MATH 342 Problem Sheet 7: Using primitive roots, and primality tests derived from Fermat's Little Theorem

Due Monday 18th March

1. Solve $7^x \equiv 6 \mod 17$

Hint You might find it easier to spot y with $7^y \equiv -6 \mod 17$ first.

2.

(i) Verify that 7 is a primitive root modulo 22.

Hint: This means that you need to show that 7 has order $\phi(22)$.

(ii) Find all solutions to $y^5 \equiv -1 \mod 22$.

Hint: If $y^5 \equiv -1 \mod 22$, why is it true that y is either primitive, or $y \equiv -1 \mod 22$?

(iii) Solve the equation $19^x \equiv 17 \mod 22$.

Hint: One way to do this is to write 19 and 17 as powers of $7 \mod 22$

3. Use the Big Number Calculator applet whose link is provided on the webpage (or an alternative, if you prefer) to determine which of the following numbers pass the Fermat primality test to base 2, by giving the residue $2^{n-1} \mod n$ in each case:

$$9331,\ 9337,\ 9341,\ 9343,\ 9347,\ 9353,\ \ 9359,\ 9367.$$

For the numbers which pass the Fermat primality test, also apply the Miller Rabin test to as many levels as possible.

4. Let p be a prime and let $q = 2^p - 1$. Using Fermat's Little Theorem for 2 mod p or otherwise, show that $p \mid q-1$. Hence, or otherwise, show that

$$2^{q-1} \equiv 1 \mod q$$

even when q is not prime.

Hint: Since $q = 2^p - 1$, we have $2^p \equiv 1 \mod q$.

Show also that is p is a prime ≥ 3 and if $2^k \mid q-1$ and $q-1 = m \times 2^k$ then $2^m \equiv 1 \mod q$.

Hint: $p \mid (q-1)$ and p is coprime to 2^k.

Remark This shows that, if p is prime, then $q = 2^p - 1$ passes Fermat's primality test, and also passes the Miller Rabin Test to all levels, even if q is not prime.

5.

a) Write down Korselt's Criterion for a composite number N to be a Carmichael number, where $N = \prod_{i=1}^r p_i^{k_i}$ is the prime factorisation of N, with $k_i \in \mathbb{Z}_+$ and $p_i \neq p_j$ for $i \neq j$

b) Check that 2465 is a Carmichael number.

c) Use Korselt's criterion to show that any Carmichael number is odd.

I will collect solutions at the lecture on Monday 18th March. Any solutions which are not handed in then, or by 5pm that day in the folder outside room 516 will not be marked.