AC, 03rd November 2008

M3P14 Elementary Number Theory— Problem Sheet 2.

This is assessed coursework. Please hand in solutions to the starred questions on **Monday 17th November.**

(1*) Find the smallest non-negative integer x simultaneously satisfying

$$\begin{cases} x & \equiv 2 \mod 3 \\ x & \equiv 3 \mod 5 \\ x & \equiv 1 \mod 4. \end{cases}$$

(2) (a) How many elements does $(\mathbb{Z}/9\mathbb{Z})$ have? And how many does $(\mathbb{Z}/9\mathbb{Z})^\times$ have? For each element of $(\mathbb{Z}/9\mathbb{Z})^\times$, find its inverse (using any method you like).
(b) What is the solution to $7x \equiv 5 \mod 9$?

(3*) Compute $2^{9990} \mod 9991$ and use your answer to say whether you believe that 9991 is prime. (Hint: by Fermat's "little" theorem, if p is prime, then, for all a, $a^p \equiv a \mod p$.)

(4) (a) Solve the congruence $x^{113} \equiv 347 \mod 463$.
(b) Solve the congruence $x^{275} \equiv 139 \mod 588$.

(5) (a) Let b, k, and n be integers that satisfy

$$\mathrm{hcf}\big(b, m\big) = 1 \quad \text{and} \quad \mathrm{hcf}\big(k, \varphi(m)\big) = 1.$$

Show that b has *exactly one* k-th root $\mod m$.
(b) Suppose instead that $\mathrm{hcf}\big(k, \varphi(m)\big) > 1$; show that either b has no k-th roots mod n, or else it has at least two roots $\mod m$.
(c) If $m = p$ is a prime, look at some examples and try to guess a formula for the number of k-th roots of b mod p (assuming that it has at least one).

(6*) Let b, k, and n be integers; assume that $\mathrm{hcf}\big(k, \varphi(m)\big) = 1$, and let $y, z > 0$ be natural numbers such that

$$ky - \varphi(m)z = 1.$$

(a) If m is a product of distinct primes, show that $x \equiv b^y \mod m$ is always a solution to

$$x^k \equiv b \mod m$$

even if $\mathrm{hcf}(b, m) > 1$.
(b) Show that the method does not work for the congruence $x^5 \equiv 6 \mod 9$.

(7)(a) Evaluate $\varphi(1)$, $\varphi(100)$, $\varphi(101)$ and $\varphi(102)$.
(b) Prove that if n is odd then $\varphi(2n) = \varphi(n)$.
(c) Prove that if $n > 2$ then $\varphi(n)$ is even.

(8) Here is a low-level proof of the Fermat-Euler theorem. Say $m \in \mathbb{N}$ and $a \in \mathbb{Z}$ with $\mathrm{hcf}(a, m) = 1$. Let S be the set $(\mathbb{Z}/m\mathbb{Z})^\times$.
(a) Prove that the map $x \mapsto ax$ is a bijection from S to itself (hint: write down an inverse).

(b) Deduce that $\prod_{s\in S} s \equiv \prod_{s\in S} as \bmod m$.
(c) If P denotes $\prod_{s\in S} s$ then prove that $P \in S$.
(d) Deduce from (b) that $P \equiv a^{\varphi(m)}P$ and from (c) that $a^{\varphi}(m) \equiv 1 \bmod m$.

(9) Let f and g be functions $\mathbb{N} \to \mathbb{C}$. Define a new function $f * g$ by

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d),$$

where the sum is, as usual, over the (positive) divisors of n. Prove that if f and g are multiplicative, then $(f * g)$ is also multiplicative.

(10) Let $d(n)$ denote the number of (positive) divisors of n, and let $\sigma(n)$ denote their sum. If $n = \prod_{i=1}^{r} p_i^{e_i}$ with $p_1, p_2, \ldots, p_r$ distinct primes, then show that
(a) $d(n) = \prod_i (e_i + 1)$,
(b) $\sigma(n) = \prod_i \frac{p_i^{e_i+1}-1}{p_i-1}$.

(11*) (a) For $x \geq 2$, show that

$$\sum_{n\leq x} \frac{\log n}{n} = \frac{1}{2}\log^2 x + A + O\Big(\frac{\log x}{x}\Big), \quad \text{and}$$
$$\sum_{2\leq n\leq x} \frac{1}{n\log n} = \log(\log x) + B + O\Big(\frac{1}{x\log x}\Big)$$

where A, B are constants.
(b) If $x \geq 2$, prove that

$$\sum_{n\leq x} \frac{d(n)}{n} = \frac{1}{2}\log^2 x + 2\gamma \log x + O(1)$$

where $d(n)$ is the number of divisors of n and γ is Euler's constant.