MATHEMATICS 300 — FALL 2018

Introduction to Mathematical Reasoning

H. J. Sussmann

INSTRUCTOR'S NOTES

Contents

Part IV

1 An introduction to elementary arithmetic

1.1 What is arithmetic?

According to the Oxford English Dictionary (OED), the Oxford Learner's Dictionafry (OPD), and *Dictionary.com* (Dc), arithmetic is

- the branch of mathematics dealing with the properties and manipulation of numbers (OED),
- the type of mathematics that deals with the adding, multiplying, etc. of numbers (OLD),
- the theory of numbers; the study of the divisibility of whole numbers, the remainders after division, etc. (Dc).

So, as you can see, arithmetic is concerned with the properties of the basic operations on numbers: addition, subtraction, multiplication and division. And, as the definition in *Dictionary.com* indicates, ***the most interesting of these operations is division***.

1.2 Numbers

And, as we have discussed before, there are many kinds of "numbers". These numbers are organized into ***number systems***. The most important examples of number systems are:

1. the integers,
2. the rational numbers,
3. the real numbers,
4. the complex numbers[1]

In mathematical language, for each of these number systems the set of numbers has a name:

- the set of all integers is called $\mathbb{Z}$; so "$x \in \mathbb{Z}$" is a way to say that x is an integer[2];
- the set of all rational numbers is called $\mathbb{Q}$; so "$x \in \mathbb{Q}$" is a way to say that x is a rational number;
- the set of all real numbers is called $\mathbb{R}$; so "$x \in \mathbb{R}$" is a way to say that x is a real number;
- the set of all complex numbers is called $\mathbb{C}$; so "$x \in \mathbb{C}$" is a way to say that x is a complex number.

1.2.1 Operations

Unary and binary operations

An operation is a way of combining one or several objects of one or several kinds, called the inputs, or arguments, of the operation and producing a new object, called the result, or output, which may be of the same kind as the arguments.
An operation with one argument is called a unary operation.
An operation with two arguments is called a binary operation.

[1] If you are not familiar with the complex numbers, do not worry; we are not going to need them in this course, but in any case I will explain what they are later.

[2] It is customary to use letters such as m, n, p, q, rather than x, for integers, but it is perfectly legitimate to use x.

Example 1.

- ***Addition of integers*** is a binary operation: it takes two integers m and n as inputs and results in an integer $m+n$, called the ***sum*** of m and n.
- ***Multiplication of integers*** is a binary operation: it takes two integers m and n as inputs and results in an integer mn, called the ***product*** of m and n.
- ***Subtraction of integers*** is a binary operation: it takes two integers m and n as inputs and results in an integer $m-n$, called the ***difference*** of m and n.
- ***Addition, multiplication, and subtraction of rational numbers*** are binary operations whose arguments and outputs are rational numbers.
- ***Addition, multiplication, and subtraction of real numbers*** are binary operations whose arguments and outputs are real numbers.
- ***Addition, multiplication, and subtraction of complex numbers*** are binary operations whose arguments and outputs are complex numbers.
- ***Minus*** (or "***negative of***" is a unary operation on the integers: it takes an integer n as input and results in an integer $-n$, called "minus n", or "the negative of n", or "the additive inverse of n". (As explained in Part I of these notes (on page 21), I strongly recommend that you read "$-n$" as "minus n" rather than, say, "negative n".)
- Thera are similar "minus" unary operations on the rational numbers, the real numbers, and the complex numbers..
- The ***scalar product*** (a.k.a ***dot product***) of vectors in two or three dimensions is a binary operation that takes as inputs two vectors $\vec{v}, \vec{w}$ and produces as output a real number $\vec{v}\cdot\vec{w}$, called the ***scalar product***, or ***dot product***, of $\vec{v}$ and $\vec{w}$.
- The ***vector product*** of vectors in three dimensions is a binary operation that takes as inputs two three-dimensional vectors $\vec{v}, \vec{w}$ and

produces as output a vector $\vec{v} \times \vec{w}$, called the ***vector product*** of $\vec{v}$ and $\vec{w}$. □

So in all the four number systems that we have seen so far—$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$—there are two important binary operations, addition and multiplication.

But these operations behave differently, and for that reason $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are very different. For example:

- In $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, the following "division theorem" is true[3]:

$$(\forall x)(\forall y)(y \neq 0 \Longrightarrow (\exists z)x = yz)\,. \tag{1.1}$$

  In other words, given any x and any y, as long as $y \neq 0$, it is possible to ***divide*** x ***by*** y ***exactly***, that is, find a "quotient" z such that $yz = x$.

- In $\mathbb{Z}$, the "division theorem" (1.1) is not true, but there is a different theorem, the division theorem for integers[4]:

$$(\forall x)(\forall y)\Big(y \neq 0 \Longrightarrow (\exists z)(x = yz + r \wedge 0 \leq r < |y|)\Big)\,. \tag{1.2}$$

  In other words, given any x and any y, as long as $y \neq 0$, it is possible to ***divide*** x ***by*** y ***with a remainder*** that is, find a "quotient" z and a "small remainder" r such that $x = yz + r$; the remainder r iius 'small" in the precise sense that $0 \leq r < |y|$..

- For example:
  - In $\mathbb{Q}$, if we take $x = 23$, $y = 6$, and we want to divide x by y, we can find z such that $x = yz$. (The value of z is $\frac{23}{6}$, of course.)
  - But in $\mathbb{Z}$ the situation is very different: if we take $x = 23$, $y = 6$, and we want to divide x by y, we can find z, r such that $x = yz + r$ and $0 \leq r < 6$. (The values of z and r are: $z = 3$, $r = 5$.)

[3]As explained in the box on page 6, if we are working in a number system $\mathfrak{N}$, the quantifiers "$(\forall x)$", "$(\forall y)$", "$(\exists z)$" mean "$(\forall x \in \mathfrak{N})$", "$(\forall y \in \mathfrak{N})$", "$(\exists z \in \mathfrak{N})$".

[4]In this case, the conventions of the box on page 6 tell us, since we have announced that we are working in $\mathbb{Z}$, that the quantifiers "$(\forall x)$", "$(\forall y)$", "$(\exists z)$", "$(\exists r)$" mean mean "$(\forall x \in \mathbb{Z})$", "$(\forall y \in \mathbb{Z})$", "$(\exists z \in \mathbb{Z})$", "$(\exists r \in \mathbb{Z})$".

AN IMPORTANT CONVENTION ABOUT QUANTIFIERS

When we are studying a particular number system $\mathfrak{N}$, then we just write "$(\forall x)$" and "$(\exists x)$" instead of "$(\forall x \in \mathfrak{N})$" and "$(\exists x \in \mathfrak{N})$". In other words: when the range of a variable in a quantifier is not specified it is understood that the range is $\mathfrak{N}$. So, for example, if we are studying $\mathbb{R}$, the real number system, and we want to say "for every real number x there exists an integer n that is larger than x", we can write "$(\forall x)(\exists n \in \mathbb{Z})n > x$". It is understood that "$(\forall x)$" means "$(\forall x \in \mathbb{R})$". But we have to write "$(\exists n \in \mathbb{Z})$", because if we wrote "$(\exists n)$" this would be interepreted as "$(\exists n \in \mathbb{R})$".

1.3 Other number systems: The integers modulo n

In order to understand how $\mathbb{Z}$ is different from other number systems, mathematicians have come to the conclusion that it is very convenient and very interesting to study lots of other number systems, in addition to $\mathbb{Z}$, $\mathbb{Q}$ and $\mathbb{R}$. So let me start by presenting a whole infinite class of new number systems: the integers modulo n.

For each natural number n such that $n \geq 2$, we define the set $\mathbb{Z}_n$ of ***integers modulo*** n.

- The members of $\mathbb{Z}_n$ are the numbers $0, 1, 2, \ldots, n-1$, so $\mathbb{Z}_n$ has n members[5].
- The operations of ***addition*** and ***multiplication*** in $\mathbb{Z}_n$ are performed as follows: to add or multiply two members a, b of $\mathbb{Z}_n$, we add them or multiply them as ordinary integers. and then "reduce the result modulo n", by subtracting a multiple of n so as to produce a result that belongs to $\mathbb{Z}_n$.

Example 2. The set $\mathbb{Z}_7$ of integers modulo 7 has seven members: 0, 1, 2, 3, 4, 5, and 6. That is,

$$\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}.$$

[5]This is why we take $n \geq 2$. We could also study $\mathbb{Z}_1$, the integers modulo 1, but this set would have only one member, namely, 0, and this would not be interesting.

To add or multiply two members of $\mathbb{Z}_7$ in $\mathbb{Z}_7$ we add them or multiply them as integers, but if the result is 7 or larger than 7 then we subtract 7, and then subtract 7 again if necessary, until we end up with a result in $\mathbb{Z}_7$. So, for example, the following are true in $\mathbb{Z}_7$:

$$\begin{aligned} 2+3 &= 5\,, \\ 3+4 &= 0\,, \\ 2+6 &= 1\,, \\ 4+5 &= 2\,, \\ 5+6 &= 4\,, \\ 2\times 3 &= 6\,, \\ 3\times 4 &= 5\,, \\ 2\times 6 &= 5\,, \\ 4\times 5 &= 6\,, \\ 5\times 6 &= 2\,. \end{aligned}$$

(For example, we get the equality $5 \times 6 = 2$ as follows: in $\mathbb{Z}$, 5 times 6 is equal to 30, but then we have to reduce modulo 7, for which purpose we have to subtract 7 four times, i.e., subtract 28, thus ending up with 2 as the final result.)

Example 3. The set $\mathbb{Z}_{12}$ of integers modulo 12 has twelve members: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11. That is,

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}\,.$$

To add or multiply two members of $\mathbb{Z}_{12}$ in $\mathbb{Z}_{12}$ we add them or multiply them as integers, but if the result is 12 or larger than 12 then we subtract 12, and then subtract 12 again if necessary, until we end up with a result belonging

to $\mathbb{Z}_{12}$. So, for example, the following are true in $\mathbb{Z}_{12}$:

$$\begin{aligned} 2+3 &= 5\,, \\ 3+4 &= 7\,, \\ 4+9 &= 1\,, \\ 9+7 &= 4\,, \\ 2\times 3 &= 6\,, \\ 3\times 4 &= 0\,, \\ 4\times 9 &= 0\,, \\ 9\times 7 &= 3\,. \end{aligned}$$

(For example, we get the equality $9 \times 7 = 3$ as follows: in $\mathbb{Z}$, 9 times 7 is equal to 63, and then we have to reduce modulo 12, for which purpose we have to subtract 12 five times, i.e., subtract 60, thus ending up with 3 as the final result.)

Example 4. The set $\mathbb{Z}_{103}$ of integers modulo 103 has 103 members, namely, all the integers n such that $0 \leq n < n$. I do not write down the full list for obvious reasons. But it is possible to write down a formal definition using the langauge of sets, as follows

$$\mathbb{Z}_{103} = \{n \in \mathbb{Z} : 0 \leq n < 103\}\,. \tag{1.3}$$

To add or multiply two members of $\mathbb{Z}_{103}$ in $\mathbb{Z}_{103}$ we add them or multiply them as integers, but if the result is 103 or larger than 103 then we subtract 103, and then subtract 103 again if necessary, until we end up with a result belonging to $\mathbb{Z}_{103}$. So, for example, the following are true in $\mathbb{Z}_{103}$:

$$\begin{aligned} 56+87 &= 40\,, \\ 56\times 87 &= 31\,. \end{aligned}$$

How do we find that $56 \times 87 = 41$? You compute the product 56×87 in $\mathbb{Z}$, and get

$$56 \times 87 = 4872 \qquad \text{in} \quad \mathbb{Z}\,.$$

Then, using the method for dividing integers that you learned in high school, you get

$$4872 = 47 \times 103 + 31 \qquad \text{in} \quad \mathbb{Z}\,.$$

so in $\mathbb{Z}_{103}$ $56 \times 87 = 31$.

Problem 1. In a number system $\mathfrak{N}$, a multiplicative inverse of a number $a \in \mathfrak{N}$ is a member b of $\mathfrak{N}$ such that $ab = 1$.

Find

1. a multiplicative inverse of 4 in $\mathbb{Z}_7$,
2. a multiplicative inverse of 23 in $\mathbb{Z}_{41}$,
3. a multiplicative inverse of 48 in $\mathbb{Z}_{103}$.

Solution:

1. To find a multiplicative inverse of 4 in $\mathbb{Z}_7$ we just use trial and error: we try multiplying 4 in $\mathbb{Z}_7$ by all the members of $\mathbb{Z}_7$ until we find one for which the product is 1. Clearly, $0 \times 4 = 0$, $1 \times 4 = 4$, and $2 \times 4 = 1$. So 2 ***is a multiplicative inverse of*** 4 ***in*** $\mathbb{Z}_7$.

2. To find a multiplicative inverse of 23 in $\mathbb{Z}_{41}$, trial and error would take too long, so we try something smarter: we look for members n of $\mathbb{Z}_{41}$ such that $23 \times n$ is close to 1, and then we try to modify n to make $23 \times n$ even closer to 41, and we keep going until we get $23 \times n = 1$. An obvious first choice of n is $n = 2$, This yields $23 \times 2 = 5$, which is not 1, but is close. Now we look for $m \in \mathbb{Z}_{41}$ such that $5 \times m$ is close to 41. An obvious choice is $m = 8$. This gives[6] $5 \times 8 = -1$. So

$$\begin{aligned}(23 \times 2) \times 8 &= 5 \times 8 \\ &= -1\,,\end{aligned}$$

while, on the other hand,

$$\begin{aligned}(23 \times 2) \times 8 &= 23 \times (2 \times 8) \\ &= 23 \times 16\,,\end{aligned}$$

so

$$23 \times 16 = -1\,.$$

Then $23 \times (-16) = 1$. So the desired multiplicative inverse of 23 is -16. And in $\mathbb{Z}_{41}$ -16 equals 25, because $25 + 16 = 0$. So, finally, our answer is $\boxed{25}$.

[6]Why is $40 = -1$. Because $-k$ is the number that added to k gives zero. And $40+1 = 0$ in $\mathbb{Z}_{41}$, so $40 = -1$ in $\mathbb{Z}_{41}$.

Verification: In $\mathbb{Z}_{41}$:

$$\begin{aligned} 23 \times 25 &= 23 \times 5 \times 5 \\ &= 115 \times 5 \\ &= (82 + 33) \times 5 \\ &= (41 \times 2 + 33) \times 5 \\ &= 33 \times 5 \\ &= 165 \\ &= 164 + 1 \\ &= 41 \times 4 + 1 \\ &= 1\,. \end{aligned}$$

3. To find a multiplicative inverse of 48 in $\mathbb{Z}_{103}$ we use the same method as for the previous question. First. we observe that 48×2 equals 96, which in 103 is equal to -7. So $48 \times 2 = -7$. Next, $7 \times 15 = 105$, so $7 \times 15 = 2$ in $\mathbb{Z}_{103}$, and then $(-7) \times 15 = -2$. Then

$$\begin{aligned} (48 \times 2) \times 15 &= (-7) \times 15 \\ &= -2\,, \end{aligned}$$

but

$$\begin{aligned} (48 \times 2) \times 15 &= 48 \times (2 \times 15) \\ &= 48 \times 30\,, \end{aligned}$$

so $48 \times 30 = -2$, and then $48 \times (-30) = 2$. Since $-30 = 73$ in $\mathbb{Z}_{103}$, we get

$$48 \times 73 = 2\,.$$

Now, $104 = 2 \times 52$, so $2 \times 52 = 1$ in $\mathbb{Z}_{103}$. Hence

$$\begin{aligned} (48 \times 73) \times 52 &= 2 \times 52 \\ &= 1\,, \end{aligned}$$

while, on the other hand, $(48 \times 73) \times 52 = 48 \times (73 \times 52)$. So $48 \times (73 \times 52) = 1$. So the desired multiplicative inverse of 48 in $\mathbb{Z}_{103}$ is 73×52.

Finally,

$$\begin{aligned} 73 \times 52 &= -30 \times 52 \\ &= -3 \times 10 \times 52 \\ &= -3 \times 520 \\ &= -3 \times 5 \\ &= -15 \\ &= 88\,. \end{aligned}$$

So our final answer is that $\boxed{88}$ is a multiplicative inverse of 48 in $\mathbb{Z}_{103}$.

Verification: In $\mathbb{Z}_{103}$

$$\begin{aligned} 48 \times 88 &= 48 \times 2 \times 2 \times 2 \times 11 \\ &= 96 \times 2 \times 2 \times 11 \\ &= 192 \times 2 \times 11 \\ &= (103 + 89) \times 2 \times 11 \\ &= 89 \times 2 \times 11 \\ &= 178 \times 11 \\ &= (103 + 75) \times 11 \\ &= 75 \times 11 \\ &= 825 \\ &= 824 + 1 \\ &= (103 \times 8) + 1 \\ &= 1\,. \end{aligned}$$

Problem 2. ***Prove*** that 6 does not have a multiplicative inverse in $\mathbb{Z}_{12}$.

Solution:

Suppose[7] 6 had a multiplicative inverse in $\mathbb{Z}_{12}$. Pick one such inverse [8] and call it x, so

$$6x = 1 \text{ in } \mathbb{Z}_{12}\,.$$

[7]Obviously, we are doing a proof by contradiction.

[8]Since $(\exists x \in \mathbb{Z}_{12})6x = 1$, where "$6x$" stands for the product of 6 and x in $\mathbb{Z}_{12}$, Rule $\exists_{use}$ allows us to pick a witness and call it x.

Multiply both sides by 2. Then, in $\mathbb{Z}_{12}$,

$$2 \times (6x) = 2 \times 1 = 2\,,$$

while on the other hand

$$2 \times (6x) = (2 \times 6) \times x = 12x = 0.x = 0\,,$$

because in $\mathbb{Z}_{12}$ $12 = 0$.

So $2 = 0$. But in $\mathbb{Z}_{12}$ 2 is not 0. So we got a contradiction. **Q.E.D.**

Problem 3. ***Prove*** that 21 does not have a multiplicative inverse in $\mathbb{Z}_{60}$.

Solution:

Suppose 21 had a multiplicative inverse in $\mathbb{Z}_{60}$. Pick one such inverse and call it x, so

$$21x = 1 \text{ in } \mathbb{Z}_{60}\,.$$

Multiply both sides by 20. Then, in $\mathbb{Z}_{60}$,

$$20 \times (21x) = 20 \times 1 = 20\,,$$

while on the other hand

$$20 \times (21x) = 20 \times (3 \times 7x) = (20 \times 3) \times 7x = 60 \times 7x = 0.7x = 0\,,$$

because in $\mathbb{Z}_{60}$ 60.

So $20 = 0$. But in $\mathbb{Z}_{60}$ 20 is not 0. So we got a contradiction. **Q.E.D.**

Problem 4. ***Prove*** that if $n \in \mathbb{N}$, $n > 1$, and n is not prime, then it is not true that every nonzero member of $\mathbb{Z}_n$ has a multiplicative inverse in $\mathbb{Z}_n$.

Solution: **YOU DO THIS ONE.**

Hint: Read carefully the solutions of problems 2 and 3 and use the same method, Write $n = pq$, with $p, q \in \mathbb{Z}$ and $1 < p < n$, so $1 < q < n$, and then $p \in \mathbb{Z}_n$ and $q \in \mathbb{Z}_n$. Prove by contradiction that p (or q if you prefer) does not have a multiplicative inverse in $\mathbb{Z}_n$. □

1.4 Rings

All the number systems that we have discussed so far ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the integers modulo n for every $n \in \mathbb{N}$ such that $n > 1$) enumerated have an operation of addition and an operation of multiplication. And these operations have certain properties that are similar for all these number systems.

Definition 1. A ring is a set $\mathfrak{R}$—whose members are called "numbers"—equipped with

1. a binary operation called ***addition***, that for every $x \in \mathfrak{R}$, $y \in \mathfrak{R}$ produces a new object $x + y$ called "x plus y", or ***the sum of*** x ***and*** y;
2. a binary operation called ***multiplication***, that for every $x \in \mathfrak{R}$, $y \in \mathfrak{R}$ produces a new object $x.y$ (or xy, or $x \times y$) called "x times y", or ***the product of*** x ***and*** y;
3. a special member 0 of $\mathfrak{R}$ called ***zero***.

in such a way that the following "ring axioms" are satisfied.

THE RING AXIOMS

RA1: $0 \in \mathfrak{R}$,
RA2: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})x + y \in \mathfrak{R}$.
RA3: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})x.y \in \mathfrak{R}$.
RA4: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})x + y = y + x$.
RA5: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\forall z \in \mathfrak{R})x + (y + z) = (x + y) + z$.
RA6: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\forall z \in \mathfrak{R})x(yz) = (xy)z$.
RA7: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\forall z \in \mathfrak{R})x(y+z) = xy+xz \wedge (x+y)z = xz+yz$.
RA8: $(\forall x \in \mathfrak{R})x + 0 = x$.
RA9: $(\forall x \in \mathfrak{R})(\exists y \in \mathfrak{R})x + y = 0$.

Let us read and try to understand the ring axioms:

- Axiom RA1 says that zero is a number, i.e., a member of our number system $\mathfrak{N}$.

- Axioms RA2 and RA3 say that numbers—i.e., members of $\mathfrak{R}$— can be ***added*** and ***multiplied***, and the result of adding or multiplying two member of $\mathfrak{R}$ is again in $\mathfrak{R}$.
- Axiom RA4 is the ***commutative law of addition***: the sum of two numbers is the same if you add them in the opposite order: $x+y = y+x$ for every $x, y \in \mathfrak{R}$.
- Axiom RA5 is the ***associative law of addition***: if x, y, z are three members of $\mathfrak{R}$ then $x + (y + z) = (x + y) + z$.
- Axiom RA6 is the ***associative law of multiplication***: if x, y, z are three members of $\mathfrak{R}$ then $x(yz) = (xy)z$.
- Axiom RA7 is the ***distributive law of multiplication with respect to addition***: if x, y, z are three members of $\mathfrak{R}$ then $x(y+z) = xy+xz$, and also $(x + y)z = xz + yz$.
- Axiom RA8 says that ***zero is an additive identity***. (An additive identity is a number a such that $x + a = x$ for every x.)
- Axiom RA9 says that ***every member of $\mathfrak{R}$ has an additive inverse***. (An additive inverse of x is a number y such that $x + y = 0$.)

1.4.1 Commutative and non-commutative rings

You may notice that we did not include in our list of axioms the commutative law of multiplication:

THE COMMUTATIVE LAW ROF MULTIPLICATION

RA10: $(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})xy = yx$.

We did so on purpose, because there are interesting rings for which the commutative law of multiplication does not hold.

Example 5. I will give you an example of a ***noncommutative ring***, i.e., a ring for which the commutative law of multiplication is not valid.

We use $M_{2\times 2}(\mathbb{R})$ to denote the set of all 2 by 2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with real entries (that is, such that a, b, c, d are real numbers).

Addition and multiplication in $M_{2\times 2}(\mathbb{R})$ are the usual operations of addition and multiplication of matrices:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix} \tag{1.4}$$

and

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \times \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}. \tag{1.5}$$

The zero of $M_{2\times 2}(\mathbb{R})$ is the matrix $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$.

It is easy (but very boring) to verify that ***the set*** $M_{2\times 2}(\mathbb{R})$***, with the operations of addition and multiplication defined by formulas (1.4) and (1.5) is a ring***.

Problem 5. ***Prove*** that in $M_{2\times 2}(\mathbb{R})$ the associative law of multiplication—that is, Axiom RA6—is true.

You have to prove that if A, B, C are 2×2 matrices, then $A(BC) = (AB)C$.

(HINT: Write $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$, $C = \begin{bmatrix} j & k \\ \ell & m \end{bmatrix}$, and compute both sides.)

Problem 6. ***Prove*** that in $M_{2\times 2}(\mathbb{R})$ the commutative law of multiplication is not valid. (HINT: Compute the products $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$ and $\begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \times \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.)

Now that we know that there exist rings for which the commutative law of multiplication does not hold, we give a name to those rings for which the law does hold:

Definition 2. A commutative ring is a ring for which Axiom RA10 (that is, the commutative law of multiplication) is true. □

1.4.2 Examples of commutative rings

The following are examples of commutative rings: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, as well as $\mathbb{Z}_n$ (the integers modulo n) for every natural number n such that $n > 1$.

The ring $M_{2\times 2}(\mathbb{R})$ that we studied before, in Example 5, is an example of a non-commutative ring.

1.4.3 The additive inverse; our first abstract algebra theorens

Axiom RA7 says that every member x of $\mathfrak{R}$ has an additive invers, i.e., a y such that $x + y = 0$.

Can we talk about ***the*** additive inverse of x? The asnwer would be "yes" if we knew that the additive inverse of x is unique, and "no" if it was not unique. (For example; we can say "Trenton is ***the*** capital of New Jersey", because New Jersey has only one capital, but we cannot say "Piscataway is ***the*** town in New Jersey", because New Jersey has lots of towns.)

It turns out that the answer is "yes, the additive inverse is unique". And this means that we can talk about ***the*** additive inverse of a mamber x of a ring $\mathfrak{R}$, and give it a name. And, as I am sure you have guessed, we will call it $-x$.

Theorem 1.. *Let $\mathfrak{R}$ be a ring, and let x be a member of x. Then there exists a unique $y \in \mathfrak{R}$ such that $x + y = 0$*

Proof. Axiom RA9 tells us that there exists a $y \in \mathfrak{R}$ siuch that $x + y = 0$. What is missing is proving that there is only one such y. So let us prove that.

We use the standard method for proving uniqueness: *if you have two of them, prove that they are the same.*

So let us suppose that y_1 and y_2, are members of $\mathfrak{R}$, such that $x + y_1 = 0$ and $x + y_2 = 0$. We want to prove that $y_1 = y_2$.

Using the ring axioms, we get

$$\begin{aligned} y_1 &= y_1 + 0 && (1.6)\\ &= y_1 + (x + y_2) && (1.7)\\ &= (y_1 + x) + y_2 && (1.8)\\ &= 0 + y_2 && (1.9)\\ &= y_2 + 0 && (1.10)\\ &= y_2\,, && (1.11) \end{aligned}$$

so $y_1 = y_2$. This proves the uniqueness of y. **Q.E.D.**

Problem 7. Write down the justifications of each of the six steps (1.6), (1.7), (1.8), (1.9), (1.10), (1.11) of the proof of Theorem 1.

And now that we know that the additive inverse of an $x \in \mathfrak{R}$ is unique, we can give it a name.

Definition 3. Let $\mathfrak{R}$ be a ring, and let x be a member of $\mathfrak{R}$. Then the unique $y \in \mathfrak{R}$ such that $x + y = 0$ is called minus x, or the negative of x, or the addittive inverse of x, and is denoted by the expression "$-x$".

It is then clear from Definition 3 that

$$(\forall x \in \mathfrak{R})x + (-x) = 0\,. \tag{1.12}$$

Using additive inverses, we can prove a very useful little theoren, called the ***cancellation law for addition***, because it tells us that when wwe have an equality $a + b = a + c$ we can "cancel" the a term and end up with $b = c$.

Theorem 2. *Let $\mathfrak{R}$ be a ring, and let a, b, c be members of $\mathfrak{R}$. Then, if $a + c = b + c$, it follows that $b = c$.*

Proof.

$$\begin{aligned}
b &= b + 0 && (1.13)\\
&= b + (a + (-a))) && (1.14)\\
&= (b + a) + (-a) && (1.15)\\
&= (a + b) + (-a) && (1.16)\\
&= (a + c) + (-a) && (1.17)\\
&= (c + a) + (-a) && (1.18)\\
&= c + (a + (-a)) && (1.19)\\
&= c + 0 && (1.20)\\
&= c\,. && (1.21)
\end{aligned}$$

So $b = c$. QED

Problem 8. Write down the justifications of each of the nine steps (1.13), (1.14), (1.15), (1.16), (1.17), (1.18), (1.19), (1.20), (1.21) of the proof of Theorem 2.

THE THREE NOTATIONS FOR MULTIPLICATION: $x.y$, xy, $x \times y$

Usually, we write "$x.y$" to denote the product of x and y (and we read this as "x times y".

But sometimes we write "'xy" rather than "$x.y$". (This is called juxtaposition: we write the name of one number and then the name of the other number, with nothing in between.)

The juxtaposition notation "xy" is more convenient when the numbers you are multiplying are being referred to by letter names, such as x, or y, or a, or b, or m, or n.

But when we are using ***numerals***[a], it would be disastrous if we used juxtaposition. For example, suppose we wanted to talk about "two times three", and we wrote "23". Then everybody would read this as "twenty-three"! So we do not want that. And it would not be any better if we wrote "2.3"? No! If we did this, then everybody would read "2.3" as "two point three", i.e., as the number which is equal to $\frac{23}{10}$, or $2 + \frac{3}{10}$. So, in order to avoid having these problems, we allow an alternative notation for the product of x times y, namely, "$x \times y$'.

And we use this notation for multiplication of numerals. So, for example, "two times three" is written as "2×3".

[a] A numeral is an expression that is the name of a natural number. For example, "1", "2", "35", "307", "$2,530,983$" are numerals. "Numeral" is not the same as "number". A numeral is not a number; it is a string of symbols that serves as the name of a number. And a numeral can stand for different numbers, depending on which number system you are working in. For example, in $\mathbb{Z}$ the numeral "85" stands for the number eighty-five. But in $\mathbb{Z}_{80}$ "85" is also another name for the number 5.

HOW TO READ THE "-" (MINUS) SIGN

I strongly recommend that you read "$-x$" as "minus x", rather that as "negative x".
Here is why: when you say "negative x", you are giving the strong impression that $-x$ is a negative number.
However, $-x$ ***need not be negative.*** For example, if $x = -5$, then $-x$ is 5, which is positive.
When you say "minus x", the danger that you will mistakenly think that $-x$ is negative is much smaller.

1.4.4 Multiplication by zero

As an application of the cancellation law, we prove that "anything multiplied by zero is zero".

Theorem 3. *Let $\mathfrak{R}$ be a ring. Then $x.0 = 0$ and $0.x = 0$ for every $x \in \mathfrak{R}$.*

Proof. We will prove that $(\forall x \in \mathfrak{R})x.0 = 0.$ and leave the proof of the other equality, i.e., $(\forall x \in \mathfrak{R})0.x = 0$, to the reader.

1. Let $x \in \mathfrak{R}$ be arbitrary.
2. $(\forall u)u = u.$ [Equality axiom]
3. $x.0 = x.0$ [Rule $\forall_{use}$]
4. $(\forall u \in \mathfrak{R})u + 0 = u).$ [Axiom RA8]
5. $0 + 0 = 0$ [Rule $\forall_{use}$]
6. $x.(0 + 0) = x.0$ [Rule SEE]
7. $x.(0 + 0) = x.0 + x.0$ [From Axiom RA7]
8. $x.0 + x.0 = x.0$ [Rule SEE]
9. $x.0 + 0 = x.0$ [Rule $\forall_{use}$, from Step 4]
10. $x.0 + x.0 = x.0 + 0$ [Rule SEE]
11. $x.0 = 0$ [From Theorem 2, and Step 10]

Q.E.D.

1.4.5 Unity; rings with unity

The basic axioms for rings never mention 1, and it is easy to give examples of rigns that do not have a "one" (see Example 7 on page 21 below). But first let us be precise:

Definition 4. In a ring $\mathfrak{R}$, a multiplicative identity, or unity, is a member u of $\mathfrak{R}$ such that $ux = x$ and $xu = x$ for every $x \in \mathfrak{R}$. □

And it is easy to prove that a unity, when it exists, is unique.

Theorem 4. *Let $\mathfrak{R}$ be a ring. Then, if a unity in $\mathfrak{R}$ exists, then there is only one unity in $\mathfrak{R}$.*

Proof. Suppose u, v are unities. Then $uv = u$, because v is a unity, so $(\forall x \in \mathfrak{R})xv = x$. And $uv = v$, because u is a unity, so $(\forall x \in \mathfrak{R})ux = x$. So $u = v$. **Q.E.D.**

Definition 5.

- A ring with unity is a ring $\mathfrak{R}$ equipped with a special member called 1 ("one") for which the following axioms hold:

THE MULTIPLICATIVE IDENTITY AXIOMS
RA11: $1 \in \mathfrak{R}$,
RA12: $(\forall x \in \mathfrak{R})(x.1 = x \wedge 1.x = x)$,
RA13: $1 \neq 0$.

- A commutative ring with unity is a commutative ring $\mathfrak{R}$ which is also a ring with unity.

So on a commutative ring with unity all 13 axioms RA1 through RA13 hold.

Example 6.

- The rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the $\mathbb{Z}_n$ for every n, are commutative rings with unity.

- The ring $M_{2\times 2}(\mathbb{R})$ introduced earlier in Example 5 is a ring with unity but is not commutative. The multiplicative identity of $M_{2\times 2}(\mathbb{R})$ is the 2×2 identity matrix $\mathbb{I}_2$, given by

$$\mathbb{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

- Let $\mathfrak{E}$ denote the set of all even integers. That is,

$$\mathfrak{E} = \{n \in \mathbb{Z} : 2|n\}.$$

  Then $\mathfrak{E}$ is a commutative ring without unity.

The following is an example of a commutative ring without unity:

Example 7. Let $\mathcal{E}$ be the set of all even integers. Then $\mathcal{E}$, with the same operations of addition and multplication as in $\mathbb{Z}$, is a commutative ring. And ***in $\mathcal{E}$ there are no units***. □

1.4.6 Unities in noncommiutative rings

As we defined it, a unity (or "multiplicative identity") of a ring $\mathfrak{R}$ is a member u of $\mathfrak{R}$ for which both equalities $x.u = x$ and $u.x = x$ hold for every $x \in \mathfrak{R}$. Naturally, if the ring $\mathfrak{R}$ is commutative, "$x.u = x$" and "$u.x = x$" are equivalent, so we could equally well have defined "unity" as a member u of $\mathfrak{R}$ for which $x.u = x$ for every $x \in \mathfrak{R}$.

If $\mathfrak{R}$ is not commutative, then the equalities "$x.u = x$" and "$u.x = x$" are not equivalent, so in principle we could consider and give a special name to members u of $\mathfrak{R}$ for which one of the equalities—but not both—holds for all $x \in \mathfrak{R}$.

So we can give the following defitniions:

Definition 6. In a ring $\mathfrak{R}$,

- A left multiplicative identity, or left unity, is a member u of $\mathfrak{R}$ such that $ux = x$ for every $x \in \mathfrak{R}$.

- A right multiplicative identity, or right unity, is a member u of $\mathfrak{R}$ such that $xu = x$ for every $x \in \mathfrak{R}$.

- A two-sided multiplicative identity, or two-sided unity, is a member u of $\mathfrak{R}$ which is both a left identity and a right identity.

  That is: a two-sided multiplicative identity is a member u of $\mathfrak{R}$ such that $xu = x$ and $ux = x$ for every $x \in \mathfrak{R}$. □

In Definition 4 we defined an "identity" to be what we are now calling "two-ided identity", and we proved that such an identity, if it exists, is unique. So some natural questions to ask now would be:

1. In a noncomutative ring $\mathfrak{R}$, is it necessarily true that a left identity, if it exists, is unique?

2. In a noncomutative ring $\mathfrak{R}$, is it necessarily true that a right identity, if it exists, is unique?

3. In a noncomutative ring $\mathfrak{R}$, is it necessarily true that a right identity is also a left identity?

4. In a noncomutative ring $\mathfrak{R}$, is it necessarily true that a left identity is also a rigth identity?

It turns out the the answer to all these questions is "no". To see this, it suffices to look at one example.

Example 8. Let us start with the noncommutative ring $M_{2\times 2}(\mathbb{R})$ of all 2×2 matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with real entries a, b, c, d. (This ring was described in Example 5.)

We then let $\mathfrak{R}$ be the subset of $M_{2\times 2}(\mathbb{R})$ consisting of all the matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ for which $c = d = 0$. That is, let

$$\mathfrak{R} = \left\{ \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{R} \right\}. \tag{1.22}$$

Mutiplication in $\mathfrak{R}$ is matrix multiplication. That is:

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix}. \tag{1.23}$$

Then it can be verified that

(1) $\mathfrak{R}$ is a noncommutative ring.

(2) $\mathfrak{R}$ has several (actually, infinitely many) left multiplicative identities.

(3) $\mathfrak{R}$ has no right multiplicative identities.

These three things are easy to prove, and I am asking you to do it. □

Problem 9. ***Prove*** the three statements (1), (2), (3) of Example 8. (HINTS:

1. To prove that $\mathfrak{R}$ is a ring, observe that
   (a) The members of $\mathfrak{R}$ are members of the ring $M_{2\times 2}(\mathbb{R})$, so the various commutative, associatve and distributive laws automatically hold in $\mathfrak{R}$, because they hold in $M_{2\times 2}(\mathbb{R})$. (For example, the associative law "$(\forall x \in \mathfrak{R})(\forall y \in \mathfrak{R})(\forall z \in \mathfrak{R})x(yz) = (xy)z$" is true because if x, y, z are in $\mathfrak{R}$ then x, y, z are in $M_{2\times 2}(\mathbb{R})$, so $x(yz) = (xy)z$ because the associative law of multiplication holds in $M_{2\times 2}(\mathbb{R})$.)
   (b) So in order to prove that $\mathfrak{R}$ is a ring, all we need to show is that if $x, y \in \mathfrak{R}$ then $x + y$, xy, and $-x$ are in $\mathfrak{R}$
2. To prove that $\mathfrak{R}$ is noncommutative it suffices to find two members x, y of $\mathfrak{R}$ such that $xy \neq yx$.
3. To prove that $\mathfrak{R}$ has many left identities, write out explicitly the condition that a member $u = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ must satisfy for u to be a left identity. (Since
$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \times \begin{bmatrix} r & s \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} ar & as \\ 0 & 0 \end{bmatrix},$$
u is a left multiplicative identuty if and only if $ar = r$ and $as = s$ for all r, s. This means that a must equal 1, and b can be any real number whatsoever.)
4. To prove that $\mathfrak{R}$ has no right identities, do a calculation similar to that of the previous step, write out explicitly the condition that a member $u = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}$ must satisfy for u to be a right identity, and show that it is not possible to find a, b for which the condition is true.

In the previous example, we found a noncommutative ring that has many left identities and no right identity. A natural question is:

(*) In a noncomutative ring $\mathfrak{R}$, is it possible that there is more that one left identity and also more than one right identity?

Remarkably, the answer is "no", because of the following very simple theorem:

Theorem 5. *If a ring $\mathfrak{R}$ has a left identity u and a right identity v, then*

1. *$u = v$,*
2. *$\mathfrak{R}$ has no left identity other than u,*
3. *$\mathfrak{R}$ has no right identity other than v.*

Proof.
Since u is a left identity, $ux = x$ for all $x \in \mathfrak{R}$, so in particular $uv = v$.
Since v is a right identity, $xv = x$ for all $x \in \mathfrak{R}$, so in particular $uv = u$.
So $uv = v$ and $uv = u$. Hence $u = v$. This proves statement (1).
To prove (2), assume there was another left identity u'.
Then ny part (1), $u' = v$ as well, so $u' = u$, and this proves statement (2).
To prove (3), assume there was another right identity v'.
Then ny part (1), $v' = u$ as well, so $v' = uv$, and this proves statement (3).
Q.E.D.

1.4.7 Fields

Definition 7. A field is a commutative ring with unity $\mathfrak{R}$ for which the following Multiplicative Inverse Axiom holds:

THE MULTIPLICATIVE INVERSE AXIOMS

RA14: For every $x \in \mathfrak{R}$ such that $x \neq 0$ there exists a $y \in \mathfrak{R}$ such that $xy = 1$. (In formal langauge: $(\forall x \in \mathfrak{R})(x \neq 0 \Longrightarrow (\exists y \in \mathfrak{R})xy = 1)$.)

So in a field all fourteen axioms RA1 to RA14 hold.

Example 9.

- $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields.
- $\mathbb{Z}$ is not a field.
- We will prove later that
  - If $n \in \mathbb{N}$ and n is prime, then $\mathbb{Z}_n$ is a field.
  - If $n \in \mathbb{N}$, $n > 1$, and n is not prime, then $\mathbb{Z}_n$ is not a field.

1.4.8 Is there a cancellation law for multiplication?

Exactly as we proved that, in a ring $\mathfrak{R}$, if we have an equality $a + b = a + c$ then we can "cancel" the a and conclude that $b = c$, one would expect to be able to prove a similar result for multiplication: if $ab = ac$ then $b = c$. This, however, is clearly impossible. For example, in the integers (or in any ring), $0.b = 0$ and $0.c = 0$ for every b, c, so if there was a cancellation law for multiplication, it would follow that $b = c$, for all b and all c.

It turns out that if we only try to cancel a when a is different from zero, then this is possible: in some rings but not in all of them.

One example of a class of rings for which the cancellation law for multiplication is valid is that of ***fields***.

Theorem 6. *Let $\mathfrak{R}$ be a field. Then the following cancellation law for multiplication holds:*

$$(\forall a \in \mathfrak{R})(\forall b \in \mathfrak{R})(\forall c \in \mathfrak{R})\Big((a \neq 0 \wedge ab = ac) \Longrightarrow b = c\Big)\,. \tag{1.24}$$

Proof. Since $a \neq 0$, it follows from Axiom RA15 that there exists $u \in \mathfrak{R}$ such that $ua = 1$. Then

$$\begin{aligned} b &= 1.b && (1.25)\\ &= (u.a).b && (1.26)\\ &= u.(a.b) && (1.27)\\ &= u.(a.c) && (1.28)\\ &= (u.a).c && (1.29)\\ &= 1.c && (1.30)\\ &= c\,. && (1.31) \end{aligned}$$

So $b = c$. **Q.E.D.**

Problem 10. Write down the justifications of each of the seven steps (1.25), (1.26), (1.27), (1.28), (1.29), (1.30), (1.31), of the proof of Theorem 6.

1.4.9 A few very simple proofs: $2 + 2 = 4$, etc.

From now on, until further notice, we work on a commutative ring with unity, called $\mathfrak{R}$. So, for example:

- *When we write "$(\forall x)$" or "$(\exists x)$", this means "$(\forall x \in \mathfrak{R})$" or "$(\exists x \in \mathfrak{R})$" (See the box on page 6.)*
- *The word "number" means "member of $\mathfrak{R}$".*

Why are we working on a general commutative ring with unity? The main reason is that, once we prove something in such a general situation, then the result is automatically valid in all the commutative rings with unity that we know, that is, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the $\mathbb{Z}_n$. (And if we learn about a new commutative ring with unity $\mathfrak{A}$, then the result will be known to be valid in $\mathfrak{A}$ as well.)

If you want to, you can think that we are working, say, just on $\mathbb{Z}$. But then if you want to use the same theorem for another ring, such as $\mathbb{R}$, you would have to do one of two things:

- *Prove the theorem again on $\mathbb{R}$,*
- *Quote the theorem proved for $\mathbb{Z}$, and point out that "the proof only uses the axioms for a commutative ring with unity, so the result is valid on $\mathbb{R}$ as well".*

In my view, it is much better to prove the theorems directly, once and for all, in the most general possible setting.

Definition 8. $2 = 1 + 1$. □

Definition 9. $3 = 2 + 1$. □

Definition 10. $4 = 3 + 1$. □

And, now that we know what 1, 2, 3, and 4 are, we are ready to prove a theorem.

Theorem 7. $2 + 2 = 4$.

Proof. First, we observe that

$$2 + 2 = 2 + 2\,, \tag{1.32}$$

by the Equality Axiom.

On the other hand,

$$2 = 1 + 1$$

by Definition 8.

Hence Rule SEE enables us to conclude that

$$2 + 2 = 2 + (1 + 1)\,. \tag{1.33}$$

On the other hand,

$$2 + (1 + 1) = (2 + 1) + 1\,, \tag{1.34}$$

by the associative law of addition.

Hence

$$2 + 2 = (2 + 1) + 1\,. \tag{1.35}$$

But

$$2 + 1 = 3\,, \tag{1.36}$$

by Definition 9.

Hence

$$2 + 2 = 3 + 1\,. \tag{1.37}$$

Finally, Definition 9 tells us that

$$3 + 1 = 4\,. \tag{1.38}$$

Hence

$$\boxed{2+2=4}\,. \tag{1.39}$$

Q.E.D.

What does "Q.E.D." mean?

"Q.E.D." stands for the Latin phrase *quod erat demonstrandum*, meaning "which is what was to be proved". It is used to indicate the end of a proof.

Theorem 8. $2 \times 2 = 4$.

Proof. The Equality Axiom implies that

$$2 \times 2 = 2 \times 2\,. \tag{1.40}$$

And Definition (8) tells us that $2 = 1 + 1$. So, using Rule SEE, we get

$$2 \times 2 = 2 \times (1 + 1)\,. \tag{1.41}$$

By the distributive law of addition,

$$2 \times (1 + 1) = 2 \times 1 + 2 \times 1\,. \tag{1.42}$$

Hence

$$2 \times 2 = 2 \times 1 + 2 \times 1\,. \tag{1.43}$$

By Basic Fact BFN4A, $2 \times 1 = 2$. Hence

$$2 \times 2 = 2 + 2\,. \tag{1.44}$$

Finally, Theorem 7 tells us that $2 + 2 = 4$. it follows that

$$\boxed{2 \times 2 = 4}\,. \tag{1.45}$$

Q.E.D.

So far, we have introduced and given names to four integers, namely, 1, 2, 3, and 4. We can then go on and introduce a few more.

Definition 11. $5 = 4 + 1$. □

Definition 12. $6 = 5 + 1$. □

Definition 13. $7 = 6 + 1$. □

Definition 14. $8 = 7 + 1$. □

Definition 15. $9 = 8 + 1$. □

And we can prove things about these numbers, such as, for example:

Theorem 9. $3 + 3 = 6$.

Proof. YOU DO THIS ONE.

Theorem 10. $3 \times 2 = 6$.

Proof. YOU DO THIS ONE.

Theorem 11. $4 + 3 = 7$.

Proof. YOU DO THIS ONE.

Problem 11. Prove Theorems 9, 10, and 11. In each proof, you are allowed to use the basic facts known so far, the definitions given so far, and the theorems proved so far. So, for example: in your proof of Theorem 9 you are allowed to use the basic facts, definitions 8, 9, 10, 11, 12, 13, 14, 15, and Theorems 7 and 8; in your proof of Theorem 10 you are allowed to use the basic facts, definitions 8, 9, 10, 11, 12, 13, 14, 14, and Theorems 7, 8, and 9; and in your proof of Theorem 11 you are allowed to use the basic facts, definitions 8, 9, 10, 11, 12, 13, 14, 14, Theorems 7, 8, 9; and 10.

Theorems 7, 8, 9, and 10. □

1.4.10 Divisibility; factors

In this section we are particularly interested in the integers and their divisibility properties. But we will state the general definitions for a general commoutative ring $\mathfrak{R}$ with unity.

If $a \in \mathfrak{R}$ and $b \in \mathfrak{R}$, you would like to "divide a by b", and obtain a "quotient" q, i.e., a $q \in \mathfrak{R}$ that multiplied by b gives you back a.

For example, if $\mathfrak{R}$ was a field, then this would always be possible (if $b \neq 0$), because b has a multiplicative inverse c, and then $a = 1.a = (b.c).a = b.(c.a)$, so we can take $q = c.a$, and we get $a = b.q$.

But on a general commutative ring with unity, such as $\mathbb{Z}$, it is not always possible to divide a by b.. For example, in $\mathbb{Z}$, if $a = 4$ and $b = 3$, then an integer q such that $3q = 4$ does not exist[9] Since dividing a by b is sometimes possible and sometimes not, we will introduce some new words to describe those situations when division is possible.

"DIVIDES", "IS DIVISIBLE BY", "FACTOR", "MULTIPLE"

Definition 16. Let $\mathfrak{R}$ be a commutative ring with unity, and let $a \in \mathfrak{R}$, $b \in \mathfrak{R}$.

1. We say that b is a factor of a if there exists a $k \in \mathfrak{R}$ such that
$$a = bk\,.$$
2. We say that a is a multiple of b if b is a factor of a.
3. We say that b divides a if b is a factor of a.
4. We say that a is divisible by b if b divides a.
5. We write
$$b|a$$
to indicate that b divides a. □

Remark 1. As the previous definition indicates, the following are five different ways of saying exactly the same thing:

- m divides n,
- m is a factor of n,
- n is a multiple of m,
- n s divisible by m,
- $m|n$. □

[9]You may say that "the result of dividing 4 by 3 is the fraction $\frac{4}{3}$". That is indeed true, but $\frac{4}{3}$ ***is not in*** $\mathbb{Z}$***.r***.

.

Reading statements with the "divides" symbol "|"

The symbol "|" is read as "divides", or "is a factor of".
For example, the statement "3|6" is read as "3 divides 6", or "3 is a factor of 6". And the statement "3|5" is read as "3 divides 5", or "3 is a factor of 5". (Naturally, "3|6" is true, but "3|5" is false.)
The vertical bar of "divides" has nothing to do with the bar used to write fractions. For example, "$3|6$***" is the statement***[a] ***"***3 ***divides*** 6***', which is true. And "***$\frac{3}{6}$***" is a noun phrase: it is one of the names of the number also known as "***$\frac{1}{2}$***", or "***0.5***".***

[a] A statement is something we can say that is true or false. A noun phrase is something we can say that stands for a thing or person. For example, "Mount Everest", "New York City", "My friend Alice", "The movie I saw on Sunday", are noun phrases. "Mount Everest is very tall", "I live in New York City", "My friend Alice studied mathematics at Rutgers", and "The movie I saw on Sunday was very boring", are statementsd.

Let us prove some theorems about divisibility. We work in a commutative ring $\mathfrak{R}$ with unity.

Theorem 12. *If a, b, c are members of $\mathfrak{R}$ such that a divides b and a divides c, then a divides $b + c$.*

Proof. Since $a|b$, Definition 16 tells us that we may pick $j \in \mathfrak{R}$ such that

$$b = aj\,. \tag{1.46}$$

Since $a|c$, Definition 16 tells us that we may pick $k \in \mathfrak{R}$ such that

$$c = ak\,. \tag{1.47}$$

Then

$$b + c = aj + ak\,. \tag{1.48}$$

The distributive law (Axiom RA7) tells us that

$$aj + ak = a(j + k)\,. \tag{1.49}$$

Therefore

$$b + c = a(j + k)\,. \tag{1.50}$$

Since $j \in \mathfrak{R}$ and $k \in \mathfrak{R}$, it follows that $j + k \in \mathfrak{R}$.

Hence Equation (1.50) implies that the exists an $\ell \in \mathfrak{R}$ such that $b + c = a\ell$. (It suffices to take $\ell = j + k$.)

So $\boxed{a \text{ divides } b + c}$. **Q.E.D.**

Theorem 13. *If a, b, c are members of $\mathfrak{R}$ such that a divides b and b divides c, then a divides c.*

Proof. **YOU DO THIS ONE.**

Problem 12. Prove Theorem 13

Corollary 1. *If a, b, c are members of $\mathfrak{R}$ such that a divides b, then a divides bc.*

Proof.

It follows from the definition of "divides" (Definition 16) that b divides bc.

So a divides b and b divides bc.

Therefore Theorem 13 tells us that $\boxed{a \text{ divides } bc}$.

Q.E.D.

1.4.11 More easy theorems

Here are some very easy but important theorems. Proving these things is the boring part of doing mathematics, and when you are an experienced mathematician you would not waste any time doing these proofs, but that's because it's easy to figure out how to do them. A beginner should know how to do these proofs, and then, once you know how to do them, you will not need to do them any more.

Theorem 14. *If $u \in \mathfrak{R}$, then*

$$-(-u) = u\,.$$

Proof.

$u + (-u) = 0$, because of Definition 3 and Equation (1.12).

$(-u) + u = u + (-u)$, by the commutative law of addition.

$(-u) + u = 0$, by Rule SEE.

$(-u) + (-(-u)) = 0$, because of Definition 3 and Equation (1.12).

$(-u) + u = (-u) + (-(-u))$, by Rule SEE.

$u = -(-u)$, by the cancellation law for addition (Theorem 2).

Q.E.D.

Theorem 15. *If $u \in \mathfrak{R}$, and $nv \in \mathfrak{R}$, then*

$$-uv = (-u).v \text{ and } uv = u(-v)\,.$$

Proof.

Let $u \in \mathfrak{R}$ $v \in \mathfrak{R}$ be arbitrary.

We will prove that $uv = (-u)v$. And we leave the other equality, $-uv = u(-v)$, to the reader.

Then

$$\begin{aligned}
-uv &= (-uv) + 0 && (1.51)\\
&= -(uv) + 0.v && (1.52)\\
&= -(uv) + (u + (-u)).v && (1.53)\\
&= -(uv) + \Big(uv + (-u)v\Big) && (1.54)\\
&= \Big((-uv) + uv\Big) + (-u)v && (1.55)\\
&= \Big(uv + (-uv)\Big) + (-u)v && (1.56)\\
&= 0 + (-u)v && (1.57)\\
&= (-u)v + 0 && (1.58)\\
&= (-u)v\,. && (1.59)
\end{aligned}$$

So $\boxed{-uv = (-u)v}$. **Q.E.D.**

Problem 13. **Provide the justification** of each of the nine steps (1.51), (1.52), (1.53), (1.54), (1.55), (1.56), (1.57), (1.58), (1.59), of the proof of Theorem 15.

Theorem 16. *If* $u \in \mathfrak{R}$ *then* $-u = (-1).n$.

Proof. Let $u \in \mathfrak{R}$ be arbitrary. Then

$$\begin{aligned} (-1).u &= -(1.u) && (1.60)\\ &= -u\,. && (1.61) \end{aligned}$$

So $\boxed{(-1).u = -u.}$ **Q.E.D.**

Theorem 17. *If* $u \in \mathfrak{R}$ *and* $v \in \mathfrak{R}$*, then*

$$(-u).(-v) = mn\,.$$

Proof. Let $u \in \mathfrak{R}$, $v \in \mathfrak{R}$ be arbitrary. Then

$$\begin{aligned} (-u).(-v) &= u.(-(-v))) && (1.62)\\ &= u.\,. && (1.63) \end{aligned}$$

So $\boxed{(-u).(-v) = mn\,.}$ **Q.E.D.**

Problem 14. **Provide the justification** of

1. each of the two steps (1.60), (1.61) of the proof of Theorem 16,
2. each of the two steps (1.62), (1.63) of the proof of Theorem 17. □

Now I would like to talk about the operation of ***subtraction*** of integers. But before I do that let us say a few words about operations in general.

1.4.12 Subtraction

We would like to be able to talk about the ***difference*** of two numbers m and n, i.e., the number $m - n$. The ri ng axioms do not say anything about differences. But they tell us that for every number x there is a number y such that $x + y = 0$, and we have proved that this number is unique and given it the name $-x$. Using this, it is easy to define subtraction.

Definition 17. If $u \in \mathfrak{R}$ and $v \in \mathfrak{R}$, then $u - v$ (read as "u minus v") is the number $u + (-v)$. □

And then we can prove a simple formula that you already know:

Theorem 18. *If $u \in \mathfrak{R}$ and $v \in \mathfrak{R}$, then*

$$(u - v) + v = u\,.$$

Proof. Let $u \in \mathfrak{R}$, $b \in \mathfrak{R}$ be arbitrary. Then

$$\begin{aligned}
(u - v) + v &= u + (-v)) + v && (1.64)\\
&= u + ((-v) + v) && (1.65)\\
&= u + (v + (-v)) && (1.66)\\
&= u + 0 && (1.67)\\
&= u\,. && (1.68)
\end{aligned}$$

So $\boxed{(u - v) + v = u}$, as desired. **Q.E.D.**

Problem 15. **Provide the justification** of each of the five steps (1.64), (1.65), (1.66), (1.67), (1.68) of the proof of Theorem 18. □

1.4.13 A few elementary formulas

You are certainly familiar with the formulas $(a + b)^2 = a^2 + 2ab + b^2$, and $(a - b)(a + b) = a^2 - b^2$. What do those formulas become for general rings?

First we need to define "square".

Definition 18. Let $\mathfrak{R}$ be a ring, and let $a \in \mathfrak{R}$. The square of a is the member a^2 of $\mathfrak{R}$ given by

$$a^2 = a.a\,. \tag{1.69}$$

Theorem 19. *Let $\mathfrak{R}$ be a ring, and let $a, b \in \mathfrak{R}$. Then*

$$(a + b)^2 = a^2 + ab + ba + b^2\,. \tag{1.70}$$

If $\mathfrak{R}$ is a commutative ring with unity, then Formula (1.70) becomes

$$(a + b)^2 = a^2 + 2ab + b^2\,. \tag{1.71}$$

Remark 2. What is the precise meaning of the sum in the right-hand side of Formula (1.70)? Addition is a ***binary*** operation: it makes sense to talk about the sum $x+y$ of ***two*** numbers. But, what is the meaning of $x+y+z$? The answer is: "$x+y+z$" means $(x+y)+z$, or $x+(y+z)$, whichever one you prefer. It does not matter which of the two you use, because $(x+y)+z$ and $x+(y+z)$ are equal, thanks to the associative law of addition.

Similarly, "$x+y+z+w$" means $(x+y)+(z+w)$, or $\big(x+(y+z)\big)+w$, or $\big((x+y)+z\big)+w$, or $x+\big((y+z)+w\big)$, or or $x+\big(y+(z+w)\big)$ whichever one you prefer. And it does not matter which of the two you use, because $(x+y)+(z+w)$, $\big(x+(y+z)\big)+w$, $\big((x+y)+z\big)+w$, $x+\big((y+z)+w\big)$, and $x+\big(y+(z+w)\big)$ are all equal, thanks to the associative law of addition.

Proof of Theorem 19.
We have

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b)\\ &= a(a+b)+b(a+b)\\ &= (aa+ab)+(ba+bb)\\ &= a^2+ab+ba+b^2\,.\end{aligned}$$

This proves Formula 1.70.

If $\mathfrak{R}$ is commutative, then $ab=ba$, so we can rewrite Formula 1.70 as

$$(a+b)^2 = a^2+ab+ab+b^2\,.$$

If in addition $\mathfrak{R}$ has a unity, then $ab+ab = 1.ab+1.ab = (1+1)ab = 2ab$, so we get Formula 1.71. **Q.E.D.**

Problem 16. Do what we did in Theorem 19 for the formula for $(a+b)(a-b)$. That is, write the statement of the theorem analogous to Theorem 19, and prove it. □

Problem 17. Do what we did in Theorem 19 for the formula for $(a+b)^3$. That is, write the definition of "cube", and then write the statement of the theorem analogous to Theorem 19, and prove it. □

1.5 Even and odd numbers

From now on, until further notice, I will be talking about "integers", but everything I say will be equally

valid if, instead of $\mathbb{Z}$, we work on an arbitrary commutative ring $\mathfrak{R}$ with unity.

There will be a very precise point when this stops: I will bring in a couple of facts, especially induction,, that are only valid for $\mathbb{Z}$, and from that moment on we will be proving results that are only valid for $\mathbb{Z}$.

1.5.1 The meaning of "even" and "odd" for integers

One of the most common properties of integers that mathematicians study is their ***parity***, that is, whether they are even or odd.

We will begin by giving a precise definition of what it means for an integer to be "even", and what it means to be "odd".

Definition 19. An integer n is <u>even</u> if n is divisible by 2.
Equivalently, n is <u>even</u> if $(\exists k \in \mathbb{Z})n = 2k$. □

Definition 20. An integer n is <u>odd</u> if $n - 1$ is even.
Equivalently, n is <u>odd</u> if $(\exists k \in \mathbb{Z})n = 2k + 1$. □

Example 10.

1. The number 0 is even, because $0 = 2 \times 0$, so 0 is divisible by 2.
2. The number 1 is odd, because $1 - 1 = 0$, so $1 - 1$ is even.
3. The number 2 is even, because $2 = 2 \times 1$, so 2 is divisible by 2.
4. The number 3 is odd, because $3 - 1 = 2$, and 2 is even. □
5. The number 0 is even, because $0 = 2 \times 0$, so $2|0$.
6. The number -1 is odd, because $(-1) - 1 = -2$, and $-2 = 2 \times (-1)$, so -2 is even and then -1 is odd. □

1.5.2 The parity of a sum and a product

We can now prove the rules that I am sure you know: "even plus even is even", "odd plus even is odd", "odd plus odd is even", "even times anything is even", "odd times odd is odd".

Theorem 20. *The sum of two even integers is even. That is: if a and b are integers and both a and b are even, then $a + b$ is even.*

Proof.

Let a and b be arbitrary even integers.
Then a and b are divisible by 2.
But we know (from Theorem 12 on page 31) that if x, y, z are integers such that $x|y$ and $y|z$ then $x|y + z$. Therefore $a + b$ is divisible by 2.

So $\boxed{a + b \text{ is even}}$. **Q.E.D.**

Theorem 21. *The sum of an even integer and an odd integer is an odd integer. That is: if a and b are integers, a is even, and b is odd, then $a + b$ is odd.*

Proof.
Let a, b be arbitrary integers.
Suppose a is even and b is odd.
Then Definition 20 tells us that $b - 1$ is even.
So it follows from Theorem 20 that $a + (b - 1)$ is even.
But $a + (b - 1) = (a + b) - 1$.
So $(a + b) - 1$ is even.
Therefore Definition 20 tells us that $\boxed{a + b \text{ is odd}}$. **Q.E.D.**

Problem 18. ***Prove*** that the product of two even integers is divisible by 4. □

Next, we prove that "odd plus odd is even", that is, that the sum of two odd integers is an even integer.

Theorem 22. *The sum of two odd integers is an even integer. That is: if a and b are integers, and a and b are both odd, then $a + b$ is even. (Or, in fully formal language: $(\forall a \in \mathbb{Z})(\forall b \in \mathbb{Z})(\text{if } 2|a - 1 \text{ and } 2|b - 1 \text{ then } 2|a + b)$.)*

Proof.
Let a, b be arbitrary integers.
Assume that a and b are odd.
We want to prove that $a + b$ is even.
Since a is odd, $a - 1$ is even.
Since b is odd, $b - 1$ is even.
Since the sum of two even integers is even, $(a - 1) + (b - 1)$ is even.
But $(a - 1) + (b - 1) = (a + b) - 2$.
So $(a + b) - 2$ is even.
On the other hand, 2 is even.
So the sum $\Big((a + b) - 2\Big) + 2$ is even.
But $\Big((a + b) - 2\Big) + 2 = a + b$.
So $\boxed{a + b}$ is even.

Q.E.D.

Next, we prove that "even times anything is even". The precise statement of this is as follows:

Theorem 23. *The product of two integers, one of which is even, is an even natural number. That is: if a, b are integers, and a is even or[10] b is even, then ab is even.*

Proof. Without loss of generality[11], we may assume that a is even.
Since a is even, we can write $a = 2k$ for some integer k.
Then $ab = (2k)b = 2(kb)$.
Since kb is an integer, it follows from Definition 19 that $\boxed{ab \text{ is even}}$.

Q.E.D.

Now that we know what happens to the product of two integers when one of them is even, there remains the case when both are odd.

Theorem 24. *The product of two odd integers is odd. That is: if a and b are odd integers, then ab is odd.*

[10] See the box on page 43 for a detailed explanation of the meaning of "or". In particular, it is important to understand that "or", im mathematics, is always ***inclusive***. So, for example, "a is even or b is even" is true when a is even, when b is even, and when both a and b are even.

[11] See the box on "Without loss of generality", on page 42.

Proof. **YOU DO THIS ONE.**

Problem 19. ***Prove*** Theorem 24. □

1.5.3 The parity of $-n$

We have already described how evenness and oddness behave when we add and multiply integers. Addition and multiplication are two of the three operations on integers that occur in the basic facts. Another important operation on integers is the unary operation "minus", so we have to see how this operation is related to evenness and oddness.

The answer is very simple:

Theorem 25. *If n is an integer, then*

- *If n is even then $-n$ is even.*
- *If n is odd then $-n$ is odd.*

Proof. YOU DO THIS ONE.

Problem 20. ***Prove*** Theorem 25. □

1.5.4 The parity of a successor: parity reversal

The successor of an integer n is the integer $n + 1$. And it is important to know how the parity of $n + 1$ is related to that of n.

The answer to this is quite easy. It is given by the following *parity reversal theorem*, that says that the parity of $n+1$ is exactly the opposite of the parity of n:

Theorem 26. *Let n be an integer. Then*

(1) If n is even then $n + 1$ is odd.
(2) If n is odd then $n + 1$ is even.
(3) If $n + 1$ is even then n is odd.
(4) If $n + 1$ is odd then n is even.

Proof.

Proof of statement (1):

Suppose n is even.
To prove that $n+1$ is odd, we have to show that $(n+1)-1$ is even.
But $(n+1)-1 = n$, and n is even.
Hence $\boxed{n+1 \text{ is odd}}$ by Theorem 21.

Proof of statement (2):

Suppose n is odd.
According to Definition 20, $n-1$ is even.
Also, we know that 2 is even.
So, by Theorem 20, $(n-1)+2$ is even.
But $(n-1)+2 = n+1$.
So $\boxed{n+1 \text{ is even}}$.

Proof of statement (3):

Suppose $n+1$ is even.
It is clear that -2 is even. (Reason: $-2 = 2 \times (-1)$, so $2|-2$.)
Theorem 20 then tell us that $(n+1)+(-2)$ is even.
But $(n+1)+(-2) = n-1$.
So $n-1$ is even.
Then, according to Definition 20, $\boxed{n \text{ is odd}}$.

Proof of statement (4):

Suppose $n+1$ is odd.
Then Definition 20 tells us that $(n+1)-1$ is even.
But $(n+1)-1 = n$.
So $\boxed{n \text{ is even}}$.

We have thus completed the proofs of all four statements. **Q.E.D.**

Without loss of generality

Suppose we want to prove that something happens in each of two (or three, or four) possible cases. Suppose all the cases are "the same", in the following precise sense: each of the cases becomes Case 1 if you just change the names of the objects involved. Then it suffices to do the proof for Case 1, because the statement for the other cases follows easily by just applying the result of Case 1.
When we are in this situation, we can say "assume, without loss of generality, that are in case 1". What this means is that, ***once we prove our result for Case 1, the result for the other cases follows automatically, and there is no need to write a separate proof for each case.*** Why is this so? The reason is that, once we have the result for Case 1, then the result for the other cases follows from this by just changing the names of the objects involved.
EXAMPLE: Suppose we want to prove that "if a is even or b is even then ab is even". Then we have to consider two cases: when a is even and when b is even. Suppose we prove what we want in the first case, when a is even. That is, we prove that "if a is even then ab is even". Then the result for the second case "if b is even then ab is even") follows immediately, because we can apply the first result with "b"in the role of "a" and "a" in the role of "b". (If you do not feel comfortable with this, think of it as follows: if we have proved that "if a is even then ab is even", then we could equally well state our result by saying that "if x is even then xy is even". But then the fact that "if b is even then ab is even follows by applying our first result with b in the role of x and a in the role of y.

1.5.5 Introduction to the proof that "every integer is even or odd and not both"

We would now like to prove that an integer cannot be both even and odd, and it has to be either even or odd.
That is, we want to prove that:

(A) If $n \in \mathbb{Z}$ then n is even or n is odd.

(B) If $n \in \mathbb{Z}$ is even then n is not odd.

(C) If $n \in \mathbb{Z}$ is odd then n is not even.

The meaning of "or" in mathematics

In English, when we use the word "or", it can have two different meanings:

1. ***Inclusive*** "or", that is, "one or the other or both".

or

2. ***Exclusive*** "or", that is, "one or the other but not both".

For example, if a store announces that

> If you are a student or a senior citizen then you are entitled to a 15% discount on your purchases.

then, obviously, anyone who is both a student and a senior citizen will be entitled to a discount. So this is an example of ***inclusive*** or.
On the other hand, if a restaurant waiter asks you "would you like tea or coffee?", then it is clear that you can have one or the other but not both, so this an example of ***exclusive*** or.

In mathematics, "or" is always inclusive.

So, if I say, for example,

> if a and b are integers and a is even or b is even, then the product ab is even,

then this also applies to the case when both a and b are even.

It turns out that ***we cannot prove (A), (B) and (C) using the basic facts about the integers that we have so far.*** And when I say "we cannot prove (A) and (B)" I do not mean that "it is very hard to prove (A) and (B)", or "nobody has figured out yet how to prove (A) and (B) but maybe some day somebody will". I mean something much stronger: ***I can prove to you that statements (A), (B) and (C) cannot be proved***

from the basic facts about the integers that we know so far, that is, from the axioms for a commutative ring with unity (that is, Axioms RA1 to RA9 on page 13, axiom RA10 on page 14, and axioms RA11 to RA13 on page 20).

You may find this hard to believe. How can I ***prove*** that something cannot be proved?

Actually, there is one obvious way for this to happen: if a statement is false, then it cannot be proved. So for example, it is not possible to prove that 4 is prime, because the statement "4 is prime" is false.

But that is not what we are talking about here. What we are talking about here is ***statements that are true but cannot be proved.*** How can that be?

Actually, if you think about this for a few minutes you will see that it is quite easy to see how this could happen. We can only talk about proofs ***from a set of axioms***. These axioms give us a list of things we know, and the game we play in Mathematics is that of proving, starting from those axioms, lots of other things.

Then we can ask: what if our axioms do not contain enough information about the object of interest to us[12]? That would mean that there are things that are true but our axioms aren't enough to imply those things.

Take an extreme hypothetical situation: suppose the set of axioms was the empty set. That is, suppose we had no axioms at all. Then we would not be able to prove anything, and yet there would still be millions of true statements.

All we are saying here is this: ***the axioms for a commutative ring with unity are not enough to imply all the statements that are true for*** $\mathbb{Z}$***.*** And the reason for this is very simple:

- $\mathbb{Z}$ is a commutative ring with unity, but so are $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the systems $\mathbb{Z}_n$, for every $n \in \mathbb{N}$ such that $n > 1$.

- Threfore any fact about $\mathbb{Z}$ that can be proved from the axioms for a commutative ring with unity must also be true in $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, and the systems $\mathbb{Z}_n$, for every $n \in \mathbb{N}$ such that $n > 1$.

- Statements (B) and (C) are false in $\mathfrak{R}$ if $\mathfrak{R} = \mathbb{Q}$ or $\mathfrak{R} = \mathbb{R}$, or $\mathfrak{R} = \mathbb{C}$. (Proof: $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields (see section 1.4.7, on page 24). Also,

[12] That is, in this case, about $\mathbb{Z}$.

in $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$, 2 is different from zero. So for every $x \in \mathfrak{R}$ there exist $y \in \mathfrak{R}$ and $z \in \mathfrak{R}$ such that $x = 2y$ and $x - 1 = 2z$. So x is even—because $x = 2y$—and x is odd—because $x = 2z + 1$. So every $s \in \mathfrak{R}$ is both even and odd.)

- So, even though (B) and (C) are true in $\mathbb{Z}$, (B) and (C) cannot be proved from the axioms of a commutative ring with unity, because if they could be proved from the axioms of a commutative ring with unity they would have to be true in every commutative ring with unity, but we know they are not true in $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.

- A similar argument applies to (A): one can construct[13] a commutative ring with unity $\mathfrak{R}$ such that (A) is not true on $\mathfrak{R}$. And this implies that (A) cannot be proved from (A).

Problem 21. Construct a commutative ring with unity $\mathfrak{R}$ such that (A) is not true on $\mathfrak{R}$.

HINT: Take $\mathfrak{R}$ to be the set of complex numbers $a + bi$ such that a and b are integers[14]. Verify that i (or $2 + i$, or $2 + 3i$) is neither even nor odd. □

In order to develop a better understanding of our problem, let us temporarily agree to call an integer n "good" if it has the property we are interested in. That is, "n is good" means "n is even or odd and not both even and odd".

Then our objective is to prove that every integer is good.

And the idea of how to do it is to follow a four-step program

1. First, we will prove that 1 is odd and not even, so 1 is good.

2. Next, we will prove that goodness is passed on from each natural number to its successor; that is: if a natural number n is good then $n + 1$ is good.

3. From the two facts above, it will follow that every natural number is good, but we will need a new and very important new basic fact to prove that, namely, the Principle of Mathematical Induction.

[13] Se Problem 21.

[14] This is a very important ring. It is called the ***ring of Gaussian integers***, and its members are the ***Gaussian integers***.

4. Finally, once we know that every natural number is good, it will be easy to conclude, using Theorem 25, that every integer is good.

So the Principle of Mathematical Induction will be needed for step 2 if the four-step program. But it will turn out that, in order to carry out the first step, i.e., to prove that 1 is good, we will need the following fact:

The successor theorem. If n is a natural number and $n \neq 1$ then $n-1$ is a natural number[15]. (That is, $(\forall n \in \mathbb{N})(n \neq 1 \Longrightarrow n-1 \in \mathbb{N})$.)

And, in order to prove the successor theorem, we will also need to use the Principle of Mathematical Induction.

So in fact the Principle of Mathematical Induction will be used twice:

- first, to prove the successor theorem, which will be needed to prove that 1 is not even,
- second, to prove that every natural number is good.

In addition, in order to prove that 1 is not even we will need another set of facts about the integers, namely, the facts about positive and negative integers.

We will start by discussing the facts about positive and negative integers.

1.6 New facts we need about $\mathbb{Z}$: ordering and induction

1.6.1 The ordering of the integers

In n is an integer, then one and only one of the following three possibilities occurs:

1. n is positive (that is, $n > 0$),
2. $-n$ is positive (that is, $-n > 0$, or, equivalently, $n < 0$),
3. $n = 0$.

The set of all positive integers is our old friend $\mathbb{N}$, the set $\mathbb{N}$ of all natural numbers.

Let us enumerate the basic facts about this set.

[15]We think of $n+1$ as the "successor" of n. So the successor theorem says that every natural number, except 1, is the succsssor of a natural number.

NEW BASIC FACTS ABOUT THE INTEGERS

BFZ1: $\mathbb{N} \subseteq \mathbb{Z}$. (That is, every natural number is an integer.)

BFZ2: $1 \in \mathbb{N} \wedge 0 \notin \mathbb{N}$. (That is: 1 is a natural number, and 0 is not a natural number.)

BFZ3: The sum and the product of two natural numbers is a natural number. number.) That is

$$(\forall m \in \mathbb{Z})(\forall n \in \mathbb{Z})(m + n \in \mathbb{N} \wedge m.n \in \mathbb{N})\,. \tag{1.72}$$

BFZ4: Every integer is either a natural number, or minus a natural number, or zero. That is:

$$(\forall n \in \mathbb{Z})(n \in \mathbb{N} \vee n = 0 \vee -n \in \mathbb{N}) \tag{1.73}$$

1.6.2 Why we need the Principle of Mathematical Induction

We now discuss the second step of the four-step program, before we do the first one, in order to explain how the Principle of Mathematical Induction comes in.

The goal of the second step is to prove that all natural numbers are good.

It follows from Theorem 26 that the property we called "goodness" is passed on from each integer n to its successor, that is:

Theorem 27. *If an integer n is good (that is, n is even or odd and not both) then $n + 1$ is good as well.*

Proof.

Let n be an arbitrary integer.

Assume n is good.

Then n is even or odd and not both even and odd.

Assume n is even.

Then n is not odd.

Since n is even Theorem 26 tells us that $n + 1$ is odd.

Since n is not odd, Theorem 26 tells us that $n+1$ is not even. (Reason[16]: if $n+1$ was even, then the theorem would imply that n is odd; but n is not odd.)

So $n+1$ is odd and $n+1$ is not even.

Hence $\boxed{n+1 \text{ is good}}$.

Now assume that n is odd.

Then n is not even.

Since n is odd Theorem 26 tells us that $n+1$ is even.

Since n is not even, Theorem 26 tells us that $n+1$ is not odd. (Reason[17]: if $n+1$ was odd, then the theorem would imply that n is even; but n is not even.)

So $n+1$ is even and $n+1$ is not odd.

Hence $\boxed{n+1 \text{ is good}}$.

So we have proved that $n+1$ is good in both cases, when n is even and when n is odd.

But one of these two cases necessarily occurs, because n is even or odd.

So $\boxed{\boxed{n+1 \text{ is good.}}}$ **Q.E.D.**

1.6.3 Why induction is needed

So, if we prove that 1 is good, we will know two things:

(1) 1 is good.

(2) If an integer n is good, then $n+1$ is good.

So, if we look at the natural numbers, then goodness is a property that

(i) is true of the first[18] natural number,

(ii) is passed on from each natural number to its successor[19].

[16] Here is another proof by contradiction !

[17] And here we have another proof by contradiction !

[18] "The first natural number" is 1, of course

[19] The "successor" of n is $n+1$.

From this it should follow that all natural numbers are good. Now can we prove that?

We could argue as follows:

- 1 is good.
- Since 1 is good, 2 must be good, because $2 = 1 + 1$.
- Since 2 is good, 3 must be good, because $3 = 2 + 1$.
- Since 3 is good, 4 must be good, because $4 = 3 + 1$.
- Since 4 is good, 5 must be good, because $5 = 4 + 1$.
  ... .
- ***And so on.***

So it would follow that all the natural numbers are good. And, once we know that, it will be easy to show that all the integers are good. (We will do that later.)

In order to actually prove rigorously that every natural number is good, we need to make precise the vague words "and so on".

1.6.4 "And so on" is dangerous

Arguing as in the previous section, by saying "this is true for $n = 1$, for $n = 2$, for $n - 3$, for $n = 4$, and so on, so it's true for all natural numbers n" is a completely invalid way of arguing that a universal proposition about natural numbers is true. Anyone who argues that way is likely to make a lot of mistakes, because there is absolutely no reason for a proposition about natural numbers n to be true for all n, just because it is true for $n = 1$, $n = 2$, $n = 3$, $n = 4$, $n = 5$, and many more values of n.

An obvious example is the statement "$n < 10,000,001$". This is clearly true for $n = 1$, $n = 2$, $n = 3$, "and so on". You can actually check that it is true for the first ten million values of n. So you may want to conclude that, with ten million examples, that is enough to imply that "$n < 10,000,001$" is true for every $n \in \mathbb{N}$. But it is very clear that for $n = 10,000,001$ the statement is false, so it is not true for all $n \in \mathbb{N}$.

A remarkable example of a similar phenomenon occurs with the expression $n^2 + n + 41$. It can be verified that $n^2 + n + 4$ is a prime number for $n = 1$, $n = 2$, and so on, up to $n = 39$.

For example:

- For $n = 1$, $n^2 + n + 41 = 43$, which is prime.

- For $n = 2$, $n^2 + n + 41 = 47$, which is prime.
- For $n = 3$, $n^2 + n + 41 = 53$, which is prime.
- For $n = 4$, $n^2 + n + 41 = 61$, which is prime.
- For $n = 5$, $n^2 + n + 41 = 71$, which is prime.
- For $n = 6$, $n^2 + n + 41 = 83$, which is prime.
- For $n = 7$, $n^2 + n + 41 = 97$, which is prime.
- For $n = 8$, $n^2 + n + 41 = 97$, which is prime.
- For $n = 9$, $n^2 + n + 41 = 131$, which is prime.
- For $n = 10$, $n^2 + n + 41 = 151$, which is prime.
- For $n = 11$, $n^2 + n + 41 = 173$, which is prime.
- For $n = 12$, $n^2 + n + 41 = 197$, which is prime.
- .....

So you may be tempted to conclude that $n^2 + n + 41$ is prime for every natural number n. But this is wrong. In fact, it is easy to see that for $n = 40$ $n^2 + n + 41$ is not prime.

1.6.5 Why induction is valid

To justify concluding that every natural number n is good we need more than the observation that 1, 2, 3, 4, 5, "and so on", are good. What we need is to know that every natural number n passes on the property of being good to its successor. If we know that then we can be sure that all the natural numbers are good, because if we count 1, 2, 3, 4, 5, ..., then at each step the corresponding number will be good, and the counting process will eventually reach every natural number[20], so all the natural numbers must be good.

The mathematical statement that makes this precise is the ***Principle of Mathematical Induction (PMI)***.

[20] Why? Because that's what the natural numbers are: they are the numbers that can be reached by counting

The Principle of Mathematical Induction is probably one of the two most important proof techniques that you will learn in this course. (The other one is proof by contradiction.) You cannot prove almost anything serious in arithmetic without using Induction.

2 Induction

2.1 Introduction to the Principle of Mathematical Induction

Remember from the previous section that we are calling an integer n "good" if n is even or odd and not both even and odd.

We want to know if it is true that ***every natural number is good***. (Actually, we want to know that every integer good. But once we know that every natural number is good, it takes only a small extra step to prove that every integer good.)

We would like to prove that the answer is "yes, every natural number is good".

How can we do that?

Suppose we prove that 1 is good. Then we will know that

1. 1 ***is good***.
2. ***Goodness is passed on from each natural number*** n ***to its successor*** $n+1$**.** (That is: if $n \in \mathbb{N}$ and n is good, then $n+1$ is good.)

Armed with this information, how can we prove that every natural number is good?

We could use the "and so on" argument, as in the previous section. But it much better not to rely on vague phrases like "and so on", and to have instead a precise, rigorous way of doing the proof.

The key point is that ***all the natural numbers are eventually arrived at by counting***, so that, if we know that something is true for $n = 1$, and when we count (that is, go from 1 to 2, then from 2 to 3, then from 3 to 4, "and so on", each time passing from a natural number n to its successor $n + 1$), then at each step the goodness property will be passed on from n to $n+1$, and eventually every natural number n will be reached by our counting process, so n will be good.

This means that

> Every property that is true of the number 1 and is passed on from each natural number to its successor must be true of all natural numbers.

And ***this is exactly what the Principle of Mathematical Induction (PMI) says***.

Example 11. Suppose you decide to paint natural numbers green according to the following rule: first, you paint the number 1 green. And then every time you paint a number n green, you go to its successor $n+1$ and paint it green. Then the PMI guarantees that every natural number is painted green. □

Example 12. Suppose there is an infinitely long queue of people standing in line: person No. 1, then person No. 2, then person No. 3, then person No. 4, and so on[21]. Suppose you have a flyer with an announcement that you want all the people in the queue to read. (For example, a message saying something like "if you come to my restaurant after the show you will get a great meal with a 20% discount"). Suppose you want everybody to read the flyer, but you have only one copy. Then all you have to do is

(1) Give the flyer to person No. 1,

and

(2) Make sure that each person passes on the flyer to the person next in line after reading it[22].

The PMI says the obvious thing: if you do (1) and (2) then everybody will eventually get your flyer. □

[21]Sure, I am talking about an infinitely long queue, with infinitely many people. And you may object that this is impossible in reality. I have two answers to that. ANSWER NO. 1: This may be impossible in reality, but you can certainly ***imagine*** it! It may be impossible in reality for a person to jump 50 feet high, but you can certainly imagine Wonder Woman doing it, so why not imagine an infinite queue? ANSWER 2: Suppose you only have a finite queue, say 40 people. Then you can consider the following property $P(n)$ of a natural number: "person n got the message or there is no person n". This makes sense of every natural number n. If you guarantee that $P(n)$ is true of every natural number n, this will imply that persons 1, 2, 3, and so on up to person 40, will get the message. Property $P(n)$ will be true of every n but for different reasons: for $n = 1, 2, 3, 4, \cdots$, up to $n = 40$, it will be true because person n gets the message. And for larger n it will be true because there is no person No. n.

[22]For example, you could include in the flyer, in big letters, the statement PLEASE PASS THIS ON TO THE PERSON NEXT IN LINE TO YOU.

2.2 The Principle of Mathematical Induction (PMI)

As explained in the previous section, the ***Principle of Mathematical Induction (PMI)*** captures as a precise mathematical statement the intuitively clear fact that when we count ***we get all the natural numbers***.

Remark 3. There are other numbers (that is, people have invented other numbers), such as zero, the negative numbers -1, -2, etc., fractions such as $\frac{2}{3}$, $\frac{22}{7}$,$-\frac{5}{2}$, 2.75, -5.16, and even "irrational numbers", that cannot be expressed as fractions. But ***we do not get these numbers by the counting process***.

So, if you prove by induction that a statement $P(n)$ is true for all natural numbers, then it does ***not*** follow that it will be true for $n = 0$, because 0 is not a natural number, so if you count $1, 2, 3, 4, \ldots$ you will never get to 0.

And it does not follow either that $P(n)$ will be true for $n = \frac{1}{2}$, because $\frac{1}{2}$ is not a natural number, so if you count $1, 2, 3, 4, \ldots$ you will never get to $\frac{1}{2}$. □

Imagine that you have some statement $P(n)$ about natural numbers that could be true or not for each natural number n. (For example, the statement $P(n)$ could be "$n(n + 1)$ is even", or "n is even or odd", or "n is not both even and odd".) Suppose the following two facts are true:

I. The statement $P(n)$ is true for $n = 1$. (That is, $P(1)$ is true.)

II. Any time the statement $P(n)$ is true for one particular n, it follows that it is true for $n+1$. (That is: if $P(n)$ is true then $P(n+1)$ is true.)

The PMI says that, under these circumstances, $P(n)$ must be true for ***every*** natural number n.

Let us add the PMI to our list of basic facts about the integers:

THE PRINCIPLE OF MATHEMATICAL INDUCTION (BASIC FACT BFZ6 ABOUT THE INTEGERS)

BFZ6: Suppose $P(n)$ is any statement about a variable natural number n. Suppose, furthermore, that

I. $P(1)$ is true.

II. Any time $P(n)$ is true for one particular n, it follows that $P(n+1)$ is true.)

Then $P(n)$ is true for every natural number n.

Let us say the same thing in formal language:

THE PRINCIPLE OF MATHEMATICAL INDUCTION (BASIC FACT BFZ6 ABOUT THE INTEGERS), FORMAL LANGUAGE VERSION

BFZ6: Suppose $P(n)$ is any statement about a variable natural number n. Then

$$\Big(P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\Big) \Longrightarrow (\forall n \in \mathbb{N})P(n)\,. \tag{2.74}$$

2.3 The proof by induction that every natural number is even or odd and not both

We are now ready, finally, to prove the theorem that we had announced before, that every integer is even or odd and not both.

We do it by carrying out the four steps of the four-step program oulined on page 45.

The first step is to prove that 1 is good. And, as explained on page 46, we neef first of all to prove the successor theorem.

2.3.1 Our first proof by induction: the successor theorem

The successor theorem is very simple, and the proof is just a couple of lines. But this is appropriate, since this is going to be our first induction proof. We are going to be doing more complicated proofs very soon.

Theorem 28. *If n is a natural number and $n \neq 1$ then $n-1$ is a natural number. (That is, $(\forall n \in \mathbb{N})(n \neq 1 \Longrightarrow n-1 \in \mathbb{N})$.)*

Proof.

Let $P(n)$ be the predicate "$n \neq 1 \Longrightarrow n-1 \in \mathbb{N}$)".
Basis step. Proof of $P(1)$.
$P(1)$ says "$1 \neq 1 \Longrightarrow 1-1 \in \mathbb{N}$)".
And this implication is true because the premise "$1 \neq 1$" is false,
So $\boxed{P(1)}$.

Inductive step. We prove that $(\forall n \in \mathbb{N})\Big(P(n) \Longrightarrow P(n+1)\Big)$.

Let $n \in \mathbb{N}$ be arbitrary. We want to prove $P(n) \Longrightarrow P(n+1)$.

Assume $P(n)$. We want to prove $P(n+1)$.
$P(n+1)$ says "$n+1 \neq 1 \Longrightarrow n \in \mathbb{N}$)".
And the implication "$n+1 \neq 1 \Longrightarrow n \in \mathbb{N}$)" is true because the conclusion "$n \in \mathbb{N}$ is true, since we are assuming that $n \in \mathbb{N}$.
So $\boxed{P(n+1)}$.

So $P(n) \Longrightarrow P(n+1)$. [Rule $\Longrightarrow_{prove}$]

Hence $\boxed{(\forall n \in \mathbb{N})\Big(P(n) \Longrightarrow P(n+1)\Big)}$ [Rule $\forall_{prove}$]

We have completed the basis step and the inductive step. Hence it follows from the PMI that $(\forall n \in \mathbb{N})P(n)$.

That is, $(\forall n \in \mathbb{N}) * n \neq 1 \Longrightarrow n \in \mathbb{N})$. **Q.E.D.**

THE FORMAT OF A PROOF BY INDUCTION

A proof by induction of a statement $(\forall n \in \mathbb{N})XXXX$ should look like this:

Let $P(n)$ be the predicate XXXX.

Basis step. Proof of $P(1)$.

. . . . . .

$\boxed{P(1)}$.

Inductive step. We prove that $(\forall n \in \mathbb{N})\Big(P(n) \implies P(n+1)\Big)$.

Let $n \in \mathbb{N}$ be arbitrary. We want to prove $P(n) \implies P(n+1)$.

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

. . . . . .

. . . . . .

$P(n+1)$.

So $P(n) \implies P(n+1)$. [Rule $\implies_{prove}$]

Hence $\boxed{(\forall n \in \mathbb{N})\Big(P(n) \implies P(n+1)\Big)}$ [Rule $\forall_{prove}$]

We have completed the basis step and the inductive step. Hence it follows from the PMI that $(\forall n \in \mathbb{N})P(n)$.

That is, $(\forall n \in \mathbb{N})XXXX$. **Q.E.D.**

2.3.2 A remark on the importance of parentheses

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.

2.3.3 Proof that 1 is not even

Theorem 29. 1 *is not even.*

Proof. Suppose 1 was even. Then we may write $1 = 2k$, $k \in \mathbb{Z}$. Then either $k \in \mathbb{N}$ or $-k \in \mathbb{N}$ or $k = 0$, by Basic fact BFZ4.

The possibility that $k = 0$ is excluded because if $k = 0$ then $1 = 2k = 2 \times .0 = 0$, so $1 = 0$. But one of the commutative ring acioms says that $1 \neq 0$, so we got a contradiction

The possibility that $-k \in \mathbb{N}$ is excluded because if $-k \in \mathbb{N}$ then $-2k \in \mathbb{N}$ (because $-2k = -k + (-k)$ and the sum of two natural numbers is a natural number), and then $1 - 2k \in \mathbb{N}$ (because $1 \in \mathbb{N}$, and the sum of two natural numbers is a natural number); but $1 = 2k$, so $1 - 2k = 0$; so $0 \in \mathbb{N}$, but Basic Facts BFZ2 says that $0 \notin \mathbb{N}$; so we got a contradiction

Hence $k \in \mathbb{N}$. And either $k = 1$ or $k \neq 1$. If $k = 1$ then $1 = 2$, because $1 = 2k$. But then $0 = 1 - 1 = 2 - 1 = 1$, so $1 = 0$. But one of the axioms for a commutative rign with identity says that $1 \neq 0$, so we got a contradiction, and this excludes the possibility that $k = 1$.

So $k \in \mathbb{N}$ and $k \neq 1$. Since $k \in \mathbb{N}$ and $k \neq 1$, the successor theorem tells us that $k - 1 \in \mathbb{N}$. But then $0 = 1 - 1 = 2k - 1 = k + (k - 1)$, and $k + (k - 1) \in \mathbb{N}$, because $k \in \mathbb{N}$, $k - 1 \in \mathbb{N}$, and the sum of two natural numbers is a natural number. So $0 \in \mathbb{N}$, but Basic Facts BFZ2 says that $0 \notin \mathbb{N}$, so we got a contradiction. **Q.E.D.**

2.3.4 The proof that every natural number is good

We now carry out step 2 of the four-step program outlined on page 45, by proving:

Theorem 30. *Every natural number is good. That is, every natural number is even or odd and no natural number is both.*

Proof. We are going to prove this result by induction.
Let $P(n)$ be the statement "n is good".

We want to prove that

$$(\forall n \in \mathbb{N}) P(n)\,. \tag{2.75}$$

We will do this by induction.

Basis step.

We want to prove that $P(1)$ is true. That is, we want to prove that 1 is good.

Theorem 29 tells us 1 is not even. And we know that 1 is odd.

So 1 is good. That is, $\boxed{P(1)}$ is true.

Inductive step.

We want to prove that $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,.$

Let n be an arbitrary natural number.

Theorem 27 tells us that if n is good then $n + 1$ is good.

So $P(n) \Longrightarrow P(n+1)$.

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

So $\boxed{(\forall n \in \mathbb{N})\Big(\text{if } P(n) \text{ then } P(n+1)\Big).}$

This completes the inductive step.

By the PMI, our desired conclusion (2.75) follows. **Q.E.D.**

2.3.5 The last step

We have now completed the third step of the four-step program laid out in section 1.5.5, on page 45, by proving that every natural number is good.

We now want to prove that every integer is good.

For thus purpose, we need a simple lemma:

Lemma 1. *Let n be an integer such that n is even or odd and not both. Then $-n$ is even or odd and not both.*

Proof. **YOU DO THIS ONE.**

Problem 22. ***Prove*** Lemma 1. □

And now, finally, we can prove the result for all integers.

Theorem 31. *Every integer is even or odd and no integer is both even and odd.*

Proof. We want to prove the universal sentence "every integer is good".

Let n be an arbitrary integer.

Then by one of the basic facts about $\mathbb{Z}$, either $n \in \mathbb{N}$ or $n = 0$ or $-n \in \mathbb{N}$.

So we have to consider three cases: $n \in \mathbb{N}$, $n = 0$, and $-n \in \mathbb{N}$.

If $n \in \mathbb{N}$, then Lemma 30 tells us that $\boxed{n \text{ is good.}}$

If $n = 0$, then n is even (because $0 = 2 \times 0$, so $2|0$) and n is not odd (because if 0 was odd then Theorem 26 would imply that 1 is even, but we know that 1 is not even).

So n is even and not odd.)

Therefore $\boxed{n \text{ is good.}}$

Finally, we look at the case when $-n \in \mathbb{N}$.

If $-n \in \mathbb{N}$, then by Lemma 30, $-n$ is good, and then, by Lemma 1, $-(-n)$ is good.

But $-(-n) = n$.

So $\boxed{n \text{ is good.}}$

So we have proved that n is good in all three cases, $n \in \mathbb{N}$, $n = 0$, and $-n \in \mathbb{N}$.

Since one of these cases must necessarily occur, we can conclude that

$\boxed{\boxed{n \text{ is good.}}}$

Since we have proved that n is even or odd and not both for an arbitrary integer n, it follows from the rule for proving universal statements that

$\boxed{\boxed{\text{every integer is even or odd and not both.}}}$ **Q.E.D.**

3 Examples of proofs by induction

3.1 Some divisibility theorems

Theorem 32. *If n is natural number, then $8^n - 5^n$ is divisible by 3.*

Proof. We want to prove that

$$(\forall n \in \mathbb{N})3|8^n - 5^n\,. \tag{3.76}$$

Let $P(n)$ be the predicate "$3|8^n - 5^n$

.

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

We are going to prove this by induction.

Basis step:

We want to prove $P(1)$.

$P(1)$ aays "$3|8^1 - 5^1$".

And $8^1 = 8$, $5^1 = 5$, so $8^1 - 5^1 = 3$.

Therefore $3|8^1 - 5^1$, so $\boxed{P(1) \text{ is true}}$

Inductive step:

We want to prove $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.

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

Assume $P(n)$.
Then $3|8^n - 5^n$.
So we can write

$$8^n - 5^n = 3k\,,\ \ k \in \mathbb{Z}\,.. \tag{3.77}$$

Then

$$8 \times (8^n - 5^n) = 3 \times 8k\,. \tag{3.78}$$

So

$$8^{n+1} - 8 \times 5^n = 3 \times 8k\,, \tag{3.79}$$

and then

$$8^{n+1} = 8 \times 5^n + 3 \times 8k\,, \tag{3.80}$$

But $8 = 5 + 3$, so

$$8 \times 5^n = 5 \times 5^n + 3 \times 5^n = 5^{n+1} + 3 \times 5^n\,, \tag{3.81}$$

so

$$8^{n+1} = 5^{n+1} + 3 \times 5^n + 3 \times 8k\,, \tag{3.82}$$

and then

$$8^{n+1} = 5^{n+1} + 3(5^n + 8k)\,, \tag{3.83}$$

so that

$$8^{n+1} - 5^{n+1} = 3(5^n + 8k)\,, \tag{3.84}$$

Let $j = 5^n + 8k$. Then $j \in \mathbb{Z}$ and

$$8^{n+1} - 5^{n+1} = 3j\,. \tag{3.85}$$

Hence $3|8^{n+1} - 5^{n+1}$. That is, $\boxed{P(n+1)}$.

Therefore $\boxed{P(n) \Longrightarrow P(n+1)}$(by Rule $\Longrightarrow_{prove}$).

So $\boxed{(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$ (by Rule $\forall_{prove}$).

This completes the inductive step.

Since we have proved $\boxed{P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$, it follows from the PMI that $(\forall n \in \mathbb{N})P(n)$, that is,. $\boxed{(\forall n \in \mathbb{N})3|8^n - 5^n}$. **Q.E.D.**

Here are a few examples of theorems similar to Theorem 32

Theorem 33. *If n is natural number, then $11^n - 4^n$ is divisible by 7.*

Theorem 34. *If n is natural number, then $22^n - 10^n$ is divisible by 12.*

Theorem 35. *If n is natural number, then $31^n - 18^n$ is divisible by 13.*

Problem 23. ***Prove*** Theorem 33. □

Problem 24. ***Prove*** Theorem 34. □

Problem 25. ***Prove*** Theorem 35. □

Problem 26. *If, after reading the proof of Theorem 32 and solving Problems 23, 24, 25, you get the feeling that these are all the same thing,* ***try to prove*** *the following general theorem:*

Theorem 36. *If a, b are integers, then for every natural number n, $a^n - b^n$ is divisible by $a = b$.*

(This is done later, see Theorem 43 on page 81. But you shoud try to prove it by yourself befoe you look at the proof.) □

3.2 An inequality

Here is another example of a proof by induction.

Theorem 37. *If n is a natural number, then $2^n < n! + 3$.*

Proof. We want to prove that

$$(\forall n \in \mathbb{N}) 2^n < n! + 3\,. \tag{3.86}$$

Let $P(n)$ be the predicate "$2^n < n! + 3$".

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

We are going to prove this by induction.

Basis step:

We want to prove $P(1)$.

$P(1)$ aays "$2^1 < 1! + 3$".

And $2^1 = 2$ and $1! + 3 = 4$.

Therefore $2^1 < 1! + 3$, so $\boxed{P(1) \text{ is true}}$

Inductive step:

We want to prove $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$.

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

Assume $P(n)$. We want to prove $P(n+1)$.
Since $P(n)$ holds, we have

$$2^n < n! + 3\,. \tag{3.87}$$

Therefore, multiplying both sides of (3.87) by 2, we get

$$2^{n+1} < 2n! + 6\,. \tag{3.88}$$

On the other hand, $n + 1 = n - 1 + 2$, so

$$(n+1)! = (n+1)n! = (n-1)n! + 2n!\,. \tag{3.89}$$

We are going to consider separately the cases $n \geq 3$ and $n < 3$.

Assume that $n \geq 3$.

Then $n - 1 \geq 2$ and $n! \geq 6$, so $(n-1)n! \geq 12$ and *a fortiori* $(n-1)n! > 3$.

· Since $(n+1)! = (n-1)n! + 2n!$, and $(n-1)n! > 3$, we have $(n+1)! > 2n! + 3$, that is

$$2n! + 3 < (n+1)!\,. \tag{3.90}$$

Since $2^{n+1} < 2n! + 6$, we have

$$\begin{aligned} 2^{n+1} &< 2n! + 6 \\ &= 2n! + 3 + 3 \\ &< (n+1)! + 3\,, \end{aligned}$$

so $2^{n+1} < (n+1)! + 3$.

That is, $\boxed{P(n+1) \text{ holds.}}$

We now consider the case when $n < 3$.

Assume that $n < 3$.

Then $n = 1$ or $n = 2$,

If $n = 1$ then $P(n+1)$ says $2^2 < 2! + 3$, that is $4 < 5$. So $P(n+1)$ is true.

If $n = 2$ then $P(n+1)$ says $2^3 < 3! + 3$, that is $8 < 9$. So $P(n+1)$ is true.

So in both cases $\boxed{P(n+1) \text{ holds.}}$

We have proved that $P(n+1)$ holds in both case, when $n \geq 3$ and when $n < 3$. So $\boxed{\boxed{P(n+1).}}$

Therefore $\boxed{P(n) \Longrightarrow P(n+1)}$(by Rule $\Longrightarrow_{prove}$).

So $\boxed{(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$ (by Rule $\forall_{prove}$).

This completes the inductive step.

Since we have proved $\boxed{P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))}$, it follows from the PMI that $(\forall n \in \mathbb{N})P(n)$, that is,. $\boxed{(\forall n \in \mathbb{N})2^n < n! + 3}$. **Q.E.D.**

Problem 27.

1. ***Prove*** that if n is a natural number then $3^n < n! + 124$.
2. Is it true that if n is a natural number then $3^n < n! + 123$?

3.3 More inequalities, with applications to the computation of some limits

Let us use induction to prove an inequality:

Theorem 38. *If x is a positive real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx\,. \tag{3.91}$$

Proof. We want to prove that

$$(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{3.92}$$

Let x be an arbitrary real number.

We want to prove that

$$(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{3.93}$$

We prove this by induction.

Let $P(n)$ be the predicate "$x > 0 \implies (1+x)^n \geq 1 + nx$".

Base step. We have to prove $P(1)$.

But $P(1)$ says "$x > 0 \implies 1 + x \geq 1 + x$", and this implication is obviously true, because its conclusion is true.

So $P(1)$ is true, and we are done with the base case.

Inductive step. We have to prove

$$(\forall n \in \mathbb{N})(P(n) \implies P(n+1))\,. \tag{3.94}$$

Let n be an arbitrary natural number. We want to prove that $P(n) \implies P(n+1)$.

Assume $P(n)$.

Then

$$x > 0 \implies (1+x)^n \geq 1 + nx\,. \tag{3.95}$$

We want to prove

$$x > 0 \implies (1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{3.96}$$

Assume $x > 0$.

Then it follows from (3.95) (by Rule $\implies_{use}$) that

$$(1+x)^n \geq 1 + nx\,. \tag{3.97}$$

Multiplying both sides of (3.97) by $1+x$ (which is possible because $1 + x > 0$), we get

$$(1+x)^{n+1} \geq (1+x)(1+nx)\,. \tag{3.98}$$

But

$$\begin{aligned}(1+x)(1+nx) &= 1 + x + nx + nx^2 \\ &= 1 + (n+1)x + nx^2 \\ &\geq 1 + (n+1)x\,.\end{aligned}$$

(The fact that $1 + (n+1)x + nx^2 \geq 1 + (n+1)x$ follows because $nx^2 \geq 0$ and then, adding $1 + (n+1)x$ to both sides, we get $1 + (n+1)x + nx^2 \geq 1 + (n+1)x$.)

So

$$(1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{3.99}$$

Since we proved (3.99) under the assumption that $x > 0$, it follows that

$$x > 0 \Longrightarrow (1+x)^{n+1} \geq 1 + (n+1)x\,. \tag{3.100}$$

That is, $P(n+1)$ holds.

Since we have proved $P(n+1)$ assuming $P(n)$, Rule $\Longrightarrow_{prove}$ allows us to conclude that $P(n) \Longrightarrow P(n+1)$.

So we have proved $P(n) \Longrightarrow P((n+1)$ for arbitrary $n \in \mathbb{N}$, Rule $\forall_{prove}$ allows us to conclude that (3.94) holds.

This compleetes the inductive step.

. Since we have also proved$P(1)$, we can use the PMI to conclude that (3.93) holds, i.e., that

$$(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{3.101}$$

Since we have proved for an arbitrary real number x, we can conclude that

$$(\forall x \in \mathbb{R})(\forall n \in \mathbb{N})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,, \tag{3.102}$$

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

Problem 28. In the proof of Theorem 38, we translated the statement to be proved into formal language as Formula (3.92) and then followed the rules of logic, plus the PMI, to prove it.

Suppose instead that we had translated the statement of Theorem 38 in a different way, as

$$(\forall n \in \mathbb{N})(\forall x \in \mathbb{R})\Big(x > 0 \Longrightarrow (1+x)^n \geq 1 + nx\Big)\,. \tag{3.103}$$

1. ***Prove that this translation is equivalent to Formula (3.92)***, as a matter of pure logic. That is, prove that no matter what the 2-variable predicate $A(x,n)$ is, and what the sets S, T are, the formulas

$$(\forall x \in S)(\forall n \in T)A(x,n)$$

and

$$(\forall n \in T)(\forall x \in S)A(x,n)$$

are equivalent. (Two formulas U, V are equivalent if $U \iff V$ is true.)

2. ***Write a different proof*** of Theorem 38, using the translation (3.103) instead of (3.92).

Problem 29. By looking carefully at the proof of Theorem 38, ***prove*** the following stronger result:

Theorem 39. *If $x \in \mathbb{R}$ and $x \geq -1$, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx\,. \tag{3.104}$$

With a little bit more work, it is possible to prove a result stronger than Theorem 38::

Theorem 40. *If x is a nonnegative real number, and n is a natural number, then*

$$(1+x)^n \geq 1 + nx + \frac{n(n-1)}{2}x^2\,. \tag{3.105}$$

Proof.

YOU DO THIS ONE.

HINT. Just repeat the proof of Theorem 38 up to the point when you multiply by $1+x$, and at that point keep the x^2 term. □

Problem 30. ***Prove*** Theorem 40. □

3.3.1 An application of Theorem 40: computing $\lim_{n\to\infty} \sqrt[n]{n}$

In this section we use the notion of "limit of a sequence". All you need to know about limits of seuences is the following sandwiching theorem": If $\{a_n\}_{n=1}^{\infty}$, $\{b_n\}_{n=1}^{\infty}$, and $\{c_n\}_{n=1}^{\infty}$, are sequences of real numbers such that $a_n \leq b_n \leq c_n$ for every $n \in \mathbb{N}$, and L is a real number such that

$$\lim_{n\to\infty} a_n = L \quad \text{and} \quad \lim_{n\to\infty} c_n = L\,,$$

then $\lim_{n\to\infty} b_n$.

Let us prove that

$$\lim_{n\to\infty} \sqrt[n]{n} = 1\,. \tag{3.106}$$

Define

$$\alpha_n = \sqrt[n]{n} - 1\,.$$

To prove (3.106), we have to prove that

$$\lim_{n\to\infty} \alpha_n = 0\,. \tag{3.107}$$

It is clear that $\alpha_n \geq 0$. (Reason: $\sqrt[n]{n} \geq 1$, because if $\sqrt[n]{n}$ was < 1, it would follow that $\left(\sqrt[n]{n}\right)^n < 1$, but $\left(\sqrt[n]{n}\right)^n = n$, and $n \geq 1$.)

Also, $1 + \alpha_n = \sqrt[n]{n}$, so

$$(1+\alpha_n)^n = n\,. \tag{3.108}$$

Using the inequality of Theorem 40, we get

$$(1+\alpha_n)^n \geq 1 + n\alpha_n + \frac{n(n-1)}{2}\alpha_n^2\,. \tag{3.109}$$

So

$$\begin{aligned} n &= (1+\alpha_n)^n \\ &\geq 1 + n\alpha_n + \frac{n(n-1)}{2}\alpha_n^2 \\ &\geq \frac{n(n-1)}{2}\alpha_n^2\,. \end{aligned}$$

Hence

$$n \geq \frac{n(n-1)}{2}\alpha_n^2\,,$$

so

$$1 \geq \frac{n-1}{2}\alpha_n^2\,,$$

and then

$$\alpha_n^2 \leq \frac{2}{n-1}\,,$$

so

$$\alpha_n \leq \sqrt{\frac{2}{n-1}}\,.$$

Hence the numbers α_n satisfy

$$0 \le \alpha_n \le \sqrt{\frac{2}{n-1}}\,.$$

So the α_n are 'sandwiched" between two sequences that converge to 0. Hence $\lim_{n\to\infty} \alpha_n = 0$ by the sandwiching theorem.

Hence (3.106 is proved.

3.4 Some formulas for sums

In this section we use the notation "$\sum_{k=1}^{n} a_k$" for "$a_1 + a_2 + \cdots + a_n$". (A precise definition of "$\sum_{k=1}^{n} a_k$", without using $\cdots$, is given in section 3.5.3 on page 77.)

Theorem 41. *If n is an arbitrary natural number, then*

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,. \tag{3.110}$$

(That is, $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.)

Proof. Let $P(n)$ be the statement "$\sum_{k=1}^{n} = \frac{n(n+1)}{2}$".

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

Base step. $P(1)$ says "$1 = \frac{1(1+1)}{2}$", which is obviously true. So $P(1)$ is true.

Inductive step.

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

Let n be an arbitrary natural number.

Assume that $P(n)$ is true.

Then $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

Therefore

$$\begin{aligned}\sum_{k=1}^{n+1} k &= (\sum_{k=1}^{n} k) + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= (n+1)\Big[\frac{n}{2} + 1\Big] \\ &= (n+1) \times \frac{n+2}{2} \\ &= \frac{(n+1)(n+2)}{2}\,.\end{aligned}$$

So

$$\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}\,.$$

That is, $P(n+1)$ holds.

We have proved $P(n+1)$ assuming $P(n)$. Hence $\boxed{P(n) \Longrightarrow P(n+1)}$.

We have preved $P(n) \Longrightarrow P(n+1)$ for an arbitrary natural number n. Therefore $(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))$, which completes the inductive step.
Hence, by the PMI, $(\forall n \in \mathbb{N})P(n)$, that is,

$$(\forall n \in \mathbb{N}) \sum_{k=1}^{n} k = \frac{n(n+1)}{2}\,.$$

Q.E.D.

Using the same method, many other formulas for sums can be proved. Here is an exmaple of a rather remarkable one:

Theorem 42. *If n is a natural number, then*

$$\sum_{k=1}^{n} k^3 = \Big[\frac{n(n+1)}{2}\Big]^2\,, \tag{3.111}$$

that is:

$$1^3 + 2^3 + 3^3 + 4^3 + \cdots + n^3 = \Big[\frac{n(n+1)}{2}\Big]^2\,.$$

Proof. **YOU DO THIS ONE.**

Problem 31.

1. ***Compute*** the sum $\sum_{k=1}^{n} k^3$ for $n = 1, 2, 3, 4, 5$ and 6.
2. ***Verify*** that in each case the sum you got is a perfect square (i.e., the square of an integer).
3. ***Prove*** Theorem 42. □

Problem 32.

1. ***Compute*** the sum $\sum_{k=1}^{n} k^2$ for $n = 1, 2, 3, 4, 5$ and 6.
2. ***Verify*** that in each case the sum you got agrees with the formula

$$\sum_{k=1}^{n} k^2 = \frac{n + 3n^2 + 2n^3}{6}\,. \tag{3.112}$$

3. ***Prove*** that Formula (3.112) holds for every natural number n. □

3.5 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

$$2{\times}3{\times}5{\times}7{\times}11{\times}13{\times}17{\times}19{\times}23{\times}29{\times}31{\times}37{\times}41{\times}43{\times}47{\times}53{\times}59{\times}61{\times}67{\times}71 \,,$$

we could write

$$2 \times 3 \times \cdots \times 71 \,. \tag{3.113}$$

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 (3.113), 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

$$3 \times 5 \times 7 \times \cdots \times 71 \,. \tag{3.114}$$

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***.

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

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

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:

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

3.5.2 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 22. The factorial of a natural number n is the number $n!$ given by

$$1! = 1\,, \tag{3.115}$$

$$(n+1)! = n! \times (n+1) \quad \text{for } n \in \mathbb{N}\,. \tag{3.116}$$

In addition, we define

$$0! = 1\,,$$

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

Example 13. Let us compute 7! using the inductive definition. Using (3.116) we get $7! = 7\times 6!$. Then using (3.116) 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, (3.115) 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. □

3.5.3 The inductive definition of summation.

Definition 23. 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 14. Let us compute $\sum_{j=1}^{5} j^2$. We have

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

3.5.4 Inductive definition of product.

Definition 24. 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 15. If you compare the inductive definition of a product with the inductive definition of the factorial, you can easily see that

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

3.5.5 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

$$(\forall n \in \mathbb{N})P(n) \tag{3.117}$$

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

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1))\,. \tag{3.118}$$

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 $1 \leq n$, because n is a natural number. (Precisely: if $n = 1$ then $1 = n$, so $1 \leq n$. And if $n \neq 1$ then ny Basic Fact BFZ9, $n - 1 \in \mathbb{N}$, so $1 < n$, and then $1 \leq n$.)

So $n + 1 \leq n + n$, i.e., $n + 1 \leq 2n$.

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 $P(n) \implies P(n+1)$ for arbitrary n, it follows that (3.118) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (3.117 holds, that is, that $(\forall n \in \mathbb{N}) n < 2^n$. **Q.E.D.**

3.5.6 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

$$(\forall n \in \mathbb{N})(n \geq 4 \implies P(n)) \,. \tag{3.119}$$

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

$$(\forall n \in \mathbb{N})\Big(n \geq 4 \implies (P(n) \implies P(n+1))\Big) \,. \tag{3.120}$$

Let n be an arbitrary natural number such that $n \geq 4$..
We want to prove that $P(n) \implies P(n+1)$.

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 $P(n) \implies P(n + 1)$.

Since we have proved $P(n) \implies P(n + 1)$ for arbitrary n, it follows that (3.120) holds.
So we have completed the basis step and the inductive step, and then the PMI tells us that (3.119) holds, that is, that $(\forall n \in \mathbb{N})\Big(n \geq 4 \implies (2^n < n!)\Big)$.
Q.E.D.

3.5.7 Another simple example

Let us prove

Theorem 43. *If a, b are arbitrary integers, then for every nonnegative integer[23] n the integer $a^n - b^n$ is divisible by $a - b$.*

Example 16. 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.

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

Let a, b be arbitrary integers.

We will prove that

$$(\forall n \in \mathbb{N}) a - b | a^n - b^n \,, \tag{3.121}$$

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

First we prove (3.121) by induction.

Let $P(n)$ be the statement[24] "$a - b$ 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

$$(\forall n \in \mathbb{N})(P(n) \Longrightarrow P(n+1)) \,. \tag{3.122}$$

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

$$a^n - b^n = (a - b)k \,. \tag{3.123}$$

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

[24] 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.

Clearly, $ak + b^n$ is an integer[25].

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

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 (3.122) holds.

So we have completed the basis step and the inductive step, and then the PMI tells us that (3.121 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 divisible 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 33.

1. ***Provide a detailed proof*** of the step that we skipped in the proof of Theorem 43, 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.)

[25]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!***.

2. ***Provide an alternative proof*** of Theorem 43, 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 divisible by 0", given that $\frac{0}{0}$ is not defined?* □

Problem 34. One of the consequences of Theorem 43 is that $10^n - 1$ is divisible by 9 for each nonnegative integer n. So, for example, if you look at the number 438, and let $s = 4 + 3 + 8$, so $s = 15$, it follows that $438 - s$ is divisible by 9, because:

$$\begin{aligned} & 438 - s \\ &= 4 \times 100 + 3 \times 10 + 4 \times 1 - (4 + 3 + 8) \\ &= 4 \times 10^2 - 4 + 3 \times 10 - 3 + 4 \times 1 - 1 \\ &= 4 \times (10^2 - 1) + 3 \times (10 - 1) + 4 \times (1 - 1)\,, \end{aligned}$$

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 divisible by 9. (For example: $572,265$ is divisible by 9 because $5 + 7 + 2 + 2 + 6 + 5 = 27$, which is divisible by 9. And $772,265$ is not divisible by 9 because $7 + 7 + 2 + 2 + 6 + 5 = 29$, which is not divisible 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 divisible by 3. (For example: $572,265$ is divisible by 3 because $5 + 7 + 2 + 2 + 6 + 5 = 27$, which is divisible by 3. And $772,265$ is not divisible by 3 because $7 + 7 + 2 + 2 + 6 + 5 = 29$, which is not divisible 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[26] of its decimal figures is divisible by 11. (For example: $572,473$ is divisible by 11 because $5 - 7 + 2 - 4 + 7 - 3 = 0$, which is divisible by 11. And $772,463$ is not divisible by 11 because $7 - 7 + 2 - 4 + 6 - 3 = 1$, which is not divisible by 11.) □

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

4 Other forms of induction

4.1 Induction with a different starting point (sometimes called "generalized induction")

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 clear that the same thing should be true if we start counting at some other starting point s_*, that is, some other integer such as, for example, 3, or 7, or 0, or -5, or -372. The general result is the following rather trivial theorem:

THE PRINCIPLE OF MATHEMATICAL INDUCTION WITH A GENERAL STARTING POINT

Theorem 44. *Let $P(n)$ be a statement about a variable integer n. Suppose we fix an integer s_*. Let $\mathbb{Z}_{\geq s_*}$ denote the set of all integers n such that $n \geq s_*$. Suppose, furthermore, that*

I. $P(s_*)$ is true.

II. Any time $P(n)$ is true for one particular $n \in \mathbb{Z}_{\geq s_*}$, it follows that $P(n+1)$ is true.

Then $P(n)$ is true for every integer n belonging to $\mathbb{Z}_{s_*}$.

And we can say the same thing in more formal language:

THE PRINCIPLE OF MATHEMATICAL INDUCTION WITH A GENERAL STARTING POINT (FORMAL LANGUAGE VERSION)

Theorem 44. Let $P(n)$ be a statement about a variable integer n. Suppose we fix an integer s_*. Let $\mathbb{Z}_{\geq s_*}$ denote the set of all integers n such that $n \geq s_*$. Suppose, furthermore, that

$$P(s_*) \tag{4.124}$$

and

$$(\forall n \in \mathbb{Z}_{\geq s_*})\big(P(n) \implies P(n+1)\big)\,. \tag{4.125}$$

Then

$$(\forall n \in \mathbb{Z}_{\geq s_*})P(n)\,. \tag{4.126}$$

And we can say the same thing in even more formal language:

THE PRINCIPLE OF MATHEMATICAL INDUCTION WITH A GENERAL STARTING POINT (VERY FORMAL LANGUAGE VERSION)

Theorem 44. Let $P(n)$ be a statement about a variable integer n. Let $s_* \in \mathbb{Z}$, and let

$$\mathbb{Z}_{\geq s_*} = \{n \in \mathbb{Z} : n \geq s_*\}\,. \tag{4.127}$$

Then

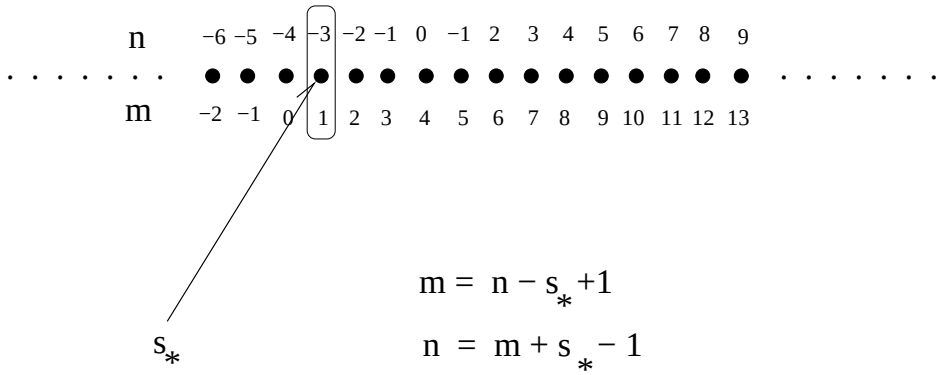
$$\Big(P(s_*) \wedge (\forall n \in \mathbb{Z}_{s_*})\big(P(n) \implies P(n+1)\big)\Big) \implies (\forall n \in \mathbb{Z}_{s_*})P(n)\,. \tag{4.128}$$

Proof of Theorem 44.

Assume that $P(n)$ is a 1-variable predicate and s_* is an arbitrary integer. We want to prove that if (4.124) and (4.125) hold, then (4.126) holds.

So we assume that (4.124) and (4.125) hold, and we try to prove that (4.126) holds.

We do the proof by "changing coordinates". That is, we relabel the integers so that s_* becomes 1, $s_* + 1$ becomes 2, and so on.



Changing coordinates on $\mathbb{Z}$ so that $n = s_*$ becomes $m = 1$

(In the picture, s_* is -3.)

Precisely, we introduce a new variable m related to n by

$$m = n + 1 - s_* \,. \tag{4.129}$$

(That is: $n = s_*$ corresponds to $m = 1$, $n = s_* + 1$ corresponds to $m = 2$, and, in general, $n = s_* + k$ corresponds to $m = k$.)

We can express n in terms of m as follows:

$$n = m + s_* - 1 \,. \tag{4.130}$$

We let $Q(m)$ be $P(n)$ expressed in terms of m. That is, we let $Q(m)$ stand for $P(m + s_* - 1)$. Then $Q(1)$ is $P(s_*)$, $Q(2)$ is $P(s_* + 1)$, $Q(3)$ is $P(s_* + 2)$, and so on.

We want to prove that $P(s_*)$, $P(s_*+1)$, $P(s_*+2)$, ..., are all true. But this amounts to proving that $Q(1)$, $Q(2)$, $Q(3)$, ... are true, i.e. that $(\forall m \in \mathbb{N})Q(m)$.

We prove this by induction. $Q(1)$ is true because $Q(1)$ is the same as $P(s_*)$, which we are assuming is true.

And $Q(m) \Longrightarrow Q(m+1)$ is true for every $m \in \mathbb{N}$, because "$Q(m) \Longrightarrow Q(m+1)$" is equivalent to "$P(m+s_*-1) \Longrightarrow P(m+s_*)$", which is also true because $m+s_*-1$ is to the right of s_*, so $P(m+s_*-1)$ implies that the successor $m+s_*$ also has property P.

So $Q(m)$ satisfies all the conditions of the ordinary PMI, and we can conclude that $Q(m)$ is true for every $m \in \mathbb{N}$. And this says that $P(m+s_*-1)$ is true for all $m \in \mathbb{N}$. Hence $P(n)$ is true for all n such that $n = m+s_*-1$ for some $m \in \mathbb{N}$. But "$n = m+s_*-1$ for some $m \in \mathbb{N}$" is equivalent to "$n \geq s_*$"

Hence $P(n)$ is true for all $n \in \mathbb{Z}_{s_*}$, and our proof is complete. **Q.E.D.**

Remark 4. Theorem 44 is a generalization of the PMI in the following precise sense: according to our definition, the set $\mathbb{Z}_{\geq 1}$ is precisely $\mathbb{N}$. So Theorem 44, if we take s_* to be 1, is exactly the PMI. □

Example 17. Let us prove the following:

Theorem 45. *If n is an integer such that $n \geq 4$, then $2^n < n!$.*

Proof. We want to prove that

$$(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow 2^n < n!)\,. \tag{4.131}$$

Let $P(n)$ be the predicate "$2^n < n!$".

We want to prove that $(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow P(n))$.

We are going to prove this by induction, using the PMI with a general starting point.

And we are going to take the starting point s_* to be 4.

Basis step:

We want to prove $P(4)$.

$P(4)$ aays "$2^4 < 4!$".

And $2^4 = 16$, $4! = 24$, so $2^4 < 4!$.

Therefore $\boxed{P(4) \text{ is true}}$

Inductive step:

We want to prove $(\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(b) \Longrightarrow P(n+1))\Big)$.

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

We want to prove $n \geq 4 \Longrightarrow (P(b) \Longrightarrow P(n+1))$.

Assume $n \geq 4$. We want to prove $P(n) \Longrightarrow P(n+1)$.

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

The inductive hypothesis $P(n)$ tells us that $2^n < n!$.

Then

$$2^{n+1} < 2n! \,. \tag{4.132}$$

But $2 \leq n+1$, so $2n! \leq (n+1)n! = (n+1)!$.

Then $2^{n+1} < (n+1)!$.

So $\boxed{P(n+1) \text{ holds}}$.

Therefore $\boxed{P(n) \Longrightarrow P(n+1)}$ (by Rule $\Longrightarrow_{prove}$).

So $\boxed{n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))}$ (by Rule $\Longrightarrow_{prove}$).

Hence $\boxed{(\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big)}$ (by Rule $\forall_{use}0$.

This completes the inductive step.

Since we have proved $\boxed{P(4) \wedge (\forall n \in \mathbb{Z})\Big(n \geq 4 \Longrightarrow (P(n) \Longrightarrow P(n+1))\Big)}$, it follows from the PMI with general starting point that $(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow P(n))$, that is,. $\boxed{(\forall n \in \mathbb{Z})(n \geq 4 \Longrightarrow 2^n < n!)}$. **Q.E.D.**

4.2 Induction going forward and backward

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. And the "generalized" form says that the same is true if yo start at any integer s_*.

It is clear that if in addition each integer n also passes on the property to its predecessor $n-1$ (that is, if $P(n) \Longrightarrow P(n_1)$ for every $n \in \mathbb{Z}$), then $P(n)$ will be true for every integer n.

INDUCTION GOING FORWARD AND BACKWARD

Theorem 46. *Let $P(n)$ be a statement about a variable integer n and let s_* be an integer. Suppose that*

I. $P(s_*)$ is true.

II. Any time $P(n)$ is true for one particular integer n, it follows that $P(n+1)$ is true.

III. Any time $P(n)$ is true for one particular integer n, it follows that $P(n-1)$ is true.

Then $P(n)$ is true for every integer n.

And we can say the same thing in more formal language:

INDUCTION GOING FORWARD AND BACKWARD (FORMAL LANGUAGE VERSION)

Theorem 46. Let $P(n)$ be a statement about a variable integer n and let s_* be an integer. Suppose that

$$P(s_*) \tag{4.133}$$

and

$$(\forall n \in \mathbb{Z})\Big(P(n) \Longrightarrow \big(P(n+1) \wedge P(n-1)\big)\Big)\,. \tag{4.134}$$

Then

$$(\forall n \in \mathbb{Z})P(n)\,. \tag{4.135}$$

And we can say the same thing in even more formal language:

INDUCTION GOING FORWARD AND BACKWARD (VERY FORMAL LANGUAGE VERSION)

Theorem 46. Let $P(n)$ be a statement about a variable integer n. Let $s_* \in \mathbb{Z}$. Then

$$\Bigg(P(s_*) \wedge (\forall n \in \mathbb{Z})\Big(P(n) \Longrightarrow \big(P(n+1) \wedge P(n-1)\big)\Big)\Bigg) \Longrightarrow (\forall n \in \mathbb{Z})P(n)\,. \tag{4.136}$$

It will be useful to reformulate the forward and backward induction condition in a slightly different way.

Suppose we prove that

$$(\forall n \in \mathbb{Z})\big(P(n) \Longleftrightarrow P(n+1)\big)\,. \tag{4.137}$$

Then given any integer n, if we assume that $P(n)$ is true, we can apply (4.137) to this particular integer, and conclude that $P(n) \iff P(n+1)$. so $P(n) \implies P(n+1)$.

And we can apply (4.137) to the integer $n-1$, and conclude that $P(n-1) \iff P(n)$. so $P(n) \implies P(n-1)$.

In other words, if (4.137) holds, then the condition (4.134) is satisfied. So, if we know that $P(s_*)$ for some starting integer s_*, we can conclude that $P(n)$ holds for every integer n.

This gives us the following slightly different version of the principle on induction going forward and backward:

INDUCTION GOING FORWARD AND BACKWARD
A SLIGHTLY DIFFERENT VERSION

Theorem 47.. *Let $P(n)$ be a statement about a variable integer n and let s_* be an integer. Suppose that*

$$P(s_*) \tag{4.138}$$

and

$$(\forall n \in \mathbb{Z})\big(P(n) \iff P(n+1)\big)\,. \tag{4.139}$$

Then

$$(\forall n \in \mathbb{Z})P(n)\,. \tag{4.140}$$

4.3 Examples of proofs using induction going forward and backward

4.3.1 A very simple example

Here is a simple example of a proof using indcuction going forwad and backward.

First let us review a fact that we already know:

(D3) *if $n \in \mathbb{Z}$, then $n^3 - n$ is divisible by 3.*

(This is easy to prove: we have

$$n^3 - n = n(n^2 - 1) = n(n-1)(n+1) = (n-1)n(n+1)\,,$$

so $n^3 - n$ is the product of three consecutive integers. One of these integers must be divisible by 3, so the product is divisible by 3. Actually, it is also true that $n^3 - n$ must be even, that is, divisible by 2, and then, since 2 and 3 are coprime, it follows that a stronger result is true: $n^3 - n$ *is divisible by* 6.)

In view of (D3), we may conjecture that a similar statement may be true for 4 instead of 3:

(D4) *if* $n \in \mathbb{Z}$*, then* $n^4 - n$ *is divisblie by* 4.

This, however, is not true. (Proof: (D4) is a universal sentence; it says that for all integers n 4 divides $n^3 - n$. To prove that (D4) is not true, it suffices to give a counterexample. Let us just take $n = 2$. Then $2^4 = 16$, so $2^4 - 2 = 14$, which is not divisible by 4.)

How about (D5)? This one turns out to be true, and we can prove it using induction going backward and forward.

Theorem 48. *If* n *is an integer, then* $n^5 - n$ *is divisible by* 5*.*

Proof. We are going to use the binomial formula for the fifth power of a sum:

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5\,, \tag{4.141}$$

which is valid for all integers a, b. (And also for real numbers or, more generally, members of any commutative ring with unity.)

Using this formula we can write, for $n \in \mathbb{Z}$,

$$\begin{aligned} (n+1)^5 &= n^5 + 5n^4 + 10n^3 + 10n^2 + 5n + 1 \\ (n+1)^5 - n^5 - 1 &= 5n^4 + 10n^3 + 10n^2 + 5n \\ &= 5(n^4 + 2n^3 + 2n^2 + n)\,, \end{aligned}$$

so $(n+1)^5 - n^5 - 1$ is divisible by 5.

But

$$(n+1)^5 - (n+1) = ((n+1)^5 - n^5 - 1) + n^5 - n\,.$$

This implies that, for all $n \in \mathbb{Z}$,

$$5|(n+1)^5 - (n+1) \iff 5|n^5 - n\,. \tag{4.142}$$

In other words, the predicate "5 divides $n^5 - n$" is passed on forward (from n to $n+1$) and backward (from $n+1$ to n). This means that we are in a perfect situation to do induction going forward and backward.

Let $P(n)$ be the predicate "5 divides $n^5 - n$". We will prove the statement "$(\forall n \in \mathbb{Z})P(n)$" by induction going forward and backward. We choose the starting point s_0 to be 0.

Basis step. $P(0)$ says "5 divides 0", which is true because every integer divides 0. So $\boxed{P(0) \text{ is true}}$.

Inductive step. We have to prove that $(\forall n \in \mathbb{Z})\big(P(n) \iff P(n+1)\big)$. But Formula (4.142) says precisely that $P(n) \iff P(n+1)$ for all $n \in \mathbb{Z}$,

This completes the inductive step. **Q.E.D.**

Problem 35. ***Prove or disprove*** each of the following statements:

1. If n is an integer, then $n^6 - n$ is divisible by 6.
2. If n is an integer, then $n^7 - n$ is divisible by 7.
3. If n is an integer, then $n^8 - n$ is divisible by 8.
4. If n is an integer, then $n^9 - n$ is divisible by 9.
5. If n is an integer, then $n^{10} - n$ is divisible by 10.
6. If n is an integer, then $n^{11} - n$ is divisible by 11.

You may find the following binomial formulas useful:

$$\begin{aligned}(a+b)^7 &= a^7 + 7a^6b + 21a^5b^2 + 35a^5b^3 + 35a^3b^4 + 21a^2b^5 + 5ab^6 + b^7\\ (a+b)^{[}11] &= a^{11} + 11a^{10}b + 55a^9b^2 + 165a^8b^3 + 330a^7b^4 + 462a67b^5\\ &\quad +462a^5b^6 + 330s^4b^7 + 165a^3b^8 + 55a^2b^9 + 11ab^{10} + b^{11}\,.\end{aligned}$$

Remark 5. If you have done problem 35 you will have discovered the cases $p = 3, 6, 7$ and 11 of ***Fermat's little theorem:*** *If p is a prime numbet and n is an arbitrary integer then $n^p - n$ is divisible by p.* (And the case $p = 2$ is trivial, because if $n \in \mathbb{Z}$ then $n^2 - n$ is always even.) □

4.3.2 Divisibility properties of products of consecutive integers

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

1. It is easy to prove that a product $n(n+1)$ of two consecutive integers must be 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 divisible by $k!$. (Recall the inductive definition of the factorial $n!$ of a natural number: $1! = 1$ and $(n+1)! = n!\times(n+1)$ for $n \in \mathbb{N}$.) In other words, the general result should be that

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})k! \,\Big|\, n(n+1)(n+2)\cdots(n+k-1) \tag{4.143}$$

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

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})k! \,\Big|\, \prod_{j=1}^{k}(n+j-1) \tag{4.144}$$

5. And we will indeed prove (4.144) 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 (4.144) 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 49. *If n is an integer, then $n(n+1)$ is even, i.e., divisible by 2. That is,*

$$(\forall n \in \mathbb{N})2|n(n+1)\,. \tag{4.145}$$

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

Let n be an arbitrary integer.

We know that n is either even or odd.

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 by induction going forward and backward.

Here is the result:

Theorem 50. *If n is an integer, then $n(n+1)(n+2)$ is divisible by 6. That is,*

$$(\forall n \in \mathbb{Z}) 6 | n(n+1)(n+2) \,. \tag{4.146}$$

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

We prove that $(\forall n \in \mathbb{Z}) P(n)$ by induction going forward and backward.

Basis step. If $n = 0$, then $n(n+1)(n+2) = 0$, so $P(0)$ is the statement "$6|0$", which is obviously true. So $\boxed{P(0)}$ is true.

Inductive step. We want to prove that

$$(\forall n \in \mathbb{Z}) \big(P(n) \iff P(n+1) \big) \,. \tag{4.147}$$

Let n be an arbitrary integer.

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

We already know that $n(n+1)$ is even. So we can write

$$n(n+1) = 2k \,, \quad k \in \mathbb{Z} \,.$$

Then

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

If 6 divides $n(n+1)(n+2)$, then $(n+1)(n+2)(n+3)$ is the sum of two integers that are divisible by 6. So 6 divides $(n+1)(n+2)(n+3)$.

If 6 divides $(n+1)(n+2)(n+3)$, then $n(n+1)(n+2)$ is the difference of two integers that are divisible by 6. So 6 divides $n(n+1)(n+2)$.

We have shown that $6|(n+1)(n+2)(n+3) \Longleftrightarrow 6|n(n+1)(n+2)$, i.e., that $P(n) \Longleftrightarrow P(n+1)$.

Since we have shown that $P(n) \Longleftrightarrow P(n+1)$ for an arbitrary integer n, it follows that $(\forall n \in \mathbb{Z})\big(P(n) \Longleftrightarrow P(n+1)\big)$, and this completes the inductive step.

It the follows from Theorem 47 that $P(n)$ is true for all integers n. That is, (4.146) holds. **Q.E.D.**

In the proof of Theorem 50 we used the fact that if $n \in \mathbb{Z}$ then $n(n+1)$ is divisible by 2. Similarly, to prove that $(\forall n \in \mathbb{Z})24|n(n+1)(n+2)(n+3)$, the proof should use the result that $(\forall n \in \mathbb{Z})6|n(n+1)(n+2)$.

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

Theorem 51. *If n is an integer, then $n(n+1)(n+2)(n+3)$ is divisible by 24. That is,*

$$(\forall n \in \mathbb{Z})24|n(n+1)(n+2)(n+3)\,. \tag{4.148}$$

Proof. **YOU DO THIS ONE.** In the proof of Theorem 50 we used the fact that if $n \in \mathbb{Z}$ then $n(n+1)$ is divisible by 2. Similarly, to prove that $(\forall n \in \mathbb{Z})24|n(n+1)(n+2)(n+3)$, the proof should use the result that $(\forall n \in \mathbb{Z})6|n(n+1)(n+2)$.

Problem 36. ***Prove*** Theorem 51. □

Theorem 52. *If n is a natural number, then $n(n+1)(n+2)(n+3)(n+4)$ is divisible by* 120*. That is,*

$$(\forall n \in \mathbb{Z})120|n(n+1)(n+2)(n+3)(n+4)\,. \tag{4.149}$$

Proof. **YOU DO THIS ONE.** In the proof of Theorem 51 we used the fact that if $n \in \mathbb{Z}$ then $n(n+1)(n+2)$ is divisible by 6. Similarly, to prove that $(\forall n \in \mathbb{Z})120|n(n+1)(n+2)(n+3)(n+4)$, the proof should use the result that $(\forall n \in \mathbb{Z})24|n(n+1)(n+2)$.

Problem 37. ***Prove*** Theorem 52.

What we have done so far is clearly the beginning of a proof by induction. We have proved the following:

(*) *for $k = 1, 2, 3, 4, 5$ the product of k consecurive integers is divisible by $k!$.*

This nmakes it natural to make the following

Conjacture. For every natural number k the product of k consecurive integers is divisible by $k!$.

But, of course, knowing that something is true for a few values of k in no way proves that it is true for all k, If we want to be sure that a statement about k is true for all k, we have to prove it.

So let us prove it.

Theorem 53. *If k is a natural number then every product of k consecutive integers is divisible by $k!$.*

Proof. As usual, our first task is to rewrite the statement we want to prove in precise formal language. And for that purpose we need to write a formula for the product of k consecutive integers.

If we start with an integer n, then the k consecutive integers starting at n ate n, $n+1$, $n+2$, ..., up to $n+k-1$. ANd the product of these k integers is $\prod_{j=1}^{k}(n+j-1)$. (For example, for $k = 3$, the product is $n(n+1)(n+2)$. The first factor is n, that is $n+j-1$ with $j-1$, and the last factor is $n+2$, that is, $n+j-1$ with $j = 3$.)

Thet what we want to prove is the following statement:

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})\, k! \Big| \prod_{j=1}^{k} (n+j-1)\,. \tag{4.150}$$

In order to prove this, we will use induction.

We let $P(k)$ be the predicate "for every integer n, the product of k consecutive integers starting with n is divisible by $k!$". That, $P(k)$ is the predicate

$$\forall n \in \mathbb{Z})\, k! \Big| \prod_{j=1}^{k} (n+j-1)\,. \tag{4.151}$$

In the proof, we are going to be working a lot with products such as $\prod_{j=1}^{k}(n+j-1)$. So it is better to give them a simpler name, to make it easier to work with them.

Let us use $a(n,k)$ to denote the product of k consecutive integers starting with n. So, for example,

$$\begin{aligned} a(2,3) &= 2 \times 3 \times 4\,, \\ a(-5,7) &= (-5) \times (-4) \times (-3) \times (-2) \times (-1) \times 0 \times 1\,, \\ a(4,9) &= 4 \times 5 \times 6 \times 7 \times 8 \times 9 \times 10 \times 11 \times 12\,. \end{aligned}$$

Then, of course, the following formula holds for all $k \in \mathbb{N}$, $n \in \mathbb{Z}$:

$$a(n,k) = \prod_{j=1}^{k} (n+j-1) \tag{4.152}$$

or, if you prefer "..." notation,

$$a(n,k) = n \times (n+1) \times (n+2) \cdots \times (n+k-2) \times (n+k-1)\,. \tag{4.153}$$

Using this notation, the predicate $P(k)$ says:

$$\forall n \in \mathbb{Z})\, k! \Big| a(n,k)\,. \tag{4.154}$$

Basis step of the induction. We want to prove that $P(1)$ is true. And $P(1)$ is true, for trivial reasons: $P(1)$ says "$(\forall n \in \mathbb{Z})1! \Big| a(n,1)$", i.e., "$(\forall n \in \mathbb{Z})1 \Big| n$", and this is true because every integer is divisible by 1. So we have proved $\boxed{P(1)}$.

Inductive step. We want to prove that

$$(\forall k \in \mathbb{N})\big(P(k) \implies P(k+1)\big)\,. \tag{4.155}$$

Let $k \in \mathbb{N}$ be arbitrary. We want to prove that

$$P(k) \implies P(k+1)\,. \tag{4.156}$$

Assume $P(k)$. That is, we assume that the product of k consecutive integers is divisible by $k!$.

We want to prove $P(k+1)$. That is, we want to prove

$$(\forall n \in \mathbb{Z})\,(k+1)!\Big|a(n,k+1)\,. \tag{4.157}$$

We are going to prove this by induction going forward and backward. This means that

* We are going to do a second induction proof, with respect to n, within the main proof by induction with respect to to k.
* We are going to call this "the n-induction", to distinguish it from the main induction, the "k-induction".

So at this point

* we are within the k-induction,
* we are about to do the n-induction,
* ee are assuming that $P(k)$ is true,
* and we are trying to prove that $P(k+1)$ is true, that is, we are trying to prove that (4.157) is true,
* and, since (4.157) is a universal sentence about "all integers n", we are goin to do the proof by induction going forward and backward.

We let $Q(n)$ be the predicate

$$(k+1)!\Big|a(n,k+1)\,. \tag{4.158}$$

We choose the starting point s_* of our induction to be 0.

Basis step of the n-induction. We want to prove that $Q(0)$ is true. But $Q(0)$ says "$(k+1)!\Big|a(0,k+1)$". And $a(0,k+1)=0$, because $a(0,k+1)$ is a product of numbers the first one of which is 0. So $Q(0)$ says "$(k+1)!\Big|0$", and this is true, because 0 is divisible by every integer. So we have proved $\boxed{Q(0)"}$.

Inductive step of the n-induction. We want to prove that

$$(\forall n\in\mathbb{Z})\big(Q(n)\iff Q(n+1)\big)\,. \tag{4.159}$$

Let $n\in\mathbb{Z}$ be arbitrary. We want to prove

$$Q(n)\iff Q(n+1)\,. \tag{4.160}$$

$Q(n)$ says that $(k+1)!$ divides $a(n,k+1)$.
And $Q(n+1)$ says that $(k+1)!$ divides $a(n+1,k+1)$.
We are going to prove that

$$a(n+1,k+1)-a(n,k+1)\quad\text{is divisible by }(k+1)!\,. \tag{4.161}$$

Before we do that,let me explain why this is a significant fact.
Suppose we have proved (4.161).
Assume $Q(n)$ holds. Then $a(n,k+1)$ is divisible by $(k+1)!$. Since $a(n+1,k+1)-a(n,k+1)$ is also divisible by $(k+1)!$, we can conclude that the sum $a(n,k+1)+(a(n+1,k+1)-a(n,k+1))$ is divisible by $(k+1)!$. But this sum is $a(n+1,k+1)$, So $a(n+1,k+1))$ is divisible by $(k+1)!$. That says that $Q(n+1)$ holds.
Conversely, assume $Q(n+1)$ holds. Then $a(n+1,k+1)$ is divisible by $(k+1)!$. Since $a(n+1,k+1)-a(n,k+1)$ is also divisible by $(k+1)!$, we can conclude that the difference $a(n+1,k+1)-\big(a(n+1,k+1)-a(n,k+1)\big)$ is divisible by $(k+1)!$. But this difference is $a(n,k+1)$, So $a(n,k+1))$ is divisible by $(k+1)!$. That says that $Q(n)$ holds.
Summarizing, we have shown that, if (4.161) is true, then $Q(n)\implies Q(n+1)$ and $Q(n+1)\implies Q(n)$, so $Q(n)\iff Q(n+1)$, which is exactly what we are trying to prove to complete the n-induction.

In other words: *all we need to do is prove (4.161) and that will complete our proof.*

We now prove (4.161).

The number $a(n, k+1)$ is the product of $k+1$ consecutive integers starting with n and ending with $n+k$. And this is clearly the product of n times k consecutive integers starting with $n+1$. That is,

$$a(n, k+1) = n \times a(n+1, k)\,. \tag{4.162}$$

Similarly, the number $a(n, k+1)$ is the product of $k+1$ consecutive integers starting with $n+1$ and ending with $n+k+1$. And this is clearly the product of k consecutive integers starting with $n+1$, mutliplied by $n+k+1$. That is,

$$a(n+1, k+1) = a(n+1, k) \times (n+1+k)\,. \tag{4.163}$$

Therefore

$$\begin{aligned} a(n+1, k+1) - a(n, k+1) &= a(n+1, k) \times (n+1+k) - n \times a(n+1, k) \\ &= (n+k+1) \times a(n+1, k) - n \times a(n+1, k) \\ &= \big((n+k+1) - n\big) \times a(n+1, k) \\ &= (k+1) \times a(n+1, k)\,. \end{aligned}$$

So we get the formula

$$a(n+1, k+1) - a(n, k+1) = (k+1) \times a(n+1, k)\,. \tag{4.164}$$

(see the example in the box below to understand this formula).

THE FORMULA
$a(n+1,k+1) - a(n,k+1) = (k+1) \times a(n+1,k)$:
AN EXAMPLE

.

Take $n = 11$, $k = 5$. Then

$$\begin{aligned}
a(11,6) &= 11 \times 12 \times 13 \times 12 \times 15 \times 16\,, \\
a(12,6) &= 12 \times 13 \times 12 \times 15 \times 16 \times 17\,, \\
a(11,6) &= 11 \times \Big(12 \times 13 \times 12 \times 15 \times 16\Big) \\
&= 11 \times a(12,5) \\
a(12,6) &= \Big(12 \times 13 \times 12 \times 15 \times 16\Big) \times 17 \\
&= 17 \times \Big(12 \times 13 \times 12 \times 15 \times 16\Big) \\
&= 17 \times a(12,5)\,,
\end{aligned}$$

so

$$\begin{aligned}
a(12,6) - a(11,6) &= (17-11) \times a(12,5) \\
&= 6 \times a(12,5)\,.
\end{aligned}$$

That is, $\boxed{a(n+1,k+1) - a(n,k+1) = (k+1) \times a(n+1,k)}$.

Now comes ***the key point:*** remember that we are within the k-induction. We are assuming $P(k)$ and trying to prove $P(k+1)$. So at this point we cah use $P(k)$. Add $P(k)$ says that

$$\forall n \in \mathbb{Z})\, k! \Big| a(n,k)\,. \tag{4.165}$$

So we can use (4.165).
Then $k!$ divides $a(n+1,k)$, so we can write $a(n,k) = m \times k!$ for some $m \in \mathbb{Z}$.
Then

$$\begin{aligned}
a(n+1,k+1) - a(n,k+1) &= (k+1) \times k! \times m \\
&= (k+1)! \times m\,,
\end{aligned}$$

so $(k+1)!$ divides $a(n+1,k+1) - a(n,k+1)$.

That is, we have proved (4.161) and, as explained before, it follows that $\boxed{Q(n) \iff Q(n+1)}$.

Since we have proved that $Q(n) \iff Q(n+1)$ for arbitrary $n \in \mathbb{Z}$, this shows that $\boxed{(\forall n \in \mathbb{Z})\big(Q(n) \iff Q(n+1)\big)}$.

This completes the inductive step of the n-induction.

We have proved that $Q(0)$ and $(\forall n \in \mathbb{Z})\big(Q(n) \iff Q(n+1)\big)$. By the PMI Going Forward and Backward, is follows that

$$(\forall n \in \mathbb{Z})Q(n)\,. \tag{4.166}$$

–] Since $Q(n)$ is the predicate "$(k+1)!\Big|a(n,k+1)$", we have proved

$$(\forall n \in \mathbb{Z})(k+1)!\Big|a(n,k+1)\,, \tag{4.167}$$

that is, we have proved $P(k+1)$.

Since we have proved $P(k+1)$ assuming $P(k)$, it follows that

$$P(k) \Longrightarrow P(k+1)\,. \tag{4.168}$$

Since we have proved (4.168) for an arbitrary natural numebr k, it follows that

$$(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)\,. \tag{4.169}$$

So we have proved $P(1)$ and $(\forall k \in \mathbb{N})\big(P(k) \Longrightarrow P(k+1)\big)$. It follows from the PMI that

$$(\forall k \in \mathbb{N})P(k)\,. \tag{4.170}$$

But $P(k)$ is the predicate "$(\forall n \in \mathbb{Z})\, k!\Big|a(n,k)$".

So we have proved

$$(\forall k \in \mathbb{N})(\forall n \in \mathbb{Z})\, k!\Big|a(n,k)\,, \tag{4.171}$$

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