# Math 246S: Homework 4 <br> Due at the beginning of tutorial Tuesday, Feb 7, 2012 at 8:10 PM sharp! 

(1) Find integers $x$ and $y$ so that $1352 x+495 y=$ g.c.d(1352,495). Can $x$ and $y$ be both chosen to be negative? Why or why not?
(2) You have two glass bottles, one holds exactly 7 liters and the other 19 liters. How do you measure 1 liter of water using these two bottles?
(3) Give a careful proof by induction that the Euclidean algorithm always allows to express g.c.d $(a, b)$ as $a x+b y$ for some integers $x, y$. Hint: Use induction on the number of steps in the Euclidean algorithm.
(4) (a) Prove that two consecutive natural numbers (for example 2013 and 2012) are relatively prime.
(b) Compute the multiplicative inverse of $2013 \bmod 2012$ using the Euclidean algorithm.
(5) Find an integer $x$ satisfying the following equation: $2 x \equiv 19(\bmod 77)$.
(6) Find a multiple of 77 that ends with 999.
(7) Find all integer solutions of $13 x+23 y=1$.
(8) You are to receive a message using the RSA system. You choose $p=7, q=19$ and $e=5$. You therefore tell the world that $N$ is 133 and $e$ is 5 . I send you an encoded message; the encoded version you receive is 100 . What is the original (before coding) message?
(9) Consider the RSA system. Suppose $N$ and $e$ are given. For a message $M<N$, the encoded message is denoted by $R$. As $M$ ranges over all the integers between 0 and $N-1$ what are all the numbers $R$ that you get? Hint: $R$ is an integer between 0 and $N-1$.

