CHAPTER

4 Number Theory

4.1 Divisibility and Modular Arithmetic

4.5 Applications of Congruences

4.3 Primes and Greatest Common Divisors

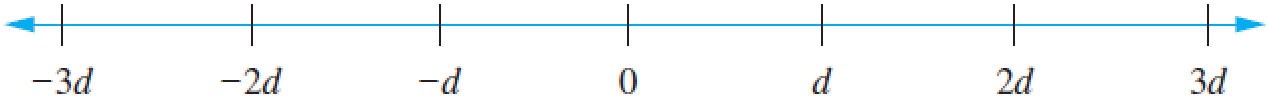
4.2 Integer Representations and Algorithms

Division

4.1 Divisibility and Modular Arithmetic

If a and b are integers with $a \neq 0$, we say that a *divides* b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a *factor* or *divisor* of b, and that b is a *multiple* of a. The notation $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Determine whether $3 \mid 7$ and whether $3 \mid 12$.



Integers Divisible by the Positive Integer d.

THEOREM

Let a, b, and c be integers, where $a \neq 0$. Then

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

COROLLARY

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

4.1 Divisibility and Modular Arithmetic

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

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:

$$q = a \mathbf{\ div\ } d, \quad r = a \mathbf{\ mod\ } d.$$

Division

4.1 Divisibility and Modular Arithmetic

10 ⌊3

r d 3 q=0

10 − 3 1

7 − 3 2

4 − 3 q = 3

r = 1

−10 ⌊3

d = 3 − 1
= 2

−(1+3)
− 4

−9 ⌊3

```
(int, int) division (a, d>0)
{ q=0;
  r=|a|;       0≤r<d
  while(r>=d)
  { r=r-d;
    q=q+1;
  }
  if (a<0) if (r>0)
  { r=d-r;
    q=-(1+q);
  }
  else q=-q;
}
```

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, a **congruence** and that m is its **modulus**.

Then $a \equiv b \pmod{m}$ if and only if a **mod** $m = b$ **mod** m.

there is an integer k such that $a = b + km$.

Determine whether 17 is congruent to 5 modulo 6

Determine whether 24 and 14 are congruent modulo 6.

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

$$a + c \equiv b + d \pmod{m} \qquad \text{and} \qquad ac \equiv bd \pmod{m}.$$

$7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$

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

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

Divide and Conquer

4.5 Applications of Congruences

Hashing Functions

Pseudorandom Numbers

Cryptography

4.5 Applications of Congruences

Hashing Functions

How can memory locations be assigned so that customer records can be retrieved quickly?

A hashing function h assigns memory location $h(k)$ to the record that has k as its key.

Hashing functions should be easily evaluated so that files can be quickly located.

Furthermore, the hashing function should be onto, so that all memory locations are possible.

$$h(k) = k \ \mathbf{mod}\ m$$

Find the memory locations assigned by the hashing function $h(k) = k \ \mathbf{mod}\ 111$ to the records of customers with Social Security numbers 064212848 and 037149212.

Hashing Functions

Because a hashing function is not one-to-one (because there are more possible keys than memory locations), more than one file may be assigned to a memory location. When this happens, we say that a **collision** occurs.

Assign a memory location to the record of the customer with Social Security number 107405723.

One way to resolve a collision is to assign the first free location following the occupied memory location assigned by the hashing function.

Pseudorandom Numbers

$$x_{n+1} = (ax_n + c) \textbf{ mod } m.$$

$m = 2^{15}$
$a = 12351$
$c = 1$
$x = 1000$
C^{++}

Find the sequence of pseudorandom numbers generated by the linear congruential method with modulus $m = 9$, multiplier $a = 7$, increment $c = 4$, and seed $x_0 = 3$.

seed $x_0 = 3$.

$x_1 =$

$x_2 =$

$x_3 =$

$x_4 =$

$x_5 =$

$a = 19$
$x_0 = 0$ (seed)
$c = 1$
$m = 381$

Number theory plays a key role in cryptography, the subject of transforming information so that it cannot be easily recovered without special knowledge. Number theory is the basis of many classical ciphers, first used thousands of years ago, and used extensively until the 20th century.

Caesar's encryption

replace A by 0, K by 10, and Z by 25.

$f(p) = (p + 3) \textbf{ mod } 26.$

"MEET YOU IN THE PARK"

Shift cipher.

$$f(p) = (p + k) \textbf{ mod } 26.$$

$$f^{-1}(p) = (p - k) \textbf{ mod } 26.$$

$f^{-1}(p) = (p - 3) \textbf{ mod } 26.$

"PHHW BRX LQ WKH SDUN"

affine cipher.

$$f(p) = (ap + b) \textbf{ mod } 26,$$

$$\gcd(a, 26) = 1.$$

Caesar cipher

$$f(p) = (p + 3) \mathbf{\ mod\ } 26.$$

$$f^{-1}(p) = (p - 3) \mathbf{\ mod\ } 26.$$

Shift cipher.

$$f(p) = (p + k) \mathbf{\ mod\ } 26.$$

$$f^{-1}(p) = (p - k) \mathbf{\ mod\ } 26.$$

Encrypt the message "STOP GLOBAL WARMING" using the shift cipher with shift $k = 11$.

affine cipher.

$$f(p) = (ap + b) \mathbf{\ mod\ } 26,$$

$$\gcd(a, 26) = 1.$$