Homework

Exercise 1.

1. Show that $((\mathbb{Z}/n\mathbb{Z})^\times, \cdot)$ is a group.
2. Prove Euler's theorem: for any positive integer n and any integer a coprime to n
$$a^{\varphi(n)} = 1 \bmod n.$$
(In other words, the order of a mod n divides $\varphi(n)$).
3. Deduce Fermats's little theorem:
$$\forall a \in \mathbb{Z},\ p \text{ prime},\ a^p = a \bmod p.$$
4. Application: show that 1763 is not a prime number.

Exercise 2. Square roots and factorization

For a positive integer n, an integer a is called a *quadratic residue* modulo n if $a \in \mathbb{Z}/n\mathbb{Z}^\times$ satisfies $x^2 = a \bmod n$ for some integer x. In this case x is called a *square root* of a modulo n.

1. Compute square roots of 1 and -1 modulo 7 and modulo 13.
2. Check that the set $(\mathbb{Z}/n\mathbb{Z}^\times)^2$ of quadratic residues modulo n is a subgroup of $\mathbb{Z}/n\mathbb{Z}^\times$.
3. Show that for any odd prime p, the number of quadratic residues modulo p is $(p-1)/2$ and that for any integer $a \in \mathbb{Z}/p\mathbb{Z}^*$, $a^{(p-1)/2} = \pm 1 \bmod p$. Deduce that a is a quadratic residue modulo p iff $a^{(p-1)/2} = 1 \bmod p$.
4. (a) Show that if a is a quadratic residue modulo p^e ($e \in \mathbb{N}^*$) then $a^{(p-1)/2} = 1 \bmod p$.
   (b) Assume that a is a quadratic residue modulo p^e. Show that a is also a quadratic residue modulo p^{e+1} (hint: try to find x such that $(x_e + p^e x)^2 = a \bmod p^{e+1}$, where $x_e^2 = a \bmod p^e$).
   (c) Deduce that a is a quadratic residue modulo p^e iff $a^{(p-1)/2} = 1 \bmod p$.
5. Compute the number of quadratic residues modulo an odd integer n.
6. Let p a prime number s.t. $p = 3 \bmod 4$. Show that $x^{\frac{p+1}{4}}$ is the square root of x mod p. Are the integers 106 and 97 quadratic residues modulo 139? If they are, compute their square roots.
Note that more generally there exists a probabilistic algorithm that computes the square roots modulo any prime number.
7. Let $n = pq$ a product of two odd primes.
   (a) Show that if one knows how to compute square roots modulo p and modulo q, then one knows how to compute square roots modulo n. Application: compute the square roots of 106 modulo 417.
   (b) Deduce that if one is able to factorize, then one can compute the square roots of any integers modulo n.
8. Suppose that you have access to an algorithm $\mathcal{A}$ that computes efficiently the square roots modulo an odd integer n (in other words $\mathcal{A}$ has polynomial complexity in the size of n). Find a probabilistic algorithm that gives the factorization of n.