Problem

Solve the congruence

$$27x \equiv 3 \pmod{91}$$

Motivation

If we had a normal linear equation $27x = 3$ without the mods, then we learnt a long time ago that we can divide both sides by 27 in order to solve for x. Unfortunately for us, division isn't quite as easy in the modular arithmetic world and we cannot simply divide by 27.

However, we can instead multiply by the *multiplicative inverse*. Notice that division by 27 is simply multiplication by $\frac{1}{27}$, and $\frac{1}{27}$ is the unique number in $\mathbb{Q}$ where $27 \times \frac{1}{27} = 1$. If we can find some number a in the mod 91 world where $27 \times a \equiv 1 \pmod{91}$, then we would be able to multiply by a in the same way we multiply by $\frac{1}{27}$.

Solution

We wish to find a number a such that $27a \equiv 1 \pmod{91}$. Of course for smaller numbers you can easily guess such an inverse. But the key to doing this generally is to use the Euclidean Algorithm. This is because by Bezout's lemma, since 27 and 91 are coprime[1], we can find numbers a, b such that:

$$27a + 91b = 1$$

In particular, after taking mod 91, this would give $27a \equiv 1 \pmod{91}$. So we now perform the (extended) Euclidean Algorithm to find this number a:

$$\begin{aligned} 91 &= 27 \times 3 + 10 \\ 27 &= 10 \times 2 + 7 \\ 10 &= 7 \times 1 + 3 \\ 7 &= 3 \times 2 + 1 \end{aligned}$$

Reversing the algorithm:

$$\begin{aligned} 1 &= 7 - 3 \times 2 \\ &= 7 - (10 - 7 \times 1) \times 2 \\ &= 7 \times 3 - 10 \times 2 \\ &= (27 - 10 \times 2) \times 3 - 10 \times 2 \\ &= 27 \times 3 - 10 \times 8 \\ &= 27 \times 3 - (91 - 27 \times 3) \times 8 \\ &= 27 \times 27 - 91 \times 8 \end{aligned}$$

So $1 = 27 \times 27 - 91 \times 8$, which means that $27 \times 27 \equiv 1 \pmod{91}$, and we can now use this to solve the linear congruence:

$$\begin{aligned} 27x &\equiv 3 && \pmod{91} \\ 27 \times 27x &\equiv 27 \times 3 && \pmod{91} \\ x &\equiv 81 && \pmod{91} \end{aligned}$$

[1] In general m and n need to be coprime in order for the multiplicative inverse of $m \pmod{n}$ to exist.