# Modular arithmetic

Q1 Let $m, n$ be positive integers such that $gcd(m, n) = 1$. Prove that for all $a \in Z_m$ and $b \in Z_n$, there exists a unique number $x \in Z_{mn}$ such that $x = a \bmod m$ and $x = b \bmod n$. This is known as the Chinese Remainder Theorem. Suppose now that $gcd(m, n) = d$ for some number $d$. Find a necessary and sufficient condition on $a$ and $b$ for such a number $x$ to exist. If it exists, how many distinct such numbers exist in $Z_{mn}$?

Q2 A number $a$ such that $1 \leq a < n$ is called a quadratic residue modulo $n$ if the congruence $x^2 = a \bmod n$ 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 $n$?

Q3. 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 $P(a) = 0 \bmod n$. 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 prime $n$. Try to generalize to polynomials of degree $d$ for $d \geq 2$.

Q4 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 $a^k = 1 \bmod n$. 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 $n - 1$. Prove that for all primes $n$, there exists a primitive root modulo $n$. Prove that $n$ is prime if and only if there exists a number $a \in Z_n$ such that $a^{n-1} = 1 \bmod n$ and $a^{(n-1)/p} \neq 1 \bmod n$ for any prime $p$ that divides $n - 1$. Hint: Try to find for each divisor $d$ of $n - 1$, the number of elements in $Z_n$ of order $d$. This may need something that we will do next week and the previous problem.

Q5 Prove Wilson's theorem that $(n - 1)! + 1 = 0 \bmod n$ if and only if $n$ is prime. While this gives a necessary and sufficient condition for a number $n$ to be prime, Fermat's little theorem only gives a necessary condition which is not sufficient. There exist composite numbers $n$ such that for all $a$, $gcd(a, n) = 1$ implies $a^{n-1} = 1 \bmod n$. 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. Find small values of $a$ for which 561 is declared to be composite by the Miller-Rabin test.