COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

Number Theory and Cryptography
Math UN3020
New York, 2023/04/12

Exercise Sheet 12

Quadratic Reciprocity and Primality Test

Exercise 1 (9 points)**.** Using the quadratic reciprocity, determine whether 66, 80 and 122 are squares modulo 127.

Exercise 2 (10 points)**.** Let p be an odd prime, $p > 3$. Prove that
3 is a quadratic residue modulo p if and only if $p \equiv 1$ or $11 \pmod{12}$,
and that
3 is a quadratic non-residue modulo p if and only if $p \equiv 5$ or $7 \pmod{12}$.
(Hint:) use quadratic reciprocity.

Exercise 3 (8 points)**.** Let n be an integer such that $3 \nmid n$, and let p be an odd prime such that $p \mid n^2 + 3$. Prove that

$$p \equiv 1 \pmod{3}.$$

(Hint:) First show that

$$\left(\frac{-3}{p}\right) = \left(\frac{n^2}{p}\right).$$

Exercise 4 (9 points). Prove that there are infinitely many primes congruent to 1 modulo 3. (Hint:) Use a method similar to Euclid's proof, and the previous exercise.

Exercise 5 (12 points). Use the criterion given in class to verify that the numbers 1105, 1729, 2465 and 2821 are Carmichael numbers.

Exercise 6 (12 points). Use the Miller-Rabin test to show that the following numbers are composite:

(a) 899.

(b) 3599.

(c) 427.

(d) 30227.