that $L = 853$. Further suppose that you know that the two most frequently occurring plaintext digraphs "E " and "S " have encryptions "FQ" and "LE", respectively. Find the deciphering key, and read the message "YAVAOCH'D!"

16. Continuing along the lines of Exercise 15, here is an example of how one can, without too much extra work, create a cryptosystem that is much harder to break. Let f_1 be one cryptosystem of the type described in Exercise 15, i.e., given by the rule $f_1(P) \equiv a_1P + b_1 \ mod \ L_1$, and let f_2 be a second cryptosystem of the same type. Here the N and M are the same, but the a's, b's and L's are different. We suppose that $L_2 > L_1$. We then construct the *product* of the two cryptosystems (see Exercise 14), i.e., we encrypt a plaintext message unit P by successively applying the two rules:

$$I \equiv a_1P + b_1 \ mod \ L_1,$$
$$C \equiv a_2I + b_2 \ mod \ L_2.$$

(In the first rule I is the nonnegative integer less than L_1 that satisfies the congruence, and in the second rule C is less than L_2.) Because the moduli L_1 and L_2 are different, Exercise 14(c) does not apply, and this product cryptosystem is not generally an affine system. Here we suppose that the two alphabets of M and N letters are always the same, but we are free to frequently change our choice of the parameters a_1, b_1, L_1, a_2, b_2, L_2, subject, of course, to the conditions: $N^2 \leq L_1 < L_2 \leq M^2$, $g.c.d.(a_1, L_1) = 1$, $g.c.d.(a_2, L_2) = 1$. Thus, the enciphering key consists of the six-tuple of parameter values $\{a_1, b_1, L_1, a_2, b_2, L_2\}$. Let the plaintext and ciphertext alphabets be as in Exercise 15, consisting of 27 and 30 letters, respectively. If the enciphering key is $\{247, 109, 757, 675, 402, 881\}$, explain how to *de*cipher, and decipher the message "D!RAJ'KCTN".

2 Enciphering Matrices

Suppose we have an N-letter alphabet and want to send digraphs (two-letter blocks) as our message units. In §1 we saw how we can let each digraph correspond to an integer considered modulo N^2, i.e., to an element of $\mathbf{Z}/N^2\mathbf{Z}$. An alternate possibility is to let each digraph correspond to a *vector*, i.e., to a pair of integers $\binom{x}{y}$ with x and y each considered modulo N. For example, if we're using the 26-letter alphabet A—Z with numerical equivalents 0—25, respectively, then the digraph NO corresponds to the vector $\binom{13}{14}$. See the diagram at the top of the next page.

We picture each digraph P as a point on an $N \times N$ square array. That is, we have an "xy-plane," except that each axis, rather than being a copy