

Math 235
Written Assignment 6

Solutions to the problems below are due at the beginning of class on Friday, May 22nd. Please follow the guidelines in the course policy handout when completing this assignment.

1. For any integer a and any natural number n , prove that a and a^{4n+1} have the same last digit.

2. For parts a) and b), use the table on page 203 of your textbook to convert letters to numbers. You may also want to use a software package such as *Mathematica* for this problem. In *Mathematica* the command `Mod[m, n]` produces the remainder upon dividing m by n . There is also a nice mod p calculator online at <http://www.mtholyoke.edu/~mpeterso/Applets/CalculatorApplet.html>.

Be sure to explain the steps of your solution in complete sentences.

a) Encrypt the plaintext message UNION COLLEGE using the RSA algorithm with enciphering modulus $n = 3713$ and enciphering exponent $k = 83$.

b) A ciphertext message produced by the RSA algorithm with enciphering modulus $n = 8023 = 71 \cdot 113$ and enciphering exponent $k = 149$ is

919 1251 5203 7700 5406 7336 2650 1639 3624 7415 2101 525 5392 4433 413

Determine the recovery exponent and the original plaintext message.

3. Let M be a plaintext message and r be the corresponding ciphertext message for an RSA code with enciphering modulus n , enciphering exponent k , and recovery exponent j . Suppose that $\gcd(M, n) \neq 1$. Prove that $r^j \equiv M \pmod{n}$.

4. Prove that if every prime that divides n also divides m , then $\phi(nm) = n\phi(m)$.

5. Let p be an odd prime and a be an integer such that $\text{ord}_p(a) = 2k$. Prove that $a^k \equiv -1 \pmod{p}$.

6. Prove that the odd prime divisors of the integer $n^4 + 1$ are of the form $8k + 1$.

7. Let r be a primitive root of the integer n . Prove that r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$.