Divisibility

Divisibility

If n and d are integers then n is **divisible by** d if, and only if, n equals d times some integer and $d \neq 0$, that is

$$n = dk, \qquad \text{for some integer } k$$

Instead of "n is divisible by d," we can say that

- n **is a multiple of** d, or
- d **is a factor of** n, or
- d **is a divisor of** n, or
- d **divides** n.

Notation:

- The notation $\boldsymbol{d|n}$ is read "d divides n." Symbolically, if n and d are integers:

$$d|n \Leftrightarrow \exists \text{an integer, say } k \text{, such that } n = dk \text{ and } d \neq 0.$$

- The notation $\boldsymbol{d \nmid n}$ is read "d does not divide n."

Example:

1. Is 21 divisible by 3?
2. Is 32 a multiple of -16?
3. Does 5 divide 40?
4. Is 6 a factor of 54?
5. Does $7|42$?
6. Is 7 a factor of -7?

Question:

If k is any nonzero integer, does k divide 0?

Yes, because $0=k.0$

Divisibility and Algebraic Expressions

1. If a and b are integers, is $3a+3b$ divisible by 3?
2. If k and m are integers, is $10km$ divisible by 5?

Theorem: For all integers a and b, if a and b are positive and a divides b then $a \leq b$.

Proof: Suppose a and b are any arbitrary but particular positive integers such that a divides b. *[We must show that $a \leq b$.]*

By definition of divisibility, there exists an integer *k* so that $b = ak$. Since both a and b are positive, *k* must be positive because both a and b are positive. It follows that

$$1 \leq k$$

because every positive integer is greater than or equal to 1. Multiplying both sides by a gives

$$a \leq ak = b$$

because multiplying both sides of an inequality by a positive number preserves the inequality. Thus $a \leq b$ *[as was to be shown]*.

Example:

Is the following statement true or false?

For all integers a and b, if $a|b$ and $b|a$ then $a=b$.

Theorem: The only divisors of 1 are 1 and -1.

Proof: Since 1.1=1 and (-1)(-1)=1, both 1 and -1 are divisors of 1. Now suppose *m* is any integer that divides 1. Then there exists an integer *n* such that 1=*mn*. Then either both *m* and *n* are positive or both *m* and *n* are negative. If both *m* and *n* are positive, then *m* is a positive integer divisor of 1. By a previous theorem, $m \leq 1$, and, since the only positive integer that is less than or equal to 1 is 1 itself, it follows that *m*=1. On the other hand, if both *m* and *n* are negative, then (-*m*)(-*n*)=*mn*=1. In this case -*m* is a positive integer divisor of 1, and so, by the same reasoning, -*m*=1 and thus *m*=-1. Therefore there are only two possibilities: either *m*=1 or *m*=-1. So the only divisors of 1 are 1 and -1.

Theorem: Transitivity of Divisibility

Prove that for all integers a, b, and c, if $a|b$ and $b|c$, then $a|c$.

Theorem: Divisibility by prime

Any integer $n>1$ is divisible by a prime number.

Theorem: Unique Factorization of Integers Theorem (Fundamental Theorem of Arithmetic)

Given any integer $n > 1$, there exist a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

and any other expression for n as a product of prime numbers is identical to this except, perhaps, for the order in which the factors are written.

Definition:

Given any integer $n > 1$, the **standard factored form** of *n* is an expression of the form

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k}$$

where k is a positive integer, $p_1, p_2, \ldots, p_k$, are prime numbers and $e_1, e_2, \ldots, e_k$, are positive integers, and

$$p_1 < p_2 < \ \ldots < p_k$$

Quotient Remainder Theorem

The Quotient-Remainder Theorem

Given any integer *n* and positive integer *d*, there exist unique integers *q* and *r* such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

$$\forall n \in \mathbb{Z}\ and\ d \in \mathbb{Z}^+, \exists!\, q, r \in \mathbb{Z}\ s.t\ n = dq + r \text{ and } 0 \leq r < d.$$

N=24, d=4, 24=4(6)+0. d|n n=dk

N=26, d=4, 26=4(6)+2,

Example:

For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.

1) $n = 54, d = 4$

2) $n = -54, d = 4$

3) $n = 54, d = 70$

Example:

For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.

1) $n = 54, d = 4$

$54 = 4(13) + 2$

2) $n = -54, d = 4$

3) $n = 54, d = 70$

Example:

For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.

1) $n = 54, d = 4$

$54 = 4(13) + 2$

$-54 = 4(-13) - 2$

2) $n = -54, d = 4$

3) $n = 54, d = 70$

Example:

For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.

1) $n = 54, d = 4$

$54 = 4(13) + 2$

2) $n = -54, d = 4$

$-54 = 4(-13) - 2$

$= 4(-13) - 4 + 4 - 2$

3) $n = 54, d = 70$

Example:

For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.

1) $n = 54, d = 4$

$54 = 4(13) + 2$

2) $n = -54, d = 4$

$$\begin{aligned} -54 &= 4(-13) - 2 \\ &= 4(-13) - 4 + 4 - 2 \\ &= 4(-14) + 2 \end{aligned}$$

3) $n = 54, d = 70$

Example:

For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.

1) $n = 54, d = 4$

$54 = 4(13) + 2$

2) $n = -54, d = 4$

$-54 = 4(-14) + 2$

3) $n = 54, d = 70$

Example:

For each of the following values of *n* and *d*, find integers *q* and *r* such that $n = dq + r$ and $0 \leq r < d$.

1) $n = 54, d = 4$

$54 = 4(13) + 2$

2) $n = -54, d = 4$

$-54 = 4(-14) + 2$

3) $n = 54, d = 70$

$54 = 70(0) + 54$

Definition:

Given an integer n and a positive integer d,

$\boldsymbol{n}$ **div** $\boldsymbol{d}$ = the integer quotient obtained when n is divided by d, and

$\boldsymbol{n}$ **mod** $\boldsymbol{d}$ = the nonnegative integer remainder obtained when n is divided by d.

Symbolically, if n and d are integers and $d > 0$, then

$$\boldsymbol{n} \textbf{ div } \boldsymbol{d} \boldsymbol{=} \boldsymbol{q} \text{ and } \boldsymbol{n} \textbf{ mod } \boldsymbol{d} = \boldsymbol{r} \iff n = dq + r,$$

where q and r are integers and $0 \leq r < d$.

Example: Computing the Day of the Week

Suppose today is Tuesday, and neither this year nor next year is a leap year. What day of the week will it be 1 year from today?

Solution

There are 365 days in a year that is not a leap year, and each week has 7 days. Now

$$365 \text{ div } 7 = 52 \text{ and } 365 \text{ mod } 7 = 1$$

because 365 = 52 · 7 + 1. Thus 52 weeks, or 364 days, from today will be a Tuesday, and so 365 days from today will be 1 day later, namely Wednesday.

More generally, if $DayT$ is the day of the week today and $DayN$ is the day of the week in N days, then

$$DayN = (DayT\ +\ N) \text{ mod } 7,$$

where Sunday $=\ 0$, Monday $=\ 1, \ldots,$ Saturday $=\ 6$.

Example: Computing the Day of the Week

Suppose today is Tuesday, and neither this year nor next year is a leap year. What day of the week will it be 1 year from today?

Solution

There are 365 days in a year that is not a leap year, and each week has 7 days. Now

$$365 \text{ div } 7 = 52 \text{ and } 365 \text{ mod } 7 = 1$$

because 365 = 52 · 7 + 1. Thus 52 weeks, or 364 days, from today will be a Tuesday, and so 365 days from today will be 1 day later, namely Wednesday.

More generally, if $DayT$ is the day of the week today and $DayN$ is the day of the week in N days, then

$$DayN = (DayT + N) \text{ mod } 7,$$

$(2 + 365) mod\ 7 = 3$

where Sunday $=\ 0$, Monday $=\ 1, \ldots,$ Saturday $=\ 6$.

Example: Suppose m is an integer. If m mod $11 = 6$, what is $4m$ mod 11?

Let

$$m \text{ mod } 11 = 6$$

$$\Longrightarrow \quad m = 11q + 6$$

Then,

$$\begin{aligned} 4m &= 4(11q + 6) = 44q + 24 \\ &= 44q + 22 + 2 \\ &= 11(4q + 2) + 2 \\ &= 11q' + 2 \end{aligned}$$

$$\Longrightarrow \quad 4m \text{ mod } 11 = 2$$

Representations of Integers

By the quotient-remainder theorem (with $d = 2$), there exist unique integers q and r such that

$$n = 2q + r \text{ and } 0 \leq r < 2.$$

But the only integers that satisfy $0 \leq r < 2$ are $r = 0$ and $r = 1$. It follows that given any integer n, there exists an integer q with

$$n = 2q + 0 \text{ or } n = 2q + 1.$$

In the case that $n = 2q + 0 = 2q$, n is even. In the case that $n = 2q + 1$, n is odd. Hence n is either even or odd, and, because of the uniqueness of q and r, n cannot be both even and odd.

The ***parity*** of an integer refers to whether the integer is even or odd. For instance, 5 has odd parity and 28 has even parity. We call the fact that any integer is either even or odd the ***parity property***.

Method of Proof by Division into Cases

To prove a statement of the form

"If A_1 or A_2 or … or A_n, then C,"

prove all of the following:

If A_1, then C,

If A_2, then C,

$\vdots$

If A_n, then C.

This process shows that C is true regardless of which of $A_1, A_2, \ldots, A_n$ happens to be the case.

Theorem: The Parity Property
Any two consecutive integers have opposite parity.

Proof:

Suppose that two [particular but arbitrarily chosen] consecutive integers are given; call them m and $m + 1$. [We must show that one of m and $m + 1$ is even and that the other is odd.] By the parity property, either m is even or m is odd. [We break the proof into two cases depending on whether m is even or odd.]

<u>Case1</u>($\boldsymbol{m}$ is even): In this case, $m = 2k$ for some integer k, and so

$$m + 1 = 2k + 1,$$

which is odd [by definition of odd]. Hence in this case, one of m and $m + 1$ is even and the other is odd.

<u>Case2(</u>$\boldsymbol{m}$ is odd): In this case, $m = 2k + 1$ for some integer k, and so

$$m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1).$$

But $k + 1$ is an integer because it is a sum of two integers. Therefore, $m + 1$ equals twice some integer, and thus $m + 1$ is even. Hence in this case also, one of m and $m + 1$ is even and the other is odd.

It follows that regardless of which case actually occurs for the particular m and $m + 1$ that are chosen, one of m and $m + 1$ is even and the other is odd. [This is what was to be shown.]

Example: Representations of Integers Modulo 4

Show that any integer can be written in one of the four forms

$$n = 4q \text{ or } n = 4q + 1 \text{ or } n = 4q + 2 \text{ or } n = 4q + 3,$$

for some integer q.

Let $d = 4$, then for every integer n, there is a unique r and q such that

$$n = 4q + r \qquad and \qquad 0 \le r < 4$$

Therefore, the only choices for r are 0,1,2 and 3. That is either

$$n = 4q \text{ or } n = 4q + 1 \text{ or } n = 4q + 2 \text{ or } n = 4q + 3,$$

Exercise: Prove that the square of any odd integer has the form $8m + 1$ for some integer m.

[Hint: use modulo 4 representation]

Solution:

Let n be any arbitrary but particular odd integer. As seen previously,

Any integer n is either $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$. for some integer q

Since n is an odd integer, n can only be either $n = 4q + 1$ or $n = 4q + 3$.

Therefore we divide into two cases.

Case 1: (When $\boldsymbol{n = 4q + 1}$)

Then $n^2 = (4q + 1)^2 = 16q^2 + 8q + 1 = 8(2q^2 + q) + 1 = 8m + 1$,

Where $m = 2q^2 + q \in \mathbb{Z}$.

Exercise: Prove that the square of any odd integer has the form $8m + 1$ for some integer m.

[Hint: use modulo 4 representation]

Solution:

Let n be any arbitrary but particular odd integer. As seen previously,

Any integer n is either $n = 4q$ or $n = 4q + 1$ or $n = 4q + 2$ or $n = 4q + 3$.

Since n is an odd integer, n can only be either $n = 4q + 1$ or $n = 4q + 3$.

Therefore we divide into two cases.

Case 2: (When $\boldsymbol{n = 4q + 3}$)

Then $n^2 = (4q + 3)^2 = 16q^2 + 24q + 9 = 8(2q^2 + 3q + 1) + 1$

$= 8m + 1,$

Where $m = 2q^2 + 3q + 1 \in \mathbb{Z}$.