Number Theory - Problem sheet 2

1. Evaluate the following Legendre symbols:-

$$\left(\frac{20964}{1987}\right), \left(\frac{4977}{1987}\right), \left(\frac{741}{9283}\right), \left(\frac{5}{160465489}\right), \left(\frac{3083}{3911}\right).$$

You may use the reciprocity law for the Jacobi symbol to shorten your calculations.

2. Find all odd primes p for which 15 is a quadratic residue.

3. Prove that 3 is a quadratic residue modulo any Mersenne prime >3.

4. Find all Euler pseudo-primes to the base 39.

5. Let a be a positive integer which is not a square. Prove that there are infinitely many odd primes p such that $\left(\frac{a}{p}\right) = -1$. (Artin conjectured that in fact a should be a primitive root for infinitely many primes p, but this has not been proven).

6. Prove that mod 91 there are precisely 36 bases for which 91 is a pseudo-prime. In general, if both p and $2p-1$ are prime numbers, show that $N = p(2p-1)$ is a pseudo-prime for precisely half of all bases mod N.

7. Let N be of the form $N = (6t+1)(12t+1)(18t+1)$, where t is a positive integer such that $6t+1, 12t+1, 18t+1$ are all primes. Prove that N is a Carmichael number. Use this construction to find 3 Carmichael numbers.

8. Let p be an odd prime, and let b be an integer >1 with $(b, p) = 1$. Show that p^2 is a pseudo-prime to the base b if and only if $b^{p-1} \equiv 1 \bmod p^2$.

9. Let $N = 561$. Find the number of bases b modulo N for which N is an Euler pseudo-prime. Show there are precisely 10 bases for which N is a strong pseudo-prime.

10. Let p be a prime > 5. Prove that

$$N = (4^p + 1)/5$$

is always a composite integer. Prove that N is always a strong pseudo-prime to the base 2.

11. Assume that n is an integer > 1 such that $F_n = 2^{2^n} + 1$ is composite. Prove that F_n is a pseudo-prime to the base 2. ($n = 5$ is the smallest positive integer for which F_n is not prime).

12. Give an example of an odd composite N and a base b such that $b^{\frac{N-1}{2}} \equiv \pm 1 \bmod N$, but N is not an Euler pseudo-prime to the base b.