Homework: 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 $a^{(p-1)/2} = 1 \bmod p$.
   (d) Application: compute the square roots of 67 modulo 81.
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 $a^{\frac{p+1}{4}}$ is the square root of $a \bmod p$. Are the integers 106 and 97 quadratic residues modulo 139? If they are, compute their square roots.
7. Let now p be any odd prime, and s and t the two integers such that $p-1 = 2^s t$ and t is odd. For this exercice we will use the fact that $\mathbb{Z}/p\mathbb{Z}^\times = \mathbb{Z}/p\mathbb{Z}^*$ is a cyclic group. Let a be a quadratic residue modulo p.

   (a) Devise a probabilistic algorithm that finds a non-quadratic residue $b \in \mathbb{Z}/p\mathbb{Z}^\times$. What is its expected complexity ?
   (b) Show that a^t belongs to the subgroup of $\mathbb{Z}/p\mathbb{Z}^\times$ generated by $c = b^{2t}$. What is the order of this subgroup? If l is an integer such that $a^{-t} = c^l \bmod p$, show that $x = b^{tl} a^{(t+1)/2}$ is a square root of a modulo p.
   (c) Let $l = l_0 + 2l_1 + \cdots + 2^{s-2} l_{s-2}$ an integer such that $a^{-t} = c^l \bmod p$, where $l_0, \ldots, l_{s-2} \in \{0, 1\}$. Suppose that $l_0, \ldots, l_i$ are already known for $i < s-2$. Show that $l_{i+1} = 1$ iff $(a^{-t}\, c^{-(l_0 + \cdots + 2^i l_i)})^{2^{s-i-3}} = -1 \bmod p$.
   (d) Use the previous questions to write down, in pseudo-language, an algorithm that computes square roots modulo p. What is its (expected) complexity ?
   (e) Application: compute the square roots of 41 modulo 113.
8. 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.
9. Suppose that you have access to an algorithm $\mathcal{A}$ that computes efficiently a square root 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.
10. What can be said about quadratic residue and square roots modulo 2^e, $e \in \mathbb{N}^*$?