ICS 6D **Due: Wednesday, November 5, 2014, 3:00PM**

Homework 4

Instructor: Sandy Irani

1. Compute $gcd(72, 42)$ and write it in the form $72 \cdot s + 42 \cdot t$ for integers s and t.

2. Compute $gcd(80, 61)$ and write it in the form $80 \cdot s + 61 \cdot t$ for integers s and t.

3. Compute $gcd(630, 147)$ and write it in the form $630 \cdot s + 147 \cdot t$ for integers s and t.

4. Find the multiplicative inverse of 52 mod 77. Note that your answer should be a number y in the range from 0 through 76 such that $x \cdot y$ mod $77 = 1$.

5. Consider the decimal number $N = 214$. Show the representation of N in the following bases:
   (a) Binary
   (b) Hex
   (c) Base 7.
   (d) Base 3.

6. Give the decimal representation for the following numbers:
   (a) $(1100110)_2$
   (b) $(346)_7$
   (c) $(B2)_{16}$

7. (a) What is the decimal representation of $(1000)_8$?
   (b) What is the largest number that can be represented with three digits base 8? (Give the base-8 representation of the number as well as its decimal representation).
   (c) What is the relationship between the values of the two numbers in the previous two questions?

8. Compute $(53)^{37}$ mod 11. (You shouldn't need a calculator).

9. Bob publishes his public key $(e, N) = (109, 221)$
   (a) Show that if you can factor N ($N = 13 \cdot 17$), then you can determine Bob's private key (both d and ϕ).
   (b) Suppose now that you intercept the message 89. Use Bob's private key to decrypt the message.

10. In this problem, we will implement the RSA algorithm to encrypt and decrypt the message "HI". You will want to use a calculator that can compute the mod function. The standard calculator on any Windows machine will work.
   (a) Use the scheme used in your text to convert the message "HI" into an integer. Call the integer m.
   (b) Set the primes p and q as follows: $p = 43$ and $q = 79$. What are the values for N and ϕ?
   (c) The value for e is chosen to be 29. Use Euclid's algorithm to verify that e and ϕ are relatively prime and to find d, the multiplicative inverse of e mod ϕ.

(d) Compute $m^e \bmod N$.

(e) The results of the previous question is the cyphertext c that is transmitted. Now in order to decrypt the message, compute $c^d \bmod N$.

(f) Did you get back m in your answer to the previous question? Translate the number back into a text message.