EECS 70 Discrete Mathematics and Probability Theory
Spring 2014 Anant Sahai

Discussion 5B

1. **Simplifying Some "Little" Exponents** For the following problems, you must both calculate the answers and show your work.

   1. What is $2^{2013} \bmod 11$? *(Hint: There's a little theorem from class which you may find useful here. Of course, if you prefer, you can always just play around and (re-)discover the relevant pattern for yourself.)*
   2. What is $2^{(5^{2013})} \bmod 11$?

2. **RSA with exponent 3**

   Consider an RSA scheme modulus $N = pq$, where p and q are prime numbers larger than 3. In this setting, Alice wants to send a message x to Bob with public key (N, e).

   1. Find a condition on p and q such that $e = 3$ is a valid exponent.
   2. Now suppose that $p = 11$, $q = 17$, and $e = 3$. Find the secret key d used in this scheme.
   3. Alice wants to send a message $x = 70$ to Bob. What is the encrypted message she sends using the public key?

3. **RSA with multiple keys**

   Members of a secret society know a secret word. They transmit this secret word x between each other many times, each time encrypting it with the RSA method. Eve who is listening to all of their communications notices that in all of the public keys they use, the exponent e is the same. Therefore the public keys used look like $(e,N_1),\ldots,(e,N_k)$ where no two N_i's are the same. Assume that the message is x such that $0 \leq x < N_i$ for every i.

   1. Suppose Eve sees the public keys $(7,35)$ and $(7,77)$ as well as the corresponding transmissions. Note that gcd(77, 35) = 7. Can Eve use this knowledge to break the encryption?
   2. The secret society has wised up to Eve and changed their choices of N, in addition to changing their word x. Now, Eve sees keys $(3,5*23)$, $(3,11*17)$, and $(3,29*41)$ along with their transmissions. Argue why Eve cannot break the encryption in the same way as above.
   3. Recall from the problem statement that these public keys imply that $(x < 5*23) \wedge (x < 11*17) \wedge (x < 29*41)$. Let us suppose for this part and the next that the society chose $x = 100$, which you can check satisfies the inequalities (though Eve doesn't know!). Is x^3 greater or less than $(5*23)(11*17)(29*41)$?
   4. Imagine that, from the transmissions above, Eve can figure out $x^3 \bmod (5*23)(11*17)(29*41)$. In addition, give her a machine that lets her take cube-roots of integers. Can Eve deduce x?

   Now we will extend this to a more abstract case. Use your answers and methods from the previous parts to answer the following:

   1. Show that if two of the N_i's have a gcd other than 1, then Eve can easily decrypt the word x.

2. Now suppose that every pair of N_i's are co-prime (i.e. they have a gcd of 1). Suppose that Eve has a machine that given the remainders of an unknown number y mod each N_i produces the remainder of y mod $N_1 \times N_2 \times \ldots N_k$. If she uses this machine on all of the encrypted messages, what does she get?
3. Eve knows how to take the t-th root of any real number (not modulo something though) for any t. Using this fact show that if $k > e$ then she can find out the secret word x.