TD - Quadratic residue - Zero-knowledge protocol

$a \neq 0$ is a *square* (or *quadratic residue*) modulo b iff it exists x such that $x^2 \equiv a \mod b$. We say that x is a *square root* of a modulo b.
In the sequel, p and q are two odd distinct prime numbers and $n = p.q$.

1. Number of squares in $\mathbb{Z}/n\mathbb{Z}^\star$

a. Verify that if $x^2 \equiv a \mod b$, then $(b-x)^2 \equiv a \mod b$.

b. Prove that if a is a square modulo n, then a is a square mod p and mod q too.

c. Proove that any square $a \neq 0$ modulo p has exactly 2 roots : x and $y = p - x$.

d. Deduce that any square a in $\mathbb{Z}/n\mathbb{Z}$ relatively prime to p and q has exactly four distinct square roots: x_1, $n - x_1$, x_2 and $n - x_2$. **Hint:** use Chinese remainder theorem.

e. By using the property that $(\mathbb{Z}/p\mathbb{Z}^\star, \times)$ is a cyclic group, prove that there are $\frac{p-1}{2}$ non zero squares modulo p.

f. Deduce the number of squares in $\mathbb{Z}/n\mathbb{Z}^\star$.

2. Intractability of computing square roots. Let $a < n$; the goal of this question is to prove that computing square roots x of $a \neq 0$ modulo n is (polynomially) more expensive than factorization of n. The proof is performed by reduction (contradiction proof).
In all this question, it is assumed that we know the four distinct roots x_1, x_2, $(n-x_1)$ et $(n-x_2)$ of a modulo n; we prove that then that the factors p and q of n can be quicly computed.

a. Let $u = x_1 - x_2 \mod n$ and $v = x_1 + x_2 \mod n$. Prove that $u.v \equiv 0 \mod n$.

b. Justify that $1 \leq u, v < n$; then explicit how to compute p and q from u and v.

c. Give an upper bound on the number of operations performed (Big O notation) with respect to the number of bits of n.

d. Argue that the function *Square* of $\mathbb{Z}/n\mathbb{Z}$ defined by $Square(x) = x^2 \mod n$ may be considered as a one-way function.

3. Quadratic authentication protocol. Let $n = pq$ an integer of 1024 bits with p and q large primes; p and q are known by a trusted third part TTP, but, a priori, not by Alice not Bob.
To authenticate to Bob, Alice chooses the integer $x_A < n$ as unique private key. Let $a = x_A^2 \mod n$; TTP delivers to Alice a passport one which are written the public integers n and a.

a. We assume that only Alice (and may be TTP) knows x_A and that nobody, except TTP, can compute square roots modulo n. Is this reasonable ?

b. To authenticate Alice, Bob reads a and n from her passport and uses the following protocol (which is repeated 2 or 3 times):

   1. Alice chooses an integer $r < n$ at random; she keeps it secret.
   2. Alice computes $y = r^2 \mod n$ and $z = x_A.r \mod n$;
   3. Alice sends y and z to Bob;
   4. Bob tests Alice's identity by verifying $a.y - z^2 = 0 \mod n$.

   Prove that if Eve, a spy who cannot compute square roots mod n, has succeeded to compute r, then Eve knows Alice's private key x_A. What to deduce?

c. However, with previous protocol, Eve can impersonate Alice; instead of steps 1 and 2, Eve chooses at random an integer z and computes $y = z^2/a \mod n$.
   To avoid this, the following *zero-knowledge* protocol is used (which is repeated k times);

   1. Alice chooses r at random, computes $y = r^2 \mod n$ and sends y to Bob;
   2. Bob chooses at random $b \in \{0, 1\}$; Bob sends b to Alice;
   3. If Alice receives 0, then she sends $z = r$ to Bob (i.e. a square root of y modulo n); else, if she receives 1, she sends to Bob $z = x_A.r \mod n$ (i.e. a square root of $y.a \mod n$).
   4. Bob tests Alice's identity by verifying that $y.a^b - z^2 = 0 \mod n$.

   Give an upper bound on the probability that Eve, who wants to impersonate Alice, can correctly answer to Bob after k executions of the protocol.