NUMBER THEORY: HOMEWORK 7

TO BE HANDED IN BY WEDNESDAY 18TH OCTOBER 2023

1. Suppose that $p > 3$ is a prime number, and that g is a primitive root modulo p.
(a) What can one say about the integer α if g^α is a quadratic residue modulo p?
(b) What can one say about the integer α if g^α is a quadratic non-residue modulo p?
(c) Hence find modulo p the sum, and the product, of all the distinct quadratic residues modulo p.

2. Let p be an odd prime number.
(a) Show that when $p \neq 17$, one has
$$\left(\frac{2023}{p}\right) = \left(\frac{7}{p}\right).$$
(b) Show that $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1 \pmod 8$ or $p \equiv 3 \pmod 8$.

3. Let p be an odd prime number, and let a and b be integers with $p \nmid ab$.
(a) Show that if a and b are both quadratic non-residues, then ab is a quadratic residue.
(b) Deduce that the congruence
$$(x^2 - a)(x^2 - b)(x^2 - ab) \equiv 0 \pmod p$$
always possesses a solution x modulo p.

4. The nth Mersenne number is defined to be $M_n = 2^n - 1$.
(a) Prove that if M_n is prime, then n is prime.
(b) By making appropriate use of the quadratic residue symbol, show that if p is a prime congruent to 3 modulo 4, and $p' = 2p + 1$ is also prime, then $2^p \equiv 1 \pmod{p'}$.
(c) Deduce that $2^{251} - 1$ is not a Mersenne prime.