Exercises 13

1. Let $p = 11$ and $q = 7$. Using the notation in the proof of the law of quadratic reciprocity (Theorem 3.17), we have $m+n+M+N = |S \times T| = 15$. Compute the numbers m, n, M, and N. Check that $\left(\frac{7}{11}\right) = (-1)^m$ and $\left(\frac{11}{7}\right) = (-1)^n$.

2. Use quadratic reciprocity to compute $\left(\frac{7}{43}\right)$. Find an integer x such that $x^2 \equiv 7 \pmod{43}$.

3. Use quadratic reciprocity to compute $\left(\frac{19}{101}\right)$. Find an integer x such that $x^2 \equiv 19 \pmod{101}$.

4. Prove that the congruence
$$(x^2-2)(x^2-17)(x^2-34) \equiv 0 \pmod{p}$$
has a solution for every prime number p.

5. Use quaratic reciprocity to find all primes p for which -2 is a quadratic residue.

6. Use quaratic reciprocity to find all primes p for which 3 is a quadratic residue.

7. Find all primes for which -3 is a quadratic residue.

8. Find all primes for which 5 is a quadratic residue.

9. Find all primes for which -5 is a quadratic residue.

11. In Exercises 11–17 we derive properties of the *Jacobi symbol*, which is a generalization of the Legendre symbol to composite moduli. Let m be an odd positive integer, and let
$$m = \prod_{i=1}^{r} p_i^{k_i}$$
be the factorization of m into the product of powers of distinct prime numbers. For any nonzero integer a, we define the Jacobi symbol $\left(\frac{a}{m}\right)$ as follows:
$$\left(\frac{a}{m}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)^{k_i}.$$
(a) Prove that if $a \equiv b \pmod{m}$, then
$$\left(\frac{a}{m}\right) = \left(\frac{b}{m}\right).$$
(b) For any integers a and b, prove that
$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$
(c) Prove that $\left(\frac{a}{m}\right) = 0$ if and only if $(a, m) > 1$.

12. Compute the Jacobi symbol $\left(\frac{38}{165}\right)$.

13. Let m be an odd positive integer, and let $(a, m) = 1$. The integer a is called a quadratic residue modulo m if there exists an integer x such that
$$x^2 \equiv a \pmod{m}$$
and a quadratic nonresidue modulo m if this congruence has no solution. Prove that if $\left(\frac{a}{m}\right) = -1$, then a is a quadratic nonresidue modulo m. Prove that a is not necessarily a quadratic residue modulo m if $\left(\frac{a}{m}\right) = 1$.
Hint: Consider $m = 21$ and $a = -1$.

14. Let $m = p^k$, where p is an odd prime and $k \geq 1$. Prove that
$$\frac{m-1}{2} \equiv \frac{k(p-1)}{2} \pmod{2}.$$
Hint: Use the binomial theorem to expand $m = ((p-1)+1)^k$.

15. Let m be an odd positive integer with standard factorization $m = \prod_{i=1}^{r} p_i^{k_i}$. Prove that
$$\frac{m-1}{2} \equiv \sum_{i=1}^{r} \frac{k_i(p_i-1)}{2} \pmod{2}.$$
Hint: Use induction on r.
Prove that
$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}.$$

16. Let m be an odd positive integer with standard factorization $m = \prod_{i=1}^{r} p_i^{k_i}$. Prove that
$$\frac{m^2-1}{8} \equiv \sum_{i=1}^{r} \frac{k_i(p_i^2-1)}{8} \pmod{8}$$
and
$$\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}.$$

17. Let m and n be relatively prime odd positive integers with standard factorizations
$$m = \prod_{i=1}^{r} p_i^{k_i}$$
and
$$n = \prod_{j=1}^{s} q_j^{\ell_j}.$$
Prove that
$$\frac{m-1}{2}\frac{n-1}{2} \equiv \sum_{i=1}^{r}\sum_{j=1}^{s} k_i \ell_j \left(\frac{p_i-1}{2}\right)\left(\frac{q_j-1}{2}\right) \pmod{2}$$
and
$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$