Chapter 2
Cardinality

We say that two nonempty sets A, B are *equivalent* or *of the same cardinality* or *of the same power* if there is a bijection from A to B. We write this as $A \sim B$.

If $f : A \to B$ is a bijection, then we also denote $A \overset{f}{\sim} B$. Note that "$\sim$" is an equivalence relation. Indeed, we have

$$\begin{cases} \text{(reflexivity) } A \overset{1_A}{\sim} A. \\ \text{(symmetry) if } A \overset{f}{\sim} B, \text{ then } B \overset{f^{-1}}{\sim} A. \\ \text{(transitivity) if } A \overset{f}{\sim} B \text{ and } B \overset{g}{\sim} C, \text{ then } A \overset{g \circ f}{\sim} C. \end{cases}$$

The equivalence class $\widehat{A} = \{B \mid A \sim B\}$ is called *the cardinality of* A, denoted by $|A|$ or $\operatorname{card} A$.

A nonempty set A is called *finite* if $A \sim \{1, 2, \ldots, n\}$, for some positive integer n. In this case, A has n elements and we put $|A| = n$.

For finite sets A, B with $|A| = |B|$ and function $f : A \to B$ we have:

$$f \text{ injective } \Leftrightarrow f \text{ bijective } \Leftrightarrow f \text{ surjective.}$$

As a nice application, we give the following:

Problem. Let p and q be primes, $p \neq q$. Then for all integers $0 \leq r_1 \leq p-1$, $0 \leq r_2 \leq q-1$, there exists an integer n which gives the remainders r_1, r_2 when divided by p and q, respectively.

Solution. Denote by

$$\mathbb{Z}_p = \left\{\overline{0}, \overline{1}, \ldots, \overline{p-1}\right\}, \ \mathbb{Z}_q = \left\{\widetilde{0}, \widetilde{1}, \ldots, \widetilde{q-1}\right\}, \ \mathbb{Z}_{pq} = \left\{\widehat{0}, \widehat{1}, \ldots, \widehat{pq-1}\right\}$$

the remainder (or residue) class sets relative to $p, q,$, respectively pq. Remember that, for any positive integer m, we can define (on the set $\mathbb{Z}$ of the integers) the

T. Andreescu et al., *Mathematical Bridges*, DOI 10.1007/978-0-8176-4629-5_2

relation of congruence modulo m by $a \equiv b \bmod m$ if and only if $a - b$ is divisible by m (or, equivalently, if a and b give equal remainders when divided by m). This is an equivalence relation on $\mathbb{Z}$, and the remainder (or residue, or congruence) class modulo m of the integer x (that is, its equivalence class with respect to the congruence relation) is readily seen to be the set $\widehat{x} = \{\ldots, x-2n, x-n, x, x+n, x+2n, \ldots\}$. The set $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$ of all the residue classes modulo m is then a ring with respect to addition and multiplication defined by $\widehat{a} + \widehat{b} = \widehat{a+b}$ and $\widehat{a} \cdot \widehat{b} = \widehat{a \cdot b}$. The reader is invited to verify that these operations are well defined (they do not depend on choosing the representatives of the remainder classes) and that they indeed provide a ring structure for the set $\mathbb{Z}_m$. Also note that $\mathbb{Z}_m = \{\widehat{0}.\widehat{1}, \ldots, \widehat{m-1}\}$.

Now we go on further with the solution of the problem and define the function $\varphi : \mathbb{Z}_{pq} \to \mathbb{Z}_p \times \mathbb{Z}_q$, by the law $\varphi(\widehat{r}) = (\overline{r}, \widetilde{r})$, $\widehat{r} \in \mathbb{Z}_{pq}$. We have

$$\left|\mathbb{Z}_{pq}\right| = \left|\mathbb{Z}_p \times \mathbb{Z}_q\right| = pq.$$

The surjectivity of φ follows if φ is injective. Thus, we have the implications

$$\varphi(\widehat{r}) = \varphi(\widehat{r'}) \Rightarrow (\overline{r}, \widetilde{r}) = (\overline{r'}, \widetilde{r'})$$

$$\Rightarrow \begin{cases} \overline{r} = \overline{r'} \\ \widetilde{r} = \widetilde{r'} \end{cases} \Rightarrow \begin{cases} p \mid r - r' \\ q \mid r - r' \end{cases} \Rightarrow pq \mid r - r',$$

so $\widehat{r} = \widehat{r'}$. This means that φ is injective and consequently surjective. There is $n \in \{0, 1, \ldots, pq-1\}$ such that

$$\varphi(\widehat{n}) = (\overline{r}_1, \widetilde{r}_2) \Leftrightarrow (\overline{n}, \widetilde{n}) = (\overline{r}_1, \widetilde{r}_2) \Rightarrow \overline{n} = \overline{r}_1 \text{ and } \widetilde{n} = \widetilde{r}_2,$$

thus $p \mid n - r_1$ and $q \mid n - r_2$. Observe that this argument can be easily extended in order to obtain a proof of the very useful Chinese remainder theorem: if $a_1, a_2, \ldots, a_n$ are pairwise relatively prime integers, then for any integers $b_1, b_2, \ldots, b_n$, the system $x \equiv b_1 (\mathrm{mod} a_1), \ldots, x \equiv b_n (\mathrm{mod} a_n)$ has a unique solution modulo $a_1 a_2 \ldots a_n$. □

If A, B are finite and there is an injective map $f : A \to B$, then we put $|A| \leq |B|$. If moreover there is an injective map $g : B \to A$, then $|A| = |B|$. This result, the Cantor-Bernstein theorem, is difficult when A and B are infinite. Here is a proof.

Theorem (Cantor-Bernstein). *If A,B are nonempty sets and there are injections $f : A \to B$, $g : B \to A$, then $|A| = |B|$, i.e., there exists a bijection $\phi : A \to B$.*

Proof. We say that $b \in B$ is an *ancestor* of $a \in A$ if

$$(\underbrace{g \circ f \circ g \circ \ldots \circ f \circ g}_{2k+1 \text{ times}})(b) = a,$$

for some k. Similarly, $a \in A$ is an *ancestor* of $b \in B$ if

$$\underbrace{(f \circ g \circ f \circ \ldots \circ g \circ f}_{2k+1 \text{ times}})(a) = b,$$

for some k. Moreover, $a' \in A$ is an *ancestor* of $a \in A$ if $f(a') \in B$ is an ancestor of a and $b' \in B$ is an *ancestor* of $b \in B$ if $g(b') \in A$ is an ancestor of b.

Denote by M_1, M_2, M_∞ the set of all elements of A which have an odd, even, respectively an infinite number of ancestors. Define analogously N_1, N_2, N_∞ for B.

We prove that the function $\phi : A \to B$, given by

$$\phi(x) = \begin{cases} g^{-1}(x), & x \in M_1 \cup M_\infty \\ f(x), & x \in M_2 \end{cases}$$

is bijective. In this sense, we prove that its inverse is $\psi : B \to A$,

$$\psi(y) = \begin{cases} f^{-1}(y), & y \in N_1 \\ g(y), & y \in N_2 \cup N_\infty \end{cases}.$$

These functions ϕ, ψ are well defined because f, g are injective.

Let $x \in A$. If $x \in M_1 \cup M_\infty$, then

$$\phi(x) = g^{-1}(x) \in N_2 \cup N_\infty,$$

so

$$\psi(\phi(x)) = g(\phi(x)) = g(g^{-1}(x)) = x.$$

If $x \in M_2$, then $\phi(x) = f(x) \in N_1$ and

$$\psi(\phi(x)) = f^{-1}(\phi(x)) = f^{-1}(f(x)) = x.$$

Hence $\psi \circ \phi = \mathbf{1}_B$.

Let $y \in B$. If $y \in N_1$, then

$$\psi(y) = f^{-1}(y) \in M_2$$

and

$$\phi(\psi(y)) = f(\psi(y)) = f(f^{-1}(y)) = y.$$

If $y \in N_2 \cup N_\infty$, then

$$\psi(y) = g(y) \in M_1 \cup M_\infty$$

and

$$\phi(\psi(y)) = g^{-1}(\psi(y)) = g^{-1}(g(y)) = y.$$

Hence $\phi \circ \psi = \mathbf{1}_A$. In conclusion, $\phi^{-1} = \psi$ and consequently, $|A| = |B|$. □

This theorem allows us to define an order relation by the law

$$|A| \leq |B| \text{ if and only if there is } f : A \to B \text{ injective.}$$

As a direct consequence, we have

$$|A| \leq |B| \text{ if and only if there is } g : B \to A \text{ surjective.}$$

Using Zorn's lemma, one can prove that this order relation is actually total. A set A is called *countable* if A is equivalent to the set $\mathbb{N}$ of nonnegative integers. A is called *at most countable* if it is finite or countable.

A set is countable if and only if its elements can be written as a sequence. This does not happen for the set of the reals or any of its (nondegenerate) intervals (see problems 2 and 7 below).

Nevertheless, a countable union of countable sets is also a countable set. Indeed, let $A = \bigcup_{n\geq 1} A_n$, where each A_n is countable. Let $A_n = \{a_{n1}, a_{n2}, \dots\}$ be an enumeration of A_n, for every natural number $n \geq 1$, and note that

$$a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots$$

is an enumeration of A (basically, the same argument shows that the set of positive rational numbers is countable, as we will immediately see). Obviously, the result remains true if every A_n is *at most* countable.

For instance, the set $\mathbb{Z}$ of all integers is countable because

$$\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, 4, -4, \dots\}.$$

We can also note that

$$\mathbb{Z} = \bigcup_{n\in\mathbb{N}} \{-n, -n+1, -n+2, \dots\},$$

which is a countable union of countable sets.

For the set $\mathbb{Q}$ of rationals we have the decomposition

$$\mathbb{Q} = \bigcup_{n\in\mathbb{Z}^*} \left\{\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \frac{4}{n}, \dots\right\},$$

so $\mathbb{Q}$ is countable. In another way, the set of positive rationals can be ordered as follows:

$$\begin{array}{cccccccc}
1/1 & \to & 1/2 & & 1/3 & \to & 1/4 & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow \ldots \\
2/1 & & 2/2 & & 2/3 & & 2/4 & \ldots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow \ldots \\
3/1 & & 3/2 & & 3/3 & & 3/4 & \ldots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow \ldots \\
4/1 & & 4/2 & & 4/3 & & 4/4 & \ldots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow \ldots \\
5/1 & & 5/2 & & 5/3 & & 5/4 & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \ldots
\end{array}$$

Each element appears many times in the table, but we consider each of them only for the first time.

The set $\mathbb{N} \times \mathbb{N}$ of pairs of nonnegative integers is countable. Indeed,

$$f : \mathbb{N} \to \mathbb{N} \times \mathbb{N} \ , \quad f(n) = (n, 0)$$

is injective and

$$g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \ , \quad g(m, n) = 2^m \cdot 3^n$$

is injective. According to the Cantor-Bernstein theorem, $\mathbb{N} \times \mathbb{N} \sim \mathbb{N}$. In addition, note that the map

$$\varphi : \mathbb{N}^* \times \mathbb{N}^* \to \mathbb{N}^* \ , \quad \varphi(m, n) = 2^{m-1} \cdot (2n - 1)$$

is bijective. One can even find a polynomial bijection between $\mathbb{N} \times \mathbb{N}$ and $\mathbb{N}$, which we leave as an interesting exercise for the reader.

Proposed Problems

1. Let A be an infinite set. Prove that for every positive integer n, A has a finite subset with n elements. Deduce that every infinite set has at least one countable subset.
2. Prove that $(0, 1)$ is not countable. Infer that $\mathbb{R}$ and $\mathbb{R} \setminus \mathbb{Q}$ are not countable.
3. Let $X,\ A,\ B$, be pairwise disjoint sets such that A, B are countable. Prove that

$$X \cup A \cup B \sim X \cup A.$$

   Deduce that for every countable set B of real numbers, $\mathbb{R} \setminus B \sim \mathbb{R}$.
4. Prove that $\mathbb{N} \times \mathbb{N} \times \mathbb{N}$ is countable and so is $\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}$.

5. Let $a < b$ be real numbers. Prove that $(0, 1) \sim (a, b) \sim \mathbb{R}$.
6. Let A be a countable set and $a \in A$. Prove that $A \setminus \{a\} \sim A$. Is this result true for every infinite set A?
7. Let $a < b$ be real numbers. Prove that $[a, b] \sim [a, b) \sim (a, b] \sim (a, b)$.
8. Prove that every ε-discrete set of real numbers is at most countable. (A set $A \subset \mathbb{R}$ is called ε-discrete if $|a - b| > \varepsilon$, for any different elements a, b of A).
9. Let S be a set of real numbers with the property that for all real numbers $a < b$, the set $S \cap [a, b]$ is finite, possibly empty. Prove that S is at most countable. Is every set S with the above property an ε-discrete set, for some positive real ε?
10. Let S be an infinite and uncountable set of real numbers. For each real number t, we put

$$S^-(t) = S \cap (-\infty, t], \quad S^+(t) = S \cap [t, \infty).$$

Prove that there exists a real number t_0 for which both sets $S^-(t_0)$ and $S^+(t_0)$ are infinite and uncountable.
11. A set M of positive real numbers has the property that the sum of any finite number of its elements is not greater than 7. Prove that the set M is at most countable.
12. Prove that the set of polynomials with integer coefficients is countable.
13. Prove that the set of algebraic numbers is countable. Deduce that the set of transcendental numbers is not countable. (A real number α is called an algebraic number if there exists a polynomial $P \not\equiv 0$ with integer coefficients such that $P(\alpha) = 0$. Otherwise, α is called transcendental.)
14. Prove that for each set X, we have $|X| < |\mathcal{P}(X)|$. We denote by $\mathcal{P}(X)$ the power set of X (that is, the set of all subsets of X, including the empty set and X). However, the set of all finite subsets of $\mathbb{N}$ is countable (thus $|\mathbb{N}| = |\mathcal{P}(\mathbb{N})|$).
15. Let $p_1, p_2, \ldots, p_k$ be distinct primes. Prove that for all integers $r_1,\ r_2,\ \ldots,\ r_k$ there is an integer n such that $n \equiv r_i (\mathrm{mod}\, p_i)$, for all $1 \leq i \leq k$.
16. Prove that there are no functions $f : \mathbb{R} \to \mathbb{R}$ with the property

$$|f(x) - f(y)| \geq 1,$$

for all $x, y \in \mathbb{R},\ x \neq y$.
17. Prove that there are no functions $f : \mathbb{R} \to \mathbb{R}$ with the property

$$|f(x) - f(y)| \geq \frac{1}{x^2 + y^2},$$

for all $x, y \in \mathbb{R},\ x \neq y$.
18. Prove that the discontinuity set of a monotone function $f : \mathbb{R} \to \mathbb{R}$ is at most countable.
19. Prove that the set of all permutations of the set of positive integers is uncountable.

20. Let f, g be two real functions such that $f(x) < g(x)$ for all real numbers x. Prove that there exists an uncountable set A such that $f(x) < g(y)$ for all $x, y \in A$.
21. Let $\mathbb{R}$ be the real line with the standard topology. Prove that every uncountable subset of $\mathbb{R}$ has uncountably many limit points.
22. Find a function $f : [0, 1] \to [0, 1]$ such that for each nontrivial interval $I \subseteq [0, 1]$ we have $f(I) = [0, 1]$.
23. Let a and k be positive integers. Prove that for every positive integer d, there exists a positive integer n such that d divides $ka^n + n$.

Solutions

1. First we will prove by induction the following proposition:

$$P(n): \text{ “The set } A \text{ has a finite subset with } n \text{ elements.”}$$

The set A is nonempty, so we can find an element $a_1 \in A$. Then $A_1 = \{a_1\}$ is a finite subset of A with one element, thus $P(1)$ is true.

Assume now that $P(k)$ is true, so A has a finite subset with k elements,

$$A_k = \{a_1, a_2, \ldots, a_k\} \subset A.$$

The set A is infinite, while A_k is finite, so the set $A \setminus A_k$ is nonempty. If we choose an element $a_{k+1} \in A \setminus A_k$, then the set

$$A_k = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$$

is a finite subset of A, with $k + 1$ elements. Hence $P(k + 1)$ is true.

Further, we prove that A has a countable subset. As we proved, for every positive integer n, we can find a finite subset $A_n \subset A$ with n elements. Then the set

$$S = \bigcup_{n \geq 1} A_n \subseteq A$$

is an infinite subset of A. Moreover, S is countable, as a countable union of finite sets.

2. Let us assume by contradiction that $A = (0, 1)$ is countable, say

$$A = \{x_n \mid n \in \mathbb{N},\ n \geq 1\}.$$

Let us consider the decimal representations of the elements of A,

$$x_1 = 0.a_{11}a_{12}a_{13}\ldots a_{1n}\ldots$$
$$x_2 = 0.a_{21}a_{22}a_{23}\ldots a_{2n}\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_n = 0.a_{n1}a_{n2}a_{n3}\ldots a_{nn}\ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$

For each integer $k \geq 1$, we choose a digit denoted b_k so that

$$b_k \neq a_{kk} \ , \ b_k \neq 9 \ , \ b_k \neq 0.$$

Now let us define the number

$$x = 0.b_1b_2b_3\ldots b_n\ldots \ .$$

Obviously, $x \in (0,1)$, so there is an integer $m \geq 1$ for which $x = x_m$. But the equality $x = x_m$ implies

$$0.b_1b_2b_3\ldots b_n\ldots = 0.a_{m1}a_{m2}a_{m3}\ldots a_{mm}\ldots \ ,$$

which is impossible, because the decimal of rank m are different, $b_m \neq a_{mm}$. Now, let us assume by way of contradiction that $\mathbb{R} = \{x_n \mid n \geq 1\}$ is countable. Obviously, there exists a subsequence $(x_{k_n})_{n\geq 1}$ of $(x_n)_{n\geq 1}$ such that

$$(0,1) = \{x_{k_n} \mid n \geq 1\}.$$

This means that $(0,1)$ is countable, which we just showed to be false.

Finally, we use the fact that the union of two countable sets is also a countable set. If $\mathbb{R} \setminus \mathbb{Q}$ is countable, it should follow that $\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$ is countable, as union of two countable sets. This contradiction shows that $\mathbb{R} \setminus \mathbb{Q}$ is not countable.

3. The sets A, B are countable so we can assume that

$$A = \{a_1, a_2, \ldots, a_n, \ldots\}, \quad B = \{b_1, b_2, \ldots, b_n, \ldots\}.$$

Let us define the map

$$f : X \cup A \cup B \to X \cup A$$

given by the formula

$$f(x) = \begin{cases} x, & \text{if } x \in X \\ a_{2n}, & \text{if } x \in A,\ x = a_n \\ a_{2n-1}, & \text{if } x \in B,\ x = b_n \end{cases}.$$

First, the map f is well defined: it takes (all) values in $X \cup A$. Hence it is surjective. For injectivity, note that f is injective on each restriction to X, A, and B. Then f is injective on $X \cup A \cup B$, if we take into account that any two of the sets

$$f(X) = X, \quad f(A) = \{a_2, a_4, \ldots, a_{2n}, \ldots\}, \quad f(B) = \{a_1, a_3, \ldots, a_{2n-1}, \ldots\}$$

are disjoint.

For the second part of the problem, let A be a countable subset of $\mathbb{R} \setminus B$. This choice is possible, because the set $\mathbb{R} \setminus B$ is nonempty and infinite. If $X = \mathbb{R} \setminus (A \cup B)$, then

$$\mathbb{R} \setminus B = X \cup A, \quad \mathbb{R} = X \cup A \cup B,$$

with A, B countable, and the conclusion follows, according to the first part of the problem.

4. We begin by proving the implication

$$A \sim B \Rightarrow A \times C \sim B \times C,$$

for all sets A, B, C. Indeed, if $f : A \to B$ is a bijection, then the map

$$\phi : A \times C \to B \times C$$

given by

$$\phi(a, c) = (f(a), c) \ , \quad a \in A, \ c \in C,$$

is also a bijection, so $A \times C \sim B \times C$.

We have already proved that $\mathbb{N} \sim \mathbb{N} \times \mathbb{N}$. According to the above remark,

$$\mathbb{N} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \times \mathbb{N}.$$

Finally, by transitivity,

$$\mathbb{N} \sim \mathbb{N} \times \mathbb{N} \sim \mathbb{N} \times \mathbb{N} \times \mathbb{N},$$

so $\mathbb{N} \sim \mathbb{N} \times \mathbb{N} \times \mathbb{N}$.

In a similar way, the sets $\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}$ are countable, too. As well, note that

$$f : \mathbb{N} \to \mathbb{N} \times \mathbb{N} \times \mathbb{N} \ , \quad f(n) = (n, 0, 0)$$

is injective and

$$g : \mathbb{N} \times \mathbb{N} \times \mathbb{N} \to \mathbb{N} \ , \quad g(m, n, p) = 2^m \cdot 3^n \cdot 5^p$$

is injective. The conclusion follows by Cantor-Bernstein theorem. This method can also be used to prove that $\mathbb{N} \times \mathbb{N} \times \ldots \times \mathbb{N}$ is countable.

5. One idea is to search a linear function $f(x) = mx + n$ from $(0,1)$ onto (a,b). In order to determine the values m, n, we impose the condition $f(0) = a$ and $f(1) = b$. It gives

$$\begin{cases} n = a \\ m + n = b \end{cases} \Rightarrow \begin{cases} n = a \\ m = b - a \end{cases}.$$

Consequently, the function $f : (0,1) \to (a,b)$, given by

$$f(x) = (b-a)x + a$$

is bijective, so $(0,1)$ is equivalent to every interval (a,b).

For the other part, it is sufficient to prove that $\mathbb{R}$ is equivalent to some open interval. Indeed, we can see that the function $\phi : \mathbb{R} \to \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$, given by $\phi(x) = \arctan x$ is bijective.

6. Assume that $A = \{a_n \mid n \in \mathbb{N}\}$, so that $a_0 = a$.

Then the bijection $f : A \setminus \{a\} \to A$ given by the formula $f(a_n) = a_{n-1}$, $n \in \mathbb{N}$, $n \geq 1$, shows us that $A \setminus \{a\} \sim A$.

$$\begin{array}{ccccccccccc} & & a_1 & & a_2 & & a_3 & & a_4 & & a_5 & & \dots \\ & \swarrow & & \swarrow & & \swarrow & & \swarrow & & \swarrow & & \swarrow & \\ a_0 & & a_1 & & a_2 & & a_3 & & a_4 & & a_5 & & \dots \end{array}.$$

The result remains true if A is an arbitrary infinite set.

Indeed, let $B = \{x_n \mid n \in \mathbb{N}\}$ be a countable subset of A. We choose $x_0 = a$, then define the function $\phi : A \setminus \{a\} \to A$ by the formula

$$\phi(x) = \begin{cases} x, & x \in A \setminus B \\ x_{n-1}, & x \in B,\ x = x_n,\ n \geq 1 \end{cases}.$$

In a classical way, we can easily prove that ϕ is bijective. Moreover, we can indicate its inverse $\phi^{-1} : A \to A \setminus \{a\}$ with

$$\phi^{-1}(x) = \begin{cases} x, & x \in A \setminus B \\ x_{n+1}, & x \in B,\ x = x_n,\ n \geq 1 \end{cases}.$$

7. We have already proved that $A \setminus \{x\} \sim A$, for every infinite set A and $x \in A$. In our case,

$$[a,b] \sim [a,b] \setminus \{b\} \Leftrightarrow [a,b] \sim [a,b),$$

$$[a,b] \sim [a,b] \setminus \{a\} \Leftrightarrow [a,b] \sim (a,b]$$

and further

$$(a,b] \sim (a,b] \setminus \{b\} \Leftrightarrow (a,b] \sim (a,b).$$

Finally, from transitivity,

$$[a,b] \sim [a,b) \sim (a,b] \sim (a,b).$$

8. For each element $x \in A$, consider the interval

$$I_x = \left(x - \frac{\varepsilon}{2}, x + \frac{\varepsilon}{2}\right).$$

If $x, y \in A,\ x \neq y$, then $I_x \cap I_y = \emptyset$.

Indeed, if there is c in $I_x \cap I_y$, then

$$\varepsilon < |x-y| \leq |x-c| + |y-c| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon,$$

which is false. Now, for each $x \in A$, we choose a rational number $r_x \in I_x$. As we have proved, $x \neq y \Rightarrow r_x \neq r_y$, which can be expressed that the map $\phi : A \to \mathbb{Q}$ given by the law $\phi(x) = r_x$, for all $x \in A$, is injective. Finally, A is at most countable because $\mathbb{Q}$ is countable.

9. For every integer n, we put $S_n = S \cap [n, n+1]$. According to the hypothesis, all sets $S_n,\ n \in \mathbb{Z}$ are finite. Thus the set

$$S = \bigcup_{n \in \mathbb{Z}} S_n$$

is at most countable, as a countable union of finite sets.

The answer to the question is negative. There exist sets S with the property from the hypothesis, which are not ε-discrete. An example is

$$S = \{\ln n \mid n \in \mathbb{N}^*\}.$$

10. First we prove that there exists r such that the set $S^-(r)$ is infinite and uncountable. If we assume the contrary, then the decomposition

$$S = \bigcup_{n \in \mathbb{Z}} S^-(n),$$

is a countable union of at most countable sets. Hence S is countable, a contradiction. Let

$$\alpha = \inf\{r \mid S^-(r) \text{ infinite and uncountable}\}$$

and similarly, we can define

$$\beta = \sup\left\{r \mid S^+(r) \text{ infinite and uncountable}\right\},$$

where cases $\alpha = -\infty$ or $\beta = \infty$ are accepted.

We prove that $\alpha \leq \beta$. If $\beta < \alpha$, then let $\beta < t < \alpha$. According to the definition of α, the set $S^-(t)$ is countable, and from the definition of β, the set $S^+(t)$ is countable. Hence S is countable, as union of two countable sets,

$$S = S^-(t) \cup S^+(t).$$

Consequently, $\alpha \leq \beta$. Then for every $\alpha \leq t_0 \leq \beta$, the sets $S^-(t_0)$ and $S^+(t_0)$ are infinite and uncountable, because

$$S^-(t_0) \supseteq S^-(\alpha), \quad S^+(t_0) \supseteq S^+(\beta).$$

11. For each integer $n \geq 1$, define the set

$$A_n = \left\{x \in M \mid x > \frac{1}{n}\right\}.$$

Easily, $M = \bigcup_{n\geq 1} A_n$. We will prove that every set A_n is finite or empty, so M is countable as a countable union of finite sets. Now we can prove that A_n has at most $7n$ elements. If for some n, the set A_n has at least $7n + 1$ elements, say $x_1, x_2, \ldots x_{7n+1} \in A$, then

$$x_1 > \frac{1}{n}\ ,\ x_2 > \frac{1}{n}\ \ ,\ \ \ldots\ \ ,\ \ x_{7n+1} > \frac{1}{n}.$$

By adding,

$$x_1 + x_2 + \cdots + x_{7n+1} > \frac{7n+1}{n} > 7,$$

which is a contradiction.

12. For each polynomial $P \in \mathbb{Z}[X]$,

$$P = a_0 + a_1X + \cdots + a_nX^n,$$

define and denote by

$$h(P) = n + |a_0| + |a_1| + \cdots + |a_n|$$

the height of P, $h(0) = 0$. Let us put for each nonnegative integer k,

$$\mathcal{P}_k = \{P \in \mathbb{Z}[X] \mid h(P) = k\}.$$

Each set $\mathcal{P}_k$ is finite, possibly empty, so

$$\mathbb{Z}[X] = \bigcup_{k\in\mathbb{N}} \mathcal{P}_k$$

is countable, as a countable union of finite sets. Indeed, there are only a finite number of polynomials with $h(P) = k$. First, note that if $h(P) = k$, then $\deg P \leq k$ and $|a_0|, |a_1|, \ldots, |a_n| \leq k$. Consequently, P is defined by a finite number of integer coefficients $a_0, a_1, \ldots, a_n$ which are less than or equal to k in absolute value.

13. The set $\mathcal{A}$ of algebraic numbers is the set of real roots of all nonconstant polynomials with integer coefficients. Using this remark, we can write

$$\mathcal{A} = \bigcup_{P\in\mathbb{Z}_1[X]} \{x \in \mathbb{R} \mid P(x) = 0\},$$

where

$$\mathbb{Z}_1[X] = \mathbb{Z}[X] \setminus \{0\}.$$

Consequently, $\mathcal{A}$ is countable as a countable union of finite sets. Indeed, each set from the union has at most k elements, where $k = \deg P$.

14. The function $\phi : X \to \mathcal{P}(X)$ given by $\phi(x) = \{x\}$, for all $x \in X$, is injective, so $|X| \leq |\mathcal{P}(X)|$. Thus we have to prove that there are no bijections from X onto $\mathcal{P}(X)$. If we assume by contradiction that there is a bijection $f : X \to \mathcal{P}(X)$, then define the set $A = \{x \in X \mid x \notin f(x)\}$, $A \in \mathcal{P}(X)$. Because of the surjectivity of f, we have $A = f(x_0)$, for some $x_0 \in X$. Now the question is

$$x_0 \in A \quad \text{or} \quad x_0 \notin A\,?$$

If $x_0 \in A$, then $x_0 \notin f(x_0)$, false because $f(x_0) = A$. If $x_0 \notin A$, then $x_0 \in f(x_0)$, false, because $f(x_0) = A$.

The last two implications follow from the definition of the set A. These contradictions solve the problem.

One way to see that the second statement of the problem is true is to consider the function that maps every finite subset $\{n_1, \ldots, n_k\}$ of $\mathbb{N}$ to the natural number $2^{n_1} + \cdots + 2^{n_k}$ (and maps the empty set to 0). This mapping is clearly a bijection (since every positive integer has a unique binary representation), and the conclusion follows.

Or, one can see that this is an enumeration of all finite sets of $\mathbb{N}$:

$$\emptyset,\ \{0\},\ \{1\},\ \{0,1\},\ \{2\},\ \{0,2\},\ \{1,2\},\ \{0,1,2\},\ \{3\}, \ldots$$

(we leave to the reader to decipher how the sets are enumerated; we think that he/she will do).

Finally, one can see that the set $\mathcal{P}_f(\mathbb{N})$ of finite parts of $\mathbb{N}$ is the union of the sets P_i, where P_i means the set of finite subsets of $\mathbb{N}$ having the sum of their elements precisely i; since every P_i is finite, $\mathcal{P}_f(\mathbb{N})$ is countable (as a countable union of finite sets). The reader will surely find a few more approaches.

15. Denote $p = p_1 p_2 \dots p_k$. Let us define the function

$$f : \mathbb{Z}_p \to \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_k}$$

by the formula

$$f(r \bmod p) = (r \bmod p_1, r \bmod p_2, \dots, r \bmod p_k) \ , \quad r \in \{0, 1, \dots, p-1\} .$$

The sets $\mathbb{Z}_p$ and $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \dots \times \mathbb{Z}_{p_k}$ have the same number of elements. In fact, the problem asks to show that f is surjective. Under our hypothesis, it is sufficient to prove that f is injective. In this sense, let $r, s \in \{0, 1, \dots, p-1\}$ be such that

$$(r \bmod p_1, r \bmod p_2, \dots, r \bmod p_k) = (s \bmod p_1, s \bmod p_2, \dots, s \bmod p_k).$$

It follows that

$$r \bmod p_1 = s \bmod p_1, \dots, r \bmod p_k = s \bmod p_k,$$

or $p_1 | r - s$, $p_2 | r - s$, $\dots$, $p_k | r - s$. Hence $p | r - s$, which is equivalent to $r \bmod p = s \bmod p$. This proves the injectivity of f.

16. For each integer k, there exists at most one element $f(x) \in [k, k+1)$. Therefore to each real number x, we can assign a unique integer $k = k(x)$ such that $f(x) \in [k, k+1)$. Thus, the function

$$\mathbb{R} \ni x \longmapsto k(x) \in \mathbb{Z}$$

is injective. This is impossible, because $\mathbb{R}$ is not countable and $\mathbb{Z}$ is countable.

Another method uses the injectivity of f. Indeed, if $x \neq y$, then $|f(x) - f(y)| \geq 1$, so the equality $f(x) = f(y)$ is not possible. The inequality from the hypothesis says that the image of the function f is a 1-discrete set, so it is at most countable. Now, the map $f : \mathbb{R} \to \operatorname{Im} f$ is injective, so

$$\operatorname{card} \mathbb{R} \leq \operatorname{card} \operatorname{Im} f.$$

This is impossible, because $\mathbb{R}$ is not countable.

17. Let us assume, by way of contradiction, that such a function f does exist. Define $g : (-1, 1) \to \mathbb{R}$, given by $g(x) = f(x)$, for all $x \in (-1, 1)$. Then

$$|g(x) - g(y)| \geq \frac{1}{2},$$

for all $x, y \in (-1, 1)$, $x \neq y$. Indeed,

$$|g(x) - g(y)| \geq \frac{1}{x^2 + y^2} \geq \frac{1}{2}.$$

Now define $h : \mathbb{R} \to \mathbb{R}$ by $h = 2 \cdot (g \circ \phi)$, where $\phi : \mathbb{R} \to (-1, 1)$ is

$$\phi(x) = \frac{2}{\pi} \arctan x.$$

Finally, the function $h : \mathbb{R} \to \mathbb{R}$ satisfies

$$|h(x) - h(y)| \geq 1,$$

for all $x, y \in \mathbb{R}$, $x \neq y$, which is impossible, as we have seen in the previous problem.

18. Let D be the discontinuity set of f. It is well known that D contains only discontinuities of the first kind if f is monotone. We mean that for each $x \in D$, there exist finite one-sided limits denoted

$$f_s(x) = \lim_{y \nearrow x} f(y) \quad , \quad f_d(x) = \lim_{y \searrow x} f(y).$$

If f is increasing, then $f_s(x) \leq f_d(x)$, with strict inequality if $x \in D$. Now, for every $x \in D$, we choose a rational number denoted

$$r_x \in (f_s(x), f_d(x))$$

and we define the function

$$D \ni x \overset{f}{\longmapsto} r_x \in \mathbb{Q}.$$

It is injective because of the implication

$$x < y \Rightarrow f_d(x) \leq f_s(y).$$

Finally, D is countable, because $\mathbb{Q}$ is countable.

19. Take any semi-convergent series of real numbers with general term a_n (for instance, $a_n = \frac{(-1)^n}{n}$) and apply Riemann's theorem: for any real number a there exists a permutation π of the set of positive integers such that $a_{\pi(1)} + a_{\pi(2)} + \ldots = a$. This gives an injection from the set of real numbers into the set of permutations of the positive integers. Since the former is uncountable, so is the desired set.

20. Let us consider a rational number $r(x)$ between $f(x)$ and $g(x)$ and look at the sets A_x of those real numbers a such that $r(a) = x$. The union of these sets (taken

over all rational numbers x) is the set of real numbers, which is uncountable. So, at least one of these sets is uncountable, and it clearly satisfies the conditions.

21. Suppose that A is a subset of $\mathbb{R}$ that has a countable set of limit points. The points from A split into two classes: those that are limit points of A (denote by B this set) and those that are not (let C be this second subset of A). But any point c from C must have a neighborhood that does not intersect A (with the exception of c), and this neighborhood may be chosen to be an open interval that contains c and has rational points as extremities. Therefore C is countable (possibly finite).

    So, if we assume that the set of limit points of A is at most countable, B is also at most countable; then, since $A = B \cup C$, the countability of A follows, and this proves the problem's claim by contraposition.

22. Let us consider on $[0, 1]$ the relation "$\sim$" defined by

$$a \sim b \Leftrightarrow a - b \in \mathbb{Q}.$$

Clearly, this is an equivalence relation; thus we can find a complete system of representatives of the equivalence classes, that is, a set $A \subseteq [0, 1]$ such that any distinct $a, b \in A$ are not in the relation $\sim$ and for each $t \in [0, 1]$, there is a (unique) $a \in A$ for which $t \sim a$. We have

$$[0, 1] = \bigcup_{a \in A} X_a$$

if we denote by X_a the equivalence class of a. Since

$$X_a = \{y \in [0, 1] | y - a \in \mathbb{Q}\} = \{a + t | t \in \mathbb{Q} \cap [-a, 1 - a]\},$$

we see that each class X_a is dense in $[0, 1]$ and is a countable set. If A was countable, then $[0, 1]$ would be countable, too, as a countable union of countable sets. Since this is not the case, we infer that A is not countable, hence a bijection $\varphi : [0, 1] \to A$ can be found.

Then we can define the desired function $f : [0, 1] \to [0, 1]$ by setting

$$f(x) = t,$$

for all $x \in X_{\varphi(t)}$ and for suitably chosen $t \in [0, 1]$. Since each $x \in [0, 1]$ belongs to exactly one set X_a and for each $a \in A$ there is a unique $t \in [0, 1]$ such that $a = \varphi(t)$, the function f is well defined.

Now, let $I \subseteq [0, 1]$ be an interval which is not reduced to one point. I contains elements from any set X_a, $a \in A$ (since the classes of equivalence are dense in $[0, 1]$). An arbitrary $t \in [0, 1]$ being given, the intersection of I with $X_{\varphi(t)}$ is nonempty; so we can consider an $x \in I \cap X_{\varphi(t)}$ for which we have $f(x) = t$. Thus, we see that f takes in I any value $t \in [0, 1]$, that is, the desired result.

This is problem 1795, proposed by Jeff Groah in *Mathematics Magazine*, 2/2008. Two more solutions can be found in the same *Magazine*, 2/2009.

23. We prove the slightly more general statement that, for positive integers a, k, d, and N, there exist positive integers n_i, $0 \leq i \leq d-1$ such that $n_i > N$ and $ka^{n_i} + n_i \equiv i \pmod{d}$ for all $0 \leq i \leq d-1$. Of course, $n = n_0$ is the solution to our problem.

The proof of the general result is by induction on d. For $d = 1$, we have nothing to prove (and even for $d = 2$, one can easily prove the statement). So, let's assume it is true for all positive integers $d < D$ and deduce it for D. Also, assume that some positive integer N has been fixed.

We can consider the (smallest) period p of a modulo D; that is, p is the smallest positive integer such that $a^{m+p} \equiv a^m$ for all $m > M$, M being a certain nonnegative integer. We then also have $a^{m+lp} \equiv a^m \pmod{D}$ for all nonnegative integers $m > M$ and l. Yet, note that $p < D$ because the sequence of powers of a modulo D either contains 0 (and then $p = 1$), or it doesn't (and then, surely, p is at most $D-1$). Consequently, $d = (D, p)$ is also less than D and we can apply the induction hypothesis to infer that there exist positive integers m_i such that $m_i > \max\{M, N\}$ and $ka^{m_i} + m_i \equiv i \pmod{d}$ for all $0 \leq i \leq d-1$.

We claim that the numbers $ka^{m_i+sp} + (m_i + sp)$, with $0 \leq i \leq d-1$, and $0 \leq s \leq D/d - 1$ are mutually distinct modulo D. Indeed, suppose that

$$ka^{m_i+sp} + (m_i + sp) \equiv ka^{m_j+tp} + (m_j + tp) \pmod{D},$$

for $i, j \in \{0, 1, \ldots, d-1\}$, and $s, t \in \{0, 1, \ldots, D/d - 1\}$. Since p is a period of a modulo D and m_i are (by choice) greater than M, we get $ka^{m_i} + (m_i + sp) \equiv ka^{m_j} + (m_j + tp) \pmod{D}$, and because d is a divisor of D, this congruence is also true modulo d. Again by the choice of the m_i, $ka^{m_i} + (m_i + sp) \equiv ka^{m_j} + (m_j + tp) \pmod{d}$ becomes $i + sp \equiv j + tp \pmod{d}$, and then $i \equiv j \pmod{d}$ (as d is also a divisor of p). But i, j are from the set $\{0, 1, \ldots, d-1\}$, thus $i = j$. Going back to the initial congruence, we see that it becomes $sp \equiv tp \pmod{D}$, yielding $s(p/d) \equiv t(p/d) \pmod{D/d}$. But p/d and D/d are relatively prime, hence we get $s \equiv t \pmod{D/d}$ which, together with $s, t \in \{0, 1, \ldots, D/d - 1\}$, implies $s = t$ and the fact that the two original numbers are equal.

Thus we have the $d \cdot (D/d) = D$ numbers $ka^{m_i+sp} + (m_i + sp)$, with $0 \leq i \leq d-1$, and $0 \leq s \leq D/d - 1$ that are mutually distinct modulo D; therefore they produce all possible remainders when divided by D (and here is our cardinality argument; remember problem 15, that is, roughly, the Chinese remainder theorem). This means that we can rename by n_h, $0 \leq h \leq D-1$, the numbers $m_i + sp$, $0 \leq i \leq d$, $0 \leq s \leq D/d - 1$ in such a way that $ka^{n_h} + n_h \equiv h \pmod{D}$ for each $0 \leq h \leq D-1$, and this is exactly what we wanted to prove for completing the induction.

This is Problem 11789, proposed by Gregory Galperin and Yury J. Ionin in *The American Mathematical Monthly*. A different solution by Mark Wildon appeared in the same *Monthly* from August to September 2016. Note, however, that our proof is nothing but a rewording of the official solution of the seventh

shortlisted number theory problem from the 47th IMO, Slovenia, 2006. (The shortlisted problems can be found on the official site of the IMO.) That problem asks to show that, given a positive integer d, there exists a positive integer n such that $2^n + n$ is divisible by d.

http://www.springer.com/978-0-8176-4394-2

Mathematical Bridges

Andreescu, T.; Mortici, C.; Tetiva, M.
2017, VIII, 309 p. 3 illus., Hardcover
ISBN: 978-0-8176-4394-2
A product of Birkhäuser Basel