

Chapter 3 The Fundamentals: Algorithms, Integers, and Matrices

[Section 3.4 The Integers and Division](#)

[Section 3.5 Primes and Greatest Common Divisors](#)

[Section 3.6 Integers and Algorithms](#)

[Section 3.8 Matrices](#)

Section 3.4 The Integers and Division

Part of number theory.

Division

- Definition: If a and b are integers with $a \neq 0$, we say a divides b if there exists integer c such that $b = ac$. Then a is also called a factor of b and b is a multiple of a .
- Notation : $a \mid b$
- **Example 1, page 201**: 3 divides 12, since $12 = (3)(4)$. 12 is a multiple of 3; 3 is a factor of 4. (However 3 does not divide 7.)
- **Theorem 2: The Division Algorithm**: Let a be an integer and d be a positive integer. Then there are unique integers q and r , with $0 \leq r < d$, such that $a = dq + r$.

Example 3: $a = 101, d = 11$ $101 = 11(9) + 2$

Definition 3:

- | | |
|-------------------------------|-----------------|
| ○ d is the divisor | 11 is divisor |
| ○ a is the dividend | 101 is dividend |
| ○ q is the quotient | 9 is quotient |
| ○ r is the remainder | 2 is remainder |

We write $q = a \text{ div } d$, and $r = a \text{ mod } d$.

In Example 3, $9 = 101 \text{ div } 11$ and $2 = 101 \text{ mod } 11$.

- **Example 4, page 203**. Since $-11 = 3(-4) + 1$. Thus $-11 \text{ div } 3 = -4$ and $-11 \text{ mod } 3 = 1$. (**Note remainder can never be negative!**).

Thus we do **NOT** choose to use $-11 = 3(-3) - 2$ because this would give us a negative remainder (-2).

Modular Arithmetic

- **Definition:** Let a, b be integers, m a positive integer.
 - We say **a is congruent to b modulo m** if m divides $a - b$.
 - Notation: $a \equiv b \pmod{m}$
 - Another way of determining: a is congruent to b modulo m if $a - b = k*m$ or $a = b + k*m$
 - $a \equiv b \pmod{m}$ if and only if $b \equiv a \pmod{m}$
- **Theorem 3:** Two numbers a and b are congruent mod m if and only if $a \pmod{m} = b \pmod{m}$ (i.e. they have the same remainder upon division by m).
- 23 is congruent to 7 modulo 4. Also 7 is congruent to 23 modulo 4.
- 24 and 14 are NOT congruent modulo 6.
- **Important Applications of Congruencies -- Hashing Functions (Example 7), Random number generation (Example 8), and Cryptology (Example 9)**

Section 3.5 Primes and Greatest common Divisors

- **Definition: Prime number.** A positive integer $p > 1$ is prime if the only factors of p are 1 and p ; otherwise it is called composite.
 - 2, 5, 7, 13 are prime. 4, 8, 9, 121 are composite.
- **Fundamental Theorem of Arithmetic:** Every positive integer can be written uniquely as the product of primes.
 - See example 4 for some prime factorizations.
- **Theorem 2:** If n is a composite integer, then n has a prime divisor less than or equal to the square root of n .
 - Proof: (Note that this is a proof by contradiction)
Let $n = ab$. At least one of the factors must be less than the square root of n , since: Suppose both were greater square root of n . Then the product ab is greater than (square root of n) * (square root of n) = n -- which is a contradiction!
- **Example 5:** Show that 101 is prime. Test primes \leq square root of 101 to see if they are factors:
 - 2, 3, 5, 7 are not factors. The next prime is 11 which is $>$ square root of 101.
- **Example 6:** Find the prime factorization of 7007. Test successive primes for factors.
 - $7007 = 7 * 1001$.
 - Test 7 again as a factor of 1001
 - $7007 = 7*7*143$.
 - 7 is not a factor of 143.

- Test next prime 11 as a factor of 143.
- $7007 = 7 \cdot 7 \cdot 11 \cdot 13$. (13 is prime so done)

Prime factorization is important in the theory and applications of cryptology.

Primes go on forever -- That is to say no matter how large an integer you choose you will be able to find a prime that is bigger than that integer.

Mersenne Primes: Primes of the form $2^p - 1$, where p is also prime. There is an efficient test for determining whether integers of this form are prime (Lucas-Lehmer test). There are not efficient tests for determining in general whether a large integer is prime. $7 = 2^3 - 1$ is a Mersenne Prime.

Twin Primes are primes that differ by 2. Examples are 7 and 11; 17 and 19; 4967 and 4969.

Greatest Common Divisor and Least Common Multiples

- **Definition:** The *greatest common divisor* of two non-zero integers a and b , $\gcd(a,b)$ is the largest integer that divides both.
- **Definition:** Two integers are **relatively prime** if their gcd is 1.
- **Definition:** The **least common multiple** of two positive integers a and b , $\text{lcm}(a,b)$ is the smallest integer that is divisible by both a and b .
- **Example 14:** To compute the gcd of two integers:
 - Find the prime factorization of each.
 - Form the gcd as the product of the smaller power of every prime that appears both factorizations
 - $120 = 2^3 \cdot 3 \cdot 5$; $500 = 2^2 \cdot 5^3$.
 - $\gcd = 2^2 \cdot 5$;
- **Example 15:** To compute the lcm of two integers:
 - Find the prime factorization of each.
 - Form the lcm as the product of the higher power of every prime that appears in one or the other (or both) factorizations.
 - $\text{lcm}(2^3 \cdot 3^5 \cdot 7^2, 2^4 \cdot 3^3) = 2^4 \cdot 3^5 \cdot 7^2$
- **Theorem 5:** For positive integers a, b ,
 $ab = \gcd(a, b) \cdot \text{lcm}(a,b)$

Section 3.6 Integers and Algorithms

Representation of integers in bases other than 10

- **Theorem 1:** (Representing a number in any base b , where b is a positive integer greater than 1). Any number n can be written uniquely in the form

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

where k is nonnegative integer, and a_k, a_{k-1}, a_1, a_0 are nonnegative integers less than b .

Examples: $b = 10$

$$2301 = 2 \cdot 10^3 + 3 \cdot 10^2 + 0 \cdot 10 + 1$$

$b = 2$

$$24 = 1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 0 \cdot 1$$

Thus the binary (base 2) representation for 24 is

$$(1\ 1\ 0\ 0\ 0)_2$$

- **Hexadecimal Expansion: Base 16.**
Digits 0-9 and A, B, C, D, E (for 10 through 15)
- **Examples 3, 4, 5** show algorithm to convert base 10 to other bases (such as 8)

Algorithm constructing expansion (page 221):

- Divide the number by base -- remainder will be rightmost digit.
- Divide the resulting quotient by base -- remainder will be the next rightmost digit.
- Keep doing this until q quotient of 0 is obtained.

Pseudocode page 221 bottom

Example 6: Converting between hexadecimal, octal, and binary.

From binary to hexadecimal:

Group into blocks of four (from right -- adding 0's to left if necessary).

Convert each block of four binary digits into corresponding hexadecimal number (see Table 1, page 222)

Skip sections for Algorithms for Integer Operations and Modular Exponentiation

The Euclidean Algorithm

- An algorithm for finding the **gcd** of two numbers. Oldest known algorithm (Euclid -- 325-265 BCE)
 - Method:
 - To find the greatest common divisor of two numbers a and b , where $a > b$. (Say $a = 287$, $b = 91$):
 - Write $a = bq + r$.
 - If r is 0, then $\text{gcd} = b$ (why?)
 - Otherwise $\text{gcd}(a,b)$ will be $\text{gcd}(b,r)$ (Proven in Lemma 1 -- we won't cover the proof)
 - So repeat the above process to compute $\text{gcd}(b,r)$.
 - Keep doing this until a remainder of 0 is obtained.

- The gcd will then be the final value of b .
- **Example 12** page 229 $\text{gcd}(414, 662) = 2$.

Section 3.8 Matrices

This section provides a foundation for work in future chapters.

- **Matrix:** Rectangular array of numbers
- **Dimension of matrix** is $m \times n$, where m is the number of rows and n is the number of columns in the matrix.
- **Example 1** gives a 3×2 matrix.
- Matrices are normally represented with capital letters (A, B, C).
- Individual elements or entries of arrays are referenced by their row and column index.
- a_{ij} is the element in the i th row and j th column.

Matrix Arithmetic

- **Matrix Addition:** If matrices A and B are both $m \times n$ matrices, then the $m \times n$ matrix $A + B$ is the matrix obtained by adding the elements in the corresponding rows and columns of A and B.
- **Matrix Multiplication:** The product AB , of two matrices A and B, is defined when A is $m \times k$ and B is $k \times n$. In this case the product is an $m \times n$ matrix obtained by calculating the ij 'th element, c_{ij} , of AB as
 - c_{ij} = the sum of the products of the corresponding elements from the i th row of A and the j th column of B.
- **Example 3** shows the computation of the product of 4×3 matrix A and 3×2 matrix B. Note that the product BA does not exist.
- **Example 4** shows matrix multiplication is not commutative. (AB is not in general equal to BA)
- Algorithm 1, page 249 gives a pseudocode representation for a straightforward matrix multiplication algorithm.
 - The number of additions and multiplication's required for this algorithm can be calculated as follows: To calculate one entry in the product matrix, we must perform k multiplications and $k-1$ additions. There are $m*n$ entries in the matrix.
 - Thus the total number of multiplications is $m*k*n$ and the total number of additions is $m*n*(k-1)$.
 - If A and B are both $n \times n$ matrices, the total number of multiplications is n^3 and the total number of additions is n^3-n^2
 - Thus as a function of n , the total number of additions and multiplications for AXB is $2n^3-n^2$, which is $O(n^3)$. We therefore say that this has time complexity $O(n^3)$.
- Matrix multiplication is **associative** -- that is $(A_1A_2)A_3 = A_1(A_2A_3)$.
- Which order requires the least number of multiplications?

- **Example 6:** Assuming dimensions are A_1 is 30×20 , A_2 is 20×40 , and A_3 is 40×10 .
 - Resulting matrix is 30×10 .
 - $(A_1A_2)A_3$: 36000 total since:
 - To calculate A_1A_2 , a 30×40 matrix, requires $30 \times 20 \times 40 = 24000$ multiplications.
 - To calculate the product of A_1A_2 and A_3 requires $30 \times 40 \times 10 = 12000$ multiplications.
 - $A_1(A_2A_3)$: 14000 total since:
 - To calculate A_2A_3 , a 20×10 matrix, requires $20 \times 40 \times 10 = 8000$ multiplications.
 - To calculate the product of A_1 and A_2A_3 requires $30 \times 20 \times 10 = 6000$ multiplications.

Transposes and Powers of Matrices

- The $n \times n$ Identity Matrix I_n : i,j 'th element is 1 if $i = j$, 0 otherwise.
- If A is an $m \times n$ matrix, then $A I_n = I_m A = A$.
- A **square matrix** is an $n \times n$ matrix.
- Powers of square matrices: $A^0 = I_n$. $A^n = A A A \dots A$ (n -times).
- A^t denotes the **transpose** of a matrix A : A^t is obtained from A by interchanging the rows and columns. That is the i,j 'th element of A^t is the j,i 'th element of A .
- See **Example 7**.
- A square matrix A is **symmetric** if $A = A^t$.

Zero-One Matrices: Matrices whose entries are either 0 or 1.

- Boolean operations:
 - join of a zero-one matrix is the 'OR'ing of corresponding elements
 - meet of a zero-one matrix is the 'AND'ing of the corresponding elements.
 - Boolean product of two matrices A and B is like multiplication except we compute the "OR" (instead of $+$) of the "AND" (instead of product) of corresponding elements in the i th row of A and j 'th column of B
- See **Examples 9 and 10, page 252-253**