Math 25 Second Exam - Part a

November 10, 2009

Instructions: You should show all of your work and reasons for your computations with the exception that you may solve simple congruences by inspection.

1. (10) Find the least nonnegative residue of $2^{12345614} \pmod{125}$. Note $125 = 5^3$.

2. (10) Recall that a Carmichael number is a composite number n so that for every $a \in U_n$, $a^{n-1} \equiv 1 \pmod{n}$.

   Show that $n = 1729 = 7 \cdot 13 \cdot 19$ is a Carmichael number. Hint: $n - 1 = 1728 = 2^6 3^3$.

3. Cryptography.

   (a) (5) Consider a simple RSA encryption scheme in which the two chosen primes are $p = 3$, $q = 11$. The public encryption key is $(e, n) = (7, 33)$. Describe how to find the decryption key in terms of the variables e and n, and then find it.

   (b) (5) If Alice and Bob have public encryption keys E_A and E_B, and private decryption keys D_A and D_B, explain how Alice would sign and send an encrypted message M to Bob, so that Bob could prove to a third-party the message was indeed from Alice. Be sure to explain why your procedure guarantees the message is from Alice.

4. (15) Primitive roots.

   (a) (6) Show that 3 is a primitive root modulo 7.

   (b) (9) Find a primitive root modulo 7^{123}.

5. (15)Consider the arithmetic function λ, defined by

$$\lambda(1) = 1, \text{ and,}$$
$$\lambda(p_1^{e_1} \cdots p_r^{e_r}) = (-1)^{e_1+\cdots+e_r}$$

(a) (5) Is λ multiplicative? completely multiplicative? Why/Why not?

(b) (10) Show that $\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{if } n \text{ is a square} \\ 0 & \text{if } n \text{ is not a square} \end{cases}$