2-28-2019

Systems of Congruences

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 $\mathbb{C}$.)

It's also possible to convert a system to a linear Diophantine equation.

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

$$\begin{aligned} 2x + 6y &= 1 \pmod 7 \\ 4x + 3y &= 2 \pmod 7 \end{aligned}$$

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:

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

If I apply this formula to the coefficient matrix for the system, I get

$$\begin{bmatrix} 2 & 6 \\ 4 & 3 \end{bmatrix}^{-1} = (2 \cdot 3 - 4 \cdot 6)^{-1} \begin{bmatrix} 3 & -6 \\ -4 & 2 \end{bmatrix} = (-18)^{-1} \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix} = 3^{-1} \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix} = 5 \cdot \begin{bmatrix} 3 & 1 \\ 3 & 2 \end{bmatrix}.$$

The inverse of 3 mod 7 is 5, since $3 \cdot 5 = 1 \pmod 7$.

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

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

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

The solution is

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

You can also solve this equation using Cramer's rule, or by row reduction. You can even use basic algebra, though it's a little tedious. Solve the first equation for one of the variables:

$$\begin{aligned} 2x + 6y &= 1 \pmod 7 \\ 2x &= y + 1 \pmod 7 \\ 4 \cdot 2x &= 4 \cdot (y + 1) \pmod 7 \\ x &= 4y + 4 \pmod 7 \end{aligned}$$

Substitute this into the second equation:

$$\begin{aligned} 4x + 3y &= 2 \pmod 7 \\ 4(4y + 4) + 3y &= 2 \pmod 7 \\ 19y + 16 &= 2 \pmod 7 \\ 5y &= -14 = 0 \pmod 7 \\ y &= 0 \pmod 7 \end{aligned}$$

Plugging this back into the x-equation gives $x = 4 \cdot 0 + 4 = 4 \pmod 7$. □

In some cases, you can convert a system to a linear Diophantine equation, which we already know how to solve.

Example. Solve the following system over $\mathbb{Z}_7$:

$$\begin{aligned} 4x + 6y &= 1 \pmod 7 \\ x + 5y &= 2 \pmod 7 \end{aligned}$$

Note that $4 \cdot 5 - 6 \cdot 1 = 0 \pmod 7$. Hence, I can't solve this system by matrix inversion or Cramer's rule.

Note, however, that the first equation is 4 times the second:

$$4(x + 5y) = 4x + 6y, \quad 4 \cdot 2 = 1.$$

So it suffices to solve

$$x + 5y = 2 \pmod 7.$$

This is equivalent to the Diophantine equation

$$x + 5y + 7z = 2.$$

Let $w = x + 5y$. This gives

$$w + 7z = 2.$$

The general solution is

$$w = 2 + 7t, \quad z = 0 - t.$$

z is just a helper variable, so ignore it. Using the w-equation, I have

$$x + 5y = w = 2 + 7t.$$

The general solution is

$$x = 2 + 7t + 5s, \quad y = -s.$$

Recall that the original system was mod 7:

$$x = 2 + 5s \pmod 7, \quad y = 6s \pmod 7.$$

Note that this is a parametrized solution. You could also do this problem by row reduction. □

Example. Solve

$$\begin{aligned} 4x + 6y &= 3 \pmod 7 \\ x + 5y &= 2 \pmod 7 \end{aligned}$$

As before, multiplying the second equation by 4 gives

$$4x + 6y = 1 \pmod 7 .$$

But the two equations now imply "$3 = 1 \pmod 7$", and this contradiction implies that the system has no solutions. □

Example. Solve

$$\begin{array}{rcrcrcll} x & + & 2y & & & = & 4 & \pmod 5 \\ 3x & + & y & + & z & = & 0 & \pmod 5 \\ x & + & y & + & 2z & = & 3 & \pmod 5 \end{array}$$

With a system this large, it's better to use row reduction.

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

$$\xrightarrow[r_2 \to 4r_2]{} \begin{bmatrix} 1 & 2 & 0 & 4 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \xrightarrow[r_1 \to r_1 + 3r_2]{} \begin{bmatrix} 1 & 0 & 4 & 2 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \xrightarrow[r_1 \to r_1 + r_3]{}$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 3 & 1 \\ 0 & 0 & 1 & 3 \end{bmatrix} \xrightarrow[r_2 \to r_2 + 2r_3]{} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 2 \\ 0 & 0 & 1 & 3 \end{bmatrix}$$

The solution is

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

Example. Solve

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

I'll do this by row reduction:

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

$$\begin{bmatrix} 1 & 3 & 0 & 3 \\ 0 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow[r_2 \to 3r_2]{} \begin{bmatrix} 1 & 3 & 0 & 3 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix} \xrightarrow[r_1 \to r_1 + 2r_2]{} \begin{bmatrix} 1 & 0 & 2 & 4 \\ 0 & 1 & 1 & 3 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

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

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

As noted above, it's possible to do a lot of linear algebra mod n. Here's an example.

Example. Compute the inverse mod 3 of the matrix

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

Recall the algorithm for inverting a matrix by row-reduction: Put a copy of the 3×3 identity matrix on the right of the original 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}.

$$\begin{bmatrix} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 2 & 0 & 0 & 1 \end{bmatrix} \xrightarrow[r_3 \to r_3 + 2r_1]{} \begin{bmatrix} 1 & 2 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 1 \end{bmatrix} \xrightarrow[r_1 \to r_1 + r_2]{}$$

$$\begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 2 & 0 & 1 \end{bmatrix} \xrightarrow[r_3 \to r_3 + 2r_2]{} \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix} \xrightarrow[r_1 \to r_1 + 2r_3]{}$$

$$\begin{bmatrix} 1 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix} \xrightarrow[r_2 \to r_2 + 2r_3]{} \begin{bmatrix} 1 & 0 & 0 & 2 & 2 & 2 \\ 0 & 1 & 0 & 1 & 2 & 2 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{bmatrix}$$

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. So, for instance, if you try apply the standard matrix inversion algorithm to find the inverse, you'll find that it won't work. $\square$
