integer a by 29, then one and only one of 29 things will happen: $29|a-j$ for $j\in\mathbb{Z}$, $0\leq j<29$.
- $\cdots$
- The division theorem, applied with $b=372,508$, says that, when you try to divide an integer a by $372,508$, then one and only one of $372,508$ things will happen: $372,508|a-j$ for $j\in\mathbb{Z}$, $0\leq j<372,508$.

11.2 Precise statement of the division theorem

And here is, finally, the division theorem:

The division theorem for integers

Theorem 46. *If a, b are integers, and $b \neq 0$, then there exist unique integers q, r such that*

$$a = bq + r \text{ and } 0 \leq r < |b|\,.$$

11.3 Proof of Theorem 46

The proof of Theorem 46 will be split up into several parts and subparts.

1. We will first prove the existence part. That is, we will prove that

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(b \neq 0 \Longrightarrow (\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < |b|)\Big)\,. \tag{11.51}$$

The proof of the existence part will be done in three steps:

(a) First we will prove the existence result for natural numbers. That is, we will prove[12]

$$(\forall a \in \mathbb{N})(\forall b \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < b)\,. \tag{11.52}$$

(b) Once we have proved (11.52), we will need a very simple argument to extend the result to the case when a is an arbitrary integer but b is still a natural number. That is, we will prove

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < b)\Big)\,. \tag{11.53}$$

(c) Finally, after proving (11.53), a trivial argument will enable us to extend the result to the case when a is an arbitrary integer but b is also an arbitrary nonzero integer. That is, we will prove (11.51).

[12] Notice that when $b \in \mathbb{N}$ we do not need to put the extra condition that $b \neq 0$, because a natural number is automatically different from zero. And notice also that when $b \in \mathbb{N}$ we do not need to write "$|b|$", because $|b| = b$.

2. Finally, after we have proved the exietence result (11.51) for general integers, we will prove the uniqueness result.

3. In addition to all this, we are going to need a preliminary theorem, in order to be able to deal with a difficulty that will arise: at one point in our proof, we will be "updating" the remainder r as follows: if, for a given n, the remainder of dividing n by b is r, then we will want the new remainder, for $n+1$, to be $r+1$. And, since $r < b$, $r+1$ has a good chance of also being $< b$, but $r+1$ ***could*** be $\geq b$. (For example, if we are trying to divide by 7, then for $n = 20$ we will have a remainder $r = 6$, and when we go up to 21 the new remainder will be 7, which is not permitted, because the remainder has to be $< b$.) What we will do is this: the only way $r+1$ can become $\geq b$ is if $r+1 = b$, and in that case we will reset the remainder to zero. But there is a problem: how do we know that if $r < b$ and $r+1$ is not $< b$ then $r+1$ has to be equal to b? Why couldn't $r+1$ be $> b$? If, for example, $b = 7$, and r was, say, 6.5, then $r+1$ would be certainly not < 7 and not $= 7$ either. Of course, this r is not an integer, and that is precisely the point: ***the fact that when*** $r+1 < b$ ***it cannot happen that*** $r > b$ ***is something that we can guarantee when*** r ***and*** b ***are integers, and it happens because*** r ***and*** b ***are integers***, so we have to be able to prove it using the basic facts that make the integers unique and different from other number systems such as, say, the reals. In other words, we will have to prove a theorem saying that if n, m are integers and $n < m$ then it cannot happen that $n+1 > m$. And that is Theorem 47 below.

11.3.1 An obvious but very important theorem

As we have just explained, we have to start by proving a very obvious but very important fact about the integers.

Theorem 47. *If* $n \in \mathbb{Z}$ *then there is no integer* m *such that* $n < m < n+1$.

In order to prove Theorem 47 we need a completely trivial lemma.

Lemma 4. *If* $n \in \mathbb{N}$ *then* $n \geq 1$.

Proof.

Let n be an arbitrary natural number.

Then either $n = 1$ or $n \neq 1$.

If $n = 1$ then of course $n \geq 1$.

If $n \neq 1$ then by Basic Fact BFZ10, $n - 1$ is a natural number.

Then the definition of "$>$" tells us that $n > 1$.

So $n \geq 1$.

We have seen that $n \geq 1$ in both cazses, when $n = 1$ and when $n \neq 1$.

So $n \geq 1$. **Q.E.D.**

Proof of Theorem 47.

Let n be an arbitrary integer.

Assume[13] that there exists an integer m such that $n < m < n+1$.

Pick one such integer and call it m_*, so that $m_* \in \mathbb{Z}$, and $n < m_* < n + 1$.

Since $n < m_*$, $m_* - n$ is a natural number.

Hence $1 \leq m_* - n$, by Lemma 4.

So $1 + n \leq m_*$.

But then the trichotomy law implies that $\sim m_* < n + 1$.

So $m_* < n + 1$ and $\sim m < n + 1$, which is a contradiction.

So we have proved that there exists an integer m such that $n < m < n + 1$. **Q.E.D.**

11.3.2 Proof of the existence part of the division theorem for natural numbers

We are now ready to prove (11.52), that is,

Theorem 46.I. *If a, b are natural numbers then there exist integers q, r such that $a = bq + r$ and $0 \leq r < b$.*

[13] A proof by contradiction !

Proof. We want to prove that

$$(\forall a \in \mathbb{N})(\forall b \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < b)\Big)\,.$$

Let a, b be arbitrary natural numbers.

We want to prove

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < b)\,. \tag{11.54}$$

The way we will prove this is by showing that, when we "count" 1, 2, 3, and so on, at each step the number n we get must satisfy

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < b)\,. \tag{11.55}$$

Since every natural number n is reached by counting, we will conclude that

$$(\forall n \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < b)\,. \tag{11.56}$$

And then we will be able to apply the specialization rule and conclude that (11.55) is true for $n = a$, i.e., that (11.54) holds.

To prove that when we count the numbers n that we get satisfy (11.55), we will first prove that (11.55) is true for $n = 1$, and then we will prove that the truth of (11.55) for a natural number n is passed on to $n + 1$.

In other words, we will prove (11.56) by induction.

So we let $P(n)$ be the statement

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < b)\,. \tag{11.57}$$

We are going to prove $(\forall n \in \mathbb{N})P(n)$ by induction.

Basis step. We prove $P(1)$. We have to produce integers q, r such that

$$1 = bq + r \ \text{ and } \ 0 \leq r < b\,. \tag{11.58}$$

This is very easy, but we have to be careful because b could be equal to 1 or not, and what happens when $b = 1$ is different from what happens when $b \neq 1$.

Consider the case when $b = 1$.

In this case, we take $q = 1$ and $r = 0$. Then (11.58) clearly holds.

Now consider the case when $b \neq 1$.

In this case, we take $q = 0$ and $r = 1$. Then (11.58) holds as well[14].

So in both cases we have produced integers q, r such that (11.58) is true. Therefore integers q, r such that (11.58) holds exist, that is,

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(1 = bq + r \wedge 0 \leq r < b)\,.$$

In other words, $P(1)$ is true.

This concludes the basis step.

Inductive step.

Let $n \in \mathbb{N}$ be arbitrary.

Assume $P(n)$ is true. We want to prove $P(n+1)$.

Since $P(n)$ is true, we can pick integers q, r such that

$$n = bq + r \text{ and } 0 \leq r < b\,.$$

Since $r < b$ and $r \in \mathbb{Z}$, the number $r + 1$ cannot be greater than b. (Reason: suppose [15] $r + 1 > b$. Then $r < b < r + 1$. But this contradicts Theorem 47.)

Hence $r + 1 \leq b$.

We distinguish two cases: $r + 1 < b$ and $r + 1 = b$.

The case when $r + 1 < b$***.*** In this case, we take $q' = q$ and $r' = r + 1$, and we get

$$n + 1 = bq' + r' \text{ and } 0 \leq r' < b\,.$$

So $P(n+1)$ is true.

[14] The reason that we had to treat the case $b = 1$ differently is that when $b = 1$ if we take $r = 1$ then the condition $r < b$ is not satisifed.

[15] A proof by contradiction !

The case when $r+1=b$***.*** In this case, we take $q'=q+1$ and $r'=0$, and we get

$$n+1=bq'+r' \text{ and } 0\leq r'<b\,,$$

because $bq'+r'=bq'+0=bq'=b(q+1)=bq+b=bq+(r+1)=(bq+r)+1=n+1$.

So $P(n+1)$ is true.

We have proved that $P(n+1)$ is true in both cases, when $r+1<b$ and when $r+1=b$. So we have proved $P(n+1)$.

We have proved $P(n+1)$ assuming $P(n)$, so we have proved $P(n)\Longrightarrow P(n+1)$.

We have proved $P(n)\Longrightarrow P(n+1)$ for an arbitrary natural number n. Hence

$$(\forall n\in\mathbb{N})(P(n)\Longrightarrow P(n+1))\,.$$

This completes the inductive step.

It follows from the PMI that

$$(\forall n\in\mathbb{N})(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(n=bq+r\wedge 0\leq r<b)\,.$$

We can then apply this to $n=a$, and conclude that

$$(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(a=bq+r\wedge 0\leq r<b)\,. \qquad (11.59)$$

We have proved (11.59) for arbitrary natural numbers a,b. That is, we have proved (11.52). **Q.E.D.**

11.3.3 Proof of the existence part of the division theorem for $a\in\mathbb{Z}$ and $b\in\mathbb{N}$

We now prove:

Theorem 46.II. *If a is an integer and b is a natural number then there exist integers q,r such that $a=bq+r$ and $0\leq r<b$.*

Proof. We want to prove that

$$(\forall a\in\mathbb{Z})(\forall b\in\mathbb{N})(\exists q\in\mathbb{Z})(\exists r\in\mathbb{Z})(n=bq+r\wedge 0\leq r<b)\,.$$

Let $a \in \mathbb{Z}$ be arbitrary.

Let $b \in \mathbb{N}$ be arbitrary.

We want to prove that (11.59) holds.

Basic Fact BFZ9 tells us that either $a \in \mathbb{N}$ or $a = 0$ or or $-a \in \mathbb{N}$.

So we consider each of these three cases.

$\boxed{\boxed{\text{Assume that } a \in \mathbb{N}}}$.

Then we can apply Theorem 46.I and conclude that $\boxed{\boxed{\text{(11.59) holds}}}$, under the asumption that $a \in \mathbb{N}$.

Next $\boxed{\boxed{\text{assume that } a = 0}}$.

Take $q = 0$ and $r = 0$.

Then $a = bq + r$ and $0 \leq r < b$.

So $\boxed{\boxed{\text{(11.59) holds}}}$ as well, under the asumption that $a = 0$.

Finally, $\boxed{\boxed{\text{assume that } -a \in \mathbb{N}}}$.

Then we can apply Theorem 46.I with $-a$ in the role of a, and conclude that we may pick integers q, r such that

$$-a = bq + r \quad\text{and}\quad 0 \leq r < b\,.$$

It follows that

$$a = b \times (-q) + (-r)\,,$$

and then, if we let $q' = -q$, $r' = -r$, we find that

$$a = bq' + r'\,.$$

This, however, does not yet achieve the desired result, because we don't know that $0 \leq r' < b$.

But we know that $0 \leq r < b$, and this implies that $-b < -r \leq 0$, i.e.,

$$-b < r' \leq 0\,.$$

Furthermore, either $r = 0$ or $r > 0$.

Let us consider each of these two cases.

$\boxed{\text{Assume first that } r = 0}$.

Then $r' = 0$, so $0 \leq r < b$.

Hence, in this case, we have $a = bq' + r'$ and $0 \leq r < b$, so $\boxed{\text{(11.59) holds}}$.

Now $\boxed{\text{aasume that } r > 0}$.

Then $-r < 0$, i.e., $r' < 0$.

So $-b < r' < 0$.

It follows that $0 < r' + b < b$.

Let $r'' = r' + b$, and $q'' = q' - 1$.

Then $0 < r'' < b$.

Also,

$$a = bq' + r' = b(q'' + 1) + r' = bq'' + b + r' = bq'' + r'' .$$

So $a = bq'' + r''$ and $0 \leq r'' < b$.

Therefore $\boxed{\text{(11.59) holds}}$.

So we have proved that (11.59) is true in both cases, when $r = 0$ and when $r > 0$.

Hence $\boxed{\boxed{\text{(11.59) holds}}}$, under the assumption that $-a \in \mathbb{N}$.

We have proved that (11.59) holds in each of the three cases, when $a \in \mathbb{N}$, when $a = 0$, and when $-a \in \mathbb{N}$.

Hence (11.59) is true.

We have proved that (11.59) is true, i.e. that $(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \land 0 \leq r < b)$, for an arbitrary integer a and an arbitrary natural number b.

Hence

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{N})(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \land 0 \leq r < b) ,$$

which is exactly what we wanted to prove. **Q.E.D.**

11.3.4 Proof of the existence part of the division theorem for $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, $b \neq 0$

We now prove:

Theorem 46.III. *If a and b are integers and $b \neq 0$, then there exist integers q, r such that $a = bq + r$ and $0 \leq r < |b|$.*
Proof. We want to prove that

$$(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})\Big(b \neq 0 \Longrightarrow (\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(n = bq + r \wedge 0 \leq r < b)\Big)\,. \tag{11.60}$$

Let $a \in \mathbb{Z}$ be arbitrary.

Let $b \in \mathbb{Z}$ be arbitrary.

Assume that $b \neq 0$.

We want to prove that

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\,, \tag{11.61}$$

Let $\beta = |b|$.

Then β is a natural number (because $b \neq 0$) and a is an integer, so we may apply Theorem 46.II and conclude that

$$(\exists q \in \mathbb{Z})(\exists r \in \mathbb{Z})(a = \beta q + r \wedge 0 \leq r < \beta)\,.$$

Pick integers q_*, r_* such that

$$a = \beta q_* + r_* \wedge 0 \leq r_* < \beta\,.$$

Define an integer q' by letting

$$q' = \begin{cases} q_* & \text{if} \quad b > 0 \\ -q_* & \text{if} \quad b < 0 \end{cases}\,.$$

Then $\beta q_* = bq'$. (Reason: if $b > 0$ then $\beta = b$ and $q' = q_*$, so $\beta q' = bq_*$; and if $b < 0$ then $\beta = -b$ and $q' = -q_*$, so $\beta q' = (-b)(-q_*) = bq_*$.)

Since $a = \beta q_* + r$ and $\beta q_* = bq'$, we have $a = bq' + r$.

Furthermore, we have $0 \leq r < \beta$ and $\beta = |b|$, so $0 \leq r < |b|$.

Hence $a = bq' + r \wedge 0 \leq r < |b|$.

Therefore (11.61) holds.

We have proved (11.61) for arbitrary integers a, b such that $b \neq 0$.

Hence (11.60) is true. **Q.E.D.**

11.3.5 Proof of the uniqueness part of the division theorem for $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, $b \neq 0$

We now prove, finally,

Theorem 46.IV. *If a and b are integers and $b \neq 0$, then there exist unique integers q, r such that $a = bq + r$ and $0 \leq r < |b|$.*
Proof.

Let $a \in \mathbb{Z}$ be arbitrary.

Let $b \in \mathbb{Z}$ be arbitrary.

Assume that $b \neq 0$.

We want to prove that

$$(\exists! q \in \mathbb{Z})(\exists! r \in \mathbb{Z})(a = bq + r \wedge 0 \leq r < |b|)\,, \tag{11.62}$$

For this purpose, we have to prove that

(*) There exist integers q, r such that $a = bq + r \wedge 0 \leq r < |b|$,

(**) If q_1, q_2, r_1, r_2 are integers such that

$$\begin{aligned} a &= bq_1 + r_1 && (11.63)\\ 0 &\leq r_1 < b && (11.64)\\ a &= bq_2 + r_2 && (11.65)\\ 0 &\leq r_2 < b\,, && (11.66) \end{aligned}$$

then $q_1 = q_2$ and $r_1 = r_2$.

Statement (*) is the existence part of the division theorem, which has already been proved, in Theorem 46.III.

We now prove statement (**), i.e., the uniqueness part.

Let q_1, q_2, r_1, r_2 be integers such that (11.63), (11.64), (11.65), and (11.66) hold.

We will prove that $q_1 = q_2$ and $r_1 = r_2$.

Without loss of generality, we may assume that $r_1 \geq r_2$. (Reason: if r_1 was $< r_2$, just change the names of r_1, r_2 and call them r_2 and r_1.)

Then

$$0 \leq r_1 - r_2 < b\,. \tag{11.67}$$

(Reason: 0 is $\leq r_1 - r_2$ because $r_1 \geq r_2$. And $r_1 - r_2 < b$ because $r_1 - r_2 \leq r_1$, since $r_2 \geq 0$, and $r_1 < b$.)

On the other hand, $a = bq_1 + r_1$ and $a = bq_2 + r_2$, so

$$bq_1 + r_1 = bq_2 + r_2\,.$$

Therefore

$$b(q_2 - q_1) = r_1 - r_2\,. \tag{11.68}$$

Then

$$|b| \cdot |q_2 - q_1| = |r_1 - r_2|\,, \tag{11.69}$$

because $|xy| = |x| \cdot |y|$ for arbitrary real numbers x, y.

Since q_1 and q_2 are integers, the number $|q_1 - q_2|$ is a nonnegative integer.

We now prove[16] that $q_1 = q_2$.

> Assume that $q_1 \neq q_2$.
>
> Then the nonnegative integer $|q_1 - q_2|$ is not zero, so it is a natural number.
>
> And then $|q_1 - q_2| \geq 1$.
>
> Therefore (11.69) implies that $|r_1 - r_2| \geq |b|$.
>
> But $r_1 - r_2 \geq 0$, because $r_1 \geq r_2$.
>
> Hence $|r_1 - r_2| = r_1 - r_2$.
>
> It follows that $r_1 - r_2 \geq |b|$.

[16] by contradiction , naturally.

So it's not true that $r_1 - r_2 < |b|$.
But (11.67) tells us that $r_1 - r_2 < |b|$.
So $r_1 - r_2 < |b|$ and $\sim r_1 - r_2 < |b|$, which is a contradiction.

This proves that $\boxed{q_1 = q_2}$.

And then (11.69) implies that $\boxed{r_1 = r_2}$.

So we have proved (**), for arbitrary integers a, b such that $b \neq 0$.

This completes the proof of the uniqueness part. So our proof is complete.
Q.**E**.**D**.