Divisibility

DEFINITION: If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c such that $b = ac$. If a divides b, we also say that a is a **divisor** or **factor** of b.

NOTATION: $d \mid n$ means n is divisible by d or d divides n.

EXAMPLE: We have: $4 \mid 12$, since $12 = 4 \cdot 3$
$4 \not\mid 15$, since $15 = 4 \cdot 3.75$

THEOREM 1: If a, b, and c are integers with $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof: Because $a \mid b$ and $b \mid c$, there are integers e and f such that $ae = b$ and $bf = c$. Hence,

$$c = bf = (ae)f = a(ef)$$

and we conclude that $a \mid c$. ■

EXAMPLE: Since $7 \mid 56$ and $56 \mid 168$, the Theorem above tells us that $7 \mid 168$.

THEOREM 2: If a, b, c, m, and n are integers with $c \neq 0$, and if $c \mid a$ and $c \mid b$, then $c \mid (ma+nb)$.

Proof: Since $c \mid a$ and $c \mid b$, by the definition above we have

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

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

$$ma + nb = mc \cdot k_1 + nc \cdot k_2 = c(mk_1 + nk_2).$$

Consequently, we see that $c \mid (ma + nb)$. ■

EXAMPLE: Since $11 \mid 22$ and $11 \mid 33$, the Theorem above tells us that 11 divides

$$4 \cdot 22 + 7 \cdot 33 = 319$$

EXAMPLE: Let k be an integer number. Show that $8 \mid (n^2 - 1)$ if $n = 4k + 1$.

Proof: We have

$$n^2 - 1 = (4k + 1)^2 - 1 = 16k^2 + 8k + 1 - 1 = 16k^2 + 8k = 8(2k^2 + k)$$

Therefore $8 \mid (n^2 - 1)$ by the definition above. ■

EXAMPLE: Let a and b be integer numbers. Show that $(a - b) \mid (a^2 - b^2)$ if $a - b \neq 0$.

Proof: We have

$$a^2 - b^2 = (a - b)(a + b)$$

Therefore $(a - b) \mid (a^2 - b^2)$ by the definition above. ■

REMARK. For more examples, see Appendix I.

THEOREM 3 (DIVISION ALGORITHM): For any integers a and b with $b \neq 0$ there exist unique integers q and r such that

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

The integers q and r are called the **quotient** and the **reminder**, respectively.

Proof 1: Consider the set S of all integers of the form $a - bk$ where k is an integer, that is,

$$S = \{a - bk \mid k \in \mathbb{Z}\}$$

Let T be the set of all nonnegative integers in S. T is nonempty, because $a - bk$ is nonnegative whenever k is an integer with

$$k \leq a/b \quad (\text{if } \ b > 0) \qquad \text{or} \qquad k \geq a/b \quad (\text{if } \ b < 0)$$

By the well-ordering property, T has a least element

$$r = a - bq$$

(These are the values for q and r specified in the theorem.) We have to prove that $0 \leq r < |b|$. We first show that $r < |b|$. Assume to the contrary that $r \geq |b|$. Then

$$r - |b| \geq 0$$

On the other hand,

$$r - |b| = a - bq - |b| = a - b\left(q + \frac{|b|}{b}\right)$$

which is of the form $a - bk$, where $k = q + \dfrac{|b|}{b}$ is an integer, since $|b|/b$ is either 1 or -1. So, $r - |b|$ is nonnegative and is of the form $a - bk$, where k is an integer. Therefore $r - |b|$ is from T. But $r - |b| < r$ which contradicts the choice of r as the least integer from T. Hence, $r < |b|$. Finally, since r is from T, it follows that $r \geq 0$. So, $0 \leq r < |b|$.

To show that these values for q and r are unique, assume that we have two equations

$$a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2$$

with $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$. By subtracting the second of these equations from the first, we find that

$$0 = b(q_1 - q_2) + (r_1 - r_2)$$

Hence, we see that

$$r_2 - r_1 = b(q_1 - q_2)$$

This tells us that b divides $r_2 - r_1$. Because $0 \leq r_1 < |b|$ and $0 \leq r_2 < |b|$, we have

$$-|b| < r_2 - r_1 < |b|$$

Hence, b can divide $r_2 - r_1$ only if $r_2 - r_1 = 0$ or, in other words, if

$$r_1 = r_2$$

Because $bq_1 + r_1 = bq_2 + r_2$ and $r_1 = r_2$, we also see that

$$q_1 = q_2$$

This shows that the quotient q and the reminder r are unique. ■

Proof 2: We distinguish two cases:

Case A: Suppose $b > 0$. Put

$$q = \lfloor a/b \rfloor, \quad r = a - b\lfloor a/b \rfloor$$

Clearly, q and r are integers. Therefore, all we have to prove is that $0 \leq r < |b|$. To show that $r \geq 0$ we note that $\lfloor a/b \rfloor \leq a/b$, therefore

$$r = a - b\lfloor a/b \rfloor \geq a - b(a/b) = a - a = 0$$

Similarly, to show that $r < |b|$ we note that $\lfloor a/b \rfloor > a/b - 1$, therefore

$$r = a - b\lfloor a/b \rfloor < a - b(a/b - 1) = a - b(a/b) + b = a - a + b = b = |b|$$

So, $r \geq 0$ and $r < |b|$, therefore $0 \leq r < |b|$.

Case B: Suppose $b < 0$. Put

$$q = \lceil a/b \rceil, \quad r = a - b\lceil a/b \rceil$$

As before, to prove that $0 \leq r < |b|$ we first show that $r \geq 0$. Since $\lceil a/b \rceil \geq a/b$ and $b < 0$, it follows that

$$r = a - b\lceil a/b \rceil \geq a - b(a/b) = a - a = 0$$

Similarly, to show that $r < b$ we note that $\lceil a/b \rceil < b + 1$, therefore

$$r = a - b\lceil a/b \rceil < a - b(a/b + 1) = a - b(a/b) - b = a - a - b = -b = |b|$$

So, $r \geq 0$ and $r < |b|$, therefore $0 \leq r < |b|$.

Finally, we show that q and r are unique in the same way as we did in Proof 1. ■

EXAMPLE: Let $a = 49$ and $b = 4$, then

$$49 = 4 \cdot 12 + 1$$

so the quotient is 12 and the reminder is 1. Note that we can also write 49 as $3 \cdot 12 + 13$, but in this case 13 is not a reminder, since it is *not* less than 4. Similarly,

if $a = 49$ and $b = -4$, then $49 = (-4) \cdot (-12) + 1$
if $a = -49$ and $b = 4$, then $-49 = 4 \cdot (-13) + 3$
if $a = -49$ and $b = -4$, then $-49 = -4 \cdot 13 + 3$

REMARK: Let $b > 0$. Because the quotient q is the largest integer such that

$$bq \leq a$$

and

$$r = a - bq$$

it follows that

$$q = \lfloor a/b \rfloor, \quad r = a - b\lfloor a/b \rfloor$$

For example,

if $a = 49$ and $b = 4$, then

$$q = \lfloor 49/4 \rfloor = \lfloor 12.25 \rfloor = 12, \quad r = 49 - 4 \cdot 12 = 49 - 48 = 1$$

if $a = -49$ and $b = 4$, then

$$q = \lfloor -49/4 \rfloor = \lfloor -12.25 \rfloor = -13, \quad r = -49 - 4 \cdot (-13) = -49 + 52 = 3$$

Similarly, if $b < 0$, then

$$q = \lceil a/b \rceil, \quad r = a - b\lceil a/b \rceil$$

For example,

if $a = 49$ and $b = -4$, then

$$q = \lceil 49/(-4) \rceil = \lceil -12.25 \rceil = -12, \quad r = 49 - (-4) \cdot (-12) = 49 - 48 = 1$$

if $a = -49$ and $b = -4$, then

$$q = \lceil -49/(-4) \rceil = \lceil 12.25 \rceil = 13, \quad r = -49 - (-4) \cdot 13 = -49 + 52 = 3$$

DEFINITION: If the remainder when n is divided by 2 is 0, then $n = 2k$ for some integer k, and we say that n is **even**, whereas if the remainder when n is divided by 2 is 1, then $n = 2k+1$ for some integer k, and we say that n is **odd**.

Thanks to the Division Algorithm for any integer number n there are only two possibilities:

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

therefore any integer number is either even or odd.

EXAMPLE: Let $b = 3$ in the Division Algorithm. Since $0 \leq r < 3$, then for any integer number n we have only three possibilities:

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

EXAMPLE: Let k be an integer number. Then $3 \nmid k^2 - 2$.

Proof: Assume to the contrary that there is an integer number k such that $3 \mid k^2 - 2$. By the definition of divisibility,

$$k^2 - 2 = 3m \tag{$*$}$$

for some integer m. On the other hand, by the Division Algorithm, there are only three possibilities:

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

where q is an integer. We show that for $k^2 - 2$ we have only two possibilities:

$$k^2 - 2 \quad \text{is either} \quad 3r + 1 \quad \text{or} \quad 3r + 2$$

where r is an integer (which gives us a contradiction with $(*)$ by the Division Algorithm). Indeed,

if $k = 3q$, then

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

if $k = 3q + 1$, then

$$\begin{aligned} k^2 - 2 = (3q + 1)^2 - 2 &= 9q^2 + 6q + 1 - 2 \\ &= 9q^2 + 6q - 1 \\ &= 9q^2 + 6q - 3 + 2 = 3(\underbrace{3q^2 + 2q - 1}_{r}) + 2 = 3r + 2 \end{aligned}$$

if $k = 3q + 2$, then

$$\begin{aligned} k^2 - 2 &= (3q+2)^2 - 2 \\ &= 9q^2 + 12q + 4 - 2 \\ &= 9q^2 + 12q + 2 \\ &= 3(\underbrace{3q^2 + 4q}_{r}) + 2 \\ &= 3r + 2 \quad \blacksquare \end{aligned}$$

REMARK. For more examples, see Appendix II.

Greatest Common Divisors

DEFINITION: A **common divisor** of two integers a and b, which are not both 0, is an integer c such that $c \mid a$ and $c \mid b$. The **greatest common divisor** (gcd) of a and b, denoted by (a, b), is the largest common divisor of integers a and b.

EXAMPLE: The common divisors of 24 and 84 are

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6, \quad \text{and} \quad \pm 12$$

Hence, $(24, 84) = 12$. Similarly, looking at sets of common divisors, we find that

$$(15, 81) = 3, \quad (100, 5) = 5, \quad (17, 25) = 1, \quad (-17, 289) = 17, \quad \text{etc.}$$

DEFINITION: The integers a and b, with $a \neq 0$ and $b \neq 0$, are **relatively prime** if

$$(a, b) = 1$$

EXAMPLE: Since

$$(12, 25) = 1$$

the numbers 12 and 25 are relatively prime.

Appendix I

EXAMPLE: Let a be an integer number. Show that $(a^2 + a + 1) \mid (a^3 - 1)$ if $a \neq 1$.

Proof: We have

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

Therefore $(a^2 + a + 1) \mid (a^3 - 1)$ by the definition of divisibility. ■

EXAMPLE: Let a and b be integer numbers. Show that $(a + 1) \mid (ab + a + b + 1)$ if $a \neq -1$.

Proof: We have

$$ab + a + b + 1 = a(b + 1) + b + 1 = (a + 1)(b + 1)$$

Therefore $(a + 1) \mid (ab + a + b + 1)$ by the definition of divisibility. ■

EXAMPLE: Let a and b be integer numbers, not both zero. Show that $(a^2 + b^2 + ab) \mid (a^4 + a^2b^2 + b^4)$.

Proof: We first note that $a^2 + b^2 + ab > 0$ for any real numbers a and b. Indeed, if $ab \geq 0$, then

$$a^2 + b^2 + ab \geq a^2 + b^2 > 0$$

Similarly, if $ab < 0$, then

$$a^2 + b^2 + ab = (a^2 + 2ab + b^2) - ab = (a + b)^2 - ab > (a + b)^2 \geq 0$$

We have

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

Therefore $(a^2 + b^2 + ab) \mid (a^4 + a^2b^2 + b^4)$ by the definition of divisibility. ■

Appendix II

EXAMPLE: Let k be an integer number. Then $4 \not| k^2 - 3$.

Proof: Assume to the contrary that there is an integer number k such that $4 \mid k^2 - 3$. By the definition of divisibility,

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

for some integer m. On the other hand, by the Division Algorithm, there are only two possibilities:

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

where q is an integer. We show that for $k^2 - 3$ we have only two possibilities:

$$k^2 - 3 \quad \text{is either} \quad 4r + 1 \quad \text{or} \quad 4r + 2$$

where r is an integer (which gives us a contradiction with $(*)$ by the Division Algorithm). Indeed,

if $k = 2q$, then

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

if $k = 2q + 1$, then

$$\begin{aligned} k^2 - 3 &= (2q + 1)^2 - 3 \\ &= 4q^2 + 4q + 1 - 3 \\ &= 4q^2 + 4q - 2 \\ &= 4q^2 + 4q - 4 + 2 = 4(\underbrace{q^2 + q - 1}_{r}) + 2 = 4r + 2 \end{aligned}$$

■

EXAMPLE: Let a and b be integer numbers. Then $4 \not| a^2 + b^2 - 3$.

Proof: Assume to the contrary that there are integer numbers a and b such that $4 \mid a^2 + b^2 - 3$. By the definition of divisibility,

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

for some integer m. On the other hand, by the Division Algorithm, for any integer k we have only two possibilities:

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

where q is an integer. Therefore, for k^2 we also have 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 is an integer. From this it follows that for a^2+b^2-3 we have only three possibilities:

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

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

or

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

where R is an integer. This gives us a contradiction with $(*)$ by the Division Algorithm. ■

EXAMPLE: Let a, b, c, and k be integer numbers. Then $8k+7 \neq a^2+b^2+c^2$.
Proof (short): Assume to the contrary that there are integer numbers a, b, c, and k such that

$$8k+7=a^2+b^2+c^2$$

On the other hand, by the Division Algorithm, for any integer k we have only eight possibilities:

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

where q is an integer. 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 is an integer. From this it follows that there is no combination of a^2, b^2, and c^2 such that $a^2+b^2+c^2=4k+7$. ■