Heaven's light is our guide"

Rajshahi University of Engineering & Technology
Department of Computer Science & Engineering

Discrete Mathematics
Course No. : CSE 2101
Chapter 3: The Fundamentals: Algorithms, the Integers and Matrices
Prepared By : Julia Rahman

3.2 The Growth of Functions

3.2 The Growth of Functions

The Big-O Notation

Definition 1:

- ✓ Let f and g be functions from integers or real numbers to real numbers. We say that f(x) is O(g(x)) if there are constants C and k such that
  $|f(x)| \leq C|g(x)|$
  whenever $x>k$.
- ✓ "f(x) is big-oh of g(x)"
- ✓ witnesses: C, k

Another Definition

- ✓ Let f and g be functions from N to R.

  Then g asymptotically dominates f, denoted f is O(g) or 'f is big-O of g,' or 'f is order g,' iff

  $$\exists k\ \exists C\ \forall n\ [n > k \rightarrow |f(n)| \leq C\ |g(n)|]$$

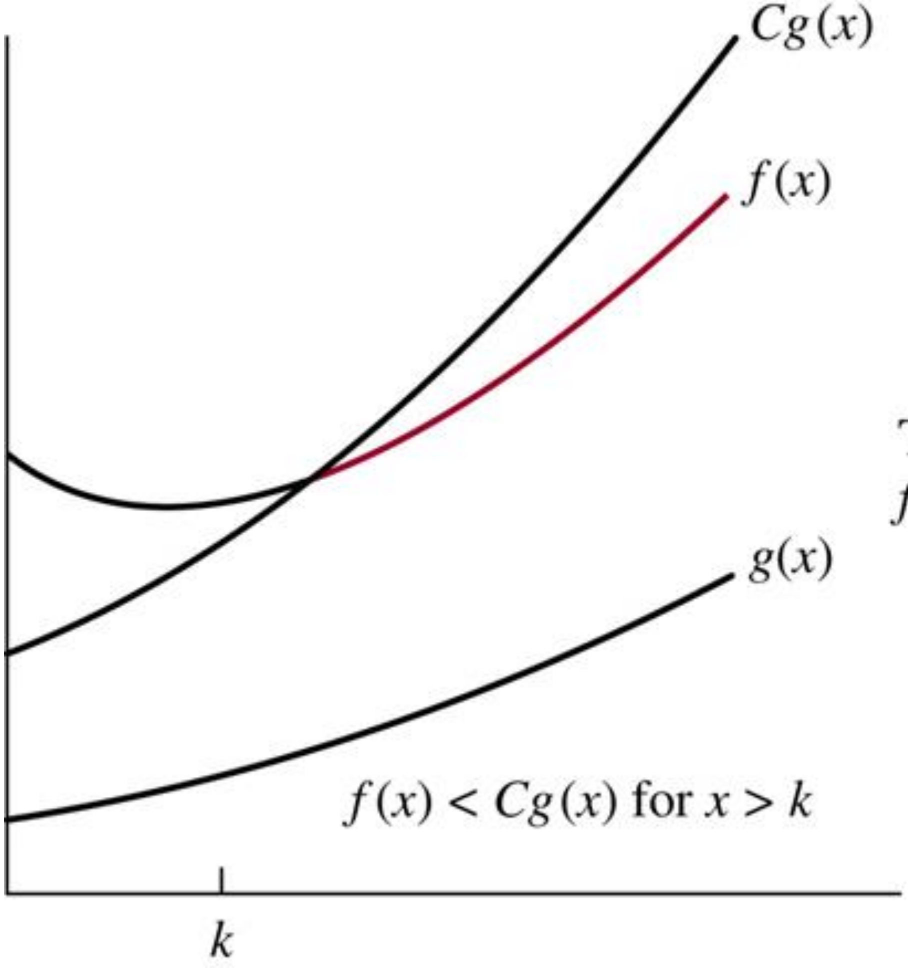
  Note:

  Choose k

  Choose C; it may depend on your choice of k

  Once you choose k and C, you must prove the truth of the implication (often by induction)

3.2 The Growth of Functions



The part of the graph of $f(x)$ that satisfies $f(x) < Cg(x)$ is shown in color.

FIGURE 2 The Function $f(x)$ is $O(g(x))$.

3.2 The Growth of Functions

- **Example 1: S**how that f(x)= x^2+ 2x + 1 is O(x^2)

  Solution : Since

  $$x^2+2x+1 \le x^2+2x^2+x^2 = 4x^2$$

  whenever $x > 1$, it follows that $f(x)$ is $O(x^2)$

  take $C = 4$ and $k = 1$

  Another :

  If $x > 2$, we see that

  $$x^2+2x+1 \le x^2+x^2+x^2 = 3x^2$$

  take $C = 3$ and $k = 2$

- **Example 2:** Show that $7x^2$ is O(x^3).

  Solution: When x > 7,

  then $7x^2 < x^3$ (multiplying both sides of x > 7 by x^2 .)

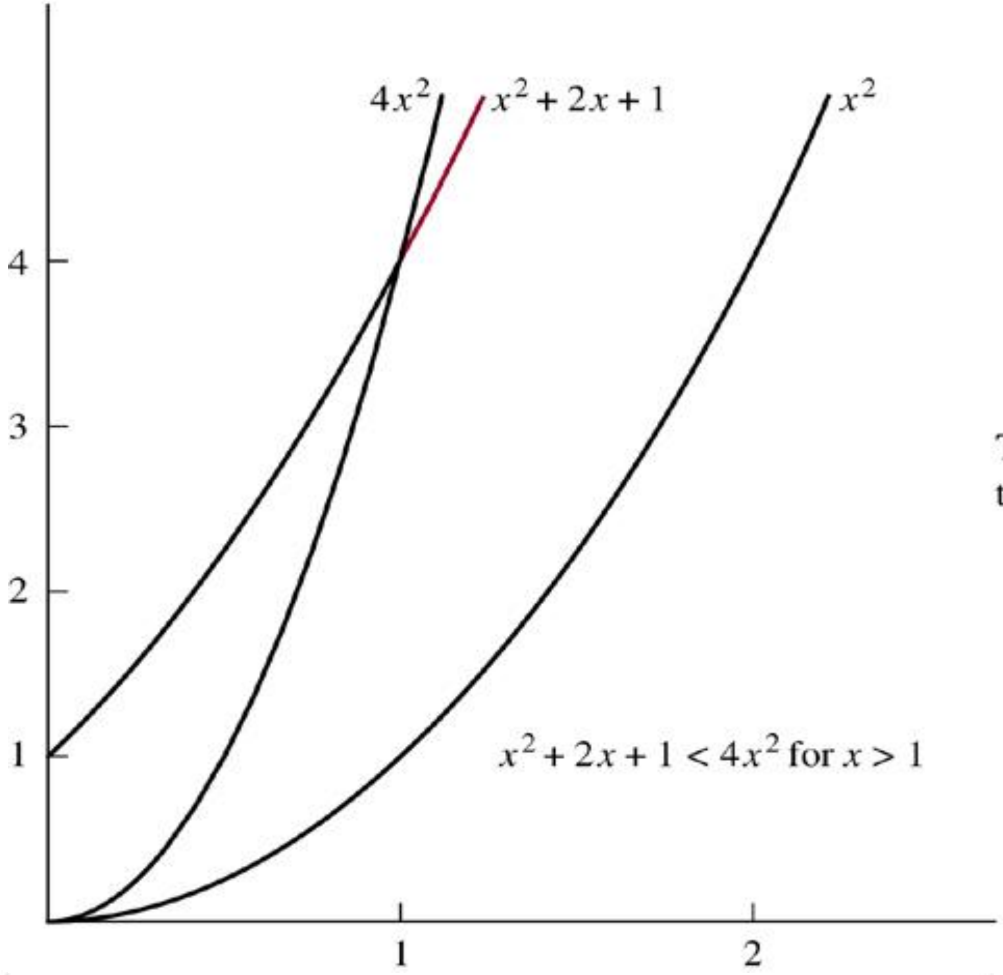
  take C = 1 and k = 7 as witnesses to establish the relationship $7x^2$ is O (x^3).

  Alternatively,

  when x > 1 , we have $7x^2 < 7x^3$,

  so that C = 7 and k = 1 are also witnesses to the relationship $7x^2$ is O (x^3).

3.2 The Growth of Functions



The part of the graph of $f(x) = x^2 + 2x + 1$ that satisfies $f(x) < 4x^2$ is shown in color.

FIGURE 1 The Function $x^2 + 2x + 1$ is $O(x^2)$.

3.2 The Growth of Functions

- **Example 3:** show that n^2 is not O(n).

  Solution: To show that n^2 is not O (n),

  - ✓ Must show no pair of constants C and k exist such that $n^2 \leq Cn$ whenever $n > k$.
  - ✓ To see that there are no such constants,

    when $n > 0$ and $n^2 \leq Cn$

    equivalent $n \leq C$ (dividing both sides by n) .
  - ✓ Now see that no matter what C and k are, the inequality $n \leq C$ cannot hold for all n with $n > k$.
  - ✓ In particular, once set a value of k, see that when n is larger than the maximum of k and C , it is not true that $n \leq C$ even though $n > k$.

- **Example 4:** Is it also true that x^3 is $O(7x^2)$?

  Solution: To determine whether x^3 is $O(7x^2)$,

  - ✓ Need to determine constants C and k such that $x^3 \leq C\,(7x^2)$ where $x > k$.
  - ✓ $x^3 \leq C(7x^2)$ is equivalent to $x \leq 7C$, (dividing the inequality by x^2).
  - ✓ No C exists for which $x \leq 7C$ for all $x > k$, because x can be made arbitrarily large.
  - ✓ It follows no witnesses C and k exist for this proposed big-O relationship. Hence, x^3 is not $O(7x^2)$.

3.2 The Growth of Functions

- **Properties of Big-O:**
  - ✓ f is O(g) if and only if $O(f) \subseteq O(g)$
  - ✓ If f is O(g) and g is O(f) then O(f) = O(g)
  - ✓ The set O(g) is closed under addition :

    If f is O(g) and h is O(g) then f + h is O(g)
  - ✓ The set O(g) is closed under multiplication by a scalar *a* (real number):
    - ▪ If f is O(g) then a*f is O(g)
    - ▪ that is,

      O(g) is a vector space.
  - ✓ if f is O(g) and g is O(h), then f is O(h).
    - ✓ In particular

      $O(\ f\ ) \subseteq O(g) \subseteq O(h)$

3.2 The Growth of Functions

Some Important Big-O Results

- **Theorem 1:** Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_{n-1}, a_n$ are real numbers. Then, $f(x)$ is $O(x^n)$.

  Proof: Using the triangle inequality, if x > 1 we have

  $$\begin{aligned} |f(x)| &= |a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0| \\ &\leq |a_n| x^n + |a_{n-1}| x^{n-1} + \ldots + |a_1| x + |a_0| \\ &= x^n \left(|a_n| + |a_{n-1}| / x + \ldots + |a_1| / x^{n-1} + |a_0| / x^n\right) \\ &\leq x^n \left(|a_n| + |a_{n-1}| + \ldots + |a_1| + |a_0|\right) \end{aligned}$$

  This shows that $|f(x)| \leq Cx^n$

  where $C = |a_n| + |a_{n-1}| + \ldots + |a_1| + |a_0|$ whenever x > 1 . Hence, the witnesses $C = |a_n| + |a_{n-1}| + \ldots + |a_1| + |a_0|$ and k = 1 show that f(x) is O (x^n).

- **Example 5:** How can big-*O* notation be used to estimate the sum of the first n positive integers?

  Solution: Because each of the integers in the sum of the first n positive integers does not exceed n, it follows that

  $$1 + 2 + \ldots + n \leq n + n + \ldots + n = n^2$$

  From this inequality, it follows that 1 + 2 + 3 + . . . + n is O(n^2), taking C = 1 and k = 1 as witnesses.

3.2 The Growth of Functions

The Growth of Combinations of Functions

- *1*
- log*n*
- *n*
- *n* log *n*
- n^2
- 2^n
- *n!*

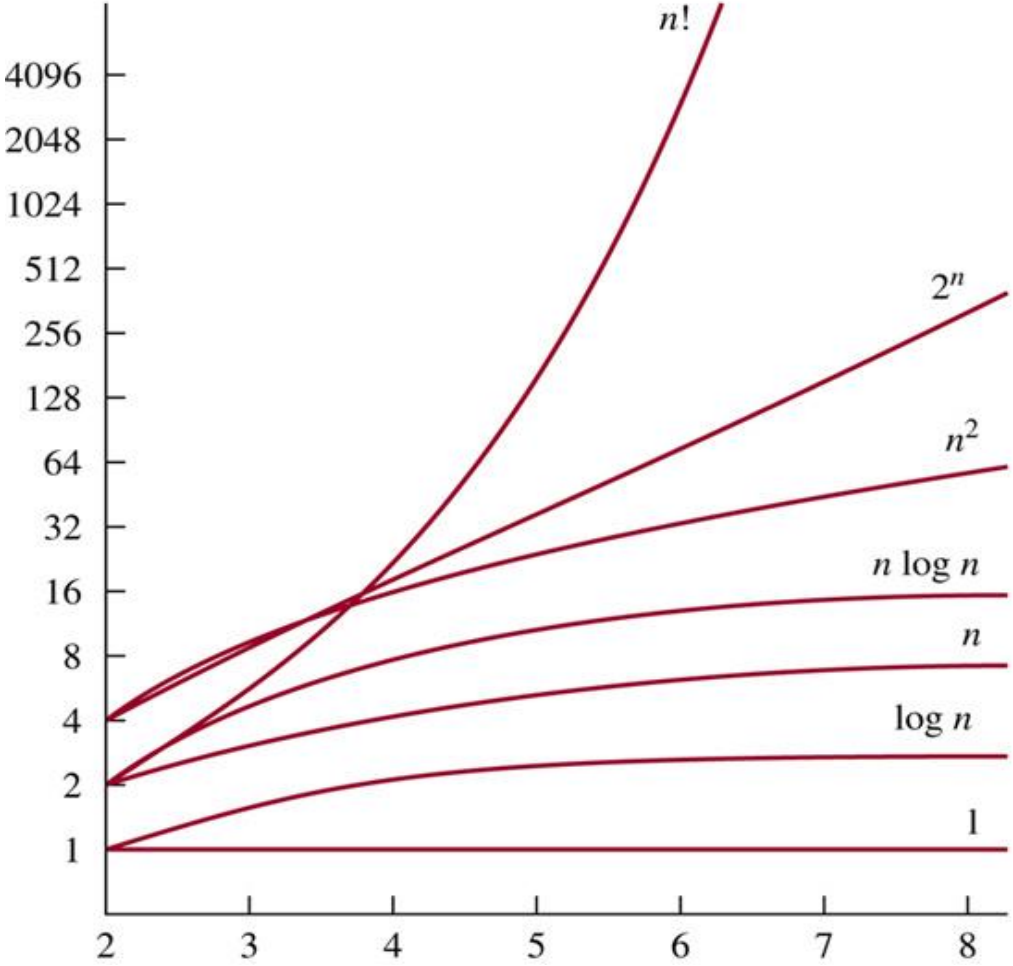


FIGURE 3 A Display of the Growth of Functions Commonly Used in Big-*O* Estimates.

3.2 The Growth of Functions

- Suppose that $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$. From the definition of big- O notation, there are constants C_1, C_2 , k_1 and k_2 such that

  $|f_1(x)| \leq C_1|g_1(x)|$ when $x > k_1$ and

  $|f_2(x)| \leq C_2|g_2(x)|$ when $x > k_2$ and

  To estimate the sum o f $f_1(x)$ and $f_2(x)$, note that

  $$\left|(f_1 + f_2)(x)\right| = \left|f_1(x) + f_2(x)\right|$$

  $$\leq |f_1(x)| + |f_2(x)| \text{ using the triangle inequality } \left|a+b\right| \leq |a| + |b|$$

When x i s greater than both k_1 and k_2 , it follows from the inequalities for $f_1(x)$ and $f_2(x)$ that

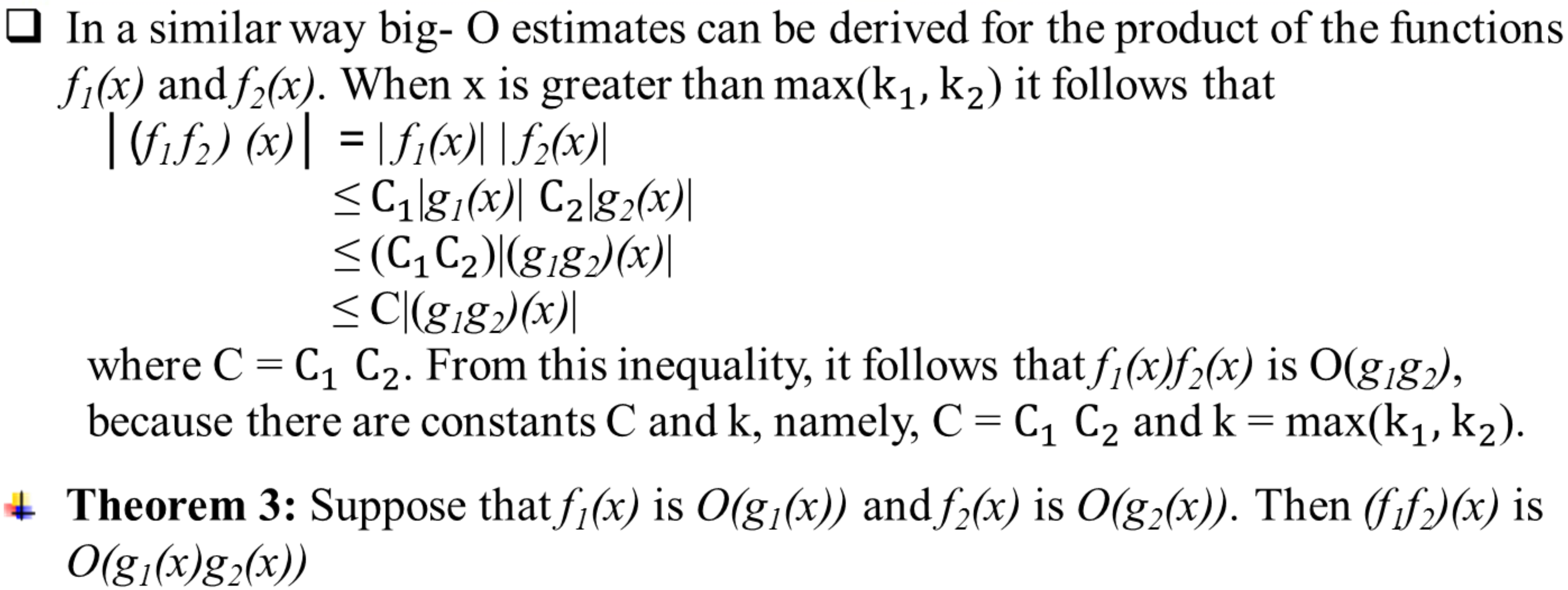
$$|f_1(x)| + |f_2(x)| \leq C_1|g_1(x)| + C_2|g_2(x)|$$
$$\leq C_1|g(x)| + C_2|g(x)|$$
$$= (C_1 + C_2)|g(x)|$$
$$= C|g(x)|$$

where $C = C_1 + C_2$ and $g(x) = \max(|g_1(x)|, |g_2(x)|)$.

- **Theorem 2:** Suppose that $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$. Then $(f_1+f_2)(x)$ is $O(max(|g_1(x)|, |g_2(x)|))$

- **Corollary 1:** Suppose that $f_1(x)$ and $f_2(x)$ are both $O(g(x))$. Then $(f_1+f_2)(x)$ is

3.2 The Growth of Functions



- In a similar way big- O estimates can be derived for the product of the functions $f_1(x)$ and $f_2(x)$. When x is greater than max(k_1, k_2) it follows that

$$\begin{aligned} \left|(f_1 f_2)\ (x)\right| &= |\,f_1(x)|\ |\,f_2(x)| \\ &\leq C_1|g_1(x)|\ C_2|g_2(x)| \\ &\leq (C_1C_2)|(g_1g_2)(x)| \\ &\leq C|(g_1g_2)(x)| \end{aligned}$$

where C = C_1 C_2. From this inequality, it follows that $f_1(x)f_2(x)$ is O(g_1g_2), because there are constants C and k, namely, C = C_1 C_2 and k = max(k_1, k_2).

- **Theorem 3:** Suppose that $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$. Then $(f_1f_2)(x)$ is $O(g_1(x)g_2(x))$

3.2 The Growth of Functions

Big-Omega and Big-Theta Notation

- Big-O notation does not provide a lower bound for the size of f(x) for large x .
- For this, big-Omega (big-Ω) notation is used.
- When we want to give both an upper and a lower bound on the size of a function f(x), relative to a reference function g(x), we use big-Theta (big-Θ) notation.
- **Definition 2:**

  Let *f* and *g* be functions from integers or real numbers to real numbers. We say that *f(x)* is *Ω(g(x))* if there are positive constants *C* and *k* such that

  $|f(x)| \geq C|g(x)|$

  whenever $x>k$.

  "f(x) is big-Omega of g(x)"
- **Example 10 :**The function $f(x) = 8x^3 + 5x^2 + 7$ is Ω(g(x)) , where g(x) is the function $g(x) = x^3$.

  This is easy to see because $f(x) = 8x^3 + 5x^2 + 7 \geq x^3$ for all positive real numbers x.

  This is equivalent to saying that $g(x) = x^3$ is $O(8x^3 + 5x^2 + 7)$,which can be established directly by turning the inequality around.

3.2 The Growth of Functions

- **Definition 3:**

  Let *f* and *g* be functions from integers or real numbers to real numbers. We say that *f(x)* is *Θ(g(x))* if f(x) is O(g(x)) and f(x) is *Ω(g(x))*.

  "f(x) is big-Theta of g(x)"

  "f(x) is of order g(x)

  f(X) is *Θ(g(x))*, then g(x) is*Θ(f(x))*

- **Example 12:** Show that $3x^2 + 8x(\log x)$ is $\Theta(x^2)$.

  Solution: Because $0 \leq 8x \log x \leq 8x^2$, it follows that $3x^2 + 8x \log x \leq 11x^2$ for $x > 1$. Consequently, $3x^2 + 8x \log x$ is O (x^2). Clearly, x^2 is O $(3x^2 + 8x \log x)$. Consequently, $3x^2 + 8x \log x$ is $\Theta(x^2)$.

- **Theorem 4:** Let $f(x)= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, where $a_0, a_1, \ldots, a_{n-1}, a_n$ are real numbers with $a_n \neq 0$. Then, *f(x)* is of order x^n.

3.3 Complexity of Algorithms

3.3 Complexity of Algorithms

- **Time Complexity:** Determine the approximate number of operations required to solve a problem of size n.
- **Space Complexity:** Determine the approximate memory required to solve a problem of size n.

❑ **Time Complexity**

- ✓ Use the Big-O notation
- ✓ Ignore house keeping
- ✓ Count the <u>expensive</u> operations only
- ✓ Basic operations:
  - ▪ searching algorithms - key comparisons
  - ▪ sorting algorithms - list component comparisons
  - ▪ numerical algorithms - floating point ops. (flops) - multiplications/divisions and/or additions/subtractions

Worst Case: maximum number of operations

Average Case: mean number of operations assuming an input probability distribution

3.3 Complexity of Algorithms

- **Examples:**
  Multiply an n x n matrix A by a scalar c to produce the matrix B:

```
procedure (n, c, A, B)
    for i from 1 to n do
        for j from 1 to n do
            B(i, j) = cA(i, j)
        end do
    end do
```

Analysis (worst case):

Count the number of floating point multiplications.

n^2 elements requires n^2 multiplications.

time complexity is

$O(n^2)$ or *quadratic* complexity.

3.4 The Integers and Division

3.4 The Integers and Division

- **Three applications of modular arithmetic :**
  1) Generating pseudorandom numbers,
  2) Assigning computer memory locations to files, and
  3) Encrypting and decrypting messages.

Division

- **Definition 1:**

  If a and b are integers with a≠0, we say that a divides b (a|b) if there is an integer c such that b=ac.
  - a is a factor of b
  - b is a multiple of a
  - $a \nmid b$ if a does not divide b
- **EXAMPLE 1:**Determine whether $3 \mid 7$ and whether $3 \mid 12$.

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

3.4 The Integers and Division

- **Theorem 1:**

  Let a, b, c be integers. Then

  1) if a|b and a|c, then a|(b+c)
  2) if a|b, then a|bc for all integers c
  3) if a|b and b|c, then a|c

  Proof:

  Proof of (1).

  - ✓ Suppose that a | b and a | c.
  - ✓ From the definition of divisibility, it follows that there are integers s and t with b = as and c = at .
  - ✓ Hence, b + c = as + at = a(s + t).
  - ✓ Therefore, a divides b + c. This establishes part (i) of the theorem.

  ❖ Proof of 2 and 3 is homework

- **Corollary 1:**

  If a, b, and c are integers such that a|b and a|c, then a|mb+nc whenever m and n are integers.

  Proof: By part (ii) of Theorem 1 it follows that a | mb and a | nc whenever m and n are integers. By part (i) of Theorem 1 it follows that a | mb + nc.

3.4 The Integers and Division

The Division Algorithm

- **Theorem 2:** (The Division Algorithm)

  Let *a* be an integer and *d* a positive integer. Then there are unique integers *q* and *r*, with $0<=r<d$, such that $a=dq+r$.

- **Definition 2:**

  In the equality given in the division algorithm,

  d is called the ***divisor***,

  a is called the ***dividend***,

  q is called the ***quotient***, and

  r is called the ***remainder.***

  This notation is used to express the quotient and remainder:

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

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

  Solution: We have $101 = 11 \cdot 9 + 2$.

  Hence, the quotient when 101 is divided by 11 is 9 = 101 div 11 , and the remainder is 2 = 101 mod 11.

3.4 The Integers and Division

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

  Solution: We have -11 = 3(-4) + 1 .

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

  Note that the remainder cannot b e negative. Consequently, the remainder i s not - 2 , even though

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

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

Modular Arithmetic

- **Definition 3:**

  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*.

  $$a \equiv b (\mathrm{mod}\ m)$$

- **Theorem 3:**

  Let *a* and *b* be integers, and let *m* be a positive integer. Then $a \equiv b (\mathrm{mod}\ m)$ if and only if *a mod m = b mod m*.

3.4 The Integers and Division

- **EXAMPLE 5:** Determine whether 1 7 is congruent to 5 modulo 6 and whether 24 and 1 4 are congruent modulo 6.

  Solution: Because 6 divides 17 - 5 = 12 , we see that 17 ≡ 5 (mod 6). However, because 24 - 14 = 10 is not divisible by 6, we see that 24 $\not\equiv$ 1 4 (mod 6).

- **Theorem 4:**

  Let m be a positive integer. The integers a and b are congruent modulo m iff there is an integer k such that a=b+km.

  Proof:

  - ✓ If a ≡ b (mod m), then m | (a - b).
  - ✓ There is an integer k such that a - b = km , so that a = b + km
  - ✓ Conversely, if there is an integer k such that a = b + km , then km = a - b.
  - ✓ Hence, m divides a - b, so that a ≡ b (mod m).

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

3.4 The Integers and Division

- **Theorem 5:**

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

  Proof:

  - ✓ Because a ≡ b (mod m) and c ≡ d (mod m), there are integers s and t with b = a + sm and d = c + tm .
  - ✓ Hence, b + d = (a + sm) + (c + tm) = (a + c) + m (s + t) and bd = (a + sm)(c + tm) = ac + m eat + cs + stm).
  - ✓ Hence, a + c ≡ b + d (mod m) and ac ≡ bd (mod m).

- **EXAMPLE 6:**

  Because 7 ≡ 2 (mod 5) and 11 ≡ 1 (mod 5), it follows from Theorem 5 that
  18 = 7 + 11 ≡ 2 + 1 = 3 (mod 5)
  and that 77 = 7 . 11 == 2 . 1 = 2 (mod 5).

- **Corollary 2:**

  Let m be a positive integer and let a and b be integers. Then
  (a+b) mod m=((a mod m)+(b mod m)) mod m and
  ab mod m = *((a mod m)(b mod m)) mod m*.

  Proof: By the definitions ***mod m*** and the definition of ***congruence modulo m*** , we know that a ≡ (a mod m)(mod m) and b ≡ (b mod m) (mod m). Hence, Theorem 5 tell us that a + b ≡ (a mod m) + (b mod m) (mod m) and ab ≡ (a mod m)(b mod m) (mod m) .

3.4 The Integers and Division

- **Applications of Congruences:**
  - ✓ Hashing functions

    $h(k) = k \bmod m$
  - ✓ Pseudorandom numbers

    $x_{n+1} = (ax_n + c) \bmod m$
  - ✓ Cryptology

    Caesar cipher: $f(p) = (p+k) \bmod 26$

3.5 Primes and Greatest Common Divisors

3.5 Primes and Greatest Common Divisors

Primes

- **Definition 1:**
  - ✓ A positive integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p.
  - ✓ Integer n is ***composite*** if and only if there exists an integer a such that a|n and 1<a<n.
- **EXAMPLE 1:**

  The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3 .
- **Theorem 1: (Fundamental Theorem of Arithmetic):**

  Every positive 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.
- **EXAMPLE 2:**

  The prime factorizations of 1 00, 64 1 , 999, and 1 024 are given by

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

  $641 = 641$,

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

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

3.5 Primes and Greatest Common Divisors

- **Theorem 2:**

  If n is a composite integer, then n has a prime divisor less than or equal to √n.
- **EXAMPLE 3:** Show that 101 is prime.

  Solution: The only primes not exceeding √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.
- **EXAMPLE 4:** Find the prime factorization of 7007.

  Solution:

  - ✓ To find the prime factorization of 7007, first perform divisions of 7007 by successive primes, beginning with 2.
  - ✓ 7 divides 7007, with 7007/7 = 1001 .
  - ✓ 1001/7 = 1 43 and 143/11 = 13 .
  - ✓ It follows that the prime factorization of 7007 is 7*7*11*13 = 7^2 *11*13 .
- **Theorem 3:**

  There are infinitely many primes.

  Mersenne primes - $2^p - 1$, where p is also prime

3.5 Primes and Greatest Common Divisors

- **EXAMPLE 5:** The numbers 2^2 - 1 = 3 , 2^3 - 1 = 7, and 2^5- 1 = 31 are Mersenne primes, while 2^{11} - 1 = 2047 is not a Mersenne prime because 2047 = 23 · 89.
- **Theorem 4:** (Prime Number Theorem)

  The ratio of the number of primes not exceeding x and x/ln x approaches 1 as x grows without bound.
- **Example 6:** f(n)=n^2-n+41, for n not exceeding 40

  For every polynomial f(n) with integer coefficients, there is a positive integer y such that f(y) is composite.
- **Example 7:** Goldbach's Conjecture (1742): every even integer n, n>2, is the sum of two primes.
- **Example 8:** There are infinitely many primes of the form n^2+1, where n is a positive integer.
- **Example 9:**
  - ✓ Twin Prime Conjecture: There are infinitely many twin primes.
  - ✓ Twin primes are primes that differ by 2.
  - ✓ such as 3 and 5, 5 and 7, 1 1 and 1 3, 1 7 and 1 9, and 4967 and 4969.

3.5 Primes and Greatest Common Divisors

- **Definition 2:**
  Let a and b be integers, not both zero. The largest integer d such that d|a and d|b is called the ***greatest common divisor*** of a and b. (or gcd(a, b))
- **EXAMPLE 10:** What is the greatest common divisor of 24 and 36?
  Solution: The positive common divisors of 24 and 36 are 1, 2, 3, 4, 6, and 12 . Hence, gcd(24, 36) = 12 .
- **EXAMPLE 11:** What is the greatest common divisor of 17 and 22?
  Solution: The integers 17 and 22 have no positive common divisors other than 1 , so that gcd(17, 22) = 1 .
- **Definition 3:** The integers a and b are ***relatively prime*** if their gcd is 1.
- **EXAMPLE 12:** That the integers 17 and 22 are relatively prime, because gcd(17, 22) = 1 .
- **Definition 4:**
  The integers $a_1, \ldots, a_{n-1}, a_n$ are pairwise relatively prime if gcd(a_i, a_j)=1 whenever $1 \leq i < j \leq n$.

3.5 Primes and Greatest Common Divisors

- **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 .

- If a . = $p_1^{a_1}$, $p_2^{a_2}$ . . . $p_n^{a_n}$ and b = $p_1^{b_1}$, $p_2^{b_2}$ . . ... $p_n^{b_n}$

Then gcd(a , b) is given by gcd(a, b) = $p_1^{\min(a_1,b_1)}$ $p_2^{\min(a_2,b_2)}$ ……. $p_n^{\min(a_n,b_n)}$

- **EXAMPLE 14:** Because the prime factorizations of 120 and 500 are 120 = 2^3*3*5 and 500 = 2^2*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

- **Definition 5:**

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

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

3.5 Primes and Greatest Common Divisors

- **EXAMPLE 15:** What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

  Solution: 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)*lcm(a,b)

3.6 Integers and Algorithms

3.6 Integers and Algorithms

- ✓ Representation of Integers

  Decimal, binary, octal, hexadecimal

- **Theorem 1:**

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

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

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

  - Base b expansion of n: $(a_k a_{k-1} \ldots a_1 a_0)_b$
  - Binary expansion, hexadecimal expansion
  - Base conversion

- **Algorithm 1:** Constructing Base b Expansions

  Procedure base b expansion(n: positive integer)

```
q:=n
k:=0
while q<>0
begin
  ak:=q mod b
  q:=$\lfloor q/b \rfloor$
  k:=k+1
end
```

3.6 Integers and Algorithms

- ✓ Computing the greatest common divisor using prime factorizations of integers is inefficient because of time consuming to find prime factorizations. More efficient method of finding the greatest common divisor, called the Euclidean algorithm.
- **Euclidean Algorithm:**

```
Procedure gcd(a, b: positive integers)
x:=a
y:=b
while y<>0
begin
  r:=x mod y
  x:=y
  y:=r
end {gcd(a,b) is x}
```

gcd (6,12):

$x = 6$ $y = 12$

while $y \neq 0$

  $r = 6 \bmod 12 = 6$

  $x = 12$ $y = 6$

while $y \neq 0$

  $r = 12 \bmod 6 = 0$

  $x = 6$ $y = 0$

while $y = 0$, end. ∴ gcd (6,12) = 6

- **Example:** Find gcd of 414 and 662 using the Euclidean algorithm.

Solution: $662 = 414 * 1 + 248$
$414 = 248 * 1 + 166$
$248 = 166 * 1 + 82$
$166 = 82 * 2 + 2$
$82 = 2 * 4 1$.

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

3.7 Applications of Number Theory

3.7 Applications of Number Theory

- *gcd*(*a*,*b*) can be expressed as a linear combination with integer coefficients of *a* and *b*.

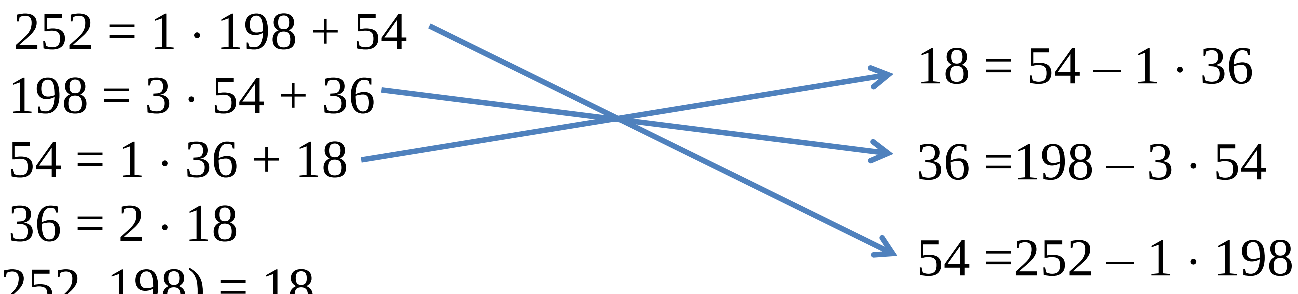
- **Theorem 1:**

  If *a* and *b* are positive integers, then there exist integers *s* and *t* such that

  $gcd(a,b) = sa+tb.$

Example 1 Express gcd(252, 198) =18 as a linear combination of 252 and 198.

Solution:



$252 = 1 \cdot 198 + 54$

$198 = 3 \cdot 54 + 36$

$54 = 1 \cdot 36 + 18$

$36 = 2 \cdot 18$

$18 = 54 – 1 \cdot 36$

$36 =198 – 3 \cdot 54$

$54 =252 – 1 \cdot 198$

$\therefore$ gcd(252, 198) = 18

$$\Rightarrow \; 18 = 54 – 1 \cdot 36 \quad = 54 – 1 \cdot (198 – 3 \cdot 54)$$

$$= 4 \cdot 54 – 1 \cdot 198 \quad = 4 \cdot (252 – 1 \cdot 198) – 1 \cdot 198$$

$$= 4 \cdot 252 – 5 \cdot 198$$

Exercise : 1(g)

3.7 Applications of Number Theory

Linear Congruences

- ✓ A congruence of the form $ax \equiv b \pmod{m}$ where *m* is a positive integer , *a* and *b* are integers , and *x* is variable, is called a **linear congruence.**
- ✓ Such congruences arise throughout number theory and its applications.
- ✓ How can we solve the linear congruence $ax \equiv b \pmod{m}$? That is, find the x that satisfy this congruence.
- ✓ One method that we will describe uses an integer ā such that aā≡1 (mod m), if such an integer exist.
- ✓ Such an integer ā is said to be an **inverse** of a modulo m.
- ✓ Theorem 3 guarantees that an inverse of a modulo m exists whenever a and m are relatively prime.

3.7 Applications of Number Theory

- **Theorem 3:**

  If *a* and *m* are relatively prime integers and *m*>1, then an inverse of modulo *m* exist. Furthermore, this inverse is unique modulo *m*. (there is a unique positive integer ā less than *m* that is an inverse of a modulo *m* and every other inverse of *a* modulo *m* is congruent to ā modulo *m*.)

  When we have an inverse of a modulo m, *ax* ≡ *1* (mod *m*) , *we solve the congruence ax* ≡ *b* (mod *m*).

  Proof: By Theorem 1 , because gcd(a , m) = 1 , there are integers s and t such that

  sa + tm = 1 .

  This implies that

  sa + tm ≡ 1 (mod m).

  Because tm ≡ 0 (mod m), it follows that

  sa ≡ 1 (mod m).

  Consequently, s is an inverse of a modulo m.

3.7 Applications of Number Theory

- **EXAMPLE 3:** Find an inverse of 3 modulo 7.

  Solution: Because gcd(3, 7) = 1, Theorem 3 tells us that an inverse of 3 modulo 7 exists. Using Euclidean algorithm to find greatest common divisor of 3 and 7 :

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

  From this equation we see that

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

  - This shows that -2 is an inverse of 3 modulo 7 . (Note that every integer congruent to -2 modulo 7 is also an inverse of 3, such as 5, -9, 12, and so on.)

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

  Solution: By Example 3 know that -2 is an inverse of 3 modulo 7.

  $-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7$[Multiplying both sides of the congruence by -2]

  Because $-6 \equiv 1 \pmod 7$ and $- 8 \equiv 6 \pmod 7$, it follows that if x is a solution, then $x \equiv - 8 \equiv 6 \pmod 7$.

  We need to determine whether every x with $x \equiv 6 \pmod 7$ is a solution. Assume that $x \equiv 6 \pmod 7$. Then $3x \equiv 3 \cdot 6 = 18 \equiv 4 \pmod 7$, which shows that all such x satisfy the congruence. We conclude that the solutions to the congruence are the integers x such that $x \equiv 6 \pmod 7$, namely, 6, 1 3 , 20, . . . and - 1 , -8,-15 , ...

3.7 Applications of Number Theory

Chinese Reminder Theorem

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

x ≡ a_1 (mod m_1),

x ≡ a_2 (mod m_2),

.

.

x ≡ a_n (mod m_n)

has a unique solution modulo m = $m_1 m_2 \ldots m_n$. (That is , there is a solution x with 0 ≤ x < m , and all other solutions are congruent modulo m to this solution.)

Proof: First let $M_k = \frac{m}{m_k}$

for k = 1 , 2 , . . . , n . That is, $M_k$is the product of the moduli except for m_k. Because m_i and m_k have no common factors greater than 1 when i≠k, it follows that gcd(m_k, M_k) = 1. Consequently, by Theorem 3, we know that there is an integer y_k, an inverse of M_k modulo m_k such that

$$M_k y_k \equiv 1 (\text{mod } m_k)$$

3.7 Applications of Number Theory

Chinese Reminder Theorem

Proof (cont.):

To construct a simultaneous solution, form the sum

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

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

$$x \equiv a_k\ M_ky_k \equiv a_k (\text{mod } m_k),$$

for k = 1 , 2, . . . , n. We have shown that x is a simultaneous solution to the n congruences.

3.7 Applications of Number Theory

Pseudoprimes

- **Theorem 5: Fermat's Little Theorem**
  - ✓ If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 \pmod{p}$$

  - ✓ Furthermore, for every integer a we have

$$a^p \equiv a \pmod{p}$$

  - ✓ Unfortunately, there are composite integer n, such that $2^{n-1} \equiv 1 \pmod{p}$. Such integers are called pseudoprimes to the base 2.
- **EXAMPLE 9:** The integer 341 is a pseudoprime to the base 2 because it is composite (341 = 11 * 31) and as

  $2^{340} \equiv 1 \pmod{341}$
- **Definition 1:**

  Let *b* be a positive integer. If *n* is a composite positive integer, and $b^{n-1} \equiv 1$ (mod *n*), then *n* is called a ***pseudoprime to the base b***.
- **Definition 2:**

  A composite integer *n* that satisfies the congruence $b^{n-1} \equiv 1$ (mod *n*) for all positive integers b with gcd(*b* , *n*)=1 is called a ***Carmichael number.***

3.7 Applications of Number Theory

- **Example 10:** The integer 561 is a Carmichael number.
  - ✓ To see this, first note that 561 is composite because 561 = 3*11*17 .
  - ✓ Next, note that if gcd(b, 561) = 1, then gcd(b, 3) = gcd(b, 11) = gcd(b, 17) =1.
  - ✓ Using Fermat's Little Theorem we find that

    $b^2 \equiv 1$ (mod 3), $b^{10} \equiv 1$ (mod 1 1), and $b^{16} \equiv 1$ (mod 17).
  - ✓ It follows that

    $b^{560} = (b^2)^{280} \equiv 1$ (mod 3),

    $b^{560} = (b^{10})^{56} \equiv 1$ (mod 11),

    $b^{560} = (b^{16})^{35} \equiv 1$ (mod 17).
  - ✓ it follows that $b^{560} \equiv 1$ (mod 561) for all positive integers b with gcd(b, 561) = 1 . Hence 561 is a Carmichael number.

3.7 Applications of Number Theory

Exercise 18. Find all solutions to the system of congruences

$$x \equiv 2 \pmod{3}$$
$$x \equiv 1 \pmod{4}$$
$$x \equiv 3 \pmod{5}$$

Sol :

$$a_1=2\ ,\ a_2=1\ ,\ a_3=3,$$
$$m_1=3\ ,\ m_2=4\ ,\ m_3=5 \qquad m=3\times4\times5=60$$
$$M_1=20\ ,\ M_2=15\ ,\ M_3=12$$
$$20\equiv2 \pmod{3} \quad \Rightarrow 20\times2\equiv1 \pmod{3}$$
$$15\equiv3 \pmod{4} \quad \Rightarrow 15\times3\equiv1 \pmod{4}$$
$$12\equiv2 \pmod{5} \quad \Rightarrow 12\times3\equiv1 \pmod{5}$$
$$\therefore x = 2\times20\times2+1\times15\times3+3\times12\times3$$
$$= 80+45+108=233\equiv53 \pmod{60}$$

3.7 Applications of Number Theory

Ex 21. Find all solutions, if any, to the system of congruences.

$$
\begin{aligned}
x &\equiv 7 \pmod{9} \\
x &\equiv 4 \pmod{12} \\
x &\equiv 16 \pmod{21}
\end{aligned}
$$

Sol. Rewrite the system as the following:

$$
\begin{array}{ll}
x \equiv 7 \pmod{9} & \\
x \equiv 1 \pmod{3} & x \equiv 0 \pmod{4} \\
x \equiv 1 \pmod{3} & x \equiv 2 \pmod{7}
\end{array}
$$

i.e.,

$$
\begin{array}{ll}
x \equiv 7 \pmod{9} & (x \equiv 1 \pmod{3}) \\
x \equiv 0 \pmod{4} & \ldots \\
x \equiv 2 \pmod{7} &
\end{array}
$$