Homework #7 MME 529

1. Use Fermat's Little Theorem to show that 297 is not prime.

2. a) Simplify 5^{5281} mod 37. Show all steps.

   b) Do you think similar type of exercises could reinforce secondary students exponent knowledge and skills?

3. Develop your own 2x2 matrix which could be used to encrypt /decrypt pair of numbers or symbols mod 31. Provide one example of an encrypted/decrypted pair to illustrate the validity of what you developed.

4. I provided two proofs of Fermat's Little Theorem. Which one do you prefer? For the one you chose, write the proof up in your own words and approach as if you were presenting it to an Algebra class (which presumably had appropriate background).

5. Consider the RSA Theorem. Where doe the proof break down if p or q is not prime?

6. Pick 2 primes and develop your own RSA encrypt/decrypt scheme. This means provide public and private keys. Show one example of a number being encrypted and decrypted.

7. Suppose we are in $\boldsymbol{Z_p}$ and find that some number **a** has the property that $\mathbf{a^k = 1 \mod p}$ where k < p -1 What relation must k have to p ? (in $\mathbf{Z_{13}}$ 3 is such a number, for example). *Why* must it have the relation you have specified?

8. In $\boldsymbol{Z_{13}}$ what is $\mathbf{\log_6(7)}$? Why?