Number theory and cryptography

HW 2

The notation is as used in the class or the book.

1. Suppose you are using the RSA scheme to receive messages, using \( p = 1733 \) and \( q = 2347 \).
   (a) Check that \( e = 31 \) is a valid encryption key.
   (b) Suppose you make the key \( e \) and the product \( pq \) public, and someone sends you the encrypted number 3436451. What is the decrypted number (i.e., the original number)?

2. Check if 3127 is a pseudoprime to the base 2. Does the test tell you whether 3127 is prime or composite?

3. Check if 561 is a pseudoprime to the base 2. Does the test tell you whether 561 is prime or composite? If not, try the Miller-Rabin test to the base 2 again. What does this test tell you?

4. (Problem V.3.5 in the book, p. 153) Let \( n = 2701 \). Use the \( B \)-numbers \( 52^2 \) and \( 53^2 \) mod \( n \) for a suitable factor-base \( B \) to factor 2701.

To do the calculations, you may use:

Wolfram alpha:
go to http://www.wolframalpha.com/
You can enter whatever you want to calculate and press the “=” sign.
to do \( ab \mod m \), do \( a \* b \mod m \);
to raise \( a \) to \( b \) modulo \( n \), type \( a^b \mod n \), e.g., \( 3^{-1} \mod 49 \) to find the inverse of 3 modulo 49
to find the prime factorization of an integer \( a \), do \text{factor}(a)
to find gcd\( (a,b) \), do \text{gcd}(a,b);

Maple:
You can type \? for help.
In maple, at the end of any command, you need to put a semicolon.
to do \( ab \mod m \), do \( a \* b \mod m \);
to find the inverse of \( e \mod m \), do \( 1/e \mod m \);
to do \( a^b \mod m \) quickly, do \( a \&^b \mod m \);
to factor an integer \( a \), do \text{ifactor}(a);
to find gcd\( (a,b) \), do \text{igcd}(a,b);
to avoid noting down and entering numbers, you can use variables.
For example: \( x = a \* b \mod m \);
to quit: \text{quit};