1. Define the Legendre symbol and the Jacobi symbol.

Legendre symbol: For odd primes \( p \) and integers \( a \) not divisible by \( p \) we put \( \left( \frac{a}{p} \right) = 1 \) or \( \left( \frac{a}{p} \right) = -1 \) according as \( a \) is a square modulo \( p \) or not.

2. Prove that \( -7 \) is a square modulo \( p \neq 7 \) if and only if \( p \equiv 1, 2, 4 \mod 7 \).

\[
\left( \frac{-7}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{7}{p} \right) = \left( \frac{-1}{p} \right) \left( \frac{1}{p} \right)^{(p-1)/2} = \left( \frac{7}{p} \right)
\]

by the quadratic reciprocity law and the first supplementary law. The last symbol is +1 if and only if \( p \equiv 1, 2, 4 \mod 7 \).

3. Solve the linear system of congruences

\[
\begin{align*}
x &\equiv 13 \mod 17 \\
x &\equiv 17 \mod 13
\end{align*}
\]

We need to compute a Bezout representation for \( \gcd(13, 17) = 1 \). From the Euclidean algorithm \( 17 - 13 = 4, 13 - 3 \cdot 4 = 1 \) we get \( 1 = 13 - 3 \cdot 4 = 13 - 3 \cdot (17 - 13) = 4 \cdot 13 - 3 \cdot 17 \).

Then the solution of the linear system is given by \( x \equiv 4 \cdot 13 - 3 \cdot 17 \cdot 17 \equiv -191 \equiv 30 \mod 13 \cdot 17 \).

4. Find all natural numbers \( m \) with \( \phi(m) = 4 \).

If \( \phi(p^a) = 4 \), then \( (p - 1)p^{a-1} = 4 \), hence either \( p = 5 \) and \( a = 1 \) or \( p = 2 \) and \( a = 3 \). If \( m = p^a q^b \), then \( \phi(m) = (p - 1)(q - 1)p^{a-1}b - 1 \), and as above the only possible primes are 2, 3, and 5. Thus we find \( m = 2 \cdot 5 \) or \( m = 4 \cdot 3 \). If \( m \) is divisible by three primes, then \( \phi(m) \geq 2 \cdot 4 = 8 \). Overall, \( \phi(m) = 4 \) if and only if \( m = 5, 8, 10, 12 \).

5. Is 21 a quadratic residue modulo 101?

\[
\left( \frac{21}{101} \right) = \left( \frac{101}{21} \right) = \left( \frac{4}{21} \right) = \left( \frac{1}{21} \right) = +1
\]

by the first supplementary law. Since 101 is prime, 21 is indeed a quadratic residue mod 101.

6. Compute \( 3^{201} \mod 75 \).

We have \( 75 = 3 \cdot 25; 3^{201} \equiv 0 \mod 3; 3^{6(25)} = 3^{20} \equiv 1 \mod 25 \) by Euler-Fermat, hence \( 3^{201} \equiv 3 \mod 75 \). Thus \( 3^{201} \equiv 3 \mod 75 \) by the Chinese remainder theorem.
(7) Prove that every prime factor of $3x^2 + 1$ is $\equiv 1 \mod 3$. Then show that there exist infinitely many primes $p \equiv 1 \mod 3$.

If $p \mid 3x^2 + 1$, then $-3x^2 \equiv 1 \mod p$. Clearly $p \nmid x$, hence $-3 \equiv (x^{-1})^2 \mod 3$, and thus $\left(\frac{-3}{p}\right) = +1$, or $p \equiv 1 \mod 3$.

Let $p_1, \ldots, p_n$ be primes $\equiv 1 \mod 3$, and consider $N = 3(p_1 \cdots p_n)^2 + 1$. Then there is some prime $p \mid N$; we have just shown that $p \equiv 1 \mod 3$; the standard argument shows that $p \neq p_i$.

(8) Assume that $p \equiv 5 \mod 8$ is prime, and that $\left(\frac{a}{p}\right) = +1$.

(a) Show that if $a^{(p-1)/4} \equiv 1 \mod p$, then $x = a^{(p+3)/8}$ solves the congruence $x^2 \equiv a \mod p$.

(b) If $a^{(p-1)/4} \equiv -1 \mod p$, then $x \equiv 2a(4a)^{(p-5)/8} \mod p$ solves the congruence $x^2 \equiv a \mod p$.

(9) Use Gauss’s Lemma to show that $\left(\frac{2}{p}\right) = (-1)^{(p-1)/4}$ for primes $p \equiv 1 \mod 4$.

Let $p = 4n + 1$ and consider the half system $\{1, 2, \ldots, 2n\}$. Multiplying through by 2 we get $2 \cdot i \equiv 2i \mod p$ for $1 \leq i \leq n$ and $2 \cdot j \equiv 2j \equiv -2(2n - j) - 1 \mod p$ for $n + 1 \leq j \leq 2n$. Thus the number of minus signs is $n$, and Gauss’s Lemma says that $\left(\frac{2}{p}\right) = (-1)^n$. Since $n = \frac{p-1}{4}$, this is the claim.