University of Minnesota, School of Mathematics

Math 4281: Introduction to Modern Algebra, Spring 2019: Midterm 2

Darij Grinberg

March 4, 2021

1 Exercise 1: Not-quite-all-rationals

1.1 Problem

Fix an integer m. An *m-integer* shall mean a rational number r such that there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$.

For example[1]:

- Each integer r is an m-integer (since $m^k r \in \mathbb{Z}$ for $k = 0$).
- The rational number $\dfrac{5}{12}$ is a 6-integer (since $6^k \cdot \dfrac{5}{12} \in \mathbb{Z}$ for $k = 2$), but neither a 2-integer nor a 3-integer (since multiplying it by a power of 2 will not "get rid of" the prime factor 3 in the denominator, and vice versa[2]).
- The 1-integers are the integers (since $1^k r = r$ for all r).
- Every rational number r is a 0-integer (since $0^k r \in \mathbb{Z}$ for $k = 1$).

Let R_m denote the set of all m-integers. Prove the following:

[1] You don't need to prove these.

[2] You would have to be more rigorous than this in your solution, if you were to make an argument like this.

(a) The set R_m (endowed with the usual addition, the usual multiplication, the usual integer 0 as zero, and the usual integer 1 as unity) is a commutative ring.
(You don't need to prove axioms like commutativity of multiplication, since these follow from the corresponding facts about rational numbers, which are well-known. You only need to check that R_m is closed under addition and multiplication[3], and contains additive inverses of all its elements.)

(b) Let $x \in \mathbb{Q}$ be nonzero. Then, $x \in R_m$ if and only if every prime p satisfying $w_p(x) < 0$ satisfies $p \mid m$. Here, we are using the notation $w_p(r)$ defined in Exercise 3.4.1 of the class notes.

1.2 Remark

Roughly speaking, an m-integer is a rational number that can be turned into an integer by multiplying it with m several times. So a rational number, written as a reduced fraction, is an m-integer if and only if a sufficiently large power of m can cancel all the primes in its denominator.

The ring R_m is an example of a ring "between $\mathbb{Z}$ and $\mathbb{Q}$". It is commonly denoted by $\mathbb{Z}\left[\dfrac{1}{m}\right]$ and pronounced "$\mathbb{Z}$ adjoined 1 over m".

Note that $R_1 = \mathbb{Z}$ and $R_0 = \mathbb{Q}$, whereas $R_2 = R_4 = R_8 = \cdots$ is the ring of all rational numbers that can be written in the form $a/2^k$ with $a \in \mathbb{Z}$ and $k \in \mathbb{N}$.

The ring R_{10} is the ring of all *decimal fractions* – i.e., of all rational numbers that can be written in decimal notation with only finitely many digits after the comma.

1.3 Solution

For each rational number r, we have the following chain of logical equivalences:

$$\begin{aligned}(r \in R_m) &\iff (r \text{ is an } m\text{-integer}) \qquad (\text{since } R_m \text{ is the set of all } m\text{-integers}) \\ &\iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k r \in \mathbb{Z}\right) \qquad (1)\end{aligned}$$

(by the definition of an m-integer).

(a) We begin by proving the following claims:

Claim 1: We have $r \in R_m$ for each integer r.

Claim 2: If $a \in R_m$ and $b \in R_m$, then $a + b \in R_m$ and $a \cdot b \in R_m$.

Claim 3: If $a \in R_m$, then $-a \in R_m$.

[*Proof of Claim 1:* Let r be an integer. Then, $\underbrace{m^0}_{=1} r = r \in \mathbb{Z}$. Hence, there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$ (namely, $k = 0$). But (1) yields the equivalence

$$(r \in R_m) \iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k r \in \mathbb{Z}\right).$$

Hence, $r \in R_m$ (since there exists a $k \in \mathbb{N}$ satisfying $m^k r \in \mathbb{Z}$). This proves Claim 1.]

[*Proof of Claim 2:* Let $a \in R_m$ and $b \in R_m$. We must show that $a + b \in R_m$ and $a \cdot b \in R_m$.

[3] This means that every $a, b \in R_m$ satisfy $a + b \in R_m$ and $ab \in R_m$.

But (1) (applied to $r = a$) yields the equivalence

$$(a \in R_m) \iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k a \in \mathbb{Z}\right).$$

Hence, there exists a $k \in \mathbb{N}$ satisfying $m^k a \in \mathbb{Z}$ (since $a \in R_m$). Consider this k, and denote it by x. Thus, $x \in \mathbb{N}$ and $m^x a \in \mathbb{Z}$.

Furthermore, (1) (applied to $r = b$) yields the equivalence

$$(b \in R_m) \iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k b \in \mathbb{Z}\right).$$

Hence, there exists a $k \in \mathbb{N}$ satisfying $m^k b \in \mathbb{Z}$ (since $b \in R_m$). Consider this k, and denote it by y. Thus, $y \in \mathbb{N}$ and $m^y b \in \mathbb{Z}$.

Note that m^x is an integer (since m is an integer and $x \in \mathbb{N}$). In other words, $m^x \in \mathbb{Z}$. Similarly, $m^y \in \mathbb{Z}$.

Now,

$$\underbrace{m^{x+y}}_{=m^x m^y} (a+b) = m^x m^y (a+b) = m^x m^y a + m^x m^y b = \underbrace{m^y}_{\in \mathbb{Z}} \underbrace{m^x a}_{\in \mathbb{Z}} + \underbrace{m^x}_{\in \mathbb{Z}} \underbrace{m^y b}_{\in \mathbb{Z}} \in \mathbb{Z}.$$

Thus, there exists a $k \in \mathbb{N}$ satisfying $m^k (a+b) \in \mathbb{Z}$ (namely, $k = x + y$). (Note that with a little bit more work, we could have also shown this for $k = \max\{x, y\}$ instead of $k = x + y$; we were just being lazy.)

But (1) (applied to $r = a + b$) yields the equivalence

$$(a + b \in R_m) \iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k (a+b) \in \mathbb{Z}\right).$$

Hence, $a + b \in R_m$ (since there exists a $k \in \mathbb{N}$ satisfying $m^k (a+b) \in \mathbb{Z}$).

Furthermore,

$$\underbrace{m^{x+y}}_{=m^x m^y} (a \cdot b) = m^x m^y (a \cdot b) = \underbrace{m^x a}_{\in \mathbb{Z}} \underbrace{m^y b}_{\in \mathbb{Z}} \in \mathbb{Z}.$$

Thus, there exists a $k \in \mathbb{N}$ satisfying $m^k (a \cdot b) \in \mathbb{Z}$ (namely, $k = x + y$).

But (1) (applied to $r = a \cdot b$) yields the equivalence

$$(a \cdot b \in R_m) \iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k (a \cdot b) \in \mathbb{Z}\right).$$

Hence, $a \cdot b \in R_m$ (since there exists a $k \in \mathbb{N}$ satisfying $m^k (a \cdot b) \in \mathbb{Z}$).

We have now proven that $a + b \in R_m$ and $a \cdot b \in R_m$. This proves Claim 2.]

[*Proof of Claim 3:* Let $a \in R_m$. We shall show that $-a \in R_m$.

We could do this similarly to our proof of Claim 2, but let us take a shortcut instead: We have $-1 \in R_m$ (by Claim 1, applied to $r = -1$). Hence, Claim 2 (applied to $b = -1$) yields $a + (-1) \in R_m$ and $a \cdot (-1) \in R_m$. Now, $-a = a \cdot (-1) \in R_m$. This proves Claim 3.]

Now, consider the set R_m. We have $0 \in R_m$ (by Claim 1, applied to $r = 0$) and $1 \in R_m$ (by Claim 1, applied to $r = 1$). Thus, the set R_m contains the elements 0 and 1.

Furthermore, every $a \in R_m$ and $b \in R_m$ satisfy $a + b \in R_m$ (by Claim 2). Thus, we can define a binary operation $+$ on the set R_m by restricting the usual addition $+$ on $\mathbb{Q}$ to the subset R_m.

Moreover, every $a \in R_m$ and $b \in R_m$ satisfy $a \cdot b \in R_m$ (by Claim 2). Thus, we can define a binary operation $\cdot$ on the set R_m by restricting the usual multiplication $\cdot$ on $\mathbb{Q}$ to the subset R_m.

Now, the exercise demands us to prove that the set R_m equipped with these two binary operations $+$ and $\cdot$ and the two elements 0 and 1 is a commutative ring. In order to do so, we must verify that the ring axioms and the "Commutativity of multiplication" axiom are satisfied.

But all of these axioms, except for the "Existence of additive inverses" axiom, are clearly satisfied because they are satisfied for $\mathbb{Q}$ (and because our R_m is a subset of $\mathbb{Q}$, and because we endowed R_m with operations $+$ and $\cdot$ that are restrictions of the corresponding operations of $\mathbb{Q}$). It thus remains to prove that the "Existence of additive inverses" axiom is satisfied.

But this is easy: If $a \in R_m$, then $-a \in R_m$ (by Claim 3), and thus there exists an element $a' \in R_m$ satisfying $a + a' = a' + a = 0$ (namely, $a' = -a$).

Thus, we have proven that R_m is a commutative ring. This solves part **(a)** of the exercise.

(b) From (1) (applied to $r = x$), we obtain the logical equivalence

$$(x \in R_m) \iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k x \in \mathbb{Z}\right).$$

But Exercise 3.4.2 **(d)** in the class notes (applied to $r = x$) yields the logical equivalence

$$\begin{aligned} &\left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k x \in \mathbb{Z}\right) \\ \iff &\left(\text{every prime } p \text{ satisfying } w_p(x) < 0 \text{ satisfies } p \mid m\right). \end{aligned}$$

Hence, we have the following chain of equivalences:

$$\begin{aligned} (x \in R_m) &\iff \left(\text{there exists a } k \in \mathbb{N} \text{ satisfying } m^k x \in \mathbb{Z}\right) \\ &\iff \left(\text{every prime } p \text{ satisfying } w_p(x) < 0 \text{ satisfies } p \mid m\right). \end{aligned}$$

This solves part **(b)** of the exercise.

---

2 Exercise 2: Rings with $x^2 = x$

2.1 Problem

Let $\mathbb{K}$ be a ring with the property that

$$u^2 = u \qquad \text{for all } u \in \mathbb{K}. \tag{2}$$

(Examples of such rings are $\mathbb{Z}/2$ as well as the "power set" ring $(\mathcal{P}(S), \triangle, \cap, \varnothing, S)$ constructed from any given set S.)

Prove the following:

- **(a)** We have $2x = 0$ for each $x \in \mathbb{K}$.
- **(b)** We have $-x = x$ for each $x \in \mathbb{K}$.
- **(c)** We have $xy = yx$ for all $x, y \in \mathbb{K}$. (In other words, the ring $\mathbb{K}$ is commutative.)

(As usual, "0" stands for the zero of the ring $\mathbb{K}$.)

[**Hint:** For part **(a)**, apply (2) to $u = x$ but also to $u = 2x = x + x$, and see what comes out. For part **(c)**, apply (2) to $u = x + y$.]

2.2 Remark

Rings $\mathbb{K}$ satisfying (2) are known as *Boolean rings* (although some people do not require them to have a unity). Thus, the exercise proves various properties of Boolean rings, including the fact that they are always commutative.

You might wonder what happens if we replace (2) by the requirement that

$$u^3 = u \qquad \text{for all } u \in \mathbb{K}. \tag{3}$$

This no longer leads to $2x = 0$ (nor to $3x = 0$ as you might perhaps expect). Instead, it can be shown that $6x = 0$ for all $x \in \mathbb{K}$. It can also be shown that it leads to $xy = yx$. See, for example, `https://math.stackexchange.com/questions/67148` .

More generally, fix an integer $n \geq 2$, and replace (2) by the requirement that

$$u^n = u \qquad \text{for all } u \in \mathbb{K}. \tag{4}$$

Then, it still can be proven that $\mathbb{K}$ is commutative! See `https://mathoverflow.net/questions/29590/` for this result.

Even more generally, we don't need to fix n in advance! In other words, instead of requiring (2) or (3) or (4), we merely require that for each $u \in \mathbb{K}$, there exists an integer $n \geq 2$ (which may depend on u) such that $u^n = u$. This is a more general setting; nevertheless it still follows that $\mathbb{K}$ is commutative! This is a result of Jacobson; see [Rogers71] for a proof.

2.3 Solution

(a) *First solution to part **(a)**:* Let $x \in \mathbb{K}$. Then, (2) (applied to $u = x$) yields $x^2 = x$. But (2) (applied to $u = x + x$) yields $(x+x)^2 = x + x = 2x$. Thus,

$$\begin{aligned} 2x &= x + x = (x+x)^2 = (x+x)(x+x) \\ &= \underbrace{x(x+x)}_{\substack{=xx+xx \\ \text{(by distributivity)}}} + \underbrace{x(x+x)}_{\substack{=xx+xx \\ \text{(by distributivity)}}} \qquad \text{(by distributivity)} \\ &= xx + xx + xx + xx = 4\underbrace{xx}_{=x^2=x} = 4x. \end{aligned}$$

Subtracting $2x$ from both sides of this equality, we obtain $0 = 4x - 2x = 2x$. Hence, $2x = 0$. This solves part **(a)** of the exercise.

*Second solution to part **(a)**:* Let $x \in \mathbb{K}$. Then, (2) (applied to $u = x$) yields $x^2 = x$. But (2) (applied to $u = -x$) yields $(-x)^2 = -x$. Hence,

$$-x = (-x)^2 = (-x)(-x) = -\underbrace{(x \cdot (-x))}_{=-(xx)} = -(-(xx)) = xx = x^2 = x.$$

Adding x to both sides of this equality, we find $(-x) + x = x + x = 2x$. Thus, $2x = (-x) + x = 0$. This solves part **(a)** of the exercise.

(b) *First solution to part **(b)**:* Let $x \in \mathbb{K}$. Part **(a)** of this exercise yields $2x = 0$. Subtracting x from both sides of this equality, we obtain $2x - x = 0 - x = -x$. Hence, $-x = \underbrace{2x}_{=x+x} - x = (x+x) - x = x$. This solves part **(b)** of this exercise.

*Second solution to part **(b)**:* Let $x \in \mathbb{K}$. We have already shown the equality $-x = x$ in our Second solution to part **(a)**. Thus, part **(b)** of the exercise is solved.

(c) Let $x, y \in \mathbb{K}$. Then, (2) (applied to $u = x$) yields $x^2 = x$. Also, (2) (applied to $u = y$) yields $y^2 = y$. But (2) (applied to $u = x + y$) yields $(x+y)^2 = x + y$. Hence,

$$\begin{aligned} x + y &= (x+y)^2 = (x+y)(x+y) \\ &= \underbrace{x(x+y)}_{\substack{=xx+xy \\ \text{(by distributivity)}}} + \underbrace{y(x+y)}_{\substack{=yx+yy \\ \text{(by distributivity)}}} \qquad \text{(by distributivity)} \\ &= \underbrace{xx}_{=x^2=x} + xy + yx + \underbrace{yy}_{=y^2=y} = x + xy + yx + y. \end{aligned}$$

Subtracting $x + y$ from both sides of this equality, we obtain

$$0 = (x + xy + yx + y) - (x + y) = xy + yx.$$

Thus, $xy = -yx$. But part **(b)** of this exercise (applied to yx instead of x) yields $-yx = yx$. Hence, $xy = -yx = yx$. This solves part **(c)** of the exercise.

3 Exercise 3: A matrix of gcds

3.1 Problem

In this exercise, we shall again use the *Iverson bracket notation*:

Let $n \in \mathbb{N}$. Let G be the $n \times n$-matrix

$$(\gcd(i,j))_{1 \le i \le n,\ 1 \le j \le n} = \begin{pmatrix} \gcd(1,1) & \gcd(1,2) & \cdots & \gcd(1,n) \\ \gcd(2,1) & \gcd(2,2) & \cdots & \gcd(2,n) \\ \vdots & \vdots & \ddots & \vdots \\ \gcd(n,1) & \gcd(n,2) & \cdots & \gcd(n,n) \end{pmatrix}.$$

Let L be the $n \times n$-matrix

$$([j \mid i])_{1 \le i \le n,\ 1 \le j \le n} = \begin{pmatrix} [1 \mid 1] & [2 \mid 1] & \cdots & [n \mid 1] \\ [1 \mid 2] & [2 \mid 2] & \cdots & [n \mid 2] \\ \vdots & \vdots & \ddots & \vdots \\ [1 \mid n] & [2 \mid n] & \cdots & [n \mid n] \end{pmatrix}.$$

Let D be the $n \times n$-matrix

$$([i = j]\, \phi(i))_{1 \le i \le n,\ 1 \le j \le n} = \begin{pmatrix} \phi(1) & 0 & 0 & \cdots & 0 \\ 0 & \phi(2) & 0 & \cdots & 0 \\ 0 & 0 & \phi(3) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \phi(n) \end{pmatrix}.$$

Prove that[4] $G = LDL^T$.

[4] We are using the standard notation A^T for the *transpose* of a matrix A. This transpose is defined as follows: If $A = (a_{i,j})_{1 \le i \le n,\ 1 \le j \le m}$, then $A^T = (a_{j,i})_{1 \le i \le m,\ 1 \le j \le n}$.

3.2 Remark

As the names suggest, the matrix L is lower-triangular[5] (so that the matrix L^T is upper-triangular), and the matrix D is diagonal. Thus, $G = LDL^T$ is an instance of an *LDU decomposition*.

The matrix G is an example of what is called a *gcd-matrix* (duh); see, e.g., `https://math.stackexchange.com/questions/1278871` for some references on it.

3.3 Solution

We recall the following fundamental property of matrices in general:

Lemma 3.1. *Let $n, m \in \mathbb{N}$. Let $\mathbb{K}$ be a ring. Let $\mathbf{D} = ([i = j]\, d_i)_{1 \leq i \leq n,\ 1 \leq j \leq n}$ be a diagonal matrix over $\mathbb{K}$ (where $d_1, d_2, \ldots, d_n$ are n elements of $\mathbb{K}$). Let $\mathbf{A} = (a_{i,j})_{1 \leq i \leq n,\ 1 \leq j \leq m}$ be an arbitrary $n \times m$-matrix over $\mathbb{K}$. Then, the product $\mathbf{DA}$ is simply given by*

$$\mathbf{DA} = (d_i a_{i,j})_{1 \leq i \leq n,\ 1 \leq j \leq m} . \tag{5}$$

(That is, multiplying a matrix $\mathbf{A}$ by a diagonal matrix $\mathbf{D}$ on the left is tantamount to rescaling each row of $\mathbf{A}$ by the corresponding diagonal entry of $\mathbf{D}$.)

Proof of Lemma 3.1. We have $\mathbf{D} = ([i = j]\, d_i)_{1 \leq i \leq n,\ 1 \leq j \leq n}$ and $\mathbf{A} = (a_{i,j})_{1 \leq i \leq n,\ 1 \leq j \leq m}$. Hence, the definition of the product of two matrices yields

$$\mathbf{DA} = \left(\sum_{k=1}^{n} [i = k]\, d_i a_{k,j} \right)_{1 \leq i \leq n,\ 1 \leq j \leq m} . \tag{6}$$

Now, fix some $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$. Then,

$$\sum_{k=1}^{n} [i = k]\, d_i a_{k,j} = \sum_{k \in \{1,2,\ldots,n\}} [i = k]\, d_i a_{k,j} = \underbrace{[i = i]}_{\substack{=1 \\ (\text{since } i=i)}} d_i a_{i,j} + \sum_{\substack{k \in \{1,2,\ldots,n\}; \\ k \neq i}} \underbrace{[i = k]}_{\substack{=0 \\ (\text{since } i \neq k \\ (\text{because } k \neq i))}} d_i a_{k,j}$$

$$\text{(here, we have split off the addend for } k = i \text{ from the sum)}$$

$$= d_i a_{i,j} + \underbrace{\sum_{\substack{k \in \{1,2,\ldots,n\}; \\ k \neq i}} 0 d_i a_{k,j}}_{=0} = d_i a_{i,j} .$$

Now, forget that we fixed i and j. We thus have shown that $\sum_{k=1}^{n} [i = k]\, d_i a_{k,j} = d_i a_{i,j}$ for all $i \in \{1, 2, \ldots, n\}$ and $j \in \{1, 2, \ldots, m\}$. Therefore, the equality (6) rewrites as $\mathbf{DA} = (d_i a_{i,j})_{1 \leq i \leq n,\ 1 \leq j \leq m}$. This proves Lemma 3.1. □

Now, let us return to solving the exercise.

Recall that $L = ([j \mid i])_{1 \leq i \leq n,\ 1 \leq j \leq n}$; thus, the definition of the transpose of a matrix yields $L^T = ([i \mid j])_{1 \leq i \leq n,\ 1 \leq j \leq n}$. Also, recall that $D = ([i = j]\, \phi(i))_{1 \leq i \leq n,\ 1 \leq j \leq n}$. Hence, (5) (applied to $\mathbb{K} = \mathbb{Z}$, $m = n$, $d_i = \phi(i)$, $\mathbf{D} = D$, $a_{i,j} = [i \mid j]$ and $\mathbf{A} = L^T$) yields

$$DL^T = (\phi(i) \cdot [i \mid j])_{1 \leq i \leq n,\ 1 \leq j \leq n} . \tag{7}$$

[5] because two positive integers i and j satisfying $i < j$ always satisfy $[j \mid i] = 0$

Now, we have $L = ([j \mid i])_{1\leq i\leq n,\ 1\leq j\leq n}$ and $DL^T = (\phi(i) \cdot [i \mid j])_{1\leq i\leq n,\ 1\leq j\leq n}$. Thus, the definition of the product of two matrices yields

$$L\left(DL^T\right) = \left(\sum_{k=1}^{n} [k \mid i] \cdot \phi(k) \cdot [k \mid j]\right)_{1\leq i\leq n,\ 1\leq j\leq n}. \tag{8}$$

Let us now recall a basic property of the Iverson bracket: If $\mathcal{A}$ and $\mathcal{B}$ are two logical statements, then

$$[\mathcal{A} \wedge \mathcal{B}] = [\mathcal{A}] \cdot [\mathcal{B}]. \tag{9}$$

Furthermore, if $\mathcal{A}$ and $\mathcal{B}$ are two equivalent logical statements, then

$$[\mathcal{A}] = [\mathcal{B}]. \tag{10}$$

Now, fix $i, j \in \{1, 2, \ldots, n\}$. Hence, i and j are positive integers; thus, $\gcd(i,j)$ is a positive integer as well. Also, $\gcd(i,j) \mid i$, so that $\gcd(i,j) \leq i$ (since $\gcd(i,j)$ and i are positive integers) and therefore $\gcd(i,j) \leq i \leq n$ (since $i \in \{1, 2, \ldots, n\}$).

Theorem 2.14.6 in the class notes (applied to $\gcd(i,j)$ instead of n) yields

$$\sum_{d\mid\gcd(i,j)} \phi(d) = \gcd(i,j). \tag{11}$$

Here, the summation sign "$\sum_{d\mid\gcd(i,j)}$" means a sum over all positive divisors d of $\gcd(i,j)$.

Also, fix $k \in \{1, 2, \ldots, n\}$. Then, Theorem 2.9.15 **(a)** in the class notes (applied to k, i and j instead of a, b and m) shows that we have the following logical equivalence:

$$(k \mid i \text{ and } k \mid j) \Longleftrightarrow (k \mid \gcd(i,j)).$$

Thus, the logical statements $(k \mid \gcd(i,j))$ and $(k \mid i \text{ and } k \mid j)$ are equivalent. Hence, (10) (applied to $\mathcal{A} = (k \mid \gcd(i,j))$ and $\mathcal{B} = (k \mid i \text{ and } k \mid j)$) yields

$$\begin{aligned}[k \mid \gcd(i,j)] &= [k \mid i \text{ and } k \mid j] = [(k \mid i) \wedge (k \mid j)] \\ &= [k \mid i] \cdot [k \mid j] \end{aligned} \tag{12}$$

(by (9), applied to $\mathcal{A} = (k \mid i)$ and $\mathcal{B} = (k \mid j)$).

Now, forget that we fixed k. We thus have proven (12) for each $k \in \{1, 2, \ldots, n\}$. Now,

$$\begin{aligned}
&\sum_{k=1}^{n} [k \mid i] \cdot \phi(k) \cdot [k \mid j] \\
&= \underbrace{\sum_{k=1}^{n}}_{= \sum_{k \in \{1,2,\ldots,n\}}} \underbrace{[k \mid i] \cdot [k \mid j]}_{\substack{=[k \mid \gcd(i,j)] \\ (\text{by } (12))}} \cdot \phi(k) = \sum_{k \in \{1,2,\ldots,n\}} [k \mid \gcd(i,j)] \cdot \phi(k) \\
&= \sum_{\substack{k \in \{1,2,\ldots,n\}; \\ k \mid \gcd(i,j)}} \underbrace{[k \mid \gcd(i,j)]}_{\substack{=1 \\ (\text{since } k \mid \gcd(i,j))}} \cdot \phi(k) + \sum_{\substack{k \in \{1,2,\ldots,n\}; \\ k \nmid \gcd(i,j)}} \underbrace{[k \mid \gcd(i,j)]}_{\substack{=0 \\ (\text{since } k \nmid \gcd(i,j))}} \cdot \phi(k) \\
&\qquad \left(\begin{array}{c} \text{since each } k \in \{1, 2, \ldots, n\} \text{ satisfies either } k \mid \gcd(i,j) \\ \text{or } k \nmid \gcd(i,j) \text{ (but not both)} \end{array} \right) \\
&= \sum_{\substack{k \in \{1,2,\ldots,n\}; \\ k \mid \gcd(i,j)}} \phi(k) + \underbrace{\sum_{\substack{k \in \{1,2,\ldots,n\}; \\ k \nmid \gcd(i,j)}} 0 \cdot \phi(k)}_{=0} = \sum_{\substack{k \in \{1,2,\ldots,n\}; \\ k \mid \gcd(i,j)}} \phi(k) \\
&= \sum_{\substack{d \in \{1,2,\ldots,n\}; \\ d \mid \gcd(i,j)}} \phi(d) \qquad (13)
\end{aligned}$$

(here, we have renamed the summation index k as d).

But each positive divisor of $\gcd(i,j)$ is $\leq \gcd(i,j)$ and therefore $\leq n$ (since $\gcd(i,j) \leq n$). Thus, each positive divisor of $\gcd(i,j)$ belongs to the set $\{1, 2, \ldots, n\}$. Hence, each positive divisor of $\gcd(i,j)$ is a $d \in \{1, 2, \ldots, n\}$ satisfying $d \mid \gcd(i,j)$. In other words,

$$\{\text{positive divisors of } \gcd(i,j)\} \subseteq \{d \in \{1, 2, \ldots, n\} \text{ such that } d \mid \gcd(i,j)\}.$$

Combining this with the relation

$$\{d \in \{1, 2, \ldots, n\} \text{ such that } d \mid \gcd(i,j)\} \subseteq \{\text{positive divisors of } \gcd(i,j)\}$$

(which is obvious), we obtain

$$\{d \in \{1, 2, \ldots, n\} \text{ such that } d \mid \gcd(i,j)\} = \{\text{positive divisors of } \gcd(i,j)\}.$$

Thus, the summation sign "$\sum_{\substack{d \in \{1,2,\ldots,n\}; \\ d \mid \gcd(i,j)}}$" is equivalent to "$\sum_{d \mid \gcd(i,j)}$" (since the latter summation sign means a sum over all positive divisors of $\gcd(i,j)$). Hence, (13) becomes

$$\sum_{k=1}^{n} [k \mid i] \cdot \phi(k) \cdot [k \mid j] = \underbrace{\sum_{\substack{d \in \{1,2,\ldots,n\}; \\ d \mid \gcd(i,j)}}}_{= \sum_{d \mid \gcd(i,j)}} \phi(d) = \sum_{d \mid \gcd(i,j)} \phi(d) = \gcd(i,j) \qquad (\text{by } (11)).$$

Now, forget that we fixed i, j. We thus have proven that

$$\sum_{k=1}^{n} [k \mid i] \cdot \phi(k) \cdot [k \mid j] = \gcd(i,j) \qquad \text{for all } i, j \in \{1, 2, \ldots, n\}.$$

In other words,

$$\left(\sum_{k=1}^{n}[k \mid i]\cdot\phi(k)\cdot[k \mid j]\right)_{1\leq i\leq n,\ 1\leq j\leq n} = (\gcd(i,j))_{1\leq i\leq n,\ 1\leq j\leq n}.$$

Hence, (8) becomes

$$L\left(DL^T\right) = \left(\sum_{k=1}^{n}[k \mid i]\cdot\phi(k)\cdot[k \mid j]\right)_{1\leq i\leq n,\ 1\leq j\leq n} = (\gcd(i,j))_{1\leq i\leq n,\ 1\leq j\leq n} = G$$

(by the definition of G). Consequently, $G = L\left(DL^T\right) = LDL^T$. The exercise is now solved.

3.4 Remark

If you know about determinants, you will easily see how to compute $\det G$ using the claim of the exercise. (**Hint:** Use the formula $\det(AB) = \det A \cdot \det B$ that holds for any two $n \times n$-matrices A and B over any commutative ring $\mathbb{K}$.)

4 Exercise 4: Idempotent and involutive elements

4.1 Problem

Let $\mathbb{K}$ be a ring.

An element a of $\mathbb{K}$ is said to be *idempotent* if it satisfies $a^2 = a$.

An element a of $\mathbb{K}$ is said to be *involutive* if it satisfies $a^2 = 1$.

(a) Let $a \in \mathbb{K}$. Prove that if a is idempotent, then $1 - 2a$ is involutive.

(b) Now, assume that 2 is *cancellable* in $\mathbb{K}$; this means that if u and v are two elements of $\mathbb{K}$ satisfying $2u = 2v$, then $u = v$. Prove that the converse of the claim of part **(a)** holds: If $a \in \mathbb{K}$ is such that $1 - 2a$ is involutive, then a is idempotent.

(c) Now, let $\mathbb{K} = \mathbb{Z}/4$. Find an element $a \in \mathbb{K}$ such that $1 - 2a$ is involutive, but a is not idempotent.

4.2 Remark

The idempotent elements of $\mathbb{R}$ are 0 and 1. The involutive elements of $\mathbb{R}$ are 1 and -1. A matrix ring like $\mathbb{R}^{n\times n}$ usually has infinitely many idempotent elements (viz., all projection matrices on subspaces of $\mathbb{R}^n$) and infinitely many involutive elements (viz., all matrices A satisfying $A^2 = I_n$; for instance, all reflections across hyperplanes are represented by such matrices).

Part **(a)** of this exercise assigns an involutive element to each idempotent element of $\mathbb{K}$. If 2 is invertible in $\mathbb{K}$ (that is, if the element $2 \cdot 1_{\mathbb{K}}$ has a multiplicative inverse), then this assignment is a bijection (as can be easily derived from part **(b)**). Part **(c)** shows that we cannot drop the "2 is cancellable" condition in part **(b)**.

4.3 Solution

Using the ring axioms and the basic rules for rings, it is easy to see that every $a \in \mathbb{K}$ satisfies

$$(1-2a)^2 = 1 - 4a + 4a^2. \tag{14}$$

[Here is a more pedantic *proof* of this fact: Let $a \in \mathbb{K}$. For any $b \in \mathbb{K}$, we have

$$\begin{aligned}(1+b)^2 &= (1+b)(1+b) = \underbrace{1(1+b)}_{=1+b} + \underbrace{b(1+b)}_{\substack{=b\cdot 1+b\cdot b\\ \text{(by distributivity)}}} \qquad \text{(by distributivity)}\\ &= 1 + b + \underbrace{b\cdot 1}_{=b} + \underbrace{b\cdot b}_{=b^2} = 1 + b + b + b^2 = 1 + 2b + b^2.\end{aligned}$$

Applying this to $b = -2a$, we obtain

$$\begin{aligned}(1+(-2a))^2 &= 1 + \underbrace{2(-2a)}_{=2\cdot(-2)a} + \underbrace{(-2a)^2}_{\substack{=(-2a)\cdot(-2a)\\ =(-2)\cdot(-2a)\cdot a}} = 1 + \underbrace{2\cdot(-2)}_{=-4}a + (-2)\cdot\underbrace{(-2a)}_{=(-2)a}\cdot a\\ &= 1 + \underbrace{(-4)\,a}_{=-4a} + \underbrace{(-2)\cdot((-2)\,a)}_{=((-2)\cdot(-2))\cdot a}\cdot a = \underbrace{1+(-4a)}_{=1-4a} + \underbrace{((-2)\cdot(-2))}_{=4}\cdot\underbrace{a\cdot a}_{=a^2}\\ &= 1 - 4a + 4a^2.\end{aligned}$$

In view of $1 + (-2a) = 1 - 2a$, this rewrites as $(1-2a)^2 = 1 - 4a + 4a^2$. Thus, (14) is proven.]

(a) Assume that a is idempotent. We must prove that $1 - 2a$ is involutive.

We have assumed that a is idempotent. In other words, $a^2 = a$ (by the definition of "idempotent"). Thus, (14) becomes $(1-2a)^2 = 1 - 4a + 4\underbrace{a^2}_{=a} = 1 - 4a + 4a = 1$. In other words, $1 - 2a$ is involutive (by the definition of "involutive"). This solves part **(a)** of the exercise.

(b) Let $a \in \mathbb{K}$ be such that $1 - 2a$ is involutive. We must prove that a is idempotent.

We know that 2 is cancellable in $\mathbb{K}$. In other words, if u and v are two elements of $\mathbb{K}$ satisfying $2u = 2v$, then

$$u = v. \tag{15}$$

We have assumed that $1 - 2a$ is involutive. In other words, $(1-2a)^2 = 1$. Comparing this with (14), we obtain $1 - 4a + 4a^2 = 1$. Hence, $4a^2 = 1 - 1 + 4a = 4a$. This rewrites as $2 \cdot 2a^2 = 2 \cdot 2a$ (since $\underbrace{2\cdot 2}_{=4}a^2 = 4a^2$ and $\underbrace{2\cdot 2}_{=4}a = 4a$). Hence, (15) (applied to $u = 2a^2$ and $v = 2a$) yields $2a^2 = 2a$. Thus, (15) (applied to $u = a^2$ and $v = a$) yields $a^2 = a$. In other words, a is idempotent. This solves part **(b)** of the exercise.

(c) We claim that $a = [2]_4$ is such an element. Indeed, $1 - 2\cdot[2]_4$ is involutive[6] (since $\underbrace{1}_{=[1]_4} - \underbrace{2\cdot[2]_4}_{=[2\cdot 2]_4=[4]_4=[0]_4} = [1]_4 - [0]_4 = [1]_4$ and thus $(1 - 2\cdot[2]_4)^2 = ([1]_4)^2 = [1^2]_4 = [1]_4 = 1$), but $[2]_4$ is not idempotent (since $([2]_4)^2 = [2^2]_4 = [4]_4 \neq [2]_4$).

[6] Keep in mind that the "1" here stands for the unity of the ring $\mathbb{K} = \mathbb{Z}/4$; this is the residue class $[1]_4$.

5 Exercise 5: The matrix approach to Fibonacci numbers

5.1 Problem

Let A be the 2×2-matrix $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ over $\mathbb{Z}$. Consider also the identity matrix $I_2 \in \mathbb{Z}^{2\times 2}$.

Let $\mathcal{F}$ be the subset

$$\{aA + bI_2 \mid a, b \in \mathbb{Z}\} = \left\{ \begin{pmatrix} b & a \\ a & a+b \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$$

of the matrix ring $\mathbb{Z}^{2\times 2}$.

(a) Prove that $A^2 = A + I_2$.

(b) Prove that the set $\mathcal{F}$ (equipped with the addition of matrices, the multiplication of matrices, the zero $0_{2\times 2}$ and the unity I_2) is a commutative ring.
(Again, you don't need to check the ring axioms, as we already know that they hold for arbitrary matrices and thus all the more for matrices in $\mathcal{F}$. But you do need to check commutativity of multiplication in $\mathcal{F}$, since it does not hold for arbitrary matrices. You also need to check that $\mathcal{F}$ is closed under addition and multiplication and has additive inverses.)

Let $(f_0, f_1, f_2, \ldots)$ be the Fibonacci sequence (which we have already encountered on homework set #5). Recall that it is defined recursively by

$$f_0 = 0, \qquad f_1 = 1, \qquad \text{and} \qquad f_n = f_{n-1} + f_{n-2} \text{ for all } n \geq 2.$$

(c) Prove that $A^n = f_n A + f_{n-1} I_2$ for all positive integers n.

(d) Prove that $f_{n+m} = f_n f_{m+1} + f_{n-1} f_m$ for all positive integers n and all $m \in \mathbb{N}$.

Now, define a further matrix $B \in \mathcal{F}$ by $B = (-1)\,A + 1 I_2 = I_2 - A$.

(e) Prove that $B^2 = B + I_2$ and $B^n = f_n B + f_{n-1} I_2$ for all positive integers n.

(f) Prove that $A^n - B^n = f_n\,(A - B)$ for all $n \in \mathbb{N}$.

(g) Prove (again!) that $f_d \mid f_{dn}$ for any nonnegative integers d and n.

[**Hint:** One way to prove **(d)** is by comparing the $(1,1)$-th entries of the two (equal) matrices $A^n A^{m+1}$ and A^{n+m+1}, after first using part **(c)** to expand these matrices.

For part **(g)**, compare the $(1,1)$-th entries of the matrices $A^d - B^d$ and $A^{dn} - B^{dn}$, after first proving that $A^d - B^d \mid A^{dn} - B^{dn}$ in the commutative ring $\mathcal{F}$. Note that divisibility is a tricky concept in general rings, but $\mathcal{F}$ is a commutative ring, which lets many arguments from the integer setting go through unchanged.]

5.2 Remark

Contrast the ring $\mathcal{F}$ with the ring $\mathbb{Z}[\phi]$ from Exercise 5 on homework set #5. Both of these rings, as we see, can be used to prove that $f_d \mid f_{dn}$ for any nonnegative integers d and n. It turns out that these rings have more in common: they are isomorphic! More precisely, the map

$$\begin{aligned} &\mathbb{Z}[\phi] \to \mathcal{F}, \\ &a + b\phi \mapsto bA + aI_2 \qquad (\text{for } a, b \in \mathbb{Z}) \end{aligned}$$

is a ring isomorphism. This makes it less surprising that these rings can substitute for one another in proving $f_d \mid f_{dn}$.

5.3 Solution sketch

We first recall that $\mathcal{F} = \{aA + bI_2 \mid a, b \in \mathbb{Z}\}$ (by the definition of $\mathcal{F}$). Hence,

$$aA + bI_2 \in \mathcal{F} \qquad \text{for all } a, b \in \mathbb{Z}. \tag{16}$$

(a) This is an easy exercise in multiplying matrices: From $A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, we obtain

$$A^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Comparing this with

$$\underbrace{A}_{=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}} + \underbrace{I_2}_{=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

we obtain $A^2 = A + I_2$. This solves part **(a)** of the exercise.

(b) Let us show the following claims:

Claim 1: We have $0_{2\times 2} \in \mathcal{F}$.

Claim 2: We have $I_2 \in \mathcal{F}$.

Claim 3: For any $U, V \in \mathcal{F}$, we have $U + V \in \mathcal{F}$ and $UV \in \mathcal{F}$ and $UV = VU$.

Claim 4: For any $U \in \mathcal{F}$, we have $-U \in \mathcal{F}$.

[*Proof of Claim 1:* We have $\underbrace{0A}_{=0_{2\times 2}} + \underbrace{0I_2}_{=0_{2\times 2}} = 0_{2\times 2}$, so that $0_{2\times 2} = 0A + 0I_2 \in \mathcal{F}$ (by (16), applied to $a = 0$ and $b = 0$). This proves Claim 1.]

[*Proof of Claim 2:* We have $\underbrace{0A}_{=0_{2\times 2}} + \underbrace{1I_2}_{=I_2} = I_2$, so that $I_2 = 0A + 1I_2 \in \mathcal{F}$ (by (16), applied to $a = 0$ and $b = 1$). This proves Claim 2.]

[*Proof of Claim 3:* Let $U, V \in \mathcal{F}$. We must prove that $U + V \in \mathcal{F}$ and $UV \in \mathcal{F}$ and $UV = VU$.

We have $V \in \mathcal{F} = \{aA + bI_2 \mid a, b \in \mathbb{Z}\} = \{cA + dI_2 \mid c, d \in \mathbb{Z}\}$ (here, we have renamed the indices a and b as c and d). In other words, there exist some $c, d \in \mathbb{Z}$ such that $V = cA + dI_2$. Consider these c, d.

We have $U \in \mathcal{F} = \{aA + bI_2 \mid a, b \in \mathbb{Z}\}$. In other words, there exist some $a, b \in \mathbb{Z}$ such that $U = aA + bI_2$. Consider these a, b.

From $a, b, c, d \in \mathbb{Z}$, we obtain $a + c \in \mathbb{Z}$ and $b + d \in \mathbb{Z}$ and $ad + bc + ac \in \mathbb{Z}$ and $ac + bd \in \mathbb{Z}$.

We have $a, b, c, d \in \mathbb{Z}$. Adding the equalities $U = aA + bI_2$ and $V = cA + dI_2$ together, we obtain

$$U + V = (aA + bI_2) + (cA + dI_2) = (a + c) A + (b + d) I_2 \in \mathcal{F}$$

(by (16), applied to $a + c$ and $b + d$ instead of a and b).

We have $AA = A^2 = A + I_2$ (by part **(a)** of the exercise).

Multiplying the equalities $U = aA + bI_2$ and $V = cA + dI_2$ together, we obtain

$$\begin{aligned} UV &= (aA + bI_2)(cA + dI_2) = ac \underbrace{AA}_{=A+I_2} + ad \underbrace{AI_2}_{=A} + bc \underbrace{I_2A}_{=A} + bd \underbrace{I_2I_2}_{=I_2} \\ &= ac (A + I_2) + adA + bcA + bdI_2 = (ad + bc + ac) A + (ac + bd) I_2 \in \mathcal{F} \end{aligned}$$

(by (16), applied to $ad + bc + ac$ and $ac + bd$ instead of a and b).

Multiplying the equalities $V = cA + dI_2$ and $U = aA + bI_2$ together, we obtain

$$\begin{aligned} VU &= (cA + dI_2)(aA + bI_2) = \underbrace{ca}_{=ac} \underbrace{AA}_{=A+I_2} + \underbrace{cb}_{=bc} \underbrace{AI_2}_{=A} + \underbrace{da}_{=ad} \underbrace{I_2A}_{=A} + \underbrace{db}_{=bd} \underbrace{I_2I_2}_{=I_2} \\ &= ac (A + I_2) + bcA + adA + bdI_2 = (ad + bc + ac) A + (ac + bd) I_2. \end{aligned}$$

Comparing this equality with $UV = (ad + bc + ac) A + (ac + bd) I_2$, we obtain $UV = VU$.

Thus, we have proven that $U + V \in \mathcal{F}$ and $UV \in \mathcal{F}$ and $UV = VU$. This proves Claim 3.]

[*Proof of Claim 4:* Let $U \in \mathcal{F}$. We have $U \in \mathcal{F} = \{aA + bI_2 \mid a, b \in \mathbb{Z}\}$. In other words, there exist some $a, b \in \mathbb{Z}$ such that $U = aA + bI_2$. Consider these a, b. Hence,

$$-\underbrace{U}_{=aA+bI_2} = -(aA + bI_2) = (-a) A + (-b) I_2 \in \mathcal{F}$$

(by (16), applied to $-a$ and $-b$ instead of a and b). This proves Claim 4.]

Let us now resume solving part **(b)** of the exercise. Claim 3 shows that for every $U, V \in \mathcal{F}$, we have $U + V \in \mathcal{F}$. Thus, addition of matrices defines a binary operation $+$ on $\mathcal{F}$. Furthermore, Claim 3 shows that for every $U, V \in \mathcal{F}$, we have $UV \in \mathcal{F}$. Thus, multiplication of matrices defines a binary operation $\cdot$ on $\mathcal{F}$. Furthermore, $0_{2\times 2} \in \mathcal{F}$ (by Claim 1) and $I_2 \in \mathcal{F}$ (by Claim 2). Hence, we can endow the set $\mathcal{F}$ with the binary operation $+$ (as addition), the binary operation $\cdot$ (as multiplication), the element $0_{2\times 2}$ (as zero) and the element I_2 (as unity). Now, we must prove that the result is a commutative ring.

Indeed, let us first prove that $\mathcal{F}$ is a ring. To that end, we shall check all the ring axioms:

- The "Existence of additive inverses" axiom is satisfied, because for every $U \in \mathcal{F}$, there exists an $U' \in \mathcal{F}$ such that $U + U' = U' + U = 0_{2\times 2}$. (Namely, we can set $U' = -U$, which is an element of $\mathcal{F}$ because of Claim 4.)

- All the remaining ring axioms are satisfied, since they are particular cases of the rules for addition and multiplication of matrices. (For example, associativity of multiplication holds in $\mathcal{F}$ because it holds for arbitrary matrices.)

Thus, $\mathcal{F}$ is a ring. Furthermore, every $U, V \in \mathcal{F}$ satisfy $UV = VU$ (by Claim 3). Hence, the ring $\mathcal{F}$ is commutative. This solves part **(b)** of the exercise.

(c) We shall solve part **(c)** of the exercise by induction on n:

Induction base: We have $A^1 = f_1 A + f_{1-1} I_2$ (since $\underbrace{f_1}_{=1} A + \underbrace{f_{1-1}}_{=f_0=0} I_2 = 1A + 0I_2 = 1A = A = A^1$). In other words, part **(c)** of the exercise holds for $n = 1$. This completes the induction base.

Induction step: Let k be a positive integer. Assume that part **(c)** of the exercise holds for $n = k$. We must now prove that part **(c)** of the exercise holds for $n = k + 1$.

We have assumed that part **(c)** of the exercise holds for $n = k$. In other words, $A^k = f_k A + f_{k-1} I_2$. But the recursive definition of the Fibonacci sequence yields $f_{k+1} = f_k + f_{k-1}$. Now,

$$A^{k+1} = A \underbrace{A^k}_{=f_kA+f_{k-1}I_2} = A\left(f_kA + f_{k-1}I_2\right) = f_k \underbrace{AA}_{\substack{=A^2=A+I_2 \\ \text{(by part } \mathbf{(a)} \\ \text{of the exercise)}}} + f_{k-1} \underbrace{AI_2}_{=A} = f_k\left(A + I_2\right) + f_{k-1}A$$
$$= \underbrace{\left(f_k + f_{k-1}\right)}_{=f_{k+1}} A + \underbrace{f_k}_{=f_{(k+1)-1}} I_2 = f_{k+1}A + f_{(k+1)-1}I_2.$$

In other words, part **(c)** of the exercise holds for $n = k + 1$. This completes the induction step. Hence, part **(c)** of the exercise is proven by induction.

(d) Let n be a positive integer. Let $m \in \mathbb{N}$. Part **(c)** of the exercise (applied to $n+m+1$ instead of n) yields

$$A^{n+m+1} = f_{n+m+1}A + \underbrace{f_{(n+m+1)-1}}_{=f_{n+m}} I_2 = f_{n+m+1}A + f_{n+m}I_2. \tag{17}$$

But part **(c)** of the exercise (applied to $m + 1$ instead of n) yields

$$A^{m+1} = f_{m+1}A + \underbrace{f_{(m+1)-1}}_{=f_m} I_2 = f_{m+1}A + f_m I_2.$$

Furthermore, part **(c)** of the exercise yields

$$A^n = f_n A + f_{n-1} I_2.$$

Multiplying the last two equalities, we obtain

$$\begin{aligned} A^{m+1}A^n &= \left(f_{m+1}A + f_m I_2\right)\left(f_nA + f_{n-1}I_2\right) \\ &= \underbrace{f_{m+1}f_n}_{=f_nf_{m+1}} \underbrace{AA}_{\substack{=A^2=A+I_2 \\ \text{(by part } \mathbf{(a)} \\ \text{of the exercise)}}} + f_{m+1}f_{n-1} \underbrace{AI_2}_{=A} + f_mf_n \underbrace{I_2A}_{=A} + \underbrace{f_mf_{n-1}}_{=f_{n-1}f_m} \underbrace{I_2I_2}_{=I_2} \\ &= f_nf_{m+1}\left(A + I_2\right) + f_{m+1}f_{n-1}A + f_mf_nA + f_{n-1}f_mI_2 \\ &= \left(f_nf_{m+1} + f_{m+1}f_{n-1} + f_mf_n\right)A + \left(f_nf_{m+1} + f_{n-1}f_m\right)I_2. \end{aligned}$$

Comparing this with

$$\begin{aligned} A^{m+1}A^n &= A^{(m+1)+n} && \left(\text{by the rules for exponents in the ring } \mathbb{Z}^{2\times 2}\right) \\ &= A^{n+m+1} && \left(\text{since } (m+1)+n = n+m+1\right) \\ &= f_{n+m+1}A + f_{n+m}I_2 && \left(\text{by (17)}\right), \end{aligned}$$

we obtain

$$f_{n+m+1}A + f_{n+m}I_2 = \left(f_n f_{m+1} + f_{m+1}f_{n-1} + f_m f_n\right) A + \left(f_n f_{m+1} + f_{n-1}f_m\right) I_2. \tag{18}$$

We now would certainly want to "compare the coefficients of I_2" in this equality, thus concluding that $f_{n+m} = f_n f_{m+1} + f_{n-1}f_m$. But why can we do this?

The simplest way to justify this is by comparing the $(1,1)$-th entries of both matrices. Indeed, for any $u, v \in \mathbb{Z}$, we have

$$u \underbrace{A}_{=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}} + v \underbrace{I_2}_{=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} = u \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + v \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} v & u \\ u & u+v \end{pmatrix}$$

and thus

$$\left(\text{the } (1,1)\text{-th entry of the matrix } uA + vI_2\right) = v. \tag{19}$$

Applying this equality to $u = f_{n+m+1}$ and $v = f_{n+m}$, we obtain

$$\left(\text{the } (1,1)\text{-th entry of the matrix } f_{n+m+1}A + f_{n+m}I_2\right) = f_{n+m}. \tag{20}$$

But applying (19) to $u = f_n f_{m+1} + f_{m+1}f_{n-1} + f_m f_n$ and $v = f_n f_{m+1} + f_{n-1}f_m$, we obtain

$$\begin{aligned} &\left(\text{the } (1,1)\text{-th entry of the matrix } \left(f_n f_{m+1} + f_{m+1}f_{n-1} + f_m f_n\right) A + \left(f_n f_{m+1} + f_{n-1}f_m\right) I_2\right) \\ &= f_n f_{m+1} + f_{n-1}f_m. \end{aligned} \tag{21}$$

But the left hand sides of the equalities (20) and (21) are equal (because of (18)). Thus, their right hand sides must also be equal. In other words, we have

$$f_{n+m} = f_n f_{m+1} + f_{n-1}f_m.$$

This solves part **(d)** of the exercise.

[*Remark:* There are many other ways to solve this part of the exercise. For example, if we rename n as $n+1$, then it takes the more symmetric form $f_{n+m+1} = f_{n+1}f_{m+1} + f_n f_m$; but this is a well-known identity (see, e.g., Exercise 3 **(e)** in UMN Spring 2018 Math 4707 midterm #1) and a particular case of [Grinbe19, Theorem 2.26 **(a)**]. It can be easily proven by induction on n (or on m). Binet's formula for the Fibonacci numbers also leads to a straightforward solution to part **(d)** of the exercise.]

(e) First, we shall show that $B^2 = B + I_2$. Indeed, $B = I_2 - A$ and thus

$$\begin{aligned} B^2 &= (I_2 - A)^2 = (I_2 - A)(I_2 - A) = \underbrace{I_2 (I_2 - A)}_{=I_2 - A} - \underbrace{A (I_2 - A)}_{=AI_2 - AA} \\ &= I_2 - A - (AI_2 - AA) = I_2 - A - \underbrace{AI_2}_{=A} + \underbrace{AA}_{\substack{=A^2 = A + I_2 \\ \text{(by part } \mathbf{(a)} \\ \text{of the exercise)}}} \\ &= I_2 - A - A + (A + I_2) = 2I_2 - A = \underbrace{(I_2 - A)}_{=B} + I_2 = B + I_2. \end{aligned}$$

It remains to prove that $B^n = f_n B + f_{n-1} I_2$ for all positive integers n.

Here is the laziest (but perfectly legitimate) way of doing this: In our solution to part **(c)** of this exercise, we have proven that $A^n = f_n A + f_{n-1} I_2$ for all positive integers n. Our proof of this fact did not use anything specific about the matrix A, other than the fact that A satisfies $A^2 = A + I_2$. Therefore, we can replace each appearance of "A" by "B" in this proof, and thus obtain a proof of the fact that $B^n = f_n B + f_{n-1} I_2$ for all positive integers n (because B satisfies $B^2 = B + I_2$). This completes the solution of part **(e)** of the exercise.

(f) Let $n \in \mathbb{N}$. We must prove that $A^n - B^n = f_n (A - B)$.

If $n = 0$, then this is easy[7]. Hence, for the rest of this proof, we WLOG assume that $n \neq 0$. Thus, n is a positive integer (since $n \in \mathbb{N}$). Hence, part **(c)** of this exercise yields $A^n = f_n A + f_{n-1} I_2$. But part **(e)** of this exercise yields $B^n = f_n B + f_{n-1} I_2$. Subtracting the last two equalities, we obtain

$$A^n - B^n = (f_n A + f_{n-1} I_2) - (f_n B + f_{n-1} I_2) = f_n (A - B).$$

This solves part **(f)** of the exercise.

(g) Given two elements α and β of $\mathcal{F}$, we say that $\alpha \mid \beta$ *in* $\mathcal{F}$ if and only if there exists some $\gamma \in \mathcal{F}$ such that $\beta = \alpha\gamma$. Thus, we have defined divisibility in $\mathcal{F}$. Basic properties of divisibility of integers (such as Proposition 2.2.4 in the class notes) still apply to divisibility in $\mathcal{F}$ (with the same proofs), since $\mathcal{F}$ is a **commutative** ring.

We recall the following fact (Lemma 2.10.11 **(a)** in the class notes):

Claim 5: Let $d \in \mathbb{N}$. Let x and y be integers. Then, $x - y \mid x^d - y^d$.

This fact has an analogue for elements of $\mathcal{F}$ instead of integers:

Claim 6: Let $d \in \mathbb{N}$. Let x and y be elements of $\mathcal{F}$. Then, $x - y \mid x^d - y^d$ in $\mathcal{F}$.

[*Proof of Claim 6:* Both proofs we gave for Claim 5 in the class notes can be modified in an obvious way to yield proofs of Claim 6, because $\mathcal{F}$ is a **commutative** ring.]

Now, let d and n be nonnegative integers. We must prove that $f_d \mid f_{dn}$.

Part **(f)** of this exercise (applied to d instead of n) yields $A^d - B^d = f_d (A - B)$.

Part **(f)** of this exercise (applied to dn instead of n) yields $A^{dn} - B^{dn} = f_{dn} (A - B)$.

But A and B are elements of $\mathcal{F}$. Thus, their powers A^d, B^d, A^{dn} and B^{dn} are elements of $\mathcal{F}$ as well (since $\mathcal{F}$ is a ring). Hence, Claim 2 (applied to n, A^d and B^d instead of d, x and y) yields $A^d - B^d \mid (A^d)^n - (B^d)^n$ in $\mathcal{F}$. In view of

$$A^d - B^d = f_d (A - B) \qquad \text{and} \qquad (A^d)^n - (B^d)^n = A^{dn} - B^{dn} = f_{dn} (A - B),$$

this rewrites as follows:

$$f_d (A - B) \mid f_{dn} (A - B) \qquad \text{in } \mathcal{F}.$$

Now, it is tempting to "cancel" $A - B$ from this divisibility, and conclude that $f_d \mid f_{dn}$ in $\mathbb{Z}$. To justify this rigorously, we proceed as follows:

We have $f_d (A - B) \mid f_{dn} (A - B)$ in $\mathcal{F}$. In other words, there exists a matrix $\gamma \in \mathcal{F}$ such that

$$f_{dn} (A - B) = f_d (A - B) \gamma \tag{22}$$

(by the definition of divisibility in $\mathcal{F}$). Consider this γ.

[7] *Proof.* Assume that $n = 0$. Thus, $A^n - B^n = \underbrace{A^0}_{=I_2} - \underbrace{B^0}_{=I_2} = I_2 - I_2 = 0_{2\times 2}$. On the other hand, from $n = 0$, we obtain $f_n = f_0 = 0$ and thus $f_n (A - B) = 0 (A - B) = 0_{2\times 2}$. Comparing this with $A^n - B^n = 0_{2\times 2}$, we obtain $A^n - B^n = f_n (A - B)$. Hence, we have proven that $A^n - B^n = f_n (A - B)$ under the assumption that $n = 0$.

We have $B = I_2 - A$ and thus

$$A - B = A - (I_2 - A) = 2 \underbrace{A}_{=\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}} - \underbrace{I_2}_{=\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}} = 2 \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & 1 \end{pmatrix}.$$

Hence,

$$(\text{the } (2,2)\text{-th entry of the matrix } A - B) = 1. \tag{23}$$

Since matrices are scaled entrywise, we now have

$$\begin{aligned} &(\text{the } (2,2)\text{-th entry of the matrix } f_{dn}(A - B)) \\ &= f_{dn} \cdot \underbrace{(\text{the } (2,2)\text{-th entry of the matrix } A - B)}_{=1} = f_{dn}. \end{aligned} \tag{24}$$

On the other hand, the matrices $A - B$ and γ belong to $\mathcal{F}$; thus, their product $(A - B)\gamma$ belongs to $\mathcal{F}$ as well, and therefore belongs to $\mathbb{Z}^{2\times 2}$ (since $\mathcal{F} \subseteq \mathbb{Z}^{2\times 2}$). In other words, $(A - B)\gamma$ is a 2×2-matrix with integer entries. Hence, each entry of $(A - B)\gamma$ is an integer, i.e., belongs to $\mathbb{Z}$. Thus, in particular,

$$(\text{the } (2,2)\text{-th entry of the matrix } (A - B)\gamma) \in \mathbb{Z}.$$

Now, (24) yields

$$\begin{aligned} f_{dn} &= \left(\text{the } (2,2)\text{-th entry of the matrix } \underbrace{f_{dn}(A - B)}_{=f_d(A-B)\gamma}\right) \\ &= (\text{the } (2,2)\text{-th entry of the matrix } f_d(A - B)\gamma) \\ &= f_d \cdot (\text{the } (2,2)\text{-th entry of the matrix } (A - B)\gamma) \end{aligned}$$

(since matrices are scaled entrywise). This yields that $f_d \mid f_{dn}$ (in the classical sense of divisibility of integers), because we know that (the $(2,2)$-th entry of the matrix $(A - B)\gamma) \in \mathbb{Z}$. This solves part **(g)** of the exercise.

[*Remark:* Once again, there are other ways to solve this part of the exercise. For example, it can be restated as "Prove that $f_u \mid f_v$ whenever u and v are nonnegative integers satisfying $u \mid v$"; but in this form, it is clearly a particular case of [Grinbe19, Theorem 2.26 **(c)**].]

6 Exercise 6: ISBNs vs. fat fingers

6.1 Problem

An *ISBN* shall mean a 10-tuple $(a_1, a_2, \ldots, a_{10}) \in \{0, 1, \ldots, 10\}^{10}$ such that

$$1a_1 + 2a_2 + \cdots + 10a_{10} \equiv 0 \bmod 11.$$

(For example, the 10-tuple $(1, 1, \ldots, 1)$ is an ISBN.)

Prove the following:

(a) If $\mathbf{a} = (a_1, a_2, \ldots, a_{10})$ and $\mathbf{b} = (b_1, b_2, \ldots, b_{10})$ are two ISBNs that are equal in all but one entry (i.e., there exists some $k \in \{1, 2, \ldots, 10\}$ such that $a_i = b_i$ for all $i \neq k$), then $\mathbf{a} = \mathbf{b}$.

(b) If an ISBN $\mathbf{a} = (a_1, a_2, \ldots, a_{10})$ is obtained from an ISBN $\mathbf{b} = (b_1, b_2, \ldots, b_{10})$ by swapping two entries (i.e., there exist $k, \ell \in \{1, 2, \ldots, 10\}$ such that $a_k = b_\ell$ and $a_\ell = b_k$ and $a_i = b_i$ for all $i \notin \{k, \ell\}$), then $\mathbf{a} = \mathbf{b}$.

6.2 Remark

What we called ISBN here is essentially the definition of an ISBN-10 – an international standard for book identifiers used from the 1970s until 2007. For example, the ISBN-10 of the Graham/Knuth/Patashnik book "Concrete Mathematics" is "0-201-55802-5", which corresponds to $(0, 2, 0, 1, 5, 5, 8, 0, 2, 5)$; you can check that this is indeed an ISBN according to our definition.

(An "X" in a real-life ISBN stands for an entry that is 10.)

As this exercise shows, ISBNs have an error-detection property: If you make a typo in a single digit or accidentally swap two digits, the result will not be an ISBN, so you will know that something has gone wrong. This helps you avoid ordering the wrong book from a bookstore or library. Credit card numbers have a similar error-detection feature.

This is one of the simplest examples of an error correction code. We may or may not see more of them in class. For now, you can think about how to define "ISBNs"

- in $\{0, 1, \ldots, 4\}^4$;
- in $\{0, 1, \ldots, 6\}^6$;
- in $\{0, 1, \ldots, 8\}^8$ (this is harder!).

6.3 Solution sketch

Before we solve the exercise, let us prove a simple claim which our solution will rest upon:

> *Claim 1:* Let u and v be two elements of $\{-10, -9, \ldots, 10\}$ such that $uv \equiv 0 \bmod 11$ and $u \neq 0$. Then, $v = 0$.

[*Proof of Claim 1:* Assume the contrary. Thus, $v \neq 0$.

We have $u \in \{-10, -9, \ldots, 10\}$, thus $-10 \leq u \leq 10$ and therefore $|u| \leq 10$. In other words, $10 \geq |u|$.

If we had $11 \mid u$, then Proposition 2.2.3 **(b)** in the class notes (applied to $a = 11$ and $b = u$) would yield $|11| \leq |u|$ (since $u \neq 0$); but this would contradict $|11| = 11 > 10 \geq |u|$. Hence, we cannot have $11 \mid u$. The same argument (applied to v instead of u) shows that we cannot have $11 \mid v$ (since $v \neq 0$). Thus, neither $11 \mid u$ nor $11 \mid v$ holds.

But 11 is a prime, and we have $11 \mid uv$ (since $uv \equiv 0 \bmod 11$). Thus, Theorem 2.13.6 in the class notes (applied to $p = 11$, $a = u$ and $b = v$) shows that $11 \mid u$ or $11 \mid v$. This contradicts the fact that neither $11 \mid u$ nor $11 \mid v$ holds. This contradiction shows that our assumption was false. Hence, Claim 1 is proven.]

(a) Let $\mathbf{a} = (a_1, a_2, \ldots, a_{10})$ and $\mathbf{b} = (b_1, b_2, \ldots, b_{10})$ be two ISBNs that are equal in all but one entry. We must prove that $\mathbf{a} = \mathbf{b}$.

We have assumed that $\mathbf{a}$ and $\mathbf{b}$ are equal in all but one entry. In other words, there exists some $k \in \{1, 2, \ldots, 10\}$ such that

$$a_i = b_i \qquad \text{for all } i \neq k. \tag{25}$$

Consider this k.

We have assumed that $\mathbf{a}$ is an ISBN. In other words, $(a_1, a_2, \ldots, a_{10}) \in \{0, 1, \ldots, 10\}^{10}$ and $1a_1 + 2a_2 + \cdots + 10a_{10} \equiv 0 \bmod 11$.

Thus,

$$\sum_{i \in \{1,2,\ldots,10\}} ia_i = 1a_1 + 2a_2 + \cdots + 10a_{10} \equiv 0 \bmod 11. \tag{26}$$

Similarly,

$$\sum_{i \in \{1,2,\ldots,10\}} ib_i \equiv 0 \bmod 11. \tag{27}$$

But

$$\begin{aligned} \sum_{i \in \{1,2,\ldots,10\}} ia_i &= ka_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} i \underbrace{a_i}_{\substack{=b_i \\ \text{(by (25))}}} \\ &\qquad \left(\text{here, we have split off the addend for } i = k \text{ from the sum}\right) \\ &= ka_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i, \end{aligned}$$

so that (26) rewrites as

$$ka_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i \equiv 0 \bmod 11. \tag{28}$$

Furthermore,

$$\begin{aligned} \sum_{i \in \{1,2,\ldots,10\}} ib_i &= kb_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i \\ &\qquad \left(\text{here, we have split off the addend for } i = k \text{ from the sum}\right), \end{aligned}$$

so that (27) rewrites as

$$kb_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i \equiv 0 \bmod 11.$$

Subtracting this congruence from the congruence (28), we obtain

$$\left(ka_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i\right) - \left(kb_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i\right) \equiv 0 - 0 = 0 \bmod 11.$$

In view of

$$\left(ka_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i\right) - \left(kb_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \neq k}} ib_i\right) = ka_k - kb_k = k\left(a_k - b_k\right),$$

this rewrites as $k(a_k - b_k) \equiv 0 \mod 11$.

We have $a_k \in \{0,1,\ldots,10\}$ (since $(a_1,a_2,\ldots,a_{10}) \in \{0,1,\ldots,10\}^{10}$) and $b_k \in \{0,1,\ldots,10\}$ (similarly). Hence, $a_k - b_k \in \{-10,-9,\ldots,10\}$. Furthermore, $k \in \{1,2,\ldots,10\} \subseteq \{-10,-9,\ldots,10\}$ and $k \neq 0$. Thus, Claim 1 (applied to $u = k$ and $v = a_k - b_k$) yields $a_k - b_k = 0$. In other words, $a_k = b_k$.

Now, (25) shows that any entry of the 10-tuple $\mathbf{a}$ is equal to the corresponding entry of the 10-tuple $\mathbf{b}$, except perhaps the k-th entry. But the equality $a_k = b_k$ shows that the k-th entries of these two 10-tuples $\mathbf{a}$ and $\mathbf{b}$ are also equal to each other. Thus, each entry of $\mathbf{a}$ is equal to the corresponding entry of $\mathbf{b}$. In other words, $\mathbf{a} = \mathbf{b}$. This solves part **(a)** of the exercise.

(b) Let $\mathbf{a} = (a_1,a_2,\ldots,a_{10})$ and $\mathbf{b} = (b_1,b_2,\ldots,b_{10})$ be two ISBNs such that $\mathbf{a}$ is obtained from $\mathbf{b}$ by swapping two entries. We must prove that $\mathbf{a} = \mathbf{b}$.

We have assumed that $\mathbf{a}$ is obtained from $\mathbf{b}$ by swapping two entries. In other words, there exist $k, \ell \in \{1,2,\ldots,10\}$ such that $a_k = b_\ell$ and $a_\ell = b_k$ and

$$a_i = b_i \qquad \text{for all } i \notin \{k,\ell\}. \tag{29}$$

Consider these k, ℓ.

We must prove that $\mathbf{a} = \mathbf{b}$. If $a_k = a_\ell$, then this is true[8]. Hence, for the rest of this solution, we WLOG assume that $a_k \neq a_\ell$. Thus, $k \neq \ell$, so that $k - \ell \neq 0$.

Also, we have $a_k \neq a_\ell$. In view of $a_k = b_\ell$ and $a_\ell = b_k$, this rewrites as $b_\ell \neq b_k$.

We have assumed that $\mathbf{a}$ is an ISBN. In other words, $(a_1,a_2,\ldots,a_{10}) \in \{0,1,\ldots,10\}^{10}$ and $1a_1 + 2a_2 + \cdots + 10a_{10} \equiv 0 \mod 11$.

Thus,

$$\sum_{i \in \{1,2,\ldots,10\}} i a_i = 1a_1 + 2a_2 + \cdots + 10a_{10} \equiv 0 \mod 11. \tag{30}$$

Similarly,

$$\sum_{i \in \{1,2,\ldots,10\}} i b_i \equiv 0 \mod 11. \tag{31}$$

But

$$\begin{aligned}\sum_{i \in \{1,2,\ldots,10\}} i a_i &= k \underbrace{a_k}_{=b_\ell} + \ell \underbrace{a_\ell}_{=b_k} + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \notin \{k,\ell\}}} i \underbrace{a_i}_{\substack{=b_i \\ \text{(by (29))}}} \\ &\qquad \left(\begin{array}{c}\text{here, we have split off the addends for } i = k \text{ and for } i = \ell \text{ from the} \\ \text{sum (and these were indeed two different addends, since } k \neq \ell\text{)}\end{array}\right) \\ &= k b_\ell + \ell b_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \notin \{k,\ell\}}} i b_i,\end{aligned}$$

so that (30) rewrites as

$$k b_\ell + \ell b_k + \sum_{\substack{i \in \{1,2,\ldots,10\};\\ i \notin \{k,\ell\}}} i b_i \equiv 0 \mod 11. \tag{32}$$

[8] *Proof.* Assume that $a_k = a_\ell$. Thus, $a_k = a_\ell = b_k$ and $a_\ell = a_k = b_\ell$. Now, from (29), we know that the equality $a_i = b_i$ holds for all $i \notin \{k,\ell\}$. But this equality also holds for $i = k$ (since $a_k = b_k$) and for $i = \ell$ (since $a_\ell = b_\ell$). Thus, this equality holds for all $i \in \{1,2,\ldots,10\}$. In other words, $\mathbf{a} = \mathbf{b}$, qed.

Furthermore,

$$\sum_{i\in\{1,2,\ldots,10\}} ia_i = kb_k + \ell b_\ell + \sum_{\substack{i\in\{1,2,\ldots,10\};\\ i\notin\{k,\ell\}}} ib_i$$
$$\left(\begin{array}{c}\text{here, we have split off the addends for } i=k \text{ and for } i=\ell \text{ from the}\\ \text{sum (and these were indeed two different addends, since } k\neq\ell)\end{array}\right),$$

so that (31) rewrites as

$$kb_k + \ell b_\ell + \sum_{\substack{i\in\{1,2,\ldots,10\};\\ i\notin\{k,\ell\}}} ib_i \equiv 0 \operatorname{mod} 11.$$

Subtracting this congruence from the congruence (32), we obtain

$$\left(kb_\ell + \ell b_k + \sum_{\substack{i\in\{1,2,\ldots,10\};\\ i\notin\{k,\ell\}}} ib_i\right) - \left(kb_k + \ell b_\ell + \sum_{\substack{i\in\{1,2,\ldots,10\};\\ i\notin\{k,\ell\}}} ib_i\right) \equiv 0-0 = 0 \operatorname{mod} 11.$$

In view of

$$\left(kb_\ell + \ell b_k + \sum_{\substack{i\in\{1,2,\ldots,10\};\\ i\notin\{k,\ell\}}} ib_i\right) - \left(kb_k + \ell b_\ell + \sum_{\substack{i\in\{1,2,\ldots,10\};\\ i\notin\{k,\ell\}}} ib_i\right) = kb_\ell + \ell b_k - kb_k - \ell b_\ell$$
$$= (k-\ell)(b_\ell - b_k),$$

this rewrites as $(k-\ell)(b_\ell - b_k) \equiv 0 \operatorname{mod} 11$.

But $\mathbf{b}$ is an ISBN; thus, $(b_1, b_2, \ldots, b_{10}) \in \{0,1,\ldots,10\}^{10}$. Hence, $b_k \in \{0,1,\ldots,10\}$ and $b_\ell \in \{0,1,\ldots,10\}$. Therefore, $b_\ell - b_k \in \{-10,-9,\ldots,10\}$. Furthermore, $k-\ell \in \{-10,-9,\ldots,10\}$ (since both k and ℓ belong to the set $\{1,2,\ldots,10\}$) and $k-\ell\neq 0$ (since $k\neq\ell$). Thus, Claim 1 (applied to $u=k-\ell$ and $v=b_\ell-b_k$) yields $b_\ell - b_k = 0$. In other words, $b_\ell = b_k$. This contradicts $b_\ell \neq b_k$. Thus, $\mathbf{a}=\mathbf{b}$ (because *ex falso quodlibet*)[9]. This solves part **(b)** of the exercise.

References

[Grinbe19] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, 10 January 2019.
`http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf`
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see `https://github.com/darijgr/detnotes/releases/tag/2019-01-10` .

[Rogers71] Kenneth Rogers, *An elementary proof of a theorem of Jacobson*, Abhandlungen Aus Dem Mathematischen Seminar Der Universität Hamburg, **35** (3-4), 1971, pp. 223–229. doi:10.1007/bf02993626.

[9] Of course, this shows that the case we are considering doesn't ever happen – i.e., our WLOG assumption left us only an impossible case to consider. But it was not clear a priori that this case was impossible; we had to work to reach this conclusion.

[Vorobi02] Nicolai N. Vorobiev, *Fibonacci Numbers*, Translated from the Russian by Mircea Martin, Springer 2002 (translation of the 6th Russian edition).