Unit 2
Integers and Matrices

2.1 Integers

- An integer is a whole number (not a fractional number) that can be positive, negative, or zero.
- The set of integers, denoted **Z**, is formally defined as follows:

  Z = {..., -3, -2, -1, 0, 1, 2, 3, ...}

EXAMPLE 1: -5, 1, 5, 8, 97, etc. are integers.

EXAMPLE 2: -1.43, 1 3/4, 3.14, .09, etc. are not integers.

Division

- Division of an integer by a positive integer produces a quotient and a remainder.
- When one integer is divided by a second nonzero integer, the quotient may or may not be an integer.
- If a and b are integers with a ≠ 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 | b denotes that a divides b.
- We write a ∤ b when a does not divide b.
- We can express a | b using quantifiers as ∃c(ac = b), where the universe of discourse is the set of integers.

EXAMPLE: Determine whether 3 | 7 and whether 3 | 12.

Solution: We see that 3 ∤ 7, because 7/3 is not an integer. On the other hand, 3 | 12 because 12/3 = 4.

THEOREM 1

Let a, b, and c be integers, where a ≠ 0. 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, where a ≠ 0, such that a | b and a | c, then a | mb + nc whenever m and n are integers.

The Division Algorithm

- When an integer is divided by a positive integer, there is a quotient and a remainder.
- Let a be an integer and d a positive integer. Then there are unique integers q and r, with 0 ≤ 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:

$$q = a \text{ div } d, \qquad r = a \text{ mod } d.$$

- Note that both a div d and a mod d for a fixed d are functions on the set of integers.
- Furthermore, when a is an integer and d is a positive integer, we have a div d = $\lfloor a/d \rfloor$ and a mod d = a − d.

<u>THEOREM 2</u>: 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.

EXAMPLE 1: 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 div 11, and the remainder is 2 = 101 mod 11.

EXAMPLE 2: 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 $0 \le r < 3$.

Modular Arithmetic

- In some situations we care only about the remainder of an integer when it is divided by some specified positive integer.

Congruence

- *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 ≡ b (mod m) to indicate that a is congruent to b modulo m.*
- *We say that a ≡ b (mod m) is a* ***congruence*** *and that m is its* ***modulus*** *(plural* ***moduli****).*
- *If a and b are not congruent modulo m, we write a ≢ b (mod m).*

EXAMPLE: Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6.

Solution: Because 6 divides 17 − 5 = 12, we see that 17 ≡ 5 (mod 6). However, because 24 − 14 = 10 is not divisible by 6, we see that 24 ≢ 14 (mod 6).

THEOREM 3

Let a and b be integers, and let m be a positive integer. Then a ≡ b (mod m) if and only if a mod m = b mod m.

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.

Proof:

- If a ≡ b (mod m), by the definition of congruence, we know that m | (a − b).
- This means that there is an integer k such that a − b = km, so that a = b + km.
- Conversely, if there is an integer k such that a = b + km, then km = a − b.
- Hence, m divides a − b, so that a ≡ b (mod m).

Congruence Class

The set of all integers congruent to an integer a modulo m is called the *congruence class* of a modulo m.

THEOREM 5

Let m be a positive integer. If a ≡ b (mod m) and c ≡ d (mod m), then

$$a + c \equiv b + d \pmod{m} \text{ and}$$

$$ac \equiv bd \pmod{m}.$$

Proof:

- We use a direct proof.

- Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by Theorem 2(Division Algorithm) there are integers s and t with $b = a + sm$ and $d = c + tm$.
- Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

- Hence,

$$a + c \equiv b + d \pmod{m} \text{ and}$$

$$ac \equiv bd \pmod{m}.$$

EXAMPLE: Let $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$, then

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

and that

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

COROLLARY 2

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

$$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$$

and

$$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m.$$

Arithmetic Modulo m

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

$$a +_m b = (a + b) \bmod m,$$

- 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

$$a \cdot_m b = (a \cdot b) \bmod m,$$

- where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers.

- The operations $+_m$ and $\cdot_m$ are called *addition* and *multiplication* modulo m and when we use these operations, we are said to be doing *arithmetic modulo* m.

EXAMPLE: Use the definition of addition and multiplication in Z_m to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution:

- Using the definition of addition modulo 11, we find that

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

and

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

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

Properties of Operation

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition and multiplication of integers. In particular, they satisfy these properties:

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 $a = 0$ 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 $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Representations of Integers

- In everyday life we use decimal notation to express integers. For example, 965 is used to denote $9 \cdot 10^2 + 6 \cdot 10 + 5$.
- However, it is often convenient to use bases other than 10.
- In particular, computers usually use binary notation (with 2 as the base) when carrying out arithmetic, and octal (base 8) or hexadecimal (base 16) notation when expressing characters, such as letters or digits.
- In fact, we can use any integer greater than 1 as the base when expressing integers.

THEOREM

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0,$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

EXAMPLE: $(245)_8$ represents $2 \cdot 8^2 + 4 \cdot 8 + 5 = 165$.

Algorithms for Integer Operations

- The algorithms for performing operations with integers using their binary expansions are extremely important in computer arithmetic.
- Throughout this discussion, suppose that the binary expansions of a and b are

$$a = (a_{n-1}a_{n-2} \ldots a_1a_0)_2$$

$$b = (b_{n-1}b_{n-2} \ldots b_1b_0)_2$$

Addition Algorithm

```
Add(a, b)        //a and b are positive integers
{
        $a = (a_{n-1}a_{n-2} \ldots a_1a_0)_2$;
        $b = (b_{n-1}b_{n-2} \ldots b_1b_0)_2$;
        $c = 0$;
        for j = 0 to n-1
        {
                $d = \lfloor (a_j + b_j + c)/2 \rfloor$;
                $s_j = a_j + b_j + c - 2d$;
                $c = d$;
        }
        $s_n = c$;
        return $(s_0s_1 \ldots s_n)$;
}
```

EXAMPLE: Add $a = (1110)_2$ and $b = (1011)_2$.

Solution:

$a = (1110)_2$

$b = (1011)_2$.

$c_0 = 0$

Iteration 1(j = 0):

$d = 0$

$s_0 = 1$

$c = 0$

Iteration 2(j = 1):

$d = 1$

$s_1 = 0$

$c = 1$

Iteration 3(j = 2):

$d = 1$

$s_2 = 0$

$c = 1$

Iteration 4(j = 3):

$d = 1$

$s_3 = 1$

$c = 1$

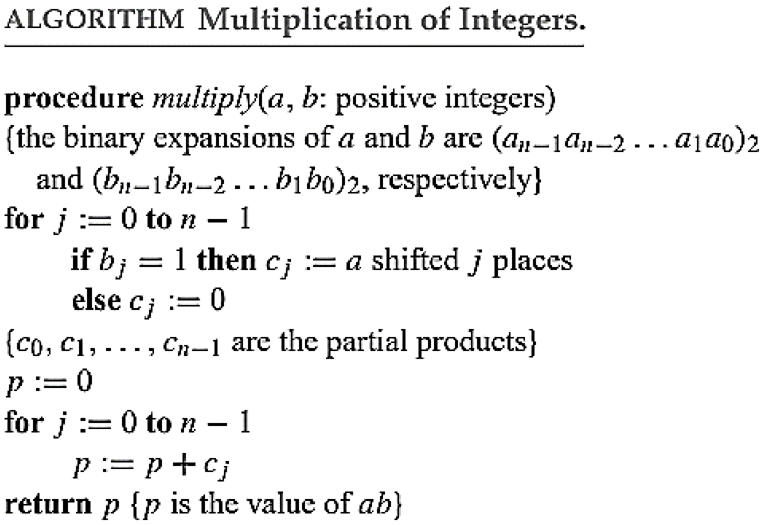
$s_4 = 1$

Hence, $a+b = s_4s_3s_2s_1s_0 = 11001$

Multiplication Algorithm

- Consider the multiplication of two n-bit integers a and b.
- The conventional algorithm (used when multiplying with pencil and paper) works as follows.
- Using the distributive law, we see that

$$\begin{aligned} ab &= a(b_0 2^0 + b_1 2^1 +\cdots+ b_{n-1}2^{n-1}) \\ &= a(b_0 2^0) + a(b_1 2^1) +\cdots+ a(b_{n-1}2^{n-1}). \end{aligned}$$



ALGORITHM Multiplication of Integers.

```
procedure multiply($a$, $b$: positive integers)
{the binary expansions of $a$ and $b$ are $(a_{n-1}a_{n-2} \ldots a_1a_0)_2$
   and $(b_{n-1}b_{n-2} \ldots b_1b_0)_2$, respectively}
for $j := 0$ to $n - 1$
      if $b_j = 1$ then $c_j := a$ shifted $j$ places
      else $c_j := 0$
{$c_0, c_1, \ldots, c_{n-1}$ are the partial products}
$p := 0$
for $j := 0$ to $n - 1$
      $p := p + c_j$
return $p$ {$p$ is the value of $ab$}
```

EXAMPLE: Find the product of a = $(110)_2$ and b = $(101)_2$.

Solution:

a = $(110)_2$

b = $(101)_2$

Iteration 1 (j = 0):

$b_0 = 1$ $c_0 = 110$

Iteration 2 (j = 1):

$b_1 = 0$ $c_1 = 0$

Iteration 1 (j = 0):

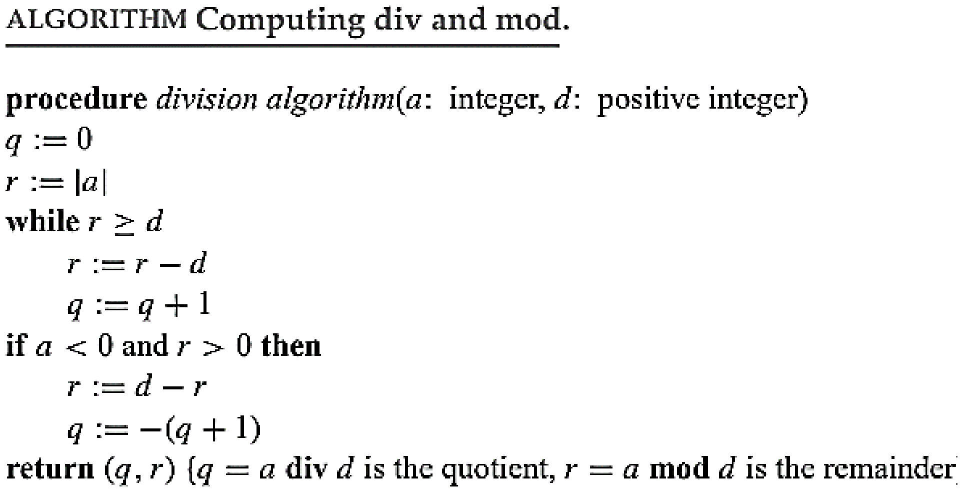
$b_2 = 1$ $c_2 = 11000$

Now,

p = 110+0+11000 = 11110

So, ab = 11110

Algorithm for div and mod



ALGORITHM Computing div and mod.

```
procedure division algorithm($a$: integer, $d$: positive integer)
$q := 0$
$r := |a|$
while $r \geq d$
    $r := r - d$
    $q := q + 1$
if $a < 0$ and $r > 0$ then
    $r := d - r$
    $q := -(q + 1)$
return $(q, r)$ {$q = a$ div $d$ is the quotient, $r = a$ mod $d$ is the remainder
```

Primes and Greatest Common Divisors

Primes

- *An integer p greater than 1 is called prime if the only positive factors of p are 1 and p.*
- *A positive integer that is greater than 1 and is not prime is called composite.*
- The integer n is composite if and only if there exists an integer a such that a | n and $1<a<n$.

EXAMPLE: The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

THEOREM 1: The Fundamental Theorem of Arithmetic

Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.

EXAMPLE: The prime factorizations of 100, 641, 999, and 1024 are given by

$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$,

$641 = 641$,

$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$,

$1024 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^{10}$.

THEOREM 2

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

Proof:

- If n is composite, by the definition of a composite integer, we know that it has a factor a with $1 < a < n$.

- Hence, by definition of a factor of a positive integer, we have n = ab, where b is a positive integer greater than 1.
- We will show that a ≤ $\sqrt{n}$ or b ≤ $\sqrt{n}$.
- If a > $\sqrt{n}$ and b > $\sqrt{n}$, then ab > $\sqrt{n}$. $\sqrt{n}$ = n, which is a contradiction.
- Consequently, a ≤ $\sqrt{n}$ or b ≤ $\sqrt{n}$.
- Because both a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$.
- This divisor is either prime or, by the fundamental theorem of arithmetic, has a prime divisor less than itself.
- In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

Mersenne Primes

The prime of the form $2^p - 1$ is called Mersenne primes, where p is also prime.

EXAMPLE: The numbers $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ and $2^7 - 1 = 127$ are Mersenne primes, while $2^{11} - 1 = 2047$ is not a Mersenne prime because 2047 = 23 · 89.

Greatest Common Divisors

- The largest integer that divides both of two integers is called the greatest common divisor of these integers.
- Let a and b be integers, not both zero. The largest integer d such that d | a and d | b is called the greatest common divisor of a and b. The greatest common divisor of a and b is denoted by gcd(a, b).

EXAMPLE: What is the greatest common divisor of 24 and 36?

Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12. Hence, gcd(24, 36) = 12.

EXAMPLE: What is the greatest common divisor of 17 and 22?

Solution: The integers 17 and 22 have no positive common divisors other than 1, so that gcd(17, 22) = 1.

Relatively Prime

The integers a and b are relatively prime if their greatest common divisor is 1.

EXAMPLE: The integers 17 and 22 are relatively prime, because gcd(17, 22) = 1.

Pairwise Relatively Prime

The integers $a_1, a_2, ..., a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

EXAMPLE: Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Solution:

- Because gcd(10, 17) = 1, gcd(10, 21) = 1, and gcd(17, 21) = 1, we conclude that 10, 17, and 21 are pairwise relatively prime.
- Because gcd(10, 24) = 2 > 1, we see that 10, 19, and 24 are not pairwise relatively prime.

Least Common Multiple

- The least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b.
- The least common multiple of a and b is denoted by lcm(a, b).

EXAMPLE: What is the least common multiple of 50 and 60?

Solution: We have

$$\text{lcm}(50,60) = 300$$

THEOREM

Let a and b be positive integers. Then ab = gcd(a, b) · lcm(a, b).

LEMMA 1

Let a = bq + r, where a, b, q, and r are integers. Then gcd(a, b) = gcd(b, r).

Proof:

- If we can show that the common divisors of a and b are the same as the common divisors of b and r, we will have shown that gcd(a, b) = gcd(b, r), because both pairs must have the same greatest common divisor.
- So suppose that d divides both a and b. Then it follows that d also divides a − bq = r.
- Hence, any common divisor of a and b is also a common divisor of b and r.
- Likewise, suppose that d divides both b and r.
- Then d also divides bq + r = a.
- Hence, any common divisor of b and r is also a common divisor of a and b.
- Consequently, gcd(a, b) = gcd(b, r).

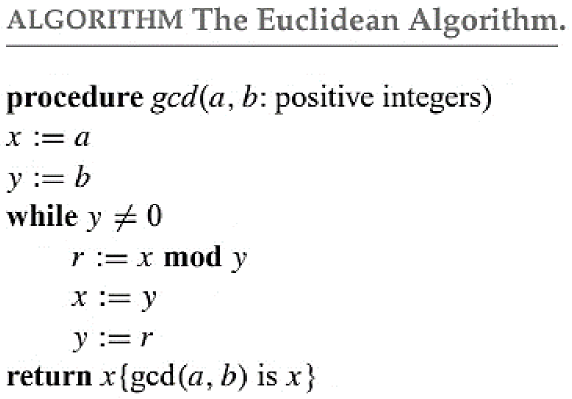
The Euclidean Algorithm

- Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient.
- The reason is that it is time-consuming to find prime factorizations.

- There is a more efficient method of finding the greatest common divisor, called the Euclidean algorithm.
- Suppose that a and b are positive integers with $a \geq b$.
- Let $r_0 = a$ and $r_1 = b$.
- When we successively apply the division algorithm, we obtain

$$
\begin{array}{ll}
r_0 = r_1q_1 + r_2 & 0 \leq r_2 < r_1, \\
r_1 = r_2q_2 + r_3 & 0 \leq r_3 < r_2, \\
\dots & \\
\dots & \\
r_{n-2} = r_{n-1}q_{n-1} + r_n & 0 \leq r_n < r_{n-1}, \\
r_{n-1} = r_nq_n. &
\end{array}
$$

- Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms.
- Furthermore, it follows from Lemma 1 that $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n$.
- Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.



ALGORITHM The Euclidean Algorithm.

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
    r := x mod y
    x := y
    y := r
return x{gcd(a, b) is x}
```

EXAMPLE: Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution:

x = 662

y = 414

Iteration 1:

r = 662 mod 414 = 248

x = 414

y = 248

Iteration 2:

r = 414 mod 248 = 166

x = 248

y = 166

Iteration 3:

r = 248 mod 166 = 82

x = 166

y = 82

Iteration 4:

r = 166 mod 82 = 2

x = 82

y = 2

Iteration 5:

r = 82 mod 2 = 0

x = 2

y = 0

Hence gcd(662,414)=2

gcds as Linear Combinations

- The greatest common divisor of two integers a and b can be expressed in the form sa+tb, where s and t are integers.
- In other words, gcd(a, b) can be expressed as a linear combination with integer coefficients of a and b.
- For example, gcd(6, 14) = 2, and 2 = (−2) · 6 + 1 · 14.

THEOREM 6: BÉZOUT'S THEOREM

If a and b are positive integers, then there exist integers s and t such that gcd(a, b) = sa + tb.

Extended Euclidean Algorithm

- The *extended Euclidean algorithm* can be used to express gcd(a, b) as a linear combination with integer coefficients of the integers a and b.

- We set $s_0 = 1, s_1 = 0$, $t_0 = 0$, and $t_1 = 1$ and let $s_j = s_{j-2} - q_{j-1}s_{j-1}$ and $t_j = t_{j-2} - q_{j-1}t_{j-1}$ for j = 2, 3,...,n, where the q_j are the quotients in the divisions used when the Euclidean algorithm finds gcd(a, b).

Algorithm:

```
procedure extended Euclidean(a, b : positive integers)
$x := a$
$y := b$
$oldolds := 1$
$olds := 0$
$oldoldt := 0$
$oldt := 1$
while $y \neq 0$
        $q := x$ div $y$
        $r := x$ mod $y$
        $x := y$
        $y := r$
        $s := oldolds - q \cdot olds$
        $t := oldoldt - q \cdot oldt$
        $oldolds := olds$
        $oldoldt := oldt$
        $olds := s$
        $oldt := t$
{ gcd$(a, b)$ is $x$, and the Bézout coefficients are given by $(oldolds)a + (oldoldt)b = x$ }
```

EXAMPLE: Express gcd(161, 28) as a linear combination of 161 and 28.

Solution:

q	x	y	r	oldolds	olds	s	oldoldt	oldt	t
5	161	28	21	**1**	**0**	1	**0**	**1**	-5
1	28	21	7	0	1	-1	1	-5	6
3	21	7	0	1	-1	4	-5	6	-23
	7	0		-1	4		**6**	-23	

Therefore, gcd(161, 28) = 7 and s = -1 and t = 6.

Exercise

1. Express gcd(252, 198) = 18 as a linear combination of 252 and 198.
2. Use the extended Euclidean algorithm to express gcd(26, 91) as a linear combination of 26 and 91.

Linear Congruencies

- A congruence of the form $ax \equiv b \ (mod\ m)$, where m is a positive integer, a and b are integers, and x is a variable, is called a *linear congruence*.

Solution of Linear Congruencies

- How can we solve the linear congruence $ax \equiv b \ (mod\ m)$, that is, how can we find all integers x that satisfy this congruence?
- One method that we will describe uses an integer $\bar{a}$ such that $\bar{a}a \equiv 1 \ (mod\ m)$, if such an integer exists. Such an integer $\bar{a}$ is said to be an inverse of $a\ modulo\ m$.
- Theorem 1 guarantees that an inverse of $a\ modulo\ m$ exists whenever a and m are relatively prime.
- Once we have an inverse $\bar{a}$ of $a\ modulo\ m$, we can solve the congruence $ax \equiv b \ (mod\ m)$ by multiplying both sides of the linear congruence by $\bar{a}$.

THEOREM 1

If a and m are relatively prime integers and $m > 1$, then an inverse of $a\ modulo\ m$ exists. Furthermore, this inverse is unique $modulo\ m$. (That is, there is a unique positive integer $\bar{a}$ less than m that is an inverse of $a\ modulo\ m$ and every other inverse of $a\ modulo\ m$ is congruent to $\bar{a}\ modulo\ m$.)

Proof:

- By BÉZOUT'S THEOREM, because $gcd(a, m) = 1$, there are integers s and t such that

$$sa + tm = 1.$$

- This implies that

$$sa + tm \equiv 1 \ (mod\ m).$$

- Because $tm \equiv 0 \ (mod\ m)$, it follows that $sa \equiv 1 \ (mod\ m)$.
- Consequently, s is an inverse of $a\ modulo\ m$.

EXAMPLE 1: Find an inverse of 3 $modulo$ 7 by first finding Bézout coefficients of 3 and 7.

Solution:

- Because $gcd(3, 7) = 1$, Theorem 1 tells us that an inverse of 3 $modulo$ 7 exists.
- The Euclidean algorithm ends quickly when used to find the greatest common divisor of 3 and 7:

$$7 = 2 \cdot 3 + 1.$$

- From this equation we see that

$$-2 \cdot 3 + 1 \cdot 7 = 1.$$

- This shows that -2 and 1 are Bézout coefficients of 3 and 7.
- We see that -2 is an inverse of 3 $modulo$ 7.
- Note that every integer congruent to -2 modulo 7 is also an inverse of 3, such as $5, -9, 12$, and so on.

EXAMPLE 2: Find an inverse of 101 $modulo$ 4620.

Solution:

- First, we use the Euclidean algorithm to show that $gcd(101, 4620) = 1$.
- Then we will reverse the steps to find Bézout coefficients a and b such that $101a + 4620b = 1$.
- It will then follow that a is an inverse of 101 $modulo$ 4620.
- The steps used by the Euclidean algorithm to find $gcd(101, 4620)$ are

$$\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1.
\end{aligned}$$

- Because the last nonzero remainder is 1, we know that gcd(101, 4620) = 1.
- We can now find the Bézout coefficients for 101 and 4620 by working backwards through these steps, expressing gcd(101, 4620) = 1 in terms of each successive pair of remainders.
- In each step we eliminate the remainder by expressing it as a linear combination of the divisor and the dividend.
- We obtain

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (23 - 7 \cdot 3) = -1 \cdot 23 + 8 \cdot 3 \\
&= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) = 8 \cdot 26 - 9 \cdot 23 \\
&= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) = -9 \cdot 75 + 26 \cdot 26 \\
&= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) = 26 \cdot 101 - 35 \cdot 75 \\
&= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) = -35 \cdot 4620 + 1601 \cdot 101.
\end{aligned}$$

- That $-35 \cdot 4620 + 1601 \cdot 101 = 1$ tells us that –35 and 1601 are Bézout coefficients of 4620 and 101, and 1601 is an inverse of 101 modulo 4620.

EXAMPLE 3: What are the solutions of the linear congruence $3x \equiv 4 \pmod{7}$?

Solution:

- By Example 1 we know that −2 is an inverse of 3 modulo 7.
- Multiplying both sides of the congruence by −2 shows that

$$-2 \cdot 3x \equiv -2 \cdot 4 \ (mod\ 7)$$

$$x \equiv -8 \ (mod\ 7)$$

- Because $-6 \equiv 1 \pmod{7}$ and $-8 \equiv 6 \pmod{7}$, it follows that if x is a solution, then $x \equiv -8 \equiv 6 (\text{mod } 7)$.
- We need to determine whether every x with $x \equiv 6 \pmod{7}$ is a solution.
- We conclude that the solutions to the congruence are the integers x such that $x \equiv 6(\text{mod}7)$, namely, 6, 13, 20,... and −1, −8, −15,....

Exercise

1. Solve the congruence $4x \equiv 5 \pmod{9}$ using the inverse of 4 modulo 9.
2. Solve the congruence $2x \equiv 7 \pmod{17}$ using the inverse of 2 modulo 7.
3. Solve each of these congruences using the modular inverses
   a. $19x \equiv 4 \pmod{141}$
   b. $55x \equiv 34 \pmod{89}$
   c. $89x \equiv 2 \pmod{232}$
4. Solve each of these congruences using the modular inverses.
   a. $34x \equiv 77 \pmod{89}$
   b. $144x \equiv 4 \pmod{233}$
   c. $200x \equiv 13 \pmod{1001}$

The Chinese Remainder Theorem

The Chinese remainder theorem, named after the Chinese heritage of problems involving systems of linear congruences, states that when the moduli of a system of linear congruences are pairwise relatively prime, there is a unique solution of the system modulo the product of the moduli.

THEOREM 2: THE CHINESE REMAINDER THEOREM

Let $m_1, m_2,...,m_n$ be pairwise relatively prime positive integers greater than one and $a_1, a_2,...,a_n$ arbitrary integers. Then the system

$x \equiv a_1 \pmod{m_1}$,

$x \equiv a_2 \pmod{m_2}$,

$$\cdots$$

$$x \equiv a_n \pmod{m_n}$$

has a unique solution modulo $m = m_1m_2 \cdots m_n$. (That is, there is a solution x with $0 \le x < m$, and all other solutions are congruent modulo to this solution.)

Proof:

- To establish this theorem, we need to show that a solution exists and that it is unique modulo m. Here we will only show that a solution exists by describing a way to construct this solution.
- To construct a simultaneous solution, first let

$$M_k = m/m_k \qquad \text{for } k = 1, 2,...,n$$

- That is, M_k is the product of the moduli except for m_k.
- Because m_i and m_k have no common factors greater than 1 when $i \neq k$, it follows that $\gcd(m_k, M_k) = 1$.
- Consequently, by Theorem 1, we know that there is an integer y_k, an inverse of M_k modulo m_k, such that

$$M_ky_k \equiv 1 \pmod{m_k}$$

- To construct a simultaneous solution, form the sum

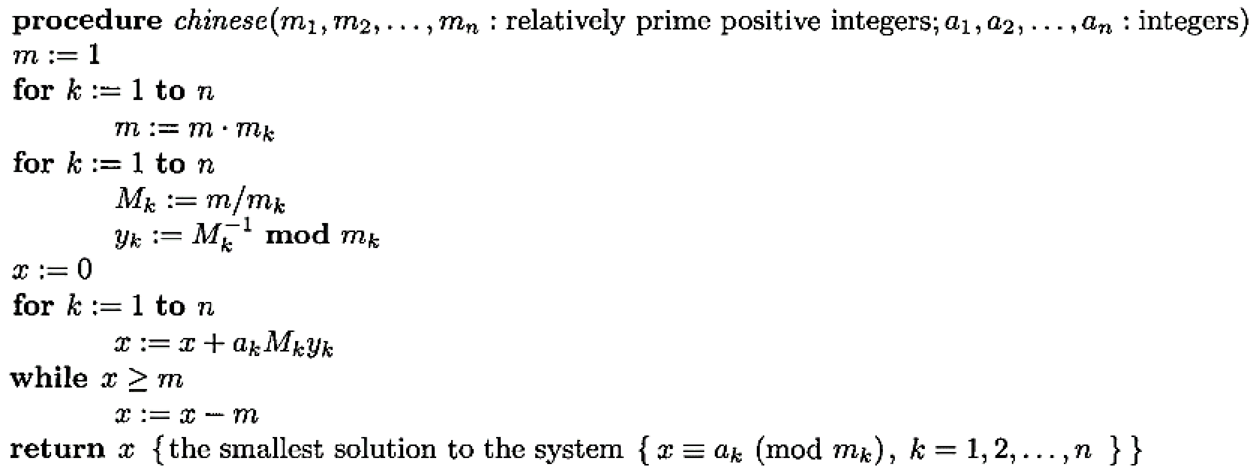
$$x = a_1M_1y_1 + a_2M_2y_2 +\cdots+ a_nM_ny_n$$

- We will now show that x is a simultaneous solution.
- First, note that because $M_j \equiv 0 \pmod{m_k}$ whenever $j \neq k$, all terms except the kth term in this sum are congruent to 0 modulo m_k.
- Because $M_ky_k \equiv 1 \pmod{m_k}$ we see that

$$x \equiv a_kM_ky_k \equiv a_k \pmod{m_k}, \qquad \text{for } k = 1, 2,...,n.$$

- We have shown that x is a simultaneous solution to the n congruences.

Algorithm:



```
procedure chinese($m_1, m_2, \ldots, m_n$ : relatively prime positive integers; $a_1, a_2, \ldots, a_n$ : integers)
$m := 1$
for $k := 1$ to $n$
        $m := m \cdot m_k$
for $k := 1$ to $n$
        $M_k := m/m_k$
        $y_k := M_k^{-1}$ mod $m_k$
$x := 0$
for $k := 1$ to $n$
        $x := x + a_k M_k y_k$
while $x \geq m$
        $x := x - m$
return $x$ {the smallest solution to the system $\{ x \equiv a_k \pmod{m_k},\ k = 1, 2, \ldots, n \}$}
```

EXAMPLE: Solve the following system of congruences using Chinese Remainder Theorem.

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Solution: To solve the system of congruences,

first let,

$m = 3 \cdot 5 \cdot 7 = 105$,

$M_1 = m/3 = 35$,

$M_2 = m/5 = 21$, and

$M_3 = m/7 = 15$.

We see that

2 is an inverse of $M_1 = 35$ modulo 3, because $35 \cdot 2 \equiv 1 \pmod 3$

1 is an inverse of $M_2 = 21$ modulo 5, because $21 \cdot 1 \equiv 1 \pmod 5$ and

1 is an inverse of $M_3 = 15 \pmod 7$, because $15 \cdot 1 \equiv 1 \pmod 7$.

The solutions to this system are those x such that

$x \equiv a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$

Exercise

1. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$, and $x \equiv 3 \pmod 5$.

2. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, and $x \equiv 4 \pmod{11}$.

Computer Arithmetic with Large Integers

- Suppose that $m_1, m_2,...,m_n$ are pairwise relatively prime moduli and let m be their product.
- By the Chinese remainder theorem, we can show that an integer a with $0 \le a < m$ can be uniquely represented by the n-tuple consisting of its remainders upon division by m_i, i = 1, 2,...,n.
- That is, we can uniquely represent a by

$$(a \bmod m_1, a \bmod m_2,...,a \bmod m_n)$$

- To perform arithmetic with large integers, we select moduli $m_1, m_2,...,m_n$, where each m_i is an integer greater than 2, $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, and $m = m_1m_2 \cdots m_n$ is greater than the results of the arithmetic operations we want to carry out.
- Once we have selected our moduli, we carry out arithmetic operations with large integers by performing component wise operations on the n-tuples representing these integers using their remainders upon division by m_i, i = 1, 2,...,n.
- Once we have computed the value of each component in the result, we recover its value by solving a system of n congruences modulo m_i, i = 1, 2,...,n.
- This method of performing arithmetic with large integers has several valuable features.
- First, it can be used to perform arithmetic with integers larger than can ordinarily be carried out on a computer.
- Second, computations with respect to the different moduli can be done in parallel, speeding up the arithmetic.

Algorithm:

Let a and b are two numbers in which we need to perform arithmetic operation.

1. Select moduli $m_1, m_2,...,m_n$, where each m_i is an integer greater than 2, $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, and $m = m_1m_2 \cdots m_n$ is greater than the results of the arithmetic operations we want to carry out20.
2. Represent the given numbers into n-tuple remainder form.
   $a = (a \bmod m_1, a \bmod m_2, ...a \bmod m_n)$
   $b = (b \bmod m_1, b \bmod m_2, ...b \bmod m_n)$
   In general,
   $a \bmod m_i = a_i$ and $b \bmod m_i = b_i$
3. Apply the arithmetic operator
   $a + b = (a_1 + b_1, a_2 + b_2, ...a_n + b_n)$
   $ab = (a_1.b_1, a_2.b_2, ...a_n.b_n)$
   Let c be the result, then n-tuple of c is
   $(c_1 \bmod m_1, c_2 \bmod m_2, ..., c_n \bmod m_n)$

where, $c_i = a_i + b_i$ for a + b and $c_i = a_i.b_i$ for ab

4. Now, applying the Chinese Remainder Theorem

   $x \equiv c_1 \pmod{m_1}$
   $x \equiv c_2 \pmod{m_2}$
   ………
   ………
   $x \equiv c_n \pmod{m_n}$

5. Solve the above conguences and get the result as

   $x = \sum_{i=1}^{n} c_i M_i M_i^{-1} \ mod\ m$

EXAMPLE: Find the sum of 15 and 27 using modulo operation.

Solution:

Let us take $m_1 = 2$, $m_2 = 3$, $m_3 = 5$ and $m_4 = 7$

a =15 = (15 mod 2, 15 mod 3, 15 mod 5, 15 mod 7) = (1, 0, 0, 1)

b = 27 = (27 mod 2, 27 mod 3, 27 mod 5, 27 mod 7) = (1, 0, 2, 6)

c = 15 + 27 = (1, 0, 0, 1) + (1, 0, 2, 6) = (2, 0, 2, 7)

Now, (2 mod 2, 0 mod 3, 2 mod 5, 7 mod 7) = (0, 0, 2, 0)

Then, $x \equiv 0 \pmod{2}$

$x \equiv 0 \pmod{3}$

$x \equiv 2 \pmod{5}$

$x \equiv 0 \pmod{7}$

To solve above system of congruences, we find

m = 2.3.5.7 = 210

$M_1 = 210/2 = 105$ $M_2 = 210/3 = 70$ $M_3 = 210/5 = 42$ $M_4 = 210/7 = 30$

Again,

$105.\ M_1^{-1} \equiv 1 \pmod{2}$ $M_1^{-1} = 1$

$70.\ M_2^{-1} \equiv 1 \pmod{3}$ $M_2^{-1} = 1$

$42.\ M_3^{-1} \equiv 1 \pmod{5}$ $M_3^{-1} = 3$

$30.\ M_4^{-1} \equiv 1 \pmod{7}$ $M_4^{-1} = 4$

So, the sum of 15 and 27 is:

$$\sum_{i=1}^{4} c_i M_i M_i^{-1} \ mod\ m = 2.3.42\ mod\ 210 = 252\ mod\ 210 = 52$$

EXAMPLE 2: Find sum of numbers 123,684 and 413,456 by representing the numbers as 4-tuple by using reminders modulo of pair-wise relatively prime numbers less than 100.

Solution:

Let us take $m_1 = 99$, $m_2 = 98$, $m_3 = 97$ and $m_4 = 95$

a =123,684 = (123,684 mod 99, 123,684 mod 98, 123,684 mod 97, 123,684 mod 95)

= (33, 8, 9, 89)

b = 413,456 = (413,456 mod 99, 413,456 mod 98, 413,456 mod 97, 413,456 mod 95)

= (32, 92, 42, 16)

Now,

a+ b = (33, 8, 9, 89) + (32, 92, 42, 16)

= (65 mod 99, 100 mod 98, 51 mod 97, 105 mod 95) = (65, 2, 51, 10).

To find the sum, that is, the integer represented by (65, 2, 51, 10), we need to solve the system of congruences

$x \equiv 65 \pmod{99}$,

$x \equiv 2 \pmod{98}$,

$x \equiv 51 \pmod{97}$,

$x \equiv 10 \pmod{95}$.

After solving, 537,140 is the unique nonnegative solution of this system less than 89,403,930. Consequently, 537,140 is the sum.

2.2 Matrices

- Matrices are used to express relationships between elements in sets.
- For instance, matrices will be used in models of communications networks and transportation systems.
- Many algorithms will be developed that use these matrix models.

Matrix

- A matrix is a rectangular array of numbers.
- A matrix with m rows and n columns is called an *m × n matrix*.
- The plural of matrix is matrices.
- A matrix with the same number of rows as columns is called *square*.
- Two matrices are *equal* if they have the same number of rows and the same number of columns and the corresponding entries in every position are equal.
- Let m and n be positive integers and let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

- The (i, j)th *element* or *entry* of **A** is the element a_{ij} , that is, the number in the ith row and jth column of **A**.
- A convenient shorthand notation for expressing the matrix **A** is to write **A** = $[a_{ij}]$, which indicates that **A** is the matrix with its (i, j)th element equal to a_{ij}.

EXAMPLE: The matrix $\begin{bmatrix} 1 & 1 \\ 0 & 2 \\ 1 & 3 \end{bmatrix}$ is a 3 × 2 matrix.

Matrix Arithmetic

Matrix Addition

- Let A = $[a_{ij}]$ and B = $[b_{ij}]$ be m × n matrices.
- The sum of A and B, denoted by A + B, is the m × n matrix that has $a_{ij} + b_{ij}$ as its (i, j)th element.
- In other words, A + B = $[a_{ij} + b_{ij}]$.
- The sum of two matrices of the same size is obtained by adding elements in the corresponding positions.
- Matrices of different sizes cannot be added, because the sum of two matrices is defined only when both matrices have the same number of rows and the same number of columns.

EXAMPLE:

$$\begin{bmatrix} 1 & 0 & -1 \\ 2 & 2 & -3 \\ 3 & 4 & 0 \end{bmatrix} + \begin{bmatrix} 3 & 4 & -1 \\ 1 & -3 & 0 \\ -1 & 1 & 2 \end{bmatrix} = \begin{bmatrix} 4 & 4 & -2 \\ 3 & -1 & -3 \\ 2 & 5 & 2 \end{bmatrix}.$$

Product of Matrix

- Let A be an m × k matrix and B be a k × n matrix.
- The product of A and B, denoted by AB, is the m × n matrix with its (i, j)th entry equal to the sum of the products of the corresponding elements from the ith row of A and the jth column of B.
- In other words, if AB = $[c_{ij}]$, then

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj}.$$

- The product of two matrices is not defined when the number of columns in the first matrix and the number of rows in the second matrix are not the same.
- Matrix multiplication is not commutative.

- That is, if A and B are two matrices, it is not necessarily true that AB and BA are the same.

EXAMPLE: Let

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 4 \\ 2 & 1 & 1 \\ 3 & 1 & 0 \\ 0 & 2 & 2 \end{bmatrix} \quad \text{and} \quad \mathbf{B} = \begin{bmatrix} 2 & 4 \\ 1 & 1 \\ 3 & 0 \end{bmatrix}.$$

Find AB if it is defined.

Solution: Because A is a 4 × 3 matrix and B is a 3 × 2 matrix, the product AB is defined and is a 4 × 2 matrix.

$$\mathbf{AB} = \begin{bmatrix} 14 & 4 \\ 8 & 9 \\ 7 & 13 \\ 8 & 2 \end{bmatrix}.$$

Transposes of Matrices

- Let A = [a_{ij}] be an m × n matrix. The transpose of A, denoted by A^t , is the n × m matrix obtained by interchanging the rows and columns of A.
- In other words, if A^t = [b_{ij}], then $b_{ij} = a_{ji}$ for i = 1, 2,...,n and j = 1, 2,...,m.

EXAMPLE: The transpose of the matrix $\begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ is the matrix $\begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$.

Symmetric Matrix

- A square matrix A is called symmetric if A = A^t .
- Thus A = [a_{ij}] is symmetric if $a_{ij} = a_{ji}$ for all i and j with 1 ≤ i ≤ n and 1 ≤ j ≤ n.
- Note that a matrix is symmetric if and only if it is square and it is symmetric with respect to its main diagonal.

EXAMPLE: The matrix $\begin{bmatrix} 2 & \mathbf{4} & \mathbf{1} \\ \mathbf{4} & 5 & \mathbf{7} \\ \mathbf{1} & \mathbf{7} & 8 \end{bmatrix}$ is symmetric.

Identity Matrix

- The *identity matrix* of order n is the n × n matrix $I_n = [\delta_{ij}]$, where $\delta_{ij} = 1$ if i = j and $\delta_{ij} = 0$ if i ≠ j.
- Hence

$$I = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

- Multiplying a matrix by an appropriately sized identity matrix does not change this matrix. In other words, when A is an m × n matrix, we have

$$\mathbf{AI}_n = \mathbf{I}_n\mathbf{A} = \mathbf{A}.$$

Powers of Matrix

Powers of square matrices can be defined. When A is an n × n matrix, we have

$$\mathbf{A}^0 = \mathbf{I}_n, \qquad \mathbf{A}^r = \underbrace{\mathbf{AAA}\cdots\mathbf{A}}_{r\ \text{times}}.$$

Zero–One Matrices

- A matrix all of whose entries are either 0 or 1 is called a zero–one matrix.
- Zero–one matrices are often used to represent discrete structures.
- Algorithms using these structures are based on Boolean arithmetic with zero–one matrices.
- This arithmetic is based on the Boolean operations ∧ and ∨, which operate on pairs of bits, defined by

$$b_1 \wedge b_2 = \begin{cases} 1 & \text{if } b_1 = b_2 = 1 \\ 0 & \text{otherwise,} \end{cases}$$

$$b_1 \vee b_2 = \begin{cases} 1 & \text{if } b_1 = 1 \text{ or } b_2 = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Join and Meet of Matrices

- Let A = $[a_{ij}]$ and B = $[b_{ij}]$ be m × n zero–one matrices.
- Then the **join** of A and B is the zero–one matrix with (i, j)th entry $a_{ij} \vee b_{ij}$.
- The join of A and B is denoted by A ∨ B.
- The **meet** of A and B is the zero–one matrix with (i, j)th entry $a_{ij} \wedge b_{ij}$.
- The meet of A and B is denoted by A ∧ B.

EXAMPLE: Find the join and meet of the zero–one matrices

$$\mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \end{bmatrix}.$$

Solution: We find that the join of A and B is

$$\mathbf{A} \vee \mathbf{B} = \begin{bmatrix} 1 \vee 0 & 0 \vee 1 & 1 \vee 0 \\ 0 \vee 1 & 1 \vee 1 & 0 \vee 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

The meet of A and B is

$$\mathbf{A} \wedge \mathbf{B} = \begin{bmatrix} 1 \wedge 0 & 0 \wedge 1 & 1 \wedge 0 \\ 0 \wedge 1 & 1 \wedge 1 & 0 \wedge 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Boolean Product of Two Matrices

- Let A = [a_{ij}] be an m × k zero–one matrix and B = [b_{ij}] be a k × n zero–one matrix.
- Then the Boolean product of A and B, denoted by A ⊙ B, is the m × n matrix with (i, j)th entry c_{ij} where

$$c_{ij} = (a_{i1} \wedge b_{1j}) \vee (a_{i2} \wedge b_{2j}) \vee \cdots \vee (a_{ik} \wedge b_{kj}).$$

- Note that the Boolean product of A and B is obtained in an analogous way to the ordinary product of these matrices, but with addition replaced with the operation ∨ and with multiplication replaced with the operation ∧.

EXAMPLE: Find the Boolean product of A and B, where

$$\mathbf{A} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}, \qquad \mathbf{B} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}.$$

Solution: The Boolean product A ⊙ B is given by

$$\mathbf{A} \odot \mathbf{B} = \begin{bmatrix} (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \\ (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (0 \wedge 1) \end{bmatrix}$$

$$= \begin{bmatrix} 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \\ 0 \vee 0 & 0 \vee 1 & 0 \vee 1 \\ 1 \vee 0 & 1 \vee 0 & 0 \vee 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}.$$

Boolean Power

- Let A be a square zero–one matrix and let r be a positive integer.
- The rth Boolean power of A is the Boolean product of r factors of A.

- The r^th^ Boolean product of A is denoted by $A^{[r]}$.
- Hence

$$\mathbf{A}^{[r]} = \underbrace{\mathbf{A} \odot \mathbf{A} \odot \mathbf{A} \odot \cdots \odot \mathbf{A}}_{r \text{ times}}.$$

- We also define $A^{[0]}$ to be I_n.

EXAMPLE: Let $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$. Find $A^{[n]}$ for all positive integers n.

Solution: We find that

$$\mathbf{A}^{[2]} = \mathbf{A} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}.$$

We also find that

$$\mathbf{A}^{[3]} = \mathbf{A}^{[2]} \odot \mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}, \qquad \mathbf{A}^{[4]} = \mathbf{A}^{[3]} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

Additional computation shows that

$$\mathbf{A}^{[5]} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}.$$

and so on.

Assignment #2

Use above exercise as assignment.