Homework Assignment HW4  Due Friday, February 27, 2015

Instructions: Do not copy work from other sources. You may freely use MAPLE or comparable software. Check your answers whenever it is reasonable to do so.

1. Consider the smallest 16-digit prime number, which is
\[ p = 10^{15} + 37 = 1000000000000037. \]
Find an integer \( a \) such that
\[ a^{4321} \equiv 418910750415330 \mod p. \]

Hint: Find integers \( r \) and \( s \) such that \( 4321r + (p - 1)s = 1 \); then use Fermat’s Little Theorem to simplify \( a^{4321r+(p−1)s} \mod p \). Do not try to run an exhaustive search through all the quadrillion possible values of \( a \mod p \).

2. Refering to the prime \( p \) given in #1, find an integer \( b \) such that
\[ b^{1234} \equiv 256360808697320 \quad \text{and} \quad b^{4321} \equiv 584631348017142 \mod p. \]

Hint: Apply the extended Euclidean Algorithm for the exponents 1234 and 4321. Do not try to run an exhaustive search through all the quadrillion possible values of \( b \mod p \).

3. Consider the integer
\[ n = 10000\cdots02673000\cdots0801. \]
Using Fermat’s Little Theorem, show that \( n \) is not prime. Does your computation provide the prime factorization of \( n \)? Explain.

4. Referring to the number \( n \) given in #3, you are given the additional information that
\[ \phi(n) = 10000\cdots02662000\cdots0532. \]
Using this additional information, determine the prime factorization of \( n \).

Hint: Assume that \( n \) has two distinct prime factors \( p \) and \( q \). From the information given, obtain a quadratic equation in \( p \) which may be solved using MAPLE. The point of this exercise is that for large values of \( n \), determining \( \phi(n) \) is of the same level of difficulty as factoring \( n \).