Question 1.

Solve the congruence $252x \equiv 1001 \pmod{7777}$, and express your final answer in terms of congruence classes in $\mathbb{Z}_{7777}$. Show and explain all steps in your calculation, including finding an inverse using the Euclidean algorithm and via back substitution following the method shown in class.

Proof. First, we find $\gcd(252, 7777)$ using the Euclidean algorithm:

$$\begin{aligned} 7777 &= 30 \cdot 252 + 217 \\ 252 &= 1 \cdot 217 + 35 \\ 217 &= 6 \cdot 35 + 7 \\ 35 &= 5 \cdot 7 + 0 \end{aligned}$$

We see that $\gcd(252, 7777) = 7$, and $1001 = 7 \cdot 143$, so this congruence has solutions. We divide the congruence by 7 to obtain an equivalent congruence

$$36x \equiv 143 \pmod{1111}$$

We perform the Euclidean algorithm on 1111 and 36:

$$\begin{aligned} 1111 &= 30 \cdot 36 + 31 \\ 36 &= 1 \cdot 31 + 5 \\ 31 &= 6 \cdot 5 + 1 \\ 5 &= 5 \cdot 1 + 0 \end{aligned}$$

Then we do back substitution:

$$\begin{aligned} 1 &= 31 - 6 \cdot 5 \\ &= 31 - 6 \cdot (36 - 1 \cdot 31) \\ &= 7 \cdot 31 - 6 \cdot 36 \\ &= 7 \cdot (1111 - 30 \cdot 36) - 6 \cdot 36 \\ &= 7 \cdot 1111 - 216 \cdot 36 \\ \implies -216 \cdot 36 &\equiv 1 \pmod{1111} \\ 895 \cdot 36 &\equiv 1 \pmod{1111} \end{aligned}$$

This means that 895 is the inverse of 36 mod 1111. We multiply both sides of the congruence we obtained before by 895 to obtain that

$$\begin{aligned} x &\equiv 127985 \pmod{1111} \\ x &\equiv 220 \pmod{1111} \end{aligned}$$

So $x = 220 + 1111 \cdot n$ for $n \in \mathbb{Z}$. Since we are looking for solutions mod 7777, we want x to be between 0 and 7777. We see by inspection that $n \in \{0, 1, 2, 3, 4, 5, 6\}$. Therefore the solutions to the congruence are $x = 220, 1331, 2442, 3553, 4664, 5775, 6886$.

□