CSE 280 Challenge Set 11

Question 1

Use the Eulcid Algorithm to find the gcd for the following pairs of numbers. Use tables as we did in class. Note that you may not need all the rows in the table below.

- $gcd(80, 32)$

$x = r'$	$y = x'$	$r = y \bmod x$

- $gcd(560, 792)$

$x = r'$	$y = x'$	$r = y \bmod x$

Question 2

Use the Extended Euclid Algorithm to express the answers to question 1 as a linear combination.

- $gcd(80, 32) = s * 80 + t * 32$

$x = r'$	$y = x'$	$r = y \bmod x$	$q = y \operatorname{div} x$	$s = t' - qs'$	$t = s'$

- $gcd(560, 792) = s * 560 + t * 792$

$x = r'$	$y = x'$	$r = y \bmod x$	$q = y \operatorname{div} x$	$s = t' - qs'$	$t = s'$

Question 3

Part 1

Create public and private RSA keys. Use the two prime numbers: $p = 163$ and $q = 431$. Calculate N (public) and ϕ. Select the **smallest** value e (public) such than $gcd(e, \phi) = 1$. Use the Extended Eulicd Algorithm to find the multiplicative inverse of $e \bmod \phi$ and call the result d (private).

Determine the equations to encrypt and decrypt. Use the table below to execute the Euclid algorithm.

$x = r'$	$y = x'$	$r = y \bmod x$	$q = y \operatorname{div} x$	$s = t' - qs'$	$t = s'$

Part 2

Use a python terminal (which is good at working with large numbers) to encrypt and decrypt the word "PIE" using the RSA keys obtained in Part 1 above. To convert the letters to numbers, use the ASCII code provided in the second column. Use the Python terminal to do the math.

Letter	ASCII	Encrypted	Decrypted	Letter
P	80			
I	73			
E	69			