

Systems of Congruences

- Systems of linear congruences relative to prime moduli can be solved by methods from linear algebra — e.g. matrix inversion, Cramer's rule, or row reduction.

Systems of linear congruences can be solved using methods from linear algebra: Matrix inversion, Cramer's rule, or row reduction. In case the modulus is prime, everything you know from linear algebra goes over to systems of linear congruences. (The reason is the \mathbb{Z}_p is a **field**, for p prime, and linear algebra works fine over any field — not just \mathbb{R} and \mathbb{C} .)

I will stick to prime moduli for simplicity. I'll assume that you know some linear algebra, even if you haven't seen it done with modular arithmetic.

In the first example, I'll use the well-known fact that a matrix is invertible if and only if its determinant is nonzero.

Example. Solve

$$2x + 6y = 1 \pmod{7}$$

$$4x + 3y = 2 \pmod{7}$$

Write the system in matrix form:

$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}.$$

The determinant of the coefficient matrix is $2 \cdot 3 - 4 \cdot 6 = -18 = 3 \pmod{7}$. In particular, it's nonzero mod 7, so the system has a solution. For a 2×2 system, it's easiest to use the formula for inverting a 2×2 matrix:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = (ad - bc)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

All I have to do is multiply both sides of the equation *on the left* by the inverse of the coefficient matrix:

$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}^{-1} \begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 \\ 2 \end{bmatrix} \begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}^{-1},$$

$$\begin{bmatrix} x \\ y \end{bmatrix} = 5 \cdot \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = 5 \cdot \begin{bmatrix} 5 \\ 4 \end{bmatrix} = \begin{bmatrix} 4 \\ 0 \end{bmatrix}.$$

Recall that $ad - bc = 3 \pmod{7}$. The inverse of 3 mod 7 is 5, since $3 \cdot 5 = 1 \pmod{7}$. This explains the 5 in the second line.

The solution is

$$x = 4 \pmod{7}, \quad y = 0 \pmod{7}. \quad \square$$

Example. Solve

$$x + 2y = 4 \pmod{5}$$

$$3x + y + z = 0 \pmod{5}$$

$$x + y + 2z = 3 \pmod{5}$$

In this case, it's better to use row reduction.

$$\begin{bmatrix} 1 & 2 & 0 & 4 \\ 3 & 1 & 1 & 0 \\ 1 & 1 & 2 & 3 \end{bmatrix} \xrightarrow{r_2 \rightarrow r_2 + 2r_1} \begin{bmatrix} 1 & 2 & 0 & 4 \\ 0 & 0 & 1 & 3 \\ 1 & 1 & 2 & 3 \end{bmatrix} \xrightarrow{r_3 \rightarrow r_3 + 4r_1} \begin{bmatrix} 1 & 2 & 0 & 4 \\ 0 & 0 & 1 & 3 \\ 0 & 4 & 2 & 4 \end{bmatrix} \xrightarrow{r_2 \leftrightarrow r_3} \begin{bmatrix} 1 & 2 & 0 & 4 \\ 0 & 4 & 2 & 4 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

$$\begin{aligned}
& \xrightarrow{r_2 \rightarrow 4r_2} \begin{bmatrix} 1 & 2 & 0 & 4 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \xrightarrow{r_1 \rightarrow r_1 + 3r_2} \begin{bmatrix} 1 & 0 & 4 & 2 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \xrightarrow{r_1 \rightarrow r_1 + r_3} \\
& \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \xrightarrow{r_2 \rightarrow r_2 + 2r_3} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix}
\end{aligned}$$

The solution is

$$x = 0 \pmod{5}, \quad y = 2 \pmod{5}, \quad z = 3 \pmod{5}. \quad \square$$

Example. Solve

$$\begin{aligned}
& + 2y + 2z = 1 \pmod{5} \\
2x + y & = 1 \pmod{5} \\
4x + 2y & = 2 \pmod{5}
\end{aligned}$$

I'll do this by row reduction:

$$\begin{aligned}
& \begin{bmatrix} 0 & 2 & 2 & 1 \\ 2 & 1 & 0 & 1 \\ 4 & 2 & 0 & 2 \end{bmatrix} \xrightarrow{r_1 \leftrightarrow r_3} \begin{bmatrix} 4 & 2 & 0 & 2 \\ 2 & 1 & 0 & 1 \\ 0 & 2 & 2 & 1 \end{bmatrix} \xrightarrow{r_1 \rightarrow 4r_1} \begin{bmatrix} 1 & 3 & 0 & 3 \\ 2 & 1 & 0 & 1 \\ 0 & 2 & 2 & 1 \end{bmatrix} \xrightarrow{r_2 \rightarrow r_2 + 3r_1} \begin{bmatrix} 1 & 3 & 0 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 \end{bmatrix} \xrightarrow{r_2 \leftrightarrow r_3} \\
& \begin{bmatrix} 1 & 3 & 0 & 3 \\ 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_2 \rightarrow 3r_2} \begin{bmatrix} 1 & 3 & 0 & 3 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow{r_1 \rightarrow r_1 + 2r_2} \begin{bmatrix} 1 & 0 & 2 & 4 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}
\end{aligned}$$

The equations are

$$x + 2z = 4 \pmod{5}, \quad y + z = 3 \pmod{5}.$$

There are multiple solutions — in fact, since there is one free variable (z), there will be 5 distinct solutions mod 5. As is customary when a system has multiple solutions, I'll write the solution in parametric form.

Set $z = t$. Then $x + 2t = 4$, so $x = 3t + 4$ (by adding $3t$ to both sides). Likewise, $y + t = 3$, so $y = 4t + 3$. The solution is

$$x = 3t + 4 \pmod{5}, \quad y = 4t + 3 \pmod{5}, \quad z = t \pmod{5}. \quad \square$$

Example. This example has little to do with solving congruences; it's presented to point out that you can work with matrices using modular arithmetic pretty much as usual. I'll compute the inverse mod 3 of the matrix

$$A = \begin{bmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 2 \end{bmatrix}.$$

To do this, tack on a copy of the 3×3 identity matrix, then row reduce the resulting 3×6 matrix. When the block on the left becomes the identity, the block on the right will have turned into A^{-1} .

$$\begin{aligned}
& \begin{bmatrix} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{bmatrix} \xrightarrow{r_3 \rightarrow r_3 + 2r_1} \begin{bmatrix} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 1 \end{bmatrix} \xrightarrow{r_1 \rightarrow r_1 + r_2} \\
& \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 1 \end{bmatrix} \xrightarrow{r_3 \rightarrow r_3 + 2r_2} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix} \xrightarrow{r_1 \rightarrow r_1 + 2r_3}
\end{aligned}$$

$$\begin{bmatrix} 1 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix} \xrightarrow{r_2 \rightarrow r_2 + 2r_3} \begin{bmatrix} 1 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix}$$

Thus,

$$A^{-1} = \begin{bmatrix} 2 & 2 & 2 \\ 1 & 2 & 2 \\ 2 & 2 & 1 \end{bmatrix}. \quad \square$$

Example. Is the following matrix invertible mod 6?

$$\begin{bmatrix} 5 & 1 \\ 3 & 1 \end{bmatrix}$$

When the modulus is not prime, results from linear algebra must be used with care. In this case, I'd like to use the determinant to tell whether the matrix is invertible.

$$\det \begin{bmatrix} 5 & 1 \\ 3 & 1 \end{bmatrix} = 5 - 3 = 2.$$

Normally, a nonzero determinant means that the matrix is invertible. However, mod n the criterion is that the determinant must be *relatively prime* to n . Since $(2, 6) = 2 \neq 1$, the matrix is not invertible. If you try to apply a standard matrix inversion algorithm to find the inverse, you'll find that it won't work. \square