In all of the following questions, show the details of your work (it is not enough to just give the answer).

Question 1. (10 points) In what follows we assume that a is small enough that you do not need to worry about the answer being too large to fit in a computer word (i.e., the word size of 64 bits on your computer is large enough for the answer).

1. Explain how, given an integer a, the integer a^{14} can be computed using only 5 integer multiplication operations.
2. Explain how, given an integer a, the integer a^{24} can be computed using only 5 integer multiplication operations.

Question 2. (10 points) Read the extension to the Euclidean gcd algorithm that is described on page 12 and on the first half of page 13 in the Module 5 notes. The below recursive algorithm `EEuclid` summarizes this extension: It takes as input a pair of nonnegative integers a and b where $a \geq b$ and returns a triple of the form (d, x, y) that satisfies equation

$$\gcd(a, b) = d = a * x + b * y$$

where x, y may be negative. In what follows, $\lfloor a/b \rfloor$ denotes the integer part of a/b (for example, $\lfloor 9/2 \rfloor = 4$).

Algorithm `EEuclid`(a, b)

1. If $b == 0$ then return $(a, 1, 0)$, otherwise continue with the next steps
2. $(d', x', y') =$ `EEuclid`$(b, a \bmod b)$
3. $d = d'$
4. $x = y'$
5. $y = x' - \lfloor a/b \rfloor * y'$
6. return (d, x, y)

Run the above algorithm on the two numbers $a = 172$ and $b = 20$. Show what happens at each level of the recursion (i.e., show the recursive call for that level and the (d, x, y) values that each call returns).

Question 3. (10 points) Read the Chinese Remainder Remainder Theorem in the Module 5 notes (second half of page 13 and first half of page 14). Use it to find an integer x, $0 < x < 105$, such that all three of the following are satisfied:

- $x = 2 \bmod 3$

- $x = 3 \bmod 5$
- $x = 2 \bmod 7$.

Question 4. (10 points) Consider the RSA encryption scheme with public key $n = 143$ and $e = 7$. Encipher the plaintext integer $M = 112$. Break the cipher by finding p, q and private key d. Decipher the ciphertext integer $C = 7$.

Date due: March 29, 2011