1. Let $n \geq 2$ be an integer, and let $a$ be an integer with $(a, n) = 1$.
   a. Define the order of $a$ modulo $n$.
   b. Compute $\text{ord}_{31} 2$ (the order of $2$ modulo $31$).
   c. Define what it means for $a$ to be a primitive root modulo $n$.

2. a. How many primitive roots are there modulo $100$?
   b. Is $2$ a primitive root modulo $79$? Justify your answer.

3. State Miller’s test.

4. State Lucas’ “converse” to Fermat’s Little Theorem.

5. Find $\lambda(400)$, where $\lambda(n)$ denotes the Carmichael $\lambda$-function, or minimal universal exponent of $n$.

6. Using the table below of indices modulo $19$ with respect to the primitive root $2$, find all solutions to the equation

   $$x^4 \equiv 11 \pmod{19}.$$

\[
\begin{array}{|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|c|}
\hline
n & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 \\
I(n) & 18 & 1 & 13 & 2 & 16 & 14 & 6 & 3 & 8 & 17 & 12 & 15 & 5 & 7 & 11 & 4 & 10 & 9 \\
\hline
\end{array}
\]

7. Describe the procedure for encrypting and decrypting a message $m$ using the RSA cryptosystem.

8. Suppose $n = pq$ where $p$ and $q$ are distinct odd primes. Explain how to factor $n$ if you know $\phi(n)$.

9. Let $p$ be an odd prime number, and let $a$ be an integer with $(a, p) = 1$.
   State and prove Euler’s criterion for the Legendre symbol $\left( \frac{a}{p} \right)$. (You may assume basic facts about primitive roots.)

10. If $p$ is an odd prime and $g$ is a primitive root mod $p$, what is $\text{ind}_g(p - 1)$?
    Justify your answer.

11. Suppose $p = 12k + 1$ is a prime. Is $k$ a quadratic residue modulo $p$?