MATH 343 (was: 396) Practice Hour Exam from April, 2004

1. Find the greatest common divisor gcd (273, 317) = d, and integers x, y so that d=273x+317y.

2. Use the Euler ϕ-function to find the number of inverible elements (under multiplication) in $\mathbf{Z}/(225)\mathbf{Z}$. Find the inverse of 11 mod 225. Find all solutions of the following equations

(a) 11x = 3 mod 225 and
(b) 5x = 2 mod 225.

3. Suppose that an affine linear encryption function e with block length 2 is used to encrypt messages written in usual alphabet with 26 letters; so that

$$e : (\mathbf{Z}/26\mathbf{Z})^2 \to (\mathbf{Z}/26\mathbf{Z})^2.$$

suppose that we are able to decrypt cipher texts

$$c_0 = \begin{pmatrix} 4 \\ 1 \end{pmatrix}, c_1 = \begin{pmatrix} 11 \\ 1 \end{pmatrix}, c_2 = \begin{pmatrix} 5 \\ 20 \end{pmatrix}$$

as coming from the plain texts

$$w_0 = \begin{pmatrix} 1 \\ 3 \end{pmatrix}, w_1 = \begin{pmatrix} 4 \\ 8 \end{pmatrix}, w_2 = \begin{pmatrix} 2 \\ 3 \end{pmatrix}.$$

Determine e.

4. Show that 2 generates the multiplicative group of integers mod 13. Find the discrete log base 2 of 6 (that is, j so $2^j = 6$ mod 13).

5. If n=$11 \cdot 17$ is the modulus to be used for RSA, and e = 3 is the encryption exponent, find the decryption exponent.