AC, 17th November 2008

M3P14 Elementary Number Theory—Problem Sheet 3.

This is assessed coursework. Please hand in solutions to the starred questions on **Monday 01st December.**

Questions with a † are harder. You should be able to do all other questions without much difficulty.

(1) Compute the following values of $\sigma(n) = \sum_{d|n} d$: (a) $\sigma(10)$, (b) $\sigma(20)$, (c) $\sigma(1728)$.

(2) (a) Show that a power of 3 can never be a perfect number.
(b) More generally if p is an odd prime, show that a power of p can never be a perfect number.
(c) Show that a number of the form $3^i 5^j$ can never be a perfect number.
(d) More generally, if p is an odd number greater than 3, show that the product $3^i p^j$ can never be a perfect number.
(†e) Show that if p, q are distinct odd primes, then $p^i q^j$ is not a perfect number.

(3) Show that there are infinitely many primes that are congruent to 5 modulo 6. (*Hint.* Use $N = 6p_1p_2 \dots p_r + 5$.)

(4) (a) Prove that $\varphi(n)$ is even if and only if $n \geq 3$.
(b) For which $n \geq 1$ is $\varphi(n)$ a multiple of 3?

(5) (a) Find all the elements of $(\mathbb{Z}/11\mathbb{Z})^\times$ that have order n mod 11, for (i) $n = 2$, (ii) $n = 3$, (iii) $n = 5$.
(b) What are the primitive roots mod 11?

(6) Let $a \in \mathbb{Z}$ have order k mod m. Let $h \geq 1$ be an integer. Prove that a^h has order k mod m if and only if $\mathrm{hcf}(h, k) = 1$.

(7) Let p be an odd prime, and let a be any integer. Prove that a^2 is not a primitive root mod p.

(8*) Prove *Wilson's Theorem*: A positive integer n is prime if and only if $(n-1)! \equiv -1 \mod n$. [*Hint:* If n is prime, partition $(\mathbb{Z}/n\mathbb{Z})^\times$ into subsets $\{a, a^{-1}\}$ and then take the product. The other direction is easier.]

(9*) Create a table of indices modulo 17 using the primitive root 3. Use your table to solve the congruence $4x \equiv 11 \mod 17$. Use your table to find all solutions of the congruence $5x^6 \equiv 7 \mod 17$.

(10*) Let p be a prime. (a) If k divides $p - 1$, show that the congruence $x^k \equiv 1 \mod p$ has exactly k distinct solutions.
(b) More generally, consider the congruence

$$x^k \equiv a \bmod p$$

Find a simple way to use the values of k, p, and the index $I(a)$ to determine how many solutions this congruence has.
(c) The number 3 is a primitive root modulo 1987. How many solutions are there to the congruence $x^{111} \equiv 729 \mod 1987$? (*Hint.* $729 = 3^6$.)

(11) For any number $m \geq 2$, not necessarily prime, we say that g is *a primitive root modulo* m if the smallest power of g that is congruent to 1 modulo m it the $\varphi(m)^{\text{th}}$ power. That is, g is a primitive root modulo m if $\text{hcf}(g, m) = 1$ and $g^k \not\equiv 1 \bmod m$ for all powers $1 \leq k < \varphi(m)$.
(a) For each number $2 \leq m \leq 25$, determine if there are primitive roots modulo m.
(b) Use your data from (a) to make a conjecture as to which m have primitive roots and which don't.
(†c) Prove that your conjecture in (b) is correct (this is actually quite hard; you should first fight with the case n the power of a prime).

(12*) Recall the statement of the Gauss Lemma: p is an odd prime, a an integer such that $p \nmid a$, $N = (p-1)/2$ and a_j (for $j = 1, ..., N$) is the unique integer with $-N \leq a_j \leq N$ and $a_j \equiv ja \mod p$. Then:

$$\left(\frac{a}{p}\right) = (-1)^{\nu_p(a)}$$

where $\nu_p(a) = \#\{a_j \mid a_j < 0\}$.

Work out from the definitions a formula for $\nu_p(-2)$. Deduce from this that if p is an odd prime then $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1$ or $3 \bmod 8$ (of course, you can also prove this from the formulae for $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$ but I'm asking you to do it directly using only the Gauss Lemma).