1. (20 points) Find any square root of $8$ in $\mathbb{Z}/23^{3}31^{2}$, using no brute force: the only methods you should employ are principal square roots, Sun Ze, and Hensel’s Lemma.

2. (15 points total) Check whether or not $n = 169 (= 13^{2})$ is a pseudoprime for the base $b = 19$ with respect to each of these primality tests:

   (a) (5 points) Fermat.
   (b) (5 points) Solovay-Strassen.
   (c) (5 points) Miller-Rabin test.

3. (20 points total)
   (a) (10 points) Someone tells you that the composite number $n = 67591$ has a prime factor $p$ for which $p - 1$ is $\{2\}$-smooth. Use Pollard’s $p - 1$ method to find $p$ and to factor $n$.

   (b) (10 points) Alice published the RSA modulus $n = 16637$, and Eve wants to factor it into $n = pq$ for two primes $p, q$. Luckily, Eve has the keys to her sister’s square-root oracle, which she is borrowing for the weekend. She inputs to the square-root oracle the perfect square $4 = 2^{2}$ in $\mathbb{Z}/16637$, and the oracle spits back the square-root $129$ for $4$ in $\mathbb{Z}/16637$. Use the oracle’s output to factor $n$ for Eve.
4. (16 points total) For each of the following assertions, either prove it, or disprove it by exhibiting a counterexample.

(a) (8 points) For all positive integers $n$ and every $x \in \mathbb{Z}/n$, one has $x^n = \bar{x}$.

(b) (8 points) For all positive integers $n$ and every $x \in \mathbb{Z}/n$, one has $x^{\varphi(n)+1} = \bar{x}$. Here $\varphi(n)$ denotes the Euler-phi function of $n$.

5. (14 points) Let $b, n$ be positive integers with $GCD(b, n) = 1$. Prove that if the Jacobi symbol $(\frac{b}{n})_2$ equals $-1$, then $b$ is definitely not a square in $\mathbb{Z}/n$, whether or not $n$ is prime.

6. (15 points) Let $p$ be a prime with $p \equiv 3 \mod 4$, and let $H$ be the subset of perfect squares in $(\mathbb{Z}/p)^\times$:

$$H := \{ \bar{x} \in (\mathbb{Z}/p)^\times : \text{there exists } \bar{z} \in (\mathbb{Z}/p)^\times \text{ with } \bar{x} = \bar{z}^2 \}. $$

Show that the squaring map

$$f : H \rightarrow H$$

$$f(\bar{x}) = \bar{x}^2$$

is a bijection from $H$ to $H$, that is, $f$ is one-to-one and onto (or injective and surjective, or a one-to-one correspondence).