Example 64. Every integer x is congruent to one of $0, 1, 2, 3, 4$ modulo 5.

We therefore say that $0, 1, 2, 3, 4$ form a **complete set of residues** modulo 5.

Another natural complete set of residues modulo 5 is: $0, \pm 1, \pm 2$

A not so natural complete set of residues modulo 5 is: $-5, 2, 4, 8, 16$

A possibly natural complete set of residues modulo 5 is: $0, 3, 3^2 = 9, 3^3 = 27, 3^4 = 81$

[We will talk more about this last case. Because we obtained a complete set of residues this way, we will say that "3 is a multiplicative generator modulo 5".]

Review. a is invertible modulo n if and only if $\gcd(a, n) = 1$. We can compute a^{-1} using the Euclidean algorithm.

Example 65. (review) Determine $16^{-1} \pmod{25}$.

Solution. Using the Euclidean algorithm, in Example 19, we found that $11 \cdot 16 - 7 \cdot 25 = 1$.
Reducing that modulo 25, we get $11 \cdot 16 \equiv 1 \pmod{25}$.
Hence, $16^{-1} \equiv 11 \pmod{25}$.

Example 66. List all invertible residues modulo 10.

Solution. $1, 3, 7, 9$
(We start with all residues $0, 1, 2, \ldots, 9$ and only keep those which have no common divisor with 10.)

5.2 Linear congruences

Let us consider the linear congruence $ax \equiv b \pmod{n}$ where we are looking for solutions x.

We will regard solutions x_1, x_2 as the same if $x_1 \equiv x_2 \pmod{n}$.

Example 67. (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 68.

(a) $3x \equiv 2 \pmod{7}$ has the solution $x = 3$. We regard $x = 10$ or $x = 17$ as the same solution. We therefore write that $x \equiv 3 \pmod{7}$ is the unique solution to the equation.

(b) $3x \equiv 2 \pmod{9}$ has no solutions x.

Why? Reducing $3x = 2 + 9m$ modulo 3, we get $0 \equiv 2 \pmod{3}$ which is a contradiction.
Just to make sure! Why does the same argument not apply to $3x \equiv 2 \pmod{7}$?

(c) $6x \equiv 3 \pmod{9}$ has solutions $x = 2$, $x = 5$, $x = 8$.

$6x = 3 + 9m$ is equivalent to $2x = 1 + 3m$ or $2x \equiv 1 \pmod{3}$. Which has solution $x \equiv 2 \pmod{3}$.

Armin Straub
straub@southalabama.edu

Theorem 69. Consider the linear congruence $ax \equiv b \pmod{n}$. Let $d = \gcd(a, n)$.

(a) The linear congruence has a solution if and only if $d|b$.

(b) If $d = 1$, then there is a unique solution modulo n.

(c) If $d|b$, then it has d different solutions modulo n.

(In fact, it has a unique solution modulo n/d.)

Proof.

(a) Finding x such that $ax \equiv b \pmod{n}$ is equivalent to finding x, y such that $ax + ny = b$.
The latter is a diophantine equation of the kind we studied earlier. In particular, we know that it has a solution if and only if $\gcd(a, n)$ divides b.

(b) If $d = 1$, then a is invertible modulo n. Multiplying the congruence $ax \equiv b \pmod{n}$ with a^{-1}, we obtain $x \equiv a^{-1}b \pmod{n}$. That's the unique solution.
Alternatively. If $d = 1$, then $ax + ny = b$ has general solution $x = x_0 + tn$, $y = y_0 - ta$ (where x_0, y_0 is some particular solution). But, modulo n, all of these lead to the same solution $x \equiv x_0 \pmod{n}$.

(c) If $d|b$, then $ax \equiv b \pmod{n}$ is equivalent to $a_1 x \equiv b_1 \pmod{n_1}$ with $a_1 = \frac{a}{d}$, $b_1 = \frac{b}{d}$, $n_1 = \frac{n}{d}$. (Make sure you see why! Spell out the congruences as equalities.) Since $\gcd(a_1, n_1) = 1$, we get a unique solution x modulo n_1.
Being congruent to x modulo n_1 is the same as being congruent to one of $x, x + n_1, \ldots, x + (d-1)n_1$ modulo n. □

Example 70. 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: $7 \cdot 3 + 3 \cdot 7 = 42 \equiv 10 \pmod{16}$, $2 \cdot 3 + 5 \cdot 7 = 41 \equiv 9 \pmod{16}$.

Armin Straub
straub@southalabama.edu

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.

Example 71. (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. $2\cdot 1-10=-8\equiv 7 \pmod{15}$, $3\cdot 1+4\cdot 10=43\equiv -2 \pmod{15}$.