Ch 14 (C) Number bases

14.2 The binary system

> 🗣️ The binary system is based upon powers of 2.

Converting binary → decimal

▼ Convert 110101_2 to decimal.

$$\begin{aligned} 110101_2 &= 1(2^5)+1(2^4)+0(2^3)+0(2^1)+1(2^0) \\ &= 1(32)+1(16)+0(8)+1(4)+0(2)+1(1) \\ &= 32+16+4+1 = 53_{10} \end{aligned}$$

Converting decimal → binary

2^0	1	2^4	16	2^8	256
2^1	2	2^5	32	2^9	512
2^2	4	2^6	64	2^{10}	1024
2^3	8	2^7	128		

▼ Convert 83_{10} to binary

Solution 1

$$\begin{aligned} 83 &= 64+19 \\ 19 &= 16+3 \\ 83 &= 64+16+2+1 \\ &= 2^6+2^4+2^1+2^0 \\ &= 1(2^6)+0(2^5)+1(2^4)+0(2^3)+0(2^2)+1(2^1)+1(2^0) \\ &= 1010011_2 \end{aligned}$$

Solution 2

$$\begin{aligned} 83 \div 2 &= 41 \text{ r } 1 \quad & 1 \\ 41 \div 2 &= 20 \text{ r } 1 \quad & 1 \\ 20 \div 2 &= 10 \text{ r } 0 \quad & 0 \\ 10 \div 2 &= 5 \text{ r } 0 \quad & 0 \\ 5 \div 2 &= 2 \text{ r } 1 \quad & 1 \\ 2 \div 2 &= 1 \text{ r } 0 \quad & 0 \\ 1 \div 2 &= 0 \text{ r } 1 \quad & 1 \end{aligned}$$

Working from bottom to top $\Rightarrow 1010011_2$

Octal system

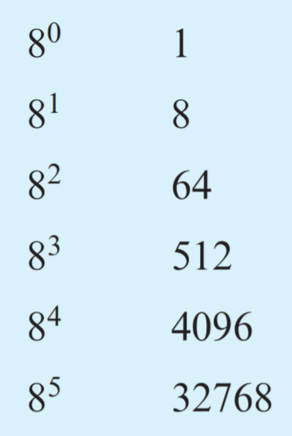
> 🗣️ The octal system is based upon powers of 8.

Converting octal → decimal

▼ Convert 325_8 to decimal

$$\begin{aligned} 325_8 &= 3(8^2)+2(8^1)+5(8^0) \\ &= 3(64)+2(8)+5(1) \\ &= 192+16+5 \\ &= 213_{10} \end{aligned}$$

Converting decimal → octal



8^0	1
8^1	8
8^2	64
8^3	512
8^4	4096
8^5	32768

▼ Convert 1001 to octal.

Solution 1

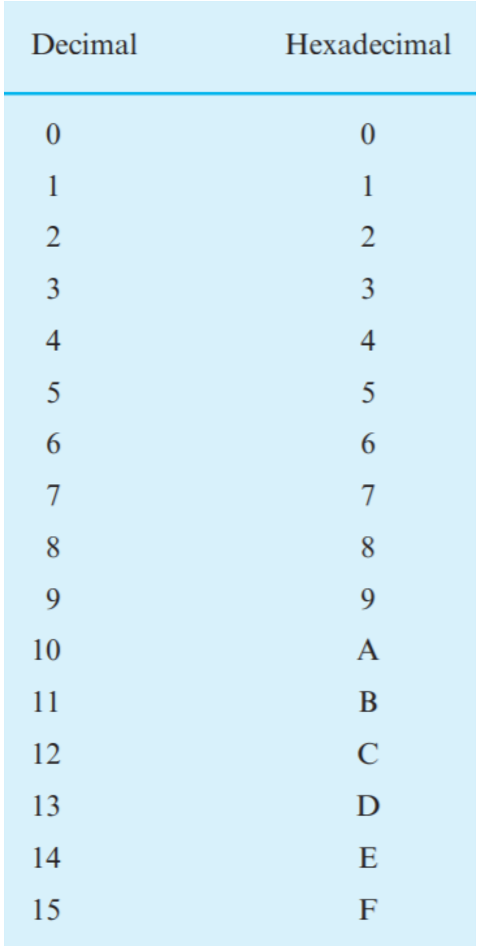
$$1001 = 512 + 489$$
$$489 = 7(64) + 41$$
$$41 = 5(8) + 1$$
$$1001 = 1(8^3) + 7(8^2) + 5(8^1) + 1(8^0) = 1751_8$$

Solution 2

$$\begin{array}{rl} 1001 \div 8 = 125 \text{ r } 1 & 1 \\ 125 \div 8 = 15 \text{ r } 5 & 5 \\ 15 \div 8 = 1 \text{ r } 7 & 7 \\ 1 \div 8 = 0 \text{ r } 1 & 1 \end{array}$$

Working from bottom to top $\Rightarrow 1751_8$.

14.4 Hexadecimal system



Decimal	Hexadecimal
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
10	A
11	B
12	C
13	D
14	E
15	F

Converting hexadecimal → decimal

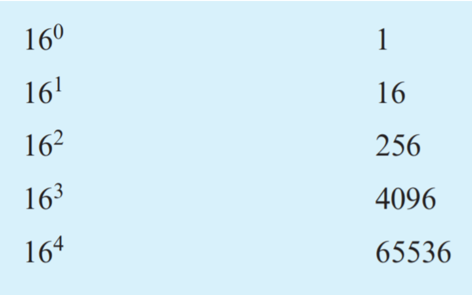
▼ Convert $93A_{16}$ to decimal

$$\begin{aligned} 93A_{16} &= 9(16^2) + 3(16^1) + A(16^0) \\ &= 9(256) + 3(16) + 10(1) \\ &= 2362_{10} \end{aligned}$$

Converting decimal → hexadecimal

▼ Convert 14397_{10} to hexadecimal

$$14397 = 3(4096) + 2109$$
$$2109 = 8(256) + 61$$
$$61 = 3(16) + 13$$
$$14397 = 3(16^3) + 8(16^2)3(16^1) + 13$$
$$14397_{10} = 383D_{16}$$



16^0	1
16^1	16
16^2	256
16^3	4096
16^4	65536

Ch 4.2 Integer Representations and Algorithms (R)

*Basically everything in Topic 1 Number bases with a little extra/advanced stuff.

*Skip everything I already knew

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 $a_k \neq 0$.

Conversion Between Binary, Octal, and Hexadecimal Expansions

▼ Example 7

Find the octal and hexadecimal expansions of $(11\ 1110\ 1011\ 1100)_2$ and the binary expansions of $(765)_8$ and $(A8D)_{16}$.

Solution:

To convert binary into octal notation, we group the binary digits into blocks of three, adding initial zeros at the start of the leftmost block if necessary.

$(11\ 1110\ 1011\ 1100)_2 \ \Rightarrow\ 011\ 111\ 010\ 111\ 100\ \Rightarrow 3\ 7\ 2\ 7\ 4$

Therefore, $(11\ 1110\ 1011\ 1100)_2 = (37274)_8$

To convert binary into hexadecimal notation, we group the binary digits into blocks of four, adding initial zeros at the start of the leftmost block if necessary.

$(11\ 1110\ 1011\ 1100)_2 \ \Rightarrow\ 0011\ 1110\ 1011\ 1100\ \Rightarrow\ 3\ E\ B\ C$

Therefore, $(11\ 1110\ 1011\ 1100)_2 = (3EBC)_{16}$

To convert octal into binary notation, we replace each octal digit by a block of three binary digits.

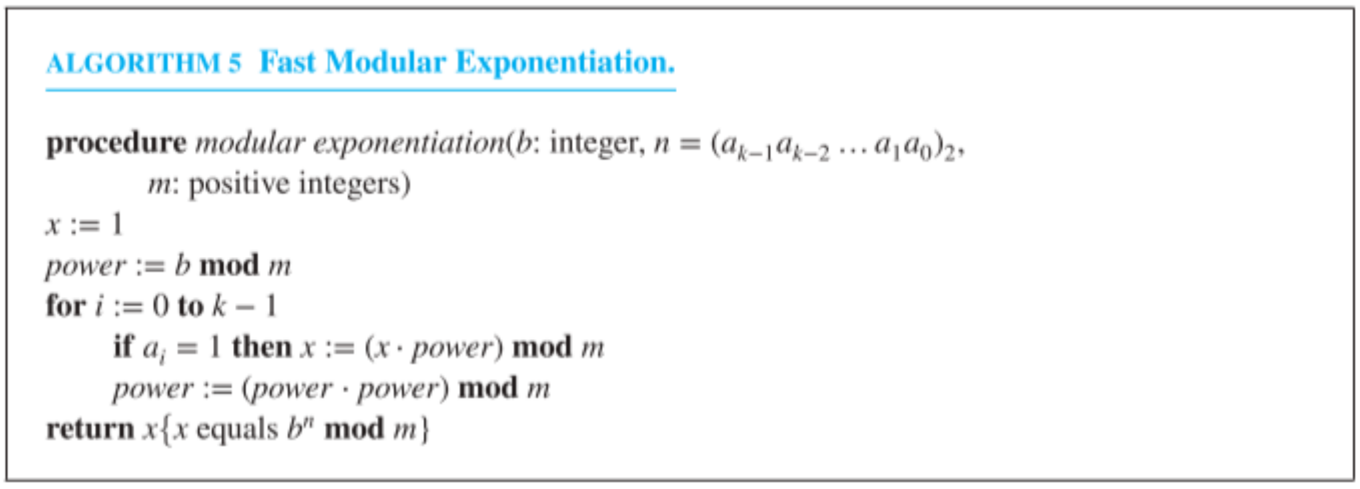
$(765)_8 \ \Rightarrow\ 111\ 110\ 101$

Therefore, $(765)_8 = (1\ 1111\ 0101)_2$

To convert hexadecimal into binary notation, we replace each hexadecimal digit by a block of four binary digits.

$(A8D)_{16} \ \Rightarrow\ 1010\ 1000\ 1101$

Therefore, $(A8D)_{16} = (1010\ 1000\ 1101)_2$.



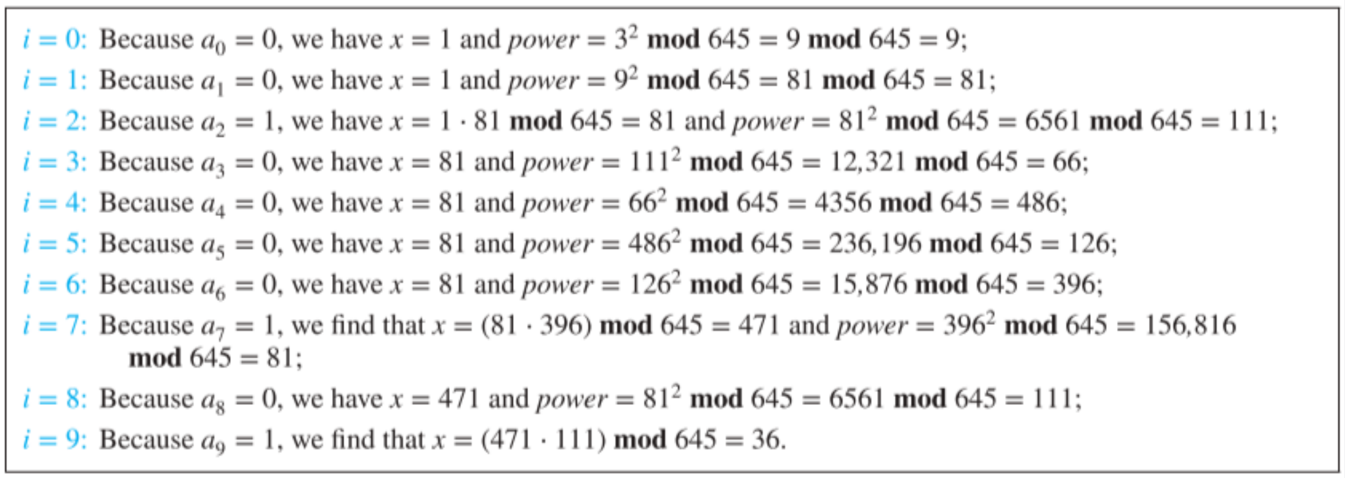
ALGORITHM 5 Fast Modular Exponentiation.

```
procedure modular exponentiation($b$: integer, $n = (a_{k-1}a_{k-2} \ldots a_1a_0)_2$,
        $m$: positive integers)
$x := 1$
$power := b$ mod $m$
for $i := 0$ to $k - 1$
    if $a_i = 1$ then $x := (x \cdot power)$ mod $m$
    $power := (power \cdot power)$ mod $m$
return $x$ {$x$ equals $b^n$ mod $m$}
```

▼ Example 12 Use Algorithm 5 to find 3^{644} **mod** 645.

Solution:

Algorithm 5 initially sets $x = 1$ and *power* = 3 **mod** 645 $= 3$. In the computation of 3^{644} **mod** 645, this algorithm determines 3^{2^j} **mod** 645 for $j = 1, 2, \ldots, 9$ by successively squaring and reducing modulo 645. If $a_j = 1$ (where a_j is the bit in the jth position in the binary expansion of 644), which is $(1010000100)_2$, it multiplies the current value of x by 3^{2^j} **mod** 645 and reduces the result modulo 645. Here are the steps used:



$i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2 \textbf{ mod } 645 = 9 \textbf{ mod } 645 = 9$;

$i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2 \textbf{ mod } 645 = 81 \textbf{ mod } 645 = 81$;

$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81 \textbf{ mod } 645 = 81$ and $power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$;

$i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2 \textbf{ mod } 645 = 12{,}321 \textbf{ mod } 645 = 66$;

$i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2 \textbf{ mod } 645 = 4356 \textbf{ mod } 645 = 486$;

$i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2 \textbf{ mod } 645 = 236{,}196 \textbf{ mod } 645 = 126$;

$i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2 \textbf{ mod } 645 = 15{,}876 \textbf{ mod } 645 = 396$;

$i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396) \textbf{ mod } 645 = 471$ and $power = 396^2 \textbf{ mod } 645 = 156{,}816 \textbf{ mod } 645 = 81$;

$i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2 \textbf{ mod } 645 = 6561 \textbf{ mod } 645 = 111$;

$i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111) \textbf{ mod } 645 = 36$.

Ch12 Sequences and series (C)

12.1 Sequences

- **sequence**: a set of numbers written down in a specific order
- **term**: each number in the sequence

12.2 Arithmetic progressions

$\rightarrow$ forming a sequence by adding a fixed amount to the previous term

> 🗣️ An arithmetic progression can be written $a, a+d, a+2d, a+3d \ldots a$ is the **first term**, d is the **common difference**.

> 💡 The nth term of an arithmetic progression is given by $a+(n-1)d$.

12.3 Geometric progressions

$\rightarrow$ forming a sequence by multiplying a fixed amount to the previous term

> 🗣️ An geometric progression can be written $a, ar, ar^2, ar^3 \ldots a$ is the **first term**, r is the **common ratio**.

> 💡 The nth term of an geometric progression is given by ar^{n-1}.

12.4 Infinite sequences

- **limit**: for $x_k,\ k=1,2,3,\ldots$ As k gets larger and larger, and approaches infinity, the terms of the sequence get closer and closer to zero. "As k tends to infinity, the **limit** of the sequences is zero." $\lim\limits_{k\to\infty}\frac{1}{k}=0$
- **converge**: when a sequence possesses a limit (meaning have a limit)
- **diverge**: the opposite of *converge* (increase indefinitely as more of its terms are added)

12.5 Series and sigma notation

- **series**: result of a sequence added, **sum.**

12.6 Arithmetic series

> 💡 The sum of the first n terms of an arithmetic series with first term a and common difference d is denoted by S_n and given by $\boxed{S_n=\frac{n}{2}(2a+(n-1)d)}$.

12.7 Geometric series

> 💡 The sum of the first n terms of an geometric series with first term a and common ratio r is denoted by S_n and given by $\boxed{S_n=\frac{a(1-r^n)}{1-r}}$ provided r is not equal to 1.

12.8 Infinite geometric series

> 💡 The sum of an infinite number of terms of a geometric series is denoted by S_∞ and is given by $\boxed{S_\infty=\frac{a}{1-r}}$ provided $-1<r<1$.

Ch 1.2.1 Theory of Divisibility (Y)

Let a and b be integers with $a \neq 0$. We say a divides b, denoted by $a \mid b$, if there exists an integer c such that $b = ac$. When a divides b, we say that a is a *divisor* (or *factor*) of b, and b is a *multiple* of a. If a does not divide b, we write $a \nmid b$. If $a \mid b$ and $0 < a < b$, then a is called a *proper divisor* of b.

- $a \mid b \rightarrow b$ is divisible by a.
- $a^\alpha \parallel b$ is sometimes used to indicate that $a^\alpha \mid b$ but $a^{\alpha+1} \nmid b$.

▼ Example

The integer 200 has the following positive divisors: $1, 2, 4, 5, 8, 10, 20, 25, 40, 50, 100, 200$.

Thus, for example, we can write $8 \mid 200,\ 50 \mid 200,\ 7 \nmid 200,\ 35 \nmid 200$.

A divisor of n is called a *trivial divisor* of n if it is either 1 or n itself. A divisor of n is called a *nontrivial divisor* if it is a divisor of n, but is neither 1, nor n.

▼ Example

For the integer 18, 1 and 18 are the trivial divisors, whereas 2, 3, 6, 9 are the nontrivial divisors. The integer 191 has only two trivial divisors and does not have any nontrivial divisors.

Theorem Let a, b, c be integers. Then
1. if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
2. if $a \mid b$, then $a \mid bc$, for any integer c.
3. if $a \mid b$ and $b \mid c$, then $a \mid c$.

Theorem (Division algorithm) For any integer a and any positive integer b, there exist unique integers q and r such that $a = bw + r,\ 0 \leq r < b$.

- a is called *dividend*, q the *quotient*, and r the *remainder*.

Consider the following equation $a = 2q + r,\ a, q, r \in \mathbb{Z},\ 0 \leq r < q$.
Then if $r = 0$, then a is *even*, whereas if $r = 1$, then a is *odd*.

A positive integer n greater than 1 is called *prime* if it only divisors are n and 1. A positive integer n that is greater than 1 and is not prime is called *composite*.

Theorem (Euclid) There are infinitely many primes.

Theorem If n is an integer ≥ 1, then there is a prime p such that $n < p \leq n! + 1$.

Theorem Given any real number $x \geq 1$, there exists a prime between x and $2x$.

If n is an integer ≥ 2, then there are no primes between $n! + 2$ and $n! + n$.

If n is a composite, then n has a prime divisor p such that $p \leq \sqrt{n}$.

Algorithm (The Sieve of Eratosthenes)

Given a positive integer $n > 1$, this algorithm will find all prime numbers up to n.

1. Create a list of integers from 2 to n.
2. For prime numbers p_i $(i = 1, 2, \dots)$ from 2, 3, 5 up to $\lfloor \sqrt{n} \rfloor$, delete all the multiples $p_i < p_i m \leq n$ from the list.
3. Print the integers remaining in the list.

Ch 1.6 Theory of Congruences (Y)

1.6.1 Basic Concepts and Properties of Congruences

Let a be an integer and n a positive integer greater than 1. We define "$a \mod n$" to be the remainder r when a is divided by n, that is
$r = a \mod n = a - \lfloor a/n \rfloor n.$

- We may also say that "r is equal to a reduced modulo n".

Let a be an integer and n a positive integer. We say that "a is *congruent* to b modulo n", denoted by $a \equiv b \pmod n$

- if n is a divisor of $a - b$, or equivalently, if $n \mid (a - b)$. Similarly, we write $a \not\equiv b \pmod n$ if a is not congruent (or incongruent) to b modulo n, or equivalently, if $n \nmid (a - b)$. Clearly, for $a \equiv b \pmod n$ (resp. $a \not\equiv b \pmod n$), we can write $a = kn - b$ (resp. $a \neq kn - b$) for some integer k. The integer n is called the *modulas*.
- $$\begin{aligned} a \equiv b \pmod n &\iff n \mid (a-b) \\ &\iff a = kn + b,\ k \in \mathbb{Z} \\ a \not\equiv b \pmod n &\iff n \nmid (a-b) \\ &\iff a \neq kn + b,\ k \in \mathbb{Z} \end{aligned}$$

Theorem Let n be a positive integer. Then the congruence modulo n is
1. *reflexive*: $a \equiv a \pmod n,\ \forall a \in \mathbb{Z}$;
2. *symmetric*: if $a \equiv b \pmod n$, then $b \equiv a \pmod n,\ \forall a, b \in \mathbb{Z}$;
3. *transitive*: if $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n,\ \forall a, b, c \in \mathbb{Z}$.

- $a \mid b$ is *reflexive*, and *transitive* but not *symmetric*. if $a \mid b$ and $b \mid a$ then $a = b$, so it's not an *equivalence relation*.

If $x \equiv a \pmod n$, then a is called a *residue* of x modulo n. The *residue class* of a modulo n, denoted by $[a]_n$ (or just $[a]$ if no confusion caused), is the set of all those integers that are congruent to a modulo n.

- Writing $a \in [b]_n$ is the same as writing $a \equiv b \pmod n$.

▼ Example: Name the sets of modulo 5.

There are five residue classes:

$$\begin{aligned} [0]_5 &= \{\dots, -15, -10, -5, 0, 5, 10, 15, 20, \dots\} \\ [1]_5 &= \{\dots, -14, -9, -4, 1, 6, 11, 16, 21, \dots\} \\ [2]_5 &= \{\dots, -13, -8, -3, 2, 7, 12, 17, 22, \dots\} \\ [3]_5 &= \{\dots, -12, -7, -2, 3, 8, 13, 18, 23, \dots\} \\ [4]_5 &= \{\dots, -11, -6, 1, 4, 9, 14, 19, 24, \dots\} \end{aligned}$$

▼ Example: In congruence modulo 5, we have...

$$\begin{aligned} [9]_5 &= \{9 + 5k : k \in \mathbb{Z}\} = \{9, 9 \pm 5, 9 \pm 10, 9 \pm 15, \dots\} \\ &= \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\} \end{aligned}$$

We also have

$$\begin{aligned} [4]_5 &= \{4 + 5k : k \in \mathbb{Z}\} = \{4, 4 \pm 5, 4 \pm 10, 4 \pm 15, \dots\} \\ &= \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\} \end{aligned}$$

So, clearly, $[4]_9 = [9]_5$.

If $x \equiv a \pmod n$ and $0 \leq a \leq n - 1$, then a is called the *least (nonnegative) residue* of x modulo n.

1.6.2 Modular Arithmetic

Theorem For all $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
1. $a \pm b \equiv c \pm d \pmod{n}$,
2. $a \cdot b \equiv c \cdot d \pmod{n}$,
3. $a^m \equiv b^m \pmod{n},\ \forall m \in \mathbb{N}$

Theorem For all $a, b, c, d \in \mathbb{Z}$ and $n \in \mathbb{Z}_{>1}$, if $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
1. $[a \pm b]_n = [c \pm d]_n$,
2. $[a \cdot b]_n = [c \cdot d]_n$,
3. $[a^m]_n = [b^m]_n,\ \forall m \in \mathbb{N}$

- $$\begin{aligned}[a]_n + [b]_n &= [a+b]_n \\ [a]_n - [b]_n &= [a-b]_n \\ [a]_n \cdot [b]_n &= [a \cdot b]_n\end{aligned}$$

▼ Example: Let $n = 12$, then

$$[7]_{12} +_{12} [8]_{12} = [7+8]_{12} = [15]_{12} = [3]_{12},$$
$$[7]_{12} -_{12} [8]_{12} = [7-8]_{12} = [-1]_{12} = [11]_{12},$$
$$[7]_{12} \cdot_{12} [8]_{12} = [7 \cdot 8]_{12} - [56]_{12} = [8]_{12}.$$

$$\hookrightarrow 7 + 8 = 15 \equiv 3 \pmod{12}$$
$$7 - 8 = -1 \equiv 11 \pmod{12}$$
$$7 \cdot 8 = 56 \equiv 8 \pmod{12}$$

Theorem The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to addition:
1. Closure: $[x] + [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
2. Associative: $([x] + [y]) + [z] = [x] + ([y] + [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
3. Commutative: $[x] + [y] = [y] + [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
4. Identity, namely, $[0]$.
5. Additive inverse: $-[x] = [-x]$, for all $[x] \in \mathbb{Z}/n\mathbb{Z}$.

Theorem The set $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n has the following properties with respect to multiplication:
1. Closure: $[x] \cdot [y] \in \mathbb{Z}/n\mathbb{Z}$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
2. Associative: $([x] \cdot [y]) \cdot [z] = [x] \cdot ([y] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.
3. Commutative: $[x] \cdot [y] = [y] \cdot [x]$, for all $[x], [y] \in \mathbb{Z}/n\mathbb{Z}$.
4. Identity, namely, $[1]$.
5. Distributivity of multiplication over addition: $[x] \cdot ([y] + [z]) = ([x] \cdot [y]) + ([x] \cdot [z])$, for all $[x], [y], [z] \in \mathbb{Z}/n\mathbb{Z}$.

Two integers x and y are said to be multiplicative inverses if $xy \equiv 1 \pmod{n}$, where n is a positive integer greater than 1.

Theorem The multiplicative inverse $1/b$ modulo n exists *iff* $gcd(b, n) = 1$.

Corollary There are $\phi(n)$ numbers b for which $1/b \pmod{n}$ exists.

Corollary The division a/b modulo n (assume that a/b is in lowest terms) is possible *iff* $1/b \pmod{n}$ exists.

Theorem $\mathbb{Z}/n\mathbb{Z}$ is a field *iff* n is prime.

Let $1/a \pmod{n} = x$, which is equivalent to $ax \equiv 1 \pmod{n}$.
Since $ax \equiv 1 \pmod{n} \iff ax - ny = 1$.

So finding the inverse becomes finding the solution of the linear Diophantine equation $ax - ny = 1$.

▼ Example: Find...

▼ $1/154 \pmod{801}$

find x and y in $154x - 801y = 1$.

$$\begin{aligned} 801 &= 154 \cdot 5 + 31 \\ 154 &= 31 \cdot 4 + 30 \\ 31 &= 30 \cdot 1 + 1 \\ 30 &= 10 \cdot 3 + 0. \end{aligned}$$

Since gcd(154, 801) = 1, and the equation $154x - 801y = 1$ is soluble.

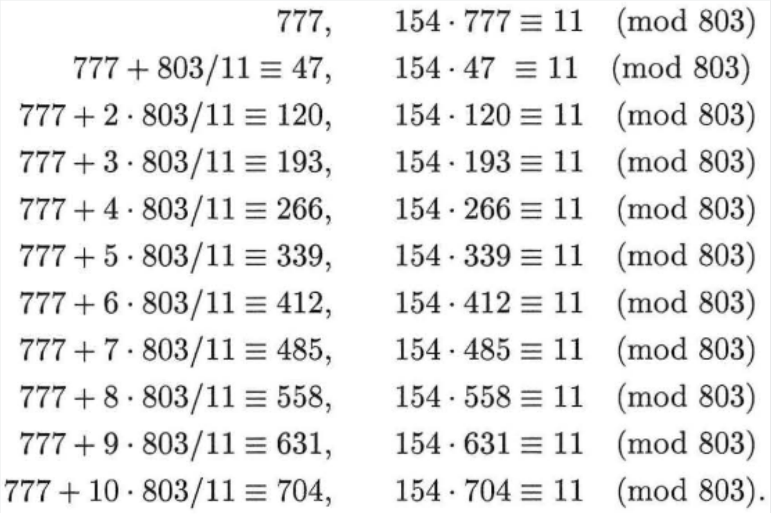
we now work backwords from the above equations

$$\begin{aligned} 1 &= 31 - 30 * 1 \\ &= 31 - (154 - 31 * 4) * 1 \\ &= 31 - 154 + 4 * 31 \\ &= 5 * 31 - 154 \\ &= 5 * (801 - 154 * 5) - 154 \\ &= 5 * 801 - 26 * 154 \\ &= 801 * 5 - 154 * 26 \end{aligned}$$

So, $x \equiv -26 \equiv 775 \pmod{801}$, that is, $1/154 \mod 801 = 775$.

▼ $4/154 \pmod{801}$

Since $4/154 \equiv 4 \cdot 1/154 \pmod{801}$, then $4/154 \equiv 4 \cdot 775 \equiv 697 \pmod{801}$.



$$\begin{aligned} 777, \quad & 154 \cdot 777 \equiv 11 \pmod{803} \\ 777 + 803/11 \equiv 47, \quad & 154 \cdot 47 \equiv 11 \pmod{803} \\ 777 + 2 \cdot 803/11 \equiv 120, \quad & 154 \cdot 120 \equiv 11 \pmod{803} \\ 777 + 3 \cdot 803/11 \equiv 193, \quad & 154 \cdot 193 \equiv 11 \pmod{803} \\ 777 + 4 \cdot 803/11 \equiv 266, \quad & 154 \cdot 266 \equiv 11 \pmod{803} \\ 777 + 5 \cdot 803/11 \equiv 339, \quad & 154 \cdot 339 \equiv 11 \pmod{803} \\ 777 + 6 \cdot 803/11 \equiv 412, \quad & 154 \cdot 412 \equiv 11 \pmod{803} \\ 777 + 7 \cdot 803/11 \equiv 485, \quad & 154 \cdot 485 \equiv 11 \pmod{803} \\ 777 + 8 \cdot 803/11 \equiv 558, \quad & 154 \cdot 558 \equiv 11 \pmod{803} \\ 777 + 9 \cdot 803/11 \equiv 631, \quad & 154 \cdot 631 \equiv 11 \pmod{803} \\ 777 + 10 \cdot 803/11 \equiv 704, \quad & 154 \cdot 704 \equiv 11 \pmod{803}. \end{aligned}$$

Theorem (Fermat's little theorem) Let a be a positive integer, and p prime. If gcd(a, p) = 1, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem (Euler's theorem) Let a and n be positive integers with gcd(a, n) = 1. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

Theorem (Carmichael's theorem) Let a and n be positive integers with gcs(a, n) = 1. Then $a^{\lambda(n)} \equiv 1 \pmod{n}$.

Ch 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 $a \not\mid b$ when a does not divide b.

▼ Example 1 Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution:

$3 \not\mid 7$, because $\dfrac{7}{3}$ is not an integer.

$3 \mid 12$, because $\dfrac{12}{3} = 4$.

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 $a \mid c$.

COLLARY 1
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.

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 $a = dq + r$.

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

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. We say that $a \equiv b \pmod{m}$ is a **congruence** and that m is its **modulus** (plural **moduli**). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

Remark: Although both notations $a \equiv b \pmod{m}$ and $a \textbf{ mod } m = b$ include "mod", then represent fundamentally different concepts. The first represents a relation on the set of integers, whereas the second represents a function.

THEOREM 3
Let a and b be integers, let m be a positive integer. Then $a \equiv b \pmod{m}$ *iff* $a \textbf{ mod } m = b \textbf{ mod } m$.

THEOREM 4
Let m be a positive integer. Then integers a and b are congruent modulo m *iff* 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 $a \equiv d \pmod{m}$, then

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

You cannot always divide both sides of a congruence by the same number.

If $ac \equiv bc \pmod{m}$, the congruence $a \equiv b \pmod{m}$ may be false.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, the congruence $a^c \equiv b^d \pmod{m}$ may be false.

COLLARY 2

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

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

and

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

▼ Example 7

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

Solution:

$19^3 \textbf{ mod } 31 = 6859 \textbf{ mod } 31 = 221 \cdot 31 + 8 \textbf{ mod } 31 = 8$

$(19^3 \textbf{ mod } 31)^4 \textbf{ mod } 23 = 8^4 \textbf{ mod } 23$

$8^4 \textbf{ mod } 23 = 4096 \textbf{ mod } 23 = 178 \cdot 23 + 2 \textbf{ mod } 23 = 2.$

Arithmetic Modulo m

Arithmetic operations (Z_m): the set $\{0, 1, \ldots, m-1\}$.

> $a +_m b = (a+b) \textbf{ mod } m$
> $a \cdot_m b = (a \cdot b) \textbf{ mod } m$

▼ Example 8

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 addtion modulo 11, we find that

$7 +_{11} 9 = (7+9) \textbf{ mod } 11 = 16 \textbf{ mod } 11 = 5.$

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

Properties $+_m$ and $\cdot_m$ satisfy

- **Closure**: If a and b belong to Z_m, then $a +_m b$ and $a \cdot_m b$ belong to Z_m.
- **Associativity**: If a, b, and c belong to 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 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 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 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 Z_m, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Ch 4.3 Primes and Greatest Common Divisors (R)

Primes

An integer p greater than 1 is called *prime iff* 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*.

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 nondecreasing size.

Trial Division

Accoring to Wikipedia

$\longrightarrow$ Test if an integer n can be divided by each number in turn that is less than n.

Ex. $n = 12$ (1, 2, 3, 4, 6, 12). Selecting only the largest powers of primes $\rightarrow$ $12 = 3 \times 4 = 3 \times 2^2$.

Theorem 2
If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

▼ Example 3

Show that 101 is prime.

Solution:

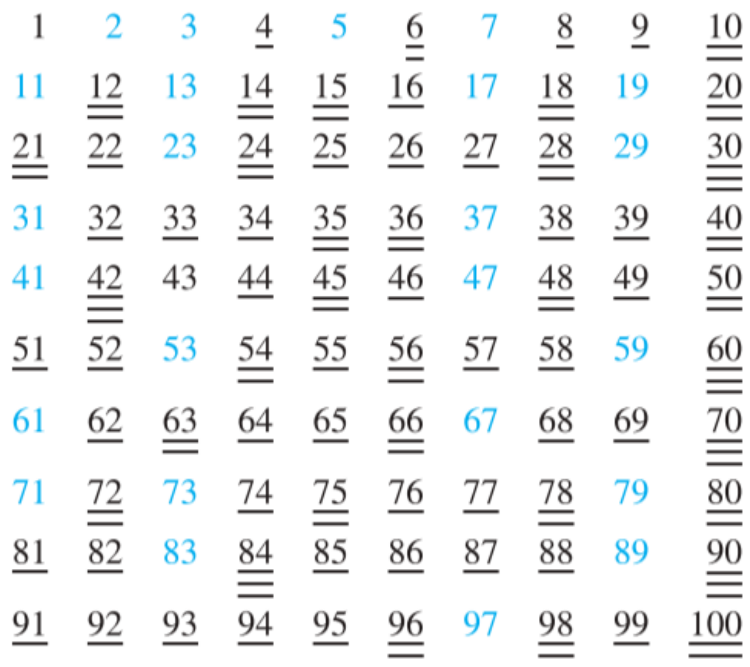
The only primes not excceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

The Sieve of Eratosthenes

$\longrightarrow$ Used to find all primes not exceeding a specified positive integer.

Ex. Find all primes between 1 and 100.

1. Delete all integers divisible by 2 other than 2.
2. Delete all integers divisible by 3 other than 3. (Because 3 is the first integer greater than 2 that is left)
3. Delete all integers divisible by 5 other than 5. (Because of the same reason)
4. Do the same for 7.
5. Done. (Because all composite integers not exceeding 100 are divisible by 2, 3, 5, or 7, all remaining integers except 1 are prime)



1	2	3	$\underline{4}$	5	$\underline{\underline{6}}$	7	$\underline{8}$	$\underline{9}$	$\underline{\underline{10}}$
11	$\underline{\underline{12}}$	13	$\underline{\underline{14}}$	$\underline{\underline{15}}$	$\underline{16}$	17	$\underline{\underline{18}}$	19	$\underline{\underline{20}}$
$\underline{\underline{21}}$	$\underline{22}$	23	$\underline{\underline{24}}$	$\underline{25}$	$\underline{26}$	$\underline{27}$	$\underline{\underline{28}}$	29	$\underline{\underline{\underline{30}}}$
31	$\underline{32}$	$\underline{33}$	$\underline{34}$	$\underline{\underline{35}}$	$\underline{\underline{36}}$	37	$\underline{38}$	$\underline{39}$	$\underline{\underline{40}}$
41	$\underline{\underline{\underline{42}}}$	43	$\underline{44}$	$\underline{\underline{45}}$	$\underline{46}$	47	$\underline{\underline{48}}$	$\underline{49}$	$\underline{\underline{50}}$
$\underline{51}$	$\underline{52}$	53	$\underline{\underline{54}}$	$\underline{55}$	$\underline{\underline{56}}$	$\underline{57}$	$\underline{58}$	59	$\underline{\underline{\underline{60}}}$
61	$\underline{62}$	$\underline{\underline{63}}$	$\underline{64}$	$\underline{65}$	$\underline{\underline{66}}$	67	$\underline{68}$	$\underline{69}$	$\underline{\underline{\underline{70}}}$
71	$\underline{\underline{72}}$	73	$\underline{74}$	$\underline{\underline{75}}$	$\underline{76}$	$\underline{77}$	$\underline{\underline{78}}$	79	$\underline{\underline{80}}$
$\underline{81}$	$\underline{82}$	83	$\underline{\underline{\underline{84}}}$	$\underline{85}$	$\underline{86}$	$\underline{87}$	$\underline{88}$	89	$\underline{\underline{\underline{90}}}$
$\underline{91}$	$\underline{92}$	$\underline{93}$	$\underline{94}$	$\underline{95}$	$\underline{\underline{96}}$	97	$\underline{\underline{98}}$	$\underline{99}$	$\underline{\underline{100}}$

Theorem 3
There are infinitely many primes.

Proof. We will prove this theorem using a proof by contradiction. We assume that there are only finitely many primes, $p_1, p_2, \ldots, p_n$. Let $Q = p_1 p_2 \cdots p_n + 1$.

By the fundamental theorem of arithmetic. Q is prime or else it can be written as the product of two more primes. However, none of the primes p_j divides Q, for if $p_j \mid Q$, then p_j divides $Q - p_1 p_2 \cdots p_n = 1$. Hence, there is a prime not in the list $p_1, p_2, \ldots, p_n$. This prime is either Q, if it is prime, or a prime factor of Q. This is a contradiction because we assumed that we have listed all the primes. Consequently, there are infinitely many primes.

Mersenne primes

$2^p - 1$ is a prime where p is also a prime.

Theorem 4 THE PRIME NUMBBER THEOREM

The ratio of $\pi(x)$, the number of primes not exceeding x, and $\dfrac{x}{\ln x}$ approaches 1 as x grows without bound.

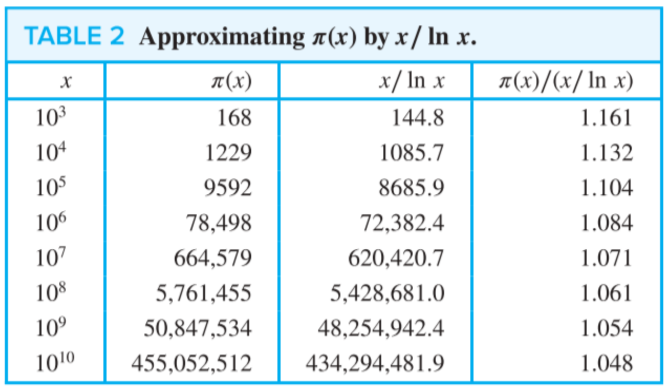


TABLE 2 **Approximating $\pi(x)$ by $x/\ln x$.**

x	$\pi(x)$	$x/\ln x$	$\pi(x)/(x/\ln x)$
10^3	168	144.8	1.161
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78,498	72,382.4	1.084
10^7	664,579	620,420.7	1.071
10^8	5,761,455	5,428,681.0	1.061
10^9	50,847,534	48,254,942.4	1.054
10^{10}	455,052,512	434,294,481.9	1.048

Goldbach's Conjecture

Every even integer n, $n > 2$, is the sum of two primes.

Twin primes

Pairs of primes that differ by 2. Ex. 3 & 5, 5 & 7, 11 & 13, 17 & 19, 4967 & 4969.

Greatest Common Divisor & Least Common Multiples

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

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

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

▼ Example 13

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.

Another way to find GCD

Given $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$.

> $$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

▼ Example 14

Because the prime factorizations of 120 and 500 are $120 = 2^3 \cdot 3 \cdot 5$ and $500 = 2^2 \cdot 5^3$, the greatest common divisor is

$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20$.

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 $\operatorname{lcm}(a, b)$.

> $$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

▼ Example 15

What is the least common mutliple of $2^3 3^5 7^2$ and $2^4 3^3$?

Solution:

We have $\operatorname{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)} 3^{\max(5,3)} 7^{\max(2,0)} = 2^4 3^5 7^2$.

Theorem 5

Let a and b be positive integers. Then $ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b)$.

The Euclidean Algorithm

LEMMA 1

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

▼ Example 16

Find the greatest common divisor of 414 and 662 using the Euclidean Algorithm.

Solution:

Successive uses of the division algorithm give:

$662 = 414 \cdot 1 + 248$

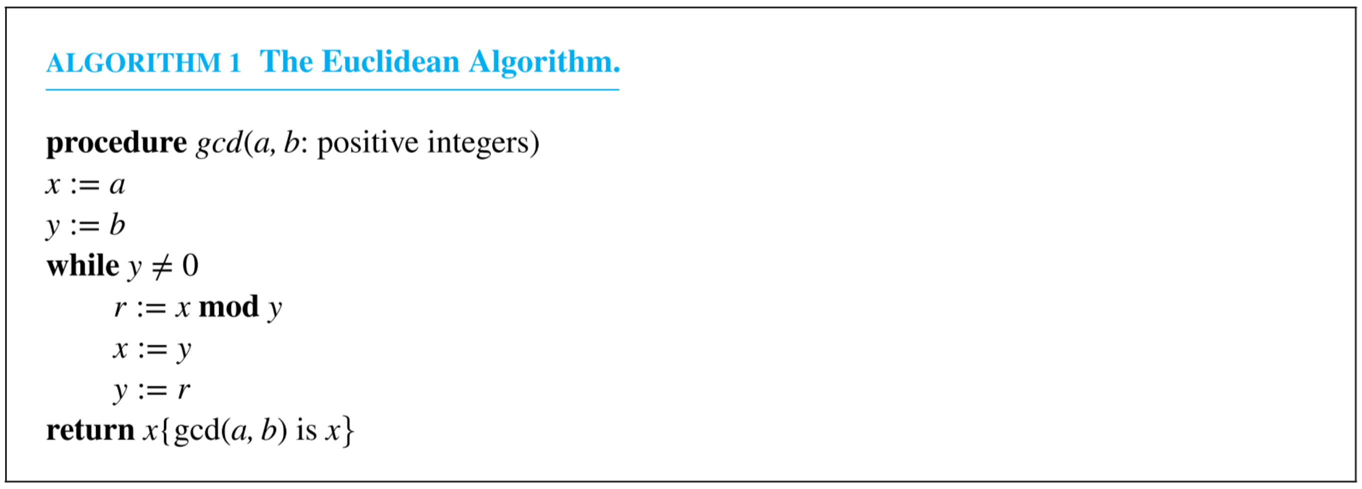
$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

$82 = 2 \cdot 41.$

Hence, $\gcd(414, 662) = 2$, because 2 is the last nonzero remainder.



ALGORITHM 1 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}
```

gcds as Linear Combinations

Theorem 6   BÉZOUT'S THEOREM
If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

If a and b are positive integers, then integers s and t such that $\gcd(a, b) = sa + tb$ are called *Bézout coefficients* of a and b. Also, the equation $\gcd(a, b) = sa + tb$ is called *Bézout's identity*.

LEMMA 2
If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.

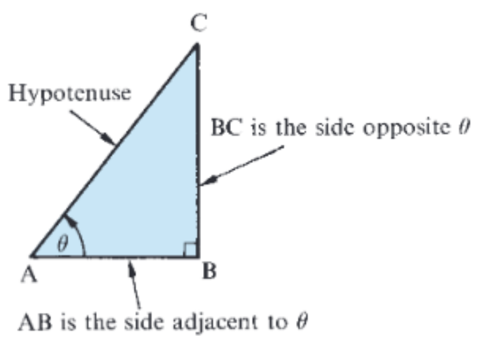
LEMMA 3
If p is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.

▼ Example 19

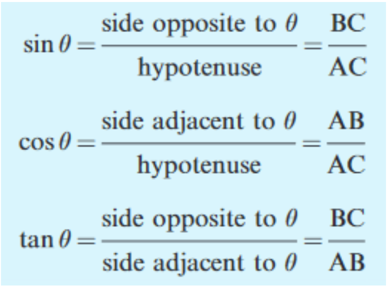
The congruence $14 \equiv 8 \pmod 6$ holds, but both sides of this congruence cannot be divided by 2 to produce a valid congruence because $\frac{14}{2} = 7$ and $\frac{8}{2} = 4$, but $7 \not\equiv 4 \pmod 6$.

Theorem 7
Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod m$.

Ch 22 Introduction to trigonometry (C)


C
Hypotenuse
BC is the side opposite θ
θ
A
B
AB is the side adjacent to θ

- **hypotenuse:** the side opposite the right angle
- **opposite**: the side opposite of θ
- **adjacent**: the remaining side



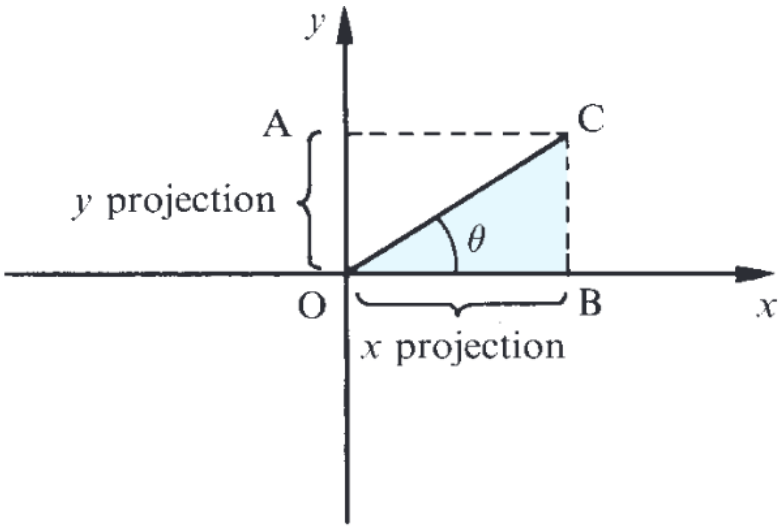
$$\sin\theta = \frac{\text{side opposite to } \theta}{\text{hypotenuse}} = \frac{BC}{AC}$$

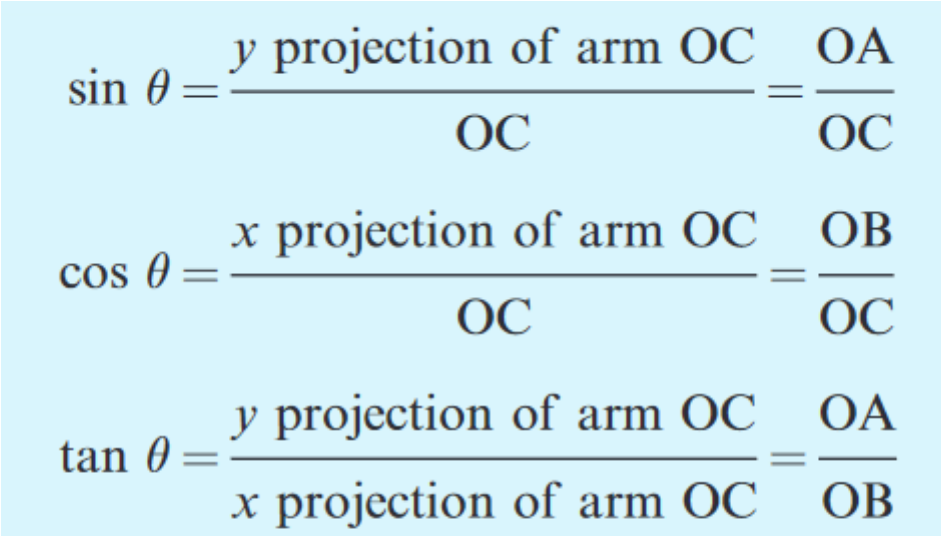
$$\cos\theta = \frac{\text{side adjacent to } \theta}{\text{hypotenuse}} = \frac{AB}{AC}$$

$$\tan\theta = \frac{\text{side opposite to } \theta}{\text{side adjacent to } \theta} = \frac{BC}{AB}$$

📝

Ch 23 Trigonometrical functions and their graphs (C)





$$\sin\theta = \frac{y \text{ projection of arm OC}}{\text{OC}} = \frac{\text{OA}}{\text{OC}}$$

$$\cos\theta = \frac{x \text{ projection of arm OC}}{\text{OC}} = \frac{\text{OB}}{\text{OC}}$$

$$\tan\theta = \frac{y \text{ projection of arm OC}}{x \text{ projection of arm OC}} = \frac{\text{OA}}{\text{OB}}$$

Ch 24 Trigonometrical identities and equations (C)

Common Trigonometrical identities

$$\frac{\sin A}{\cos A} = \tan A$$

$$\begin{aligned}\sin(A+B) &= \sin A\cos B + \sin B\cos A\\ \sin(A-B) &= \sin A\cos B - \sin B\cos A\\ \sin 2A &= 2\sin A\cos A\end{aligned}$$

$$\begin{aligned}\cos(A+B) &= \cos A\cos B - \sin A\sin B\\ \cos(A-B) &= \cos A\cos B + \sin A\sin B\\ \cos 2A &= (\cos A)^2 - (\sin A)^2 = \cos^2 A - \sin^2 A\end{aligned}$$

$$\begin{aligned}\tan(A+B) &= \frac{\tan A + \tan B}{1 - \tan A\tan B}\\ \tan(A-B) &= \frac{\tan A - \tan B}{1 + \tan A\tan B}\end{aligned}$$

$$\begin{aligned}\sin A + \sin B &= 2\sin\left(\frac{A+B}{2}\right)\cos\left(\frac{A-B}{2}\right)\\ \sin A - \sin B &= 2\sin\left(\frac{A-B}{2}\right)\cos\left(\frac{A+B}{2}\right)\\ \cos A + \cos B &= 2\cos\left(\frac{A+B}{2}\right)\cos\left(\frac{A-B}{2}\right)\\ \cos A - \cos B &= -2\sin\left(\frac{A-B}{2}\right)\sin\left(\frac{A+B}{2}\right)\end{aligned}$$

$$\begin{aligned}\sin\theta &= \sin(180^\circ - \theta)\\ &= -\sin(\theta - 180^\circ)\\ &= -\sin(360^\circ - \theta)\end{aligned}$$

$$\begin{aligned}\cos\theta &= -\cos(180^\circ - \theta)\\ &= -\cos(\theta - 180^\circ)\\ &= \cos(360^\circ - \theta)\end{aligned}$$

$$\begin{aligned}\tan\theta &= -\tan(180^\circ - \theta)\\ &= \tan(\theta - 180^\circ)\\ &= -\tan(360^\circ - \theta)\end{aligned}$$

$$\begin{aligned}\sin A &= -\sin(-A)\\ \cos A &= \cos(-A)\\ \tan A &= -\tan(-A)\end{aligned}$$

▼ Solve $\tan(2\theta + 20^\circ) = 0.3 \quad 0^\circ \leq \theta \leq 360^\circ$

Let $z = 2\theta + 20^\circ$. As $0^\circ \leq \theta \leq 360^\circ$ then $20^\circ \leq z \leq 740^\circ$.

First we solve $\tan z = 0.3 \quad 0^\circ \leq z \leq 360^\circ$

This leads to $z = 16.7^\circ + 360^\circ,\ 196.7^\circ + 360^\circ = 376.7^\circ,\ 556.7^\circ$.

By adding a further 360° values of z in the range 720° to 1080° are found. These are $z = 736.7^\circ,\ 916.7^\circ$.

Hence values of z in the range $0^\circ - 1080^\circ$ are $z = 16.7^\circ,\ 196.7^\circ,\ 376.7^\circ,\ 556.7^\circ, 736.7^\circ,\ 916.7^\circ$.

Values of z in the range $20^\circ - 740^\circ$ are thus $z = 196.7^\circ,\ 376.7^\circ,\ 556.7^\circ,\ 736.7^\circ$.

The values of θ in the range 0-360 are found using $\theta = (z - 20^\circ)/2$:

$$\theta = \frac{z - 20^\circ}{2} = 88.35^\circ,\ 178.35^\circ,\ 268.35^\circ,\ 358.35^\circ.$$

Ch 19 The exponential function (C)

Exponential expression

> The most common exponential expression is e^x, where e is the exponential contant, 2.71828...

Exponential Normal Rules

$$\begin{aligned} e^a e^b &= e^{a+b} \\ \frac{e^a}{e^b} &= e^{a-b} \\ e^0 &= 1 \\ (e^a)^b &= e^{ab} \end{aligned}$$

The exponential function and its graph

- Never negative
- when x = 0, y = 1
- x ⬆️ e^x⬆️ → exponential growth

Ch 20 The logarithm function (C)

Intro to logarithms

$y = a^x$ and $\log_a y = x$ are equivalent.

- **base**: can be any positive number other than 1

Calculating logarithms to any base

$\log_a X = \frac{\log_{10} X}{\log_{10} a} \quad \log_a X = \frac{\ln_{10} X}{\ln_{10} a}$

$\log_a a = 1$

Laws of logarithms

$\log A + \log B = \log AB$

$\log A - \log B = \log \frac{A}{B}$

$\log 1 = 0$

$n \log A = \log A^n$

Ch 34 Gradients of curves (C)

Given a function $y = f(x)$ we denote its gradient function by $\frac{dy}{dx}$ or simply by y'.

Gradient function of $y = x^n$

If $y = x^n$ then $y' = nx^{n-1}$.

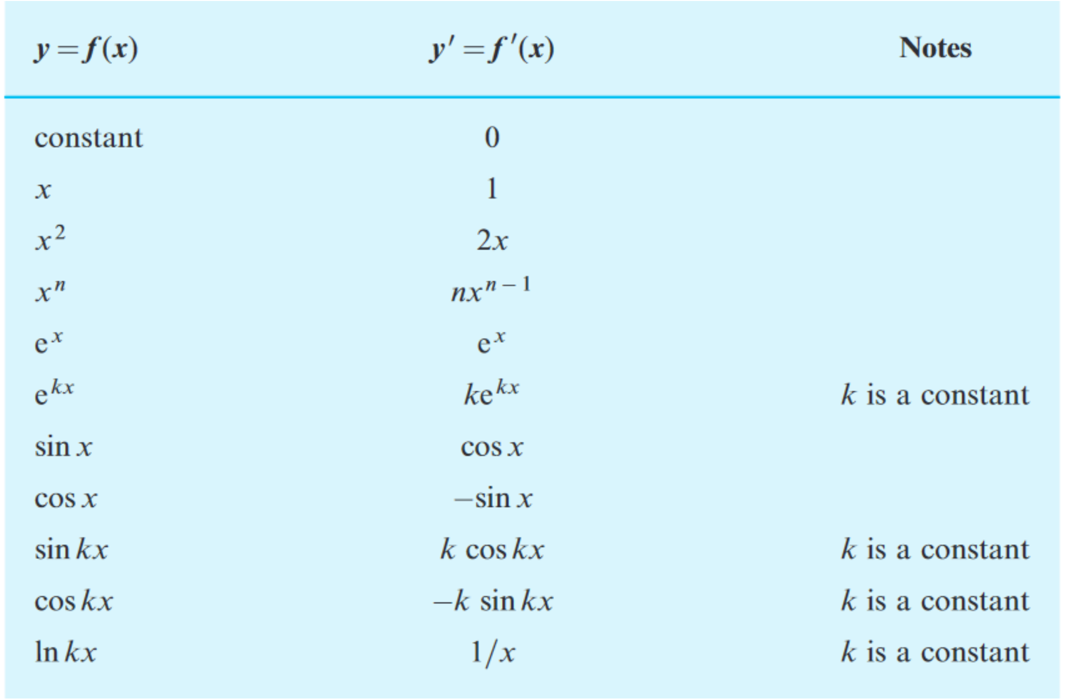
Rules for finding gradient functions

Rule 1: If $y = f(x) + g(x)$ then $y' = f'(x) + g'(x)$.
Rule 2: If $y = f(x) - g(x)$ then $y' = f'(x) - g'(x)$.
Rule 3: If $y = kf(x)$, where k is a number, then $y' = kf'(x)$.

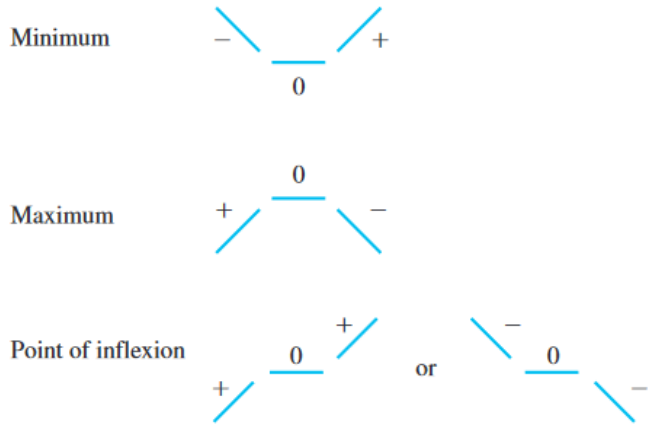
Higher derivatives

y'' or $\frac{d^2y}{dx^2}$ is found by differentiating y'.

Finding max & min points of a curve



$y = f(x)$	$y' = f'(x)$	Notes
constant	0	
x	1	
x^2	$2x$	
x^n	nx^{n-1}	
e^x	e^x	
e^{kx}	ke^{kx}	k is a constant
$\sin x$	$\cos x$	
$\cos x$	$-\sin x$	
$\sin kx$	$k \cos kx$	k is a constant
$\cos kx$	$-k \sin kx$	k is a constant
$\ln kx$	$1/x$	k is a constant



Stationary points are located by setting the gradient function equal to zero, that is $y' = 0$.

If y'' is positive at the stationary point, the point is a minimum.
If y'' is negative at the stationary point, the point is a maximum.
If y'' is equal to zero, this test does not tell us anything and the previous method should be used.

Ch 35 Techniques of differentiation (C)

Product Rule

> If $y = uv$ then $y' = u'v + uv'$

Quotient Rule

> If $y = \frac{u}{v}$ then $y' = \frac{vu' - uv'}{v^2}$

Chain Rule

> If $y = y(x)$ and $x = x(t)$, then $y' = \frac{dy}{dx} \times \frac{dx}{dt}$

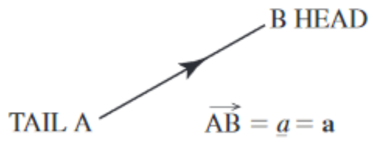
Ch 26 Vectors (C)

Introduction to Vectors and Scalars

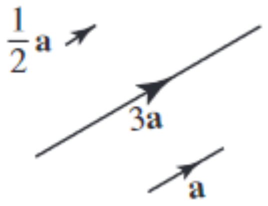
Magnitude: single number. i.e. 3 km 3 is the magnitude

Scalars: quantities that can be described by a single number. I.e. temperature, length, volume, density...

A vector has both magnitude and direction.

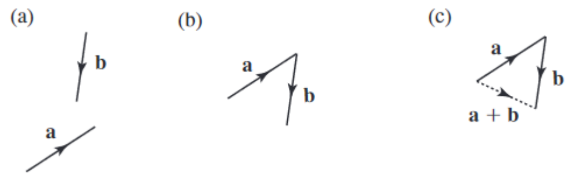


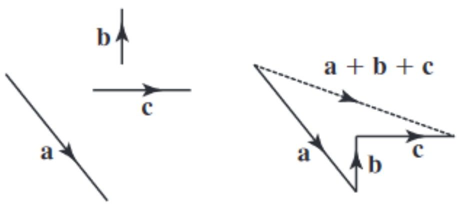
Multiplying a vector by a scalar



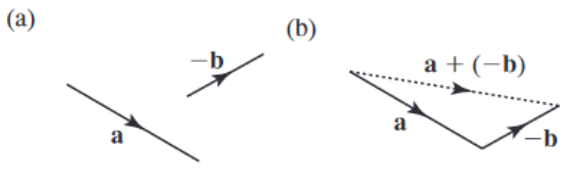
Adding and subtracting vectors

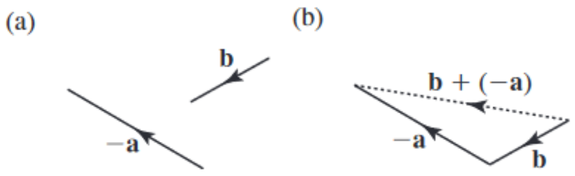
The resultant of **a** and **b** is the sum **a** + **b**.





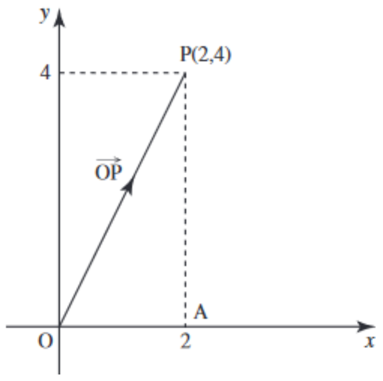
Subtraction of vectors: a + (-b)





Representing vectors using Cartesian components

The unit vectors in the x and y directions are **i** and **j** respectively.



The vector $\overrightarrow{OP}$ is 2i + 4j

If **r** = x**i** + y**j**, then $|\mathbf{r}| = \sqrt{x^2 + y^2}$

The scalar product (dot product)

Given two vectors, **a** and **b**, their scalr product, denoted by $\mathbf{a} \cdot \mathbf{b}$, is given by
$\mathbf{a} \cdot \mathbf{b} = |\mathbf{a}||\mathbf{b}| \cos \theta$
where θ is the angle between **a** and **b**.

$\mathbf{i} \cdot \mathbf{i} = 1 \quad \mathbf{j} \cdot \mathbf{j} = 1 \quad \mathbf{i} \cdot \mathbf{j} = 0 \quad \mathbf{j} \cdot \mathbf{i} = 0$

If $\mathbf{a} = a_1\mathbf{i} + a_2\mathbf{j},\ \mathbf{b} = b_1\mathbf{i} + b_2\mathbf{j}$ then
$\mathbf{a} \cdot \mathbf{b} = a_1 b_1 + a_2 b_2$

Ch 7.2 Matrices

$\rightarrow$ Not commutative ($T_1 \times T_2 \neq T_2 \times T_1$)

$$\begin{aligned} x' &= ax + by \\ y' &= xc + dy \end{aligned} \qquad \begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$$

$$\begin{aligned} x'' &= (Aa + Bc)x + (Ab + Bd)y \\ y'' &= (Ca + Dc)x + (Cb + Dd)y \end{aligned} \qquad \begin{bmatrix} x'' \\ y'' \end{bmatrix} = \begin{bmatrix} A & B \\ C & D \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} x \\ y \end{bmatrix}$$

Systems of Notation

Column Vector Notation

Above

Row Vector Notation

$$\begin{bmatrix} x' & y' \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \cdot \begin{bmatrix} a & c \\ b & d \end{bmatrix}$$

The Determinant of a Matrix

$\rightarrow$ Scalar quantity

The determinant of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ which is $ad - cb$.

▼ Example

The determinant of $\begin{bmatrix} 3 & 2 \\ 1 & 2 \end{bmatrix}$ is $3 \times 2 - 1 \times 2 = 4$.

Ch 27 Matrices (C)

What is a matrix?

Element: Each number in a matrix

Size: Number of rows and number of columns in order

$$A = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 4 & 6 \end{bmatrix} \qquad B = \begin{bmatrix} 1 \\ 2 \\ -4 \end{bmatrix} \qquad C = \begin{bmatrix} 1 & 1 & 2 \\ -3 & 4 & 5 \\ \frac{1}{2} & 2 & 1 \end{bmatrix}$$

$$2 \times 3 \qquad\qquad 3 \times 1 \qquad\qquad 3 \times 3$$

Square matrix: same number of rows as columns

Diagonal matrix: a square matrix where all elements are 0 except those on the diagonal (top left to bottom right - **leading diagonal**)

Identify matrix: a diagonal matrix where all diagonal entries are 1

$\rightarrow$ when multiplying identity matrices, it leaves the matrix unchanged, just like multiply 1.

Addition, subtraction and multiplication of matrices

Add & **Subtract**: same size

Multiply & **Divide**: by a scalar (number)

Multiply: by another matrix if conditions met

Divide: never by another matrix

$+/-$

$$\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} 5 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 4 \\ 4 & 4 \end{bmatrix}$$

$\begin{bmatrix} 1 & 2 & 9 \\ -1 & \frac{1}{2} & 0 \end{bmatrix}$ and $\begin{bmatrix} 1 \\ 0 \\ 7 \end{bmatrix}$ cannot be added nor subtracted from one another.

$\times / \div$

$$\frac{1}{4} \begin{bmatrix} 16 \\ 8 \end{bmatrix} = \begin{bmatrix} 4 \\ 2 \end{bmatrix}$$

Multiply two matrices

If A has size $p \times q$ and B has size $q \times s$, then AB has size $p \times s$.

If $p \neq s$, then BA does not exist.

Possible

$\begin{bmatrix} 1 & 4 & 9 \\ 2 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 9 \\ 8 & 7 \\ -7 & 3 \end{bmatrix}$ 2 x 3 3 x 2

Not Possible

$\begin{bmatrix} 3 & 7 & 2 \\ -1 & 0 & -10 \end{bmatrix} \begin{bmatrix} 1 & -7 \\ -1 & 2 \end{bmatrix}$ 2 x 3 2 x 2

Inverse

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then $A^{-1} = \dfrac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

- leading diagonal interchanged
- remaining elements change sign
- resulting matrix multiply by $\dfrac{1}{ad - bc}$

$AA^{-1} = A^{-1}A = I$ (identity matrix)

If $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ then its determinant is $|A| = \begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc.$

Singular matrix: its determinant is zero. Hence cannot have an inverse.

Application

$AX = B$
$X = A^{-1}B$ provided A^{-1} exists.

▼ Example

$$x + 2y = 13$$
$$2x - 5y = 8$$

$$\begin{bmatrix} 1 & 2 \\ 2 & -5 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 13 \\ 8 \end{bmatrix} \qquad AX = B$$

$$X = A^{-1}B$$

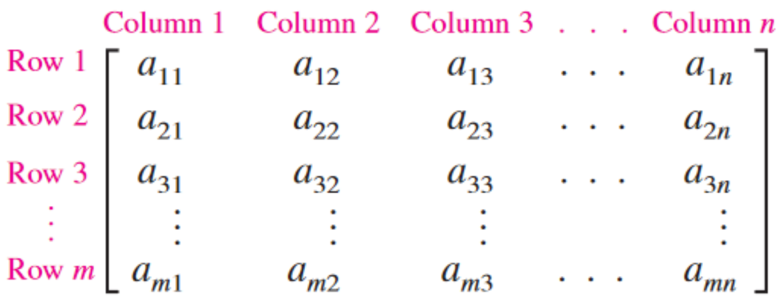
$$X = \frac{1}{-9} \begin{bmatrix} -5 & -2 \\ -2 & 1 \end{bmatrix} \begin{bmatrix} 13 \\ 8 \end{bmatrix} = -\frac{1}{9} \begin{bmatrix} -81 \\ -18 \end{bmatrix} = \begin{bmatrix} 9 \\ 2 \end{bmatrix}$$

Therefore the solution is $x = 9, y = 2$.

Ch 8.1 Matrices and Systems of Equations (L)

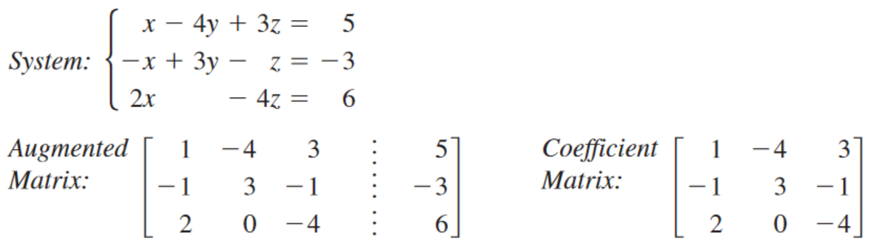
Definition of Matrix

An $m \times n$ matrix has m rows and n columns. Matrices are usually denoted by capital letters.



$$\begin{array}{c|ccccc|}
 & \text{Column 1} & \text{Column 2} & \text{Column 3} & \cdots & \text{Column } n \\
\text{Row 1} & a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\
\text{Row 2} & a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\
\text{Row 3} & a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\
\vdots & \vdots & \vdots & \vdots & & \vdots \\
\text{Row } m & a_{m1} & a_{m2} & a_{m3} & \cdots & a_{mn}
\end{array}$$

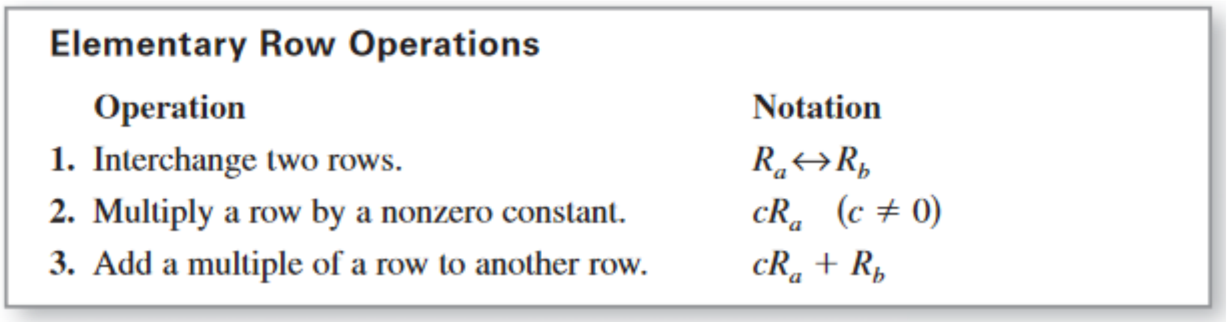
Augmented Matrix



$$\textit{System: } \begin{cases} x - 4y + 3z = 5 \\ -x + 3y - z = -3 \\ 2x \qquad - 4z = 6 \end{cases}$$

$$\textit{Augmented Matrix: } \begin{bmatrix} 1 & -4 & 3 & \vdots & 5 \\ -1 & 3 & -1 & \vdots & -3 \\ 2 & 0 & -4 & \vdots & 6 \end{bmatrix} \qquad \textit{Coefficient Matrix: } \begin{bmatrix} 1 & -4 & 3 \\ -1 & 3 & -1 \\ 2 & 0 & -4 \end{bmatrix}$$

Elementary Row Operations

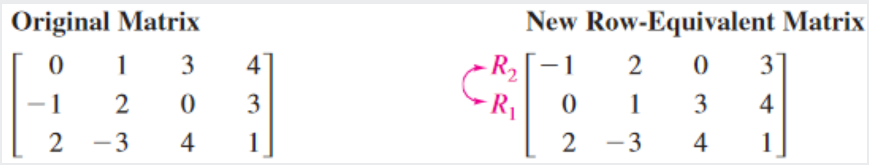


Elementary Row Operations

Operation	Notation
1. Interchange two rows.	$R_a \leftrightarrow R_b$
2. Multiply a row by a nonzero constant.	$cR_a \quad (c \neq 0)$
3. Add a multiple of a row to another row.	$cR_a + R_b$

▼ Example 3

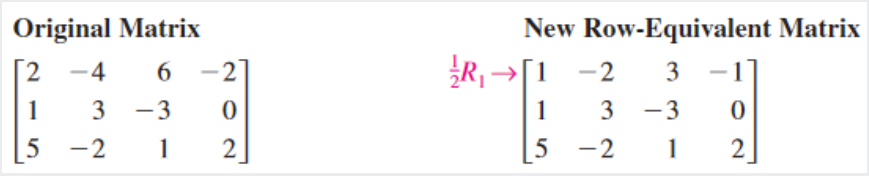
a. Interchange the first and second rows of the original matrix.



Original Matrix **New Row-Equivalent Matrix**

$$\begin{bmatrix} 0 & 1 & 3 & 4 \\ -1 & 2 & 0 & 3 \\ 2 & -3 & 4 & 1 \end{bmatrix} \qquad \begin{array}{c} R_2 \\ R_1 \\ \\ \end{array} \begin{bmatrix} -1 & 2 & 0 & 3 \\ 0 & 1 & 3 & 4 \\ 2 & -3 & 4 & 1 \end{bmatrix}$$

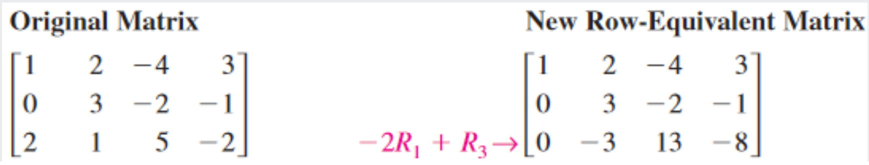
b. Multiply the first row of the original matrix by $\frac{1}{2}$.



Original Matrix **New Row-Equivalent Matrix**

$$\begin{bmatrix} 2 & -4 & 6 & -2 \\ 1 & 3 & -3 & 0 \\ 5 & -2 & 1 & 2 \end{bmatrix} \qquad \begin{array}{c} \frac{1}{2}R_1 \rightarrow \\ \\ \\ \end{array} \begin{bmatrix} 1 & -2 & 3 & -1 \\ 1 & 3 & -3 & 0 \\ 5 & -2 & 1 & 2 \end{bmatrix}$$

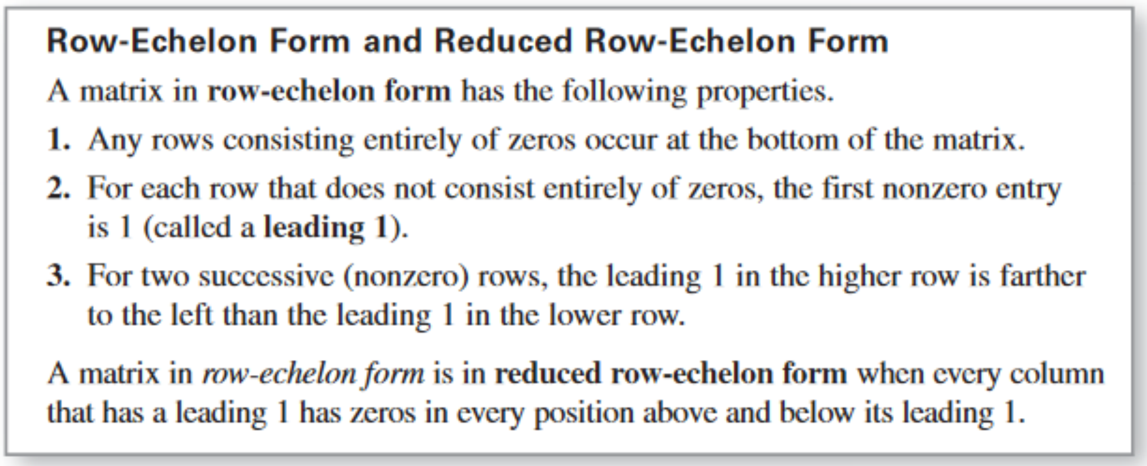
c. Add -2 times the first row of the original matrix to the third row.



Original Matrix **New Row-Equivalent Matrix**

$$\begin{bmatrix} 1 & 2 & -4 & 3 \\ 0 & 3 & -2 & -1 \\ 2 & 1 & 5 & -2 \end{bmatrix} \qquad \begin{array}{c} \\ \\ -2R_1 + R_3 \rightarrow \end{array} \begin{bmatrix} 1 & 2 & -4 & 3 \\ 0 & 3 & -2 & -1 \\ 0 & -3 & 13 & -8 \end{bmatrix}$$

Gaussian Elimination with Back-Substitution



Row-Echelon Form and Reduced Row-Echelon Form

A matrix in **row-echelon form** has the following properties.

1. Any rows consisting entirely of zeros occur at the bottom of the matrix.
2. For each row that does not consist entirely of zeros, the first nonzero entry is 1 (called a **leading 1**).
3. For two successive (nonzero) rows, the leading 1 in the higher row is farther to the left than the leading 1 in the lower row.

A matrix in *row-echelon form* is in **reduced row-echelon form** when every column that has a leading 1 has zeros in every position above and below its leading 1.

echelon refers to the stair-step pattern formed by the nonzero entries of the matrix

▼ Example 5

Determine whether each matrix is in row-echelon form. If it is, determine whether the matrix is in reduced row-echelon form.

$$\textbf{a.}\ \begin{bmatrix}1 & 2 & -1 & 4\\ 0 & 1 & 0 & 3\\ 0 & 0 & 1 & -2\end{bmatrix} \qquad \textbf{b.}\ \begin{bmatrix}1 & 2 & -1 & 2\\ 0 & 0 & 0 & 0\\ 0 & 1 & 2 & -4\end{bmatrix}$$

$$\textbf{c.}\ \begin{bmatrix}1 & -5 & 2 & -1 & 3\\ 0 & 0 & 1 & 3 & -2\\ 0 & 0 & 0 & 1 & 4\\ 0 & 0 & 0 & 0 & 1\end{bmatrix} \qquad \textbf{d.}\ \begin{bmatrix}1 & 0 & 0 & -1\\ 0 & 1 & 0 & 2\\ 0 & 0 & 1 & 3\\ 0 & 0 & 0 & 0\end{bmatrix}$$

$$\textbf{e.}\ \begin{bmatrix}1 & 2 & -3 & 4\\ 0 & 2 & 1 & -1\\ 0 & 0 & 1 & -3\end{bmatrix} \qquad \textbf{f.}\ \begin{bmatrix}0 & 1 & 0 & 5\\ 0 & 0 & 1 & 3\\ 0 & 0 & 0 & 0\end{bmatrix}$$

Ans: (a), (c), (d), and (f) are in row-echelon form.

(d) and (f) are in *reduced* row-echelon form.

The order in which the elementary row operations are performed is important.

1. Write out the augmented matrix.
2. Use the elementary row operations, having leading 1 in upper left corner.
3. Use the elementary row operations, having zeros below the leading 1.
4. Repeat for the second column with diagonal 1s and following 0s.
5. Write it back in system form when it's in row-echelon form, and use back-substitution to work out the solution.

🚫 Entire row of zeros except the last entry means there are no solutions.

$$\left[\begin{array}{rrr:r}1 & -1 & 2 & 4\\ 0 & 1 & -1 & 2\\ 0 & 0 & 0 & -2\\ 0 & 5 & -7 & -11\end{array}\right]$$

Gauss-Jordan Elimination

⟶ continues the reduction process until a *reduced* row-echelon form is obtained.

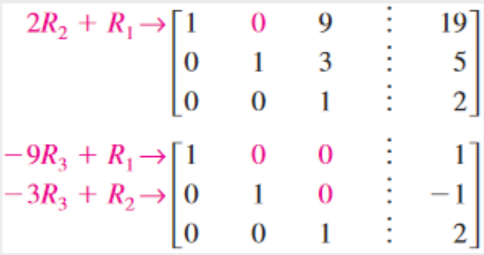
▼ Example 8

Use Gauss-Jordan elimination to solve the system $\begin{cases} x-2y+3z & =9\\ -x+3y & =-4\\ 2x-5y+5z & =17\end{cases}$.

Solution:

Using Gaussian elimination to obtain the row-echelon form $\begin{bmatrix} 1 & -2 & 3 & \vdots & 9 \\ 0 & 1 & 3 & \vdots & 5 \\ 0 & 0 & 1 & \vdots & 2 \end{bmatrix}$.

Now apply the elementary row operations until you obtain zeros above each of the leading 1s.



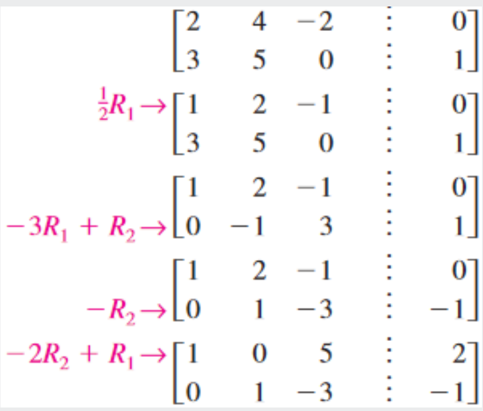
$$\begin{array}{r} 2R_2 + R_1 \rightarrow \\ \\ \\ \end{array} \begin{bmatrix} 1 & 0 & 9 & \vdots & 19 \\ 0 & 1 & 3 & \vdots & 5 \\ 0 & 0 & 1 & \vdots & 2 \end{bmatrix}$$

$$\begin{array}{r} -9R_3 + R_1 \rightarrow \\ -3R_3 + R_2 \rightarrow \\ \\ \end{array} \begin{bmatrix} 1 & 0 & 0 & \vdots & 1 \\ 0 & 1 & 0 & \vdots & -1 \\ 0 & 0 & 1 & \vdots & 2 \end{bmatrix}$$

$$\begin{cases} x = 1 \\ y = -1 \\ z = 2 \end{cases}. \quad \Rightarrow \quad (1, -1, 2).$$

▼ Example 9 **A System with an Infinite Number of Solutions**

Solve the system $\begin{cases} 2x + 4y - 2z & = 0 \\ 3x + 5y & = 1 \end{cases}$.



$$\begin{bmatrix} 2 & 4 & -2 & \vdots & 0 \\ 3 & 5 & 0 & \vdots & 1 \end{bmatrix}$$

$$\begin{array}{r} \frac{1}{2}R_1 \rightarrow \\ \\ \end{array} \begin{bmatrix} 1 & 2 & -1 & \vdots & 0 \\ 3 & 5 & 0 & \vdots & 1 \end{bmatrix}$$

$$\begin{array}{r} \\ -3R_1 + R_2 \rightarrow \end{array} \begin{bmatrix} 1 & 2 & -1 & \vdots & 0 \\ 0 & -1 & 3 & \vdots & 1 \end{bmatrix}$$

$$\begin{array}{r} \\ -R_2 \rightarrow \end{array} \begin{bmatrix} 1 & 2 & -1 & \vdots & 0 \\ 0 & 1 & -3 & \vdots & -1 \end{bmatrix}$$

$$\begin{array}{r} -2R_2 + R_1 \rightarrow \\ \\ \end{array} \begin{bmatrix} 1 & 0 & 5 & \vdots & 2 \\ 0 & 1 & -3 & \vdots & -1 \end{bmatrix}$$

The corresponding system of equation is $\begin{cases} x + 5z & = 2 \\ y - 3z & = -1 \end{cases}$.

Solve for x and y in terms of z, you have $x = -5z + 2$ and $y = 3z - 1$.

Let a represent any real number and let $z = a$.

Ans: $x = -5a + 2$ and $y = 3a - 1$. $\Rightarrow$ $(-5a + 2, 3a - 1, a)$

Ch 8.2 Operations with Matrices (L)

Equality of Matrices

Two matrices are equal when their corresponding entries are equal.

Matrix Addition and Scalar Multiplication

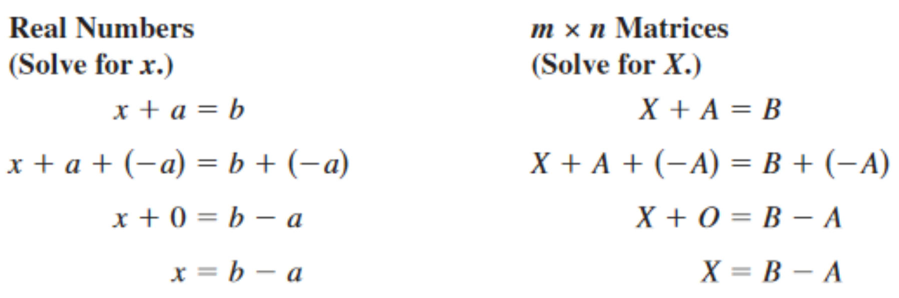
> 💡 If $A = [a_{ij}]$ and $B = [b_{ij}]$ are matrices of order $m \times n$, then their sum is the $m \times n$ matrix given by $A + B = [a_{ij} + b_{ij}]$. The sum of two matrices of different orders is undefined.

> 💡 If $A = [a_{ij}]$ as an $m \times n$ matrix and c is a scalar, then the **scalar multiple** of A by c is the $m \times n$ matrix given by $cA = [ca_{ij}]$.

Properties of Matrix Addition and Scalar Multiplication

Let A, B, and C be $m \times n$ matrices and let c and d be scalars.

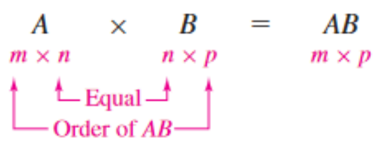
1. $A + B = B + A$ *Commutative*
2. $A + (B + C) = (A + B) + C$ *Associative (Addition)*
3. $(cd)A = c(dA)$ *Associative (Scalar Multiplication)*
4. $1A = A$ *Scalar Identity*
5. $c(A + B) = cA + cB$ *Distributive*
6. $(c + d)A = cA + dA$ *Distributive*



Real Numbers **(Solve for x.)**	**$m \times n$ Matrices** **(Solve for X.)**
$x + a = b$	$X + A = B$
$x + a + (-a) = b + (-a)$	$X + A + (-A) = B + (-A)$
$x + 0 = b - a$	$X + O = B - A$
$x = b - a$	$X = B - A$

Additive identity O

Matrix Multiplication



Properties of Matrix Multiplication

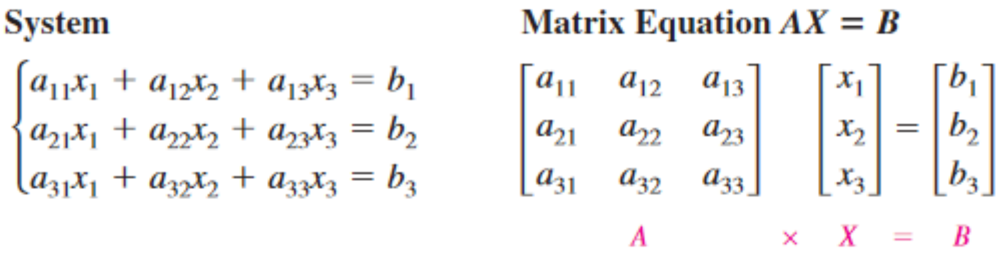
Let A, B, and C be matrices and let c be a scalar.

1. $A(BC) = (AB)C$ *Associative (Multiplication)*
2. $A(B + C) = AB + AC$ *Distributive*
3. $(A + B)C = AC + BC$ *Distributive*
4. $c(AB) = (cA)B = A(cB)$ *Associative (Scalar Multiplication)*

Identity Matrix (I_n or I)

Consisting of 1s on its main diagonal and 0s elsewhere. $AI_n = A$ and $I_n A = A$.

Applications



System	Matrix Equation $AX = B$
$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3 \end{cases}$	$\underset{A}{\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}} \times \underset{X}{\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}} \underset{=}{=} \underset{B}{\begin{bmatrix} b_1 \\ b_2 \\ b_3 \end{bmatrix}}$

▼ Example 12 **Solving a System of Linear Equations**

$$\begin{cases} x_1 - 2x_2 + x_3 & = -4 \\ x_2 + 2x_3 & = 4 \\ 2x_1 + 3x_2 - 2x_3 & = 2 \end{cases}$$

Solution:

a. In matrix form, $AX = B$, the system can be written as follows.

$$\begin{bmatrix} 1 & -2 & 1 \\ 0 & 1 & 2 \\ 2 & 3 & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -4 \\ 4 \\ 2 \end{bmatrix}$$

b. The augmented matrix is formed by adjoining matrix B to matrix A.

$$[A \vdots B] = \begin{bmatrix} 1 & -2 & 1 & \vdots & -4 \\ 0 & 1 & 2 & \vdots & 4 \\ 2 & 3 & -2 & \vdots & 2 \end{bmatrix}$$

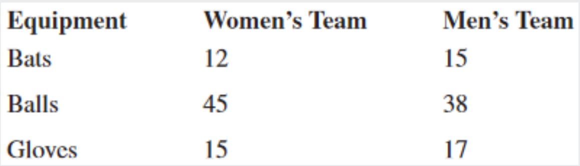
Using Gauss-Jordan elimination, you can rewrite this matrix as

$$[I \vdots X] = \begin{bmatrix} 1 & 0 & 0 & \vdots & -4 \\ 0 & 1 & 0 & \vdots & 2 \\ 0 & 0 & 1 & \vdots & 1 \end{bmatrix}$$

So, the solution of the matrix equation is

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} -1 \\ 2 \\ 1 \end{bmatrix}.$$

▼ Example 13 **Softball Team Expenses**



Equipment	Women's Team	Men's Team
Bats	12	15
Balls	45	38
Gloves	15	17

Each bat costs \$80, each ball costs \$6, and each glove costs \$60. Use matrices to find the total cost of equipment for each team.

Solution:

$$E = \begin{bmatrix} 12 & 15 \\ 45 & 38 \\ 15 & 17 \end{bmatrix} \quad \text{and} \quad C = [80 \quad 6 \quad 60].$$

$$\begin{aligned} CE &= [80 \quad 6 \quad 60] \begin{bmatrix} 12 & 15 \\ 45 & 38 \\ 15 & 17 \end{bmatrix} \\ &= [80(12) + 6(45) + 60(15) \quad 80(15) + 6(38) + 60(17)] \\ &= [2130 \quad 2448] \end{aligned}$$

So, the total cost of equipment for the women's team is \$2130, and the total cost of equipment for the men's team is \$2448.

📝

Ch 8.3 The Inverse of a Square Matrix (L)

The Inverse of a Matrix

Let A be an $n \times n$ matrix and let I_n be the $n \times n$ identity matrix. If there exists a matrix A^{-1} such that $AA^{-1} = I_n = A^{-1}A$ then A^{-1} is called the **inverse** of A.

Finding Inverse Matrices

If a matrix A has an inverse, then A is called **invertible** (or **nonsingular**).

A nonsquare matrix cannot have an inverse.

▼ Example 2 **Finding the Inverse of a Matrix**

Find the inverse of $A = \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}$.

Solution:

Solve the matrix equation $AX = I$ for X.

$$\begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix} \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} x_{11} + 4x_{21} & x_{12} + 4x_{22} \\ -x_{11} - 3x_{21} & -x_{12} - 3x_{22} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{cases} x_{11} + 4x_{21} & = 1 \\ -x_{11} - 3x_{21} & = 0 \end{cases} \qquad \begin{cases} x_{12} + 4x_{22} & = 0 \\ -x_{12} - 3x_{22} & = 1 \end{cases}$$

$x_{11} = -3$ and $x_{21} = 1$.

$x_{12} = -4$ and $x_{22} = 1$.

So, $X = A^{-1}$

$$= \begin{bmatrix} -3 & -4 \\ 1 & 1 \end{bmatrix}$$

The Inverse of a 2×2 Matrix

Only works for 2 x 2 matrices.

$$A^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

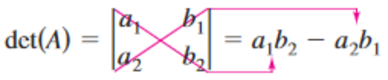
Systems of Linear Equations

If A is an invertible matrix, then the system of linear equations represented by $AX = B$ has a unique solution given $X = A^{-1}B$.

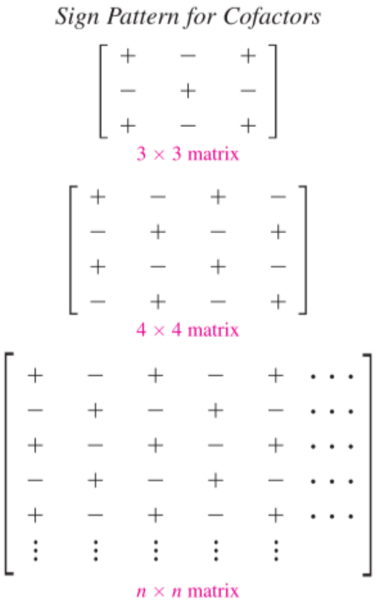
Ch 8.4 The Determinant of a Square Matrix (L)

The Determinant of a 2 x 2 Matrix

$A = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix} \quad \det(A) = |A| = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = a_1b_2 - a_2b_1.$



$\det(A) = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = a_1b_2 - a_2b_1$



Sign Pattern for Cofactors

$\begin{bmatrix} + & - & + \\ - & + & - \\ + & - & + \end{bmatrix}$

3 × 3 matrix

$\begin{bmatrix} + & - & + & - \\ - & + & - & + \\ + & - & + & - \\ - & + & - & + \end{bmatrix}$

4 × 4 matrix

$\begin{bmatrix} + & - & + & - & + & \cdots \\ - & + & - & + & - & \cdots \\ + & - & + & - & + & \cdots \\ - & + & - & + & - & \cdots \\ + & - & + & - & + & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \end{bmatrix}$

n × *n* matrix

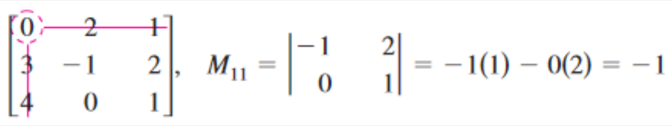
Minors and Cofactors

If A is a square matrix, then the **minor** M_{ij} of the entry a_{ij} is the determinant of the matrix obtained by deleting the *i*th row and the *j*th column of A. The **cofactor** C_{ij} of the entry a_{ij} is $C_{ij} = (-1)^{i+j} M_{ij}$.

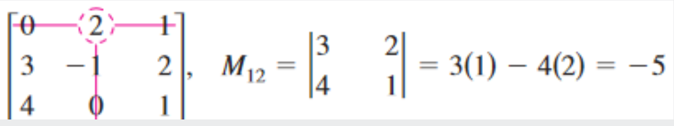
▼ Example 2 **Finding the Minors and Cofactors of a Matrix**

Find al the minors and cofactors of $A = \begin{bmatrix} 0 & 2 & 1 \\ 3 & -1 & 2 \\ 4 & 0 & 1 \end{bmatrix}$.

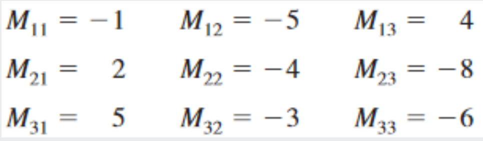
Solution:



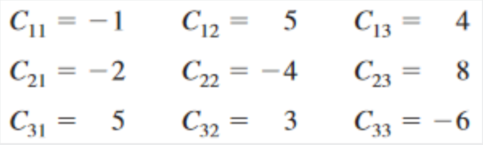
$\begin{bmatrix} 0 & 2 & 1 \\ 3 & -1 & 2 \\ 4 & 0 & 1 \end{bmatrix}, \quad M_{11} = \begin{vmatrix} -1 & 2 \\ 0 & 1 \end{vmatrix} = -1(1) - 0(2) = -1$



$\begin{bmatrix} 0 & 2 & 1 \\ 3 & -1 & 2 \\ 4 & 0 & 1 \end{bmatrix}, \quad M_{12} = \begin{vmatrix} 3 & 2 \\ 4 & 1 \end{vmatrix} = 3(1) - 4(2) = -5$



$M_{11} = -1$	$M_{12} = -5$	$M_{13} = 4$
$M_{21} = 2$	$M_{22} = -4$	$M_{23} = -8$
$M_{31} = 5$	$M_{32} = -3$	$M_{33} = -6$



$C_{11} = -1$	$C_{12} = 5$	$C_{13} = 4$
$C_{21} = -2$	$C_{22} = -4$	$C_{23} = 8$
$C_{31} = 5$	$C_{32} = 3$	$C_{33} = -6$

The Determinant of a Square Matrix

If A is a square matrix (of order 2 x 2 or greater), then the determinant of A is the sum of the entries in any row (or column) of A multiplied by their respective cofactors. Also called **expanding by cofactors**.

$|A| = a_{11}C_{11} + a_{12}C_{12} + \cdots + a_{1n}C_{1n}.$

▼ Example 3 **The Determinant of a 3 x 3 Matrix**

Find the determinant of $A = \begin{bmatrix} 0 & 2 & 1 \\ 3 & -1 & 2 \\ 4 & 0 & 1 \end{bmatrix}$.

$C_{11} = -1, \;\; C_{12} = 5, \;\; C_{13} = 4.$

So, by the definition of a determinant, you have

$$\begin{aligned} |A| &= a_{11}C_{11} + a_{12}C_{12} + a_{13}C_{13} \\ &= 0(-1) + 2(5) + 1(4) \\ &= 14 \end{aligned}$$

Ch 1.1 Systems of Linear Equations (K)

What does the term *linear equation* mean?

An equation is where two mathematical expressions are defined as being equal.

A set of linear equations is called a **linear system**.

Not linear equations:

a. $x^2 - 1 = 0$	*Quadratic equation, the power of x is 2*
b. $x + y^4 + \sqrt{z} = 9$	*The power of y is 4, and z is 1/2*
c. $\sin x - y + z = 3$	*Trigonometric function*

A system that has no solution is called **inconsistent**, whereas if it has at least one solution is called **consistent**.

Ch 1.2 Gaussian Elimination (K)

Reduced row echelon form (rref)

1. If there are any rows containing only zero entries, then they are located in the bottom part of the matrix
2. If the row contains non-zero entries, then the first non-zero entry is a 1 (leading 1)
3. The leading 1's of the two consecutive non-zero rows go strictly from top left to bottom right of the matrix
4. The only non-zero entry in a column containing a leading 1 is the leading 1

▼ Example 1.9

$\begin{bmatrix} 1 & 5 & -3 & \mid & -9 \\ 0 & -13 & 5 & \mid & 37 \\ 0 & 0 & 5 & \mid & -15 \end{bmatrix}$ into something like $\begin{bmatrix} 1 & 0 & 0 & \mid & * \\ 0 & 1 & 0 & \mid & * \\ 0 & 0 & 1 & \mid & * \end{bmatrix} \Rightarrow$ $\begin{bmatrix} 1 & 0 & 0 & \mid & 2 \\ 0 & 1 & 0 & \mid & -4 \\ 0 & 0 & 1 & \mid & -3 \end{bmatrix}$

📝

Ch 3.2.2 Revision of linear combination (K)

🗣️ Let $v_1, v_2, ...$ and v_n be vectors in a vector space. If a vector x can be expressed as $x = k_1v_1 + k_2v_2 + \cdots + k_nv_n$ (where k's are scalars), then we say x is a **linear combination** of the vectors $v_1, v_2, v_3 ...$ and v_n.

▼ Example 3.8

Let $v_1 = t^2 - 1, v_2 = t^2 + 3t - 5, v_3 = t$ be vectors in P_2.

Show that the quadratic polynomial $\mathbf{x} = 7t^2 - 15$ is a linear combination of $\{v_1, v_2, v_3\}$.

Solution:

$$\begin{aligned} k_1v_1 + k_2v_2 + \cdots + k_nv_n &= k_1(t^2 - 1) + k_2(t^2 + 3t - 5) + k_3t \\ &= (k_1 + k_2)t^2 + (3k_2 + k_3)t - (k_1 + 5k_2) \\ &= 7t^2 - 15 \end{aligned}$$

$$\begin{aligned} k_1 + k_2 &= 7 \\ 3k_2 + k_3 &= 0 \\ k_1 + 5k_2 &= 15 \end{aligned} \qquad 5v_1 + 2v_2 - 6v_3 = \mathbf{x} \qquad 5(t^2 - 1) + 2(t^2 + 3t - 5) - 6t = 7t^2 - 15$$

This conclude that x is a linear combination of $\{v_1, v_2, v_3\}$.

💡 A non-empty subset S containing vectors u and v is a subspace of a vector space V $\Leftrightarrow$ *(iff)* any linear combination $k\mathbf{u} + c\mathbf{v}$ is also in S (k and c are scalars).

▼ Example 3.9

Let S be the subset of vectors of the form $(x \;\; y \;\; 0)^T$ in the vector space $\mathbb{R}^3$. Show that S is a subspace of $\mathbb{R}^3$.

Using the above proposition, we need to show that any linear combination $k\mathbf{u} + c\mathbf{v}$ is in S for any vectors $\mathbf{u}$ and $\mathbf{v}$ in S.

It is clear that S is non-empty because the zero vector is in S. Let $u = (a \;\; b \;\; 0)^T$ and $v = (c \;\; d \;\; p)^T$ be in S. Then for real scalars k_1 and k_2 we have

$$\begin{aligned} k_1\mathbf{u} + k_2\mathbf{v} = k_1\begin{pmatrix} a \\ b \\ 0 \end{pmatrix} + k_2\begin{pmatrix} c \\ d \\ 0 \end{pmatrix} \\ = \begin{pmatrix} k_1a \\ k_1b \\ 0 \end{pmatrix} + \begin{pmatrix} k_2c \\ k_2d \\ 0 \end{pmatrix} = \begin{pmatrix} k_1a + k_2c \\ k_1b + k_2d \\ 0 \end{pmatrix} \end{aligned}$$

Hence $k_1\mathbf{u} + k_2\mathbf{v}$ is also in S.

Ch 30 Statistics (C)

Averages: the mean, median and mode

$$\text{mean} = \overline{x} = \frac{\text{sum of the values}}{\text{total number of values}} = \frac{\Sigma_{i=1}^{n} x_i}{n}$$

The **median** of a set of numbers is found by listing the numbers in ascending order and then selecting the value that lies halfway along the list.

The **mode** of a set of values is that value that occurs most often.

The variance and standard deviation

When calculating variance/standard deviation with group/class data, remember to use midpoint value instead of the original values for x_i.

$$\text{variance} = \frac{\Sigma_{i=1}^{n}(x_i - \overline{x})^2}{n}$$

$$\text{standard deviation} = \sqrt{\frac{\Sigma_{i=1}^{n}(x_i - \overline{x})^2}{n}}$$

Ch 31 Probability (C)

All probabilities lie in the range $[0, 1]$.

Complementary events

$\rightarrow$ one or the other must occur, each excludes the other

$\rightarrow$ The sum of the probabilities of the two complementary events must always equal 1 (*total probability*).

Calculating theoretical probabilities

$\rightarrow$ when the events are equally likely, fair, unbiased

When all events are equally likely

$$P\begin{pmatrix}\text{obtaining our} \\ \text{chosen event}\end{pmatrix} = \frac{\text{number of ways the chosen event can occur}}{\text{total number of possibilities}}$$

Calculating experimental probabilities

$\rightarrow$ when events are not equally likely

$$P\begin{pmatrix}\text{chosen event} \\ \text{occurs}\end{pmatrix} = \frac{\text{number of ways the chosen event occurs}}{\text{total number of times the experiment is repeated}}$$

Independent events

If events A and B are independent, then the probabilities of obtaining A and B is given by $P(A \text{ and } B) = P(A) \times P(B)$