Computational Number Theory
HW 2

Due Date: 16/09/2025

For calculations, use your own program or a tool (Sage or Pari/GP, latter has a mobile version).

1. For each equation below decide whether it has any solutions and if it has, find the solutions using the Tonelli-Shanks method.
   (a) $x^2 = 5$ in $\mathbb{Z}_{103}$;
   (b) $x^2 = 2$ in $\mathbb{Z}_{103}$;
   (c) $x^2 = 6$ in $\mathbb{Z}_{101}$.
2. Let p be an odd prime. Find the sizes of each of the following sets.
   (i) $A = \{(x, y) \in \mathbb{Z}_p^2 : x + y = 1\}$;
   (ii) $B = \{(x, y) \in \mathbb{Z}_p^2 : xy = 1\}$;
   (iii) $C = \{(x, y) \in \mathbb{Z}_p^2 : x^2 - y^2 = 1\}$.
3. Let p be an odd prime and let $dk = (p - 1)$. For $a \neq 0 \in \mathbb{Z}_p$, show that $x^d = a$ has a solution if and only if $a^k = 1$.
   Hint: Use the fact that $x^{p-1} - 1$ is divisible by $x^k - 1$.