MATH 342 Problem Sheet 6: Orders of elements, primitive roots

Due Monday 11th March

1. List all the divisors d of 12 and compute the values of Euler's function $\phi(d)$ for them. Compute the sum of all $\phi(d)$ and make sure that this sum is equal to 12.

2. Show that $5^{58} + 5^{26} + 5^6$ is divisible by 3.

3. Compute $|n|_m$ in each of the following cases:

a) $|3|_5$,

b) $|9|_4$,

c) $|2|_7$

d) $|10|_{11}$

e) $|24|_{11}$

In which cases is $n \mod m$ a primitive root in G_m?

4. Find all the primitive roots mod 9.

5. Calculate the number of elements of G_{35} of order 12.
Hint: If the order $\mod 35$ is 12, then 12 is the lcm of the orders $\mod 5$ and $\mod 7$. This is a consequence of what was proved in lectures, because $G_{35} \cong G_5 \times G_7$. What are the possible orders of elements in G_5 and G_7? If m_1 and m_2 are the orders of an element $\mod 5$ and $\mod 7$ respectively, what are the possible values of m_1 and m_2 giving lcm 12?

6. Find all solutions to:

a) $x^7 \equiv 1 \mod 9$

b) $x^{15} \equiv 1 \mod 9$

7. Find the orders of $|8|_9$ and $|14|_{17}$ and hence find $|8|_{27}$ and $|14|_{289}$. *Hint* For any prime p and any $a \in \mathbb{Z}_+$, $|a|_{p^{n+1}} = |a|_{p^n}$ or $p \cdot |a_{p^n}|$. If $n = |14|_{17}$ then one way to compute $14^n \mod 289$ is to write $14 = 17 - 3$ and compute $(17-3)^n \mod 289$ using the binomial theorem. It might also be a good idea to write $n = n_1 \times n_2$ and find a and b such that $(17-3)^{n_1} = a \times 17 + b \mod 289$.

Alternatively, if you like, you can use the Big Number Calculator on the module webpage to calculate $14^n \mod 289$.

8.

a) Show that for any odd prime $p > 3$, 3 divides $(p^n - 1)/(p-1)$ if and only $p \equiv 2 \mod 3$ if n is even, or $p \equiv 1 \mod 3$ and 3 divides n.

b) Show that 3^2 divides $(p^n - 1)/(p-1)$ if and only if $p \equiv -1 \mod 9$ and n is even; or $p \equiv 2$ or 5 mod 9 and $6 \mid n$; or $p \equiv 1 \mod 3$ and $9 \mid n$.

I will collect solutions at the lecture on Monday 11th March. Any solutions which are not handed in then, or by 5pm that day in the folder outside room 516 will not be marked.

Remark The last question is motivated by the study of odd perfect numbers (which probably do not exist). We know from question 3 on Problem Sheet 3 that if N is an odd perfect number then N can be written in the form $\prod_{k=0}^{r} p_k^{n_0}$ distinct primes p_i with $n_i \geq 1$, n_0 is odd with $p_0 \equiv 1 \mod 4$ and $n_0 \equiv 1 \mod 4$, and n_i is even for $i \geq 1$. We can number the p_i for $i \geq 1$ so that $p_i < p_{i+1}$ for $1 \leq i < r$. So if $p_1 = 3$ then $3^2 \mid N$. The facts you are asked to prove in the question above imply that if $p_1 = 3$ then one of the following hold:

- $p_0 \equiv 2$ or $5 \mod 9$ and $n_0 \equiv -1 \mod 6$;
- $p_0 \equiv -1 \mod 9$ and $n_0 \equiv -1 \mod 9$;

- there is some $i \geq 2$ such that $p_i \equiv 1 \mod 3$ and $n_i \equiv -1 \mod 9$;
- there are two different values of $i \geq 2$ such that $p_i \equiv 1 \mod 3$ and $n_i \equiv -1 \mod 3$;
- there is one such $i \geq 1$ and $p_0 \equiv -1 \mod 3$.