Quick links : 3.1 · 3.2 · 3.3 · 3.4

Exercise 3.1

If we try to map $KH \leftrightarrow HE$ and $XW \leftrightarrow TH$ we find matrices which do not give any English deciphered text.

On the other hand, mapping $KH \leftrightarrow TH$ and $XW \leftrightarrow HE$, yields the matrices

$$D = \begin{pmatrix} 23 & 7 \\ 18 & 5 \end{pmatrix} \in M_{2\times 2}\left(\mathbb{Z}/26\mathbb{Z}\right), \qquad D^{-1} = \begin{pmatrix} 9 & 3 \\ 4 & 5 \end{pmatrix}, \tag{3.1.1}$$

that satisfy $D \cdot c_j = m_j$ where

$$c_1 = \text{vect("KH")} = \begin{pmatrix} 10 \\ 7 \end{pmatrix} \qquad c_2 = \text{vect("XW")} = \begin{pmatrix} 23 \\ 22 \end{pmatrix}$$
$$m_1 = \text{vect("TH")} = \begin{pmatrix} 19 \\ 7 \end{pmatrix} \qquad m_2 = \text{vect("HE")} = \begin{pmatrix} 7 \\ 4 \end{pmatrix}.$$

Converting the ciphertext into 8 vectors (18, 14), (13, 0), (5, 16), (2, 7), (12, 22), (15, 19), (21, 4), (21, 24), we get the plaintext "SENATOR TOOK BRIBE".

Exercise 3.2

a) The ciphertext corresponds to the sequence of integers $\in \{0, ..., 28\}$ given by

$$[22, 20, 23, 7, 20, 17, 22, 25, 13, 16, 17, 26, 23, 21, 20, 4, 23, 20, 28, 9, 7, 0, 11, 6, 16, 6, 9, 27].$$

The length is 28, which is indeed a multiple of 4. This yields the following sequence of 7 vectors in $(\mathbb{Z}/29^2\mathbb{Z})^2$:

$$\begin{pmatrix} 658 \\ 674 \end{pmatrix}, \begin{pmatrix} 597 \\ 663 \end{pmatrix}, \begin{pmatrix} 393 \\ 519 \end{pmatrix}, \begin{pmatrix} 688 \\ 584 \end{pmatrix}, \begin{pmatrix} 687 \\ 821 \end{pmatrix}, \begin{pmatrix} 203 \\ 325 \end{pmatrix}, \begin{pmatrix} 470 \\ 288 \end{pmatrix}.$$

On the other hand, the end of the plain text corresponds to the sequence

$$\begin{pmatrix} 207 \\ 3 \end{pmatrix}, \begin{pmatrix} 484 \\ 17 \end{pmatrix}, \begin{pmatrix} 555 \\ 511 \end{pmatrix}.$$

We can compute the deciphering matrix and vector :

$$A' = \begin{pmatrix} 14 & 781 \\ 821 & 206 \end{pmatrix}, b' = \begin{pmatrix} 322 \\ 202 \end{pmatrix}$$

e.g. using SAGE:

```
M = matrix(Integers(29^2),
           [[687, 821, 0, 0, 1, 0],
            [0, 0, 687, 821, 0, 1],
            [203, 325, 0, 0, 1, 0],
            [0, 0, 203, 325, 0, 1],
```

```
            [470, 288, 0, 0, 1, 0],
            [0, 0, 470, 288, 0, 1]])

V = matrix(Integers(29^2),
           [[207],[3],[484],[17],[555],[511]])

M.inverse() * V  #this gives the coefficients of A and of b
```

This finally yields the message "HIT ARMY BASE! HEADQUARTERS" (including the spaces).

b) The enciphering matrix is $(A')^{-1} = A = \begin{pmatrix} 103 & 30 \\ 10 & 7 \end{pmatrix}$ and the enciphering vector is $b = -(A')^{-1} \cdot b' = \begin{pmatrix} 301 \\ 412 \end{pmatrix}$. We find the ciphertext

$$!\text{NJUFYKTEGOUL\_IB!VFEXU!JHALGQCJ?}$$

where "_" represents a space.

Exercise 3.3

a) We will proceed as follows:

$$\ker(A) = \{0\} \iff A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \iff \gcd(\det(A), N) = 1.$$

$\boxed{A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \implies \ker(A) = \{0\}}$. If B is the inverse of A and $x \in \ker(A)$, then $x = (BA)x = B(Ax) = B \cdot 0 = 0$.

$\boxed{\ker(A) = \{0\} \implies A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}$. Consider the map

$$\begin{array}{rccc} f_A: & (\mathbb{Z}/N\mathbb{Z})^2 & \longrightarrow & (\mathbb{Z}/N\mathbb{Z})^2 \\ & v & \longmapsto & A \cdot v \end{array}$$

The assumption $\ker(A) = \{0\}$ is equivalent to saying that f_A is injective, while the conclusion $A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we are looking for is equivalent to saying that f_A is bijective.

But $X := (\mathbb{Z}/N\mathbb{Z})^2$ is a finite set, and any injective map $X \to X$ from a finite set to itself must be bijective. Hence, f_A is bijective and A is invertible.

$\boxed{\gcd(\det(A), N) = 1 \implies A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}$

Recall that $\gcd(\det(A), N) = 1$ is equivalent to saying that $\det(A) \in \mathbb{Z}/N\mathbb{Z}$ is inverible. Now, it is known that

$$^{\mathrm{t}}\mathrm{cof}(A) \cdot A = \det(A) I_2 \tag{3.3.1}$$

where the *adjugate* matrix $^{\mathrm{t}}\mathrm{cof}(A)$ is the transpose of the matrix of cofactors of A. Therefore, A is invertible with inverse given by

$$A^{-1} = \frac{1}{\det(A)} \, ^{\mathrm{t}}\mathrm{cof}(A).$$

$\boxed{\gcd(\det(A), N) = 1 \iff A \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}$.

Let B be the inverse of A. Then $\det(A)\det(B) = \det(AB) = \det(I_2) = 1 \in \mathbb{Z}/N\mathbb{Z}$, so $\det(A)$ is invertible in $\mathbb{Z}/N\mathbb{Z}$, so $\gcd(\det(A), N) = 1$ follows.

b) Let $k \geq 1$. We have seen that a matrix $A \in M_k(\mathbb{Z}/N\mathbb{Z})$ is invertible if and only if $\ker(A) = \{0\}$. Moreover, observe that $\ker(A) = \{0\}$ if and only if the columns $C_1, ..., C_k$ of A are linearly independent over $\mathbb{Z}/N\mathbb{Z}$. Indeed, if $v = {}^{\mathrm{t}}(a_1, .., a_k)$ is a column-vector, then $A \cdot v = \sum_{i=1}^{k} a_i C_i$.

Thus $|\mathrm{GL}_k(\mathbb{Z}/n\mathbb{Z})|$ is the number of k-uplets $(C_1, ..., C_k)$, where each $C_i \in (\mathbb{Z}/N\mathbb{Z})^k$ that are $\mathbb{Z}/N\mathbb{Z}$-linearly independent[2].

Furthermore, by the Chinese reminder theorem, we have a ring isomorphism $\mathbb{Z}/N\mathbb{Z} \cong \prod_{p|N} \mathbb{Z}/p^{v_p(N)}\mathbb{Z}$, where $N = \prod_{p|N} p^{v_p(N)}$ is the factorization of N.This yields a ring isomorphism

$$M_k\big(\mathbb{Z}/N\mathbb{Z}\big) \cong \prod_{p|N} M_k\big(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}\big), \tag{3.3.2}$$

which implies

$$|\,\mathrm{GL}_k\left(\mathbb{Z}/N\mathbb{Z}\right)| = \prod_{p|N} |\,\mathrm{GL}_k\left(\mathbb{Z}/p^{v_p(N)}\mathbb{Z}\right)|, \tag{3.3.3}$$

so it is sufficient to compute $|\,\mathrm{GL}_k\left(\mathbb{Z}/p^r\mathbb{Z}\right)|$ for prime p and an integer $r \geq 1$.

We treat two cases (this is not really induction). Assume first that $\boxed{r = 1}$. Computing $|\,\mathrm{GL}_k(\mathbb{F}_p)|$ amounts to counting the number of k-uplets $(C_1, ..., C_k)$ of vectors in $(\mathbb{Z}/p\mathbb{Z})^k$ that are $\mathbb{F}_p$-linearly independent. How many choices do we have for $C_1 = (a_{11}, ..., a_{1k})$? To ensure the condition of linear independence, we just need $C_1 \neq 0$. So there are $p^k - 1$ choices. Because $\mathbb{F}_p$ is a field, C_2 is linearly independent with C_1 if and only if C_2 is not a multiple of C_1. So there are $p^r - p$ possibilities for C_2. Continuing like this, we finally get

$$|\,\mathrm{GL}_k(\mathbb{F}_p)| = \prod_{j=0}^{k-1} \left(p^k - p^j\right). \tag{3.3.4}$$

Now suppose that $\boxed{r \geq 2}$. The map $\mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ given by $x \pmod{p^r} \longmapsto x \pmod{p}$ induces a group morphism

$$f : \mathrm{GL}_k(\mathbb{Z}/p^r\mathbb{Z}) \to \mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z}).$$

By the first isomorphism theorem (the analogue of the "rank-nullity theorem" from linear algebra), one has

$$|\ker(f)| \cdot |\,\mathrm{Im}(f)| = |\,\mathrm{GL}_k(\mathbb{Z}/p^r\mathbb{Z})|. \tag{3.3.5}$$

[2]In general, it is not true that a matrix $A \in M_k(R)$ over a commutative ring R is invertible if and only its columns are R-linearly independent – there are counter-examples over $\mathbb{Z}$. Exercise 5.23B in *Exercises in Modules and Rings* by T. Y. Lam, based on a result of N. McCoy, states that the columns of A are R-linearly independent if and only if $\det(A)$ is not a zero divisor of R, which is in general weaker than $\det(A) \in R^\times$. But those two notions coincide for *finite* rings R as $\mathbb{Z}/N\mathbb{Z}$.

We claim that f is surjective, that is $\mathrm{Im}(f) = \mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z})$ and $|\ker(f)| = (p^{r-1})^{k^2}$. From this, it will follow that

$$|\,\mathrm{GL}_k(\mathbb{Z}/p^r\mathbb{Z})| = (p^{r-1})^{k^2} \cdot \prod_{j=0}^{k-1} \left(p^k - p^j\right). \tag{3.3.6}$$

(In particular this implies $|\,\mathrm{GL}_2(\mathbb{Z}/p^r\mathbb{Z})| = (p^{r-1})^4(p^2-1)(p^2-p) = (p^{2r}-p^{2r-2})(p^{2r}-p^{2r-1})$.).

- Given a matrix $A \in \mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z})$, its coefficients are given by integers A_{ij} modulo p. We claim that the matrix $A' \in M_{k\times k}(\mathbb{Z}/p^r\mathbb{Z})$ given by the coefficients $A_{ij} \pmod{p^r}$ is invertible. This is because its determinant is coprime to p (since $A \in \mathrm{GL}_k(\mathbb{Z}/p\mathbb{Z})$), hence coprime to p^r. Since $A = f(A')$, this shows surjectivity of f.

- The kernel is easily seen to consists of all matrices

$$\begin{pmatrix} 1+pb_{11} & pb_{12} & \cdots & pb_{1n} \\ pb_{21} & 1+pb_{22} & \cdots & pb_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ pb_{n1} & \cdots & \cdots & 1+pb_{nn} \end{pmatrix} \tag{3.3.7}$$

  where $b_{ij} \in \mathbb{Z}/p^r\mathbb{Z}$. Those matrices are pairwise distinct provided that we take $b_{ij} \in \{0, ..., p^{r-1}-1\} \pmod{p^r}$. So there are $(p^{r-1})^{k^2}$ such matrices, as claimed.

Exercise 3.4

a) We simply find "KDXS M ATGI WTXILTCO".

Vigenère cipher is not vulnerable to frequency analysis, since a given letter (e.g. "E") in the plaintext can be ciphered to different letters (unless all the letters E have the same position modulo the length of the password in the plaintext).

b) There are two main steps to decipher the message, knowing that the Vigenère method was used. Firstly, we determine (i.e. make a guess) the length k of the keyword. Then we will guess what the key should be, using as few "brute-force method" as possible (keep in mind that if $k = 6$, the are already $26^6 \simeq 3 \cdot 10^8$ possible keys). We can make the assumption that the plaintext is in English ; however we prefer not making any assumption on the key (and even if we did, running over the k-letters words from the dictionary does not seem reasonable). Let us mention that the cipher text has 164 characters.

We give two methods to guess the length k. In part b), we use the index of coincidence. Namely, the following table summarizes the individual indices $\mathrm{CoInd}(s_i)$ (where $0 \leq i \leq k-1$) as well as the average index, for the different values of k that we tested,

Key length k	Average index	Individual indices CoInd(s_i)
1	0.045	0.045
2	0.043	0.042, 0.044
3	0.045	0.046, 0.048, 0.041
4	0.043	0.045, 0.037, 0.041, 0.051
5	0.039	0.032, 0.049, 0.035, 0.049, 0.028
6	0.039	0.044, 0.037, 0.042, 0.037, 0.045, 0.025
7	**0.076**	0.061, 0.050, 0.108, 0.043, 0.114, 0.075, 0.083
8	0.041	[...]
9	0.037	[...]
10	0.041	[...]
11	0.044	[...]
12	0.037	[...]
13	0.046	[...]
14	0.072	[...]

As we see from the table, the most likely length is $k = 7$, because the average index is the closest to the index for an English text which is ~ 0.068. Notice that $k = 14$ also gives a quite high average index, which is not surprising since 14 is a multiple of 7.

c) In part c), we can perform Kasiski test, probably also discovered by Charles Babbage. The following strings (on the first line) appear at several places (s_i, s_{i+1}) indexed by i (second line of the table), and the prime factorization of the difference of those indices is given in the third line.

String	(g,s)	(t,n)	(s,s)	(v,y)	(g,l)	(d, b)	(k,a)	(p,b)
i	84, 98, 111	36, 64	92, 162	66, 80	56, 158	118, 132	82, 96	38, 73, 154
Factorization of differences	$2 \cdot 7; 13$	$2^2 \cdot 7$	$2 \cdot 5 \cdot 7$	$2 \cdot 7$	$2 \cdot 3 \cdot 7$	$2 \cdot 7$	$2 \cdot 7$	$5 \cdot 7; 3^4$

Clearly, the factor 7 pops up quite frequently, so it confirms our previous guess about the length of the key, namely $k = 7$.

d) The strategy to discover the key $\beta := (\beta_0, ..., \beta_{k-1})$ is the following. For every $0 \leq j < i \leq k-1$, we seek $\gamma = \gamma_{i,j}$ such that the mutual coincidence index MutCoInd$(s_i, s_j + \gamma)$ is "high", i.e. close to 0.068. There might be several possible values of $\gamma_{i,j}$ that we should try, because the "correct value" $\gamma_{i,j} = \beta_i - \beta_j$ might not be the one for which MutCoInd$(s_i, s_j + \gamma)$ is maximal (e.g. it might be the second best or third best value).

For instance, when $(j, i) = (0, 1)$, we get the following table of MutCoInd$(s_1, s_0 + \gamma_{1,0})$ for the various values of $\gamma_{1,0}$:

$\gamma_{1,0}$	CoInd
0	0.03993
1	0.02778
2	0.03646
3	0.05035
4	0.03646
5	0.03819
6	0.03472
7	0.03819
8	0.03299
9	0.02604
10	0.03125
11	0.03125
12	0.06424

$\gamma_{1,0}$	CoInd
13	0.05035
14	0.04514
15	0.03125
16	0.02604
17	0.03819
18	0.04167
19	0.03819
20	0.03819
21	0.03819
22	0.03125
23	0.03646
24	0.04167
25	0.05556

Thus the maximal value is attained at $\gamma_{1,0} = 12$, but we also get a large value at $25, 13, 3$. Similarly, if $(j, i) = (0, 2)$, we can check that the maximal value of $\mathrm{MutCoInd}(s_2, s_0+\gamma_{2,0})$ is attained at $\gamma_{2,0} = 24$, but $11, 23$ also give high values.

For the various (i, j), we can thus collect the likely values of $\gamma_{i,j} = \beta_i - \beta_j$ (ordered by "likelihood", i.e. by decreasing values of $\mathrm{MutCoInd}(s_i, s_j + \gamma_{i,j}) > 0.05$) :

i	j	Possible $\gamma_{i,j}$
1	0	12, 25
2	0	24, 23, 11
3	0	7, 20
4	0	0, 12, 18
5	0	5, 9
6	0	12, 11, 25, 2
2	1	20, 21, 25
3	1	8, 4
4	1	13, 24, 6, 5
5	1	12, 17, 2
6	1	0, 25
3	2	9, 10
4	2	19, 14, 3
5	2	7, 23, 17
6	2	14, 5, 0
4	3	10, 6, 9
5	3	24
6	3	5, 17
5	4	4, 6, 7, 12
6	4	2, 12, 20, 13
6	5	16, 6

For instance, when $i = 5, j = 3$, then the value $\gamma = 24$ gives a mutual index of coincidence of 0.073, while the index is < 0.057 for the other values of γ, so we can make the guess that

$$\boxed{\gamma_{5,3} = \beta_5 - \beta_3 = 24.}$$

Now we can look for relations between the different $\gamma_{i,j}$, namely

$$\gamma_{i,j} = \beta_i - \beta_j = \beta_i - \beta_k - (\beta_j - \beta_k) = \gamma_{i,k} - \gamma_{j,k}.$$

For instance, according to our table, we should have $\gamma_{2,1} \in \{20, 21, 25\}$ should be equal to

$$\underbrace{\gamma_{2,0}}_{\in\{24,23,11\}} - \underbrace{\gamma_{1,0}}_{\in\{12,25\}}. \tag{3.4.1}$$

We see that $25 \equiv 24 - 25 \equiv 11 - 12 \pmod{26}$, while the values $\gamma_{2,1} = 21$ or 20 can't be written as a difference as 25 can. This leads us to the guess

$$\boxed{\gamma_{2,1} = \beta_2 - \beta_1 = 25.}$$

Continuing like this (heuristically and experimentally), we should have $\gamma_{5,2} - \gamma_{3,2} = \beta_5 - \beta_3 = 24 \equiv -2$, which gives the values

$$\boxed{\gamma_{5,2} = 7}$$

from the above table. Similarly, $\gamma_{5,0} - \gamma_{3,0} = \beta_5 - \beta_3 = 24 \equiv -2$ yields the guess

$$\boxed{\gamma_{5,0} = 5 \qquad \gamma_{3,0} = 7.}$$

Moreover, the relation $\gamma_{6,0} - \gamma_{6,1} = \gamma_{1,0}$ implies that $\boxed{\gamma_{6,1} = 0}$ according to the table, and $\gamma_{6,0} \in \{12, 25\}$.

Thus we got 6 independent equations involving the 7 unkowns $\beta_0, ..., \beta_6$.

e) It would be possible to perform a frequency analysis on each of the 7 blocks to get a further hint, and thus determine the β_i completely and uniquely.

Otherwise we can check, for every $\beta_0 \in \{0, ..., 25\}$, some values of $\gamma_{i,0}$ as in the table above. The correct values for $1 \leq i \leq 6$ happen to be $(25, 24, 7, 12, 5, 25)$. We have to be a bit lucky or clever while trying and guessing. But at the end, we are now in position to find the keyword, and hence the plaintext, which we let the reader discover!