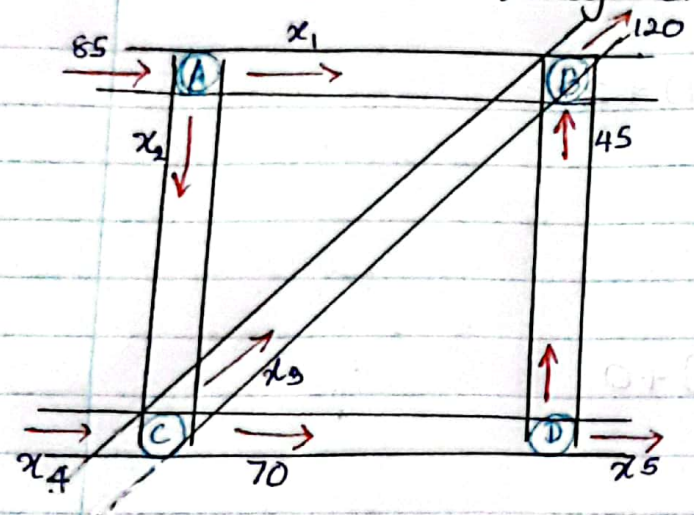
Modular Algorithms for Linear Algebra.

Make a linear system for following traffic flow.



$$x_1 + x_2 = 85 \quad (A)$$
$$x_1 + x_3 + 45 = 120 \quad (B)$$
$$x_3 + 70 = x_4 + x_2 \quad (C)$$
$$45 + x_5 = 70 \quad (D)$$
$$85 + x_4 = 120 + x_5 \quad (\text{Full system})$$

We can find x_i's (ie $\{1, 2, 3, 4, 5\}$) by solving following linear system.

$$\begin{aligned} x_1 + x_2 &= 85 \\ x_1 + x_3 &= 75 \\ x_2 - x_3 + x_4 &= 70 \\ x_5 &= 25 \\ x_4 - x_5 &= 35 \end{aligned}$$

Elementry Number Theory.

* Division Algorithm

Given integers a and b with $b > 0$, there exists unique integers q and r s.t, $a = bq + r$ where $0 \le r < b$.

(q : quotient
r : remainder)

Example

① $a = 5, b = 3, r = ?, q = ?$

$5 = 3(q) + r \quad = 5 = 3(1) + 2$

$q = 1, \quad r = 2$ //

② $a = -3, b = 1, r = ?, q = ?$

$(-3) = 1(q) + r \quad = \quad 1(-3) + 0$

$\therefore \quad q = -3, \quad r = 0$ //

③ $a = -2, b = -7, q = ?, r = ?$

$(-2) = (-7)q + r = (-7)(1) + 5$

$q = 1, \quad r = 5$ //

④ $a = -7, \quad b = -2, \quad q = ?, \quad r = ?$

$(-7) = (-2)(q) + r \quad = (-2)(4) + 1$

$q = 4, \quad r = 1$ //

Euclidean Algorithm

- This is used to find the gcd of two non-zero integers.
- Let $a, b \in \mathbb{Z} \setminus \{0\}$ and $\gcd(a,b) = r_n$

ans =

→

$$a = q_1 b + r_1 \quad ; \quad 0 \le r_1 < b$$

$$b = q_2 r_1 + r_2 \quad ; \quad 0 \le r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \quad ; \quad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad ; \quad 0 \le r_n < r_{n-1}$$

$$r_{n-1} = q_{n+1} r_n + 0$$

$$\gcd(a, b) = r_n .$$

* ~~gcd of~~ $\gcd(a, b)$ can be written as a linear combination of a and b as,

$$xa + yb = r_n \qquad x, y \in \mathbb{R}$$

* Here x and y are called as Bézout's coefficients

Example

① $\gcd(12374, 3054) = ?$

$$12374 = (4)(3054) + 158$$
$$3054 = (19)(158) + 52$$
$$158 = (3)(52) + (2) = \gcd(12374, 3054)$$
$$52 = (26)(2) + 0$$

Find Bézout's coefficients of $x(12374) + y(3054) = 2$

$$x(12374) + y(3054) = 2$$

$x(12374) + y(3054) = (158) - 3(52)$

$x(12374) + y(3054) = (158) - 3[3054 - 19(158)]$

~~$x(12374) + (y+19)(3054) - (-19)(158) =$~~

$x(12374) + y(3054) = 58x(158) - 3(3054)$

$x(12374) + y(3054) = 58(12374 - 4(3054)) - 3(3054)$

$x(12374) + y(3054) = (58)(12374) - (232+3)(3054)$

$x(12374) + y(3054) = 58(12374) + (-235)(3054)$

$\therefore$ $x = 58$, $y = -235$ } Bézout's coefficients.

Theory of Congruences

Let n be a fixed positive integer. Two integers a and b are said to be congruent modulo n,

$a \equiv b \pmod{n} \rightarrow n \mid a-b$

$a = qn + b$

Congruent classes

If we consider modulo 4 congruence relation,

$[0] = \{x \mid x \equiv 0 \bmod 4\} = \{\ldots, -8, -4, 0, 4, 8, \ldots\}$

$[1] = \{x \mid x \equiv 1 \bmod 4\} = \{\ldots, -7, -3, 1, 5, 9, \ldots\}$

$[2] = \{x \mid x \equiv 2 \bmod 4\} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$

$[3] = \{x \mid x \equiv 3 \bmod 4\} = \{\ldots, -5, -1, 3, 7, 11, \ldots\}$

↓ columns

$a \equiv b \pmod{4} \Leftrightarrow a, b$ are in the same column

Chinese Remainder Theorem

Steps

NOTE

Given: $x \equiv b_1 \pmod{p_1}$
$x \equiv b_2 \pmod{p_2}$
$\vdots$
$x \equiv b_k \pmod{p_k}$

- Let p_i's, (where $i \in \{1, 2, \ldots, k\}$) $\in \mathbb{Z}$ be pairwise comprime (i.e $\gcd(p_i, p_{i+n}) = 1$
- $b_i \in \mathbb{Z}$

Then the system has solutions, as a unique congruence class,
$\{y \in \mathbb{Z} : y \equiv x \pmod{p_1 p_2 \ldots p_k}\}$

Given: $x \equiv a_i \pmod{m_i}$, for $i = 1, \ldots, r$
(m_i are pairwise relatively prime)
The solution set of congruences,
$x \equiv a_1 b_1 \frac{M}{m_1} + \ldots + a_r b_r \frac{M}{m_r} \pmod{M}$

Step 1 : Calculate $M = m_1 . m_2 \ldots m_r$

Step 2 : Calculate $\frac{M}{m_i}$, for $i = 1, \ldots, r$

To find b_i

Step 3 : Determine b_i using $b_i \frac{M}{m_i} \equiv 1 \pmod{m_i}$ or

3) i) : Find c_i in $\frac{M}{m_i} \equiv c_i \bmod m_i$ using try and error metho

3) ii) : Find b_i using $b_i \cdot c_i \equiv 1 \bmod(m_i)$
(use try & error method)

Step 4: Find the solution of set of congruence by,
$x \equiv a_1 b_1 \frac{M}{m_1} + \dots + a_r b_r \frac{M}{m_1} \pmod{M}$.

Example

Use CRT to find an x s.t

$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 7$
$x \equiv 10 \pmod{11}$

$\gcd(5,7) = \gcd(5,11) = \gcd(7,11) = 1$

* $M = 5 \times 7 \times 11 = 385$

* $\frac{M}{m_1} = \frac{385}{5} = 77$

$\frac{M}{m_2} = \frac{385}{7} = 55$

$\frac{M}{m_3} = \frac{385}{11} = 35$

* $b_i \frac{M}{m_i} \equiv 1 (\bmod m_i)$

$b_1 \cdot 77 \equiv 1 \pmod 5$
$3 \cdot 77 \equiv 1 \pmod 5$ } $b_1 = 3$

$b_2 \cdot 55 \equiv 1 \pmod 7$
$6 \cdot 55 \equiv 1 \pmod 7$ } $b_2 = 6$

$b_3 \cdot 35 \equiv 1 \pmod{11}$

- $35 \equiv c_i \pmod{11}$

  $c_i \equiv 2$

- $2 b_3 \equiv 1 \pmod{11}$

  $2 \cdot 6 \equiv 1 \pmod{11}$

$\Big\}$ $b_3 = 6$

$\therefore x \equiv (2)(3)(77)+(3)(6)(55)+(10)(6)(35) \pmod{385}$

$x \equiv 3552 \pmod{385}$

(2)

Use CRT to find an x s.t

$$\left.\begin{aligned} 2x &\equiv 6 \pmod{14} \\ 3x &\equiv 9 \pmod{15} \\ 5x &\equiv 20 \pmod{60} \end{aligned}\right\} \quad \begin{aligned} x &\equiv 3 \pmod{7} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 4 \pmod{6} \end{aligned}$$

$\gcd(7,5) = \gcd(7,6) = \gcd(5,6) = 1$

* $M = 7 \times 5 \times 6 = 210$
* $\frac{M}{m_1} = \frac{210}{7} = 30$
* $\frac{M}{m_2} = \frac{210}{5} = 42$
* $\frac{M}{m_3} = \frac{210}{6} = 35$
* $b_i \frac{M}{m_i} \equiv 1 \pmod{m_i}$

$b_1 \cdot 30 \equiv 1 \pmod{7}$

$4 \cdot 30 \equiv 1 \pmod{7}$

$\Big\}$ $b_1 = 4$

$b_2 \cdot 42 \equiv 1 \pmod 5$
$3 \cdot 42 \equiv 1 \pmod 5$ $\Big\}$ $b_2 = 3$

$b_3 \cdot 35 \equiv 1 \pmod 6$
$5 \cdot 35 \equiv 1 \pmod 6$ $\Big\}$ $b_3 = 5$

$x \equiv a_1(3)(4)(30) + (3)(3)(42) + (4)(5)(35) \pmod{210}$
$\equiv 1438 \pmod{210}$

Modular Algorithms

Variants of modular algorithms:

1. Big prime (with $m = p$ for a prime p)
2. Small primes (with $m = p_1 p_2 \cdots p_r$ for pairwise distinct primes $p_1, \ldots, p_r$ using CRT)
3. Prime power modular algorithms (with $m = p^r$ for a prime p) using lifting.

Modular Determinant computation

Hadamard's inequality

Let $A \in \mathbb{R}^{n \times n}$ with row vectors $f_1, f_2, \ldots, f_n \in \mathbb{R}^{1 \times n}$.
$B \in \mathbb{R}$. $|a_i| \leq B$, $\forall a_i$ where a_i is the i^{th} entry of A.

$$A^{n \times n} = \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} \quad \text{where } f_n = (a_1, a_2, \ldots, a_n)$$

Since $|a_i| \leq B$,

$$\|f_1\|_2 = \sqrt{a_1^2 + a_2^2 + a_3^2 + \ldots + a_n^2} \leq \sqrt{B^2 + B^2 + \ldots + B^2} = \sqrt{nB^2}$$

$$\|f_1\|_2 \leq n^{1/2} B$$

$$|\det A| \leq \|f_1\| \|f_2\| \ldots \|f_n\|$$

$$\leq (n^{1/2}B)(n^{1/2}B)\ldots(n^{1/2}B)$$

$$|\det A| \leq n^{n/2} \cdot B^n$$

$$|\det(A)| \leq \underbrace{n^{n/2} B^n}$$

↑ Hadamard's bound

Using Big Prime

Given ; Compute detA using Big Prime.

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

Steps :

Step 1 : Find the Hadamard's bound(H)

Step 2 : Find a big prime P s.t $P > 2H+1$

Step 3 : Convert A in $\mathbb{Z}$ into A_p in $\mathbb{Z}/p\mathbb{Z}$

$$A_p = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} (\text{mod } P)$$

$$A_p = \begin{pmatrix} a_1 (\text{mod } P) & a_2 (\text{mod } P) \\ a_3 (\text{mod } P) & a_4 (\text{mod } P) \end{pmatrix}$$

Step 4 : Find $\det(A_p)$

Then, $[\det A) \equiv (\det A_p) (\text{mod } P)$

Step 5 : Write the congruence relation class. The least absolute value in the class is the determinant. (with its' original sign)

Example

$A = \begin{pmatrix} 4 & 5 \\ 6 & -7 \end{pmatrix}$. Choose a suitable prime and use big-prime modular method to compute the det A.

$n = 2, \quad B = 7$

$\therefore H = n^{\frac{n}{2}} B^n = 2 \cdot 7^2 = 49 \times 2$

$H = 98$

Choose $P > 2H + 1 = 2 \times 98 + 1$

$P > 197$

$\therefore$ Choose $P = 199$

$A_p = \begin{pmatrix} 4 & 5 \\ 6 & -7 \end{pmatrix} (\text{mod } 199)$

$= \begin{pmatrix} 4 & 5 \\ 6 & 192 \end{pmatrix}$

$\det A_p = 4 \times 192 - 6 \times 5$

$= 768 - 30$

$= 738$

$\therefore \det A \equiv 738 (\text{mod } 199)$

$\det A \equiv 141 (\text{mod } 199)$

if $\det A = d$

$d_i \in \{\ldots, -257, -58, 141, 340, 539, \ldots\}$

$\det A = \min |d_i|$ (with its original sign)

$\det A = -58$ //

Small Primes modular Computation.

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}$$

Step 1: Find the Hadamard's bound (H)

Step 2: Find small primes P_i s.t $P_1 P_2 \ldots P_r > 2H+1$

Step 3: Convert A in $\mathbb{Z}$ into A_{P_i} in $\mathbb{Z}/P_i\mathbb{Z}$ $\forall i \in \{1,2,\ldots,r\}$

$$A_{P_i} = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} (\text{mod } P_i) = \begin{pmatrix} a_1 (\text{mod } P_i) & a_2 (\text{mod } P_i) \\ a_3 (\text{mod } P_i) & a_4 (\text{mod } P_i) \end{pmatrix}$$

Step 4: Find $\det(A_{P_i})$ $\forall P_i$ wher $i \in \{1,2,\ldots,r\}$

Then $(\det A) \equiv (\det A_{P_i}) (\text{mod } P_i)$ $\forall i = 1,2,\ldots,r$
(Here we have a system)

Step 5: Solve above system using CRT.

Step 6: Follow step 5 in Big Prime.

Example

Let $A = \begin{pmatrix} 4 & 5 \\ 6 & -7 \end{pmatrix}$. Use small-primes modular method Compute det A

$H = n^{n/2} B^n = 2^{2/2} \cdot 7^2 = 98$

$P_1 \cdot P_2 \cdots P_r > 2H+1 = 197$

$\therefore P_1 P_2 P_3 P_4 = 2.3.5.7 > 197$

rough work

$P_1 = 2$

$P_1 P_2 = 2.3 = 6$

$P_1 P_2 P_3 = 6.5 = 30$

$P_1 P_2 P_3 P_4 = 30 \times 7 = 210$

$210 > 199$

$\therefore r = 4$

$A_{P_1} = \begin{pmatrix} 4 & 5 \\ 6 & -7 \end{pmatrix} \pmod 2$

$= \begin{pmatrix} 0 & 1 \\ 0 & -4 \end{pmatrix}$: ....

$\det A_{P_1} = 0$

$\det A \equiv 0 \pmod 2$

$A_{P_2} = \begin{pmatrix} 4 & 5 \\ 6 & -7 \end{pmatrix} \pmod 3$

$= \begin{pmatrix} 1 & 2 \\ 0 & 2 \end{pmatrix}$

$\det A_{P_2} = 2$

$\det A \equiv 2 \pmod 3$

$A_{P_3} = \begin{pmatrix} 4 & 5 \\ 6 & -7 \end{pmatrix} \pmod 5$

$= \begin{pmatrix} 4 & 0 \\ 1 & 3 \end{pmatrix}$

$\det A_{P_3} = 12$

$\det A \equiv 12 \pmod 5$

$\det A \equiv 2 \pmod 5$

$A_{P_4} = \begin{pmatrix} 4 & 5 \\ 6 & -7 \end{pmatrix} \pmod 7$

$= \begin{pmatrix} 4 & 5 \\ 6 & 0 \end{pmatrix}$

$\det A_{P_4} = -30$

$\det A \equiv -30 \pmod 7$

$\det A \equiv 5 \pmod 7$

Lets take $\det A = x$

$x \equiv 0 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 5 \pmod 7$

$gcd(2,3) = gcd(2,5) = gcd(2,7) = gcd(3,5) = gcd(3,7) = gcd(5,7) = 1$

* $M = (2)(3)(5)(7) = 210$

* $\frac{M}{m_1} = \frac{210}{2} = 105$

$\frac{M}{m_2} = \frac{210}{3} = 70$

$\frac{M}{m_3} = \frac{210}{5} = 42$

$\frac{M}{m_4} = \frac{210}{7} = 30$

* $b_i \frac{M}{m_i} \equiv 1 \pmod{m_i}$

$b_1 \cdot 105 \equiv 1 \pmod 2$
$1 \cdot 105 \equiv 1 \pmod 2$ } $b_1 = 1$

$b_2 \cdot 70 \equiv 1 \pmod 3$
$4 \cdot 70 \equiv 1 \pmod 3$ } $b_2 = 4$

$b_3 \cdot 42 \equiv 1 \pmod 5$
$3 \cdot 42 \equiv 1 \pmod 5$ } $b_3 = 3$

$b_4 \cdot 30 \equiv 1 \pmod 7$
$4 \cdot 30 \equiv 1 \pmod 7$ } $b_4 = 4$

$x \equiv (0)(1)(105) + 2(4)(70) + (2)(3)(42) + (5)(4)(30) \pmod{(210)}$
$x \equiv 1412 \pmod{210}$
$x \equiv 152 \pmod{210}$

smallest abs. value

$\det A \in \{\ldots -268, -58, 362, 572, \ldots\}$

$\therefore \det A = -58$ //