INTEGERS

Preliminaries

We recall the following definitions for the set of natural numbers $\mathbb{N}$ and the set of integers $\mathbb{Z}$:

$$\mathbb{N} = \{0, 1, 2, 3, \ldots\}$$
$$\mathbb{Z} = \{k, -k \mid k \in \mathbb{N}\} = \{0, 1, -1, 2, -2, 3, -3, \ldots\}$$

We also define

$$\mathbb{N}^* = \mathbb{N} - \{0\} = \{1, 2, 3, \ldots\}$$
$$\mathbb{Z}^* = \mathbb{Z} - \{0\} = \{1, -1, 2, -2, 3, -3, \ldots\}$$
$$[n] = \{k \in \mathbb{N} \mid 1 \leq k \leq n\} = \{1, 2, 3, \ldots, n\}$$

Odd and even integers

We partition the set of integers $\mathbb{Z}$ into even and odd integers as follows:

Def: Let $n \in \mathbb{Z}$ be an integer. We say that

n even $\Leftrightarrow \exists k \in \mathbb{Z} : n = 2k$

n odd $\Leftrightarrow \exists k \in \mathbb{Z} : n = 2k+1$

We note that the statements

n odd $\Leftrightarrow$ n even

n even $\Leftrightarrow$ n odd

require the well-ordering principle for their proof, which will be given in the following section. In the following, we will assume that these statements have already been shown, and use them in our arguments, when needed.

- The following proposition is useful in arguments with integers

Prop: $\forall a,b \in \mathbb{Z}: (ab \text{ even} \Leftrightarrow a \text{ even} \vee b \text{ even})$

We also have the contrapositive statement, obtained by negating both sides:

Corollary: $\forall a,b \in \mathbb{Z}: (ab \text{ odd} \Leftrightarrow a \text{ odd} \wedge b \text{ odd})$

From both statements, the choice $a=b$ gives.

Corollary: $\forall a \in \mathbb{Z}: a^2 \text{ even} \Leftrightarrow a \text{ even}$
$\forall a \in \mathbb{Z}: a^2 \text{ odd} \Leftrightarrow a \text{ odd}$

We now prove the main proposition:

Proof

Let $a,b \in \mathbb{Z}$ be given.

($\Rightarrow$): We show the contrapositive statement

$a \text{ odd} \wedge b \text{ odd} \Rightarrow ab \text{ odd}$

Assume that a odd $\wedge$ b odd. Then, we have:

a odd $\Rightarrow \exists k \in \mathbb{Z} : a = 2k+1$

b odd $\Rightarrow \exists k \in \mathbb{Z} : b = 2k+1$

Choose $k, \lambda \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2\lambda+1$.

Then, we have:

$ab = (2k+1)(2\lambda+1) = 4k\lambda + 2k + 2\lambda + 1 =$

$= 2(2k\lambda + k + \lambda) + 1 \Rightarrow$

$\Rightarrow \exists \mu \in \mathbb{Z} : ab = 2\mu + 1$ (for $\mu = 2k\lambda + k + \lambda \in \mathbb{Z}$)

$\Rightarrow$ ab odd

($\Leftarrow$): Assume that a even $\vee$ b even. We distinguish between the following cases

Case 1: Assume that a even. Then,

a even $\Rightarrow \exists k \in \mathbb{Z} : a = 2k$

Choose $k \in \mathbb{Z}$ such that $a = 2k$. Then, we have

$ab = (2k)b = 2(kb) \Rightarrow$

$\Rightarrow \exists \mu \in \mathbb{Z} : ab = 2\mu$ (for $\mu = kb \in \mathbb{Z}$)

$\Rightarrow$ ab even.

Case 2: Assume that b even. Then,

b even $\Rightarrow \exists k \in \mathbb{Z} : b = 2k$

Choose $k \in \mathbb{Z}$ such that $b = 2k$. Then, we have

$ab = a(2k) = 2(ak) \Rightarrow$

$\Rightarrow \exists \mu \in \mathbb{Z} : ab = 2\mu$ (for $\mu = ak \in \mathbb{Z}$)

$\Rightarrow$ ab even

From the above, we conclude that

$\forall a, b \in \mathbb{Z}$: ab even $\Leftrightarrow$ a even $\vee$ b even. $\square$

EXAMPLES

a) Show that

$\forall a, b \in \mathbb{Z}: (a \text{ odd} \wedge b \text{ odd} \Rightarrow a+b \text{ even})$

Solution

Let $a, b \in \mathbb{Z}$ be given and assume that a odd $\wedge$ b odd.

Then, we have:

$$\begin{cases} a \text{ odd} \\ b \text{ odd} \end{cases} \Rightarrow \begin{cases} \exists k \in \mathbb{Z}: a = 2k+1 \\ \exists \lambda \in \mathbb{Z}: b = 2\lambda + 1 \end{cases}$$

Choose $k, \lambda \in \mathbb{Z}$ such that $a = 2k+1$ and $b = 2\lambda + 1$.

It follows that:

$$a+b = (2k+1) + (2\lambda+1) = 2k + 2\lambda + 2 =$$
$$= 2(k+\lambda+1) \Rightarrow$$
$$\Rightarrow \exists \mu \in \mathbb{Z}: a+b = 2\mu \quad (\text{for } \mu = k+\lambda+1 \in \mathbb{Z})$$
$$\Rightarrow a+b \text{ even}.$$

From the above, we conclude that

$\forall a, b \in \mathbb{Z}: (a \text{ odd} \wedge b \text{ odd} \Rightarrow a+b \text{ even})$ □

b) Show that: $\forall a \in \mathbb{Z}: (a \text{ odd} \Rightarrow 3a+7 \text{ even})$.

Solution

Let $a \in \mathbb{Z}$ be given and assume that a odd.

Then, we have:

a odd $\Rightarrow \exists k \in \mathbb{Z}: a = 2k+1$

Choose $k \in \mathbb{Z}$ such that $a = 2k+1$. It follows that:

$3a+7 = 3(2k+1)+7 = 6k+3+7 = 6k+10 = 2(3k+5) \Rightarrow$
$\Rightarrow \exists \mu \in \mathbb{Z} : 3a+7 = 2\mu$
$\Rightarrow$ $3a+7$ even
We have thus shown that
$\forall a \in \mathbb{Z} : (a \text{ odd} \Rightarrow 3a+7 \text{ even})$. □

c) Show that:
$\forall x \in \mathbb{Z} : x^3+x^2+x$ even $\Leftrightarrow$ x even
Solution
Let $x \in \mathbb{Z}$ be given.
($\Rightarrow$): We show the contrapositive statement
x odd $\Rightarrow x^3+x^2+x$ odd
Assume that x odd. Then, we have:
x odd $\Rightarrow \exists k \in \mathbb{Z} : x = 2k+1$
Choose $k \in \mathbb{Z}$ such that $x = 2k+1$. It follows that
$x^3+x^2+x = (2k+1)^3 + (2k+1)^2 + (2k+1) =$
$= 8k^3 + 3(2k)^2 + 3(2k) + 1 + (2k)^2 + 2(2k) + 1 + 2k + 1$
$= 8k^3 + 12k^2 + 6k + 1 + 4k^2 + 4k + 1 + 2k + 1$
$= 8k^3 + (12+4)k^2 + (6+4+2)k + (1+1+1)$
$= 8k^3 + 16k^2 + 12k + 3$
$= 2(4k^3 + 8k^2 + 6k + 1) + 1 \Rightarrow$
$\Rightarrow \exists \lambda \in \mathbb{Z} : x^3+x^2+x = 2\lambda+1$ (for $\lambda = 4k^3+8k^2+6k+1 \in \mathbb{Z}$)
$\Rightarrow$ x^3+x^2+x odd
($\Leftarrow$): Assume that x even. Then, we have:
x even $\Rightarrow \exists k \in \mathbb{Z} : x = 2k$

Choose $k \in \mathbb{Z}$ such that $x = 2k$. It follows that

$x^3 + x^2 + x = (2k)^3 + (2k)^2 + 2k = 8k^3 + 4k^2 + 2k$

$= 2(4k^3 + 2k^2 + k) \Rightarrow$

$\Rightarrow \exists \lambda \in \mathbb{Z} : x^3 + x^2 + x = 2\lambda$

$\Rightarrow$ $x^3 + x^2 + x$ even.

We have thus shown that

$\forall x \in \mathbb{Z} : (x^3 + x^2 + x$ even $\Leftrightarrow x$ even$)$. □

d) Show that: $\forall n \in \mathbb{Z} : n^2 + 3n + 5$ odd

Solution

Let $n \in \mathbb{Z}$ be given. We distinguish between the following cases.

Case 1: Assume that n even. Then, we have

n even $\Rightarrow \exists k \in \mathbb{Z} : n = 2k$

Choose $k \in \mathbb{Z}$ such that $n = 2k$. It follows that

$n^2 + 3n + 5 = (2k)^2 + 3(2k) + 5 = 4k^2 + 6k + 5$

$= 4k^2 + 6k + 4 + 1 = 2(2k^2 + 3k + 2) + 1 \Rightarrow$

$\Rightarrow \exists \lambda \in \mathbb{Z} : n^2 + 3n + 5 = 2\lambda + 1$ (for $\lambda = 2k^2 + 3k + 2 \in \mathbb{Z}$)

$\Rightarrow$ $n^2 + 3n + 5$ odd.

Case 2: Assume that n odd. Then, we have:

n odd $\Rightarrow \exists k \in \mathbb{Z} : n = 2k + 1$

Choose $k \in \mathbb{Z}$ such that $n = 2k + 1$. It follows that

$n^2 + 3n + 5 = (2k+1)^2 + 3(2k+1) + 5$

$= 4k^2 + 4k + 1 + 6k + 3 + 5$

$= 4k^2 + (4+6)k + (1+3+5)$

$= 4k^2 + 10k + 9$

$= 4k^2 + 10k + 8 + 1$

$= 2(2k^2 + 5k + 4) + 1 \Rightarrow$

$\Rightarrow \exists \lambda \in \mathbb{Z} : n^2 + 3n + 5 = 2\lambda + 1$ (for $\lambda = 2k^2 + 5k + 4 \in \mathbb{Z}$)

$\Rightarrow$ $n^2 + 3n + 5$ odd

We have thus shown in both cases that

$\forall n \in \mathbb{Z} : n^2 + 3n + 5$ odd $\square$

EXERCISES

(1) Let $a, b, x \in \mathbb{Z}$ be given. Prove that

a) x odd $\wedge$ $a+b$ odd $\Rightarrow$ $ax+b$ odd

b) x odd $\wedge$ $a+b$ even $\Rightarrow$ $ax+b$ even

c) x even $\wedge$ b odd $\Rightarrow$ $ax+b$ odd

d) x even $\wedge$ b even $\Rightarrow$ $ax+b$ even

(2) Let $a, b, c, x \in \mathbb{Z}$ be given. Prove that

a) x odd $\wedge$ $a+b+c$ odd $\Rightarrow$ ax^2+bx+c odd

b) x odd $\wedge$ $a+b+c$ even $\Rightarrow$ ax^2+bx+c even.

c) x even $\wedge$ c odd $\Rightarrow$ ax^2+bx+c odd

d) x even $\wedge$ c even $\Rightarrow$ ax^2+bx+c even.

(3) Let $a, b, n \in \mathbb{Z}$ be given. Prove that

$an^3 - bn$ odd $\Rightarrow$ $a-b$ odd.

(4) Let $x, y \in \mathbb{Z}$ be given. Prove that

a) xy odd $\Rightarrow$ x odd $\wedge$ y odd

b) $(x+1)y^2$ even $\Leftrightarrow$ x odd $\vee$ y even

c) xy even $\wedge$ $x+y$ even $\Rightarrow$ x even $\wedge$ y even

d) $3x+1$ even $\rightarrow$ $5x+2$ odd

e) x odd $\wedge$ $3x+5y$ even $\Rightarrow$ y odd

The well-ordering principle

- We will now show that
  $\forall n \in \mathbb{Z}$: n odd $\Rightarrow$ n not even
  $\forall n \in \mathbb{Z}$: n not even $\Rightarrow$ n odd
  The first statement can be shown with a contradiction argument, however the proof of the second statement requires using the well-ordering principle. Combining the two statements gives
  $\forall n \in \mathbb{Z}$: n odd $\Leftrightarrow$ n not even
  $\forall n \in \mathbb{Z}$: n even $\Leftrightarrow$ n not odd
- The well-ordering principle is an axiom of $\mathbb{N}$ that cannot be shown via the obvious laws of algebra.

> **Axiom:** Let S such that $\emptyset \neq S \subseteq \mathbb{N}$ and define the set:
> $M = \{m \in S \mid \forall x \in S - \{m\} : m < x\}$
> Then $M \neq \emptyset$.

interpretation: If $\emptyset \neq S \subseteq \mathbb{N}$, then S has at least one element that is strictly less than all other elements of S.

We will now prove that M can have only one element. We use the notation $|M|$ to denote the

number of elements in M and will show that

Prop: Let $\$$ such that $\emptyset \neq \$ \subseteq \mathbb{N}$ and define the set
$M = \{m \in \$ \mid \forall x \in \$ - \{m\} : m < x\}$
Then: $|M| = 1$.

Proof

From the well-ordering principle, we have
$\emptyset \neq \$ \subseteq \mathbb{N} \Rightarrow M \neq \emptyset \Rightarrow |M| > 0 \Rightarrow |M| \geq 1$
To show that $|M| \leq 1$, we assume that $|M| > 1$ and derive a contradiction. Since $|M| > 1 \Rightarrow |M| \geq 2$, we choose $a, b \in M$ such that $a \neq b$. Then, we have:
$a \in M \Rightarrow a \in \$ \wedge \forall x \in \$ - \{a\} : a < x$
$\Rightarrow \forall x \in \$ - \{a\} : a < x$
$\Rightarrow a < b$ (for $x > b \in M \Rightarrow x \in \$$)
and
$b \in M \Rightarrow b \in \$ \wedge \forall x \in \$ - \{b\} : b < x$
$\Rightarrow \forall x \in \$ - \{b\} : b < x$
$\Rightarrow b < a$ (for $x = a \in M \Rightarrow x \in \$$)
It follows that $a < b \wedge b < a$ which is a contradiction and conclude that $|M| \leq 1$. Then, we have:
$\begin{cases} |M| \geq 1 \\ |M| \leq 1 \end{cases} \Rightarrow |M| = 1$ □

▸ **notation:** Since the set M has a unique element $a \in M$, we denote that element as $a = \min(\$)$.

We shall now prove our main results:

Prop: $\forall n \in \mathbb{Z} : (n \text{ odd} \Rightarrow n \text{ not even})$

Proof

Let $n \in \mathbb{Z}$ be given and assume that n odd.
To show that n not even, we assume that n is even in order to derive a contradiction. It follows that

$$\begin{cases} n \text{ odd} \\ n \text{ even} \end{cases} \Rightarrow \begin{cases} \exists k \in \mathbb{Z} : n = 2k+1 \\ \exists \lambda \in \mathbb{Z} : n = 2\lambda \end{cases}$$

Choose $k, \lambda \in \mathbb{Z}$ such that $n = 2k+1$ and $n = 2\lambda$.
Then, we have:

$$\begin{cases} n = 2k+1 \\ n = 2\lambda \end{cases} \Rightarrow 2\lambda = 2k+1 \Rightarrow \lambda = \frac{2k+1}{2} = k + 1/2$$

and therefore

$$k \in \mathbb{Z} \Rightarrow k + 1/2 \notin \mathbb{Z} \Rightarrow \lambda \notin \mathbb{Z}$$

which is a contradiction since λ was chosen with $\lambda \in \mathbb{Z}$. We conclude that n not even.
We have thus shown that
$\forall n \in \mathbb{Z} : (n \text{ odd} \Rightarrow n \text{ not even})$. □

Prop: $\forall n \in \mathbb{Z} : (n \text{ not even} \Rightarrow n \text{ odd})$

Proof

Let $n \in \mathbb{Z}$ be given and assume that n not even.

▸ We define the set

$A = \{n - 2x \mid x \in \mathbb{Z} \wedge n - 2x \geq 0\}$

and note that the belonging condition of A is

$y \in A \Leftrightarrow \exists x \in \mathbb{Z} : (n - 2x \geq 0 \wedge y = n - 2x)$

▸ We will apply the well-ordering principle on A and extract $a = \min(A)$, so we must show that $\emptyset \neq A \subseteq \mathbb{N}$.

• Proof of $A \neq \emptyset$

We distinguish between the following cases.

Case 1: Assume that $n \geq 0$. Choose $x = -1$. Then, we have:

$n - 2x = n - 2(-1) = n + 2 \geq 2 > 0 \Rightarrow n - 2x \geq 0.$

Choose $y = n - 2x$. It follows that

$\exists x \in \mathbb{Z} : (n - 2x \geq 0 \wedge y = n - 2x)$

$\Rightarrow y \in A \Rightarrow A \neq \emptyset.$

Case 2: Assume that $n < 0$. Choose $x = n - 1$. Then, we have

$n - 2x = n - 2(n - 1) = n - 2n + 2 = -n + 2 > 2 > 0$

Choose $y = n - 2x$. It follows that

$\exists x \in \mathbb{Z} : (n - 2x \geq 0 \wedge y = n - 2x)$

$\Rightarrow y \in A \Rightarrow A \neq \emptyset.$

In both cases we have shown that $A \neq \emptyset$.

• Proof of $A \subseteq \mathbb{N}$.

Let $y \in A$ be given. Then, we have

$y \in A \Rightarrow \exists x \in \mathbb{Z} : (n - 2x \geq 0 \wedge y = n - 2x)$

Choose $x \in \mathbb{Z}$ such that $n-2x \geq 0$ and $y = n-2x$.
It follows that

$$\begin{cases} y = n-2x \geq 0 \\ x \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} y \geq 0 \Rightarrow y \in \mathbb{N} \\ y \in \mathbb{Z} \end{cases}$$

We have thus shown that
$(\forall y \in A : y \in \mathbb{N}) \Rightarrow A \subseteq \mathbb{N}$.

• Main argument: Since $\emptyset \neq A \subseteq \mathbb{N}$, the well-ordering principle applies and we may thus define $a = \min(A)$.
It follows that

$$\begin{aligned} a = \min(A) &\Rightarrow a \in A \\ &\Rightarrow \exists k \in \mathbb{Z} : (n-2k \geq 0 \wedge n-2k = a) \\ &\Rightarrow \exists k \in \mathbb{Z} : n = 2k+a \qquad (1) \end{aligned}$$

▸ We will show that $a > 0$. We note that
$a \in A \Rightarrow a \in \mathbb{N} \Rightarrow a \geq 0$
To show that $a \neq 0$, we assume that $a = 0$ in order to derive a contradiction. From Eq. (1), it follows that
$(\exists k \in \mathbb{Z} : n = 2k) \Rightarrow n$ even
which is a contradiction because by hypothesis n not even. We conclude that $a \neq 0$ and thus
$a \geq 0 \wedge a \neq 0 \Rightarrow a > 0$

▸ We will show that $a < 2$. To show that $a < 2$, we assume that $a \geq 2$ in order to derive a contradiction. Define $b = a-2$. We will show that $b \in A$. From Eq. (1) choose $k \in \mathbb{Z}$ such that $n = 2k+a$. Then, we have:

$b = a - 2 = 2k + a - 2k - 2 = n - 2k - 2 = n - 2(k+1)$

and

$a \geq 2 \Rightarrow b = a - 2 \geq 0 \Rightarrow n - 2(k+1) \geq 0$

We have thus shown that

$\exists x \in \mathbb{Z} : (n - 2x \geq 0 \wedge b = n - 2x)$ (for $x = k+1 \in \mathbb{Z}$)

$\Rightarrow b \in A \Rightarrow b \geq \min(A) = a \Rightarrow b \geq a$

This contradicts $b = a - 2 < a$. We conclude that $a < 2$.

From the above, it follows that

$a = 1 \Rightarrow \exists k \in \mathbb{Z} : n = 2k + 1$

$\Rightarrow$ n odd.

We have thus shown that

$\forall n \in \mathbb{Z} : (n \text{ not even} \Rightarrow n \text{ odd})$. □

Division theorem

A generalization of the above argument gives the following theorem

$$\forall a \in \mathbb{Z}^* : \forall b \in \mathbb{Z} : \exists! q, r \in \mathbb{Z} : (b = aq + r \wedge 0 \leq r < |a|)$$

We say that q is the quotient of the division of b by a and r is the remainder. Both q, r are unique under the constraint $0 \leq r < |a|$.

Divisability.

We begin with the following definition

Def: Let $a \in \mathbb{Z}^*$ and $b \in \mathbb{Z}$. We say that
$$a|b \Leftrightarrow \exists k \in \mathbb{Z} : b = ak$$

The notation $a|b$ reads "a divides b" and means that the remainder of the division of b by a is zero.

Properties

① $\forall a,b \in \mathbb{Z}^* : \forall c \in \mathbb{Z} : ((a|b \wedge b|c) \Rightarrow a|c)$

Proof

Let $a,b \in \mathbb{Z}^*$ and $c \in \mathbb{Z}$ be given and assume that $a|b$ and $b|c$. Then, we have

$$\begin{cases} a|b \\ b|c \end{cases} \Rightarrow \begin{cases} \exists x \in \mathbb{Z} : b = ax \\ \exists y \in \mathbb{Z} : c = by \end{cases}$$

Choose $x, y \in \mathbb{Z}$ such that $b = ax$ and $c = by$.
It follows that

$$c = by = (ax)y = a(xy) \Rightarrow$$
$$\Rightarrow \exists\, \lambda \in \mathbb{Z} : c = a\lambda \quad (\text{for } \lambda = xy \in \mathbb{Z})$$
$$\Rightarrow a|c.$$

We have thus shown that
$\forall a,b \in \mathbb{Z}^* : \forall c \in \mathbb{Z} : ((a|b \wedge b|c) \Rightarrow a|c)$ □

② $\boxed{\forall a \in \mathbb{Z}^* : \forall b,c,x,y \in \mathbb{Z} : ((a|b \wedge a|c) \Rightarrow a|(bx+cy))}$

Proof

Let $\underline{a \in \mathbb{Z}^*}$ and $\underline{b,c,x,y \in \mathbb{Z}}$ be given and assume that $\underline{a|b}$ and $\underline{a|c}$. Then, we have:

$$\begin{cases} a|b \\ a|c \end{cases} \Rightarrow \begin{cases} \exists \lambda \in \mathbb{Z} : b = a\lambda \\ \exists \mu \in \mathbb{Z} : c = a\mu \end{cases}$$

Choose $\lambda, \mu \in \mathbb{Z}$ such that $b = a\lambda$ and $c = a\mu$. Then, we have

$$bx+cy = (a\lambda)x + (a\mu)y = a(\lambda x) + a(\mu y) = a(\lambda x + \mu y) \Rightarrow$$

$\Rightarrow \exists k \in \mathbb{Z} : bx+cy = ak$ (for $k = \lambda x + \mu y \in \mathbb{Z}$)

$\Rightarrow \underline{a|(bx+cy)}$

We have thus shown that
$\forall a \in \mathbb{Z}^* : \forall b,c,x,y \in \mathbb{Z} : ((a|b \wedge a|c) \Rightarrow a|(bx+cy))$ □

EXAMPLES

a) Show that $\forall x \in \mathbb{Z} : (2 \mid (x^2-1) \Rightarrow 4 \mid (x^2-1))$

Solution

Let $x \in \mathbb{Z}$ be given and assume that $2 \mid (x^2-1)$. It follows that

$2 \mid (x^2-1) \Rightarrow \exists k \in \mathbb{Z} : x^2 - 1 = 2k$

$\Rightarrow \exists k \in \mathbb{Z} : x^2 = 2k+1$

$\Rightarrow x^2$ odd

$\Rightarrow x$ odd

$\Rightarrow \exists k \in \mathbb{Z} : x = 2k+1$

Choose $k \in \mathbb{Z}$ such that $x = 2k+1$. Then, we have:

$x^2 - 1 = (2k+1)^2 - 1 = 4k^2 + 4k + 1 - 1 = 4k^2 + 4k$

$= 4(k^2+k)$

$\Rightarrow \exists \lambda \in \mathbb{Z} : x^2 - 1 = 4\lambda$ (for $\lambda = k^2 + k \in \mathbb{Z}$)

$\Rightarrow 4 \mid (x^2-1)$.

We have thus shown that

$\forall x \in \mathbb{Z} : (2 \mid (x^2-1) \Rightarrow 4 \mid (x^2-1))$

b) Show that: $\forall x \in \mathbb{Z} : (\overline{3 \mid x} \Rightarrow 3 \mid (x^2-1))$

Solution

Let $x \in \mathbb{Z}$ be given and assume that $\overline{3 \mid x}$. From the division theorem, it follows that

$\overline{3 \mid x} \Rightarrow \exists a \in \mathbb{Z} : x = 3a+1 \vee x = 3a+2$

Choose $a \in \mathbb{Z}$ such that $x = 3a+1 \vee x = 3a+2$. We distinguish between the following cases.

Case 1: Assume that $x = 3a+1$. Then, we have

$x^2-1 = (3a+1)^2-1 = (3a+1-1)(3a+1+1) = 3a(3a+2)$

$\Rightarrow \exists k \in \mathbb{Z} : x^2-1 = 3k \quad (\text{for } k = a(3a+2) \in \mathbb{Z})$

$\Rightarrow 3 \mid (x^2-1)$

Case 2: Assume that $x = 3a+2$. Then, we have

$x^2-1 = (3a+2)^2-1 = (3a+2-1)(3a+2+1)$

$= (3a+1)(3a+3) = 3(3a+1)(a+1)$

$\Rightarrow \exists k \in \mathbb{Z} : x^2-1 = 3k \quad (\text{for } k = (3a+1)(a+1) \in \mathbb{Z})$

$\Rightarrow 3 \mid (x^2-1)$

In both cases, we have shown that $3 \mid (x^2-1)$.

We conclude that

$\forall x \in \mathbb{Z} : (\overline{3 \mid x} \Rightarrow 3 \mid (x^2-1))$ □

EXERCISES

(5) Let $a, b \in \mathbb{Z}$ be given. Show that

a) $a \mid b \Rightarrow a^2 \mid b^2$

b) $a \mid b \wedge b \mid a \Rightarrow a = b \vee a = -b$

c) $3 \nmid a \wedge 3 \nmid b \Rightarrow 3 \mid (a^2 - b^2)$

d) $3 \mid (2a^2 + 1) \Rightarrow 3 \nmid a$

e) $4 \mid (a^2 + b^2) \Rightarrow a$ even $\vee$ b even

f) $3 \mid (a^3 - a)$

g) $5 \mid (a^5 - 5a^3 + 4a)$

(6) Let $a, b, c \in \mathbb{Z}$ such that
$3 \mid c \wedge 3 \mid (a+b+c) \wedge 3 \mid (3a+b)$
Prove that $\forall x \in \mathbb{Z}: 3 \mid (ax^2 + bx + c)$.

(7) Let $a, b, x \in \mathbb{Z}$ be given. Prove that

a) $4 \mid 2a+b \wedge 4 \mid x-2 \Rightarrow 4 \mid ax+b$

b) $5 \mid 2a-b \wedge 5 \mid x-3 \Rightarrow 5 \mid ax^3 - b$

(8) Let $a, b, c \in \mathbb{Z}$ be given such that
$4 \mid c \wedge 4 \mid (a+b+c) \wedge 4 \mid 3a+b \wedge 4 \mid 5a+b$
Prove that $\forall x \in \mathbb{Z}: 4 \mid (ax^2 + bx + c)$.

▼ Method of induction

Let $a \in \mathbb{Z}$ and define $\mathbb{Z}_a = \{x \in \mathbb{Z} \mid x \geq a\}$. The method of induction can be used to prove statements of the form: $\forall x \in \mathbb{Z}_a : p(x)$.
It is based on Peano's theorem:

Thm : Let $a \in \mathbb{Z}$. Then:

$$\left.\begin{array}{l} p(a) \text{ true} \\ \forall x \in \mathbb{Z}_a : (p(x) \Rightarrow p(x+1)) \end{array}\right\} \Rightarrow \forall x \in \mathbb{Z}_a : p(x)$$

This theorem can be shown via the well-ordering principle.

▶ **Method** : To show $\forall x \in \mathbb{Z}_a : p(x)$ true

- 1 For $x = a$, show that $p(x)$ is true
- 2 Assume that for $x = k > a$, $p(k)$ is true
- 3 Show that $p(k+1)$ true
- 4 It follows that $\forall x \in \mathbb{Z}_a : p(x)$ true.

EXAMPLES

a) Show that $1+2+3+\cdots+n = \frac{n(n+1)}{2}$, $\forall n \in \mathbb{N} - \{0\}$

Proof

For $n=1$: LHS $= 1$

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

thus the statement is true.

For $n=k$, assume that

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

For $n=k+1$, we will show that

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

Since:

$$1+2+3+\cdots+(k+1) = [1+2+3+\cdots+k] + (k+1) =$$

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

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

It follows that $\forall n \in \mathbb{N}-\{0\}: 1+2+3+\cdots+n = \frac{n(n+1)}{2}$ □

b) Show that $\forall n \in \mathbb{N}: 3 \mid (2^{2n}-1)$.

Proof

For $n=0$: $2^{2n}-1 = 2^0-1 = 1-1 = 0 = 3\cdot 0 \Rightarrow 3 \mid 2^{2n}-1$.

For $n=k$: assume that $3 \mid (2^{2k}-1)$.

For $n=k+1$: we will show that $3 \mid (2^{2(k+1)}-1)$.

We have:

$3 \mid (2^{2k}-1) \Rightarrow \exists a \in \mathbb{Z} : 2^{2k} - 1 = 3a$

$\Rightarrow \exists a \in \mathbb{Z} : 2^{2k} = 3a + 1$

Choose $a \in \mathbb{Z}$ such that $2^{2k} = 3a + 1$. It follows that:

$2^{2(k+1)} - 1 = 2^{2k+2} - 1 = 2^{2k} \cdot 4 - 1 = 4(3a+1) - 1 =$

$= 12a + 4 - 1 = 12a + 3 = 3(4a + 1)$

$\Rightarrow \exists \lambda \in \mathbb{Z} : 2^{2(k+1)} - 1 = 3\lambda$ (for $\lambda = 4a + 1 \in \mathbb{Z}$)

$\Rightarrow 3 \mid (2^{2(k+1)} - 1)$

We conclude, by induction, that

$\forall n \in \mathbb{N} : 3 \mid (2^{2n} - 1)$ □

EXERCISES

(9) Prove the following identities for $n \in \mathbb{N}$, $n > 0$. By induction

a) $1 \cdot 2 + 2 \cdot 3 + 3 \cdot 4 + \cdots + n(n+1) = (1/3)\, n(n+1)(n+2)$, $n > 0$

b) $1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2$

c) $2 + 4 + 6 + \cdots + 2n = n(n+1)$

d) $1 \cdot 2^2 + 2 \cdot 3^2 + \cdots + n(n+1)^2 = (1/12)\, n(n+1)(n+2)(3n+5)$

e) $1^3 + 3^3 + 5^3 + \cdots + (2n-1)^3 = n^2(2n^2 - 1)$, $n \geq 2$

f) $2^3 + 4^3 + 6^3 + \cdots + (2n)^3 = 2n^2(n+1)^2$, $n > 1$

g) $2 + 2^2 + 2^3 + \cdots + 2^n = 2 \cdot (2^n - 1)$, $n \geq 3$

h) $\frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$, $n \geq 2$

i) $1 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + \cdots + n\,5^n = \dfrac{5 + (4n-1) \cdot 5^{n+1}}{16}$

(10) Prove the following statements by induction

a) $\forall n \in \mathbb{N} - \{0\}: \; 49 \mid (4 \cdot 8^n + 21n - 4)$

b) $\forall n \in \mathbb{N} - \{0\}: \; 9 \mid (2^{2n} + 15n - 1)$

c) $\forall n \in \mathbb{N} - \{0\}: 288 \mid (7^{2n+1} - 48n - 7)$

d) $\forall n \in \mathbb{N} - \{0\}: \; 64 \mid (7^{2n} + 16n - 1)$

e) $\forall n \in \mathbb{N} - \{0\}: \; 4 \mid (5^n - 1)$

f) $\forall n \in \mathbb{N} - \{0\}: \; 81 \mid (10^{n+1} - 9n - 10)$

g) $\forall n \in \mathbb{N} - \{0\}: \; 7 \mid (3^{2n} - 2^n)$

(11) Show that $A_n = (1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n}$ is an even integer for $n \in \mathbb{N} - \{0\}$.