HOMEWORK No 4 (February 2, 2005)

Exercise 1. *Associate the letters of the alphabet* $\Omega = \{A, B, C, \ldots, Z\}$ *with the (ordered) set of elements* $\{\alpha_0 = [0], \alpha_1 = [1], \alpha_2 = [2], \ldots, \alpha_{25} = [25]\}$ *of* $\mathbf{Z_{26}}$.
(a) *An (affine) code* $f : \mathbf{Z_{26}} \longrightarrow \mathbf{Z_{26}}$ *is defined by* $f(x) = \alpha_{11} \otimes x \ominus \alpha_{18}$. *Encipher the word* MATHEMATICS.
(b) *Find the inverse mapping to* f *and decipher the word* JAEHVGZGWM.

Exercise 2. *Associate the letters of the alphabet* $\Omega = \{A, B, C, \ldots, Z\}$ *with the (ordered) set of elements* $\{\alpha_0 = [0], \alpha_1 = [1], \alpha_2 = [2], \ldots, \alpha_{25} = [25]\}$ *of* $\mathbf{Z_{26}}$.
(a) *Find the affine code* $f : \mathbf{Z_{26}} \longrightarrow \mathbf{Z_{26}}$ *such that* O *is encoded as* A *and* U *is encoded as* Y.
(b) *Show that, in this code, there are two letters that coincide with their codes. Determine them.*

Exercise 3. *Associate the letters of the alphabet* $\Omega = \{A, B, C, \ldots, Z\}$, *the set of the digits* $\{0, 1, 2, \ldots, 9\}$ *and the " blank " symbol with the (ordered) set of elements* $\{\alpha_0 = [0], \alpha_1 = [1], \alpha_2 = [2], \ldots, \alpha_{25} = [25], \alpha_{26} = [26], \alpha_{27} = [27], \ldots, \alpha_{35} = [35], \alpha_{36} = [36]\}$ *of* $\mathbf{Z_{37}}$.
(a) *Decipher the message*

$$FSIHZE3WOZDLVJ7OC0BFZOTLWM8D3AR8X \quad WF$$

enciphered using an affine code $f : \mathbf{Z_{37}^2} \longrightarrow \mathbf{Z_{37}^2}$ *and knowing that the first two letters of the message are* T H *and that the message ends with letters* M A I L.
(a) *Answer the message, using the same code, by* THANK YOU.

Exercise 4. *Suppose that in an R.S.A. Public Key Cryptosystem,* $p = 11, q = 17$ *and* $e = 107$ *(a naive choice). Encrypt the word* $LOVE$ *using two-digits blocks and the 26-letter alphabet of Exercise 1. What is the "secret" key* d *?*

Exercise 5. *Solve the following two quadratic equations :*
(a) $z^2 - 2z - 2\,(1 - 2i) = 0$ *;*
(b) $z^2 + 2z - 2\,(1 + 2i) = 0$.

Solutions will be sent to all students by e-mail.
They will be also available in the display case opposite of my office 4205HP
on Monday, February 7, 2005.