

Example 93. (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 94. Solve the system

$$7x + 3y \equiv 10 \pmod{16}$$

$$2x + 5y \equiv 9 \pmod{16}.$$

Solution. As a first step we solve the system:

$$7x + 3y = 10$$

$$2x + 5y = 9$$

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

$$ax + by \equiv r \pmod{n}$$

$$cx + dy \equiv s \pmod{n}$$

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

The matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is invertible if and only if $ad - bc \neq 0$ (that is, $ad - bc$ is invertible).

The matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ 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 for a direct approach modulo 16.

Example 95. 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 Euclidian 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. $2 \cdot 1 - 10 = -8 \equiv 7 \pmod{15}$, $3 \cdot 1 + 4 \cdot 10 = 43 \equiv -2 \pmod{15}$.

Example 96. (Sun-Tsu) Find a number that leaves the remainders 2, 3, 2 when divided by 3, 5, 7 respectively.

Solution. In other words, we need to solve $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$.

Let us break the problem into three pieces:

- $x \equiv 1 \pmod{3}$, $x \equiv 0 \pmod{5}$, $x \equiv 0 \pmod{7}$. To satisfy the mod 5 and mod 7 congruences, $x = 35z$. We solve $35z \equiv 1 \pmod{3}$ and find $z = 2$. Hence, $x = 35 \cdot 2 = 70$ does the trick.
- $x \equiv 0 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 0 \pmod{7}$. To satisfy the mod 3 and mod 7 congruences, $x = 21z$. We solve $21z \equiv 1 \pmod{5}$ and find $z = 1$. Hence, $x = 21 \cdot 1 = 21$ does the trick.
- $x \equiv 0 \pmod{3}$, $x \equiv 0 \pmod{5}$, $x \equiv 1 \pmod{7}$. To satisfy the mod 3 and mod 5 congruences, $x = 15z$. We solve $15z \equiv 1 \pmod{7}$ and find $z = 1$. Hence, $x = 15 \cdot 1 = 15$ does the trick.

Combining these three, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$ has solution

$$x \equiv 2 \cdot 70 + 3 \cdot 21 + 2 \cdot 15 = 233 \equiv 23 \pmod{105}.$$

Check the answer!

Example 97. Solve $x \equiv 2 \pmod{3}$, $3x \equiv 2 \pmod{5}$, $5x \equiv 2 \pmod{7}$.

Solution. Note that $3^{-1} \equiv 2 \pmod{5}$ and $5^{-1} \equiv 3 \pmod{7}$.

Hence, we can simplify the system to $x \equiv 2 \pmod{3}$, $x \equiv 2 \cdot 2 \equiv -1 \pmod{5}$, $x \equiv 2 \cdot 3 \equiv -1 \pmod{7}$.

Reusing our three pieces from the previous example, we get $x \equiv 2 \cdot 70 - 1 \cdot 21 - 1 \cdot 15 = 104 \equiv -1 \pmod{105}$.

Check the answer!