DEFINITION 1

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$. When a divides b we say that ***a*** is a ***factor*** of b and that ***b*** is a ***multiple*** of a. The notation $a|b$ denotes that a divides b. Write $a \nmid b$ when a does not divide b.

EXAMPLE 1.1

Determine if $3|7$

Solution: if $3|7$ then there is an integer c such that $7 = 3c$. Solving for $c = \frac{7}{3}$. However, since 7 is a prime number there can be no integer $c = \frac{7}{3}$ unless the denominator is either 1 or 7. Since $3 \notin \{1,7\}$ there is no integer c and, hence $3 \nmid 7$.

EXAMPLE 1.2

Determine if $3|12$

Solution: if $3|12$ then there is an integer c such that $12 = 3c$. Solving for $c = \frac{12}{3} = 4$. Hence, $3|12$.

EXAMPLE 2

Let n and d be positive integers. How many positive integers not exceeding n are divisible by d?

Solution: The positive integers divisible by d are all the integers of the form dk, where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk \leq n$, or with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

EXAMPLE 2.1

How many positive integers not exceeding $n = 28$ are divisible by 4?

Solution: $k = \left\lfloor \frac{28}{4} \right\rfloor = 7$

THEOREM 1

Let a, b, and c be integers. Then

(i) if $a|b$ and $a|c$ then $a|(b + c)$;
(ii) if $a|b$, then $a|bc$ for all integers c;
(iii) if $a|b$ and $b|c$, then $a|c$.

COROLLARY 1

If a, b, and c are integers such that $a|b$ and $a|c$, then $a|mb + nc$ whenever m and n are integers.

THEOREM 2

THE DIVISION ALGORITHM. Let a be an integer and d a ***positive*** integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

DEFINITION 2

In the equality given in the division algorithm, d is called the *divisor*, a is called the *dividend*, q is called the *quotient*, and r is called the *remainder*. This notation is used to express the quotient and remainder:

$q = a \textbf{ div } d$
$r = a \textbf{ mod } d$

EXAMPLE 3

What are the quotient and remainder when 101 is divided by 11?
Solution: Recall $a = dq + r$ where $a = 101$ and $d = 11$.

$q = a \textbf{ div } d = 101 \textbf{ div } 11 = 9$
$r = a \textbf{ mod } d = 101 \textbf{ mod } 11 = 2$
$a = dq + r = 101 = 11 \cdot 9 + 2$

EXAMPLE 4

What are the quotient and remainder when -11 is divided by 3?
Solution: Recall $a = dq + r$ where $a = -11$ and $d = 3$.

$q = a \textbf{ div } d = -11 \textbf{ div } 3 = -4$
$r = a \textbf{ mod } d = -11 \textbf{ mod } 3 = -11 - (3 \cdot -4) = -11 - (-12) = 1$
$a = dq + r = -11 = 3 \cdot -4 + 1$
Recall $0 \leq r < d = 0 \leq r < 3 \therefore r \neq -2$

DEFINITION 3

If a and b are integers and m is a positive integer, then a is **congruent** to b modulo m if m divides $a - b$. We use the notation $a \equiv b \pmod{m}$ to indicate that a is congruent to b modulo m. If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

THEOREM 3

Let a and b be integers, and m is a positive integer. Then $a \equiv b \pmod{m}$ if and only if a **mod** m = b **mod** m.

EXAMPLE 5.1

Determine whether 17 is congruent to 5 modulo 6.
Solution: $17 \equiv 5 \ (mod\ 6) = 6|(17 - 5) = 6|12.\ 6|12 \Rightarrow 12 = 6c \Rightarrow c = 2$ and, yes $17 \equiv 5 \ (mod\ 6)$.

EXAMPLE 5.2

Determine whether 24 is congruent to 14 modulo 6.
Solution: $24 \equiv 14 \ (mod\ 6) = 6|(24 - 14) = 6|10.\ 6|10 \Rightarrow 10 = 6c \Rightarrow c = \frac{10}{6}$. There is no integer equal to $10/6$. Hence $24 \not\equiv 14 \ (mod\ 6)$

THEOREM 4

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

THEOREM 5

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then $a + c = b + d \pmod{m}$ and $ac = bd \pmod{m}$.

EXAMPLE 6

Show that $18 \equiv 3 \pmod{5}$ given $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$
Solution: By Theorem 5 $a + c = b + d \pmod{m}$ if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$.
Let $a = 7, c = 11, b = 3,$ and $d = 1.$ Then $18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$.

COROLLARY 2 Let m be a positive integer and let a and b be integers. Then

$$(a+b)\mathbf{mod}\, m = ((a\ \mathbf{mod}\ m) + (b\ \mathbf{mod}\ m))\mathbf{mod}\, m$$

and

$$ab\ \mathbf{mod}\ m = \big((a\ \mathbf{mod}\ m)(b\ \mathbf{mod}\ m)\big)\mathbf{mod}\, m.$$

Arithmetic Modulo m

Under construction

Applications of Congruences

EXAMPLE 8 **Pseudorandom Numbers.** Randomly chosen numbers are often needed for computer simulations. Different methods have been devised for generating numbers that have properties of randomly chosen numbers. Because numbers generated by systematic methods are not truly random, they are called **pseudorandom numbers**.

The most commonly used procedure for generating pseudorandom numbers is the **linear congruential method**. We choose four integers: the **modulus** m, the **multiplier** a , the **increment** c, and **seed** x_0, with $2 \le a < m$, and $0 \le x_0 < m$. We generate a sequence of pseudorandom numbers $[x_n]$, with $0 \le x_n < m$ for all n, by successively using the congruence

$$x_{n+1} = (ax_n + c)\mathbf{mod}\, m$$

Cryptology

EXAMPLE 9 What is the secret message produced from the message "MEET YOU IN THE PARK" using the Caesar cipher?

Solution: The Caesar cipher is $f(p) = (p+3)\mathbf{mod}\ 26$ where $0 \le p \le 25$ and capital letters of the English alphabet are replaced by the integers $p|0 \le p \le 25$. For example, the letter A is replaced by 0, the letter B by 1, and so on.

First replace the letters in the message with their corresponding integers.

M	**E**	**E**	**T**	**Y**	**O**	**U**	**I**	**N**	**T**	**H**	**E**	**P**	**A**	**R**	**K**
12	4	4	19	24	14	20	8	13	19	7	4	15	0	17	10

Now replace each of these numbers p by $f(p) = (p+3)\mathbf{mod}\ 26$.

12	4	4	19	24	14	20	8	13	19	7	4	15	0	17	10
15	7	7	22	1	17	23	11	16	22	10	7	18	3	20	13

Now replace the encrypted integers by their corresponding letters.

15	7	7	22	1	17	23	11	16	22	10	7	18	3	20	13
P	H	H	W	B	R	X	L	Q	W	K	H	S	D	U	N

EXAMPLE 10 What letter replaces the letter K when the function $f(p) = (7p + 3) \mathbf{mod}\ 26$ is used for encryption?

Solution: First, note that 10 represents K. Then, using the encryption function specified, it follows that $f(10) = (7 \cdot 10 + 3) \mathbf{mod}\ 26 = 21$. Because 21 represents V, K is replaced by V in the encrypted message.