Number Theory: Quadratic Reciprocity

(1) Prove for odd primes p that $\left(\frac{-3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 6 \\ -1 & \text{if } p \equiv -1 \pmod 6 \end{cases}$

(2) Find all primes p for which $\frac{2^{p-1}-1}{p}$ is a perfect square.

(3) Prove that if r is a quadratic residue of m where $m > 2$, then $r^{\phi(m)/2} \equiv 1 \pmod m$.

(4) For any prime p of the form $4k+3$, prove that $x^2 + (p+1)/4 \pmod p$ is not solvable.

(5) Let $1, 2, \ldots, p-1 \pmod p$ be divided into two disjoint sets S and T such that $s_1 s_2 \in S$, $t_1 t_2 \in T$, and $s_1 t_1 \in T$ for all $s_i \in S$ and all $t_i \in T$. Prove that S must be the set of quadratic residues.

(6) Show that if p is a prime of the form $4k+1$ then the sum of the quadratic residues $\pmod p$ in the interval $[1, p)$ is $p(p-1)/4$.

(7) Prove that if the prime p is of the form $3k+2$, then all residues are cubic residues. Prove that if p is of the form $3k+1$, then only one third of non-zero residues are cubic residues.

(8) Prove that for any arbitrary prime number $p > 5$, the equation

$$x^4 + 4^x = p$$

has no solution in whole numbers.

(9) Prove for all primes p that $x^8 \equiv 16 \pmod p$ is solvable.

(10) Let p be an odd prime. Prove that every primitive root of p is a quadratic non-residue. Prove that every quadratic nonresidue is a primitive root if and only if p is of the form $2^{2^n} + 1$ where n is a non-negative integer: i.e. $p = 3$ or p is a Fermat number.

(11) Show that if p is an odd prime and $gcd(a, p) = 1$, then $x^2 = a \pmod{p^a}$ has exactly $1 + \left(\frac{a}{p}\right)$ solutions.

(12) Suppose that m is an odd number. Show that if $gcd(a, p) = 1$ then the number of solutions to $x^2 \equiv a \pmod m$ is

$$\prod_{p|m} \left(1 + \left(\frac{a}{p}\right)\right).$$

Prove that if m is an odd square-free number, then the equation holds for all integers a.

(13) Find all primes p such that $\left(\frac{10}{p}\right) = 1$.

(14) Prove that there are infinitely many primes of the form $3n+1$ and infinitely many of th form $3n-1$.

(15) Show that if $p = 2^{2^n} + 1$ is prime, then 3 is a primitive root $\pmod p$ and that 5 and 7 are primitive roots if $n > 1$.

(16) Given that 1111118111111 is prime, determine whether 1001 is a quadratic residue (mod 1111118111111).

(17) Show that if x is not divisible by 3, then $4x^2 + 3$ has at least one prime factor of the form $12n + 7$. Deduce that there are infinitely many primes of this sort.

(18) Suppose that $gcd(ab, p) = 1$ and that $p > 2$. Show that the number of solutions (x, y) to $ax^2 + by^2 \equiv 1 \pmod p$ is $p - \left(\frac{-ab}{p}\right)$.