UNIT 2: Integers and Matrices.

- The part of mathematics involving the integers and their properties belong to the branch of mathematics called number theory.
- If 'a' and 'b' are integers with $a \neq 0$, we say that 'a' divides 'b' if there is an integer 'c' such that $b = ac$. When 'a' divides 'b' we say that 'a' is a factor of 'b' and that 'b' is multiple of 'a'. The notation $a|b$ denotes that 'a' divides 'b'. We write $a \nmid b$ when 'a' does not divide 'b'.
- Example: Determine 3|7 and whether 3|12.
  Solution: It follows that $3 \nmid 7$, because $\frac{7}{3}$ is not an integer. $3|12$ because $12/3 = 4$.

- Example: Let 'n' and 'd' be positive integers. How many positive integers not exceeding 'n' are divisible by 'd'?
  Solution: The positive integers divisible by 'd' are all the integers of the form 'dk', where k is a positive integer. Hence, the number of positive integers divisible by d that dont exceed n equals the number of integers k with $0 < dk \leq n$, or with $0 < k \leq n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

(ii) if a|b, then a|bc for all integers.

→ Given that a|b, by the definition of divisibility we can say that there is an integer p such that b = ap, so for any integer c, we can write, bc = apc. This means that a divides bc since pc is an integer too.

iii) Given that a|b and b|c, by the definition of divisibility we have integers p and q such that b = ap and c = bq i.e c = apq. Since, pq is an integer we conclude that a divides c.

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

Solution:

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

Example: 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~~ $-4 = -11 \text{ div } 3$, and the remainder $1 = -11 \bmod 3$.

- Note that the remainder cannot be negative. Consequently, the remainder is not -2, even though $-11 = 3(-3) - 2$.

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

- Integer a is divisible by the integer d if and only if the remainder is zero when a is divided by d.

MODULAR ARITHMETIC:

If a and b are integers and m is a positive integer, the 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. If a and bare not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

Theorem: Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$.

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

Solution: Because 6 divides $17-5=12$, we see that $17 \equiv 5 \pmod 6$

- $24-14=10$ is not divisible by 6, we see that $24 \not\equiv 14 \pmod 6$.

Theorem 4: Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod m$, then $m \mid (a-b)$. This means that there is an integer k such that ~~$a = b + km$~~ $a - b = km$, 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 $a \equiv b \pmod m$.

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

- Theorem 5: Let m be a positive integer. If $a \equiv b \pmod m$ and $c \equiv d \pmod m$, then.

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

Proof: Because $a \equiv b \pmod m$ and $c \equiv d \pmod m$, there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence,

$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ (5)

Corollary 2: Let 'm' be a positive integer and let 'a' and 'b' be integers. Then.

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

and

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

Proof: By the definition mod m and the definition of congruence modulo m, we know that $a \equiv (a \bmod m) \pmod m$ and $b \equiv (b \bmod m) \pmod m$. Hence, theorem 5 tell us that.

$$a+b \equiv (a \bmod m) + (b \bmod m) \pmod m$$

and.

$$ab \equiv (a \bmod m)(b \bmod m) \pmod m.$$

$a \equiv b \pmod n$, $a, b \in Z$ and $n \in Z^+$

① a and b have same "remainder" when they are divided by n

② $a = k \cdot n + b$

③ $a - b = k \cdot n$ (a-b is multiple of n)

$n \mid (a-b)$ (n divides a-b)

Example. $10 \equiv 14 \pmod 4$

$10 \div 4 = 2\ R2$

$14 \div 4 = 3\ R2$

$10 \equiv -2 \pmod 4$

$10 \div 4 = 2\ R2$

$-2 \div 4 = -1\ R2$

~~$10 = 14$~~

$10 = k \cdot 4 + 14$

$10 - 14 = k \cdot 4$

$-4 = k \cdot 4$

$k = -1$

$n \mid (a - b)$

$4 \mid (10 - 14)$

Does $53 \equiv 17 \pmod 3$

$53 \equiv 14 \pmod 3$

$53 \equiv 11 \pmod 3$

$3 \mid (53 - 17)$

$3 \mid 36$ ✓

$3 \mid (53 - 14)$

$3 \mid 39$ ✓

$3 \mid (53 - 11)$

$3 \mid 43$ ✗

$17 \pmod 3 \equiv 14 \pmod 3$

Congruences are equivalence classes.

In mod 4

$[0] = \{\dots, -4, 0, 4, \dots\}$

$[1] = \{\dots, -3, 1, 5, 9, \dots\}$

$[2] = \{\dots, -2, 2, 6, 10, \dots\}$

$[3] = \{\dots, -1, 3, 7, 11, \dots\}$

mod n

$[0], \dots, [n-1]$

$5 \div 4 = 4 \cdot 1 + 1$

$9 \div 4 = 4 \cdot 2 + 1$

$2 \div 4 = 4 \times 0 + 2$

$10 \div 4 = 4 \times 2 + 2$

$7 \div 3 = 4 \times 1 + 3$

Mod 4

[0]	[1]	[2]	[3]
0	1	2	3
4	5	6	7
8	9	10	11
12	13	14	15

$a = nq + r$

$n = 4$ in this exam.

$r =$ equivalent class.

Applications of Congruences → (teach these in detail @ end of this chapt.)
- Hashing function.
- Pseudo random numbers
- Cryptology.

PRIMES and Greatest Common Divisors.

- A prime is an integer greater than 1 that is divisible only by 1 ~~and~~ and by itself.
- A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater ~~that~~ than 1 and is not prime is called composite.
- The integer n is composite if and only if there exists an integer a such that $a|n$ and $1 < a < n$.
- Ex, of Prime 2, 3, 5, 7, 11, 13, 17, 19 ...
  Ex of composite 4, 6, 9, ...

- **Theorem 1: The 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: Prime factorization.

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

$641 = 641$

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

$1024 = 2^{10}$

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

Proof: If n is composite, by the definition of a composite integer, we know that it has a ~~factor~~ a with $1 < a < n$. Hence, by the definition of a factor of a positive integer, we have $n = ab$, where b is a positive integer greater than 1.

We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n} \cdot \sqrt{n} = n$, which is a contradiction.

Consequently, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$. Because both a and b are divisors of n, we see that n has a positive divisor not exceeding $\sqrt{n}$. This divisor is either prime or by the Fundamental Theorem of Arithmetic, has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$.

- From above Theorem, it follows that an integer is prime if it is not divisible by any prime less than or equal to its square root.

- **Example:** Show 101 is Prime.

Solution: The only primes not exceeding $\sqrt{101}$ are 2, 3, 5 and 7. Because 101 is not divisible by 2, 3, 5 and 7, it follows that 101 is Prime.

Example: Find the prime factorization of 7007.

Solution: · First perform divisions of 7007 by successive primes, beginning with 2.

· None of the primes 2, 3 and 5 divides 7007.

· But $7 \mid 7007$. $\frac{7007}{7} = 1001$.

· Next, divide ~~7007~~ 1001 by successive primes, beginning with 7. ~~7007~~ $\frac{1001}{7} = 143$.

· Continue by dividing 143 by successive primes, beginning with 7.

~~7~~ $7 \nmid 143$, $11 \mid 143$, $\frac{143}{11} = 13$.

· Because 13 is prime, the procedure is completed.

· The prime factorization of $7007 = 7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

· 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 fundamental Theorem of arithmetic, Q is prime or else it can be written as the product of two or 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 $p_1, p_2, p_3, \ldots, p_n$. 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, ~~the~~ there are infinitely many primes.

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

Ex.

- $2^2 - 1 = 3$
- $2^3 - 1 = 7$
- $2^5 - 1 = 31$

$2^{11} - 1 = 2047 \Rightarrow$ is not Mersenne

$2047 = 23 \cdot 89$.

Theorem 4: The Prime Number Theorem:
The ratio of the number of primes not exceeding x and $\frac{x}{\ln x}$ approaches 1 as x grows without bound.

- Search size X
- Prime density $(x) \sim \frac{1}{\ln(x)}$
- Number of primes $(x) \sim \frac{x}{\ln(x)}$
- $\lim_{x \to \infty} \frac{\Pi(x)}{\frac{x}{\ln(x)}} = 1$, $\Pi(x)$ = actual count

  $\frac{x}{\ln(x)}$ = estimate.

Example: No. of primes not exceeding 100.

$\Pi(x) = \pi(x) = 25$ = actual count

$\frac{100}{\ln(100)} = 21.714$, $\frac{1}{\ln(100)}\% = 21.7\%$

$X = 1000$

$\pi(1000) = 168$ = actual count

$\frac{1000}{\ln(1000)} = 144.764$

density $= \frac{1}{\ln(1,000)}$ % $= 14.48\%$

- $X = 10,000$

$\pi(10000) = 1,229$

$\frac{10000}{\ln(10,000)} = 1085.736$

density $= \frac{1}{\ln(10,000)} = 10.8\%$

- $X = 100,000$

$\pi(100,000) = 9,592$

$\frac{100,000}{\ln(100,000)} = 8685.889$

density $= \frac{1}{\ln(100,000)} = 8.685\%$

- $X = 1,000,000$

$\pi(1,000,000) = 78,498$

$\frac{1,000,000}{\ln(1,000,000)} = 72,382.413.$

density $= \frac{1}{\ln(100,000)} = 7.23\%$

- $X = 1,000,000,000$

$\pi(1,000,000,000) =$

$\frac{1,000,000,000}{\ln(1,000,000,000)} = 48254942.4$

density $= \frac{1}{\ln(1,000,000,000)}$

$= 4.825\%$

(12)

↳ Proportion of Prime less than 1 billion = 4.825%
Average gap between primes is : $\ln(1 \text{ billion}) = 20.723$

~~Prime Index~~ $= p_x \sim x \ln(x)$, if $x = 1$ billion then we can calculate approximate value of 1billionth prime

- Goldbach's Conjecture: The conjecture that every even integer n, $n>2$, is sum of two primes is called Goldbach's conjecture.

- Twin Primes: The primes that differ by 2, such as 3 and 5, 5 and 7, 11 & 13, 17 & 19, and 4967 and 4969.

The twin Prime Conjecture: The twin Prime conjecture asserts that there are infinitely many twin primes.

What is Conjecture?

Greatest Common Divisor

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

- Example: What is the greatest common divisor of 24 & 56?
  Ans: 12.

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

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

- The integers 'a' and 'b' are relatively Prime if their greatest common divisor is 1.

∴ Here, 17 and 22 are relatively Prime.

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

Solution: $\gcd(10, 17) = 1$, $\gcd(10, 21) = 1$, $\gcd(17, 21) = 1$

∴ 10, 17, & 21 are pairwise relative prime.

- $\gcd(10, 24) = 2 > 1$.

10, 19, 24 are not pairwise relative prime.

- Find the gcd of two integers using prime factorization of these integers.
- Suppose that the prime factorizations of the integers 'a' and 'b', neither equal to zero, are.

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

where each exponent is a non negative integer, and where all primes occurring in the prime factorization of either 'a' or 'b' are included in both factorization, with zero exponents if necessary. Then $\gcd(a, b)$ is given by

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

where $\min(x, y)$ represents the minimum of the two numbers x and y.

- Example: gcd(120, 500) = ?

$120 = 2 \times 2 \times 2 \times 3 \times 5 = 2^3 \cdot 3^1 \cdot 5^1$

$500 = 2 \times 2 \times 5 \times 5 \times 5 = 2^2 \cdot 3^0 \cdot 5^3$

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

$= 2^2 \cdot 3^0 \cdot 5^1 = 4 \times 5 = 20.$

- 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 lcm(a, b).

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

- Example: lcm(120, 500) = ?

$120 = 2^3 \cdot 3^1 \cdot 5^1$

$500 = 2^2 \cdot 3^0 \cdot 5^3$

$\text{lcm}(120, 500) = 2^{\max(3,2)} \cdot 3^{\max(1,0)} \cdot 5^{\max(1,3)}$

$= 2^3 \cdot 3^1 \cdot 5^3 = 8 \times 3 \times 125 = 3000.$

Theorem 5:

Let 'a' and 'b' be positive integers. Then.

$ab = \gcd(a,b) \cdot \text{lcm}(a,b).$

· The Euclidean Algorithm.

Lemma 1: Let $a = bq + r$, where a, b, q and r are integers. Then $\gcd(a,b) = \gcd(b,r)$

Proof: Suppose that d divides both a and b. Then it follows that d divides $a - bq = r$ (Theorem 1 section 3.4) Hence any common divisor of a and b is also common divisor of b and r.
Like-wise, suppose that d divides both b and r. Then d also divides $bq + r = a$. Hence, any common divisor of b and r is also common divisor of a and b.

Consequently, $\gcd(a,b) = \gcd(b,r)$
Suppose that 'a' and 'b' are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$. When we successively apply the division algorithm, we obtain.

$$r_0 = r_1 q_1 + r_2 \quad 0 \leq r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3 \quad 0 \leq r_3 < r_2$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n \quad 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_n q_n.$$

Eventually a remainder of zero occurs in this sequence of successive divisions, because the sequence of remainders $a = r_0 > r_1 > r_2 > \cdots \geq 0$ cannot contain more than a terms. Furthermore, it follows from Lemma 1 that

$$\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) \cdots = \gcd(r_{n-2}, r_{n-1})$$
$$= \gcd(r_{n-1}, r_n) = \gcd(r_n, 0) = r_n.$$

Hence, the greatest common divisor is the last nonzero remainder in the sequence of divisions.

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

Solution:

$662 = 414 \cdot 1 + 248$

$414 = 248 \cdot 1 + 166$

$248 = 166 \cdot 1 + 82$

$166 = 82 \cdot 2 + 2$

$82 = 2 \cdot 41$

Hence, gcd (414, 662) = 2, because two is last non-zero remainder.

Extended Euclidean Algorithm.

The extended Euclidean algorithm is an algorithm to compute integers x and y such that

$$ax + by = \gcd(a, b)$$

given a and b.

Example: Find two integers 'a' and 'b' such that

$$1914a + 899b = \gcd(1914, 899).$$

- First use the Euclidean algorithm to find GCD.

$1914 = 2 \times 899 + 116$

$899 = 7 \times 116 + 87$

$116 = 1 \times 87 + 29$

$87 = 2 \times 29 + 0$

Last non-zero remainder = 29.

gcd (1914; 899) = 29

Now using the extended algorithm.

$29 = 116 + (-1) \times 87$

$87 = 899 + (-7) \times 116$

$29 = 116 + (-1) \times (899 + (-7) \times 116)$

$= 8 \times 116 + (-1) \times 899$

$= (-1) \times 899 + 8 \times (1914 - 2 \times 899)$

$= (-1) \times 899 - 16 \times 899 + 8 \times 1914$

$= (-17) 899 + 8 \times 1914$

$29 = 8 \times 1914 - 17 \times 899$

$a = 8, \quad b = -17$

What is lemma? ~~Obie~~ Big O?

Integer and algorithms.

~~The term algorithm refers to procedures for performing arithmetic operations using the decimal~~

Representation of Integers.

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

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

where, k is non negative integer, $a_0, a_1 \cdots a_k$ are non-negative integers less than b, and $a_k \neq 0$.

$(245)_8 = 2 \cdot 8^2 + 4 \cdot 8 + 5 = 165$

Algorithm 1: Constructing Base b Expansions.

Procedure: base b expansion (n: positive integer).

```
q := n
k := 0
while q ≠ 0
begin
    a_k := q mod b
    q := ⌊q/b⌋
    k := k + 1
end {the base b expansion of n is (a_{k-1} ... a_1 a_0)}
```

- In algorithm 1, q represents the quotient obtained by successive divisions by b, starting with q = n. The digits in the base b expansion are the remainders of these divisions and are given by q mod b. The algorithm terminates when a quotient q = 0 is reached.

- Example.

  Find the base 8, or octal expansion of $(12345)_{10}$

- q = n = 12345, b = 8

  $a_0 = 12345 \bmod 8 = 1$

  $q = \lfloor 12345/8 \rfloor = 1543.$

- $a_1 = 1543 \bmod 8 = 1$

  $q = \lfloor 1543/8 \rfloor = 192$

- $a_2 = 192 \bmod 8 = 0$

  $q = \lfloor 192/8 \rfloor = 24$

- $a_3 = 24 \bmod 8 = 0$

  $q = \lfloor 24/8 \rfloor = 3$

- $a_4 = 3 \bmod 8 = 3$

  $q = \lfloor 3/8 \rfloor = 0$

- k=0.

$q_0 = 12345 \bmod 8 = 1$

$q = \lfloor q/b \rfloor = 1543$

k=1

$q_1 = 1543 \bmod 8 = 7$

$q = \lfloor 1543/8 \rfloor = 192$

- k=2

$a_2 = 192 \bmod 8 = 0$

$q = \lfloor 192/8 \rfloor = 24$

- k=3

$a_3 = 24 \bmod 8 = 0$

$q = \lfloor 24/8 \rfloor = 3$

- k=4

$a_4 = 3 \bmod 8 = 3$

$q = 0$

$(12345)_{10} = (30071)_8$

- Algorithms for Integer Operations.
- Algorithms 2. Addition of Integers.

Procedure add (a, b: positive integers)
{ the binary expansions of 'a' and 'b' are $(a_{n-1}a_{n-2}\cdots a_1a_0)_2$ and $(b_{n-1}b_{n-2}\cdots b_1b_0)_2$, respectively }

```
c := 0
for j := 0 to n-1
begin
    d := ⌊(a_j + b_j + c)/2⌋
    s_j := a_j + b_j + c - 2d
    c := d
end
    s_n := c
```

{ the binary expansion of the sum is $(s_n s_{n-1}\cdots s_0)_2$ }

Algorithm 3 Multiplying Integers.

```
Procedure multiply ( a, b: positive integers)
{ the binary expansions of a and b are (a_{n-1}, a_{n-2} ... a_1 a_0)_2
    and (b_{n-1} b_{n-2} ... b_1 b_0)_2, respectively }

for j := 0 to n-1
begin
      if b_j = 1 then c_j := a shifted j places
      else c_j := 0
end
{ c_0, c_1, ..., c_{n-1} are the partial products }
p := 0
for j := 0 to n-1
    p := p + c_j
{ p is the value of ab }
```

Algorithm 4: Computing div and mod.

```
Procedure division algorithm ( a: integer, d: positive integer)
q := 0
r := |a|
while r ≥ d
begin
      r := r - d
      q := q + 1
end
if a < 0 and r > 0 then
begin
  r := d - r
  q := -(q+1)
end
{ q := a div d is the quotient, r = a mod d is the remainder }
```

Modular Exponentiation.

- In cryptography it is important to be able to find $b^n \bmod m$ efficiently where b, n and m are large integers. It is impractical to first compute b^n and then find its remainder when divided by m because b^n will be a huge number. Instead, we can use an algorithm that employs the binary expansion of the exponent n, say $n = (a_{k-1} \cdots a_1 a_0)_2$.

Algorithm 5 Modular Exponentiation.

Procedure modular exponentiation (b: integer, $n = (a_{k-1}a_{k-2} \cdots a_1 a_0)_2$ m: positive integers)

```
x := 1
power := b mod m
for i := 0 to k-1
begin
    if a_i = 1 then x := (x · power) mod m
    power := (power · power) mod m.
end
{ x equals b^n mod m }
```

Example Use algorithm 5 to find $3^{644} \bmod 645$.

Solution:

$b = 3$, $n = 644$ $m = 645$

Algorithm 5 initially sets $x = 1$ and power $= 3 \bmod 645 = 3$. In the computation of $3^{644} \bmod 645$, this algorithm determines $3^{2^j} \bmod 645$ for $j = 1, 2, \ldots, 9$ by successively squaring and reducing modulo 645.

- $i=0$: Because $a_0=0$, we have $x=1$ and power $=3^2 \bmod 645 = 9$
- Copy from book Page 239

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 a variable, is called a linear congruence.

- To find all integers x that satisfy this congruence we need an integer $\bar{a}$ such ~~to~~ that $\bar{a}a \equiv 1 \pmod{m}$, if such an integer exists. Such an integer $\bar{a}$ is said to be an inverse of modulo 'm'.
- Theorem 3: guarantees that an inverse of 'a' modulo 'm' exists whenever 'a' and 'm' are relatively prime
- Theorem: If a and m are relatively prime integers and $m>1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m. (That is, there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and every other inverse of a modulo m is congruent to $\bar{a}$ modulo m).

Proof: Because $\gcd(a,m)=1$, there are integers s and t such that

$$sa + tm = 1$$

This implies that

$$sa + tm \equiv 1 \pmod{m}$$

- Because $tm = 0 \pmod{m}$ it follows that

$$sa \equiv 1 \pmod{m}$$

- Consequently, 's' is an inverse of 'a' modulo 'm'.

Example: (i) Find an integer x for which $56x \equiv 1 \bmod 93$.

$ax \equiv b \bmod (m)$

$a = 56, \quad b = 1 \quad m = 93, \quad x = ?$

gcd (56, 93)

$93 = 56 \times 1 + 37$

$56 = 37 \times 1 + 19$

$37 = 19 \times 1 + 18$

$19 = 18 \times 1 + 1$

gcd(56, 93) = 1,

$sa + tm = 1$

~~$56s + 93t = 1$~~

$1 = 19 - 18$

$= 19 - (37 - 19)$

$= 19 \times 2 - 37$

$= (56 - 37 \times 1) \times 2 - 37$

$= 56 \times 2 - 37 \times 3$

- $56 \times 5 + 93(-3) = 1$

$56 \times 5 \equiv 1 \bmod (93)$

$x = 5$ is the solution.

Example (ii) Find all integers x for which $5x \equiv 12 \bmod 19$

Solution:

$ax \equiv b \pmod m$

$a = 5, \; b = 12, \; m = 19, \; x = ?$

gcd(a, m)

$5x \equiv 12 \pmod{19}$

or $5x - 19t = 12$

- gcd(5, 19) = 1

∵ 1 | 12, this method will give solutions.

$19 = 5 \times 3 + 4$

$5 = 4 \times 1 + 1$

$1 = 5 - 4$

$1 = 5 - (19 - 5 \times 3) = 5 - 19 + 5 \times 3$

$1 = 5 \times 4 - 19 \times 1$

$x = 4$

$1 = 4 \times 5 - 1 \times 19$

Multiply by 12, on both sides we get

$12 = 5 \times 48 - 19 \times 12$

- $(x_0, d_0) = (48, 12)$
- $5 \times 48 \equiv 12 \pmod{19}$.
- Hence a particular answer to $5x \equiv 12 \pmod{19}$ is $x = 48$.
- General solution $x = 19t + 48$, $t \in \mathbb{Z}$

THEOREM 4: The Chinese Remainder Theorem.

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

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_n \pmod{m_n}$$

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

Example.

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$

$\gcd(3,5) = 1$
$\gcd(3,7) = 1$
$\gcd(5,7) = 1$

$\therefore$ 3, 5 & 7 are relatively prime.

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

$M_1 = \frac{m}{3} = 35$, $M_2 = \frac{m}{5} = 21$, $M_3 = \frac{m}{7} = 15$

Example. • 2 is an inverse of $M_1 = 35 \bmod 3$, because $35 \equiv 2 \pmod 3$.

• 1 is an inverse of $M_2 = 21 \bmod 5$, because $21 \equiv 1 \pmod 5$

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

• The solution of the system are those x, such that

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$
$= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$
$\equiv 23 \pmod{105}$

$233 = 105 \times 2 + 23$

• It follows that 23 is the smallest positive integer that is a simultaneous solution.

· Solve the system of congruences.

$x \equiv 1 \pmod 3$

$x \equiv 4 \pmod 5$

$x \equiv 6 \pmod 7$

Solution:

$m = 3 \times 5 \times 7 = 105$

$M_1 = 35$

$M_2 = 21$

$M_3 = 15$

· 2 is inv

· Same as previous

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$x \equiv 1 \times 35 \times 2 + 4 \times 21 \times 1 + 6 \times 15 \times 1$

$x \equiv 70 + 84 + 90$

$x \equiv 244$

$x \equiv 34 \pmod{105}$

· 34 is smallest positive integer that is a simultaneous solution.

· $x = 105l + 34 \quad l \in \mathbb{Z}$

Example

Find all solution to the system of congruences.

$x \equiv 2 \pmod 3$

$x \equiv 1 \pmod 4$

$x \equiv 3 \pmod 5$

Solution:

$\gcd(3,4)=1$, $\gcd(4,5)=1$, $\gcd(3,5)=1$

$\therefore$ 3, 4 and 5 are relatively prime

$m = 3 \times 4 \times 5 = 60$

$M_1 = 20$, $M_2 = 15$ $M_3 = 12$

- 2 is an inverse of $M_1 = 20 \bmod 3$, because

$20 \equiv 2 \pmod 3$

$y_1 = 2$

- $y_2 = 3$

$15 \equiv 3 \pmod 4$

- $y_3 = 2$

$\because 12 \equiv 2 \pmod 5$

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$x \equiv 2 \times 20 \times 2 + 1 \times 15 \times 3 + 3 \times 12 \times 2$

$x \equiv 80 + 45 + 72$

$x \equiv 197$

$x \equiv 17 \pmod{60}$

$x = 17$

$x = 60 \times l + 17 \quad l \in Z$

- Suppose that $m_1, m_2 \ldots m_n$ are pairwise relative prime integers greater than or equal to 2 and let 'm' be their product. By the Chinese Remainder theorem, we can show that integer a with $0 \leq a < m$ can be uniquely represented by n-tuple consisting of its remainders upon division by m_i, $i = 1, 2 \ldots n$. That is we can uniquely represent 'a' by.

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

Example With $m_1 = 3$ $m_2 = 4$, we can represent non-negative integers less than 12.

$0 = (0,0)$	$4 = (1,0)$	$8 = (2,0)$
$1 = (1,1)$	$5 = (2,1)$	$9 = (0,1)$
$2 = (2,2)$	$6 = (0,2)$	$10 = (1,2)$
$3 = (0,3)$	$7 = (1,3)$	$11 = (2,3)$

- To perform arithmetic with large integers, we select moduli $m_1, m_2, \ldots m_n$, where each m_i is an integer greater than 2, $\gcd(m_i, j) = 1$, whenever $i \neq j$, and $m = m_1 m_2 \cdots m_n$ is greater than the result of the arithmetic operations we want to carry out.
- Once we have selected our moduli, we carry out arithmetic operations with large integers by performing component wise operations on the n-tuples representing these integers using their remainders upon division by m_i, $i = 1, 2, \ldots, n$.

Once we have computed the value of each n_2 component in the result, we recover its value by solving a system of n congruences modulo m_i, $i = 1, 2 \ldots n$.

- This method of performing arithmetic with large integers has following features.
  (1) It can be used to perform arithmetic with integers larger than can ordinarily be carried out on computer.
  (2) Computations with respect to the different moduli can be done in parallel, speeding up the arithmetic.

Example Suppose performing arithmetic with integers less than 100 on a certain processor is much quicker.

- We use $m_1 = 99$, $m_2 = 98$, $m_3 = 97$, $m_4 = 95$ to add and multiply 123,684 and 413,456.
- 123,684 can be represented by
  (33, 8, 9, 89)

  413,456 can be represented by
  (32, 92, 42, 16)

- $\therefore m_1 m_2 m_3 m_4 = 89,403,930$
  Every number less than 89,403,903 can be represented uniquely by 4-tuples.
- To find the sum of 123,684 and 413,456 we work with these 4-tuples.

$(33, 8, 9, 89) + (32, 92, 42, 16)$

$= (65 \bmod 99,\ 100 \bmod 98,\ 51 \bmod 97,$
$105 \bmod 95)$

$= (65, 2, 51, 10)$

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

$x \equiv 65 \pmod{99}$

$x \equiv 2 \pmod{98}$

$x \equiv 51 \pmod{97}$

$x \equiv 10 \pmod{95}$

- $x = 537,140$

MATRICES: A matrix is a rectangular array of numbers. A matrix with m rows and n columns is called m x n matrix.

- The plural of matrix is matrices.
- A matrix with same no. of rows as columns is called square matrix.
- Two matrices are equal if they have the same number of rows and the same number of columns and the corresponding entries in every position are equal.
- A square matrix A is called symmetric if $A = A^T$. Thus $A = [a_{ij}]$ is symmetric if $a_{ij} = a_{ji}$ for all i and j with $1 \leq i \leq n$ and $1 \leq j \leq n$.
- A matrix is symmetric if and only if it is a square and it is symmetric with respect to its main diagonal.

Example $\begin{bmatrix} 1 & 1 & 0 \\ 1 & 6 & 1 \\ 0 & 1 & 0 \end{bmatrix}$ is symmetric.

Zero-one Matrices.

- A matrix with entries that are either 0 or 1 is called a zero-one matrix.
- Zero-one matrix are often used to represent discrete structures.
- The Boolean arithmetic is based on the Boolean operations $\vee$ and $\wedge$, which operate on pairs of bits defined by.

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

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

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

Example: Find the join and meet of the zero-one matrices

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

Solution.

Join of A and B is.

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

The meet of A and B is.

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

Boolean Product of two matrices.

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

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

- The Boolean product of A and B is obtained in an analogous way to the ordinary product of these matrices, but with addition replaced by with the operation $\vee$ and the multiplication replaced with the operation $\wedge$.

Example: Find the Boolean Product of A and B, where

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

Solution: The Boolean Product $A \odot B$ is given by.

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

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

- **Algorithm: The Boolean Product**

```
Procedure Boolean product (A, B : zero-one matrices)
for i := 1 to m
    for j := 1 to n
    begin
      c_ij := 0
      for q := 1 to k
          c_ij := c_ij ∨ (a_iq ∧ b_qj)
    end.
{ C = [c_ij] is the Boolean product of A and B }
```

- Boolean powers of a square zero-one matrix are used in studies of path in graphs, which are used to model such things as communications path in computer networks.

- Let A be a square ~~matrix~~ zero-one matrix and let r be a positive integer. The rth Boolean power of A is the Boolean product of r factors of A. The r^{th} Boolean product of A is denoted by $A^{[r]}$. Hence,

$$A^{[r]} = \underbrace{A \odot A \odot A \ldots \odot A}_{r \text{ time.}}$$

Also

$$A^{[0]} = I_n.$$

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

Solution: We define that

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

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

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

$A^{[n]} = A^{[5]}$ for all positive integers n with $n \geq 5$.

- There are n^2 entries in $A \odot B$.
- A total of n ORs and n ANDs are used to find an entry of $A \odot B$.
- Hence, $2n$ bit operations are used to find each entry.
- Therefore, $2n^3$ bit operations are required to compute $A \odot B$.

• Hashing function:

$$h(k) = k \bmod m$$

For example, when $m = 111$, the record of the customer with social Security number 064212848 is assigned to the memory location 14, because.

$$h(064212848) = 064212848 \bmod 111 = 14.$$

• Pseudorandom Numbers

We choose four integers, the modulus m, multiplier a, increment c and seed x_0, with $2 \le a < m$, $0 \le c < m$ and $0 \le x_0 < m$.

We generate a sequence of pseudorandom numbers $\{x_n\}$, with $0 \le x_n < m$ for all n, by successively using the congruence.

$$x_{n+1} = (a x_n + c) \bmod m.$$

Let $m = 9$, $a = 7$, $c = 4$ & $x_0 = 3$.

$$x_1 = (7x_0 + 4) \bmod 9 = 7$$

$$x_2 = (7x_1 + 4) \bmod 9 = 8.$$

CRYPTOLOGY:

• First replace each letter by an integer from 0 to 25, based on its position in the alphabet. For example, replace A by 0, K by 10 and Z by 25. Cesar's encryption method can be represented by the function f that assigns to the non-negative integers p, $p \le 25$, the integer $f(p)$ in set $\{0, 1, \ldots 25\}$ with

$$f(p) = (p+3) \bmod 26$$

In the encrypted version of the message, the letter represented by p is replaced with the letter represented by $(p+3) \bmod 26$.

Example: What is the secret message produced from the message "MEET YOU IN THE PARK" using Caesar Ciphers?

Solution:

First replace the letters in the message with the numbers

12 4 4 19 24 14 20 8 13 19 7 4 15 0 17 10

Now replace each of these numbers p by $f(p) = (p+3) \bmod 26$. This gives.

15 7 7 22 1 17 23 11 16 22 10 7 18 3 20 13

Translating this back to letter produces the encrypted message.

"PHHW BRX LQ WKH SOUN".

- To recover the original message from a secret message encrypted by the Caesar cipher.

$f^{-1}(p) = (p-3) \bmod 26$ ..

The process of determining the original message from the encrypted message is called decryption.

- Generalized Cesar cipher

$$f(p) = (p+k) \bmod 26$$

Such cipher is called a shift cipher. Note that decryption can be carried out using

$$f^{-1}(p) = (p-k) \bmod 26$$

- Some of the basic properties of divisibility of integers are given in Theorem 1.

Theorem 1: Let a, b and c be the integers.

(i) if $a|b$ and $a|c$, then $a|(b+c)$

(ii) if $a|b$, then $a|bc$ for all integers c;

(iii) if $a|b$ and $b|c$, then $a|c$

Proof: Suppose that $a|b$ and $a|c$. Then, 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 $b+c$.

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.

What is Corollary?: