

$$\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

(see Exercise 10 of §I.2). Using the matrix form of the definition, prove that f_n is even if and only if n is divisible by 3. More generally, prove that f_n is divisible by a if and only if n is divisible by b for the following a and b : (a) $a = 2$, $b = 3$; (b) $a = 3$, $b = 4$; (c) $a = 5$, $b = 5$; (d) $a = 7$, $b = 8$; (e) $a = 8$, $b = 6$; (f) $a = 11$, $b = 10$.

7. You intercept the message "SONAFQCHMWPTVEVY", which you know resulted from a *linear* enciphering transformation of digraph-vectors, where the sender used the usual 26-letter alphabet A—Z with numerical equivalents 0—25, respectively. An earlier statistical analysis of a long string of intercepted ciphertext revealed that the most frequently occurring ciphertext digraphs were "KH" and "XW" in that order. You take a guess that those digraphs correspond to "TH" and "HE", respectively, since those are the most frequently occurring digraphs in most long plaintext messages on the subject you think is being discussed. Find the deciphering matrix, and read the message.
8. You intercept the message "ZRIXXYVBMNPO", which you know resulted from a linear enciphering transformation of digraph-vectors in a 27-letter alphabet, in which A—Z have numerical equivalents 0—25, and blank=26. You have found that the most frequently occurring ciphertext digraphs are "PK" and "RZ". You guess that they correspond to the most frequently occurring plaintext digraphs in the 27-letter alphabet, namely, "E " (E followed by blank) and "S ." Find the deciphering matrix, and read the message.
9. You intercept the message "!IWGVIEX!ZRADRYD", which was sent using a linear enciphering transformation of digraph-vectors in a 29-letter alphabet, in which A—Z have numerical equivalents 0—25, blank=26, ?=27, !=28. You know that the last five letters of plaintext are the sender's signature "MARIA".
 - (a) Find the deciphering matrix, and read the message.
 - (b) Find the enciphering matrix, and, impersonating Maria's friend Jo, send the following reply in code: "DAMN FOG! JO!"
10. In this exercise we are again working with the Cyrillic alphabet (see Exercise 12 of the last section). We use a 34-letter alphabet, where in addition to the numerical equivalents listed before we have blank=33. Suppose that still the two most frequently occurring digraphs in Russian are taken to be "HO" and "ET". Meanwhile, we find that in a long string of ciphertext the most frequently occurring digraphs are "IOT" and "ЧМ". We know that the encryption uses a linear enciphering transformation of digraph-vectors in the 34-letter alphabet. Read the intercepted message "СХНСЪШОШШЗ".
11. Prove that the *product* (see Exercise 14 of the last section) of a cryptosystem with enciphering matrix $A_1 \in M_2(\mathbf{Z}/N\mathbf{Z})^*$ and a cryptosys-