Tutorial Sheet 7

Sept 21, 23, 24

1. Let n be a positive integer and let $n-1 = 2^s t$, where s is a nonnegative integer and t is an odd positive integer. We say that n passes Miller's test for the base b if either $b^t \equiv 1(\mod n)$ or $b^{2^j t} \equiv -1(\mod n)$ for some j with $0 \leq j \leq s-1$. It can be shown that a composite integer n passes Miller's test for fewer than $n/4$ bases b with $1 < b < n$. A composite positive integer n that passes Miller's test to the base b is called a *strong pseudoprime* to the base b.
   (a) Show that if n is prime and b is a positive integer not a multiple of n then n passes Miller's test to the base b.
   (b) Show that 2047 is a strong pseudoprime to the base 2 by showing that it passes Miller's test to the base 2, but is composite.

2. Recall that$n$ is a *Carmichael number* if n is composite and $a^{n-1} \equiv 1(\mod n)$ for all $2 \leq a \leq n-1, gcd(a,n) = 1$.
   (a) Show that 1729 is a Carmichael number.
   (b) Show that 2821 is a Carmichael number.
   (c) Show that if$n = p_1 p_2 \cdots p_k$, where $p_1, p_2, ..., p_k$ are distinct primes that satisfy $p_j - 1 | n-1$ for $j = 1, 2, ..., k$, then n is a Carmichael number.

3. If m is a positive integer, the integer a is a quadratic residue of m if $gcd(a,m) = 1$ and the congruence $x^2 \equiv a(\mod m)$ has a solution. In other words, a quadratic residue of m is an integer relatively prime to m that is a perfect square modulo m. If a is not a quadratic residue of m and $gcd(a,m) = 1$, we say that it is a quadratic nonresidue of m. For example, 2 is a quadratic residue of 7 because gcd(2, 7) = 1 and $3^2 \equiv 2(\mod 7)$ and 3 is a quadratic nonresidue of 7 because gcd(3, 7) = 1 and $x^2 \equiv 3(\mod 7)$ has no solution.
   (a) Which integers are quadratic residues of 11?
   (b) Show that if p is an odd prime and a is an integer not divisible by p, then the congruence $x^2 \equiv a(\mod p)$ has either no solutions or exactly two incongruent solutions modulo p.
   (c) Show that if p is an odd prime, then there are exactly $(p-1)/2$ quadratic residues of p among the integers $1, 2, ..., p-1$.

4. If p is an odd prime and a is an integer not divisible by p, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if a is a quadratic residue of p and -1 otherwise.
   (a) Show that if p is an odd prime and a and b are integers with $a \equiv b(\mod p)$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
   (b) Prove Euler's criterion, which states that if p is an odd prime and a is a positive integer not divisible by p, then$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(\mod p)$. [Hint: If a is a quadratic residue modulo p, apply Fermat's little theorem; otherwise, apply Wilson's theorem]
   (c) Use the above to show that if p is an odd prime and a and b are integers not divisible by p, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

5. Show that if p is an odd prime, then -1 is a quadratic residue of p if $p \equiv 1(\mod 4)$, and -1 is not a quadratic residue of p if $p \equiv 3(\mod 4)$.

6. Find all solutions of the congruence $x^2 \equiv 29(\mod 35)$. [Hint: Find the solutions of this congruence modulo 5 and modulo 7, and then use the Chinese remainder theorem.]