CHAPTER

4

Number Theory and Cryptography

4.1 Divisibility and Modular Arithmetic

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 $b = ac$ (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.

EXAMPLE 1 Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution: We see that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3 \mid 12$ because $12/3 = 4$. ◀

THEOREM 1 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 $a \mid c$.

4.1.3 The Division Algorithm

When an integer is divided by a positive integer, there is a quotient and a remainder, as the division algorithm shows.

THEOREM 2 **THE DIVISION ALGORITHM** Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, 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:

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

- d is called the *divisor*.
- a is called the *dividend*.
- q is called the *quotient*.
- r is called the *remainder*.

EXAMPLE 3 What are the quotient and remainder when 101 is divided by 11?

Solution: We have

$$101 = 11 \cdot 9 + 2.$$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \textbf{ div } 11$, and the remainder is $2 = 101 \textbf{ mod } 11$. ◀

EXAMPLE 4 What are the quotient and remainder when -11 is divided by 3?

Solution: We have

$$-11 = 3(-4) + 1.$$

Hence, the quotient when -11 is divided by 3 is $-4 = -11$ **div** 3, and the remainder is $1 = -11$ **mod** 3.

Note that the remainder cannot be negative. Consequently, the remainder is *not* -2, even though

$$-11 = 3(-3) - 2,$$

because $r = -2$ does not satisfy $0 \leq r < 3$. ◀

Remark: A programming language may have one, or possibly two, operators for modular arithmetic, denoted by mod (in BASIC, Maple, Mathematica, EXCEL, and SQL), % (in C, C++, Java, and Python), rem (in Ada and Lisp), or something else. Be careful when using them, because for $a < 0$, some of these operators return $a - m\lceil a/m \rceil$ instead of a **mod** $m = a - m\lfloor a/m \rfloor$ (as shown in Exercise 24). Also, unlike a **mod** m, some of these operators are defined when $m < 0$, and even when $m = 0$.

4.1.4 Modular Arithmetic

Modular Equivalences

Let a, b, and n be any integers and suppose $n > 1$. The following statements are all equivalent:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ for some integer k
4. a and b have the same (nonnegative) remainder when divided by n
5. $a \bmod n = b \bmod n$

THEOREM 5 Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

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

EXAMPLE 6 Because $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, it follows from Theorem 5 that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod{5}$$

and that

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod{5}.$$

Evaluating Congruences

Determine which of the following congruences are true and which are false.

a. $12 \equiv 7 \pmod 5$ b. $6 \equiv -8 \pmod 4$ c. $3 \equiv 3 \pmod 7$

Getting Started with Modular Arithmetic

The most practical use of modular arithmetic is to reduce computations involving large integers to computations involving smaller ones. For instance, note that $55 \equiv 3 \pmod 4$ because $55 - 3 = 52$, which is divisible by 4, and $26 \equiv 2 \pmod 4$ because $26 - 2 = 24$, which is also divisible by 4. Verify the following statements.

a. $55 + 26 \equiv (3 + 2) \pmod 4$ b. $55 - 26 \equiv (3 - 2) \pmod 4$

c. $55 \cdot 26 \equiv (3 \cdot 2) \pmod 4$ d. $55^2 \equiv 3^2 \pmod 4$

Modular Exponentiation

Let a, b, and n be integers with $n > 1$. Then

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod{n},$$

or, equivalently,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

In particular, if m is a positive integer, then

$$a^m \equiv [(a \bmod n)^m] \pmod{n}.$$

$$\boxed{x^7 \bmod n = \{(x^4 \bmod n)(x^2 \bmod n)(x^1 \bmod n)\} \bmod n.}$$

EXAMPLE 7 Find the value of $(19^3 \mathbf{\ mod\ } 31)^4 \mathbf{\ mod\ } 23$.

$$\boxed{(19^3 \mathbf{\ mod\ } 31)^4 \mathbf{\ mod\ } 23 = 2.}$$

Home work

$(19^3 \mathbf{\ mod\ } 31)^4 \mathbf{\ mod\ } 23$,

$19^3 \mathbf{\ mod\ } 31 = 6859 \mathbf{\ mod\ } 31 = 8$.

$8^4 = 4096$. Because $4096 = 178 \cdot 23 + 2$,

$4096 \mathbf{\ mod\ } 23 = 2$.

Hence, $(19^3 \mathbf{\ mod\ } 31)^4 \mathbf{\ mod\ } 23 = 2$.

Computing a^k *mod* n When k Is a Power of 2

Find $144^4 \bmod 713$.

Solution

$$\begin{aligned}
144^4 \bmod 713 &= (144^2)^2 \bmod 713 \\
&= (144^2 \bmod 713)^2 \bmod 713 \\
&= (20736 \bmod 713)^2 \bmod 713 \\
&= 59^2 \bmod 713 \\
&= 3481 \bmod 713 \\
&= 629
\end{aligned}$$

Computing a^k *mod* n When k Is Not a Power of 2

Example: Find 12^{43} *mod* 713.

Solution First write the exponent as a sum of powers of 2:

$$43 = 2^5 + 2^3 + 2 + 1 = 32 + 8 + 2 + 1.$$

Next compute 12^{2^k} for $k = 1, 2, 3, 4, 5$.

$$\begin{aligned}
12 \bmod 713 &= 12 \\
12^2 \bmod 713 &= 144 \\
12^4 \bmod 713 &= 144^2 \bmod 713 = 59 \\
12^8 \bmod 713 &= 59^2 \bmod 713 = 629 \\
12^{16} \bmod 713 &= 629^2 \bmod 713 = 639 \\
12^{32} \bmod 713 &= 639^2 \bmod 713 = 485
\end{aligned}$$

$$\boxed{12^{43} = 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1.}$$

$$\begin{aligned}
&12^{43} \bmod 713 \\
&\quad = \{(12^{32} \bmod 713) \cdot (12^8 \bmod 713) \cdot (12^2 \bmod 713) \cdot (12 \bmod 713)\} \bmod 713.
\end{aligned}$$

By substitution,

$$\begin{aligned}
12^{43} \bmod 713 &= (485 \cdot 629 \cdot 144 \cdot 12) \bmod 713 \\
&= 527152320 \bmod 713 \\
&= 48.
\end{aligned}$$

Computing the **mod** *m* Function of Products and Sums

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

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

4.1.5 Arithmetic Modulo *m*

We can define arithmetic operations on $\mathbf{Z}_m$, the set of nonnegative integers less than m, that is, the set $\{0, 1, \ldots, m-1\}$. In particular, we define addition of these integers, denoted by $+_m$ by

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

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by $\cdot_m$ by

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

The operations $+_m$ and $\cdot_m$ are called addition and multiplication modulo m

EXAMPLE 8 Use the definition of addition and multiplication in $\mathbf{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution:

$$7 +_{11} 9 = (7 + 9) \mathbf{\ mod\ } 11 = 16 \mathbf{\ mod\ } 11 = 5,$$

and

$$7 \cdot_{11} 9 = (7 \cdot 9) \mathbf{\ mod\ } 11 = 63 \mathbf{\ mod\ } 11 = 8.$$

Hence, $7 +_{11} 9 = 5$ and $7 \cdot_{11} 9 = 8$.

Closure If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.

Associativity If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Commutativity If a and b belong to $\mathbf{Z}_m$, then $a +_m b = b +_m a$ and $a \cdot_m b = b \cdot_m a$.

Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. That is, if a belongs to $\mathbf{Z}_m$, then $a +_m 0 = 0 +_m a = a$ and $a \cdot_m 1 = 1 \cdot_m a = a$.

Additive inverses If $a \neq 0$ belongs to $\mathbf{Z}_m$, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is, $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.

Distributivity If a, b, and c belong to $\mathbf{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Properties

4.5 Applications of Congruences

- Hashing Functions
- Pseudorandom Numbers
- Check Digits

4.5.1 Hashing Functions

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

- A common hashing function is $h(k) = k \textbf{ mod } m$, where m is the number of memory locations.
- Because this hashing function is onto, all memory locations are possible.

Example: Let $h(k) = k \textbf{ mod } 111$. This hashing function assigns the records of customers with social security numbers as keys to memory locations in the following manner:

$h(064212848) = 064212848 \textbf{ mod } 111 = 14$

$h(037149212) = 037149212 \textbf{ mod } 111 = 65$

$h(107405723) = 107405723 \textbf{ mod } 111 = 14$, but since location 14 is already occupied, the record is assigned to the next available position, which is 15.

the record is assigned to the next available position, which is 15.

- The hashing function is not one-to-one as there are many more possible keys than memory locations. When more than one record is assigned to the same location, we say a *collision* occurs. Here a collision has been resolved by assigning the record to the first free location.
- For collision resolution, we can use a *linear probing function*:

$$h(k,i) = (h(k) + i) \textbf{ mod } m, \text{ where } i \text{ runs from } 0 \text{ to } m - 1.$$

- There are many other methods of handling with collisions. You may cover these in a later CS course.

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value.

The input to the hash function is of arbitrary length but output is always of fixed length.

4.5.2 Pseudorandom Numbers

Pseudorandom Numbers

- Randomly chosen numbers are needed for many purposes, including computer simulations.
- *Pseudorandom numbers* are not truly random since they are generated by systematic methods.
- The *linear congruential method* is one commonly used procedure for generating pseudorandom numbers.
- Four integers are needed: the *modulus* m, the *multiplier* a, the *increment* c, and *seed* x_0, with $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \leq x_n < m$ for all n, by successively using the recursively defined function

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

- If psudorandom numbers between 0 and 1 are needed, then the generated numbers are divided by the modulus, x_n/m.

Pseudorandom Numbers

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

Solution: Compute the terms of the sequence by successively using the congruence $x_{n+1} = (7x_n + 4)$ **mod** 9, with $x_0 = 3$.

$$x_1 = 7x_0 + 4 \textbf{ mod } 9 = 7\cdot 3 + 4 \textbf{ mod } 9 = 25 \textbf{ mod } 9 = 7,$$
$$x_2 = 7x_1 + 4 \textbf{ mod } 9 = 7\cdot 7 + 4 \textbf{ mod } 9 = 53 \textbf{ mod } 9 = 8,$$
$$x_3 = 7x_2 + 4 \textbf{ mod } 9 = 7\cdot 8 + 4 \textbf{ mod } 9 = 60 \textbf{ mod } 9 = 6,$$
$$x_4 = 7x_3 + 4 \textbf{ mod } 9 = 7\cdot 6 + 4 \textbf{ mod } 9 = 46 \textbf{ mod } 9 = 1,$$
$$x_5 = 7x_4 + 4 \textbf{ mod } 9 = 7\cdot 1 + 4 \textbf{ mod } 9 = 11 \textbf{ mod } 9 = 2,$$
$$x_6 = 7x_5 + 4 \textbf{ mod } 9 = 7\cdot 2 + 4 \textbf{ mod } 9 = 18 \textbf{ mod } 9 = 0,$$
$$x_7 = 7x_6 + 4 \textbf{ mod } 9 = 7\cdot 0 + 4 \textbf{ mod } 9 = 4 \textbf{ mod } 9 = 4,$$
$$x_8 = 7x_7 + 4 \textbf{ mod } 9 = 7\cdot 4 + 4 \textbf{ mod } 9 = 32 \textbf{ mod } 9 = 5,$$
$$x_9 = 7x_8 + 4 \textbf{ mod } 9 = 7\cdot 5 + 4 \textbf{ mod } 9 = 39 \textbf{ mod } 9 = 3.$$

The sequence generated is 3,7,8,6,1,2,0,4,5,3,7,8,6,1,2,0,4,5,3,…

It repeats after generating 9 terms.

4.5.3 Check Digits

- A common method of detecting errors in strings of digits is to add an extra digit at the end, which is evaluated using a function. If the final digit is not correct, then the string is assumed not to be correct.

Example: Retail products are identified by their *Universal Product Codes* (*UPC*s). Usually these have 12 decimal digits, the last one being the check digit. The check digit is determined by the congruence:

$$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}.$$

EXAMPLE 5 a. Suppose that the first 11 digits of the UPC are 79357343104. What is the check digit?

b. Is 041331021641 a valid UPC?

Solution:

a. $3\cdot7 + 9 + 3\cdot3 + 5 + 3\cdot7 + 3 + 3\cdot4 + 3 + 3\cdot1 + 0 + 3\cdot4 + x_{12} \equiv 0 \pmod{10}$

$21 + 9 + 9 + 5 + 21 + 3 + 12 + 3 + 3 + 0 + 12 + x_{12} \equiv 0 \pmod{10}$

$98 + x_{12} \equiv 0 \pmod{10}$

$x_{12} \equiv 0 \pmod{10}$ So, the check digit is 2.

b. $3\cdot0 + 4 + 3\cdot1 + 3 + 3\cdot3 + 1 + 3\cdot0 + 2 + 3\cdot1 + 6 + 3\cdot4 + 1 \equiv 0 \pmod{10}$

$0 + 4 + 3 + 3 + 9 + 1 + 0 + 2 + 3 + 6 + 12 + 1 = 44 \equiv 4 \not\equiv \pmod{10}$

Hence, 041331021641 is not a valid UPC.

Books are identified by an *International Standard Book Number* (ISBN-10), a 10 digit code. The first 9 digits identify the language, the publisher, and the book. The tenth digit is a check digit, which is determined by the following congruence

$$x_{10} \equiv \sum_{i=1}^{9} i x_i \pmod{11}.$$

The validity of an ISBN-10 number can be evaluated with the equivalent $\sum_{i=1}^{10} i x_i \equiv 0 \pmod{11}.$

EXAMPLE 6

a. Suppose that the first 9 digits of the ISBN-10 are 007288008. What is the check digit?

b. Is 084930149X a valid ISBN10?

Solution:

a. $X_{10} \equiv 1\cdot 0 + 2\cdot 0 + 3\cdot 7 + 4\cdot 2 + 5\cdot 8 + 6\cdot 8 + 7\cdot 0 + 8\cdot 0 + 9\cdot 8 \pmod{11}.$

$X_{10} \equiv 0 + 0 + 21 + 8 + 40 + 48 + 0 + 0 + 72 \pmod{11}.$

$X_{10} \equiv 189 \equiv 2 \pmod{11}$. Hence, $X_{10} = 2$.

b. $1\cdot 0 + 2\cdot 8 + 3\cdot 4 + 4\cdot 9 + 5\cdot 3 + 6\cdot 0 + 7\cdot 1 + 8\cdot 4 + 9\cdot 9 + 10\cdot 10 =$

$0 + 16 + 12 + 36 + 15 + 0 + 7 + 32 + 81 + 100 = 299 \equiv 2 \not\equiv 0 \pmod{11}$

Hence, 084930149X is not a valid ISBN-10.

X is used for the digit 10.