Modular arithmetic

Q1 A number a such that $1 \leq a < n$ is called a quadratic residue modulo n if the congruence $x^2 - a \equiv 0 \bmod n$ has a solution. If n is a prime number, how many quadratic residues are there modulo n? If $n = pq$ is a product of two distinct odd prime numbers, how many quadratic residues are there modulo n?

Q2. Let n be a prime number and $P(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{d-1} x^{d-1} + x^d$ be a polynomial of degree d with coefficients $a_i \in Z_n$ for $0 \leq i < d$. An element $a \in Z_n$ is called a root of the polynomial if $P(a) \equiv 0 \bmod n$. Prove that a polynomial of degree $d \geq 1$ has at most d roots in Z_n. For all primes n, prove that there exists a polynomial of degree 2 that has no roots in Z_n. Such a polynomial is called irreducible modulo n. Try to explicitly construct such a polynomial for any general n. Try to generalize to polynomials of degree d for $d \geq 2$.

Q3 Let n be a prime number and a a number not divisible by n. The order of a modulo n is the smallest positive number k such that $a^k \equiv 1 \bmod n$. Prove that the order of a divides $n - 1$. The number a is said to be a primitive root modulo n if its order is $n - 1$. Find all primitive roots modulo n for $n = 3, 5, 7, 11, 13$. Prove that for all primes n, there exists a primitive root modulo n. Hint: Try to find for each divisor d of $n - 1$, the number of elements in Z_n of order d.

Q4 While Wilson's theorem gives a necessary and sufficient condition for a number n to be prime, Fermat's little theorem only gives a sufficient condition which is not necessary. There exist composite numbers n such that for all a, $gcd(a, n) = 1$ implies $a^{n-1} \equiv 1 \bmod n$. Such numbers are called Carmichael numbers. Prove that a number n is a Carmichael number if and only if n is a product of distinct primes and for every prime p that divides n, $p - 1$ divides $n - 1$. The smallest composite Carmichael number is $561 = 3 \times 11 \times 17$ and it is known that there are infinitely many of them.

Q5 Let m_1, m_2 be arbitrary positive integers. Prove that the congruences $x \equiv a_1 \bmod m_1$ and $x \equiv a_2 \bmod m_2$ have a common solution if and only if $a_1 - a_2$ is divisible by $gcd(m_1, m_2)$. This generalizes the CRT to the case when $gcd(m_1, m_2) > 1$. How many distinct solutions are there modulo $m_1 m_2$ in the general case? Can you find an explicit description of all possible solutions?