Math 353 Exam #2 Wednesday, November 20, 2002

1. (a) (10 pts) Show that 2 is a primitive root of 19.

   (b) (15 pts) Use part (a) to find $\text{ord}_{19}\, b$ for $1 \le b \le 18$.

b	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\text{ord}_{19}\, b$	1	18					3											

   (c) (5 pts) List the primitive roots of 19 (use the table in part (b)):

   (d) (10 pts) How many solutions does each congruence have (use part (b)):

   (i) $x^8 \equiv 7 \pmod{19}$

   (ii) $x^{27} \equiv 3 \pmod{19}$.

2. (15 pts) Show that if p is prime and $d|(p-1)$, then there is a number c with $\text{ord}_p\, c = d$.

3. (20 pts) Find $\tau(720)$, $\phi(720)$, $\sigma(720)$ and $\lambda(720)$.

4. (13 pts) Recall that a composite n is called a *pseudoprime* to the base a if $a^{n-1} \equiv 1 \pmod{n}$. Suppose p is prime, $p \equiv 2 \pmod{3}$ and let $n = 4p$. Show that n is **not** a pseudoprime to any base a with $1 < a < n$ and $(a, n) = 1$. (Hint: consider $\text{ord}_n\, a$)

5. (12 pts) If n has prime factorization $n = p_1^{e_1} \cdots p_k^{e_k}$, define $\Omega(n) = e_1 + e_2 + \cdots + e_k$. If $n = 1$, define $\Omega(n) = 0$ (i.e. $\Omega(n)$ is the number of prime powers that divide n). Prove that $f(n) = 2^{\Omega(n)}$ is a multiplicative function.

   Bonus (10 points) Prove that $\tau(n) \le 2^{\Omega(n)}$ for all $n \in \mathbb{N}$.