COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
*New York, 2023/04/19*

Exercise Sheet 13

## Quadratic congruences and Cryptography

**Exercise 1** (15 points)**.** Let $p$ be an odd prime, $p \neq 3$. Similarly to HW12, Exercise 2, determine the values of $p$ such that 5 is a quadratic residue modulo $p$.

**Exercise 2** (15 points)**.** Let $p$ be a prime and assume that $p \equiv 3 \pmod 4$. Prove that, if $a$ is a quadratic residue modulo $p$, then the two square roots of $a$ are

$$\pm a^{(p+1)/4}\,.$$

**Exercise 3** (15 points)**.** For an odd prime $p$, consider the equation

$$ax^2 + bx + c = 0\,,$$

where $a, b, c \in \mathbb{Z}_p$, $a \neq 0$ are the parameters and $x$ is the unknown. Discuss the number of solutions of the equation in $\mathbb{Z}_p$, depending on the parameters $a, b, c$.
(Hint:) Define $\Delta = b^2 - 4ac$. The number of solutions depends on $\left(\frac{\Delta}{p}\right)$.

**Exercise 4** (15 points)**.** Bob publishes his RSA public key $(N, e) = (1517, 7)$. Alice sends him a message, the encrypted message is

$$515, 816, 331, 200.$$

Determine Bob's private key and decrypt the message.