MATH 124, PROBLEM SET 2 (SOLUTIONS)

For the problem set due September 19, 2014:

1.) By definition of $\phi(n)$, we want to subtract out the number of multiples of p_i in $n = p_1^{a_1} \cdots p_m^{a_m}$. Note that $\frac{n}{p_1}$ counts the multiples of p_1 in n. By inclusion-exclusion, $\frac{n}{p_1} + \frac{n}{p_2} - \frac{n}{p_1 p_2}$ counts the multiples of p_1 and p_2 (we subtract out multiples of both, as they were counted twice). Extending this logic,

$$\phi(n) = n - \left(\sum_{i=1}^{m} \frac{n}{p_i} - \sum_{i<j}^{m} \frac{n}{p_i p_j} + \sum_{i<j<k}^{m} \frac{n}{p_i p_j p_k} - \cdots \right) = n \prod_{i=1}^{m} \left(1 - \frac{1}{p_i}\right).$$

Multiplicativity follows since if $(a, b) = 1$, then a and b's primes are distinct. One can then separate the product expression in $\phi(ab)$ into two parts to get $\phi(a)\phi(b)$.

Remark. A lot of people gave the proof from class. As said by the hint, we wanted the approach from above, which is independent of CRT and implies multiplicativity, rather than requiring it.

2.) Let $(m, n) = 1$ and ψ multiplicative. Then

$$\Psi(mn) = \sum_{d|mn} \psi(d) = \sum_{r|m, s|n} \psi(rs) = \sum_{r|m, s|n} \psi(r)\psi(s) = \sum_{r|m} \psi(r) \sum_{s|n} \psi(s) = \Psi(m)\Psi(n).$$

Observe that $\sigma(n) = \sum_{d|n} d = \sum_{d|n} I(d)$ where $I(d) = d$ is multiplicative (since integers are multiplicative). Likewise, $d(n) = \sum_{d|n} 1 = \sum_{d|n} J(d)$ where $J(d) = 1$ is multiplicative.

3.) (a) We know that the order of 2 (mod 29) is 28. This suggests that the congruence classes corresponding to $1, 2^4, 2^8, \ldots, 2^{24}$ are distinct solutions, which follows since

$$(2^{4k})^7 = (2^{28})^k \equiv 1 \pmod{29}.$$

This list is exhaustive since our equation can have at most seven solutions, because 29 is prime.

(b) Observe that $x^7 - 1 = (x - 1)(\sum_{k=0}^{6} x^k)$. We have seven solutions for the $x^7 - 1$. The six solutions corresponding to our new equation are therefore the same list, excluding 1.

Remark. Having at most $\deg(x^7 - 1) = 7$ solutions (mod p) applies a result from class known as *Lagrange's theorem* (not the group theory one).

4.) Since $(a, n) = 1$, if $\{x_i\}$ is the set of all numbers coprime to n, then $\{ax_i\}$ is the same set. Hence

$$\prod_{i=1}^{\phi(n)} x_i = \prod_{i=1}^{\phi(n)} a x_i = a^{\phi(n)} \prod_{i=1}^{\phi(n)} x_i.$$

Since $(x_i, n) = 1$ for all i, cancellation gives

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

5.) Since $\phi(100) = \phi(2^2 5^2) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 40$, by Euler's theorem we have $n^{\phi(100)} = n^{40} \equiv 1 \pmod{100}$ when $(n, 100) = 1$. Otherwise, n is a multiple of 2 or 5, which would make the last digit of n^{40} even or 5. Therefore, n^{40} does not end in ...01 only for multiples of 2 or 5.

6.) Equivalently, we want $2^{2^{6k+2}} \equiv -3 \equiv 16 \pmod{19}$. It then suffices to show $2^{6k+2} \equiv 4 \pmod{18}$, as $2^{18} \equiv 1 \pmod{19}$ by Fermat's little theorem. To see why, if $2^{6k+2} = 18m + 4$, then

$$2^{2^{6k+2}} = 2^{18m+4} \equiv 1^m \cdot 2^4 \equiv 16 \pmod{19}.$$

One easily checks that $2^6 \equiv 10 \pmod{18}$, and that $10 \cdot 10 \equiv 10 \pmod{18}$, so $2^{6k} \equiv 10 \pmod{18}$ and therefore $2^{6k+2} \equiv 10 \cdot 2^2 \equiv 4 \pmod{18}$.

7.) Since $s > n$, then (by the *pigeonhole principle*) there exists b with congruence class different from all the $\{a_i\}$. Let $c = -b$. If $s \mid a_i + c = a_i - b$, then $a_i \equiv b \pmod{s}$, a contradiction. Hence $s \nmid a_i + c$ for all i, as desired.

8.) Per the hint, we proceed by contradiction. Suppose n is the smallest number such that

$$b, b^b, b^{b^b}, b^{b^{b^b}}, \dots \pmod{n}$$

does not converge $\pmod{n}$. We want to show that for some $m < n$,

$$b, b^b, b^{b^b}, b^{b^{b^b}}, \dots \pmod{m}$$

does not converge $\pmod{m}$, as this contradicts the minimality of n.

Notice that the sequence of exponents is the same as the sequence (plus an extra 1 term). Consider the powers of b, i.e., $b, b^2, b^3, \dots$. This must enter a cycle $\pmod{n}$ of some length m. Clearly $m < n$, since at best it goes through all the non-zero residues of n (if it went to zero, it would stay at zero to give a cycle length of 1). Finally, if the sequence does not converge $\pmod{n}$, then the sequence of its exponents could not converge $\pmod{m}$. (Think about this! Refer to Question 6's solution for similar, but not identical, intuition.)

Remarks.

- The method of passing to the exponent was explored in Question 6 and is implied by the sequence itself. Writing out the hint as above should have made you look for m, suggesting this proof.
- Note that m is not necessarily equal to $\phi(n)$, because we do *not* require $(b, n) = 1$. In fact, no power of b might be congruent to 1 (e.g., $2 \pmod{4}$).
- This problem is adapted from the 1991 USAMO: http://www.artofproblemsolving.com/Wiki/index.php/1991_USAMO_Problems/Problem_3.