

3. Math 235 Fall 2023, Worksheet 3: The Pigeonhole Principles

There are several results known as “the pigeonhole principle”. They are all fairly trivial facts in elementary set theory, and are often used (both in mathematics and in everyday logic) without explicit reference. Here are some of them:

Theorem 3.0.1. Assume you have chosen k elements from an n -element set S .

- (a) If $k > n$, then at least two of your chosen elements must be equal.
- (b) If $k = n$ and no two of your chosen elements are equal, then you must have chosen all elements of S .
- (c) If $k < n$, then there is at least one element of S that is not among your chosen elements.
- (d) If $k = n$ and each element of S is among your chosen elements, then no two of your chosen elements are equal.

The name “pigeonhole principle” refers to a widespread illustration of this principle in terms of pigeons and pigeonholes. Namely, by viewing S as a set of pigeonholes, and your k chosen elements as k pigeons, you can rewrite Theorem 3.0.1 as follows:¹

Theorem 3.0.2. Assume that k pigeons are nesting in n pigeonholes.

- (a) If $k > n$, then at least two pigeons share a pigeonhole.
- (b) If $k = n$ and no two pigeons share a pigeonhole, then all pigeonholes are inhabited.
- (c) If $k < n$, then there is at least one pigeonhole that has no pigeon.
- (d) If $k = n$ and each pigeonhole is inhabited, then no two pigeons share a pigeonhole.

The most convenient formulation of Theorem 3.0.1 to use in mathematical proofs is the following:

¹The pigeonhole principles are also known as “box principles” or “Dirichlet’s principles” among people with a less vivid imagination.

Theorem 3.0.3. Let $f : U \rightarrow V$ be a map between two finite sets U and V .

- (a) If $|U| > |V|$, then f cannot be injective.
- (b) If $|U| = |V|$ and f is injective, then f is bijective.
- (c) If $|U| < |V|$, then f cannot be surjective.
- (d) If $|U| = |V|$ and f is surjective, then f is bijective.

Some even more elementary facts are occasionally known as “the pigeonhole principle” as well. For instance:

Theorem 3.0.4. Let A and B be two subsets of a finite set C .

- (a) If $|A| + |B| > |C|$, then $A \cap B \neq \emptyset$.
- (b) If $|A| + |B| = |C|$ and $A \cap B = \emptyset$, then $A \cup B = C$.
- (c) If $|A| + |B| < |C|$, then $A \cup B \neq C$.
- (d) If $|A| + |B| = |C|$ and $A \cup B = C$, then $A \cap B = \emptyset$.

Theorem 3.0.4 (a) is actually a trivial corollary of the fact that $|A \cup B| = |A| + |B|$ whenever A and B are disjoint (and of the fact that a larger set cannot fit into a smaller one); however, it is philosophically similar to Theorem 3.0.3 (a). (Both theorems are saying something along the lines of “when things take up too much space in total, they have to overlap”.) Likewise, the remaining parts of Theorem 3.0.4 are akin to the corresponding parts of Theorem 3.0.3.

There are more complicated versions of the pigeonhole principle around (but all based on the same rough ideas). We will encounter one of them on this worksheet.

As before, \mathbb{N} means the set $\{0, 1, 2, \dots\}$.

3.1. Example problems

Here are a few simple applications of the pigeonhole principle. More can be found in [Grinbe20, Chapter 6] and in various other sources (some of which are listed at the beginning of [Grinbe20, Chapter 6]).

Exercise 3.1.1. Prove that there are two people alive right now with the exact same number of hairs on their heads.

Solution idea. We can safely assume that any human has at most 5 000 000 hairs on their head (in fact, the typical number of hairs on a human head is around 100 000), but the world population is far larger (over 7 billion). Thus, we can apply Theorem

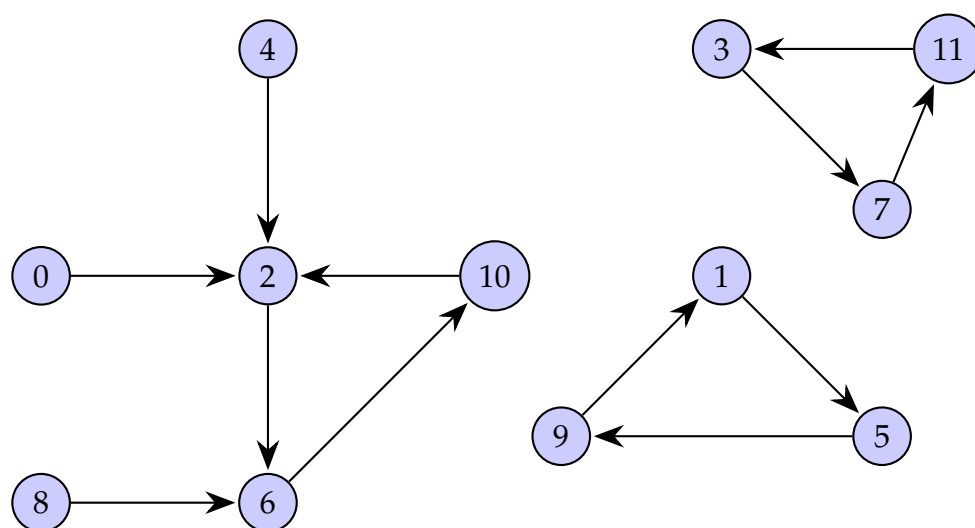
3.0.3 (a) to $U = \{\text{humans alive right now}\}$ and $V = \{0, 1, \dots, 5\,000\,000\}$ and to f being the map that sends each person to their number of hairs. We thus conclude that this map cannot be injective, i.e., it sends two people to the same number. But this means that these two people have the same number of hairs.

(Alternatively, it suffices to find two baldies.) \square

Example 3.1.1 is surprisingly old; it appeared in a 1622 book by Jean Leurechon (see [RitHee13]).

Exercise 3.1.2. Let X be an n -element set. Let $f : X \rightarrow X$ be any map. Let $x \in X$. Prove that there exist two integers i and j such that $0 \leq i < j \leq n$ and $f^i(x) = f^j(x)$.

[**Example:** Let X be the 12-element set $\{0, 1, \dots, 11\}$, and let $f : X \rightarrow X$ be the map given by the following picture:



(Here, an arrow from node “ i ” to node “ j ” means that $f(i) = j$.) Now, if $x = 0$, then $f^1(x) = f^4(x)$, so that there exist two integers i and j such that $0 \leq i < j \leq 12$ and $f^i(x) = f^j(x)$ (namely, $i = 1$ and $j = 4$).]

Solution idea. The $n + 1$ elements $f^0(x), f^1(x), \dots, f^n(x)$ all belong to the n -element set X . Hence, Theorem 3.0.1 (a) (applied to $k = n + 1$) shows that two of them are equal. But this is precisely what we claim. \square

Exercise 3.1.3. Let $n \geq 1$. Let a_1, a_2, \dots, a_n be any n integers. Prove that there exist some $p, q \in \{1, 2, \dots, n\}$ with $p \leq q$ and $n \mid a_p + a_{p+1} + \dots + a_q$.

Solution idea. For each $i \in \{0, 1, \dots, n\}$, we let b_i be the remainder that the integer $a_1 + a_2 + \dots + a_i$ leaves when divided by n . (Note that $a_1 + a_2 + \dots + a_0$ is the empty sum, thus equals 0.)

Thus, we have defined $n + 1$ remainders b_0, b_1, \dots, b_n . These $n + 1$ remainders all are contained in the n -element set $\{0, 1, \dots, n - 1\}$, so that Theorem 3.0.1 (a) yields

that two of them are equal. In other words, there exist integers i and j such that $0 \leq i < j \leq n$ and $b_i = b_j$. Consider these i and j .

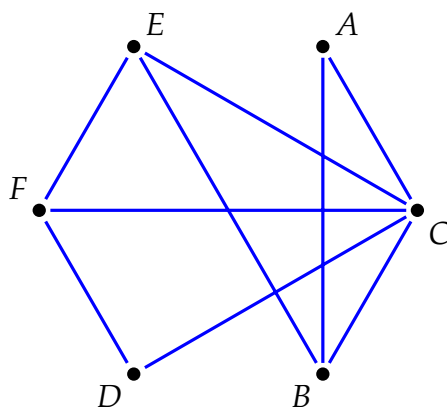
The equality $b_i = b_j$ means that the integers $a_1 + a_2 + \cdots + a_i$ and $a_1 + a_2 + \cdots + a_j$ leave the same remainder when divided by n . But this, in turn, entails that their difference is divisible by n ². However, their difference is

$$(a_1 + a_2 + \cdots + a_i) - (a_1 + a_2 + \cdots + a_j) = -(a_{i+1} + a_{i+2} + \cdots + a_j)$$

(since $i < j$). Hence, we have shown that $-(a_{i+1} + a_{i+2} + \cdots + a_j)$ is divisible by n . In other words, $a_{i+1} + a_{i+2} + \cdots + a_j$ is divisible by n (since the sign of an integer clearly does not affect divisibility). Hence, there exist some $p, q \in \{1, 2, \dots, n\}$ with $p \leq q$ and $n \mid a_p + a_{p+1} + \cdots + a_q$ (namely, $p = i + 1$ and $q = j$). \square

Exercise 3.1.4. Let $n \geq 2$ be an integer. At a conference long ago, n scientists have met; some of them have exchanged handshakes among each other³. Prove that two of these n scientists have shaken the same number of hands during the conference. (We assume that any pair of scientists shakes hands at most once. We also assume that no one shakes their own hands.)

[**Example:** Let $n = 6$, and consider the following situation:



Here, A, B, C, D, E, F are the 6 scientists, and a line segment connects any pair of scientists that has exchanged a handshake. Thus, scientist A has shaken 2 hands; B has shaken 3 hands; C has shaken 5 hands; D has shaken 2 hands; etc.. Thus, A and D have shaken the same number of hands.]

Solution idea. (See [Grinbe20, §6.2.2] for details.) Assume the contrary. Thus, any two distinct scientists have shaken different numbers of hands.

²We are here using the following fundamental fact about remainders: If two integers u and v leave the same remainder when divided by n , then their difference $u - v$ is divisible by n . This is just a restatement of Proposition 2.5.3 on Worksheet 2 (specifically, of the “if $u \% n = v \% n$, then $u \equiv v \pmod{n}$ ” direction of that proposition).

³Handshakes (a form of greeting popular in the distant past) are understood to be symmetric: If a shakes b ’s hands, then b also shakes a ’s hands.

Let U be the set of our n scientists. Let V be the set $\{0, 1, \dots, n-1\}$. Thus, both U and V are n -element sets; hence, $|U| = |V|$. From $n \geq 2$, we obtain $n-1 \neq 0$ and $0 \in V$ and $n-1 \in V$.

Define a map $f : U \rightarrow V$ as follows: For each scientist $s \in U$, we let $f(s)$ be the number of hands that s has shaken. This is well-defined, because s has shaken at most $n-1$ hands⁴ and thus we have $f(s) \in \{0, 1, \dots, n-1\} = V$.

We have assumed that any two distinct scientists have shaken different numbers of hands. In other words, the map f is injective. Hence, Theorem 3.0.3 (b) yields that f is bijective (since $|U| = |V|$). Thus, in particular, f is surjective. Hence, there exists a scientist $a \in U$ such that $f(a) = n-1$ (since $n-1 \in V$), and there exists a scientist $b \in U$ such that $f(b) = 0$ (since $0 \in V$). Consider these a and b . Note that $a \neq b$ (why?).

Now, $f(a) = n-1$ shows that a must have shaken everyone's hands (except for a themselves) (why?). Hence, a must have shaken b 's hands in particular (since $a \neq b$). On the other hand, $f(b) = 0$ shows that b must have shaken no hands at all. The previous two sentences contradict each other. Thus, Exercise 3.1.4 is solved. \square

One of the more advanced versions of the pigeonhole principle is the following generalization of Theorem 3.0.3 (a):

Theorem 3.1.1. Let $f : U \rightarrow V$ be a map between two finite sets U and V . Let $m \in \mathbb{N}$.

If $|U| > m \cdot |V|$, then there exist $m+1$ distinct elements u_1, u_2, \dots, u_{m+1} of U such that

$$f(u_1) = f(u_2) = \dots = f(u_{m+1}).$$

Proof of Theorem 3.1.1. Assume that $|U| > m \cdot |V|$.

I am sure you will agree that if you sum the number 1 over all elements of U , you get

$$\sum_{u \in U} 1 = |U| \cdot 1 = |U|. \quad (1)$$

However, for each $u \in U$, there is a unique $v \in V$ satisfying $f(u) = v$ (obviously). Thus, we can break up the sum $\sum_{u \in U} 1$ as follows:

$$\sum_{u \in U} 1 = \sum_{v \in V} \sum_{\substack{u \in U; \\ f(u)=v}} 1. \quad (2)$$

Now, for each $v \in V$, let $n(v)$ be the number of all $u \in U$ satisfying $f(u) = v$. (In other words, $n(v)$ denotes the number of times that the map f takes the value v .) Hence, (2)

⁴Here we use our assumptions that any pair of scientists shakes hands at most once, and that no one shakes their own hands.

becomes

$$\sum_{u \in U} 1 = \sum_{v \in V} \underbrace{\sum_{\substack{u \in U; \\ f(u)=v}} 1}_{=n(v) \cdot 1} = \sum_{v \in V} n(v) \cdot 1 = \sum_{v \in V} n(v).$$

(since this sum has $n(v)$ many addends, and each addend is 1)

Thus,

$$\begin{aligned} \sum_{v \in V} n(v) &= \sum_{u \in U} 1 = |U| && \text{(by (1))} \\ &> m \cdot |V|. \end{aligned} \tag{3}$$

However, if each $v \in V$ would satisfy $n(v) \leq m$, then we would have

$$\sum_{v \in V} \underbrace{n(v)}_{\leq m} \leq \sum_{v \in V} m = |V| \cdot m = m \cdot |V|,$$

which would contradict (3). Thus, it is not true that each $v \in V$ satisfies $n(v) \leq m$. In other words, there exists some $v \in V$ that satisfies $n(v) > m$. Consider this v . From $n(v) > m$, we obtain $n(v) \geq m + 1$. In other words, there are at least $m + 1$ different elements $u \in U$ satisfying $f(u) = v$ (since $n(v)$ was defined as the number of such u). In other words, there exist $m + 1$ distinct elements u_1, u_2, \dots, u_{m+1} of U such that

$$f(u_1) = f(u_2) = \dots = f(u_{m+1}) = v.$$

This proves Theorem 3.1.1. □

The following exercise is known as the *Erdős–Szekeres theorem*:

Exercise 3.1.5. Let $n, m \in \mathbb{N}$. Let $\mathbf{a} = (a_1, a_2, \dots, a_k)$ be a sequence of real numbers with length $k > nm$. Prove that \mathbf{a} has

- a weakly increasing subsequence of length $n + 1$ (i.e., there exist integers i_1, i_2, \dots, i_{n+1} satisfying $1 \leq i_1 < i_2 < \dots < i_{n+1} \leq k$ and $a_{i_1} \leq a_{i_2} \leq \dots \leq a_{i_{n+1}}$), **or**
- a strictly decreasing subsequence of length $m + 1$ (i.e., there exist integers i_1, i_2, \dots, i_{m+1} satisfying $1 \leq i_1 < i_2 < \dots < i_{m+1} \leq k$ and $a_{i_1} > a_{i_2} > \dots > a_{i_{m+1}}$).

[**Example:** If $n = 2$ and $m = 2$ and $\mathbf{a} = (1, 4, 3, 5, 2)$, then \mathbf{a} has the strictly decreasing subsequence $(4, 3, 2)$ of length 3. It is easy to construct examples where \mathbf{a} has a weakly increasing subsequence of length 3 instead, or when \mathbf{a} has both.]

Solution idea. Assume the contrary. Thus, \mathbf{a} has neither a weakly increasing subsequence of length $n + 1$ nor a strictly decreasing subsequence of length $m + 1$.

We shall use the notation $[p]$ for the set $\{1, 2, \dots, p\}$, where p is an arbitrary nonnegative integer.

We define a map $f : [k] \rightarrow [n]$ as follows: For each $j \in [k]$, we let $f(j)$ be the maximum length of a weakly increasing subsequence of (a_1, a_2, \dots, a_j) that ends with a_j (that is, the maximum $p \in \mathbb{N}$ such that there exist integers i_1, i_2, \dots, i_p satisfying $1 \leq i_1 < i_2 < \dots < i_p = j$ and $a_{i_1} \leq a_{i_2} \leq \dots \leq a_{i_p}$). This $f(j)$ really belongs to $[n]$ (why?⁵), so this map f is well-defined.

We have $|[k]| = k > nm = mn = m \cdot |[n]|$. Hence, Theorem 3.1.1 (applied to $U = [k]$ and $V = [n]$) shows that there exist $m + 1$ distinct elements u_1, u_2, \dots, u_{m+1} of $[k]$ such that

$$f(u_1) = f(u_2) = \dots = f(u_{m+1}). \quad (4)$$

Consider these $m + 1$ elements. WLOG assume that $u_1 < u_2 < \dots < u_{m+1}$. If some $i \in [m]$ would satisfy $a_{u_i} \leq a_{u_{i+1}}$, then it would satisfy $f(u_{i+1}) \geq f(u_i) + 1$ (why?⁶), which would contradict (4). Hence, the subsequence $(a_{u_1}, a_{u_2}, \dots, a_{u_{m+1}})$ of \mathbf{a} is strictly decreasing. This contradicts our assumption (why?). Thus, Exercise 3.1.5 is solved. \square

3.2. Class problems

The following problems are to be discussed during class.

Exercise 3.2.1. Prove that in the USA (population ca. 332 million), you can find two people that have the same birthday and the same last 4 digits of their credit card number. (Everyone is assumed to have at least one credit card.)

Again, we will use the notation $[p]$ for the set $\{1, 2, \dots, p\}$, where p is an arbitrary nonnegative integer.

Exercise 3.2.2. Let n be a positive integer. Let S be an $(n + 1)$ -element subset of $[2n]$. Prove the following:

- (a) There exist two distinct elements s and t of S such that $s = t + n$.
- (b) There exist two distinct elements s and t of S such that $s - t = 1$.
- (c) There exist two distinct elements s and t of S such that $\gcd(s, t) = 1$.
- (d) There exist two distinct elements s and t of S such that $s \mid t$.

⁵Hint: Recall us “assuming the contrary”.

⁶Hint: Recall that $f(u_i)$ was defined as the maximum length of a weakly increasing subsequence of $(a_1, a_2, \dots, a_{u_i})$ that ends with a_{u_i} . Thus, there exists such a subsequence having length $f(u_i)$. If we had $a_{u_i} \leq a_{u_{i+1}}$, then we could extend this subsequence by inserting an $a_{u_{i+1}}$ at its end, and would obtain a weakly increasing subsequence of $(a_1, a_2, \dots, a_{u_{i+1}})$ that ends with $a_{u_{i+1}}$. But the maximum length of such a subsequence is $f(u_{i+1})$.

The next exercise is slightly geometric. We treat the Euclidean plane as the vector space \mathbb{R}^2 , identifying each point p on the plane with the pair (x_p, y_p) of its Cartesian coordinates. A *lattice point* means a point $p = (x, y) \in \mathbb{R}^2$ whose coordinates x and y are integers.

Exercise 3.2.3. Five lattice points are chosen in the plane. Prove that you can always choose two of these five points such that the midpoint between these two points is again a lattice point.

Exercise 3.2.4. Let (f_0, f_1, f_2, \dots) be the Fibonacci sequence. Let m be a positive integer. For each $i \in \mathbb{N}$, let g_i be the remainder of f_i upon division by m . Prove that the sequence (g_0, g_1, g_2, \dots) is purely periodic (i.e., there exists a positive integer N such that every $i \in \mathbb{N}$ satisfies $g_{i+N} = g_i$).

Exercise 3.2.5. Given any five points on a sphere, show that some four of them must lie on a closed hemisphere.

(63rd Putnam contest 2002, Problem A2)

Exercise 3.2.6. Let m and n be two positive integers. At a symposium long ago, $\binom{m+n-2}{m-1}$ scientists have met; some of them have exchanged handshakes among each other. Prove that

- you can find m of these scientists that have all shaken each other's hands,
or
- you can find n of these scientists among which no two have shaken each other's hands.

(We make the same assumptions about handshakes as in Exercise 3.1.4.)

3.3. Homework exercises

Solve 4 of the 10 exercises below and upload your solutions on gradescope by October 24.

Don't be worried if your solutions do not use the pigeonhole principle in any of its forms! Due to the simplicity of the principle, it is fairly easy to avoid it or use something equivalent.

Exercise 3.3.1. Let a, b, c be three odd integers. Prove that at least one of the three integers $ab - 1$, $bc - 1$ and $ca - 1$ is divisible by 4.

Exercise 3.3.2. Let S be a 10-element subset of the set $\{1, 2, \dots, 100\}$. Prove that there exist two disjoint nonempty subsets A and B of S such that $\sum_{a \in A} a = \sum_{b \in B} b$. (Note that A and B are allowed to have any positive sizes, including 1.)

[**Example:** If $S = \{3, 9, 13, 19, 26, 60, 74, 80, 84, 94\}$, then $\sum_{a \in A} a = \sum_{b \in B} b$ is satisfied for $A = \{3, 9, 94\}$ and $B = \{26, 80\}$ (as well as for various other choices).]

Exercise 3.3.3. A number of people have been settled in n apartments B_1, B_2, \dots, B_n (with each person settled in exactly one apartment). (Roommates are allowed.) Now, all these people are removed from their apartments and re-settled in $n + 1$ new apartments C_1, C_2, \dots, C_{n+1} in such a way that none of these $n + 1$ new apartments stays empty.

A person is said to have *gained space* if he has fewer roommates after the resettlement than he used to have before.

Prove that at least two people have gained space.

Exercise 3.3.4. Consider any six points on the circumference of a circle with radius 1. Prove that some two of these six points have distance ≤ 1 .

Exercise 3.3.5. Each lattice point in the Euclidean plane has been colored with one of n colors. Prove that there exists a rectangle whose four vertices are lattice points all having the same color.

Exercise 3.3.6. Let (a_0, a_1, a_2, \dots) be the sequence of integers defined recursively by $a_0 = 0$ and $a_1 = a_2 = 1$ and

$$a_n = a_{n-1}a_{n-2} + a_{n-3} \quad \text{for all } n \geq 3.$$

Let m be a positive integer. For each $i \in \mathbb{N}$, let b_i be the remainder of a_i upon division by m . Prove that the sequence (b_0, b_1, b_2, \dots) is purely periodic.

Exercise 3.3.7. Let $n \in \mathbb{N}$. Consider a $2n \times 2n$ -table. Assume that at most $3n$ of its $(2n)^2$ many squares have been colored black. Prove that it is possible to remove n rows and n columns from the table in such a way that no black squares remain in the table.

[**Hint:** When $n \geq 2$, find two rows and two columns that contain at least 6 black squares among them.]

Exercise 3.3.8. Let n be a positive integer.

- (a) Let S be an $(n + 1)$ -element subset of $[2n - 1]$. Prove that we can find three distinct elements u, v, w of S such that $u + v = w$.
- (b) Is this still true if we let S be a subset of $[2n]$ instead of a subset of $[2n - 1]$?

Exercise 3.3.9. Let $n \geq 2$ be an integer. Let A be an $n \times n$ -matrix with real entries. Assume that in each row of A , the sum of the two largest entries is positive. Is it possible that in each column of A , the sum of the two largest entries is negative?

We remark that Exercise 3.3.9 would not hold if the word “two” were replaced by “three” throughout it. For instance, in the 4×4 -matrix $\begin{pmatrix} -1 & -1 & -7 & 3 \\ -1 & -1 & -7 & 3 \\ -1 & -1 & 3 & -7 \\ -1 & -1 & 3 & -7 \end{pmatrix}$, each row has a positive sum of its three largest entries, but each column has a negative sum of its three largest entries. This counterexample was found by Jonathan Parlett.

The next exercise is more loosely related to the pigeonhole principle (to Theorem 3.0.4 if any):

Exercise 3.3.10. Let A be a rectangular matrix with real entries. Assume that the entries in each **row** of A are weakly increasing from left to right. Now we sort the entries in each **column** of A so that they become weakly increasing from top to bottom. (Each entry stays within its column.) Thus, we obtain a new matrix B . Prove that the entries in each **row** of B are still weakly increasing from left to right.

[**Example:** If $A = \begin{pmatrix} 1 & 3 & 6 \\ 2 & 2 & 5 \\ 1 & 2 & 3 \end{pmatrix}$, then $B = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 5 \\ 2 & 3 & 6 \end{pmatrix}$.]

References

- [Grinbe20] Darij Grinberg, *Math 235: Mathematical Problem Solving*, 10 August 2021. <https://www.cip.ifi.lmu.de/~grinberg/t/20f/mps.pdf>
- [RitHee13] Benoît Rittaud, Albrecht Heeffer, *The Pigeonhole Principle, Two Centuries Before Dirichlet*, *The Mathematical Intelligencer*, 36(2), pp. 27–29.