EXAM 2. NAME:____________________

1) (8pts) Show that if p is a prime and $a \in \mathbb{Z}$ then $p | (a^p + a(p-1)!)$.

2) (8pts) Show that if n is a pseudoprime to the base a then n is a pseudoprime to the base a^k for all positive k.

3) (12pts) Show that if $2 \nmid a$ or $8|a$ then $a^5 \equiv a \pmod{40}$.

4) a) (6pts) Show that $\phi(p \cdot n) = \begin{cases} (p-1)\phi(n) & \text{if } p \nmid n \\ p\phi(n) & \text{if } p|n \end{cases}$ for p a prime.

b) (6pts) Find all n with $\phi(n) = 4$. (Show your work.)

5) a) (8pts) Find all n with $\sigma(n) = 12$. (Show your work.)

b) (3pts) Find $\tau(48)$.

6) (8pts) Show that if $m \in \mathbb{Z}^+$ and there is an integer a relatively prime to m such that $\operatorname{ord}_m a = m - 1$ then m is prime.

7) a) (7pts) Find a complete set of incongruent primitive roots modulo 11.

b) (4pts) Find a complete set of incongruent primitive roots modulo $2 \cdot 11$.

c) (3pts) If r is a primitive root modulo 13 then give possible primitive roots modulo 13^2.

d) (3pts) If r is a primitive root modulo 13^2 then give a primitive root modulo 13^k for all $k \in \mathbb{Z}^+$.

8) a) (4pts) Encrypt OK $(14, 10)$ using $C \equiv 3P + 12 \pmod{26}$.

b) (4pts) What is the decryption cipher for part (a)?

9) (8pts) Encrypt DO NOT $(3, 14, \quad 13, 14, 19)$ using the Vigenere cipher with the key KEY $(10, 4, 24)$.

10) (8pts) Suppose you have a message P, $1 < P < n$ and an RSA modulus n. How can you find the decryption exponent if $(n, P) > 1$?