Exercise 11. Let $p > 2$ be prime. Let $\left( \frac{a}{p} \right)$ be the Legendre symbol. Prove the following calculation rules.

(a) $\left( \frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}}$

(b) $\left( \frac{a}{p} \right) \left( \frac{b}{p} \right) = \left( \frac{ab}{p} \right)$

(c) $\left( \frac{a}{p} \right) = \left( \frac{b}{p} \right)$, if $a \equiv b \mod p$

Exercise 12. Let $p$ be prime, $g$ a primitive element modulo $p$ and $a, b \in \mathbb{Z}_p^*$. Show the following:

(a) $a$ is a quadratic residue modulo $p$ if and only if there exists an even $i \in \mathbb{N}_0$ with $a \equiv g^i \mod p$.

(b) If $p$ is odd, then exactly one half of the elements $x \in \mathbb{Z}_p^*$ are quadratic residues modulo $p$.

(c) The product $ab$ is a quadratic residue modulo $p$ if and only if $a$ and $b$ are both either quadratic residues or quadratic non-residues modulo $p$.

Exercise 13. Establish a message decryption with the Goldwasser-Micali cryptosystem. Start by finding the cryptosystem’s parameters.

(a) Find a pseudo-square modulo $n = p \cdot q = 31 \cdot 79$ by using the algorithm from the lecture notes. Start with $a = 10$ and increase $a$ by 1 until you find a quadratic non-residue modulo $p$. For $b$, start with $b = 17$ and proceed analogously.

(b) Decrypt the ciphertext $c = (1418, 2150, 2153)$. 