BASIC NUMBER THEORY

I Modulo arithmetic

We recall the following set definitions

a) The set of natural numbers

$\mathbb{N} = \{0, 1, 2, 3, \dots\}$

$\mathbb{N}^* = \mathbb{N} - \{0\} = \{1, 2, 3, \dots\}$

b) The set of integers

$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$

$\mathbb{Z}^* = \mathbb{Z} - \{0\} = \{1, -1, 2, -2, 3, -3, \dots\}$

We now use these to define divisibility and modulo equivalence.

Def: Let $a, b \in \mathbb{Z}$ be given. We say that <u>a divides b</u> (i.e. $a|b$) if and only if there is some integer k such that $b = ak$:

$\forall a, b \in \mathbb{Z}: (a|b \Leftrightarrow \exists k \in \mathbb{Z}: b = ak)$

Def: (modulo equivalence).

$\forall a, b, m \in \mathbb{Z}: (a \equiv b \pmod m \Leftrightarrow m | (a-b))$

Def: Let $a \in \mathbb{Z}^*$. We define the set Δ_a of all divisors of a as:

$\Delta_a = \{b \in \mathbb{Z} \mid (b|a)\}$

EXAMPLES

a) Show that $17 \equiv 3 \bmod 7$

Solution

$17 - 3 = 14 = 7 \cdot 2 \Rightarrow \exists k \in \mathbb{Z} : 17 - 3 = 7k$ (for $k = 2$)

$\Rightarrow 7 \mid (17 - 3)$

$\Rightarrow 17 \equiv 3 \bmod 7$

b) Evaluate $\Delta_2, \Delta_4, \Delta_6$

Solution

$\Delta_2 = \{b \in \mathbb{Z} \mid (b \mid 2)\} = \{1, -1, 2, -2\}$

$\Delta_4 = \{b \in \mathbb{Z} \mid (b \mid 4)\} = \{1, -1, 2, -2, 4, -4\}$

$\Delta_6 = \{b \in \mathbb{Z} \mid (b \mid 6)\} = \{1, -1, 2, -2, 3, -3, 6, -6\}$

↳ Modulo arithmetic satisfies the reflexive, symmetric, and transitive properties.

c) Show that $\forall a, m \in \mathbb{Z} : a \equiv a \bmod m$

Solution

Let $a, m \in \mathbb{Z}$ be given. Then:

$a - a = 0 = 0m \Rightarrow \exists k \in \mathbb{Z} : a - a = km$

$\Rightarrow m \mid (a - a)$

$\Rightarrow a \equiv a \bmod m$

It follows that $\forall a, m \in \mathbb{Z} : a \equiv a \bmod m$

d) Show that

$$\forall a,b,m \in \mathbb{Z} : (a \equiv b \bmod m \Rightarrow b \equiv a \bmod m)$$

Solution

Let $a,b,m \in \mathbb{Z}$ be given. Assume that $a \equiv b \bmod m$.

Then,

$$a \equiv b \bmod m \Rightarrow m \mid (a-b)$$
$$\Rightarrow \exists k \in \mathbb{Z} : a-b = mk$$

Choose a $k_0 \in \mathbb{Z}$ such that $a-b = mk_0$. Then:

$$b-a = -(a-b) = -mk_0 = m(-k_0) \Rightarrow$$
$$\Rightarrow \exists k \in \mathbb{Z} : b-a = mk \quad (\text{for } k = -k_0)$$
$$\Rightarrow m \mid (b-a)$$
$$\Rightarrow b \equiv a \bmod m$$

We have thus shown that

$$\forall a,b,m \in \mathbb{Z} : (a \equiv b \bmod m \Rightarrow b \equiv a \bmod m).$$

e) Show that

$$\forall a,b,c,m \in \mathbb{Z} : \left(\begin{cases} a \equiv b \bmod m \\ b \equiv c \bmod m \end{cases} \Rightarrow a \equiv c \bmod m \right)$$

Solution

Let $a,b,c,m \in \mathbb{Z}$ be given. Assume that $a \equiv b \bmod m$ and $b \equiv c \bmod m$. Then,

$$\begin{cases} a \equiv b \bmod m \\ b \equiv c \bmod m \end{cases} \Rightarrow \begin{cases} m \mid (a-b) \\ m \mid (b-c) \end{cases} \Rightarrow$$
$$\Rightarrow \begin{cases} \exists k \in \mathbb{Z} : a-b = mk \\ \exists \lambda \in \mathbb{Z} : b-c = m\lambda \end{cases}$$

Choose $k_0, \lambda_0 \in \mathbb{Z}$ such that $a-b = mk_0$ and $b-c = m\lambda_0$.
It follows that

$$a-c = (a-b)+(b-c) = mk_0 + m\lambda_0 = m(k_0+\lambda_0) \Rightarrow$$
$$\Rightarrow \exists \mu \in \mathbb{Z} : a-c = m\mu \quad (\text{for } \mu = k_0+\lambda_0)$$
$$\Rightarrow m \mid (a-c)$$
$$\Rightarrow \underline{a \equiv c \bmod m}$$

We have thus shown that

$$\forall a,b,c,m \in \mathbb{Z}: \left(\begin{cases} a \equiv b \bmod m \\ b \equiv c \bmod m \end{cases} \Rightarrow a \equiv c \bmod m \right)$$

f) Show that $\forall a,b \in \mathbb{Z} : \Delta_a \cap \Delta_b \subseteq \Delta_{ab}$.

Solution

Let $a,b \in \mathbb{Z}$ be given. Let $x \in \Delta_a \cap \Delta_b$ be given. Then:

$$x \in \Delta_a \cap \Delta_b \Rightarrow x \in \Delta_a \wedge x \in \Delta_b \Rightarrow$$
$$\Rightarrow x \mid a \wedge x \mid b \Rightarrow$$
$$\Rightarrow \begin{cases} \exists k \in \mathbb{Z} : a = kx \\ \exists \lambda \in \mathbb{Z} : b = \lambda x \end{cases}$$

Choose $k_0, \lambda_0 \in \mathbb{Z}$ such that $a = k_0 x$ and $b = \lambda_0 x$.
It follows that:

$$ab = (k_0 x)(\lambda_0 x) = x(k_0 \lambda_0 x) \Rightarrow$$
$$\Rightarrow \exists \mu \in \mathbb{Z} : ab = \mu x \quad (\text{for } \mu = k_0 \lambda_0 x)$$
$$\Rightarrow x \mid ab$$
$$\Rightarrow x \in \Delta_{ab}.$$

From the above argument:

$$\forall a,b \in \mathbb{Z} : \forall x \in \Delta_a \cap \Delta_b : x \in \Delta_{ab} \Rightarrow$$
$$\Rightarrow \forall a,b \in \mathbb{Z} : \Delta_a \cap \Delta_b \subseteq \Delta_{ab}.$$

Division theorem

The division theorem is useful in divisibility proofs, and we state it without proof:

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

▸ interpretation : The division theorem establishes that when we divide two integers b with a we obtain a unique quotient q and remainder r with $0 \leq r < |a|$. such that the division identity $b = aq + r$ is satisfied.

▸ notation : The unique quotient q and remainder r are denoted as: $q = b \div a$ and $r = b \bmod a$.

↳ A convincing explanation of this result can be made in terms of the well-known long division algorithm from high school, which will always produce a unique quotient and remainder. A rigorous proof uses the well-ordering principle, which in axiomatic set theory requires the axiom of choice.

- Choosing the value of a yields the following useful corollaries:

For $a = 2$: $\forall b \in \mathbb{Z} : \exists! \, q \in \mathbb{Z} : (b = 2q \vee b = 2q+1)$

For $a = 3$: $\forall b \in \mathbb{Z} : \exists! \, q \in \mathbb{Z} : (b = 3q \vee b = 3q+1 \vee b = 3q+2)$

For $a = 4$: $\forall b \in \mathbb{Z} : \exists! \, q \in \mathbb{Z} : (b = 4q \vee b = 4q+1 \vee b = 4q+2 \vee b = 4q+3)$.

EXAMPLES

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

Solution

Let $x \in \mathbb{Z}$ be given and assume that $x^2 \equiv 1 \pmod 2$. Then,

$x^2 \equiv 1 \pmod 2 \Rightarrow 2 \mid (x^2-1) \Rightarrow$

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

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

$\Rightarrow x^2 \bmod 2 = 1.$

From the division theorem:

$\exists! k \in \mathbb{Z}: (x = 2k \vee x = 2k+1).$

We distinguish between the following cases.

Case 1: Assume that $x = 2k$ for some $k \in \mathbb{Z}$.

Then $x^2 = (2k)^2 = 4k^2 = 2(2k^2) \Rightarrow$

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

$\Rightarrow x^2 \bmod 2 = 0 \longleftarrow$ Contradiction.

therefore, this case does not materialize.

Case 2: Assume that $x = 2k+1$ for some $k \in \mathbb{Z}$

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

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

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

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

$\Rightarrow x^2 \equiv 1 \pmod 4.$

From the above argument, we find:

$\forall x \in \mathbb{Z}: (x^2 \equiv 1 \pmod 2 \Rightarrow x^2 \equiv 1 \pmod 4).$

8) Show that $\forall x \in \mathbb{Z}: (x \not\equiv 0 \pmod 3 \Rightarrow x^2 \equiv 1 \pmod 3)$

Solution

Let $x \in \mathbb{Z}$ be given. Assume $x \not\equiv 0 \pmod 3$. Then:

$$x \not\equiv 0 \pmod 3 \Rightarrow 3 \mid (x-0) \Rightarrow 3 \mid x \Rightarrow$$
$$\Rightarrow \exists k \in \mathbb{Z}: x = 3k$$
$$\Rightarrow \exists k \in \mathbb{Z}: (x = 3k+1 \vee x = 3k+2)$$

via the division theorem. We distinguish between the following cases

Case 1: Assume that $x = 3k+1$ for some $k \in \mathbb{Z}$. Then,

$$x^2 - 1 = (3k+1)^2 - 1 = (9k^2 + 6k + 1) - 1 = 9k^2 + 6k$$
$$= 3(3k^2 + 2k) \Rightarrow$$
$$\Rightarrow \exists \lambda \in \mathbb{Z}: x^2 - 1 = 3\lambda \quad (\text{for } \lambda = 3k^2 + 2k).$$

Case 2: Assume that $x = 3k+2$ for some $k \in \mathbb{Z}$. Then,

$$x^2 - 1 = (3k+2)^2 - 1 = (9k^2 + 12k + 4) - 1 =$$
$$= 9k^2 + 12k + 3 = 3(3k^2 + 4k + 1) \Rightarrow$$
$$\Rightarrow \exists \lambda \in \mathbb{Z}: x^2 - 1 = 3\lambda \quad (\text{for } \lambda = 3k^2 + 4k + 1)$$

In both cases, we have shown:

$$(\exists \lambda \in \mathbb{Z}: x^2 - 1 = 3\lambda) \Rightarrow 3 \mid (x^2 - 1)$$
$$\Rightarrow x^2 \equiv 1 \pmod 3$$

From the above argument:

$$\forall x \in \mathbb{Z}: (x \not\equiv 0 \pmod 3 \Rightarrow x^2 \equiv 1 \pmod 3)$$

EXERCISES

(1) 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) $a \not\equiv 0 \pmod 3 \wedge b \not\equiv 0 \pmod 3 \Rightarrow a^2 \equiv b^2 \pmod 3$

d) $2a^2 + 1 \equiv 0 \pmod 3 \Rightarrow a \not\equiv 0 \pmod 3$

e) $a^3 \equiv a \pmod 3$

f) $a^5 \equiv 5a^3 - 4a \pmod 5$

(2) Let $a, b, c \in \mathbb{Z}$ such that

$c \equiv 0 \pmod 3 \wedge a + b + c \equiv 0 \pmod 3 \wedge 3a + b \equiv 0 \pmod 3$

Show that $\forall x \in \mathbb{Z}: ax^2 + bx + c \equiv 0 \pmod 3$

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

a) $\begin{cases} 2a + b \equiv 0 \pmod 4 \\ x \equiv 2 \pmod 4 \end{cases} \Rightarrow ax + b \equiv 0 \pmod 4$

b) $\begin{cases} 2a \equiv b \pmod 5 \\ x \equiv 3 \pmod 5 \end{cases} \Rightarrow ax^3 \equiv b \pmod 5$

(4) Let $a, b, c \in \mathbb{Z}$ be given such that

$4 \mid c \wedge 4 \mid (a + b + c) \wedge 4 \mid (3a + b) \wedge 4 \mid (5a + b)$

Show that $\forall x \in \mathbb{Z}: ax^2 + bx + c \equiv 0 \pmod 4$.

▼ 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 $3 \mid (2^{2(k+1)}-1)$.

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

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

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

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

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

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

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

It follows by induction that

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

EXERCISES

⑤ Prove the following identities by induction

a) $\forall n \in \mathbb{N}^*: 1\cdot 2 + 2\cdot 3 + 3\cdot 4 + \dots + n(n+1) = (1/3)n(n+1)(n+2)$

b) $\forall n \in \mathbb{N}^*: 1+3+5+\dots+(2n+1) = (n+1)^2$

c) $\forall n \in \mathbb{N}^*: 2+4+6+\dots+2n = n(n+1)$

d) $\forall n \in \mathbb{N}^*: 1\cdot 2^2 + 2\cdot 3^2 + \dots + n(n+1)^2 = (1/12)n(n+1)(n+2)(3n+5)$

e) $\forall n \in \mathbb{N}^* - \{1\}: 1^3 + 3^3 + 5^3 + \dots + (2n-1)^3 = n^2(2n^2-1)$

f) $\forall n \in \mathbb{N}^* - \{1\}: 2^3 + 4^3 + 6^3 + \dots + (2n)^3 = 2n^2(n+1)^2$

g) $\forall n \in \mathbb{N}^* - \{1,2\}: 2 + 2^2 + \dots + 2^n = 2(2^n - 1)$

h) $\forall n \in \mathbb{N}^* - \{1\}: \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \dots + \frac{1}{2^n} = 1 - \frac{1}{2^n}$

i) $\forall n \in \mathbb{N}^*: 1\cdot 5 + 2\cdot 5^2 + 3\cdot 5^3 + \dots + n5^n = \frac{5 + (4n-1)5^{n+1}}{16}$

⑥ Show the following statements by induction

a) $\forall n \in \mathbb{N}^*: 4\cdot 8^n + 21n \equiv 4 \pmod{49}$

b) $\forall n \in \mathbb{N}^*: 2^{2n} + 15n \equiv 1 \pmod{9}$

c) $\forall n \in \mathbb{N}^*: 7^{2n+1} \equiv 48n + 7 \pmod{288}$

d) $\forall n \in \mathbb{N}^*: 5^n \equiv 1 \pmod{4}$

e) $\forall n \in \mathbb{N}^*: 10^{n+1} \equiv 9n + 10 \pmod{81}$

f) $\forall n \in \mathbb{N}^*: 7^{2n} \equiv 1 - 16n \pmod{64}$

g) $\forall n \in \mathbb{N}^*: 3^{2n} \equiv 2^n \pmod{7}$

⑦ Show that

$\forall n \in \mathbb{N}^*: (1+\sqrt{2})^{2n} + (1-\sqrt{2})^{2n} \equiv 0 \pmod{2}$.