Elementary Number Theory and Cryptography,
M'mas 2011, Problem Sheet 9 (primitive roots, quadratic residues).

1. (a) Find all primes less than 20 for which 3 is a primitive root.
   (b) If g is a primitive root modulo 37, which of the numbers g^2, g^3, ..., g^8 are primitive roots modulo 37?
   (c) Suppose g is a primitive root modulo p. Try to find a rule for deciding whether g^k is a primitive root modulo p.
   Prove that this rule is correct.

2. (a) Use index calculus to solve the equation
$$x^{13} \equiv 15 \pmod{37}\,.$$
   You may use that, for the primitive root $g = 2$ modulo 37, one has
$$I(3) = 26\,, \quad I(5) = 23\,.$$
   (b) (*) Using the above, or otherwise, try to find a closed expression for a solution of the equation
$$4^k x^{13} \equiv 15 \pmod{37}$$
   for any $k \geqslant 0$.
   [Hint: It may be useful to determine $I(4)$.]

3. If a and b are related via $a + b \equiv 0 \pmod{p}$, how are the indices $I(a)$ and $I(b)$ related?

4. Show that there is no primitive root modulo 8.
   More generally, show that there is no primitive root modulo 2^n for $n \geqslant 3$.

5. (a) Produce a list of all the QRs and NRs modulo the prime 23.
   (b) Is 7^{11} a QR modulo 23? Justify your answer.
   (c) Determine
$$\left(\frac{2^k \cdot 5^\ell}{23}\right)$$
   for arbitrary k, $\ell \in \mathbb{Z}_{>0}$.

6. Without writing down a solution, determine whether each of the following congruences has a solution in integers.
   (a) $x^2 \equiv -1 \pmod{5987}$,
   (b) $x^2 \equiv 6780 \pmod{6781}$,
   (c) $x^2 + 14x - 35 \equiv 0 \pmod{337}$,
   (d) $x^2 - 64x + 943 \equiv 0 \pmod{3011}$.

7. Use Gauss's lemma from the lectures to evaluate each of the Legendre symbols below (i.e., find the integer ν such that $\left(\frac{a}{p}\right) = (-1)^\nu$).
$$(a)\ \left(\frac{8}{11}\right) \qquad (b)\ \left(\frac{7}{13}\right) \qquad (c)\ \left(\frac{5}{19}\right) \qquad (d)\ \left(\frac{6}{31}\right).$$

8. Use the Quadratic Reciprocity Law to compute the following Legendre symbols:
$$(a)\ \left(\frac{65}{101}\right) \qquad (b)\ \left(\frac{101}{2011}\right) \qquad (c)\ \left(\frac{111}{641}\right) \qquad (d)\ \left(\frac{31706}{43789}\right).$$

9. Is 3 a quadratic residue modulo (the prime) 1234567891?