

Math 4707 Spring 2018 (Darij Grinberg): homework set 1 with solutions

Contents

0.1. Binomial coefficient basics	1
0.2. A fraction appears	7
0.3. Lemmas for the Sierpinski gasket appearing in Pascal’s triangle . . .	13
0.4. More on Fibonacci numbers	26
0.5. Some basic counting	29

0.1. Binomial coefficient basics

Definition 0.1. The notation \mathbb{N} shall always stand for the set $\{0, 1, 2, \dots\}$ of non-negative integers.

Definition 0.2. If $n \in \mathbb{N}$, then $n!$ shall denote the product $1 \cdot 2 \cdot \dots \cdot n$. For example, $3! = 1 \cdot 2 \cdot 3 = 6$ and $1! = 1$ and $0! = (\text{empty product}) = 1$. (An empty product is defined to be 1.)

Notice that

$$n! = n \cdot (n - 1)! \quad \text{for any positive integer } n. \tag{1}$$

Definition 0.3. (a) We define the *binomial coefficient* $\binom{n}{k}$ by

$$\binom{n}{k} = \frac{n(n - 1) \cdot \dots \cdot (n - k + 1)}{k!}$$

for every $n \in \mathbb{Q}$ and $k \in \mathbb{N}$.

For example, $\binom{-3}{4} = \frac{(-3)(-4)(-5)(-6)}{4!} = 15$ and $\binom{4}{1} = \frac{4}{1!} = 4$ and

$$\binom{4}{0} = \frac{(\text{empty product})}{0!} = \frac{1}{1} = 1.$$

(b) If $n \in \mathbb{Q}$ and $k \in \mathbb{Q} \setminus \mathbb{N}$, then $\binom{n}{k}$ is defined to be 0.

See [Grinbe16, Chapter 3] for various properties of binomial coefficients. You are free to use those shown in [Grinbe16, §3.1] without proof. In particular, you are free to use the following fact:

Proposition 0.4 (recurrence of the binomial coefficients). Let $n \in \mathbb{Q}$ and $k \in \mathbb{Z}$. Then,

$$\binom{n}{k} = \binom{n - 1}{k - 1} + \binom{n - 1}{k}.$$

(This is exactly [Grinbe16, Proposition 3.11] when k is a positive integer. The cases $k = 0$ and $k < 0$ are easy.)

Proposition 0.5 (upper negation). We have

$$\binom{m}{n} = (-1)^n \binom{n-m-1}{n} \quad (2)$$

for any $m \in \mathbb{Q}$ and $n \in \mathbb{Z}$.

(This follows from [Grinbe16, Proposition 3.16] when $n \in \mathbb{N}$. The case $n \notin \mathbb{N}$ is easy.)

Proposition 0.6. We have

$$\binom{m}{n} = \binom{m}{m-n} \quad (3)$$

for any $m \in \mathbb{N}$ and $n \in \mathbb{N}$ satisfying $m \geq n$.

(This is exactly [Grinbe16, Proposition 3.8].)

Proposition 0.7. We have

$$\binom{m}{m} = 1 \quad (4)$$

for every $m \in \mathbb{N}$.

(This is exactly [Grinbe16, Proposition 3.9].)

Proposition 0.8. We have

$$\binom{m}{n} = 0 \quad (5)$$

for every $m \in \mathbb{N}$ and $n \in \mathbb{N}$ satisfying $m < n$.

(This is exactly [Grinbe16, Proposition 3.6].)

Exercise 1. (a) Show that $\binom{-1}{k} = (-1)^k$ for each $k \in \mathbb{N}$.

(b) Show that $\binom{-2}{k} = (-1)^k (k+1)$ for each $k \in \mathbb{N}$.

(c) Show that $\frac{1! \cdot 2! \cdot \dots \cdot (2n)!}{n!}$ is a perfect square (i.e., the square of an integer) whenever $n \in \mathbb{N}$ is even.

Remark 0.9. Parts **(a)** and **(b)** of Exercise 1 are known facts. I found part **(c)** on https://www.reddit.com/r/math/comments/7rybhp/factorial_problem/.

Exercise 1 now also appears in [Grinbe16, Exercise 3.5 and Remark 3.18].

Solution to Exercise 1. (a) First solution to Exercise 1 (a): Let $k \in \mathbb{N}$. Then, Proposition 0.5 (applied to $m = -1$ and $n = k$) yields

$$\begin{aligned} \binom{-1}{k} &= (-1)^k \binom{k - (-1) - 1}{k} \\ &= (-1)^k \underbrace{\binom{k}{k}}_{=1} \quad (\text{since } k - (-1) - 1 = k) \\ &\quad \text{(by Proposition 0.7 (applied to } m=k)) \\ &= (-1)^k. \end{aligned}$$

This solves Exercise 1 (a).

Second solution to Exercise 1 (a): Let $k \in \mathbb{N}$. Then, the definition of $k!$ yields $k! = 1 \cdot 2 \cdot \dots \cdot k$. But the definition of $\binom{-1}{k}$ yields

$$\begin{aligned} \binom{-1}{k} &= \frac{(-1)(-2)\cdots(-1-k+1)}{k!} \\ &= \frac{(-1)(-2)\cdots(-k)}{k!} \quad (\text{since } -1-k+1 = -k) \\ &= \frac{1}{k!} \cdot \underbrace{(-1)(-2)\cdots(-k)}_{=(-1)^k \cdot (1 \cdot 2 \cdots k)} = \frac{1}{k!} \cdot (-1)^k \cdot \underbrace{(1 \cdot 2 \cdots k)}_{=k!} \\ &= \frac{1}{k!} \cdot (-1)^k \cdot k! = (-1)^k. \end{aligned}$$

This solves Exercise 1 (a).

(b) First solution to Exercise 1 (b): Let $k \in \mathbb{N}$. Then, $k+1 \in \mathbb{N}$ and $k+1 \geq k$. Hence, Proposition 0.6 (applied to $m = k+1$ and $n = k$) yields

$$\begin{aligned} \binom{k+1}{k} &= \binom{k+1}{(k+1)-k} = \binom{k+1}{1} \quad (\text{since } (k+1) - k = 1) \\ &= \frac{(k+1)((k+1)-1)\cdots((k+1)-1+1)}{1!} \\ &\quad \left(\text{by the definition of } \binom{k+1}{k} \right) \\ &= \underbrace{\frac{1}{1!}}_{=1 \text{ (since } 1! \cdot 1)} \cdot \underbrace{(k+1)((k+1)-1)\cdots((k+1)-1+1)}_{=k+1 \text{ (since this product has only 1 factor)}} \\ &= 1 \cdot (k+1) = k+1. \end{aligned}$$

But Proposition 0.5 (applied to $m = -2$ and $n = k$) yields

$$\begin{aligned} \binom{-2}{k} &= (-1)^k \binom{k - (-2) - 1}{k} = (-1)^k \underbrace{\binom{k+1}{k}}_{=k+1} \quad (\text{since } k - (-2) - 1 = k + 1) \\ &= (-1)^k (k + 1). \end{aligned}$$

This solves Exercise 1 (b).

Second solution to Exercise 1 (b): Let $k \in \mathbb{N}$. Then, the definition of $(k + 1)!$ yields

$$(k + 1)! = 1 \cdot 2 \cdots (k + 1) = 1 \cdot (2 \cdot 3 \cdots (k + 1)) = 2 \cdot 3 \cdots (k + 1).$$

On the other hand, applying (1) to $n = k + 1$, we find

$$(k + 1)! = (k + 1) \cdot \left(\underbrace{(k + 1) - 1}_{=k} \right)! = (k + 1) \cdot k!.$$

But the definition of $\binom{-2}{k}$ yields

$$\begin{aligned} \binom{-2}{k} &= \frac{(-2)(-3)\cdots(-2-k+1)}{k!} \\ &= \frac{(-2)(-3)\cdots(-(k+1))}{k!} \quad (\text{since } -2 - k + 1 = -(k + 1)) \\ &= \frac{1}{k!} \cdot \underbrace{(-2)(-3)\cdots(-(k+1))}_{=(-1)^k \cdot (2 \cdot 3 \cdots (k+1))} = \frac{1}{k!} \cdot (-1)^k \cdot \underbrace{(2 \cdot 3 \cdots (k+1))}_{=(k+1)!} \\ &= \frac{1}{k!} \cdot (-1)^k \cdot \underbrace{(k+1)!}_{=(k+1) \cdot k!} = \frac{1}{k!} \cdot (-1)^k \cdot (k+1) \cdot k! = (-1)^k (k+1). \end{aligned}$$

This solves Exercise 1 (b).

(c) We shall use the \prod notation for finite products. In a nutshell: If u and v are integers, and if b_u, b_{u+1}, \dots, b_v are any numbers, then $\prod_{i=u}^v b_i$ denotes the product $b_u b_{u+1} \cdots b_v$. (See [Grinbe16, §1.4] for properties of this notation. Notice that the product $\prod_{i=u}^v b_i$ is understood to be an empty product when $u > v$, and in this case is defined to be 1.)

We first claim that

$$\frac{1! \cdot 2! \cdots (2n)!}{n!} = 2^n \cdot \left(\prod_{i=1}^n ((2i-1)!) \right)^2 \quad (6)$$

for every $n \in \mathbb{N}$.

We give two proofs (6): one by astutely transforming the left-hand side, another by straightforward induction.

[First proof of (6): Let $n \in \mathbb{N}$. Then, we can group the factors of the product $1! \cdot 2! \cdot \dots \cdot (2n)!$ into pairs of successive factors. We thus obtain

$$\begin{aligned}
 & 1! \cdot 2! \cdot \dots \cdot (2n)! \\
 &= (1! \cdot 2!) \cdot (3! \cdot 4!) \cdot \dots \cdot ((2n-1)! \cdot (2n)!) = \prod_{i=1}^n \left((2i-1)! \cdot \underbrace{(2i)!}_{\substack{=2i \cdot (2i-1)! \\ \text{(by (1), applied} \\ \text{to } n=2i)}} \right) \\
 &= \prod_{i=1}^n \underbrace{((2i-1)! \cdot 2i \cdot (2i-1)!)}_{=2i \cdot (2i-1)!^2} = \prod_{i=1}^n (2i \cdot (2i-1)!^2) \\
 &= \underbrace{\left(\prod_{i=1}^n (2i) \right)}_{=2^n \prod_{i=1}^n i} \cdot \underbrace{\left(\prod_{i=1}^n ((2i-1)!^2) \right)}_{=\left(\prod_{i=1}^n ((2i-1)!) \right)^2} = 2^n \underbrace{\left(\prod_{i=1}^n i \right)}_{=1 \cdot 2 \cdot \dots \cdot n = n!} \cdot \left(\prod_{i=1}^n ((2i-1)!) \right)^2 \\
 &= 2^n n! \cdot \left(\prod_{i=1}^n ((2i-1)!) \right)^2.
 \end{aligned}$$

Dividing both sides of this equality by $n!$, we find

$$\frac{1! \cdot 2! \cdot \dots \cdot (2n)!}{n!} = 2^n \cdot \left(\prod_{i=1}^n ((2i-1)!) \right)^2.$$

This proves (6).]

[Second proof of (6): We shall prove (6) by induction on n :

Induction base: Comparing

$$\frac{1! \cdot 2! \cdot \dots \cdot (2 \cdot 0)!}{0!} = \underbrace{\frac{1}{0!}}_{=1} \cdot \underbrace{(1! \cdot 2! \cdot \dots \cdot (2 \cdot 0)!)}_{\substack{=1! \cdot 2! \cdot \dots \cdot 0! \\ =(\text{empty product})=1}} = 1$$

with

$$\underbrace{2^0}_{=1} \cdot \left(\underbrace{\prod_{i=1}^0 ((2i-1)!)}_{=(\text{empty product})=1} \right)^2 = 1 \cdot 1^2 = 1,$$

we obtain $\frac{1! \cdot 2! \cdot \dots \cdot (2 \cdot 0)!}{0!} = 2^0 \cdot \left(\prod_{i=1}^0 ((2i-1)!) \right)^2$. In other words, (6) holds for $n = 0$. This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that (6) holds for $n = m$. We must prove that (6) holds for $n = m + 1$.

Applying (1) to $n = m + 1$, we find

$$(m+1)! = (m+1) \cdot \left(\underbrace{(m+1) - 1}_{=m} \right)! = (m+1) \cdot m!.$$

On the other hand, applying (1) to $n = 2m + 2$, we find

$$(2m+2)! = (2m+2) \cdot \left(\underbrace{(2m+2) - 1}_{=2m+1} \right)! = (2m+2) \cdot (2m+1)!.$$

We have assumed that (6) holds for $n = m$. In other words, we have

$$\frac{1! \cdot 2! \cdot \dots \cdot (2m)!}{m!} = 2^m \cdot \left(\prod_{i=1}^m ((2i-1)!) \right)^2.$$

Now,

$$\begin{aligned} & \frac{1! \cdot 2! \cdot \dots \cdot (2(m+1))!}{(m+1)!} \\ &= \frac{1! \cdot 2! \cdot \dots \cdot (2m+2)!}{(m+1) \cdot m!} \\ & \quad (\text{since } 2(m+1) = 2m+2 \text{ and } (m+1)! = (m+1) \cdot m!) \\ &= \frac{1}{(m+1) \cdot m!} \cdot \underbrace{(1! \cdot 2! \cdot \dots \cdot (2m+2)!)}_{=(1! \cdot 2! \cdot \dots \cdot (2m)!) \cdot (2m+1)! \cdot (2m+2)!} \\ &= \frac{1}{(m+1) \cdot m!} \cdot (1! \cdot 2! \cdot \dots \cdot (2m)!) \cdot (2m+1)! \cdot \underbrace{(2m+2)!}_{=(2m+2) \cdot (2m+1)!} \\ &= \frac{1}{(m+1) \cdot m!} \cdot (1! \cdot 2! \cdot \dots \cdot (2m)!) \cdot (2m+1)! \cdot (2m+2) \cdot (2m+1)! \\ &= \underbrace{\frac{2m+2}{m+1}}_{=2} \cdot \underbrace{\frac{1! \cdot 2! \cdot \dots \cdot (2m)!}{m!}}_{=2^m \cdot \left(\prod_{i=1}^m ((2i-1)!) \right)^2} \cdot ((2m+1)!)^2 \\ &= 2 \cdot 2^m \cdot \left(\prod_{i=1}^m ((2i-1)!) \right)^2 \cdot ((2m+1)!)^2. \end{aligned}$$

Comparing this with

$$\begin{aligned}
 & \underbrace{2^{m+1}}_{=2 \cdot 2^m} \cdot \left(\underbrace{\prod_{i=1}^{m+1} ((2i-1)!)}_{=\left(\prod_{i=1}^m ((2i-1)!)\right) \cdot (2(m+1)-1)!} \right)^2 \\
 &= 2 \cdot 2^m \cdot \left(\left(\prod_{i=1}^m ((2i-1)!)\right) \cdot \underbrace{(2(m+1)-1)!}_{=2m+1} \right)^2 \\
 &= 2 \cdot 2^m \cdot \left(\left(\prod_{i=1}^m ((2i-1)!)\right) \cdot (2m+1)! \right)^2 \\
 &= 2 \cdot 2^m \cdot \left(\prod_{i=1}^m ((2i-1)!)\right)^2 \cdot ((2m+1)!)^2,
 \end{aligned}$$

we obtain

$$\frac{1! \cdot 2! \cdot \dots \cdot (2(m+1))!}{(m+1)!} = 2^{m+1} \cdot \left(\prod_{i=1}^{m+1} ((2i-1)!) \right)^2.$$

In other words, (6) holds for $n = m + 1$. This completes the induction step. Thus, (6) is proven again.]

Now, let $n \in \mathbb{N}$ be **even**. Then, $n/2 \in \mathbb{N}$. Thus, $2^{n/2}$ is an integer. Now, (6) yields

$$\begin{aligned}
 \frac{1! \cdot 2! \cdot \dots \cdot (2n)!}{n!} &= \underbrace{2^n}_{=(2^{n/2})^2} \cdot \left(\prod_{i=1}^n ((2i-1)!) \right)^2 = (2^{n/2})^2 \cdot \left(\prod_{i=1}^n ((2i-1)!) \right)^2 \\
 &= \left(2^{n/2} \cdot \prod_{i=1}^n ((2i-1)!) \right)^2.
 \end{aligned}$$

The right-hand side of this equality is a perfect square (since $2^{n/2}$ is an integer, and $\prod_{i=1}^n ((2i-1)!)$ is an integer as well). Thus, $\frac{1! \cdot 2! \cdot \dots \cdot (2n)!}{n!}$ is a perfect square. This solves Exercise 1 (c). \square

0.2. A fraction appears

Definition 0.10. Let x be a real number. Then, $\lfloor x \rfloor$ is defined to be the unique integer n satisfying $n \leq x < n + 1$. This integer $\lfloor x \rfloor$ is called the *floor* of x , or the *integer part* of x . For example,

$$\lfloor n \rfloor = n \quad \text{for every } n \in \mathbb{Z}; \quad (7)$$

$$\left\lfloor n + \frac{1}{2} \right\rfloor = n \quad \text{for every } n \in \mathbb{Z}; \quad (8)$$

$$\begin{aligned} \lfloor 1.32 \rfloor &= 1; & \lfloor \pi \rfloor &= 3; & \lfloor 0.98 \rfloor &= 0; \\ \lfloor -2.3 \rfloor &= -3; & \lfloor -0.4 \rfloor &= -1. \end{aligned}$$

Exercise 2. Let $n \in \mathbb{N}$. Prove that

$$\sum_{k=0}^n (-1)^k (k+1) = (-1)^n \left\lfloor \frac{n+2}{2} \right\rfloor.$$

First solution to Exercise 2. We shall solve Exercise 2 by induction on n :

Induction base: Comparing

$$\underbrace{(-1)^0}_{=1} \left\lfloor \underbrace{\frac{0+2}{2}}_{=1} \right\rfloor = \lfloor 1 \rfloor = 1$$

with $\sum_{k=0}^0 (-1)^k (k+1) = \underbrace{(-1)^0}_{=1} \underbrace{(0+1)}_{=1} = 1$, we find $\sum_{k=0}^0 (-1)^k (k+1) = (-1)^0 \left\lfloor \frac{0+2}{2} \right\rfloor$.

In other words, Exercise 2 holds for $n = 0$. This completes the induction base.

Induction step: Let m be a positive integer. Assume that Exercise 2 holds for $n = m - 1$. We must prove that Exercise 2 holds for $n = m$.

We have assumed that Exercise 2 holds for $n = m - 1$. In other words,

$$\sum_{k=0}^{m-1} (-1)^k (k+1) = (-1)^{m-1} \left\lfloor \frac{(m-1)+2}{2} \right\rfloor.$$

Now,

$$\begin{aligned}
 \sum_{k=0}^m (-1)^k (k+1) &= \underbrace{\sum_{k=0}^{m-1} (-1)^k (k+1)}_{=(-1)^{m-1} \left\lfloor \frac{(m-1)+2}{2} \right\rfloor} + (-1)^m (m+1) \\
 &= \underbrace{(-1)^{m-1}}_{=-(-1)^m} \left\lfloor \frac{(m-1)+2}{2} \right\rfloor + (-1)^m (m+1) \\
 &= -(-1)^m \left\lfloor \frac{(m-1)+2}{2} \right\rfloor + (-1)^m (m+1) \\
 &= (-1)^m (m+1) - (-1)^m \left\lfloor \frac{(m-1)+2}{2} \right\rfloor \\
 &= (-1)^m \left((m+1) - \left\lfloor \frac{(m-1)+2}{2} \right\rfloor \right). \tag{9}
 \end{aligned}$$

Now, we claim

$$(m+1) - \left\lfloor \frac{(m-1)+2}{2} \right\rfloor = \left\lfloor \frac{m+2}{2} \right\rfloor. \tag{10}$$

[Proof of (10): We are in one of the following two cases:

Case 1: The integer m is even.

Case 2: The integer m is odd.

Let us first consider Case 1. In this case, the integer m is even. In other words, $m = 2g$ for some $g \in \mathbb{Z}$. Consider this g .

Now, $m = 2g$, so that $\frac{(m-1)+2}{2} = \frac{(2g-1)+2}{2} = g + \frac{1}{2}$. Hence,

$$\left\lfloor \frac{(m-1)+2}{2} \right\rfloor = \left\lfloor g + \frac{1}{2} \right\rfloor = g \quad (\text{by (8) (applied to } n = g)).$$

Also, from $m = 2g$, we obtain $\frac{m+2}{2} = \frac{2g+2}{2} = g+1$. Hence,

$$\left\lfloor \frac{m+2}{2} \right\rfloor = \lfloor g+1 \rfloor = g+1 \quad (\text{by (7) (applied to } n = g+1)).$$

Comparing this with

$$\left(\underbrace{m}_{=2g} + 1 \right) - \underbrace{\left\lfloor \frac{(m-1)+2}{2} \right\rfloor}_{=g} = (2g+1) - g = g+1,$$

we find $(m+1) - \left\lfloor \frac{(m-1)+2}{2} \right\rfloor = \left\lfloor \frac{m+2}{2} \right\rfloor$. Thus, (10) is proven in Case 1.

Let us now consider Case 2. In this case, the integer m is odd. In other words, $m = 2g + 1$ for some $g \in \mathbb{Z}$. Consider this g .

Now, $m = 2g + 1$, so that $\frac{(m-1)+2}{2} = \frac{((2g+1)-1)+2}{2} = g+1$. Hence,

$$\left\lfloor \frac{(m-1)+2}{2} \right\rfloor = \lfloor g+1 \rfloor = g+1 \quad (\text{by (7) (applied to } n = g+1)).$$

Also, from $m = 2g + 1$, we obtain $\frac{m+2}{2} = \frac{(2g+1)+2}{2} = (g+1) + \frac{1}{2}$. Hence,

$$\left\lfloor \frac{m+2}{2} \right\rfloor = \left\lfloor (g+1) + \frac{1}{2} \right\rfloor = g+1 \quad (\text{by (8) (applied to } n = g+1)).$$

Comparing this with

$$\left(\underbrace{m}_{=2g+1} + 1 \right) - \underbrace{\left\lfloor \frac{(m-1)+2}{2} \right\rfloor}_{=g+1} = (2g+1+1) - (g+1) = g+1,$$

we find $(m+1) - \left\lfloor \frac{(m-1)+2}{2} \right\rfloor = \left\lfloor \frac{m+2}{2} \right\rfloor$. Thus, (10) is proven in Case 2.

We thus have proven (10) in each of the two Cases 1 and 2. Thus, (10) always holds.]

Now, (9) becomes

$$\sum_{k=0}^m (-1)^k (k+1) = (-1)^m \underbrace{\left((m+1) - \left\lfloor \frac{(m-1)+2}{2} \right\rfloor \right)}_{\substack{= \left\lfloor \frac{m+2}{2} \right\rfloor \\ (\text{by (10)})}} = (-1)^m \left\lfloor \frac{m+2}{2} \right\rfloor.$$

In other words, Exercise 2 holds for $n = m$. This completes the induction step. Thus, Exercise 2 is proven by induction. \square

Let me stress that the above solution of Exercise 2 was almost completely straightforward. The only step that might have taken some creativity was to distinguish the two cases based on whether m is even or odd in the proof of (10). But this, too, has a clear motivation: It allows us to get rid of the floor function, which is the only thing preventing both sides of (10) from being explicit polynomials in m .

It is clear that the floors $\left\lfloor \frac{(m-1)+2}{2} \right\rfloor$ and $\left\lfloor \frac{m+2}{2} \right\rfloor$ can be rewritten without the floor function if m is even, and also (differently) if m is odd; thus, treating these two cases separately becomes completely natural.

Remark 0.11. The floor function has its own share of curious properties (see, e.g., its Wikipedia page). One of these is the identity

$$\lfloor x \rfloor + \left\lfloor x + \frac{1}{2} \right\rfloor = \lfloor 2x \rfloor \quad \text{for every } x \in \mathbb{R}. \quad (11)$$

This is actually a particular case of Hermite's identity, which states that for every $x \in \mathbb{R}$ and every positive integer n , we have

$$\sum_{k=0}^{n-1} \left\lfloor x + \frac{k}{n} \right\rfloor = \lfloor nx \rfloor.$$

Convince yourself that (10) can easily be derived (without distinguishing between any cases!) from (11).

Second solution to Exercise 2. We notice that

$$\begin{aligned} & \sum_{k=0}^n (-1)^k (k+1) \\ &= (-1)^0 1 + (-1)^1 2 + (-1)^2 3 + (-1)^3 4 + \cdots + (-1)^n (n+1) \\ &= 1 - 2 + 3 - 4 \pm \cdots + (-1)^n (n+1). \end{aligned} \quad (12)$$

Notice that the sign of the last addend on the right hand side depends on whether n is even or odd. Thus, we distinguish between the following two cases:

Case 1: The integer n is even.

Case 2: The integer n is odd.

Let us first consider Case 1. In this case, the integer n is even. Thus, $(-1)^n = 1$. Hence, (12) becomes

$$\begin{aligned} & \sum_{k=0}^n (-1)^k (k+1) \\ &= 1 - 2 + 3 - 4 \pm \cdots + \underbrace{(-1)^n}_{=1} (n+1) \\ &= 1 - 2 + 3 - 4 \pm \cdots + (n+1) \\ &= \underbrace{(1-2)}_{=-1} + \underbrace{(3-4)}_{=-1} + \underbrace{(5-6)}_{=-1} + \cdots + \underbrace{((n-1)-n)}_{=-1} + (n+1) \\ &= \underbrace{((-1) + (-1) + (-1) + \cdots + (-1))}_{\substack{n/2 \text{ addends} \\ =n/2 \cdot (-1) = -n/2}} + (n+1) \\ &= -n/2 + (n+1) = n/2 + 1. \end{aligned} \quad (13)$$

But n is even; thus, $n = 2g$ for some $g \in \mathbb{Z}$. Consider this g . From $n = 2g$, we

obtain $\frac{n+2}{2} = \frac{2g+2}{2} = g+1$. Hence,

$$\left\lfloor \frac{n+2}{2} \right\rfloor = \lfloor g+1 \rfloor = g+1$$

(by (7) (applied to $g+1$ instead of n)). Hence,

$$\underbrace{(-1)^n}_{=1} \underbrace{\left\lfloor \frac{n+2}{2} \right\rfloor}_{=g+1} = \underbrace{g}_{\substack{=n/2 \\ \text{(since } n=2g)}} + 1 = n/2 + 1.$$

Comparing this with (13), we obtain $\sum_{k=0}^n (-1)^k (k+1) = (-1)^n \left\lfloor \frac{n+2}{2} \right\rfloor$. Hence,

Exercise 2 is solved in Case 1.

Let us next consider Case 2. In this case, the integer n is odd. Thus, $(-1)^n = -1$. Hence, (12) becomes

$$\begin{aligned} & \sum_{k=0}^n (-1)^k (k+1) \\ &= 1 - 2 + 3 - 4 \pm \cdots + \underbrace{(-1)^n}_{=-1} (n+1) \\ &= 1 - 2 + 3 - 4 \pm \cdots - (n+1) \\ &= \underbrace{(1-2)}_{=-1} + \underbrace{(3-4)}_{=-1} + \underbrace{(5-6)}_{=-1} + \cdots + \underbrace{(n-(n+1))}_{=-1} \\ &= \underbrace{((-1) + (-1) + (-1) + \cdots + (-1))}_{(n+1)/2 \text{ addends}} \\ &= (n+1)/2 \cdot (-1) = -(n+1)/2. \end{aligned} \tag{14}$$

But n is odd; thus, $n = 2g+1$ for some $g \in \mathbb{Z}$. Consider this g . From $n = 2g+1$, we obtain $\frac{n+2}{2} = \frac{(2g+1)+2}{2} = (g+1) + \frac{1}{2}$. Hence,

$$\left\lfloor \frac{n+2}{2} \right\rfloor = \left\lfloor (g+1) + \frac{1}{2} \right\rfloor = g+1$$

(by (8) (applied to $g+1$ instead of n)). Hence,

$$\underbrace{(-1)^n}_{=-1} \underbrace{\left\lfloor \frac{n+2}{2} \right\rfloor}_{=g+1} = - \left(\underbrace{g}_{\substack{=(n-1)/2 \\ \text{(since } n=2g+1)}} + 1 \right) = -((n-1)/2 + 1) = -(n+1)/2.$$

Comparing this with (14), we obtain $\sum_{k=0}^n (-1)^k (k+1) = (-1)^n \left\lfloor \frac{n+2}{2} \right\rfloor$. Hence, Exercise 2 is solved in Case 2.

We thus have solved Exercise 2 in both Cases 1 and 2. Hence, Exercise 2 always holds. \square

0.3. Lemmas for the Sierpinski gasket appearing in Pascal's triangle

Exercise 3. Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

(a) Prove that $\binom{2a}{2b} \equiv \binom{a}{b} \pmod{2}$.

(b) Prove that $\binom{2a+1}{2b} \equiv \binom{a}{b} \pmod{2}$.

(c) Prove that $\binom{2a}{2b+1} \equiv 0 \pmod{2}$.

(d) Prove that $\binom{2a+1}{2b+1} \equiv \binom{a}{b} \pmod{2}$.

[**Hint:** Prove all four parts simultaneously by an induction on a , using Proposition 0.4.]

Before we solve this exercise, we make our life a bit easier by stating explicit formulas for binomial coefficients of the form $\binom{0}{b}$ and $\binom{1}{b}$ for arbitrary $b \in \mathbb{Z}$. (These are the least interesting binomial coefficients around – but we want to have them at our disposal.)

We shall use the *Iverson bracket notation*: If \mathcal{A} is any logical statement, then the *truth value* of \mathcal{A} is defined to be the integer

$$\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases} \in \{0, 1\}.$$

This truth value is denoted by $[\mathcal{A}]$. For example, $[1 + 1 = 2] = 1$ (since $1 + 1 = 2$ is true), whereas $[1 + 1 = 1] = 0$ (since $1 + 1 = 1$ is false).

Lemma 0.12. Let $b \in \mathbb{Z}$.

(a) We have $\binom{0}{b} = [b = 0]$.

(b) We have $\binom{1}{b} = [b \in \{0, 1\}]$.

The proof of this lemma is completely straightforward yet takes up a lot of space. Sorry for the waste of paper:

Proof of Lemma 0.12. (a) We are in one of the following three cases:

Case 1: We have $b < 0$.

Case 2: We have $b = 0$.

Case 3: We have $b > 0$.

Let us first consider Case 1. In this case, we have $b < 0$. Hence, $b \notin \mathbb{N}$, so that $b \in \mathbb{Q} \setminus \mathbb{N}$, and thus $\binom{0}{b} = 0$ (by Definition 0.3 (b)). But we don't have $b = 0$ (since we have $b < 0$); thus, $[b = 0] = 0$. Comparing this with $\binom{0}{b} = 0$, we obtain $\binom{0}{b} = [b = 0]$. Thus, Lemma 0.12 (a) is proven in Case 1.

Let us now consider Case 2. In this case, we have $b = 0$. Thus, $\binom{0}{b} = \binom{0}{0} = 1$. Comparing this with $[b = 0] = 1$ (since we have $b = 0$), we obtain $\binom{0}{b} = [b = 0]$. Thus, Lemma 0.12 (a) is proven in Case 2.

Let us finally consider Case 3. In this case, we have $b > 0$. Thus, $0 < b$. Therefore, Proposition 0.8 (applied to $m = 0$ and $n = b$) yields $\binom{0}{b} = 0$. But we don't have $b = 0$ (since we have $b > 0$); thus, $[b = 0] = 0$. Comparing this with $\binom{0}{b} = 0$, we obtain $\binom{0}{b} = [b = 0]$. Thus, Lemma 0.12 (a) is proven in Case 3.

We thus have proven Lemma 0.12 (a) in all three Cases 1, 2 and 3. Hence, Lemma 0.12 (a) always holds.

(b) We have $b \in \mathbb{Z}$. Thus, we are in one of the following four cases:

Case 1: We have $b < 0$.

Case 2: We have $b = 0$.

Case 3: We have $b = 1$.

Case 4: We have $b > 1$.

Let us first consider Case 1. In this case, we have $b < 0$. Hence, $b \notin \mathbb{N}$, so that $b \in \mathbb{Q} \setminus \mathbb{N}$, and thus $\binom{1}{b} = 0$ (by Definition 0.3 (b)). But we don't have $b \in \{0, 1\}$ (since we have $b < 0$); thus, $[b \in \{0, 1\}] = 0$. Comparing this with $\binom{1}{b} = 0$, we obtain $\binom{1}{b} = [b \in \{0, 1\}]$. Thus, Lemma 0.12 (b) is proven in Case 1.

Let us now consider Case 2. In this case, we have $b = 0$. Thus, $\binom{1}{b} = \binom{1}{0} = 1$. Comparing this with $[b \in \{0, 1\}] = 1$ (since we have $b = 0 \in \{0, 1\}$), we obtain $\binom{1}{b} = [b \in \{0, 1\}]$. Thus, Lemma 0.12 (b) is proven in Case 2.

Let us now consider Case 3. In this case, we have $b = 1$. Thus,

$$\binom{1}{b} = \binom{1}{1} = \frac{1}{1!} \quad \left(\text{by the definition of } \binom{1}{1} \right) \\ = 1.$$

Comparing this with $[b \in \{0, 1\}] = 1$ (since we have $b = 1 \in \{0, 1\}$), we obtain $\binom{1}{b} = [b \in \{0, 1\}]$. Thus, Lemma 0.12 **(b)** is proven in Case 3.

Let us finally consider Case 4. In this case, we have $b > 1$. Thus, $1 < b$. Therefore, Proposition 0.8 (applied to $m = 1$ and $n = b$) yields $\binom{1}{b} = 0$. But we don't have $b \in \{0, 1\}$ (since we have $b > 1$); thus, $[b \in \{0, 1\}] = 0$. Comparing this with $\binom{1}{b} = 0$, we obtain $\binom{1}{b} = [b \in \{0, 1\}]$. Thus, Lemma 0.12 **(b)** is proven in Case 4.

We thus have proven Lemma 0.12 **(b)** in all four Cases 1, 2, 3 and 4. Hence, Lemma 0.12 **(b)** always holds. \square

Solution to Exercise 3. Forget that we fixed a and b . We claim the following:

$$\text{Claim 1: Let } a \in \mathbb{N} \text{ and } b \in \mathbb{Z}. \text{ Then, we have } \binom{2a}{2b} \equiv \binom{a}{b} \pmod{2} \\ \text{and } \binom{2a+1}{2b} \equiv \binom{a}{b} \pmod{2} \text{ and } \binom{2a}{2b+1} \equiv 0 \pmod{2} \text{ and } \binom{2a+1}{2b+1} \equiv \\ \binom{a}{b} \pmod{2}.$$

(This Claim 1 combines the statements of all four parts of Exercise 3 into one large statement, and also extends the domain for b from \mathbb{N} to \mathbb{Z} . The latter is a minor trick; it will slightly simplify the proof below. The former is crucial to our proof below: We will prove Claim 1 by induction on a . In the induction step (from $a = c - 1$ to $a = c$), we shall use the induction hypothesis in a way that wouldn't be possible if we were proving parts **(a)**, **(b)**, **(c)** and **(d)** of the exercise separately (because we would be using the induction hypothesis of one of them in the induction step of the other); instead, we need the four parts together so they can "help each other out". There is a way to solve the four parts of Exercise 3 separately, but it is more complicated than what we shall do below.)

[*Proof of Claim 1:* We shall prove Claim 1 by induction on a :

Induction base: We are going to prove that Claim 1 holds for $a = 0$.

Let $a \in \mathbb{N}$ and $b \in \mathbb{Z}$ be such that $a = 0$. From $a = 0$, we obtain

$$\binom{a}{b} = \binom{0}{b} = [b = 0] \tag{15}$$

(by Lemma 0.12 **(a)**).

We have $a = 0$, thus $2a = 0$. Hence,

$$\begin{aligned} \binom{2a}{2b} &= \binom{0}{2b} = [2b = 0] \\ &\quad \text{(by Lemma 0.12 (a) (applied to } 2b \text{ instead of } b)) \\ &= [b = 0] \quad \text{(since the condition } 2b = 0 \text{ is equivalent to } b = 0) \\ &= \binom{a}{b} \quad \text{(by (15)).} \end{aligned}$$

Thus, of course, $\binom{2a}{2b} \equiv \binom{a}{b} \pmod{2}$.

We have $a = 0$, thus $2a + 1 = 2 \cdot 0 + 1 = 1$. Hence,

$$\begin{aligned} \binom{2a+1}{2b} &= \binom{1}{2b} = [2b \in \{0, 1\}] \\ &\quad \text{(by Lemma 0.12 (b) (applied to } 2b \text{ instead of } b)) \\ &= [2b = 0] \\ &\quad \left(\begin{array}{l} \text{since the condition } 2b \in \{0, 1\} \text{ is equivalent to } 2b = 0 \\ \text{(because } 2b \text{ cannot be } 1 \text{ (since } 2b \text{ is even but } 1 \text{ is not))} \end{array} \right) \\ &= [b = 0] \quad \text{(since the condition } 2b = 0 \text{ is equivalent to } b = 0) \\ &= \binom{a}{b} \quad \text{(by (15)).} \end{aligned}$$

Thus, of course, $\binom{2a+1}{2b} \equiv \binom{a}{b} \pmod{2}$.

We have $2a = 0$, thus

$$\begin{aligned} \binom{2a}{2b+1} &= \binom{0}{2b+1} = [2b+1 = 0] \\ &\quad \text{(by Lemma 0.12 (a) (applied to } 2b+1 \text{ instead of } b)) \\ &= 0 \end{aligned}$$

(since $2b+1 = 0$ is false (since $2b+1$ is an odd integer, but 0 is not)). Thus, of

course, $\binom{2a}{2b+1} \equiv 0 \pmod{2}$.

We have $2a + 1 = 1$. Hence,

$$\begin{aligned}
 \binom{2a+1}{2b+1} &= \binom{1}{2b+1} = [2b+1 \in \{0, 1\}] \\
 &\quad (\text{by Lemma 0.12 (b) (applied to } 2b+1 \text{ instead of } b)) \\
 &= [2b+1 = 1] \\
 &\quad \left(\begin{array}{l} \text{since the condition } 2b+1 \in \{0, 1\} \text{ is equivalent to } 2b+1 = 1 \\ \text{(because } 2b+1 \text{ cannot be 0 (since } 2b+1 \text{ is odd but 0 is not))} \end{array} \right) \\
 &= [b = 0] \quad (\text{since the condition } 2b+1 = 1 \text{ is equivalent to } b = 0) \\
 &= \binom{a}{b} \quad (\text{by (15)}).
 \end{aligned}$$

Thus, of course, $\binom{2a+1}{2b+1} \equiv \binom{a}{b} \pmod{2}$.

We thus have proven the four congruences $\binom{2a}{2b} \equiv \binom{a}{b} \pmod{2}$ and $\binom{2a+1}{2b} \equiv \binom{a}{b} \pmod{2}$ and $\binom{a}{b} \pmod{2}$ and $\binom{2a}{2b+1} \equiv 0 \pmod{2}$ and $\binom{2a+1}{2b+1} \equiv \binom{a}{b} \pmod{2}$. In other words, Claim 1 holds. Thus, we have shown that Claim 1 holds for $a = 0$. This completes the induction base.

Induction step: Let c be a positive integer. Assume (as the induction hypothesis) that Claim 1 holds for $a = c - 1$. We must show that Claim 1 holds for $a = c$.

We have assumed that Claim 1 holds for $a = c - 1$. In other words, for every $b \in \mathbb{Z}$, we have

$$\binom{2(c-1)}{2b} \equiv \binom{c-1}{b} \pmod{2}$$

and

$$\binom{2(c-1)+1}{2b} \equiv \binom{c-1}{b} \pmod{2} \tag{16}$$

and

$$\binom{2(c-1)}{2b+1} \equiv 0 \pmod{2}$$

and

$$\binom{2(c-1)+1}{2b+1} \equiv \binom{c-1}{b} \pmod{2}. \tag{17}$$

Now, let $b \in \mathbb{Z}$. Then, $2c - 1 = 2(c - 1) + 1$. Thus,

$$\binom{2c-1}{2b} = \binom{2(c-1)+1}{2b} \equiv \binom{c-1}{b} \pmod{2} \tag{18}$$

(by (16)). From $2c - 1 = 2(c - 1) + 1$, we also obtain

$$\binom{2c-1}{2b+1} = \binom{2(c-1)+1}{2b+1} \equiv \binom{c-1}{b} \pmod{2} \tag{19}$$

(by (17)). Finally, from $2c - 1 = 2(c - 1) + 1$ and $2b - 1 = 2(b - 1) + 1$, we obtain

$$\binom{2c - 1}{2b - 1} = \binom{2(c - 1) + 1}{2(b - 1) + 1} \equiv \binom{c - 1}{b - 1} \pmod{2} \quad (20)$$

(by (17) (applied to $b - 1$ instead of b)). (Notice that it is perfectly kosher to apply (17) to $b - 1$ instead of b : In fact, we know that (17) holds for each $b \in \mathbb{Z}$, which needs not be equal to the b that we are currently considering!)

Proposition 0.4 (applied to $n = c$ and $k = b$) yields

$$\binom{c}{b} = \binom{c - 1}{b - 1} + \binom{c - 1}{b}. \quad (21)$$

Now, Proposition 0.4 (applied to $n = 2c$ and $k = 2b$) yields

$$\begin{aligned} \binom{2c}{2b} &= \underbrace{\binom{2c - 1}{2b - 1}}_{\substack{\equiv \binom{c - 1}{b - 1} \pmod{2} \\ \text{(by (20))}}} + \underbrace{\binom{2c - 1}{2b}}_{\substack{\equiv \binom{c - 1}{b} \pmod{2} \\ \text{(by (18))}}} \\ &\equiv \binom{c - 1}{b - 1} + \binom{c - 1}{b} = \binom{c}{b} \pmod{2} \end{aligned} \quad (22)$$

(by (21)). Furthermore, Proposition 0.4 (applied to $n = 2c$ and $k = 2b + 1$) yields

$$\begin{aligned} \binom{2c}{2b + 1} &= \underbrace{\binom{2c - 1}{2b + 1 - 1}}_{\substack{\equiv \binom{c - 1}{b} \pmod{2} \\ \text{(by (18))}}} + \underbrace{\binom{2c - 1}{2b + 1}}_{\substack{\equiv \binom{c - 1}{b} \pmod{2} \\ \text{(by (19))}}} \\ &\equiv \binom{c - 1}{b} + \binom{c - 1}{b} = 2 \binom{c - 1}{b} \equiv 0 \pmod{2}. \end{aligned} \quad (23)$$

Now, forget that we fixed b . We thus have proven the congruences (22) and (23) for each $b \in \mathbb{Z}$.

Let us fix $b \in \mathbb{Z}$ again. We can apply (23) to $b - 1$ instead of b (because we have proven the congruence (23) for each $b \in \mathbb{Z}$)¹. As a result, we obtain

$$\binom{2c}{2(b - 1) + 1} \equiv 0 \pmod{2}.$$

In view of $2(b - 1) + 1 = 2b - 1$, this rewrites as

$$\binom{2c}{2b - 1} \equiv 0 \pmod{2}. \quad (24)$$

¹This is the reason why we “unfixed” b and then fixed b again: We wanted to apply (23) to a different value of b .

Next, Proposition 0.4 (applied to $n = 2c + 1$ and $k = 2b$) yields

$$\begin{aligned} \binom{2c+1}{2b} &= \underbrace{\binom{2c+1-1}{2b-1}}_{\substack{= \binom{2c}{2b-1} \equiv 0 \pmod{2} \\ \text{(by (24))}}} + \underbrace{\binom{2c+1-1}{2b}}_{\substack{= \binom{2c}{2b} \equiv \binom{c}{b} \pmod{2} \\ \text{(by (22))}}} \\ &\equiv 0 + \binom{c}{b} = \binom{c}{b} \pmod{2}. \end{aligned} \tag{25}$$

Finally, Proposition 0.4 (applied to $n = 2c + 1$ and $k = 2b + 1$) yields

$$\begin{aligned} \binom{2c+1}{2b+1} &= \underbrace{\binom{2c+1-1}{2b+1-1}}_{\substack{= \binom{2c}{2b} \equiv \binom{c}{b} \pmod{2} \\ \text{(by (22))}}} + \underbrace{\binom{2c+1-1}{2b+1}}_{\substack{= \binom{2c}{2b+1} \equiv 0 \pmod{2} \\ \text{(by (23))}}} \\ &\equiv \binom{c}{b} + 0 = \binom{c}{b} \pmod{2}. \end{aligned} \tag{26}$$

Now, forget that we fixed b . We thus have proven the congruences (25) and (26) for each $b \in \mathbb{Z}$.

Hence, altogether, we have proven the four congruences (22), (25), (23) and (26) for each $b \in \mathbb{Z}$. In other words, we have shown that for every $b \in \mathbb{Z}$, we have $\binom{2c}{2b} \equiv \binom{c}{b} \pmod{2}$ and $\binom{2c+1}{2b} \equiv \binom{c}{b} \pmod{2}$ and $\binom{2c}{2b+1} \equiv 0 \pmod{2}$ and $\binom{2c+1}{2b+1} \equiv \binom{c}{b} \pmod{2}$. In other words, Claim 1 holds for $a = c$. This completes the induction step. Thus, Claim 1 is proven.]

Clearly, Exercise 3 follows immediately from Claim 1. \square

Remark 0.13. Exercise 3 is a particular case (namely, the case $p = 2$) of the following result:

Theorem 0.14 (Lucas's theorem). Let p be a prime. Let a and b be two integers. Let c and d be two elements of $\{0, 1, \dots, p-1\}$. Then,

$$\binom{ap+c}{bp+d} \equiv \binom{a}{b} \binom{c}{d} \pmod{p}.$$

It is not too hard to prove Theorem 0.14 using some further properties of binomial coefficients (most importantly, the Vandermonde convolution identity) and some basic facts about prime numbers (mainly: if a prime p divides a product cd of two integers c and d , then $p \mid c$ or $p \mid d$). See, e.g., [Grinbe17] for such a proof.

Notice that Theorem 0.14 shows that the conditions " $a \in \mathbb{N}$ and $b \in \mathbb{N}$ " in Exercise 3 can be loosened to " $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$ ".

Exercise 4. Let $n \in \mathbb{N}$. Let a and b be two elements of $\{0, 1, \dots, 2^n - 1\}$. Prove that

$$\binom{2^n + a}{b} \equiv \binom{a}{b} \pmod{2} \quad \text{and}$$

$$\binom{2^n + a}{2^n + b} \equiv \binom{a}{b} \pmod{2}.$$

[Here, “ $\{0, 1, \dots, 2^n - 1\}$ ” means the set of all integers k satisfying $0 \leq k \leq 2^n - 1$.]

[**Hint:** Induction on n . You can use Exercise 3 here even if you have not solved it.]

Back in class, Exercise 4 helped us prove that Pascal’s triangle becomes a Sierpinski gasket (see, e.g., the Wikipedia) if its entries are replaced by their parities.

Solution to Exercise 4. We shall solve Exercise 4 by induction on n :

Induction base: It is easy to see that Exercise 4 holds for $n = 0$ ². This completes the induction base.

Induction step: Let $m \in \mathbb{N}$. Assume that Exercise 4 holds for $n = m$. We must prove that Exercise 4 holds for $n = m + 1$.

We have assumed that Exercise 4 holds for $n = m$. In other words, if a and b are two elements of $\{0, 1, \dots, 2^m - 1\}$, then

$$\binom{2^m + a}{b} \equiv \binom{a}{b} \pmod{2} \quad \text{and} \quad (27)$$

$$\binom{2^m + a}{2^m + b} \equiv \binom{a}{b} \pmod{2}. \quad (28)$$

²*Proof.* Assume that $n = 0$. We must prove that Exercise 4 holds.

We have $n = 0$, so that $2^n = 2^0 = 1$ and thus $2^n - 1 = 0$.

Let a and b be as in Exercise 4. Thus,

$$\begin{aligned} a \in \{0, 1, \dots, 2^n - 1\} &= \{0, 1, \dots, 0\} && \text{(since } 2^n - 1 = 0\text{)} \\ &= \{0\}, \end{aligned}$$

so that $a = 0$. Similarly, $b = 0$. From $a = 0$ and $b = 0$, we obtain $\binom{a}{b} = \binom{0}{0} = 1$. But from $n = 0$, $a = 0$ and $b = 0$, we obtain

$$\binom{2^n + a}{b} = \binom{2^0 + 0}{0} = \binom{1}{0} = 1 \equiv 1 = \binom{a}{b} \pmod{2}$$

and

$$\binom{2^n + a}{2^n + b} = \binom{2^0 + 0}{2^0 + 0} = \binom{1}{1} = 1 \equiv 1 = \binom{a}{b} \pmod{2}.$$

Thus, Exercise 4 is solved (for our values of n , a and b). We thus have shown that Exercise 4 holds for $n = 0$.

We first show the following simple observation:

Observation 1: Let $g \in \{0, 1, \dots, 2^{m+1} - 1\}$.

(a) If g is even, then there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $g = 2h$.

(b) If g is odd, then there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $g = 2h - 1$.

[*Proof of Observation 1:* **(a)** Assume that g is even. Thus, $g = 2c$ for some $c \in \mathbb{Z}$. Consider this c . We have $2c = g \in \{0, 1, \dots, 2^{m+1} - 1\}$, so that $0 \leq 2c \leq 2^{m+1} - 1 < 2^{m+1} = 2 \cdot 2^m$. From $0 \leq 2c$, we obtain $0 \leq c$. From $2c < 2 \cdot 2^m$, we obtain $c < 2^m$, so that $c \leq 2^m - 1$ (since c is an integer). Combining this with $0 \leq c$, we obtain $0 \leq c \leq 2^m - 1$, so that $c \in \{0, 1, \dots, 2^m - 1\}$. Thus, there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $g = 2h$ (namely, $h = c$). This proves Observation 1 **(a)**.

(b) Assume that g is odd. Thus, $g = 2c + 1$ for some $c \in \mathbb{Z}$. Consider this c . We have $2c + 1 = g \in \{0, 1, \dots, 2^{m+1} - 1\}$, so that $0 \leq 2c + 1 \leq 2^{m+1} - 1$. Hence, $2c + 1 \geq 0$. But $2c + 1 \neq 0$ (since $2c + 1$ is odd, but 0 is even). Combining this with $2c + 1 \geq 0$, we obtain $2c + 1 > 0$. Since $2c + 1$ is an integer, this yields $2c + 1 \geq 0 + 1$, so that $2c \geq 0$ and thus $c \geq 0$. Also, $2c + 1 \leq 2^{m+1} - 1$, so that $2c \leq 2^{m+1} - 1 - 1 = \underbrace{2^{m+1}}_{=2 \cdot 2^m} - 2 = 2 \cdot 2^m - 2 = 2 \cdot (2^m - 1)$ and thus $c \leq 2^m - 1$.

Combining this with $c \geq 0$, we obtain $0 \leq c \leq 2^m - 1$, so that $c \in \{0, 1, \dots, 2^m - 1\}$. Thus, there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $g = 2h + 1$ (namely, $h = c$). This proves Observation 1 **(b)**. Thus, Observation 1 is fully proven.]

Now, let a and b be two elements of $\{0, 1, \dots, 2^{m+1} - 1\}$. We are going to prove the two congruences

$$\binom{2^{m+1} + a}{b} \equiv \binom{a}{b} \pmod{2} \quad \text{and} \quad (29)$$

$$\binom{2^{m+1} + a}{2^{m+1} + b} \equiv \binom{a}{b} \pmod{2}. \quad (30)$$

We are in one of the following two cases:

Case 1: The integer a is even.

Case 2: The integer a is odd.

Let us first consider Case 1. In this case, the integer a is even. Thus, Observation 1 **(a)** (applied to $g = a$) shows that there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $a = 2h$. Consider this h , and denote it by c . Thus, $c \in \{0, 1, \dots, 2^m - 1\}$ satisfies $a = 2c$.

We are in one of the following two subcases:

Subcase 1.1: The integer b is even.

Subcase 1.2: The integer b is odd.

Let us first consider Subcase 1.1. In this case, the integer b is even. Thus, Observation 1 (a) (applied to $g = b$) shows that there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $b = 2h$. Consider this h , and denote it by d . Thus, $d \in \{0, 1, \dots, 2^m - 1\}$ satisfies $b = 2d$.

From $a = 2c$ and $b = 2d$, we obtain

$$\binom{a}{b} = \binom{2c}{2d} \equiv \binom{c}{d} \pmod{2} \quad (31)$$

(by Exercise 3 (a) (applied to c and d instead of a and b)).

From $2^{m+1} = 2 \cdot 2^m$ and $a = 2c$, we obtain $2^{m+1} + a = 2 \cdot 2^m + 2c = 2(2^m + c)$.

From $2^{m+1} = 2 \cdot 2^m$ and $b = 2d$, we obtain $2^{m+1} + b = 2 \cdot 2^m + 2d = 2(2^m + d)$.

From $2^{m+1} + a = 2(2^m + c)$ and $b = 2d$, we obtain

$$\begin{aligned} \binom{2^{m+1} + a}{b} &= \binom{2(2^m + c)}{2d} \\ &\equiv \binom{2^m + c}{d} \quad \left(\text{by Exercise 3 (a) (applied to } 2^m + c \text{ and } d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{c}{d} \quad \left(\text{by (27) (applied to } c \text{ and } d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{a}{b} \pmod{2} \quad \left(\text{by (31)} \right). \end{aligned}$$

Thus, the congruence (29) holds.

From $2^{m+1} + a = 2(2^m + c)$ and $2^{m+1} + b = 2(2^m + d)$, we obtain

$$\begin{aligned} \binom{2^{m+1} + a}{2^{m+1} + b} &= \binom{2(2^m + c)}{2(2^m + d)} \\ &\equiv \binom{2^m + c}{2^m + d} \quad \left(\text{by Exercise 3 (a) (applied to } 2^m + c \text{ and } 2^m + d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{c}{d} \quad \left(\text{by (28) (applied to } c \text{ and } d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{a}{b} \pmod{2} \quad \left(\text{by (31)} \right). \end{aligned}$$

Thus, the congruence (30) holds.

We thus have proven the congruences (29) and (30) in Subcase 1.1.

We still need to deal with Subcase 1.2, as well as Case 2 (which we are going to split into two Subcases again). This will be mostly analogous to what we have done in Subcase 1.1 above.

Let us consider Subcase 1.2. In this case, the integer b is odd. Thus, Observation 1 (a) (applied to $g = b$) shows that there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $b = 2h + 1$. Consider this h , and denote it by d . Thus, $d \in \{0, 1, \dots, 2^m - 1\}$ satisfies $b = 2d + 1$.

From $a = 2c$ and $b = 2d + 1$, we obtain

$$\binom{a}{b} = \binom{2c}{2d+1} \equiv 0 \pmod{2} \quad (32)$$

(by Exercise 3 (c) (applied to c and d instead of a and b)).

From $2^{m+1} = 2 \cdot 2^m$ and $a = 2c$, we obtain $2^{m+1} + a = 2 \cdot 2^m + 2c = 2(2^m + c)$.

From $2^{m+1} = 2 \cdot 2^m$ and $b = 2d + 1$, we obtain $2^{m+1} + b = 2 \cdot 2^m + (2d + 1) = 2(2^m + d) + 1$.

From $2^{m+1} + a = 2(2^m + c)$ and $b = 2d + 1$, we obtain

$$\begin{aligned} \binom{2^{m+1} + a}{b} &= \binom{2(2^m + c)}{2d + 1} \\ &\equiv 0 \quad \left(\begin{array}{l} \text{by Exercise 3 (c) (applied to } 2^m + c \text{ and } d \\ \text{instead of } a \text{ and } b \end{array} \right) \\ &\equiv \binom{a}{b} \pmod{2} \quad (\text{by (32)}). \end{aligned}$$

Thus, the congruence (29) holds.

From $2^{m+1} + a = 2(2^m + c)$ and $2^{m+1} + b = 2(2^m + d) + 1$, we obtain

$$\begin{aligned} \binom{2^{m+1} + a}{2^{m+1} + b} &= \binom{2(2^m + c)}{2(2^m + d) + 1} \\ &\equiv 0 \quad \left(\begin{array}{l} \text{by Exercise 3 (c) (applied to } 2^m + c \text{ and } 2^m + d \\ \text{instead of } a \text{ and } b \end{array} \right) \\ &\equiv \binom{a}{b} \pmod{2} \quad (\text{by (32)}). \end{aligned}$$

Thus, the congruence (30) holds.

We thus have proven the congruences (29) and (30) in Subcase 1.2.

We now have proven the congruences (29) and (30) in both Subcases 1.1 and 1.2. Since these two Subcases cover Case 1, we thus know that the congruences (29) and (30) hold in Case 1.

Let us now consider Case 2. In this case, the integer a is odd. Thus, Observation 1 (b) (applied to $g = a$) shows that there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $a = 2h + 1$. Consider this h , and denote it by c . Thus, $c \in \{0, 1, \dots, 2^m - 1\}$ satisfies $a = 2c + 1$.

We are in one of the following two subcases:

Subcase 2.1: The integer b is even.

Subcase 2.2: The integer b is odd.

Let us first consider Subcase 2.1. In this case, the integer b is even. Thus, Observation 1 (a) (applied to $g = b$) shows that there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $b = 2h$. Consider this h , and denote it by d . Thus, $d \in \{0, 1, \dots, 2^m - 1\}$ satisfies $b = 2d$.

From $a = 2c + 1$ and $b = 2d$, we obtain

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 2c + 1 \\ 2d \end{pmatrix} \equiv \begin{pmatrix} c \\ d \end{pmatrix} \pmod{2} \quad (33)$$

(by Exercise 3 **(b)** (applied to c and d instead of a and b)).

From $2^{m+1} = 2 \cdot 2^m$ and $a = 2c + 1$, we obtain $2^{m+1} + a = 2 \cdot 2^m + (2c + 1) = 2(2^m + c) + 1$.

From $2^{m+1} = 2 \cdot 2^m$ and $b = 2d$, we obtain $2^{m+1} + b = 2 \cdot 2^m + 2d = 2(2^m + d)$.

From $2^{m+1} + a = 2(2^m + c) + 1$ and $b = 2d$, we obtain

$$\begin{aligned} \begin{pmatrix} 2^{m+1} + a \\ b \end{pmatrix} &= \begin{pmatrix} 2(2^m + c) + 1 \\ 2d \end{pmatrix} \\ &\equiv \begin{pmatrix} 2^m + c \\ d \end{pmatrix} && \left(\begin{array}{l} \text{by Exercise 3 (b) (applied to } 2^m + c \text{ and } d \\ \text{instead of } a \text{ and } b \end{array} \right) \\ &\equiv \begin{pmatrix} c \\ d \end{pmatrix} && \left(\text{by (27) (applied to } c \text{ and } d \text{ instead of } a \text{ and } b \right) \\ &\equiv \begin{pmatrix} a \\ b \end{pmatrix} \pmod{2} && \left(\text{by (33)}. \right) \end{aligned}$$

Thus, the congruence (29) holds.

From $2^{m+1} + a = 2(2^m + c) + 1$ and $2^{m+1} + b = 2(2^m + d)$, we obtain

$$\begin{aligned} \begin{pmatrix} 2^{m+1} + a \\ 2^{m+1} + b \end{pmatrix} &= \begin{pmatrix} 2(2^m + c) + 1 \\ 2(2^m + d) \end{pmatrix} \\ &\equiv \begin{pmatrix} 2^m + c \\ 2^m + d \end{pmatrix} && \left(\begin{array}{l} \text{by Exercise 3 (b) (applied to } 2^m + c \text{ and } 2^m + d \\ \text{instead of } a \text{ and } b \end{array} \right) \\ &\equiv \begin{pmatrix} c \\ d \end{pmatrix} && \left(\text{by (28) (applied to } c \text{ and } d \text{ instead of } a \text{ and } b \right) \\ &\equiv \begin{pmatrix} a \\ b \end{pmatrix} \pmod{2} && \left(\text{by (33)}. \right) \end{aligned}$$

Thus, the congruence (30) holds.

We thus have proven the congruences (29) and (30) in Subcase 2.1.

Let us now consider Subcase 2.2. In this case, the integer b is odd. Thus, Observation 1 **(b)** (applied to $g = b$) shows that there exists some $h \in \{0, 1, \dots, 2^m - 1\}$ such that $b = 2h + 1$. Consider this h , and denote it by d . Thus, $d \in \{0, 1, \dots, 2^m - 1\}$ satisfies $b = 2d + 1$.

From $a = 2c + 1$ and $b = 2d + 1$, we obtain

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 2c + 1 \\ 2d + 1 \end{pmatrix} \equiv \begin{pmatrix} c \\ d \end{pmatrix} \pmod{2} \quad (34)$$

(by Exercise 3 **(d)** (applied to c and d instead of a and b)).

From $2^{m+1} = 2 \cdot 2^m$ and $a = 2c + 1$, we obtain $2^{m+1} + a = 2 \cdot 2^m + (2c + 1) = 2(2^m + c) + 1$.

From $2^{m+1} = 2 \cdot 2^m$ and $b = 2d + 1$, we obtain $2^{m+1} + b = 2 \cdot 2^m + (2d + 1) = 2(2^m + d) + 1$.

From $2^{m+1} + a = 2(2^m + c) + 1$ and $b = 2d + 1$, we obtain

$$\begin{aligned} \binom{2^{m+1} + a}{b} &= \binom{2(2^m + c) + 1}{2d + 1} \\ &\equiv \binom{2^m + c}{d} \quad \left(\text{by Exercise 3 (d) (applied to } 2^m + c \text{ and } d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{c}{d} \quad \left(\text{by (27) (applied to } c \text{ and } d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{a}{b} \pmod{2} \quad \left(\text{by (34)}. \right) \end{aligned}$$

Thus, the congruence (29) holds.

From $2^{m+1} + a = 2(2^m + c) + 1$ and $2^{m+1} + b = 2(2^m + d) + 1$, we obtain

$$\begin{aligned} \binom{2^{m+1} + a}{2^{m+1} + b} &= \binom{2(2^m + c) + 1}{2(2^m + d) + 1} \\ &\equiv \binom{2^m + c}{2^m + d} \quad \left(\text{by Exercise 3 (d) (applied to } 2^m + c \text{ and } 2^m + d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{c}{d} \quad \left(\text{by (28) (applied to } c \text{ and } d \text{ instead of } a \text{ and } b \text{)} \right) \\ &\equiv \binom{a}{b} \pmod{2} \quad \left(\text{by (34)}. \right) \end{aligned}$$

Thus, the congruence (30) holds.

We thus have proven the congruences (29) and (30) in Subcase 2.2.

We now have proven the congruences (29) and (30) in both Subcases 2.1 and 2.2. Since these two Subcases cover Case 2, we thus know that the congruences (29) and (30) hold in Case 2.

We now have proven the congruences (29) and (30) in both Cases 1 and 2. Thus, the congruences (29) and (30) always hold.

Now, forget that we fixed a and b . We thus have shown that if a and b are two elements of $\{0, 1, \dots, 2^{m+1} - 1\}$, then the congruences (29) and (30) always hold. In other words, if a and b are two elements of $\{0, 1, \dots, 2^{m+1} - 1\}$, then

$$\begin{aligned} \binom{2^{m+1} + a}{b} &\equiv \binom{a}{b} \pmod{2} \quad \text{and} \\ \binom{2^{m+1} + a}{2^{m+1} + b} &\equiv \binom{a}{b} \pmod{2}. \end{aligned}$$

In other words, Exercise 4 holds for $n = m + 1$. This completes the induction step. The induction proof of Exercise 4 is thus complete. \square

0.4. More on Fibonacci numbers

Definition 0.15. The *Fibonacci sequence* is the sequence (f_0, f_1, f_2, \dots) of integers which is defined recursively by $f_0 = 0, f_1 = 1$, and

$$f_n = f_{n-1} + f_{n-2} \quad \text{for all } n \geq 2. \tag{35}$$

Its first terms are

$$\begin{array}{cccccc} f_0 = 0, & f_1 = 1, & f_2 = 1, & f_3 = 2, & f_4 = 3, & f_5 = 5, \\ f_6 = 8, & f_7 = 13, & f_8 = 21, & f_9 = 34, & f_{10} = 55, & \\ f_{11} = 89, & f_{12} = 144, & f_{13} = 233. & & & \end{array}$$

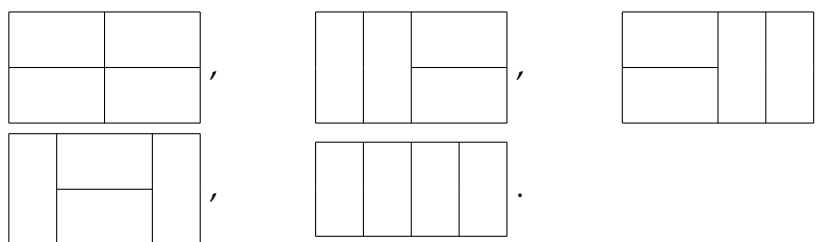
Exercise 5. Let $n \in \mathbb{N}$. Let $R_{n,2}$ denote the set $[n] \times [2]$, which we regard as a rectangle of width n and height 2 (by identifying the squares with pairs of coordinates). (Note: I might have been careless in class and confused width with height a few times. In case of doubt, follow the conventions just given.)

A *vertical domino* is a set of the form $\{(i, j), (i, j + 1)\}$ for some $i \in \mathbb{Z}$ and $j \in \mathbb{Z}$.

A *horizontal domino* is a set of the form $\{(i + 1, j), (i, j)\}$ for some $i \in \mathbb{Z}$ and $j \in \mathbb{Z}$.

A *domino tiling* of $R_{n,2}$ means a set of disjoint dominos (i.e., vertical dominos and horizontal dominos) whose union is $R_{n,2}$.

For example, there are 5 domino tilings of $R_{4,2}$, namely



Written as a set of dominos, the second of these tilings is

$$\{ \{(1, 1), (1, 2)\}, \{(2, 1), (2, 2)\}, \{(3, 1), (4, 1)\}, \{(3, 2), (4, 2)\} \}.$$

We have seen in class (January 17) that

$$\text{the number of domino tilings of } R_{n,2} \text{ is } f_{n+1}. \tag{36}$$

A domino tiling S of $R_{n,2}$ is said to be *axisymmetric* if reflecting it across the vertical axis of the rectangle $R_{n,2}$ leaves it unchanged. (Formally, if S is regarded as a set, it means that for every domino $\{(i, j), (i', j')\} \in S$, its “mirror domino” $\{(n + 1 - i, j), (n + 1 - i', j')\}$ is also in S .) For example, among the 5 domino tilings of $R_{4,2}$ listed above, exactly 3 are axisymmetric (namely, the first, the fourth and the fifth).

Let s_n be the number of axisymmetric domino tilings of $R_{n,2}$.

(a) Prove that $s_n = f_{(n+1)/2}$ if n is odd.

(b) Prove that $s_n = f_{n/2+2}$ if n is even.

Solution of Exercise 5 (sketched). (a) Assume that n is odd. Let $m = (n + 1) / 2$; this m is an element of $[n]$ (since n is odd). More precisely, m is the “middle” element of $[n]$ (that is, the set $[n]$ has as many elements $< m$ as it has elements $> m$). The m -th column of the rectangle $R_{n,2}$ (i.e., the subset $\{(m, 1), (m, 2)\}$) is the vertical axis of symmetry of this rectangle. Let us denote the vertical domino $\{(m, 1), (m, 2)\}$ (that is, the domino that falls along this m -th column) as M .

Every axisymmetric domino tiling of $R_{n,2}$ contains the domino M ³. Thus, every axisymmetric domino tiling of $R_{n,2}$ has the following form:

- The m -th column of $R_{n,2}$ is covered by the vertical domino M .
- The first $m - 1$ columns are covered by some dominos forming a domino tiling of $R_{m-1,2}$.
- The last $m - 1$ columns are covered by some dominos, namely by the reflections of the dominos covering the first $m - 1$ columns across the vertical axis of symmetry of $R_{n,2}$.

Thus, in order to construct an axisymmetric domino tiling of $R_{n,2}$, all we need to do is to choose a domino tiling of $R_{m-1,2}$. But (36) (applied to $m - 1$ instead of n) shows that the number of latter domino tilings is $f_{(m-1)+1} = f_m$. Thus, the number of axisymmetric domino tilings of $R_{n,2}$ is f_m as well. In other words, $s_n = f_m$ (since s_n is the number of axisymmetric domino tilings of $R_{n,2}$). In view of $m = (n + 1) / 2$, this rewrites as $s_n = f_{(n+1)/2}$. This solves Exercise 5 (a).

(b) Assume that n is even. Let $m = n/2$; this m is an element of $[n]$ (since n is even). The vertical axis of symmetry of the rectangle $R_{n,2}$ falls right between the m -th and $(m + 1)$ -st columns of $R_{n,2}$. Let us denote this axis by a . Thus, an axisymmetric domino tiling of $R_{n,2}$ is a tiling that is preserved under reflection across a .

Let N_1 and N_2 be the two horizontal dominos $\{(m, 1), (m + 1, 1)\}$ and $\{(m, 2), (m + 1, 2)\}$.

³*Proof.* Assume the contrary. Then, there exists some axisymmetric domino tiling T of $R_{n,2}$ that does not contain M . Consider this T .

The cell $(m, 1)$ of $R_{n,2}$ must be covered by **some** domino D in T . This D cannot be a vertical domino (since then it would be M , but T does not contain M); thus, it must be a horizontal domino. Let D' be the reflection of D across the vertical axis of $R_{n,2}$. Then, $D' \in T$ (since $D \in T$, but T is axisymmetric). Moreover, $D \neq D'$ (indeed, one of D and D' intersects columns $m - 1$ and m , while the other intersects columns m and $m + 1$), so that D and D' must be disjoint (since T is a tiling, so that any two distinct dominos in T are disjoint).

But $(m, 1) \in D$ and thus also $(m, 1) \in D'$ (indeed, the cell $(m, 1)$ lies on the vertical axis of symmetry of $R_{n,2}$, and thus is preserved under reflection across this axis). Hence, the sets D and D' are not disjoint. This contradicts the fact that D and D' are disjoint. This contradiction shows that our assumption was wrong, qed.

A domino D is said to *cut across* a if and only if D contains both a cell to the left of a and a cell to the right of a . Clearly, the only dominos that cut across a are N_1 and N_2 .

A domino tiling T of $R_{n,2}$ will be called *split* if it contains no domino cutting across a . Every split axisymmetric domino tiling of $R_{n,2}$ has the following form:

- The first m columns of $R_{n,2}$ are covered by some dominos forming a domino tiling of $R_{m,2}$.
- The last m columns are covered by some dominos, namely by the reflections of the dominos covering the first m columns across a .

Thus, in order to construct a split axisymmetric domino tiling of $R_{n,2}$, all we need to do is to choose a domino tiling of $R_{m,2}$. But (36) (applied to m instead of n) shows that the number of latter domino tilings is f_{m+1} . Thus,

$$(\text{the number of split axisymmetric domino tilings of } R_{n,2}) = f_{m+1}. \quad (37)$$

Now, let us count the axisymmetric domino tilings of $R_{n,2}$ that are not split. To no one's surprise, we shall call these domino tilings *non-split*.

Every non-split domino tiling of $R_{n,2}$ must contain the two dominos N_1 and N_2 ⁴. Hence, every non-split axisymmetric domino tiling of $R_{n,2}$ has the following

⁴*Proof.* Let T be a non-split domino tiling of $R_{n,2}$. We must prove that T contains N_1 and N_2 .

Assume the contrary. Thus, at least one of N_1 and N_2 is not contained in T .

The domino tiling T is non-split, i.e., it is not split. Thus, it contains a domino that cuts across a . In other words, it contains one of the dominos N_1 and N_2 (since N_1 and N_2 are the only dominos that cut across a). In other words, $N_1 \in T$ or $N_2 \in T$. We WLOG assume that $N_1 \in T$ (since the proof in the case $N_2 \in T$ is analogous). Hence, $N_2 \notin T$ (since at least one of N_1 and N_2 is not contained in T).

A domino in T will be called *western* if it fully lies to the left of the vertical axis a . Let w be the number of all western dominos in T . Then, altogether, these western dominos cover precisely $2w$ cells (since each domino covers 2 cells). In other words, the total number of cells covered by western dominos in T is $2w$; in particular, it is even.

The cell $(m,2)$ of $R_{n,2}$ must be covered with **some** domino in T . If this domino would cut across a , then it would have to be N_2 (because N_1 and N_2 are the only dominos that cut across a , but only N_2 among them contains the cell $(m,2)$), which would contradict the fact that $N_2 \notin T$. Hence, this domino cannot cut across a . Hence, this domino must fully lie to the left of the vertical axis a ; in other words, it is western. Thus, the cell $(m,2)$ is covered by a western domino in T .

We thus know that all the $2m$ cells to the left of a are covered by western dominos in T , except for the cell $(m,1)$ (which is covered by the domino N_1 , which cuts across a). (Indeed, we have shown that the cell $(m,2)$ is covered by a western domino in T ; the same is true for all the cells in columns $1, 2, \dots, m-1$, because they lie too far away from a to be covered by a non-western domino.) Thus, we have found $2m-1$ cells that are covered by western dominos in T . These are the **only** cells that are covered by western dominos in T (because we have already seen that $(m,1)$ is not covered by a western domino in T ; furthermore, any cell to the right of a cannot be covered by a western domino at all). Hence, the total number of cells covered by western dominos in T is $2m-1$.

But we have already shown that the total number of cells covered by western dominos is even. Comparing these two results, we see that $2m-1$ is even. This is clearly absurd. This contradiction shows that our assumption was wrong, qed.

form:

- The m -th and $(m + 1)$ -st columns of $R_{n,2}$ are covered by the horizontal dominos N_1 and N_2 .
- The first $m - 1$ columns of $R_{n,2}$ are covered by some dominos forming a domino tiling of $R_{m-1,2}$.
- The last $m - 1$ columns are covered by some dominos, namely by the reflections of the dominos covering the first $m - 1$ columns across a .

Thus, in order to construct a non-split axisymmetric domino tiling of $R_{n,2}$, all we need to do is to choose a domino tiling of $R_{m-1,2}$. But (36) (applied to $m - 1$ instead of n) shows that the number of latter domino tilings is $f_{(m-1)+1} = f_m$. Thus,

$$(\text{the number of non-split axisymmetric domino tilings of } R_{n,2}) = f_m. \quad (38)$$

But the definition of s_n yields

$$\begin{aligned} s_n &= (\text{the number of axisymmetric domino tilings of } R_{n,2}) \\ &= \underbrace{(\text{the number of split axisymmetric domino tilings of } R_{n,2})}_{\substack{= f_{m+1} \\ \text{(by (37))}}} \\ &\quad + \underbrace{(\text{the number of non-split axisymmetric domino tilings of } R_{n,2})}_{\substack{= f_m \\ \text{(by (38))}}} \\ &= f_{m+1} + f_m = f_{m+2} \end{aligned}$$

(since (35) (applied to $m + 2$ instead of n) yields $f_{m+2} = f_{(m+2)-1} + f_{(m+2)-2} = f_{m+1} + f_m$). In view of $m = n/2$, this rewrites as $s_n = f_{n/2+2}$. This solves Exercise 5 (b). \square

0.5. Some basic counting

Definition 0.16. Let $n \in \mathbb{Z}$. Then, $[n]$ shall denote the set $\{1, 2, \dots, n\}$. This is an empty set if $n \leq 0$.

Recall that if $n \in \mathbb{N}$ and $k \in \mathbb{Z}$, and if S is an n -element set, then

$$\binom{n}{k} \text{ is the number of } k\text{-element subsets of } S. \quad (39)$$

(This is proven, e.g., in [Grinbe16, Proposition 3.12], or in any text on combinatorics.)

Exercise 6. Let $n \in \mathbb{N}$, $a \in \mathbb{N}$ and $b \in \mathbb{N}$. Let N be the number of subsets of $[n]$ that contain exactly a even elements and exactly b odd elements.

- (a) Prove that $N = \binom{n/2}{a} \binom{n/2}{b}$ if n is even.
 (b) Compute N when n is odd.

Solution to Exercise 6 (sketched). (a) Roughly speaking, our argument is as follows: Let P be the set of all even elements of $[n]$; let Q be the set of all odd elements of $[n]$. We know that N is the number of subsets of $[n]$ that contain exactly a even elements and exactly b odd elements. In order to construct such a subset, we can choose its a even elements and its b odd elements separately. The a even elements must be chosen from the set P ; thus, choosing them means choosing an a -element subset of P . There are $\binom{|P|}{a}$ ways to make this choice (by (39), applied to P , $|P|$ and a instead of S , n and k). The b odd elements must be chosen from the set Q ; thus, choosing them means choosing a b -element subset of Q . There are $\binom{|Q|}{b}$ ways to make this choice (by (39), applied to Q , $|Q|$ and b instead of S , n and k). Hence, altogether, our choices can be made in $\binom{|P|}{a} \binom{|Q|}{b}$ many ways; thus, $N = \binom{|P|}{a} \binom{|Q|}{b}$. But when n is even, both sets P and Q have exactly $n/2$ elements. In other words, $|P| = n/2$ and $|Q| = n/2$. Hence, the equality $N = \binom{|P|}{a} \binom{|Q|}{b}$ rewrites as $N = \binom{n/2}{a} \binom{n/2}{b}$ in this case. This solves Exercise 6 (a).

Here is a more rigorous way to write up the same solution. Let P be the set of all even elements of $[n]$; let Q be the set of all odd elements of $[n]$. Let \mathcal{N} be the set of all subsets of $[n]$ that contain exactly a even elements and exactly b odd elements. Thus, $|\mathcal{N}| = N$ (since N was defined to be the number of such subsets).

For any set X and every $k \in \mathbb{N}$, we let $\mathcal{P}_k(X)$ denote the set of all k -element subsets of X . Now, the two maps

$$\begin{aligned} \mathcal{N} &\rightarrow \mathcal{P}_a(P) \times \mathcal{P}_b(Q), \\ S &\mapsto (S \cap P, S \cap Q) \end{aligned}$$

and

$$\begin{aligned} \mathcal{P}_a(P) \times \mathcal{P}_b(Q) &\rightarrow \mathcal{N}, \\ (U, V) &\mapsto U \cup V \end{aligned}$$

are well-defined and mutually inverse⁵. Hence, these maps are bijections. Thus, there exists a bijection $\mathcal{N} \rightarrow \mathcal{P}_a(P) \times \mathcal{P}_b(Q)$. Therefore,

$$|\mathcal{N}| = |\mathcal{P}_a(P) \times \mathcal{P}_b(Q)| = |\mathcal{P}_a(P)| \cdot |\mathcal{P}_b(Q)|. \quad (40)$$

⁵Instead of proving this in detail (which is straightforward), let me unfold the notations and explain what the maps do. The first map sends any $S \in \mathcal{N}$ (that is, any subset S of $[n]$ that contains exactly a even elements and exactly b odd elements) to the pair $(S \cap P, S \cap Q)$, which

But every finite set S and every $k \in \mathbb{N}$ satisfy

$$|\mathcal{P}_k(S)| = \binom{|S|}{k}. \quad (41)$$

(Indeed, this equality just says that the number of k -element subsets of S is $\binom{|S|}{k}$; this is just a restatement of (39) in a more formal language.)

Recall that $|\mathcal{N}| = N$. Comparing this with (40), we find

$$\begin{aligned} N &= \underbrace{|\mathcal{P}_a(P)|}_{\substack{= \binom{|P|}{a} \\ \text{(by (41))}}} \cdot \underbrace{|\mathcal{P}_b(Q)|}_{\substack{= \binom{|Q|}{b} \\ \text{(by (41))}}} = \binom{|P|}{a} \binom{|Q|}{b}. \\ &= \binom{|P|}{a} \binom{|Q|}{b} \end{aligned}$$

Now, assume that n is even. Then, there are exactly $n/2$ even numbers in the set $[n]$. In other words, the set of all even elements of $[n]$ has size $n/2$. In other words, the set P has size $n/2$ (since P is the set of all even elements of $[n]$). In other words, $|P| = n/2$. Similarly, $|Q| = n/2$. Now,

$$N = \binom{|P|}{a} \binom{|Q|}{b} = \binom{n/2}{a} \binom{n/2}{b}$$

(since $|P| = n/2$ and $|Q| = n/2$). This solves Exercise 6 (a) (rigorously this time).

(b) If n is odd, then $N = \binom{(n-1)/2}{a} \binom{(n+1)/2}{b}$. The proof is analogous to the above solution of Exercise 6 (a). \square

Exercise 7. A set S of integers shall be called *self-starting* if its size $|S|$ is also its smallest element. (For example, $\{3, 5, 6\}$ is self-starting, while $\{2, 3, 4\}$ and $\{3\}$ are not.)

Let $n \in \mathbb{N}$.

(a) For any $k \in [n]$, find the number of self-starting subsets of $[n]$ having size k .

(b) Find the number of all self-starting subsets of $[n]$.

Our following solution to Exercise 7 imitates [Fall2017-HW1s, solution to Exercise 8] (which solves a quite similar exercise, but the answers are different).

Before we solve this exercise, let us recall a useful fact:⁶

consists of the set $S \cap P$ (this is the set of all even elements of S ; it is an a -element set, because S contains exactly a even elements) and the set $S \cap Q$ (this is the set of all odd elements of S ; it is a b -element set). In other words, the first map splits any $S \in \mathcal{N}$ into its set of even elements and its set of odd elements. The second map sends any pair $(U, V) \in \mathcal{P}_a(P) \times \mathcal{P}_b(Q)$ to the union $U \cup V \in \mathcal{N}$. In other words, the second map takes a pair (U, V) consisting of an a -element set of even numbers and a b -element set of odd numbers, and combines them to the set $U \cup V$ (which belongs to \mathcal{N} , because it has exactly a even elements and exactly b odd elements). From this point of view, it should be clear that the maps are well-defined and mutually inverse.

⁶See Definition 0.15 for the definition of f_{m+1} .

Proposition 0.17. Let $m \in \{-1, 0, 1, \dots\}$. Then,

$$\sum_{k=0}^m \binom{m-k}{k} = f_{m+1}.$$

Proposition 0.17 has been mentioned in class (Proposition 1.18 from January 22), but wasn't proven there. There are several places where a proof can be found, however. For example, [Fall2017-HW2s, Exercise 3 (b)] shows that

$$f_{n+2} = \sum_{k=0}^n \binom{n-k+1}{k} \quad \text{for each } n \in \mathbb{N}. \quad (42)$$

It is easy to derive Proposition 0.17 from this:

Proof of Proposition 0.17. If $m = -1$, then Proposition 0.17 can easily be checked (indeed, it boils down to $0 = f_{(-1)+1}$ in this case, which follows from $f_0 = 0$). Thus, we WLOG assume that we don't have $m = -1$. Hence, $m \neq -1$, so that $m \in \{-1, 0, 1, \dots\} \setminus \{-1\} = \{0, 1, 2, \dots\} = \mathbb{N}$.

If $m = 0$, then Proposition 0.17 can easily be checked (indeed, it boils down to $\binom{0-0}{0} = f_{0+1}$ in this case, which follows from $f_1 = 1$). Thus, we WLOG assume that we don't have $m = 0$. Hence, $m \neq 0$, so that m is a positive integer (since $m \in \mathbb{N}$). Therefore, $m-1 \in \mathbb{N}$. Now, (42) (applied to $n = m-1$) yields

$$f_{(m-1)+2} = \sum_{k=0}^{m-1} \underbrace{\binom{(m-1)-k+1}{k}}_{\substack{= \binom{m-k}{k} \\ \text{(since } (m-1)-k+1=m-k)}} = \sum_{k=0}^{m-1} \binom{m-k}{k}. \quad (43)$$

On the other hand, $0 < m$ (since m is a positive integer). Thus, Proposition 0.8 (applied to 0 and m instead of m and n) yields $\binom{0}{m} = 0$. Now,

$$\begin{aligned} \sum_{k=0}^m \binom{m-k}{k} &= \sum_{k=0}^{m-1} \binom{m-k}{k} + \underbrace{\binom{m-m}{m}}_{= \binom{0}{m} = 0} = \sum_{k=0}^{m-1} \binom{m-k}{k} \\ &= f_{(m-1)+2} \quad \text{(by (43))} \\ &= f_{m+1}. \end{aligned}$$

This proves Proposition 0.17. □

Solution to Exercise 7. (a) Fix $k \in [n]$. Let K be the subset $\{k+1, k+2, \dots, n\}$ of $[n]$. In other words, K is the set of all elements of $[n]$ that are larger than k . Clearly, $|K| = n - k$.

The self-starting subsets of $[n]$ having size k are exactly the subsets of $[n]$ having size k and smallest element k . Thus, the maps

$$\begin{aligned} \{\text{self-starting subsets of } [n] \text{ having size } k\} &\rightarrow \{\text{subsets of } K \text{ having size } k-1\}, \\ S &\mapsto S \setminus \{k\} \end{aligned}$$

and

$$\begin{aligned} \{\text{subsets of } K \text{ having size } k-1\} &\rightarrow \{\text{self-starting subsets of } [n] \text{ having size } k\}, \\ T &\mapsto T \cup \{k\} \end{aligned}$$

are well-defined⁷ and mutually inverse⁸, and thus are bijections.

⁷This means the following:

- If S is a self-starting subset of $[n]$ having size k , then $S \setminus \{k\}$ is a subset of K having size $k - 1$.
- If T is a subset of K having size $k - 1$, then $T \cup \{k\}$ is a self-starting subset of $[n]$ having size k .

Checking this is straightforward; you can do it in your head (we shall outline the argument further below), but don't forget to do this! If you don't check well-definedness, then it may happen that one of your "maps" does not exist; for example, convince yourself that there is no map

$$\begin{aligned} \{\text{subsets of } [n]\} &\rightarrow \{\text{subsets of } [n]\}, \\ S &\mapsto S \cup \{|S| + 1\}, \end{aligned}$$

because the set $S \cup \{|S| + 1\}$ is not always a subset of $[n]$ (namely, it fails to be so when $|S| = n$). Anyway, let us check that our two maps are well-defined:

- First, we must show that if S is a self-starting subset of $[n]$ having size k , then $S \setminus \{k\}$ is a subset of K having size $k - 1$.

Indeed, let S be a self-starting subset of $[n]$ having size k . Since S is self-starting, we know that the size of S is also its smallest element (by the definition of "self-starting"). In other words, k is the smallest element of S (since the size of S is k). Thus, k is an element of S , and all elements of S other than k are larger than k .

We have $|S| = k$ (since S has size k). Since k is an element of S , we have $|S \setminus \{k\}| = |S| - 1 = k - 1$ (since $|S| = k$). Thus, the set $S \setminus \{k\}$ has size $k - 1$.

Furthermore, recall that all elements of S other than k are larger than k . In other words, all elements of $S \setminus \{k\}$ are larger than k . In other words, all elements of $S \setminus \{k\}$ belong to K (since K is the set of all elements of $[n]$ that are larger than k). In other words, $S \setminus \{k\}$ is a subset of K .

Hence, we have shown that $S \setminus \{k\}$ is a subset of K having size $k - 1$. Thus, our first map is well-defined.

- Next, we must prove that if T is a subset of K having size $k - 1$, then $T \cup \{k\}$ is a self-starting subset of $[n]$ having size k .

Indeed, let T be a subset of K having size $k - 1$. Thus, $|T| = k - 1$. Also, all elements of T belong to K (since T is a subset of K) and thus are larger than k (since K is the set of all elements of $[n]$ that are larger than k). Thus, k is not an element of T . Hence, $|T \cup \{k\}| = |T| + 1 = k$ (since $|T| = k - 1$). In other words, the set $T \cup \{k\}$ has size k . Clearly, the set $T \cup \{k\}$ is a subset of $[n]$ (since $T \subseteq K \subseteq [n]$ and $\{k\} \subseteq [n]$).

Also, recall that all elements of T are larger than k . Thus, all elements of $T \cup \{k\}$ other than k are larger than k (since all elements of $T \cup \{k\}$ other than k are elements of T). Hence, k is the smallest element of $T \cup \{k\}$ (since k is clearly an element of $T \cup \{k\}$). Since k is the size of $T \cup \{k\}$, this rewrites as follows: The size of $T \cup \{k\}$ is also the smallest element of $T \cup \{k\}$. In other words, the set $T \cup \{k\}$ is self-starting (by the definition of "self-starting").

Thus, we have shown that $T \cup \{k\}$ is a self-starting subset of $[n]$ having size k . This shows that our second map is well-defined.

Hence, there exists a bijection from $\{\text{self-starting subsets of } [n] \text{ having size } k\}$ to $\{\text{subsets of } K \text{ having size } k - 1\}$. Therefore,

$$\begin{aligned}
 & |\{\text{self-starting subsets of } [n] \text{ having size } k\}| \\
 &= |\{\text{subsets of } K \text{ having size } k - 1\}| \\
 &= \binom{|K|}{k-1} \\
 &\quad \left(\begin{array}{l} \text{because for any finite set } Q \text{ and any } m \in \mathbb{N}, \text{ we have} \\ |\{\text{subsets of } Q \text{ having size } m\}| = \binom{|Q|}{m} \end{array} \right) \\
 &= \binom{n-k}{k-1} \quad (\text{since } |K| = n - k). \tag{44}
 \end{aligned}$$

In other words, the number of self-starting subsets of $[n]$ having size k is $\binom{n-k}{k-1}$.

(b) Any self-starting subset of $[n]$ must have at least one element (namely, its size); thus, its size must be one of the integers $1, 2, \dots, n$. Hence,

$$\begin{aligned}
 & |\{\text{self-starting subsets of } [n]\}| \\
 &= \sum_{k=1}^n \underbrace{|\{\text{self-starting subsets of } [n] \text{ having size } k\}|}_{= \binom{n-k}{k-1} \text{ (by (44))}} \\
 &= \sum_{k=1}^n \binom{n-k}{k-1} = \sum_{k=0}^{n-1} \underbrace{\binom{n-(k+1)}{k}}_{= \binom{n-1-k}{k} \text{ (since } n-(k+1)=n-1-k)} \\
 &\quad \text{(here, we have substituted } k \text{ for } k-1 \text{ in the sum)} \\
 &= \sum_{k=0}^{n-1} \binom{n-1-k}{k} = f_{(n-1)+1} \quad (\text{by Proposition 0.17 (applied to } m = n-1)) \\
 &= f_n.
 \end{aligned}$$

In other words, the number of all self-starting subsets of $[n]$ is the Fibonacci number f_n . This solves Exercise 7 (b). \square

⁸For this, you need to show that

- If S is a self-starting subset of $[n]$ having size k , then $(S \setminus \{k\}) \cup \{k\} = S$.
- If S is a subset of K having size $k - 1$, then $(S \cup \{k\}) \setminus \{k\} = S$.

This is again entirely straightforward, and it is perfectly fine to do this in your head, but you should do it.

References

- [Grinbe16] 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>.
- [Grinbe17] Darij Grinberg, *The Lucas and Babbage congruences*, 25 December 2017.
<http://www.cip.ifi.lmu.de/~grinberg/lucascong.pdf>
- [Fall2017-HW1s] Darij Grinberg, *Math 4707 & Math 4990 Fall 2017 (Darij Grinberg): homework set 1 with solutions*.
<http://www-users.math.umn.edu/~dgrinber/comb/hw1s.pdf>
- [Fall2017-HW2s] Darij Grinberg, *Math 4707 & Math 4990 Fall 2017 (Darij Grinberg): homework set 2 with solutions*.
<http://www-users.math.umn.edu/~dgrinber/comb/hw2s.pdf>
-