Computational Number Theory
HW 2

Due Date: 25/02/2024

Use your first, second programming assignments for calculations as needed.

1. Find all the roots of $x^2 - 1$ in $\mathbb{Z}_n$, where $n = 17 \times 19$.

2. Find the unique solution to $x^7 = 2$ in $\mathbb{Z}_{41}$.

3. Let p be an odd prime and $d|(p-1)$. Show that $\{a \in \mathbb{Z}_p : a^d = 1\} = \{a^{(p-1)/d} : a \in \mathbb{Z}_p^*\}$.

4. (a) Let d, n be integers such that $1 \leq d \leq n$.

   Find $|\{0 \leq k \leq n-1 : dk \equiv 0 \bmod n\}|$.

   (b) Let $1 \leq d \leq p-1$, where p is an odd prime. Find the number of roots of $x^d - 1$ in $\mathbb{Z}_p$. Hint: One approach is to express an arbitrary solution as the power of a fixed primitive root, and use (a). Alternatively, use a similar result as Exercise 3 from HW1, with suitable modification.

5. Find the roots of $x^2 - 4$ in $\mathbb{Z}_{343}$. Note that $343 = 7^3$, and use the Hensel lifting method.