MATH 342 Problem Sheet 5: The Euler function and powers

Due Monday 4th March

1. Compute

a) $\phi(348)$

b) $\phi(34606)$

2. Show that $n^{13} \equiv n \mod 7$ for any $n \in \mathbb{Z}$.

3. Let $n \in \mathbb{Z}$. Show that, if 3 does not divide n, then 3 does divide $n^6 + 1091$.

4. Show that $2^{70} + 3^{70}$ is divisible by 13.

5. Show that $7^{400} - 3^{400} \equiv 0 \mod 1000$.

6. Show that, for any $a \in \mathbb{Z}_+$ which is coprime to 100, $a^{20} \equiv 1 \mod 100$.
Hint: It is enough to show that for any $a \in \mathbb{Z}_+$ which is coprime to 100, $a^{20} \equiv 1 \mod 4$ and $a^{20} \equiv 1 \mod 25$.

7. Show that $n = 2^{17} - 1$ is prime by using Fermat's Little Theorem $2^{p-1} \equiv 1 \mod p$ for any prime p dividing n.

8. Let $n \in \mathbb{Z}_+$ with $n \geq 2$ and write

$$n = \prod_{k=1}^{r} p_k^{n_k}$$

for some $r \geq 1$ and distinct primes p_k and integers $n_k \geq 1$. The formula for $\phi(n)$ is then

$$\phi(n) = \prod_{k=1}^{r} (p_k^{n_k - 1}(p_k - 1))$$

Explain why $p_k - 1$ factorises as the product of at least two primes (not necessarily distinct) if $p_k \geq 5$. Deduce that if $\phi(n)$ is the product of at most two primes (not necessarily distinct) then:

(i) $r \leq 2$;

(ii) if $r = 2$ then one of the primes p_k, say p_1, is 2, and $n_1 = n_2 = 1$ if $p_2 \geq 5$, and $n_1 + n_2 \leq 3$ (so that either both n_1 and n_2 are 1 or one of them is 1 and the other is 2) if $p_2 = 3$;

(iii) if $r = 1$, then $n_1 = 1$ if $p_1 \geq 5$, $n_1 \leq 2$ if $p_1 = 3$ and $n_1 \leq 3$ if $p_1 = 2$.

These conditions imply that if $\phi(n)$ is the product of at most two prime factors, for an integer $n \geq 2$, then n must be one of the following (although not all of these are possible):

$$2,\ 4,\ 8,\ 3,\ 6,\ 12,\ 9,\ 18,\ p,\ 2p$$

where p is a prime ≥ 5.

9. Compute $\phi(n)$ for each n in the list at the end of the previous question. Use this to find all integers $n \in \mathbb{Z}_+$ such that $\phi(n) = 6$, and to show that there is no $n \in \mathbb{Z}_+$ for which $\phi(n) = 14$.

I will collect solutions at the lecture on Monday 4th March. Any solutions which are not handed in then, or by 5pm that day in the folder outside room 516 will not be marked.