Exact Solution of Equations

\[
\begin{bmatrix}
1 & \frac{1}{2} & \frac{1}{3} & \frac{1}{4} \\
\frac{1}{2} & 1 & \frac{1}{4} & \frac{1}{4} \\
\frac{1}{3} & \frac{1}{4} & 1 & \frac{1}{6} \\
\frac{1}{4} & \frac{1}{5} & \frac{1}{6} & \frac{1}{7}
\end{bmatrix}
\begin{bmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4
\end{bmatrix}
=
\begin{bmatrix}
1 \\
2 \\
3 \\
4
\end{bmatrix}
\]
Solving Equations with Integer Coefficients

- Consider an equation of the form $Ax = b$ where the entries are integers or can be made integer by scaling.
- We can solve such a system using the floating-point arithmetic.
- The results will be approximately correct, due to roundoff errors introduced during the computation.
- The floating-point arithmetic is often the preferred approach, however in some situations the exact rational solution is desired.
- In some number theory problems or when the system of equations is ill-conditioned, the floating-point calculations would be inadequate.
- For example, a system of equations involving the Hilbert matrix is notoriously difficult to obtain for dimension above 10.
There are essentially two approaches for solving $Ax = b$ exactly:
- Direct computation using multi-precision arithmetic
- Congruence techniques

The multiple-modulus approach for the congruence technique solves $Ax = b$ in mod $p_i$ for several different moduli $n_1, n_2, \ldots, n_k$ and then combines these results using the Chinese remainder theorem.

Another congruence method, developed by Dixon, solves $Ax = b$ in $\text{GF}(p)$ and uses successive refinements to obtain the solution in mod $p^k$ for a suitably large integer $k$.

Note that mod $p^k$ is not the arithmetic of $\text{GF}(p^k)$.
The congruence techniques find the rational solution of $Ax = b$ with integer coefficients of unlimited size: We increase either the size of each modulus and the number of moduli. Assume that the dimension of the matrix $A$ is $m \times m$, while $x$ and $b$ are $m \times 1$. We denote the determinant of $A$ by $d = \det(A)$ and the adjoint matrix of $A$ by $\text{adj}(A)$, thus, we have

$$A \text{ adj}(A) = \text{adj}(A) A = d \ I$$

where $I$ is the $m \times m$ unit matrix. The solution vector is written as

$$x = \frac{1}{d} \text{ adj}(A) b$$
Let \( n_1, n_2, \ldots, n_k \) be the set of pairwise relative prime numbers and 
\[
N = \prod_{i=1}^{k} n_i
\]
Assume that we choose the moduli set in such a way that each modulus fits into the word size of the computer.
Furthermore, we need to have \( N > 2 \max(|d|, |A_{ij}|) \) and 
\[
\gcd(N, d) = 1, \text{ which implies } \gcd(n_i, d) = 1 \text{ for } i = 1, 2, \ldots, k
\]
The selection of the proper set of the moduli may be difficult, because it requires estimation of the determinant, and furthermore, relative primality is not guaranteed.
It was also suggested that to use a preselected moduli set, knowing that it will fail for some \( A \) matrices.
Steps of the Congruence Technique

Step 1: Using the GE algorithm, solve $k$ linear systems $Ax_i = b \mod n_i$ to find $k$ vectors $x_i \mod n_i$ for $i = 1, 2, \ldots, k$.

Step 2: Compute the determinant $d_i \mod n_i$ for $i = 1, 2, \ldots, k$.

Step 3: Also, compute $y_i = d_i \cdot x_i \mod n_i$ for $i = 1, 2, \ldots, k$.

Step 4: Apply the MRC Algorithm to $(y_1, y_2, \ldots, y_k)$ to compute $y$.

Step 5: Apply the MRC Algorithm to $(d_1, d_2, \ldots, d_k)$ to compute $d$.

Step 6: The exact rational solution is given as

$$x = \frac{1}{d} \cdot y$$
Consider the set of linear equations

\[
\begin{bmatrix}
21 & 12 \\
15 & 17 \\
\end{bmatrix}
\begin{bmatrix}
x_1 \\
x_2 \\
\end{bmatrix}
=
\begin{bmatrix}
1 \\
2 \\
\end{bmatrix}
\]

The determinant of \( A \) is 177 and the largest entry of \( A \) is 21, and therefore, we can select \( N = n_1 n_2 n_3 = 7 \cdot 11 \cdot 13 = 1001 \)
An $2 \times 2$ Example

- Step 1: We need to solve this system of equations mod 7, 11, and 13
- For each modulus, the system is reduced and solved

Solving mod 7:

$$\begin{bmatrix} 0 & 5 \\ 1 & 3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \pmod{7}$$

- We apply the GEA mod 7 and obtain $(x_1, x_2) = (0, 3)$
- We also find the determinant mod 7 as $d = 2$
An $2 \times 2$ Example

- **Solving mod 11:**
  
  \[
  \begin{bmatrix}
  10 & 1 \\
  4 & 6 \\
  \end{bmatrix}
  \begin{bmatrix}
  x_1 \\
  x_2 \\
  \end{bmatrix}
  =
  \begin{bmatrix}
  1 \\
  2 \\
  \end{bmatrix} \pmod{11}
  \]

  We apply the GEA mod 11 and obtain $(x_1, x_2) = (4, 5)$

  We also find the determinant mod 11 as $d = 1$

- **Solving mod 13:**
  
  \[
  \begin{bmatrix}
  8 & 12 \\
  2 & 4 \\
  \end{bmatrix}
  \begin{bmatrix}
  x_1 \\
  x_2 \\
  \end{bmatrix}
  =
  \begin{bmatrix}
  1 \\
  2 \\
  \end{bmatrix} \pmod{13}
  \]

  We apply the GEA mod 13 and obtain $(x_1, x_2) = (4, 5)$

  We also find the determinant mod 13 as $d = 8$
Congruent Solutions

- Mod 7: \((x_1, x_2) = (0, 3)\) and \(d = 2\) \(\rightarrow\) \((y_1, y_2) = (0, 6)\)
- Mod 11: \((x_1, x_2) = (4, 5)\) and \(d = 1\) \(\rightarrow\) \((y_1, y_2) = (4, 5)\)
- Mod 13: \((x_1, x_2) = (4, 5)\) and \(d = 8\) \(\rightarrow\) \((y_1, y_2) = (6, 1)\)

- Apply the MRC algorithm to \(y_1\): \(\text{MRC}(0, 4, 6; 7, 11, 13)\)
- Apply the MRC algorithm to \(y_2\): \(\text{MRC}(6, 5, 1; 7, 11, 13)\)
- Apply the MRC algorithm to \(d\): \(\text{MRC}(2, 1, 8; 7, 11, 13)\)

- The MRC setup requires the computation of \(c_{12}, c_{13},\) and \(c_{23}\) as

\[
\begin{align*}
c_{12} &= n_1^{-1} \pmod{n_2} = 7^{-1} \pmod{11} = 8 \\
c_{13} &= n_1^{-1} \pmod{n_3} = 7^{-1} \pmod{13} = 2 \\
c_{23} &= n_2^{-1} \pmod{n_3} = 11^{-1} \pmod{13} = 6
\end{align*}
\]
The Computation of $x_1$

- The first column of the lower triangular matrix is the given set of remainders $(0, 4, 6)$ from which we compute the rest of the columns:

  
  \[
  \begin{align*}
  0 \\
  4 \cdot (4 - 0) \cdot 8 \pmod{11} &= 10 \\
  6 \cdot (6 - 0) \cdot 2 \pmod{13} &= 12 \cdot (12 - 10) \cdot 6 \pmod{13} &= 12
  \end{align*}
  \]

- To compute $x_1$, we perform the summation

  \[
  x_1 = 0 + 10 \cdot 7 + 12 \cdot 7 \cdot 11
  \]

  \[
  = 994
  \]

  \[
  = -7 \pmod{1001}
  \]

- The last step is necessary to obtain the correctly signed result
The first column of the lower triangular matrix is the given set of remainders \((6, 5, 1)\) from which we compute the rest of the columns:

\[
\begin{align*}
6 \\
5 \cdot (5 - 6) \cdot 8 \pmod{11} &= 3 \\
1 \cdot (1 - 6) \cdot 2 \pmod{13} &= 3 \cdot (3 - 3) \cdot 6 \pmod{13} = 0
\end{align*}
\]

To compute \(x_2\), we perform the summation

\[
x_2 = 6 + 3 \cdot 7 + 0 \cdot 7 \cdot 11 = 27 = +27 \pmod{1001}
\]
The Computation of $d$

- The first column of the lower triangular matrix is the given set of remainders $(2, 1, 8)$ from which we compute the rest of the columns:

\[
\begin{align*}
2 \\
1 & (1 - 2) \cdot 8 \pmod{11} = 3 \\
8 & (8 - 2) \cdot 2 \pmod{13} = 12 \ (12 - 3) \cdot 6 \pmod{13} = 2 \\
\end{align*}
\]

- To compute $d$, we perform the summation

\[
d = 2 + 3 \cdot 7 + 2 \cdot 7 \cdot 11 \\
= 177 \\
= +177 \pmod{1001}
\]
The Final Solution

Therefore, the exact rational solution of the linear equations

\[
\begin{bmatrix}
21 & 12 \\
15 & 17
\end{bmatrix}
\begin{bmatrix}
x_1 \\
x_2
\end{bmatrix} =
\begin{bmatrix}
1 \\
2
\end{bmatrix}
\]

is found as

\[
\begin{bmatrix}
x_1 \\
x_2
\end{bmatrix} =
\begin{bmatrix}
-7 \\
\frac{27}{177}
\end{bmatrix}
\]

The result is correct assuming the any of the intermediate values did not exceed \( N = 1001 \)