Example 54. Show that $41|2^{20}-1$.

Solution. In other words, we need to show that $2^{20}\equiv 1 \pmod{41}$.
$2^5=32\equiv -9 \pmod{41}$. Hence, $2^{20}=(2^5)^4\equiv(-9)^4=81^2\equiv(-1)^2=1 \pmod{41}$.

We saw last time that we can calculate with congruences. However:

Example 55. (caution!) If $a\equiv b \pmod{n}$, then $ac\equiv bc \pmod{n}$ for any integer c.
However, the converse is not true! We can have $ac\equiv bc \pmod{n}$ without $a\equiv b \pmod{n}$ (even assuming that $c\not\equiv 0$).

For instance. $2\cdot 4\equiv 2\cdot 1 \pmod{6}$ but $4\not\equiv 1 \pmod{6}$
However. $2\cdot 4\equiv 2\cdot 1 \pmod{6}$ means $2\cdot 4=2\cdot 1+6m$. Hence, $4=1+3m$, or, $4\equiv 1 \pmod{3}$.

Similarly, $ab\equiv 0 \pmod{n}$ does not always imply that $a\equiv 0 \pmod{n}$ or $b\equiv 0 \pmod{n}$.

For instance. $4\cdot 15\equiv 0 \pmod{6}$ but $4\not\equiv 0 \pmod{6}$ and $15\not\equiv 0 \pmod{6}$

These issues do not occur when n is a prime, as the next results shows.

Lemma 56. Let p be a prime.

(a) If $ab\equiv 0 \pmod{p}$, then $a\equiv 0 \pmod{p}$ or $b\equiv 0 \pmod{p}$.

(b) Suppose $c\not\equiv 0 \pmod{p}$. If $ac\equiv bc \pmod{p}$, then $a\equiv b \pmod{p}$.

Proof.

(a) This statement is equivalent to Lemma 23: if $p|ab$ then $p|a$ or $p|b$.

(b) $ac\equiv bc \pmod{p}$ means that p divides $ac-bc=(a-b)c$.
Since p is a prime, it follows that $p|(a-b)$ or $p|c$.
In the latter case, $c\equiv 0 \pmod{p}$, which we excluded. Hence, $p|(a-b)$. That is, $a\equiv b \pmod{p}$. □

5.1 Congruences: modular inverses

We saw that $ac\equiv bc \pmod{n}$ does not always imply $a\equiv b \pmod{n}$.
For instance, $2\cdot 4\equiv 2\cdot 1 \pmod{6}$ but $4\not\equiv 1 \pmod{6}$.
The reason is that 2 is not invertible modulo 6.

The issue is that $2|6$ which results in $2\cdot 3\equiv 0 \pmod{6}$.

Let us briefly discuss residues that are invertible modulo n.

Example 57. Note that $3\cdot 7\equiv 1 \pmod{10}$. Hence, we write $3^{-1}\equiv 7 \pmod{10}$ and say that 7 is the **modular inverse** of 3 modulo 10.

Comment. As expected, we have $(x^{-1})^{-1}\equiv x \pmod{n}$. Here, $(3^{-1})^{-1}\equiv 7^{-1}\equiv 3 \pmod{10}$.

Example 58. Solve $3x\equiv 4 \pmod{10}$.

Solution. From the previous problem, we know that $3^{-1}\equiv 7 \pmod{10}$.
Hence, $x\equiv 3^{-1}\cdot 4\equiv 7\cdot 4=8 \pmod{10}$.

Example 59. Determine $4^{-1} \pmod{13}$.

Brute force solution. We need to find a residue x such that $4x \equiv 1 \pmod{13}$. We can try the values $0, 1, 2, 3, \ldots, 12$ and find that $x = 10$ is the only solution modulo 13 (because $4 \cdot 10 \equiv 1 \pmod{13}$).

This approach may be fine for small examples when working by hand, but is not practical for serious congruences. On the other hand, the Euclidean algorithm can compute modular inverses extremely efficiently (see below).

Glancing. In this special case, we can actually see the solution if we notice that $4 \cdot 3 = 12$, so that $4 \cdot 3 \equiv -1 \pmod{13}$ and therefore $4^{-1} \equiv -3 \pmod{13}$. [Or, equivalently, $-4^{-1} \equiv 10 \pmod{13}$.]

Solution. Since $\gcd(4, 13) = 1$, Bézout's identity promises that $4r + 13s = 1$ for some integers r, s. Reducing $4r + 13s = 1$ modulo 13, we find $4r \equiv 1 \pmod{13}$, so that $4^{-1} \equiv r \pmod{13}$.

Using the Euclidean algorithm, we find, for instance, $r = 10$ and $s = -3$. Hence, $4^{-1} \equiv 10 \pmod{13}$.

Example 60. Solve $4x \equiv 5 \pmod{13}$.

Solution. From the previous problem, we know that $4^{-1} \equiv -3 \pmod{13}$.

Hence, $x \equiv 4^{-1} \cdot 5 \equiv -3 \cdot 5 = -2 \pmod{13}$.

Advanced comment. We were able to solve $4x \equiv 5 \pmod{13}$ by computing 4^{-1} using the Euclidean algorithm instead of relying on brute force. However, for more complicated equations like $4^x \equiv 5 \pmod{13}$, we don't know any method of finding solutions x that is significantly better than brute force. Indeed, certain cryptographic methods depend precisely on the difficulty of solving congruences like $4^x \equiv 5 \pmod{13}$.

[Such a congruence is called a **discrete logarithm problem** because the solution to $4^x = 5$ is $x = \log_4(5)$.]

Example 61. 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, $16^{-1} \equiv 11 \pmod{25}$.

Let $a, b \in \mathbb{Z}$, not both zero. Recall that the diophantine equation $ax + by = c$ has a solution if and only if c is a multiple of $\gcd(a, b)$. In particular, $ax + by = 1$ has a solution if and only if $\gcd(a, b) = 1$.

Lemma 62. a is invertible modulo n if and only if $\gcd(a, n) = 1$.

Proof. The congruence $ax \equiv 1 \pmod{n}$ is equivalent to $ax + ny = 1$ where y is some integer. Note that $ax + ny = 1$ is a diophantine equation (we are looking for integer solutions x, y) and that it has a solution if and only if $\gcd(a, n) = 1$. □

Corollary 63. Let p be a prime. Then all nonzero residues are invertible modulo p.

Advanced comment. It is common to write $\mathbb{Z}/n\mathbb{Z}$ for the set of all residues modulo n. The fact that we can add and multiply as usual, makes $\mathbb{Z}/n\mathbb{Z}$ into a (finite) **ring**.

Let p be a prime. The fact that, in addition, all nonzero residues are invertible makes $\mathbb{Z}/p\mathbb{Z}$ into a (finite) **field**. The fields we are familiar with, such as $\mathbb{Q}$ (rationals), $\mathbb{R}$ (reals), $\mathbb{C}$ (complex numbers) are all infinite.