Discrete Structures (CSC 160)

(Lecture Note for B.Sc. CSIT Second Semester)

By Prajwal B. S. Kansakar

Prime College

October, 2018

Note: This is a work in progress. Please send your suggestions and comments at

prajwalknk@gmail.com

Contents

Unit 2

Integers and Matrices

2.1 Integers

2.1.1 The Integers and Division

A nonzero integer a is said to **divide** an integer b if there exists an integer c such that

$$b = ac.$$

In this case we say that a is a **factor** or **divisor** of b and b is a **multiple** of a. If a divides b then we denote it by $a \mid b$; if a does not divide b, we denote it by $a \nmid b$.

For example, $a = 3$ divides $b = 21$ because there exists an integer $c = 7$ such that $21 = 3 \times 7$. So $3 \mid 21$. Similarly, $a = 4$ divides $b = -64$ because there exists an integer $c = -16$ such that $-64 = 4 \times (-16)$. Also, $a = 5$ divides $b = 0$ because there exists $c = 0$ such that $0 = 5 \times 0$. However, $a = 3$ does not divide $b = 14$ because there is no integer c such that $14 = 3 \times c$. So $3 \nmid 14$.

Theorem: Let a, b and c be integers. Then

(i) if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$.

(ii) if $a \mid b$ then $a \mid bc$ for all integers c.

(iii) if $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof:

(i) If $a \mid b$, then $b = am$ for some integer m. If $a \mid c$, then $c = an$ for some integer n. So

$$b + c = am + an = a(m + n).$$

That is, there exists an integer $k = m + n$ such that $b + c = ak$ and therefore $a \mid (b + c)$.

(ii) If $a \mid b$, then $b = an$ for some integer n. So $bc = anc$. That is, there exists an integer $k = nc$ such that $bc = ak$ and therefore $a \mid bc$.

(iii) If $a \mid b$, then there exists an integer m such that $b = am$. If $b \mid c$, then there exists an integer n such that $c = bn$. Then

$$c = bn = bam = abm = ak$$

where $k = bm$. Therefore $a \mid c$.

□

Corollary: If a, b and c are integers such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ for any integers m and n.

Proof: If $a \mid b$, then $a \mid mb$ and if $a \mid c$ then $a \mid nc$ for any integers m and n (by Theorem 1 (ii)). Therefore $a \mid mb + nc$ (by Theorem 1 (i)). □

If $d \mid a$, then there is an integer q such that $a = dq$. But if $d \nmid a$, then there is a quotient as well as a remainder as shown by the following theorem which is commonly called The Division Algorithm.

Theorem (The Division Algorithm): Let a be an integer and d be a positive integer. Then there exists unique integers q and r with $0 \le r < d$ such that

$$a = dq + r.$$

The number a in the above theorem is called the **dividend**, d is called the **divisor**, q is called the **quotient** and r is called the **remainder**. We denote the quotient q and remainder r by the following notation:

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

For example, if $a = 107$ and $d = 5$, then there exists quotient $q = 21$ and remainder $r = 2$ such that

$$107 = 5 \times 21 + 2.$$

Similarly if $a = -87$ and $d = 4$, then there exists quotient $q = -22$ and remainder $r = 1$ such that

$$-87 = 4 \times (-22) + 1.$$

Note that the remainder r is always greater than or equal to zero. If the remainder is zero, then the integer a is divisible by d.

2.1.2 Primes and Greatest Common Divisors

An integer p greater than 1 is said to be **prime** if the only positive divisors of p are 1 and p itself. A positive integer greater than 1 that is not prime is called **composite**.

For example, 5, 7, 11 etc. are prime integers whereas 4, 9, 15 etc are composite integers. Note that 1 is neither prime nor composite.

Theorem (The Fundamental Theorem of Arithmetic): Every positive integer greater than 1 is either a prime or can be written uniquely as the product of two or more primes where the prime factors are written in order of nondecreasing size.
Such unique way of writing an integer as product of primes is called its **prime factorization**.

Example:
Write the following integers in its prime factorization form:

1. $7 = 7$
2. $9 = 3 \times 3 = 3^2$
3. $14 = 2 \times 7$
4. $28 = 2 \times 2 \times 7 = 2^2 \times 7$
5. $2010 = 2 \times 3 \times 5 \times 67$
6. $2205 = 3 \times 3 \times 5 \times 7 \times 7 = 3^2 \times 5 \times 7^2$

Theorem: There are infinitely many primes.

Proof: Suppose that there are only finitely many primes, say $p_1, p_2, \cdots, p_n$. Let

$$q = p_1 p_2 \cdots p_n + 1.$$

By the Fundamental Theorem of Arithmetic, q is either a prime or can be written as a product of two or more primes. Since $q \neq p_i$ for any $i = 1, 2, \cdots, n$, so q is not a prime. Therefore q must be a product of two or more of the primes $p_1, \cdots, p_n$. But $p_i \nmid q$ for any i because otherwise $p_i \mid (q - p_1 p_2 \cdots p_n) = 1$. So q is not a product of primes as well which contradicts the Fundamental Theorem of Arithmetic. Therefore, there must be infinitely many primes. □

Given two integers a and b not both zero, their **greatest common divisor**, denoted by $\gcd(a, b)$, is defined as the largest integer d such that $d \mid a$ and $d \mid b$.

For example, $\gcd(75, 60) = 15$, $\gcd(-24, 36) = 12$, $\gcd(28, 0) = 28$.

If

$$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} \qquad \text{and} \qquad b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$$

are prime factorizations of a and b respectively, then

$$\gcd(a, b) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \cdots p_n^{\min(r_n, s_n)}.$$

Examples:

1. Find $\gcd(120, 500)$.
   Solution: We have the prime factorizations of 120 and 500 as

   $$\begin{aligned} 120 &= 2^3 \times 3 \times 5 \\ 500 &= 2^2 \times 5^3. \end{aligned}$$

   Therefore

   $$\gcd(120, 500) = 2^{\min(3,2)} \times 3^{\min(1,0)} \times 5^{\min(1,3)} = 2^2 \times 3^0 \times 5^1 = 4 \times 5 = 20.$$

Two integers a and b are said to be **relatively prime** if $\gcd(a, b) = 1$.

For example, the integers 15 and 22 are relatively prime because $\gcd(15, 22) = 1$. Similarly 3 and 11 are also relatively prime as $\gcd(3, 11) = 1$.

The integers $a_1, a_2, \cdots, a_n$ are said to be **pairwise relatively prime** if $\gcd(a_i, a_j) = 1$ for each $1 \leq i, j \leq n, i \neq j$.

For example, $6, 35, 17$ are pairwise relatively prime because $\gcd(6, 35) = 1$, $\gcd(35, 17) = 1$ and $\gcd(6, 17) = 1$.

Given two positive integers a and b, their **least common multiple**, denoted by $\text{lcm}(a, b)$, is defined as the smallest positive integer d such that $a \mid d$ and $b \mid d$.

For example, $\text{lcm}(15, 20) = 60$, $\text{lcm}(12, 36) = 36$.

If

$$a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} \quad \text{and} \quad b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$$

are prime factorizations of a and b respectively, then

$$\text{lcm}(a, b) = p_1^{\max(r_1, s_1)} p_2^{\max(r_2, s_2)} \cdots p_n^{\max(r_n, s_n)}.$$

Examples:

1. Find $\text{lcm}(120, 500)$.
   Solution: We have the prime factorizations of 120 and 500 as

   $$\begin{aligned} 120 &= 2^3 \times 3 \times 5 \\ 500 &= 2^2 \times 5^3. \end{aligned}$$

   Therefore

   $$\text{lcm}(120, 500) = 2^{\max(3,2)} \times 3^{\max(1,0)} \times 5^{\max(1,3)} = 2^3 \times 3^1 \times 5^3 = 3000.$$

Theorem: For positive integer a and b,

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

Proof: Let $a = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ and $b = p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$ so that

$$\gcd(a, b) = p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \cdots p_n^{\min(r_n, s_n)}$$

and

$$\text{lcm}(a, b) = p_1^{\max(r_1, s_1)} p_2^{\max(r_2, s_2)} \cdots p_n^{\max(r_n, s_n)}.$$

Then

$$\begin{aligned} \gcd(a, b) \cdot \text{lcm}(a, b) &= (p_1^{\min(r_1, s_1)} p_2^{\min(r_2, s_2)} \cdots p_n^{\min(r_n, s_n)})(p_1^{\max(r_1, s_1)} p_2^{\max(r_2, s_2)} \cdots p_n^{\max(r_n, s_n)}) \\ &= p_1^{\min(r_1, s_1) + \max(r_1, s_1)} p_2^{\min(r_2, s_2) + \max(r_2, s_2)} \cdots p_n^{\min(r_n, s_n) + \max(r_n, s_n)}. \end{aligned}$$

But $\min(r, s) + \max(r, s) = r + s$ for any integers r and s and therefore

$$\gcd(a, b) \cdot \text{lcm}(a, b) = p_1^{r_1 + s_1} p_2^{r_2 + s_2} \cdots p_n^{r_n + s_n} = (p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n})(p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}) = ab.$$

□

2.1.3 Euclidean and Extended Euclidean Algorithm

If the prime factorization of two integers a and b are known, then it is very easy to calculate their greatest common divisor as shown in previous examples. However, finding prime factorization of an integer can be a very time-consuming process. So we use the **Euclidean algorithm** which is a more efficient method of finding the GCD between two integers. It is based upon the fact given by the division algorithm that for any two integers a and b, we can find quotient q and remainder $0 \leq r < b$ such that $a = bq + r$ and the following theorem which uses this result:

Theorem: If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

So the GCD of a and b is the same as the GCD of the divisor b and the remainder r. We can use this fact to successively reduce the remainder to zero. At this stage, the last nonzero remainder in the sequence of divisions would be the GCD between a and b.

Procedure gcd(a, b : positive integers)

```
    $x = a$
    $y = b$
    WHILE $y \neq 0$ {
        $r = x$ mod $y$
        $x = y$
        $y = r$
    }
```

$\{\gcd(a, b)$ is $x\}$.

For example, to find the GCD of 306 and 657, using division algorithm we first write

$$657 = 306 \times 2 + 45.$$

By above theorem, $\gcd(657, 306) = \gcd(306, 45)$. Again we can write

$$306 = 45 \times 6 + 36$$

so that $\gcd(306, 45) = \gcd(45, 36)$ by the theorem. Now

$$45 = 36 \times 1 + 9$$

so that $\gcd(45, 36)) = \gcd(36, 9)$. Finally,

$$36 = 9 \times 4 + 0$$

so $\gcd(36, 9) = \gcd(9, 0)$. But $\gcd(9, 0) = 9$ so $\gcd(657, 306) = 9$ is the last nonzero remainder in the sequence of divisions.

Theorem: If a and b are positive integers, then there exists integers s and t such that

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

The **extended Euclidean algorithm** can be used to find the integers s and t of the above theorem. Since $\gcd(657, 306) = 9$ so there exists integers s and t such that

$$9 = 657s + 306t.$$

To find such s and t, we start from the second-last division step which we can write as

$$9 = 45 - 36 \times 1.$$

But from the third-last division step, we can write the remainder 36 as $36 = 306 - 45 \times 6$. Substituting this in the above equation we get

$$9 = 45 - 36 \times 1 = 45 - (306 - 45 \times 6) = 45 \times 7 - 306.$$

Again from the first division step, we can write the remainder 45 as $45 = 657 - 306 \times 2$. Substituting this in the previous equation, we get

$$9 = (657 - 306 \times 2) \times 7 - 306 = 657 \times 7 + 306 \times (-15).$$

Thus $s = 7$ and $t = -15$.

Procedure extgcd(a, b : nonnegative integers with $a \geq b$)

```
IF $b = 0$ THEN $d = a, s = 1, t = 0$
ELSE {
    $s_2 = 1, s_1 = 0, t_2 = 0, t_1 = 1$
    WHILE $b \neq 0${
        $q = a$ div $b, r = a$ mod $b, s = s_2 - qs_1, t = t_2 - qt_1$
        $a = b, b = r, s_2 = s_1, s_1 = s, t_2 = t_1, t_1 = t$
    }
    $d = a, s = s_2, t = t_2$
}
```

$\{d$ is the $\gcd(a, b)$ with coefficients s and $t.\}$

2.1.4 Integers and Algorithms

1. **Addition:** This is an algorithm for adding two positive integers a and b whose binary expansions 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.

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

   ```
   $c = 0$
   FOR $i = 0$ TO $n - 1${
   ```

```
        $d = \left\lfloor \frac{(a_i + b_i + c)}{2} \right\rfloor$
        $s_i = a_i + b_i + c - 2d$
        $c = d$
    }
    $s_n = c$
    {the binary expansion of the sum is $(s_n s_{n-1} \cdots s_0)_2$}.
```

For example, let us add two 4-bit binary numbers $a_3a_2a_1a_0 = 1111$ and $b_3b_2b_1b_0 = 1010$ using this algorithm:

$c = 0$

i	a_i	b_i	$d = \left\lfloor \frac{a_i + b_i + c}{2} \right\rfloor$	$s_i = a_i + b_i + c - 2d$	$c = d$
0	1	0	0	1	0
1	1	1	1	0	1
2	1	0	1	0	1
3	1	1	1	1	1

$s_4 = c = 1.$

Hence the addition of binary digits $a_3a_2a_1a_0 = 1111$ and $b_3b_2b_1b_0 = 1010$ results in $s_4s_3s_2s_1s_0 = 11001$.

2. **Multiplication:** This is an algorithm to multiply two positive integers a and b whose binary expansions 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.

   Procedure multiply(a, b: positive integers with binary expansions $(a_{n-1}a_{n-2} \cdots a_1a_0)_2$ and $(b_{n-1}b_{n-2} \cdots b_1b_0)_2$ respectively)

```
    FOR $i = 0$ TO $n - 1${
        IF $b_i = 1$ THEN $c_i = a$ followed by $i$ zeros
        ELSE $c_i = 0$
    }
    {$c_0, c_1, \cdots, c_{n-1}$ are the partial products}
    $p = 0$
    FOR $i = 0$ TO $n - 1$
        $p = p + c_i$
    {$p$ is the value of $ab$}
```

   For example, let us multiply two 4-bit binary numbers $a_3a_2a_1a_0 = 1111$ and $b_3b_2b_1b_0 = 1010$ using this algorithm:

   $p = 0$

i	b_i	c_i	$p = p + c_i$
0	0	0	0
1	1	11110	11110
2	0	0	11110
3	1	1111000	10010110

Hence the multiplication of binary digits $a_3a_2a_1a_0 = 1111$ and $b_3b_2b_1b_0 = 1010$ results in 10010110.

3. **Division and Remainder:** For an integer a and a positive integer d, we find the quotient $q = a$ div d and the remainder $r = a$ mod d.

   Procedure division(a: integer, d: positive integer)

```
$q = 0$
$r = |a|$
WHILE $r \geq d${
    $r = r - d$
    $q = q + 1$
}
IF $a < 0${
    IF $r > 0$ THEN {
        $r = d - r$
        $q = -(q + 1)$
    }
    ELSEIF $r = 0$ THEN
        $q = -q$
}
{$q$ is the quotient and $r$ is the remainder}
```

2.1.5 Modular Arithmetic

Given two integers a and b and a positive integer m, we say that a **is congruent to** b **modulo** m if m divides $a - b$. We use the notation $a \equiv b(\text{mod } m)$ to denote that a is congruent to b modulo m. If m does not divide $a - b$ then we write $a \not\equiv b(\text{mod } m)$.

For example, $a = 37$ is congruent to $b = 7$ modulo $m = 3$ and we write $37 \equiv 7(\text{mod } 3)$ because 3 divides $37 - 7 = 30$. Similarly, $-27 \equiv 6(\text{mod } 11)$. But $86 \not\equiv 5(\text{mod } 10)$ because 10 does not divide $86 - 5 = 81$.

Basic properties of congruence modulo m: Let a, b, c be integers and m a positive integer. Then

1. $a \equiv a(\text{mod } m)$ for any integer a.

   Proof: Since $a - a = 0 = m \times 0$ so m divides $a - a$ for any integer a. Therefore $a \equiv a(\text{mod } m)$.

2. If $a \equiv b(\bmod m)$ then $b \equiv a(\bmod m)$.

   Proof: If $a \equiv b(\bmod m)$ then m divides $a - b$ i.e. $a - b = mk$ for some integer k. Then $b - a = m \times (-k)$ as well i.e. m divides $b - a$ and so $b \equiv a(\bmod m)$.

3. If $a \equiv b(\bmod m)$ and $b \equiv c(\bmod m)$ then $a \equiv c(\bmod m)$.

   Proof: If $a \equiv b(\bmod m)$ then $a - b = mk$ for some integer k and if $b \equiv c(\bmod m)$ then $b - c = ml$ for some integer l. So

   $$a - c = a - b + b - c = mk + ml = m(k + l)$$

   and therefore m divides $a - c$. Hence $a \equiv c(\bmod m)$.

Theorem 1: Let m be a positive integers. Then $a \equiv b(\bmod m)$ if and only if there is an integer k such that $a = b + km$.

Proof: Suppose $a \equiv b(\bmod m)$. Then by definition, m divides $a-b$ so there exists some integer k such that $a - b = km$ i.e. $a = b + km$. Conversely, suppose that $a = b + km$ for some integer k. Then $a - b = km$ i.e., m divides $a - b$ and therefore $a \equiv b(\bmod m)$. □

Theorem 2: Let a and b be integers and m a positive integer. Then $a \equiv b(\bmod m)$ if and only if $a \bmod m = b \bmod m$.

Proof: Let $a \bmod m = r_1$ and $b \bmod m = r_2$ so that $a = q_1m + r_1$, $b = q_2m + r_2$ for some unique integers q_1, q_2, r_1, r_2 with $0 \leq r_1, r_2 < m$.
Suppose $a \equiv b(\bmod m)$. Then $a = b + km$ for some integer k. So

$$a = b + km = q_2m + r_2 + km = (q_2 + k)m + r_2.$$

But $a = q_1m + r_1$ as well. So by uniqueness of quotients and remainders, we get $r_1 = r_2$.
Conversely suppose that $r_1 = r_2$ so that $a - q_1m = b - q_2m$. Then $a - b = (q_1 - q_2)m$ i.e., m divides $a - b$. Hence $a \equiv b(\bmod m)$. □

For example, $37 \equiv 7(\bmod 3)$ is equivalent to the fact that $37 \bmod 3 = 7 \bmod 3 = 1$. Also $86 \not\equiv 5(\bmod 4)$ because $86 \bmod 4 \neq 5 \bmod 4$.

Corollary: 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 of remainder, $a \bmod m = a - km$ and $b \bmod m = b - lm$ for some integers k and l. Now

$$(a + b) - ((a \bmod m) + (b \bmod m)) = (a + b) - ((a - km) + (b - lm)) = (k + l)m,$$

that is, $(a + b) - ((a \bmod m) + (b \bmod m))$ is divisible by m and therefore

$$a + b \equiv ((a \bmod m) + (b \bmod m)) \mod m.$$

Hence by Theorem 2,

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

Similarly

$$ab - ((a \text{ mod } m)(b \text{ mod } m)) = ab - ((a-km)(b-lm)) = (al+bk-klm)m,$$

that is, $ab - ((a \text{ mod } m)(b \text{ mod } m))$ is divisible by m and therefore

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

Hence by Theorem 2,

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

□

Theorem 3: Let m be a positive integer. If $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then $a+c \equiv b+d(\text{mod } m)$ and $ac \equiv bd(\text{mod } m)$.

Proof: If $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$ then (by Theorem 1), $a = b+sm$ and $c = d+tm$ for some integers s and t. So

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

and therefore $a+c \equiv b+d(\text{mod } m)$. Also

$$ac = (b+sm)(d+tm) = bd+btm+smd+stm^2 = bd+(bt+sd+stm)m$$

and therefore $ac \equiv bd(\text{mod } m)$. □

Corollary: Let m be a positive integer. If $a \equiv b(\text{mod } m)$ then $ac \equiv bc(\text{mod } m)$ and $a+c \equiv b+c(\text{mod } m)$ for any integer c.

Proof: Since m divides $0 = c-c$ so $c \equiv c(\text{mod } m)$ for any integer c. Hence (by Theorem 3 above), $ac \equiv bc(\text{mod } m)$ and $a+c \equiv b+c(\text{mod } m)$. □

2.1.6 Applications of Number Theory

1. **Linear Congruences:**

   An **inverse of** a **modulo** m is an integer s such that $sa \equiv 1(\text{mod } m)$. For example, -2 is an inverse of 3 modulo 7 because $-2 \cdot 3 \equiv 1(\text{mod } 7)$.

   If $\gcd(a,m) = 1$, then we can calculate inverse of a modulo m as follows: since $\gcd(a,m) = 1$, by using the extended Euclidean algorithm, we can find integers s and t such that $sa+tm = 1$ i.e, $sa-1 = tm$. Since m divides tm, so m divides $sa-1$ i.e. $sa \equiv 1(\text{mod } m)$. So we have found an inverse s of a modulo m. Note that if s is an inverse of a modulo m, then so is an integer $s+mk$ for any integer k because

   $$(s+mk)a-1 = sa+mka-1 = sa-1+mka = tm+mka = m(t+ka)$$

   i.e., $(s+mk)a \equiv 1(\text{mod } m)$.

   Therefore to find the inverse of a modulo m where $\gcd(a,m) = 1$, we do the following:

Step 1. Use the extended Euclidean algorithm to find integers s and t such that

$$sa + tm = 1.$$

Step 2. Then inverse of a modulo m are all integers of the form $s + mk$ for any integer k.

Examples:

(a) Find an inverse of 3 modulo 7.
Solution: Since $\gcd(3, 7) = 1$ so by the extended Euclidean algorithm we have,

$$\begin{aligned} 7 &= 3 \times 2 + 1 \\ 3 &= 1 \times 3 + 0 \end{aligned}$$

Therefore from second-last equation

$$1 = (-2) \times 3 + 1 \times 7.$$

So $s = -2$ is an inverse of 3 modulo 7 as is any integer of the form $-2 + 7k$ where k is any integer. The smallest positive inverse is $-2 \text{ mod } 7 = 5$.

A congruence of the form $ax \equiv b(\text{mod } m)$ where a and b are integers, m is a positive integer and x is an unknown, is called a **linear congruence**.

If $\gcd(a, m) = 1$, then the above linear congruence can be solved. If c is one solution of $ax \equiv b(\text{mod } m)$ i.e., $ac - b = mq$ for some integer q, then any integer congruent to c modulo m is again a solution i.e., any integer of the form $c + mk$ where k is any integer is also a solution of the linear congruence because

$$a(c + mk) - b = ac + amk - b = ac - b + amk = mq + amk = m(q + ak)$$

i.e., $a(c + mk) \equiv b(\text{mod } m)$.

For example, $3x \equiv 4(\text{mod } 7)$ is a linear congruence. Since $\gcd(3, 7) = 1$, this linear congruence can be solved. One solution of this linear congruence is 6 because $3 \cdot 6 \equiv 4(\text{mod } 7)$. Another solution is -8 because $3 \cdot -8 \equiv 4(\text{mod } 7)$. But $6 \equiv -8(\text{mod } 7)$. In fact any integer a that is congruent to 6 modulo 7 is a solution of this linear congruence so that the solutions are integers of the form $6 + 7k$ for any integer k.

To find solution of $ax \equiv b(\text{mod } m)$, we first find an **inverse** s **of** a **modulo** m i.e. an integer s such that $sa \equiv 1(\text{mod } m)$. Multiplying both sides by b, we get $sab \equiv b(\text{mod } m)$. That is $a(sb) \equiv b(\text{mod } m)$ which implies that sb is a solution of the linear congruence $ax \equiv b(\text{mod } m)$. Also any integer of the form $sb + km$ for any integer k is a solution of the linear congruence $ax \equiv b(\text{mod } m)$ as below:
$a(sb + km) - b = sab + kma - b = (sa - 1)b + kma$ where m divides $sa - 1$ so m divides $(sa - 1)b + kma$ i.e., m divides $a(sb + km) - b$. So $sb + km$ is also a solution of $ax \equiv b(\text{mod } m)$.

Therefore to solve the linear congruence $ax \equiv b(\text{mod } m)$, where $\gcd(a, m) = 1$, we do the following:

Step 1. Since $\gcd(a, m) = 1$, find an inverse s of a modulo m.

Step 2. Then solution of the linear congruence $ax \equiv b(\text{mod } m)$ are all integers of the form $sb + km$ for any integer k.

Examples:

(a) Solve the linear congruence $3x \equiv 4(\text{mod } 7)$.
Solution: Here $a = 3$, $b = 4$ and $m = 7$. Since $\gcd(3, 7) = 1$, we calculate an inverse s of 3 modulo 7. Using extended Euclidean algorithm, we have

$$7 = 3 \times 2 + 1$$
$$3 = 1 \times 3 + 0$$

From second-last equation

$$1 = (-2) \times 3 + 1 \times 7.$$

So $s = -2$ is an inverse of 3 modulo 7. Therefore $sb = -2 \times 4 = -8$ is one solution of $3x \equiv 4(\text{mod } 7)$ as is any integer of the form $-8 + 7k$ for any integer k. The smallest positive integer solution is $-8 \text{ mod } 7 = 6$.

2. **Chinese Remainder Theorem:** If $m_1, m_2, \cdots, m_n$ are pairwise relatively prime integers and $a_1, a_2, \cdots, a_n$ are arbitrary integers, then the system of linear congruences

$$x \equiv a_1(\text{mod } m_1),$$
$$x \equiv a_2(\text{mod } m_2),$$
$$\vdots$$
$$x \equiv a_n(\text{mod } m_n)$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$. That is, if x_1 and x_2 are two such solutions, then $x_1 \equiv x_2(\text{mod } m)$.

To find such solution, we do the following:

Step 1. Let $m = m_1 m_2 \cdots m_n$ and $M_k = \dfrac{m}{m_k}$ for each $k = 1, 2, \cdots, n$.

Step 2. Since $\gcd(M_k, m_k) = 1$, find an inverse s_k of M_k modulo m_k for each k.

Step 3. Then solution of the given system of linear congruences is any integer x such that

$$x \equiv a_1 M_1 s_1 + a_2 M_2 s_2 + \cdots + a_n M_n s_n (\text{mod } m).$$

Example:

(a) Solve the following Chinese remainder problem:

$$x \equiv 2(\text{mod } 3), x \equiv 3(\text{mod } 5), x \equiv 2(\text{mod } 7).$$

Solution: Here $a_1 = 2, a_2 = 3, a_3 = 2$ and $m_1 = 3, m_2 = 5, m_3 = 7$. Let

$$m = m_1 m_2 m_3 = 3 \times 5 \times 7 = 105,$$

and

$$M_1 = \frac{m}{m_1} = 35, M_2 = \frac{m}{m_2} = 21, M_3 = \frac{m}{m_3} = 15.$$

Calculation of inverse s_1 of $M_1 = 35$ modulo $m_1 = 3$:

Using extended Euclidean algorithm,

$$\begin{aligned} 35 &= 3 \times 11 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

so by back-substitution from second last equation,

$$1 = 3 - 2 \times 1 = 3 - (35 - 11 \times 3) \times 1 = (-1) \times 35 + 12 \times 3.$$

Therefore $s_1 = -1$.

Calculation of inverse s_2 of $M_2 = 21$ modulo $m_2 = 5$:

Using extended Euclidean algorithm,

$$\begin{aligned} 21 &= 5 \times 4 + 1 \\ 5 &= 1 \times 4 + 0 \end{aligned}$$

so by back-substitution

$$1 = 1 \times 21 + (-4) \times 5.$$

Therefore $s_2 = 1$.

Calculation of inverse s_3 of $M_3 = 15$ modulo $m_3 = 7$:

Using extended Euclidean algorithm,

$$\begin{aligned} 15 &= 7 \times 2 + 1 \\ 7 &= 1 \times 7 + 0 \end{aligned}$$

so by back-substitution

$$1 = 1 \times 15 + (-2) \times 7.$$

Therefore $s_3 = 1$.

Hence one solution of the given system is

$$a_1 M_1 s_1 + a_2 M_2 s_2 + a_3 M_3 s_3 = 2 \times 35 \times (-1) + 3 \times 21 \times 1 + 2 \times 15 \times 1 = 23$$

as is any integer of the form $23 + mk = 23 + 105k$ for any integer k.

3. **Computer Arithmetic with Large Integers:**
   Representation of an integer by an n-tuple: Let $m_1, m_2, \ldots, m_n$ be integers all greater than or equal to 2 and pairwise relatively prime. Suppose $m = m_1 m_2 \cdots m_n$. Then any integer a such that $0 \leq a < m$ can be uniquely represented by an n-tuple as follows:

$$(a \bmod m_1, a \bmod m_2, \cdots, a \bmod m_n).$$

For example, let $m_1 = 3, m_2 = 5, m_3 = 8$ be three pairwise relatively prime integers. Then $m = m_1m_2m_3 = 120$, so every integer a such that $0 \leq a < 120$ can be uniquely represented as a 3-tuple. For instance, $a = 39$ is represented as

$$(39 \text{ mod } 3, 39 \text{ mod } 5, 39 \text{ mod } 8) = (0, 4, 7).$$

When large integers are involved in arithmetic operations, a computer may not be able to handle the data that is generated or the time taken to generate the results may be very high. In such cases, it is preferable to have a way where we can instead work on a number of small integers, perform the operations on those small integers and then combine the results to get the solution to the original problem. This approach has the advantage that we are able to perform arithmetic operations on integers larger than those that can usually be handled by a computer and also the operations on smaller integers can be done in parallel, thus speeding up the process.

We can use the Chinese remainder theorem to perform addition operation on large integers a and b by working on smaller integers as described above. For this, we first select n pairwise relatively prime integers $m_1, m_2, \ldots, m_n$ each greater than or equal to 2 such that $0 \leq a, b < m$ where $m = m_1m_2\cdots m_n$. Then there is a unique representation of a and b as n-tuples with components as the remainders obtained after dividing a and b by m_i, $1 \leq i \leq n$. That is, a is represented as

$$(a \text{ mod } m_1, a \text{ mod } m_2, \ldots, a \text{ mod } m_n)$$

and b is represented as

$$(b \text{ mod } m_1, b \text{ mod } m_2, \ldots, b \text{ mod } m_n).$$

We now carry out the addition operation of a and b by performing component wise addition operation modulo m on the n-tuple representation. Once we have computed the value of each component in the result, we recover the sum of a and b by solving a system of n congruences modulo m_i, $1 \leq i \leq n$ by again using the Chinese remainder theorem.

Example: Find the sum of numbers 123684 and 413456 by representing the numbers as 4-tuple by using remainders modulo of pairwise relatively prime numbers less than 100.

Solution: Let $a = 123684$ and $b = 413456$. Let $m_1 = 99$, $m_2 = 98$, $m_3 = 97$ and $m_4 = 95$ be four pairwise relatively prime integers less than 100. Then representing a as a 4-tuple, we get

$$(a \text{ mod } 99, a \text{ mod } 98, a \text{ mod } 97, a \text{ mod } 95) = (33, 8, 9, 89).$$

Representing b as a 4-tuple, we get

$$(b \text{ mod } 99, b \text{ mod } 98, b \text{ mod } 97, b \text{ mod } 95) = (32, 92, 42, 16).$$

The integer $a + b$ is represented as a 4-tuple by

$$(33 + 32 \text{ mod } 99, 8 + 92 \text{ mod } 98, 9 + 42 \text{ mod } 97, 89 + 16 \text{ mod } 95) = (65, 2, 51, 10).$$

We now find the integer represented by this 4-tuple by solving the following system of congruences using Chinese remainder theorem:

$$\begin{aligned} x &\equiv 65 (\operatorname{mod} 99), \\ x &\equiv 2 (\operatorname{mod} 98), \\ x &\equiv 51 (\operatorname{mod} 97), \\ x &\equiv 10 (\operatorname{mod} 95). \end{aligned}$$

Here $a_1 = 65$, $a_2 = 2$, $a_3 = 51$, $a_4 = 10$, $m_1 = 99$, $m_2 = 98$, $m_3 = 97$ and $m_4 = 95$. Let

$$m = m_1 m_2 m_3 m_4 = 89403930,$$

and

$$M_1 = \frac{m}{m_1} = 903070, M_2 = \frac{m}{m_2} = 912285, M_3 = \frac{m}{m_3} = 921690, M_4 = \frac{m}{m_4} = 941094.$$

Now, inverse of $M_1 = 903070$ modulo $m_1 = 99$ is $s_1 = 37$, inverse of $M_2 = 912285$ modulo $m_2 = 98$ is $s_2 = 33$, inverse of $M_3 = 921690$ modulo $m_3 = 97$ is $s_3 = 24$ and inverse of $m_4 = 941094$ modulo $m_4 = 95$ is $s_4 = 4$. (DO THE DETAIL CALCULATIONS YOURSELF)
Hence the solution of the given system is

$$x \equiv a_1 M_1 s_1 + a_2 M_2 s_2 + a_3 M_3 s_3 + a_4 M_4 s_4 (\operatorname{mod} m) \equiv 3397886480 (\operatorname{mod} m)$$

The smallest positive value of x satisfying this congruence is 537140 which is our solution i.e., $a + b = 537140$.

4. **Primality testing and pseudoprimes:** Given an integer p, the testing done to determine whether p is prime or not, is called **primality testing**. One way of determining primes uses the following theorem of Fermat:

   Theorem (Fermat's Little Theorem): If p is prime then for any integer a such that $\gcd(a, p) = 1$, we have
   $$a^{p-1} \equiv 1 (\operatorname{mod} p).$$

   Therefore by Fermat's little theorem, if we can find an integer a such that $\gcd(a, p) = 1$ but $a^{p-1} \not\equiv 1 \pmod p$, then we have conclusive proof that p is not prime i.e. p is composite. But note that the converse of this theorem is not true. So even if we find integers a (no matter how many) such that $\gcd(a, p) = 1$ and $a^{p-1} \equiv 1 \pmod p$, it is not a conclusive proof that p is a prime number. It may still be a composite number. If an integer p satisfying the above conditions actually happens to be a composite number then we call such p a **pseudoprime** to the base a. Therefore primality testing using Fermat's little theorem cannot conclusively determine every time whether a given integer p is prime or not.

   The following procedure tests an integer for primality using Fermat's little theorem. The test will output one of two results: "p is Composite" or "p is Probably Prime".

Step 1. Choose a random integer $a \in \{2, 3, \cdots, p - 1\}$.

Step 2. Compute $\gcd(a, p)$. If it is greater than 1, then stop and output "p is Composite". Otherwise go to the next step.

Step 3. If $a^{p-1} \not\equiv 1 \pmod{p}$, then stop and output "$p$ is Composite".

Step 4. If $a^{p-1} \equiv 1 \pmod{p}$, then p may be a prime number. Do one of the following:

Return to Step 1 and repeat the process with a new a.

OR

Output "p is Probably Prime" and stop.

2.2 Matrices

A **zero-one matrix** or a **Boolean matrix** is a matrix all of whose entries are either 0 or 1.

For example,

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

is a zero-one matrix of order 3×4.

2.2.1 Boolean Matrix Operations

Two or more Boolean matrices can be combined to form new Boolean matrices using different operations. We study those operations in this section.

Join of Boolean matrices: Given two $m \times n$ Boolean matrices $A = [a_{ij}]$ and $B = [b_{ij}]$, their **join**, denoted by $A \vee B$ is an $m \times n$ Boolean matrix $A \vee B = [c_{ij}]$ whose entries $c_{ij} = a_{ij} \vee b_{ij}$ are defined as follows:

$$c_{ij} = a_{ij} \vee b_{ij} = \begin{cases} 1 & \text{if either } a_{ij} = 1 \text{ or } b_{ij} = 1 \\ 0 & \text{if } a_{ij} = b_{ij} = 0 \end{cases}$$

Example:

1. Given

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

find $A \vee B$.

Solution: We have

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

Meet of Boolean matrices: Given two $m \times n$ Boolean matrices $A = [a_{ij}]$ and $B = [b_{ij}]$, their **meet**, denoted by $A \wedge B$ is an $m \times n$ Boolean matrix $A \wedge B = [c_{ij}]$ whose entries $c_{ij} = a_{ij} \wedge b_{ij}$ are defined as follows:

$$c_{ij} = a_{ij} \wedge b_{ij} = \begin{cases} 1 & \text{if } a_{ij} = b_{ij} = 1 \\ 0 & \text{if either } a_{ij} = 0 \text{ or } b_{ij} = 0 \end{cases}$$

Example:

1. Find $A \wedge B$ if

$$A = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

. **Solution:** We have

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

Boolean product: Given an $m \times p$ Boolean matrix $A = [a_{ij}]$ and an $p \times n$ Boolean matrix $B = [b_{jk}]$, their **Boolean product**, denoted by $A \odot B$, is an $m \times n$ Boolean matrix $A \odot B = [c_{ik}]$ whose entries c_{ik} are defined as

$$c_{ik} = (a_{i1} \wedge b_{1k}) \vee (a_{i2} \wedge b_{2k}) \vee \cdots \vee (a_{ip} \wedge b_{pk}).$$

Example:

1. If

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}$$

then find $A \odot B$.
Solution: We have

$$A \odot B$$

$$= \begin{pmatrix} (1 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 1) & (1 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 0) & (0 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 1) & (0 \wedge 0) \vee (1 \wedge 0) \vee (0 \wedge 1) \\ (1 \wedge 1) \vee (1 \wedge 0) \vee (0 \wedge 1) & (1 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 0) & (1 \wedge 0) \vee (1 \wedge 1) \vee (0 \wedge 1) & (1 \wedge 0) \vee (1 \wedge 0) \vee (0 \wedge 1) \\ (0 \wedge 1) \vee (0 \wedge 0) \vee (1 \wedge 1) & (0 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 0) & (0 \wedge 0) \vee (0 \wedge 1) \vee (1 \wedge 1) & (0 \wedge 0) \vee (0 \wedge 0) \vee (1 \wedge 1) \end{pmatrix}$$

$$= \begin{pmatrix} 1 \vee 0 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 0 \vee 0 \\ 0 \vee 0 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 0 \vee 0 \\ 1 \vee 0 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 1 \vee 0 & 0 \vee 0 \vee 0 \\ 0 \vee 0 \vee 1 & 0 \vee 0 \vee 0 & 0 \vee 0 \vee 1 & 0 \vee 0 \vee 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix}.$$

If A is an $n \times n$ Boolean matrix, then for an integer $r > 0$, we define the r^{th} **Boolean power** of A, denoted by $A^{[r]}$, as

$$A^{[r]} = \underbrace{A \odot A \odot \cdots \odot A}_{r \text{ times}}.$$

If $r = 0$, we define $A^{[0]} = I_n$.

Complement of Boolean matrix: Given am $m \times n$ Boolean matrix $A = [a_{ij}]$, its complement, denoted by $\overline{A}$, is an $m \times n$ Boolean matrix $\overline{A} = [b_{ij}]$, whose entries b_{ij} are defined as follows:

$$b_{ij} = \begin{cases} 1 & \text{if } a_{ij} = 0 \\ 0 & \text{if } a_{ij} = 1 \end{cases}$$

Example:

1. Find $\overline{A}$ if $A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$

   Solution: We have

$$\overline{A} = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

2.3 Exercise

2.3.1 Integers

1. Compute the following

   (a) $97 \bmod 12$, 97 div 12

   (b) $126 \bmod 25$, 126 div 25

   (c) $168 \bmod 8$, 168 div 8

   (d) $16 \bmod 25$, 16 div 25

   (e) $-526 \bmod 12$, -526 div 12

   (f) $-242 \bmod 56$, -242 div 56

   (g) $-25 \bmod 31$, -25 div 31

   (h) $-65 \bmod 13$, -65 div 13

2. Find the GCD of the following pair of integers using the Euclidean algorithm:

   (a) $143, 227$

   (b) $306, 657$

   (c) $272, 147$

   (d) $12378, 3054$

   (e) $56, 72$

   (f) $24, 138$

   (g) $119, 272$

   (h) $1769, 2378$

3. Use the extended Euclidean algorithm to express the GCD above as a linear combination of the given numbers.
4. Show that 15 is an inverse of 7 modulo 26.
5. Show that 937 is an inverse of 13 modulo 2436.
6. Find an inverse of 4 modulo 9.
7. Find an inverse of 2 modulo 17.
8. Find an inverse of 19 modulo 141.
9. Find an inverse of 144 modulo 233.
10. Solve the following linear congruences:

    (a) $25x \equiv 15 \pmod{29}$

    (b) $5x \equiv 2 \pmod{26}$

    (c) $8x \equiv 15 \pmod{21}$

    (d) $36x \equiv 8 \pmod{5}$

    (e) $34x \equiv 60 \pmod{19}$

    (f) $140x \equiv 133 \pmod{11}$

11. Solve the following Chinese remainder problem:

    (a) $x \equiv 2 \pmod{3}, x \equiv 1 \pmod{4}, x \equiv 3 \pmod{5}$

    (b) $x \equiv 1 \pmod{3}, x \equiv 2 \pmod{5}, x \equiv 3 \pmod{7}$

    (c) $x \equiv 5 \pmod{11}, x \equiv 14 \pmod{29}, x \equiv 15 \pmod{31}$

    (d) $x \equiv 5 \pmod{6}, x \equiv 4 \pmod{11}, x \equiv 3 \pmod{17}$

    (e) $x \equiv 1 \pmod{2}, x \equiv 2 \pmod{3}, x \equiv 3 \pmod{5}, x \equiv 4 \pmod{11}$

(f) $x \equiv 1 \pmod{5}$, $x \equiv 9 \pmod{6}$, $x \equiv 1 \pmod{7}$, $x \equiv 9 \pmod{11}$

12. Find the sum of 236988 and 332367 by decomposing it into a 4-tuple obtained by dividing them by the integers $m_1 = 99$, $m_2 = 98$, $m_3 = 97$ and $m_4 = 95$.

2.3.2 Matrices

1. Compute the join $A \vee B$ and the meet $A \wedge B$ of the following Boolean matrices. Also compute $\overline{A}$ and $\overline{B}$.

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

2. Compute Boolean product $A \odot B$ of following Boolean matrices.

$$A = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Also compute $\overline{A}$ an $\overline{B}$.

3. Compute Boolean product of following Boolean matrices.

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

4. Compute B^3 of matrix B above.