The following questions, or parts of questions, count for assessment: 1(i)(ii)(iii), 2, 3, 4, 7, 8, 9. These are marked *. Please hand in your solutions, via the Coursework Box on Level 8 of the Laver Building, by Friday 6th December.

1. Find all solutions (if there are any) to each of the following congruences:
(i)* $x^2 \equiv -5 \pmod{7^3}$; (ii)* $x^2 \equiv 3 \pmod{7^3}$;
(iii)* $x^3 + 6x^2 + x + 5 \equiv 0 \pmod{13^2}$; (iv) $x^3 + x^2 + 8 \equiv 0 \pmod{11^3}$.

Total for question: [14]

2*. (i) Find all n for which $\varphi(n) = m$ for $m = 4, 10, 14, 24$. **[10]**
(ii) Show that if $n > 2$ then $\varphi(n)$ is even. **[3]**
(iii) Let $p \geq 5$ be prime. Show that the equation $\varphi(n) = 2p$ has exactly two solutions if $2p+1$ is prime, and none otherwise. **[7]**

Total for question: [20]

3*. Let $m, n \in \mathbb{N}$ with $\gcd(m, n) = 1$. Show that the positive divisors d of mn are precisely the numbers of the form kl where k, l are any positive divisors of m, n respectively, and that each d can be represented in this form in only one way. **[6]**

4*. A function $f\colon \mathbb{N} \longrightarrow \mathbb{N}$ is called a *multiplicative function* if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.
Let $\sigma(n)$ denote the sum of all positive divisors of n, and let $\tau(n)$ denote the number of positive divisors of n. Show that σ and τ are multiplicative functions. (Use Question 3.) Write down expressions for $\sigma(p^e)$ and $\tau(p^e)$, where p is prime. Hence find formulae for $\sigma(n)$ and $\tau(n)$ in terms of the prime factorisations of n. Use your formulae to evaluate $\sigma(n)$ and $\tau(n)$ for $n = 6, 12, 91, 1092$. **[15]**

5. Let f be a multiplicative function as in Question 4, and define a new function $F\colon \mathbb{N} \longrightarrow \mathbb{N}$ by

$$F(n) = \sum_{d \mid n} f(d).$$

(The sum is over all *positive* divisors d of n.) Show that F is a multiplicative function.

6. A *perfect number* is a natural number n whose positive divisors (excluding n itself) add up to n. Thus for example 28 is a perfect number since $1+2+4+7+14=28$. Show that n is a perfect number if and only if $\sigma(n)=2n$. Hence show that if $n=2^{m-1}p$ where $p=2^m-1$ is a prime, then n is a perfect number. Use Exercise Sheet 2, Question 5(iii) to find 4 perfect numbers. [Euler proved that every *even* perfect number has the form $2^{m-1}p$ with $p=2^m-1$ prime. It is not known whether there are any *odd* perfect numbers.]

7*. In each of the following cases, apply the Miller-Rabin test with the given base a to investigate the primality of the given number n. Use the Binary Powering Algorithm to find $a^m \bmod n$ for the appropriate number m, and show your working.
(i) $n=629$, $a=3$; (ii) $n=1601$, $a=2$; (iii) $n=5461$, $a=2$.
5 for each part: total for question: [15]

8*. Apply Pollard's $p-1$ algorithm with base $a=2$ to find a factor of n in the following cases:
(i) $n=1079$; (ii) $n=2573$; (iii) $n=4097$.
5 for each part: total for question: [15]

9*. Apply Pollard's Rho algorithm with given iteration function f and given initial value x_0 to find a factor of n in the following cases:
(i) $n=1189$, $f(x)=x^2+2$, $x_0=1$;
(ii) $n=3127$, $f(x)=x^2+2$, $x_0=2$;
(iii) $n=3959$, $f(x)=x^2+1$, $x_0=1$.
5 for each part: total for question: [15]

Nigel Byott
November 2002