III. DIVISIBILITY

DEFINITION: If $n, d \in \mathbb{Z}$ and $d \neq 0$, then $\boldsymbol{n}$ **is divisible by** $\boldsymbol{d}$ if, and only if, $n = d \cdot k$ for some $k \in \mathbb{Z}$.

NOTATION: $\boldsymbol{d \mid n}$ means $\boldsymbol{n}$ **is divisible by** $\boldsymbol{d}$ or $\boldsymbol{d}$ **divides** $\boldsymbol{n}$**.**

1. $\forall \boldsymbol{k} \in \mathbb{Z}^+, (\boldsymbol{3k+1})(\boldsymbol{3k+2})(\boldsymbol{3k+3})$ **is divisible by 3. (TRUE)**

Proof. We have

$$(3k+1)(3k+2)(3k+3) = 3(3k+1)(3k+2)(k+1). \qquad (*)$$

Since $k \in \mathbb{Z}$, it follows that $(3k+1)(3k+2)(k+1) \in \mathbb{Z}$. This, $(*)$ and the definition above give the desired result. ■

2. $\forall \boldsymbol{k} \in \mathbb{Z}^+$**, if** $\boldsymbol{n = 4k+1}$**, then 8 divides** $\boldsymbol{n^2 - 1}$**. (TRUE)**

Proof. We have

$$n^2 - 1 = (4k+1)^2 - 1 = 16k^2 + 8k + 1 - 1 = 16k^2 + 8k = 8(2k^2 + k). \qquad (*)$$

Since $k \in \mathbb{Z}$, it follows that $(2k^2 + k) \in \mathbb{Z}$. This, $(*)$ and the definition above give the desired result. ■

3. $\forall \boldsymbol{a, b, c} \in \mathbb{Z}^+$**, if** $\boldsymbol{a|b}$ **and** $\boldsymbol{a|c}$**, then** $\boldsymbol{a|(b+c)}$**. (TRUE)**

Proof. Since $a|b$ and $a|c$, by the definition above we have

$$b = a \cdot k_1, \quad c = a \cdot k_2$$

for some $k_1, k_2 \in \mathbb{Z}$. Therefore

$$b + c = a \cdot k_1 + a \cdot k_2 = a(k_1 + k_2). \qquad (*)$$

Since $k_1, k_2 \in \mathbb{Z}$, it follows that $(k_1 + k_2) \in \mathbb{Z}$. We also note that $a \neq 0$, for $a \in \mathbb{Z}^+$. This, $(*)$ and the definition above give the desired result. ■

4. Let $\boldsymbol{a, b} \in \mathbb{Z}$**,** $\boldsymbol{a \neq 0, b \neq 0}$**. If** $\boldsymbol{a|b}$ **and** $\boldsymbol{b|a}$**, then** $\boldsymbol{a = b}$ **or** $\boldsymbol{a = -b}$**. (TRUE)**

Proof. Since $a|b$ and $b|a$, by the definition above we have

$$b = ak_1, \quad a = bk_2 \qquad (*)$$

for some $k_1, k_2 \in \mathbb{Z}$. Multiplying out these equalities, we obtain

$$ab = abk_1k_2. \qquad (**)$$

Since $a \neq 0$ and $b \neq 0$, it follows that $ab \neq 0$, therefore we can cancel out ab from $(**)$. We get

$$1 = k_1 k_2.$$

From this it follows that $k_1 = k_2 = 1$ or $k_1 = k_2 = -1$. This and $(*)$ give the desired result. ■

5. $\forall a, b \in \mathbb{Z}$, if $a - b \neq 0$, then $(a - b)|(a^2 - b^2)$. (TRUE)

Proof. We have

$$a^2 - b^2 = (a - b)(a + b). \qquad (*)$$

Since $a, b \in \mathbb{Z}$, it follows that $(a - b) \in \mathbb{Z}$ and $(a + b) \in \mathbb{Z}$. Since $a - b \neq 0$, this, $(*)$ and the definition above give the desired result. ■

6*. $\forall a \in \mathbb{Z}^+$, $(a^2 + a + 1)|(a^3 - 1)$. (TRUE)

Proof. We have

$$a^3 - 1 = (a^2 + a + 1)(a - 1). \qquad (*)$$

Since $a \in \mathbb{Z}^+$, it follows that $(a^2 + a + 1) \in \mathbb{Z}^+$ and $(a - 1) \in \mathbb{Z}$. This, $(*)$ and the definition above give the desired result. ■

7*. $\forall a, b \in \mathbb{Z}^+$, $(a + 1)|(ab + a + b + 1)$. (TRUE)

Proof. We have

$$ab + a + b + 1 = a(b + 1) + b + 1 = (a + 1)(b + 1). \qquad (*)$$

Since $a, b \in \mathbb{Z}^+$, it follows that $(a + 1) \in \mathbb{Z}^+$ and $(b + 1) \in \mathbb{Z}^+$. This, $(*)$ and the definition above give the desired result. ■

8. $\forall a, b \in \mathbb{Z}^+$, $(a^2 + b^2 + ab)|(a^4 + a^2b^2 + b^4)$. (TRUE)**

Proof. We have

$$\begin{aligned} a^4 + a^2b^2 + b^4 = (a^4 + 2a^2b^2 + b^4) - a^2b^2 &= (a^2 + b^2)^2 - a^2b^2 \\ &= (a^2 + b^2)^2 - (ab)^2 \qquad (*) \\ &= (a^2 + b^2 + ab)(a^2 + b^2 - ab). \end{aligned}$$

Since $a, b \in \mathbb{Z}^+$, it follows that $(a^2 + b^2 + ab) \in \mathbb{Z}^+$, and $(a^2 + b^2 - ab) \in \mathbb{Z}$. This, $(*)$ and the definition above give the desired result. ■

THEOREM (The Quotient-Remainder Theorem):
For any $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$, there exist unique numbers $q, r \in \mathbb{Z}$ such that

$$n = d \cdot q + r, \quad \text{where} \quad 0 \leq r < d.$$

9. $\forall k \in \mathbb{Z}$, $3 \nmid k^2 - 2$. (TRUE)**

Proof (Indirect). Suppose, contrary to our claim, that

$$\exists k \in \mathbb{Z} \mid 3 \text{ divides } k^2 - 2.$$

By the definition above we have

$$k^2 - 2 = 3m \qquad (*)$$

for some $m \in \mathbb{Z}$. On the other hand, by the theorem above we have only three possibilities:

$$k = 3q, \quad k = 3q + 1, \quad \text{or} \quad k = 3q + 2,$$

where $q \in \mathbb{Z}$. Therefore, for k^2 we have only two possibilities:

$$k^2 = 9q^2 = 3r,$$

$$k^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(\underbrace{3q^2 + 2q}_{r}) + 1 = 3r + 1,$$

or

$$k^2 = (3q+2)^2 = 9q^2 + 12q + 4 = 9q^2 + 12q + 3 + 1 = 3(\underbrace{3q^2 + 4q + 1}_{r}) + 1 = 3r + 1,$$

where $r \in \mathbb{Z}$, for $q \in \mathbb{Z}$. Consider each of them.

Case I. Let $k^2 = 3r$. Substituting this into $(*)$, we get

$$3r - 2 = 3m,$$

hence

$$3r = 3m + 2,$$

which contradicts the theorem above.

Case II. Let $k^2 = 3r + 1$. Substituting this into $(*)$, we get

$$3r + 1 - 2 = 3m,$$

hence

$$3r = 3m + 1,$$

which contradicts the theorem above. ■

10. $\forall k \in \mathbb{Z}$, $4 \nmid k^2 - 3$. (TRUE)**

Proof (Indirect). Suppose, contrary to our claim, that

$$\exists k \in \mathbb{Z} \mid 4 \text{ divides } k^2 - 3.$$

By the definition above we have

$$k^2 - 3 = 4m \qquad (*)$$

for some $m \in \mathbb{Z}$. On the other hand, by the theorem above we have only two possibilities:

$$k = 2q \quad \text{or} \quad k = 2q + 1,$$

where $q \in \mathbb{Z}$. Therefore, for k^2 we have also only two possibilities:

$$k^2 = 4q^2 = 4r$$

or

$$k^2 = 4q^2 + 4q + 1 = 4(\underbrace{q^2 + q}_{r}) + 1 = 4r + 1,$$

where $r \in \mathbb{Z}$, for $q \in \mathbb{Z}$. Consider each of them.

Case I. Let $k^2 = 4r$. Substituting this into $(*)$, we get

$$4r - 3 = 4m,$$

hence

$$4r = 4m + 3,$$

which contradicts the theorem above.

Case II. Let $k^2 = 4r + 1$. Substituting this into $(*)$, we get

$$4r + 1 - 3 = 4m,$$

hence

$$4r = 4m + 2,$$

which contradicts the theorem above. ■

11^{**}. $\forall a, b \in \mathbb{Z}$, $4 \nmid a^2 + b^2 - 3$. (TRUE)

Proof (Indirect). Suppose, contrary to our claim, that

$$\exists a, b \in \mathbb{Z} \mid 4 \text{ divides } a^2 + b^2 - 3.$$

By the definition above we have

$$a^2 + b^2 - 3 = 4m \qquad (*)$$

for some $m \in \mathbb{Z}$. On the other hand, by the theorem above for any $k \in \mathbb{Z}$ we have only two possibilities:

$$k = 2q \quad \text{or} \quad k = 2q + 1,$$

where $q \in \mathbb{Z}$. Therefore, for k^2 we have also only two possibilities:

$$k^2 = 4q^2 = 4r$$

or

$$k^2 = 4q^2 + 4q + 1 = 4(\underbrace{q^2 + q}_{r}) + 1 = 4r + 1,$$

where $r \in \mathbb{Z}$, for $q \in \mathbb{Z}$. From this it follows that for $a^2 + b^2 - 3$ we have only three possibilities:

$$a^2 + b^2 - 3 = 4r_1 + 4r_2 - 3 = 4(\underbrace{r_1 + r_2}_{R}) - 3 = 4R - 3,$$
$$a^2 + b^2 - 3 = 4r_1 + 4r_2 + 1 - 3 = 4(\underbrace{r_1 + r_2}_{R}) - 2 = 4R - 2,$$

or

$$a^2 + b^2 - 3 = 4r_1 + 4r_2 + 2 - 3 = 4(\underbrace{r_1 + r_2}_{R}) - 1 = 4R - 1,$$

where $R \in \mathbb{Z}$, for $r_1, r_2 \in \mathbb{Z}$. If we compare each of them with $(*)$, we obtain contradictions as in the proofs above. ■

12. $\forall a, b, c \in \mathbb{Z}$ and $\forall k \in \mathbb{Z}^+$, $8k + 7 \neq a^2 + b^2 + c^2$. (TRUE)**

Proof (Indirect). Suppose, contrary to our claim, that

$$\exists a, b \in \mathbb{Z} \text{ and } k \in \mathbb{Z}^+ |\ 8k + 7 = a^2 + b^2 + c^2. \qquad (*)$$

On the other hand, by the theorem above for any $k \in \mathbb{Z}$ we have only eight possibilities:

$$k = 8q, \quad k = 8q + 1, \ldots, k = 8q + 6, \quad \text{or} \quad k = 8q + 7,$$

where $q \in \mathbb{Z}$. From this one can deduce that for k^2 we have only three possibilities:

$$k^2 = 8r, \quad k^2 = 8r + 1, \quad \text{or} \quad k^2 = 8r + 4,$$

where $r \in \mathbb{Z}$. From this it follows that there is no combination which gives

$$a^2 + b^2 + c^2 = 4R + 7.$$

We obtain a contradiction. ■