Example 55. (review) Solve $16x \equiv 4 \pmod{25}$.

Solution. We first find $16^{-1} \pmod{25}$. Bézout's identity: $-7 \cdot 25 + 11 \cdot 16$.
Reducing this modulo 25, we get $11 \cdot 16 \equiv 1 \pmod{25}$.
Hence, $16^{-1} \equiv 11 \pmod{25}$.
It follows that $16x \equiv 4 \pmod{25}$ has the (unique) solution $x \equiv 16^{-1} \cdot 4 \equiv 11 \cdot 4 \equiv 19 \pmod{25}$.

Example 56. Solve the system

$$\begin{aligned} 7x + 3y &\equiv 10 \pmod{16} \\ 2x + 5y &\equiv 9 \pmod{16}. \end{aligned}$$

Solution. As a first step we solve the system:

$$\begin{aligned} 7x + 3y &= 10 \\ 2x + 5y &= 9 \end{aligned}$$

However you prefer solving this system (two options below), you will find the unique solution $x = \frac{23}{29}$, $y = \frac{43}{29}$.
To obtain a solution to the congruences modulo 16, all we have to do is to determine $29^{-1} \pmod{16}$ and then use that to reinterpret the solution we just obtained.
$29^{-1} \equiv (-3)^{-1} \equiv 5 \pmod{16}$. Thus, $x = 29^{-1} \cdot 23 \equiv 5 \cdot 7 \equiv 3 \pmod{16}$ and $y = 29^{-1} \cdot 43 \equiv 5 \cdot 11 \equiv 7 \pmod{16}$.
Comment. We should check our answer: $7 \cdot 3 + 3 \cdot 7 = 42 \equiv 10 \pmod{16}$, $2 \cdot 3 + 5 \cdot 7 = 41 \equiv 9 \pmod{16}$.

A naive way to solve 2×2 systems. To solve $7x + 3y = 10$, $2x + 5y = 9$, we can use the second equation to write $x = \frac{9}{2} - \frac{5}{2}y$ and substitute that into the first equation: $7\left(\frac{9}{2} - \frac{5}{2}y\right) + 3y = 10$, which simplifies to $\frac{63}{2} - \frac{29}{2}y = 10$. This yields $y = \frac{43}{29}$. Using that value in, say, the first equation, we get $7x + 3 \cdot \frac{43}{29} = 10$, which results in $x = \frac{23}{29}$.
Solving 2×2 systems using matrix inverses. The equations $7x + 3y = 10$, $2x + 5y = 9$ can be expressed as

$$\begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 10 \\ 9 \end{bmatrix},$$

assuming we are familiar with the basic matrix-vector calculus. A solution is then given by

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 7 & 3 \\ 2 & 5 \end{bmatrix}^{-1} \begin{bmatrix} 10 \\ 9 \end{bmatrix} = \frac{1}{35 - 6} \begin{bmatrix} 5 & -3 \\ -2 & 7 \end{bmatrix} \begin{bmatrix} 10 \\ 9 \end{bmatrix} = \frac{1}{29} \begin{bmatrix} 23 \\ 43 \end{bmatrix}.$$

Here, we used that

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix},$$

one of the few formulas worth memorizing.
Advanced comment. It follows from the matrix inverse discussion that the system

$$\begin{aligned} ax + by &\equiv r \pmod{n} \\ cx + dy &\equiv s \pmod{n} \end{aligned}$$

has a unique solution modulo n if $\gcd(ad - bc, n) = 1$.

The matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible if and only if $ad - bc \neq 0$ (that is, $ad - bc$ is invertible).
The matrix $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ is invertible modulo n if and only if $\gcd(ad - bc, n) = 1$ (that is, $ad - bc$ is invertible modulo n).

Comment. You can also see Theorem 4.9 and Example 4.11 in our textbook for a direct approach modulo 16.

Armin Straub
straub@southalabama.edu

Example 57. (extra) Solve the system

$$\begin{aligned} 2x - y &\equiv 7 \pmod{15} \\ 3x + 4y &\equiv -2 \pmod{15}. \end{aligned}$$

Solution. As a first step we solve the system:

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

You can solve the system any way you like. For instance, using a matrix inverse, we find

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ 3 & 4 \end{bmatrix}^{-1} \begin{bmatrix} 7 \\ -2 \end{bmatrix} = \frac{1}{11} \begin{bmatrix} 4 & 1 \\ -3 & 2 \end{bmatrix} \begin{bmatrix} 7 \\ -2 \end{bmatrix} = \frac{1}{11} \begin{bmatrix} 26 \\ -25 \end{bmatrix}.$$

To obtain a solution to the congruences modulo 15, we determine that $11^{-1} \equiv -4 \pmod{15}$ (you might be able to see this modular inverse; in any case, practice using the Euclidean algorithm to compute these). Therefore, $x = 11^{-1} \cdot 26 \equiv -4 \cdot 11 \equiv 1 \pmod{15}$ and $y = 11^{-1} \cdot (-25) \equiv -4 \cdot 5 \equiv 10 \pmod{15}$.

Check our answer. $2 \cdot 1 - 10 = -8 \equiv 7 \pmod{15}$, $3 \cdot 1 + 4 \cdot 10 = 43 \equiv -2 \pmod{15}$.

5 More on primes

Example 58. (Euclid) There are infinitely many primes.

Proof. Assume (for contradiction) there is only finitely many primes: $p_1, p_2, \ldots, p_n$.
Consider the number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.
Each prime p_i divides $N - 1$ and so p_i does not divide N.
Thus any prime dividing N is not on our list. Contradiction. □

Historical note. This is not necessarily a proof by contradiction, and Euclid (300BC) himself didn't state it as such. Instead, one can think of it as a constructive machinery of producing more primes, starting from any finite collection of primes.