1. Determine $\mathcal{P}_{21}$, the set of bases $b$ for which $21$ is a pseudoprime to the base $b$. (Do this by hand, using a calculator, but use theory to save on computations.)

2. (a) Let $G$ be an abelian group of order $n$ and let $m \geq 1$ be an integer. Prove that $G[m] = G[(n, m)]$.

   (b)* Let $n = pq$, where $p, q$ are distinct primes, and put $m = (p - 1, q - 1)$. Show that $\mathcal{P}_n \cong \mathbb{F}_p^\times [m] \times \mathbb{F}_q^\times [m]$ and conclude that $|\mathcal{P}_n| = m^2$.

3. (a) Which of the three numbers $111, 10000, 21112$ are squares in $\mathbb{F}_{22307}$? Justify your answer. (Do not use the prime factorization of your numbers.)

   (b) For which primes $p$ is $11$ a quadratic residue mod $p$? (Give your answer in terms of congruence conditions on $p$.)

4. (a) Let $m$ be a squarefree odd integer, and let $(a, m) = 1$. Show that $x^2 \equiv a \pmod{m}$ has a solution if and only if $(a_p) = 1$, for all primes $p|m$.

   (b)* Extend part (a) to all odd integers $m$.

5. MAPLE problem (refer to the MAPLE instruction sheet):

   (a) Write a one-line program $\text{pseudo}(n, b)$ to test whether or not $n$ is a pseudoprime to the base $b$. (Your program should return true or false.) Test your program for $n = 30857$ and $b = 3$ and $b = 5$. What can you conclude from your output about $n$?

   (b) Use the command $\text{jacobi}$ in the $\text{numtheory}$ package to write a one-line program $\text{Epseudo}(n, b)$ to test whether or not $n$ is an Euler pseudoprime to the base $b$. Test your program for $n$ and $b$ as in part (a). Comment on the different results obtained (if any).

   (c) Use your previous program and Maple’s random number generator $\text{rand}(1..n)$ to write a program $\text{SolS}(n, k)$ which implements $k$ tests of the Solovay-Strassen primality test for $n$. Test your program on the numbers $n_1 = 13999457$, $n_2 = 104729$, and $n_3 = 340561$. First do 5 passes, then 10, then 100. What can you conclude from the output for each number?