AOU
الجامعة العربية المفتوحة
Arab Open University

Arab Open University
Faculty of Computer Studies

MT131 - Discrete Mathematics

4. Number Theory, Cryptography, and Matrices

The Integers and Division

Division:

Let $a, b \in \mathbf{Z}$ with $a \neq 0$.

- $a \mid b \equiv$ "*a* **divides** *b*".

We say that "*a* is a **factor** of *b*", "*a* is a **divisor** of *b*", and "*b* is a **multiple** of *a*".

- *a* does not divide *b* is denoted by $a \nmid b$.
- We can express $a \mid b$ using the quantifier

$$\exists c \ (b = ac), \text{ Domain} = \mathbf{Z}.$$

$3 \mid -12 \Leftrightarrow$ **True**, but $3 \mid 7 \Leftrightarrow$ **False**.

The Divides Relations

- For every a, b, $c \in \mathbf{Z}$, we have

  1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.
  2. If $a \mid b$, then $a \mid (bc)$.
  3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

Examples:

- $3 \mid 12$ and $3 \mid 9 \rightarrow 3 \mid (12 + 9) \rightarrow 3 \mid 21 \ (21 \div 3 = 7)$
- $2 \mid 6 \rightarrow 2 \mid (6 \times 3) \rightarrow 2 \mid 18 \ (18 \div 2 = 9)$
- $4 \mid 8$ and $8 \mid 64 \rightarrow 4 \mid 64 \ (64 \div 4 = 16)$

The Division Algorithm

- let a be an integer and d a positive integer, then there exist unique integers q and r such that:

$$a = d \times q + r \quad , 0 \leq r < d .$$

- d is called **divisor** and a is called **dividend.**
- q is the **quotient** and r is the **remainder** (**must be positive integer**).

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

Example

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

$$101 = 11 \times 9 + 2$$

$$\mathbf{q = 101 \text{ div } 11 = 9}$$

$$\mathbf{r = 101 \text{ mod } 11 = 2}$$

$$q = 101 \text{ div } 11 = \left\lfloor \frac{101}{11} \right\rfloor = \lfloor 9.18 \rfloor = 9$$

$$r = 101 - (9) \times 11 = 2$$

Examples

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

$$-11 = 3 \times (-4) + 1$$

$$q = -4 \,,\, r = 1$$

$$q = -11 \operatorname{div} 3 = \left\lfloor \frac{-11}{3} \right\rfloor = \lfloor -3.6 \rfloor = -4$$

$$r = -11 - (-4) \times 3 = 1 = -11 \bmod 3$$

- **Note**:

$-11 \neq 3 \times (-3) - 2$ **because** r **can't be negative.**

Examples

- Find a and b if :

$$2a + b = 46 \text{ mod } 7 \quad \text{and} \quad a + 2b = 47 \text{ div } 9.$$

$$46 = 6 \times 7 + \mathbf{4} \quad \text{and} \quad 47 = \mathbf{5} \times 9 + 2 \rightarrow$$

$$46 \text{ mod } 7 = 4 \quad \text{and} \quad 47 \text{ div } 9 = 5 \rightarrow$$

$$2a + b = 4 \text{ (1)}$$

$$a + 2b = 5 \text{ (2)}$$

By solving (1) and (2) for a and b,

$$\text{(1)} - 2\times\text{(2)} \longrightarrow -3b = -6 \longrightarrow b = 2 \text{ and } a = 1.$$

Modular Congruence

Theorem: Let a, $b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. We say that a **is congruent to** b **modulo** m written

$$a \equiv b \,(\text{mod } m),$$

if and only if

1) $a \text{ mod } m = b \text{ mod } m$, or

2) $m \mid (a - b)$ i.e. $(a - b) \text{ mod } m = 0.$

Examples

Is 17 congruent to 5 modulo 6?

$$17 \bmod 6 = 5 \quad \text{and} \quad 5 \bmod 6 = 5,$$

$$\text{also} \;\; 6 \mid (17 - 5) \leftrightarrow 6 \mid 12 \text{ where } 12 \div 6 = 2,$$

$$\text{then} \;\; 17 \equiv 5 \pmod{6}$$

Is 24 congruent to 14 modulo 6?

$$\text{Since,} \quad 24 \bmod 6 = 0 \text{ and } \; 14 \bmod 6 = 2,$$

$$\text{also } 6 \nmid (24 - 14) \leftrightarrow 6 \nmid 10,$$

$$\text{then, } 24 \not\equiv 14 \pmod{6}.$$

Useful Congruence Theorems

Let a, b, c, $d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$.

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

1) $a + c \equiv b + d \pmod{m}$, and

2) $ac \equiv bd \pmod{m}$

e.g. Let $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$ then:

$(7 + 11) \equiv (2 + 1) \pmod{5} \leftrightarrow 18 \equiv 3 \pmod{5}$ and

$(7 \times 11) \equiv (2 \times 1) \pmod{5} \leftrightarrow 77 \equiv 2 \pmod{5}$.

Cryptology

- Caesar’s encryption method can be represented by the function $f(p) = (p + 3) \bmod 26$, $0 \leq p \leq 25$. The letter “A” is replaced by 0, “B” by 1, …, and “Z” by 25.

Cryptology

e.g. What is the secret message produce from the message "GOOD MORNING ZERO"?

First replace the letters in the message with numbers

p : 6 14 14 3 12 14 17 13 8 13 6 25 4 17 14

Second replace p by $f(p) = (p + 3) \bmod 26$

$f(p)$: 9 17 17 6 15 17 20 16 11 16 9 2 7 20 17

Translate this back to letters produces the encrypted message

"JRRG PRUQLQJ CHUR "

- To recover the original message from a secrete message. The inverse function $f^{-1}(p) = (p - 3) \bmod 26$ can be used. This process is called **decryption**.

Cryptology

Example: Encrypt the message “STOP GLOBAL WARMING” using the encrypting function $f(x) = (x + 11)$ mod 26, $0 \leq x \leq 25$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

18 19 14 15   6 11 14 1 0 11   22 0 17 12 8 13 6.

Apply the shift $f(x) = (x + 11)$ mod 26, yielding

3 4 25 0   17 22 25 12 11 22   7 11 2 23 19 24 17.

Translating the numbers back to letters produces the cipher text

“DEZA RWZMLW HLCXTYR”

Cryptology

Example: Decrypt the message “LEWLYPLUJL PZ H NYLHA ALHJOLY” using the encrypting function $f(x) = (x + 7) \bmod 26$, $0 \leq x \leq 25$.

Solution: Replace each letter with the corresponding element of $\mathbf{Z}_{26}$.

11 4 22 11 24 15 11 20 9 11 15 25 7 13 24 11 7 0 0 11 7 9 14 11 24.

Shift each of the numbers by −7 modulo 26, yielding

4 23 15 4 17 8 4 13 2 4 8 18 0 6 17 4 0 19 19 4 0 2 7 4 17.

Translating the numbers back to letters produces the decrypted message

“EXPERIENCE IS A GREAT TEACHER”

Hashing Functions

Suppose that a computer has only the 20 memory locations 0, 1, 2, …, 19. Use the hashing function h where

$$h(x) = (x + 5) \bmod 20$$

to determine the memory locations in which 57, 32, and 98 are stored.

- **$h(57) = (57 + 5) \bmod 20 = 62 \bmod 20 = 2$**
- **$h(32) = 37 \bmod 20 = 17$**
- **$h(98) = 103 \bmod 20 = 3$**

Primes and Greatest Common Divisors

- A positive integer $p > 1$ is **prime** if the only positive factors of p are 1 and p.

Some primes: 2, 3, 5, 7, 11, 13, 17, ...

- Non-prime integer greater than 1 are called **composite**, because they can be **composed** by multiplying two integers greater than 1.

Fundamental Theorem of Arithmetic

- Every positive integer greater than 1 has a unique representation as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size. (tree or division)

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

$$641 = 641$$

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

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

↑

Prime Factorization

Theorem

- If n is a **composite** integer, then n has prime divisor $\leq \sqrt{n}$.

e.g. 49 → prime numbers less than $\sqrt{49}$ are 2, 3, 5, 7

16 → prime numbers less than $\sqrt{16}$ are 2, 3.

- An integer n is **prime** if it is not divisible by any prime $\leq \sqrt{n}$.

e.g. 13 where $\sqrt{13}$ = 3.6 so the prime numbers are 2, 3 but non of them divides 13 so 13 is prime.

Prime Factorization Technique

- To find the prime factor of an integer n :

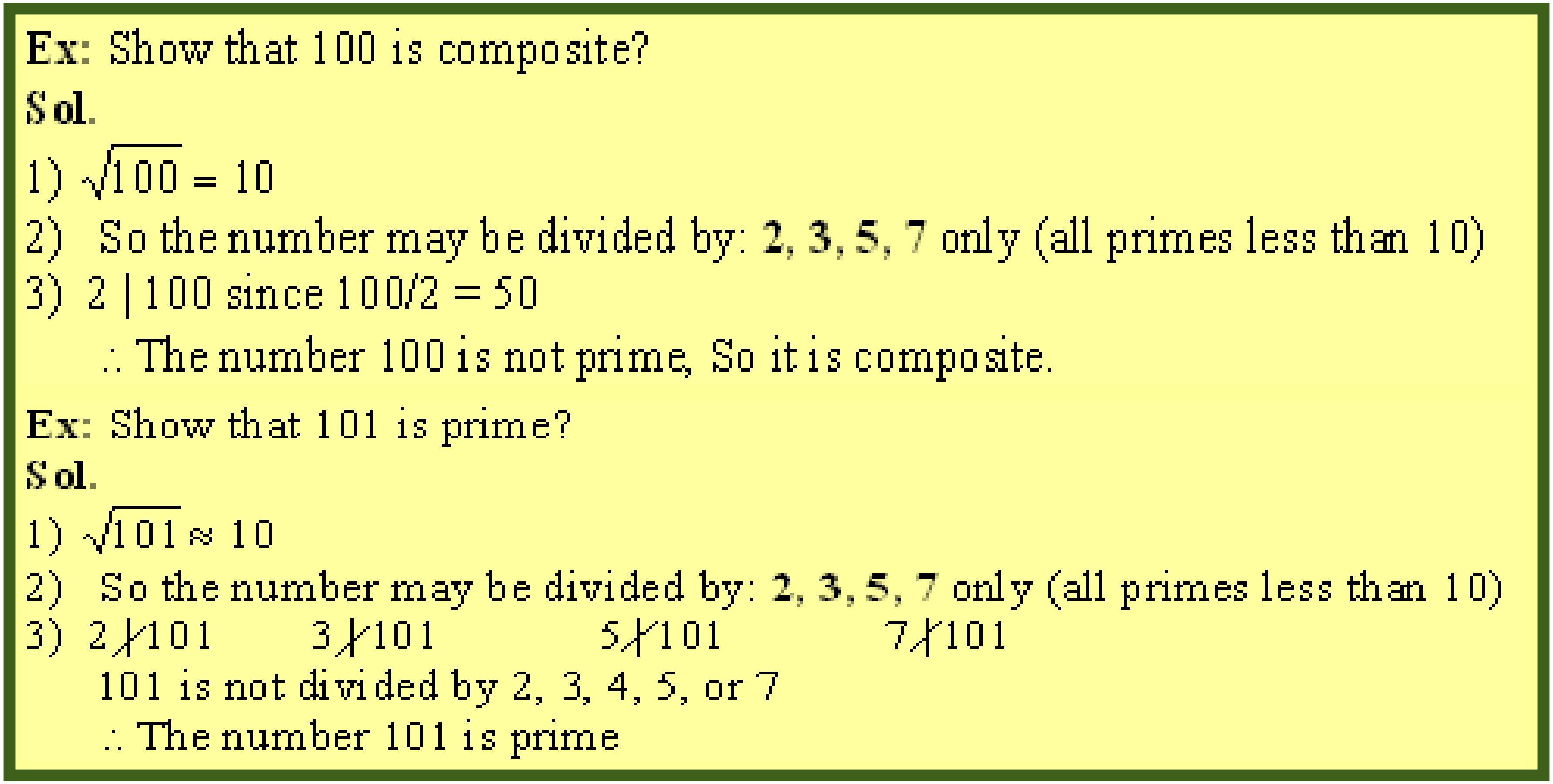
  1. Find $\sqrt{n}$.

  2. List all primes $\leq \sqrt{n}$,

     2, 3, 5, 7, … , up to $\sqrt{n}$.

  3. Find all prime factors that divides n.

Examples



Ex: Show that 100 is composite?

Sol.

1) $\sqrt{100} = 10$

2) So the number may be divided by: **2, 3, 5, 7** only (all primes less than 10)

3) $2 \mid 100$ since $100/2 = 50$

$\therefore$ The number 100 is not prime, So it is composite.

Ex: Show that 101 is prime?

Sol.

1) $\sqrt{101} \approx 10$

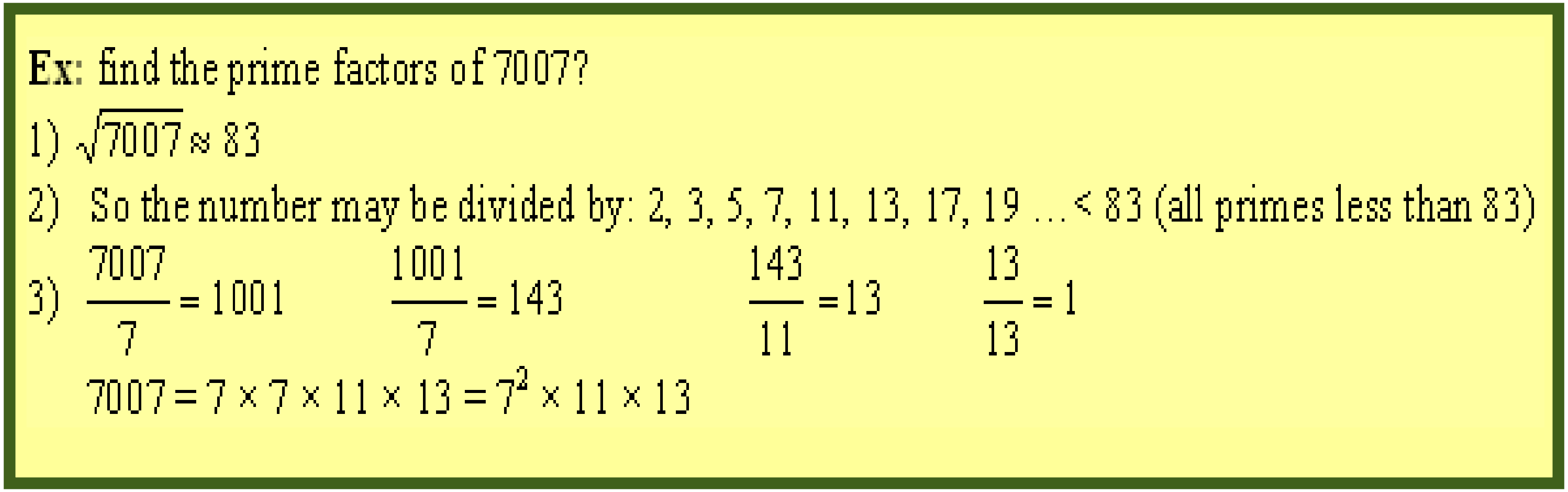
2) So the number may be divided by: **2, 3, 5, 7** only (all primes less than 10)

3) $2 \nmid 101$ $3 \nmid 101$ $5 \nmid 101$ $7 \nmid 101$

101 is not divided by 2, 3, 4, 5, or 7

$\therefore$ The number 101 is prime

Examples



Ex: find the prime factors of 7007?

1) $\sqrt{7007} \approx 83$

2) So the number may be divided by: 2, 3, 5, 7, 11, 13, 17, 19 …< 83 (all primes less than 83)

3) $\frac{7007}{7} = 1001 \qquad \frac{1001}{7} = 143 \qquad \frac{143}{11} = 13 \qquad \frac{13}{13} = 1$

$7007 = 7 \times 7 \times 11 \times 13 = 7^2 \times 11 \times 13$

Greatest Common Divisors

- The **greatest common divisor** gcd(a, b) of integers a, b (not both 0) is the largest (most positive) integer d that is a divisor both of a and of b.

- **To find gcd: 1. Find all positive common divisors of both *a* and *b*, then take the largest divisor:**

  e.g. Find gcd(24, 36)?

  Divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24

  Divisors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36

  Common divisors: 1, 2, 3, 4, 6, 12

  Maximum = 12, so gcd(24, 36) = 12

Ways to Find GCD

2. Use prime factorization:

Take the minimum power of common factors

Example: Find gcd(24, 180)

$24 = 2\times2\times2\times3 = 2^3\times3$

$180 = 2\times2\times3\times3 = 2^2\times3^2\times5$

$\text{gcd}(24, 36) = 2^{\min(3,2)}\times3^{\min(1,2)}\times5^{\min(0,1)} = 2^2\times3^1 = 12$

Examples

- Find gcd(360, 3500)?

  $360 = 2^3 \times 3^2 \times 5$

  $3500 = 2^2 \times 5^3 \times 7$

  $\therefore\ \gcd(360, 3500) = 2^2 \times 5 = 20$

- Find gcd(17, 22)?

  No common divisors so **gcd(17, 22) = 1** so, the numbers 17 and 22 are called **relatively prime.**

Least Common Multiple

- lcm(*a*, *b*) of positive integers, *a* and *b*, is the smallest positive integer that is a multiple both of *a* and of *b*.
- Find lcm(6, 10)?

Take the maximum power of all factors

$$6 = 2 \times 3\ ,\ 10 = 2 \times 5$$

$$\mathrm{lcm}(6, 10) = 2^{\max(1,1)}\times 3^{\max(1,0)}\times 5^{\max(0,1)} = 2\times3\times5 = 30$$

- Find lcm(24, 180)?

$$24 = 2^3 \times 3^1\ ,\quad 180 = 2^2 \times 3^2 \times 5$$

$$\therefore\ \mathrm{lcm}(24, 36) = 2^3 \times 3^2 \times 5 = 360.$$

Integers and Algorithms

Introduction:

The term algorithm originally referred to procedures for performing arithmetic operations using the decimal representations of integers. These algorithms, adapted for use with binary representations, are the basis for computer arithmetic.

Representations of Integers

In everyday life we use decimal notation to express integers.

For example, **965** is used to denote

$$\mathbf{9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0} .$$

However, it is often convenient to use bases other than 10.

Representations of Integers

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 positive integer greater than 1 as the base when expressing integers.

Binary Expansions (Binary to Decimal)

What is the decimal expansion of the integer that has $(101011111)_2$ as its binary expansion?

Solution: We have

$$
\begin{aligned}
(\mathrm{l}\ 01011111)_2 &= 1\cdot 2^8 + 0\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 \\
&\quad + 1\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2^1 + 1\cdot 2^0 \\
&= 256 + 64 + 16 + 8 + 4 + 2 + 1 \\
&= 351
\end{aligned}
$$

Hexadecimal Expansions

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

Any to Decimal

What are the decimal expansions of the of the hexadecimal number $(2AE0B)_{16}$ and $(3016)_7$?

Solution: We have

$$(2AE0B)_{16} = 2\cdot16^4 + 10\cdot16^3 + 14\cdot16^2 + 0\cdot16^1 + 11\cdot16^0 = (175627)_{10}\,.$$

$$(3016)_7 = 3\cdot7^3 + 0\cdot7^2 + 1\cdot7^1 + 6\cdot7^0 = (356)_{10}\,.$$

Base Conversion (Decimal to Any)

Find the binary expansion of $(241)_{10}$.

Solution: First divide 241 by 2 to obtain

$41 = 2 \cdot 120 + 1.$

Successively dividing quotients by 2 gives

$120 = 2 \cdot 60 + 0$

$60 = 2 \cdot 30 + 0$

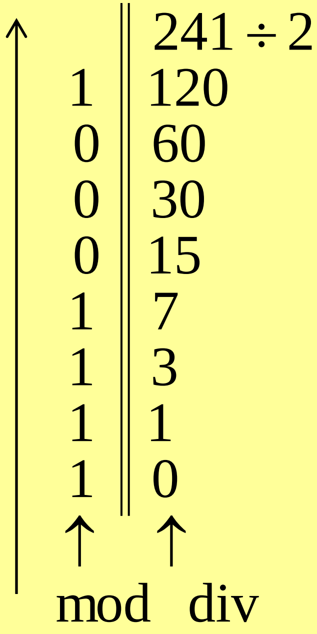
$30 = 2 \cdot 15 + 0$

$15 = 2 \cdot 7 + 1$

$7 = 2 \cdot 3 + 1$

$3 = 2 \cdot 1 + 1$

$1 = 2 \cdot 0 + 1$



	$241 \div 2$
1	120
0	60
0	30
0	15
1	7
1	3
1	1
1	0
↑	↑
mod	div

Therefore, $(241)_{10} = \overrightarrow{(11110001)}_2$

Decimal to Any

Find the base 8 expansion of $(12345)_{10}$.

Solution:

First, divide l2345 by 8 to obtain

$$12345 = 8 \cdot 1543 + 1.$$

Successively dividing quotients by 8 gives:

$$1543 = 8 \cdot 192 + 7,$$

$$192 = 8 \cdot 24 + 0,$$

$$24 = 8 \cdot 3 + 0,$$

$$3 = 8 \cdot 0 + 3.$$

	12345 ÷ 8
1	1543
7	192
0	24
0	3
3	0

Therefore, $(12345)_{10} = (30071)_8$.

Example

Find the hexadecimal expansion of $(177130)_{10}$.

Solution:

$$177130 = 16 \cdot 11070 + 10$$

$$11070 = 16 \cdot 691 + 14 \,,$$

$$691 = 16 \cdot 43 + 3 \,,$$

$$43 = 16 \cdot 2 + 11 \,,$$

$$2 = 16 \cdot 0 + 2.$$

	177130 ÷16
10	11070
14	691
3	43
11	2
2	0

Therefore, $(177130)_{10} = (2B3EA)_{16}$

Octal ↔ Binary ↔ Hexadecimal

Oct	Binary
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Hex	Binary
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
0	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

- $(307)_8 \rightarrow (011\ 000\ 111)_2$
- $(5B7)_{16} \rightarrow (0101\ 1011\ \ 0111)_2$
- $(1010011110\,1)_2$
  $= (0101,0011,1101)_2 \rightarrow (53D)_{16}$
- $(1010011110\,1)_2$
  $= (010,100,111,101)_2 \rightarrow (2475)_8$
- $(607)_8 \rightarrow (110,000,111)_2$
  $= (0001,1000,0111)_2 \rightarrow (1A7)_{16}$

Zero-One Matrices

All elements of a zero-one matrix are 0 or 1, representing **False** & **True** respectively.

e.g.

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

Zero-One Matrix Operations

- The join of A and B (both $m \times n$ zero-one matrices) is

$$A \vee B :\equiv [a_{ij} \vee b_{ij}].$$

- The meet of A and B (both $m \times n$ zero-one matrices) is:

$$A \wedge B \equiv [a_{ij} \wedge b_{ij}].$$

Example

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

- The join between A and B is $A \vee B = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$
- The meet between A and B is $A \wedge B = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

Boolean Products

Let $A = [a_{is}]$ *be an* $m \times k$ *zero-one matrix, and* $B = [b_{sj}]$ *be an* $k \times n$ *zero-one matrix.*

The ***Boolean Product*** *of* A *and* B, *denoted by* $A \odot B$, *is the* $m \times n$ *zero-one matrix with (i,j)th entry defined by:*

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

Example

Let $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$

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

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

Boolean Powers

- For a square zero-one matrix *A*, and any $k \geq 0$, the k^{th} Boolean power *of A* is simply the Boolean product of *k* copies of *A*.

$$A^{[k]} \equiv \underbrace{A \odot A \odot \ldots \odot A}_{k \text{ times}}$$

Example

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

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

Example

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

$$\mathbf{A}^{[2]} = \mathbf{A} \odot \mathbf{A} = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \mathbf{A}^{[3]} = \mathbf{A}^{[2]} \odot \mathbf{A} = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

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

$$\mathbf{A}^{[5]} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \mathbf{A}^{[\mathbf{n}]} = \mathbf{A}^{\mathbf{5}} \quad \text{for all positive integers } n \text{ with } n \geq 5.$$