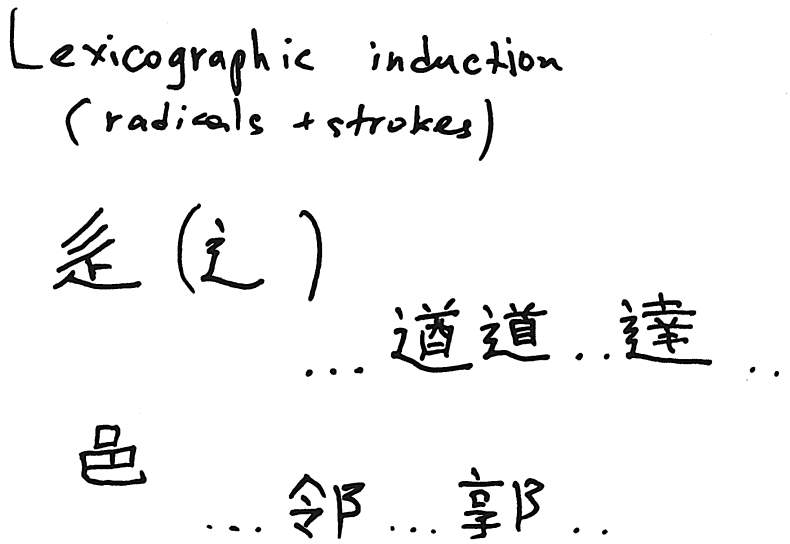
Basic concepts in mathematics: Diary

Nikita Kalinin, Diego Armando Sulca, Raphaël Fesler, Shuliang Gao



Guangdong Technion Israel Institute of Technology
Shantou, China
December 16, 2025

Contents

0 Preface

From a cup of coffee, a spoonful of coffee is poured into a cup of milk. Then a spoonful of the resulting mixture is poured back into the cup of coffee. Which is greater: the amount of milk in the cup of coffee or the amount of coffee in the cup of milk?

This course is intended for first-year students in mathematics and computer science; they have to learn how to read and write proofs.

It is not obvious at all why we need to prove something (professors demand it, but why?). The truth is that by proving we understand things better and discover new beauties (e.g., the formula $1^3 + 2^3 + \cdots + n^3 = (1 + 2 + .. + n)^2$).

So, to reconcile the concept of proof with students, it is better to introduce proofs in questions whose answers are not obvious and are debatable. Examples logic puzzles, games (who has a winning strategy?), impossibility proofs (e.g., tiling a chessboard missing opposite corners with dominoes), and induction. These topics occupy the first few lectures.

How do you learn to prove? Let us use the metaphor "Mathematics is a language". When you learn a foreign language, you have different activities: listening, speaking, reading, writing. The same is true for mathematics. To study it, students should spend time reading and writing mathematics, listening to lectures, thinking about problems, and discussing ideas.

Also, mathematicians love mathematics because proofs are beautiful!

Solution to the coffee-milk problem:

Let's try to guess the answer. To do that, consider an extreme case (this is the first idea). Suppose there is just one spoonful of liquid in each cup. Then after pouring the coffee into the milk, we take the entire mixture back. The mixture will be uniform, so the amount of coffee and milk will be equal. Will it always be equal?

Since one spoonful was poured "there and back," the total volume of liquid in each cup did not change (this is the second idea).

Therefore (the third idea), the amount of coffee lost equals the amount of milk gained.

The volumes of coffee and milk in the cups can be different, you can pour the spoon back and forth ten times, you can even stir the mixture poorly — it doesn't matter: the amount of milk in the coffee will always equal the amount of coffee in the milk!

0.1 :: on collaboration and the use of AI

Collaboration. You are encouraged to discuss problems with classmates: compare approaches, explain ideas to one another, and ask for critique. Explaining your reasoning often reveals subtleties and gaps that you can then address. However, each student must write up their own solution independently, in their own words, after any discussion. Do not share written solutions or allow others to copy your work.

Attempt first. Before seeking help from classmates or AI tools, make a genuine attempt on each problem: write down an outline, partial calculations, or a strategy you tried (even if it failed). Learning to prove requires practice—like training for a sport—so expect to try, err, and revise.

AI: permitted uses. You may use AI tools to: (i) spot logical gaps or unclear steps in a solution you have already written, (ii) improve clarity and writing style, (iii) receive high-level hints about relevant definitions or theorems. When you do so, begin with your own draft (typed or a photo) and ask for feedback on that draft.

AI: not permitted uses (unless explicitly allowed). Do not ask AI to produce full solutions for graded assignments or to translate someone else's solution into "your own words." Do not paste problem statements and accept verbatim answers. Use AI as a reviewer, not as an author. If you are unsure whether a use is allowed, ask the instructor.

Reflection Logs. It is useful to reflect on how you use AI, so record the tool and its purpose in your diary, and then track how it affects your understanding and your ability to solve problems, write solutions, and read material without any outside help. Note that during the exams or midterms you cannot rely on anything except yourself.

Academic integrity. Copying another person's solution or submitting AI-generated solutions as your own is plagiarism. Violations will be handled under the university's academic integrity policy.

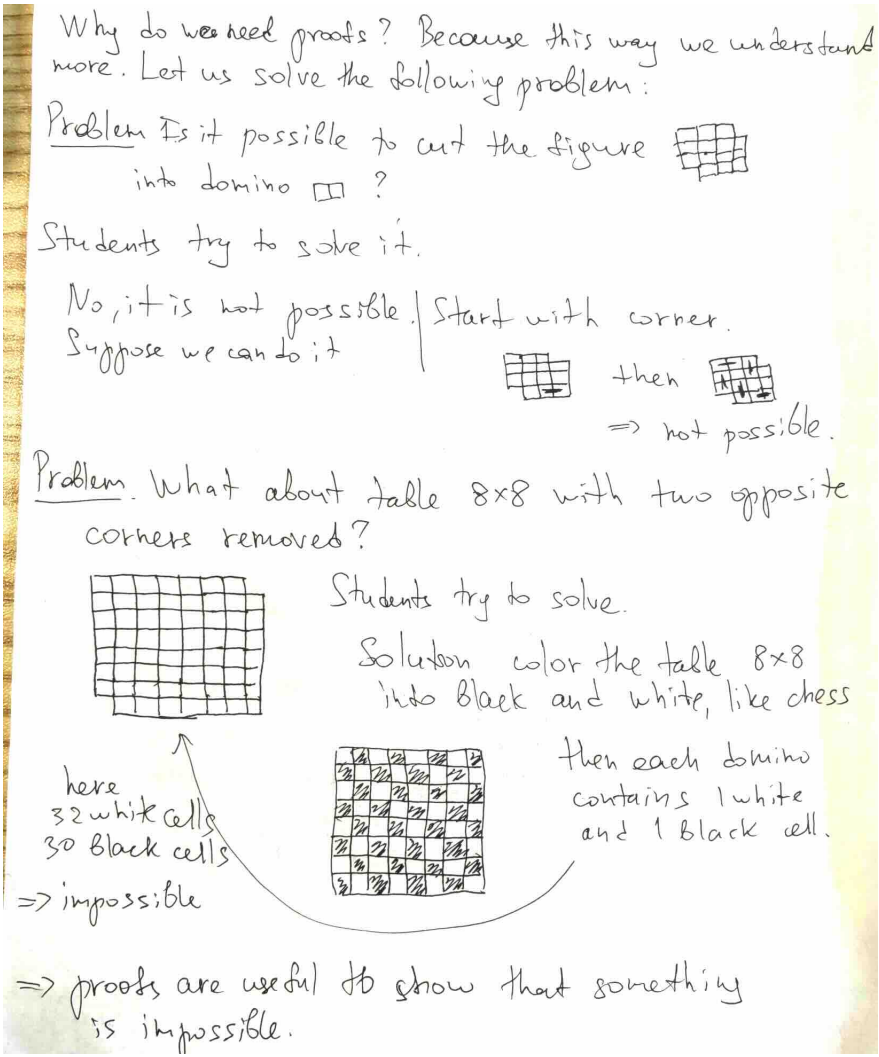
0.2 :: credits

The first chapter consists of edited AI-translated excerpts from the excellent book (in Russian) of Kanel-Belov and Kovaldgi "How to solve non-standard probelms" https://old.mccme.ru/free-books/olymp/KanKov.pdf

1 Methods of proving

1.1 :: parity, induction

1.1.1 :: :: parity



Many problems become much easier once one notices that some quantity has a fixed *parity* (it is always even or always odd). Once a parity is fixed, any situation in

which that quantity would have the opposite parity is impossible. Sometimes one has to construct this quantity, for example by considering the parity of a sum or product, by pairing objects up, by noticing an alternating pattern, or by colouring objects in two colours.

Example 1. *A grasshopper makes jumps of length 1 m along a straight line and eventually returns to its starting point. Show that it made an even number of jumps.*

Solution. If the grasshopper ends where it started then the number of jumps to the right must equal the number of jumps to the left. Consequently the total number of jumps is even.

Example 2. *Does there exist a closed broken line with seven segments that crosses each of its segments exactly once?*

Solution. Suppose such a broken line existed. Any two crossing segments can be paired. The number of segments must therefore be even, which contradicts the assumption that there are seven segments.

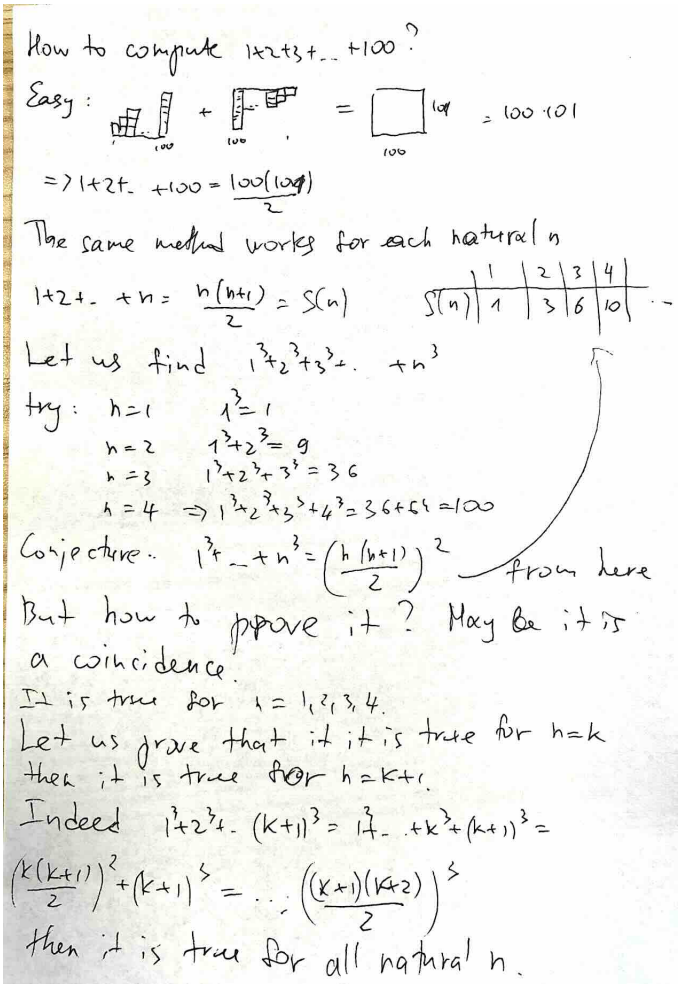
Example 3. *Martians may have any number of arms. One day all Martians joined hands in such a way that no free arms remained. Prove that the number of Martians with an odd number of arms is even.*

Solution. Call Martians with an even number of arms *even* and those with an odd number of arms *odd*. Since the hands form pairs, the total number of hands is even. The total number of hands of the even Martians is clearly even, so the total number of hands of the odd Martians must also be even. But each odd Martian contributes an odd number of hands, so there must be an even number of them.

Such pictures are called *graphs*, they consist of *vertices* (representing Martians) and *edges* (representing a handshaking pair of hands). The number of edges incident to a vertex (i.e. the number of hands of a Martian) is called the *degree* (or *valency*) of a vertex. See Section 5.1.

We proved that in each graph the number of vertices of odd degree is even.

1.1.2 :: :: induction



The method of mathematical induction is used to prove statements of the form "For every natural number n a certain property holds." Such a statement can be viewed as an infinite chain of assertions: "For $n = 1$ the property holds", "For $n = 2$ the property holds", and so on. The first assertion in the chain is called the base (or the foundation) of the induction and is usually easy to check. One then proves the induction step: "If the assertion with number n is true, then the assertion with number $n + 1$ is true." Sometimes one needs a stronger form of the induction step: "If all assertions with numbers from 1 to n are true, then the assertion with number

$n+1$ is true." There is also the technique of *inductive descent*, in which one proves that if an assertion with number n (with $n > 1$) can be reduced to one or several assertions with smaller numbers and the first assertion is true, then all assertions are true.

If both the base and the induction step have been proved, then all assertions in the chain hold; this is the principle of mathematical induction.

Example 1. *Prove that the number consisting of 243 consecutive ones is divisible by 243.*

Solution. Notice that $243 = 3^5$. We shall prove a more general statement: the number consisting of 3^n consecutive ones is divisible by 3^n. For $n = 1$ the assertion says that 111 is divisible by 3, which is true. Suppose the number consisting of 3^{n-1} ones is divisible by 3^{n-1}. Write

$$\underbrace{11\cdots1}_{3^n \text{ times}} = \underbrace{11\cdots1}_{3^{n-1} \text{ times}} \times \underbrace{10\cdots010\cdots01}_{\text{a block containing only one non zero digit}}.$$

It is not hard to check that the second factor on the right–hand side is divisible by 3. Multiplying a multiple of 3^{n-1} by a multiple of 3 yields a multiple of 3^n. Therefore the number of 3^n ones is divisible by 3^n, completing the induction.

Example 2. *Several lines and circles are drawn in the plane. Prove that the regions into which the plane is divided can be coloured in two colours so that adjacent regions (sharing a segment or an arc) are coloured differently.*

Solution. First erase all the lines and circles, remembering where they were. Colour the entire plane one colour. Then restore the boundaries one by one, recolouring the regions they divide. When adding a line, recolour in the opposite colour all regions on one side of it and leave unchanged those on the other side. When adding a circle, recolour all regions lying inside it and leave unchanged those outside. In this way each time you add a boundary the recoloured regions lie on one side only. Consequently any two neighbouring regions (sharing part of a boundary) always have different colours.

Example 3. *Prove that if $x + \frac{1}{x}$ is an integer, then $x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.*

Solution. Set $T_n = x^n + \frac{1}{x^n}$. Note that $T_0 = 2$ and $T_1 = x + 1/x$ are integers. Observe that

$$T_n T_1 = (x^n + \tfrac{1}{x^n})(x + \tfrac{1}{x}) = x^{n+1} + \tfrac{1}{x^{n+1}} + x^{n-1} + \tfrac{1}{x^{n-1}} = T_{n+1} + T_{n-1}.$$

Thus $T_{n+1} = T_n T_1 - T_{n-1}$. By induction on n this recurrence shows that all T_n are integers.

Example 4. (if time permits) *Five robbers have obtained a sack of gold sand. They wish to divide it so that each robber is sure he received at least one fifth of the gold. They have no measuring instruments, but each can judge by eye the amount of a pile of sand. Opinions about the size of the piles may differ. How can they divide the loot?*

Solution (First method). First two robbers divide the sand between themselves: one divides the sack into two piles that he believes equal, and the other chooses his pile. Each of these two divides his share into four equal (to his mind) parts, and the third robber takes one part from each. Now these three each divide their share into three parts and the fourth robber takes one part from each. Finally these four divide their shares into two parts and the fifth robber takes one part from each. Each robber can check that the portion he receives is at least one fifth according to his judgment.

Solution (Second method). Find the most modest robber and give him his portion first. To do so, ask the first robber to separate what he believes to be 1/5 of the sack. Ask the second robber whether the separated part is larger than 1/5: if he thinks it is larger, have him reduce it to what he considers 1/5; if he thinks it is not larger, ask the third robber, and so on. When someone finally agrees that the separated part is exactly 1/5, give that part to the last person who modified it. Among the remaining robbers find the most modest of those and repeat. In the end every robber receives a portion he believes is at least 1/5 of the original amount.

1.1.3 :: :: problems for tutorial

1. You have coins of 3 HKD and 5 HKD. Prove that any number of HKD greater than seven can be exchanged for coins of 3 and 5 HKD.

2. Several lines divide the plane into regions. Each line grow hair on one side. Prove that there is a region all of whose boundaries have hair "outside". [1]

[1] Comment: Induct on the number of lines. Removing one line yields a configuration where the claim holds; then restore the line and pick an appropriate subregion on the hatched side.

3. From a 128×128 square one unit square was removed. Prove that the remaining shape can be tiled with L shaped trominoes consisting of three unit squares.

4. For every natural k prove the inequality $2^k > k$.

5. Prove the Cauchy–Schwarz inequality in the form

$$\frac{x_1 + x_2 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 x_2 \cdots x_n},$$

where $x_1, \ldots, x_n$ are non negative numbers. [2]

1.1.4 :: :: problems for workshop

1. Can one break 25 HKD into ten coins of denominations 1, 3 and 5 HKD?[3]

2. Nine gears are arranged in a circle, each meshing with the next. The first meshes with the second, the second with the third, ..., the ninth with the first. Can they all rotate at the same time? What happens if there are n gears?[4]

3. A row contains 100 towers. You may interchange any two towers that have exactly one tower between them. Is it possible in this way to reverse the entire order of the towers?[5]

4. Six numbers $1, 2, 3, 4, 5, 6$ lie on the table. You are allowed to add 1 to any two of them. Can all the numbers eventually be made equal?[6]

---

[2] Comment: A common proof uses induction on n by first proving the case where n is a power of two and then reducing the general case to the nearest lower power of two. This problem invites the reader to explore that technique. See details in Section 5, page 149.

[3] Comment: Let x, y and z be the numbers of 1–, 3– and 5–HKD coins. Then $x + 3y + 5z = 25$ and $x + y + z = 10$. Subtracting yields $2y + 4z = 15$, which has no integer solutions. Therefore it is impossible.

[4] Comment: An odd number of meshed gears arranged in a cycle cannot all turn, because each contact reverses the sense of rotation. For an even number of gears a consistent rotation is possible.

[5] Comment: Label the positions $1, \ldots, 100$. A permitted move swaps the towers in positions i and $i + 2$, both of which have the same parity (both odd or both even). Consequently each tower always occupies squares of the same parity as its starting position. In the reversed arrangement the tower originally at position 1 would have to move to position 100 and hence to a square of opposite parity. This is impossible, so a complete reversal cannot be achieved.

[6] Comment: Each move increases the sum of the numbers by 2. If eventually all six numbers were equal to k, then $6k = 1 + 2 + 3 + 4 + 5 + 6 + 2t = 21 + 2t$. The left side is even, while $21 + 2t$ is odd for all t. Hence the numbers can never all become equal.

5. All dominoes from the standard set are laid out in a single chain according to the usual rule (neighbouring halves show the same number). One end of the chain has a five. What can be at the other end?[7]

6. Can a line that does not pass through any vertex of an 11–gon intersect all of its sides?[8]

7. On a table stand seven overturned cups. You may simultaneously turn over any two cups. Is it possible to end up with all the cups upright?[9]

[7] Comment: In the usual "double six" set the tiles are the pairs (i, j) with $1 \leq i \leq j \leq 6$. Each number $1, \ldots, 6$ occurs exactly six times. Consider the graph whose vertices are the numbers and whose edges correspond to dominoes. In this graph every vertex has even degree, so the tiles can be arranged in a closed Eulerian circuit. Cutting this circuit yields an open chain whose two ends are identical. Hence if one end displays a five, the other end must also display a five.

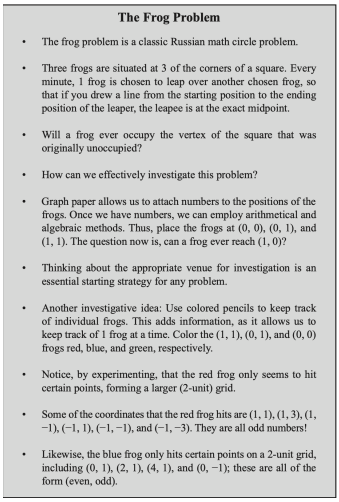
[8] Comment: In any polygon the number of intersections of a straight line with the sides is even (becasue the line goes inside the polygon, then outside, then inside,... finally it goes outside). Since 11 is odd, no such line exists.

[9] Comment: The parity of the number of overturned cups changes by 0 or 2 at each move. Starting with seven (odd) and wanting to end with zero (even) is impossible.

1.1.5 :: :: 1st homework

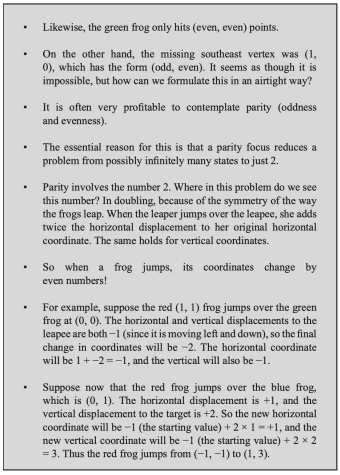
Read:

Paul Zeitz - The Art and Craft of Mathematical Problem Solving, pp. 13-15.

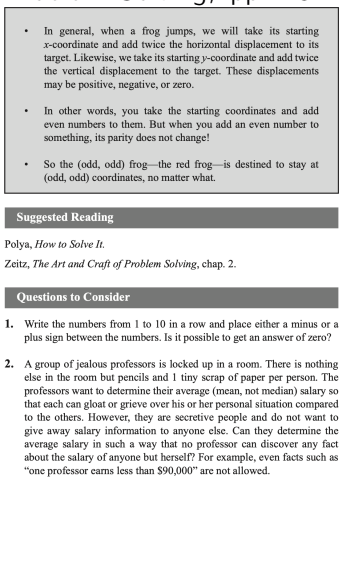


The Frog Problem

- The frog problem is a classic Russian math circle problem.
- Three frogs are situated at 3 of the corners of a square. Every minute, 1 frog is chosen to leap over another chosen frog, so that if you drew a line from the starting position to the ending position of the leaper, the leapee is at the exact midpoint.
- Will a frog ever occupy the vertex of the square that was originally unoccupied?
- How can we effectively investigate this problem?
- Graph paper allows us to attach numbers to the positions of the frogs. Once we have numbers, we can employ arithmetical and algebraic methods. Thus, place the frogs at (0, 0), (0, 1), and (1, 1). The question now is, can a frog ever reach (1, 0)?
- Thinking about the appropriate venue for investigation is an essential starting strategy for any problem.
- Another investigative idea: Use colored pencils to keep track of individual frogs. This adds information, as it allows us to keep track of 1 frog at a time. Color the (1, 1), (0, 1), and (0, 0) frogs red, blue, and green, respectively.
- Notice, by experimenting, that the red frog only seems to hit certain points, forming a larger (2-unit) grid.
- Some of the coordinates that the red frog hits are (1, 1), (1, 3), (1, −1), (−1, 1), (−1, −1), and (−1, −3). They are all odd numbers!
- Likewise, the blue frog only hits certain points on a 2-unit grid, including (0, 1), (2, 1), (4, 1), and (0, −1); these are all of the form (even, odd).



- Likewise, the green frog only hits (even, even) points.
- On the other hand, the missing southeast vertex was (1, 0), which has the form (odd, even). It seems as though it is impossible, but how can we formulate this in an airtight way?
- It is often very profitable to contemplate parity (oddness and evenness).
- The essential reason for this is that a parity focus reduces a problem from possibly infinitely many states to just 2.
- Parity involves the number 2. Where in this problem do we see this number? In doubling, because of the symmetry of the way the frogs leap. When the leaper jumps over the leapee, she adds twice the horizontal displacement to her original horizontal coordinate. The same holds for vertical coordinates.
- So when a frog jumps, its coordinates change by even numbers!
- For example, suppose the red (1, 1) frog jumps over the green frog at (0, 0). The horizontal and vertical displacements to the leapee are both −1 (since it is moving left and down), so the final change in coordinates will be −2. The horizontal coordinate will be 1 + −2 = −1, and the vertical will also be −1.
- Suppose now that the red frog jumps over the blue frog, which is (0, 1). The horizontal displacement is +1, and the vertical displacement to the target is +2. So the new horizontal coordinate will be −1 (the starting value) + 2 × 1 = +1, and the new vertical coordinate will be −1 (the starting value) + 2 × 2 = 3. Thus the red frog jumps from (−1, −1) to (1, 3).



- In general, when a frog jumps, we will take its starting x-coordinate and add twice the horizontal displacement to its target. Likewise, we take its starting y-coordinate and add twice the vertical displacement to the target. These displacements may be positive, negative, or zero.
- In other words, you take the starting coordinates and add even numbers to them. But when you add an even number to something, its parity does not change!
- So the (odd, odd) frog—the red frog—is destined to stay at (odd, odd) coordinates, no matter what.

Suggested Reading

Polya, *How to Solve It.*

Zeitz, *The Art and Craft of Problem Solving*, chap. 2.

Questions to Consider

1. Write the numbers from 1 to 10 in a row and place either a minus or a plus sign between the numbers. Is it possible to get an answer of zero?
2. A group of jealous professors is locked up in a room. There is nothing else in the room but pencils and 1 tiny scrap of paper per person. The professors want to determine their average (mean, not median) salary so that each can gloat or grieve over his or her personal situation compared to the others. However, they are secretive people and do not want to give away salary information to anyone else. Can they determine the average salary in such a way that no professor can discover any fact about the salary of anyone but herself? For example, even facts such as "one professor earns less than $90,000" are not allowed.

Write:

Problem 1. Write the full solution (with all details) of the problem that we cannot cut a square 4×4 without opposite corners into domino. Write the solution where we use case-by-case strategy, without using coloring.

Problem 2. Write the solution of the problem that we cannot cut a square 8×8 without opposite corners into domino (you can use coloring).

Problem 3. Show that you can cut a square in n squares for each $n > 6$.

Problem 4. The numbers $1, 2, \ldots, 101$ are written on a blackboard. You are allowed to erase any two numbers and write their difference in their place. After repeating this operation 100 times only one number remains. Prove that this number cannot be zero.

1.2 :: pigeonhole principle, correspondence, invariants

From a hundred rabbits, you can never assemble a horse;
a hundred suspicions do not consitute a proof.

Crime and Punishment, F. Dostoevsky

1.2.1 :: :: proof by contradiction

One of the most widely used techniques in elementary mathematics is the *proof by contradiction*. The general strategy is to assume that the statement to be proved is false and then show that this assumption leads to an impossibility. Having reached a contradiction, one concludes that the original statement must in fact be true.

Example 1. *Prove that there are infinitely many prime numbers.*

Solution. Suppose the contrary, namely that there are only finitely many primes. List them as $p_1, p_2, \ldots, p_n$. Consider the number

$$N = p_1\, p_2 \cdots p_n + 1.$$

By construction N is not divisible by any of the primes p_i. Therefore N has no prime divisors at all, which contradicts the fundamental fact that every integer greater than 1 has at least one prime divisor. Hence there cannot be only finitely many primes.

Example 2. *Five boys found nine mushrooms. Prove that at least two of them must have found the same number of mushrooms.*

Solution. Assume that the boys all found different numbers of mushrooms. Order them by increasing number of mushrooms: the first boy picked at least 0 mushrooms, the second at least 1, the third at least 2, the fourth at least 3 and the fifth at least 4. Altogether they would have picked at least $0 + 1 + 2 + 3 + 4 = 10$ mushrooms, contradicting the fact that there were only nine mushrooms. Thus at least two boys must have collected the same number of mushrooms.

Example 3. *Prove that there does not exist a tetrahedron (triangular pyramid) in which each edge is adjacent to an obtuse angle of one of its faces.*

Solution. Suppose such a tetrahedron exists. In any triangle the side opposite an obtuse angle is the largest side. Therefore each edge of the tetrahedron must be strictly shorter than some other edge that is adjacent to the obtuse angle. Since

the number of edges in a tetrahedron is finite, this strict inequality cannot cycle indefinitely; the assumed configuration leads to an infinite descending chain of lengths, which is impossible. Hence no such tetrahedron exists.

Example 4. *Prove that* $\log_2 3$ *is an irrational number.*

Solution. Assume otherwise and write $\log_2 3 = \frac{p}{q}$ with p and q positive integers. Then $2^{p/q} = 3$, i.e. $2^p = 3^q$. The left side is even while the right side is odd. This contradiction shows that $\log_2 3$ is irrational.

1.2.2 :: :: pigeonhole principle

In its simplest form the pigeonhole principle says that if ten rabbits sit in nine boxes, then some box must contain at least two rabbits. A more general formulation is: "If n rabbits sit in k boxes, then there exists a box containing at least $\lceil n/k \rceil$ rabbits and a box containing at most $\lfloor n/k \rfloor$ rabbits." Do not be alert by fractional rabbits—if $10/9$ rabbits must sit in a box, then in fact at least two do.

Proof of the principle. Assume that each of the k boxes contains strictly fewer than n/k rabbits. Then altogether there are fewer than $(n/k)\,k = n$ rabbits, which contradicts the assumption that there are n rabbits. This simple argument illustrates why similar reasoning occurs throughout combinatorics.

The pigeonhole principle may seem obvious, but in order to apply it one must sometimes think carefully about what plays the role of "rabbits" and what plays the role of "boxes". For example, if each element of a set A corresponds to exactly one element of a set B, then one may call the elements of A rabbits and those of B boxes.

The principle also has continuous versions. For instance: "If n rabbits eat m kg of grass, then some rabbit ate at least m/n kg and some rabbit ate at most m/n kg." In this formulation the rabbits play the role of boxes for the grass, while the grass plays the role of rabbits sitting in boxes.

Example 1. *There are 400 students in a school. Prove that at least two of them were born on the same day of the year.*

Solution. There are 366 days in a year. Think of the students as rabbits and the days of the year as boxes. Then some box must contain at least $\lceil 400/366 \rceil = 2$ students, i.e. two students share a birthday.

Example 2. *The ocean covers more than half of the Earth's surface. Prove that somewhere in the ocean there are two antipodal points (diametrically opposite points on the globe).*

Solution. Reflect the ocean through the centre of the Earth. The union of the ocean and its reflection covers more than the entire surface of the Earth, so there is a point that lies in both. Such a point and its antipode are both in the ocean.

Example 3. *Sixty five schoolchildren came to an exam. They were given three tests. On each test the score was one of* 2, 3, 4 *or* 5. *Must there be two pupils who got the same grades on all three tests?*

Solution. There are $4^3 = 64$ possible triples of grades. Since 65 pupils take part, by the pigeonhole principle at least two of them must have identical triples of grades.

Example 4. *Prove that among any five people there are two who have the same number of acquaintances among these five people (a person may be unacquainted with everyone).*[10]

1.2.3 :: :: invariants

Invariant — a quantity which does not change as a result of certain operations (for example, cutting and rearranging parts of a figure does not change the total area). If an invariant distinguishes two configurations, then it is impossible to pass from one to the other. As an invariant one can use *parity* or a *coloring*. In problems about the sum of digits, the remainders upon division by 3 or 9 are often used.

Semi-invariant — a quantity that changes only in one direction (that is, it can only increase or only decrease). The concept of a semi-invariant is often used when proving that a process terminates.

Example 1. A wonder-apple tree grows both bananas and pineapples. In one move one is allowed to pick two fruits from it. If two bananas or two pineapples are picked, then one more pineapple grows; if one banana and one pineapple are picked, then one banana grows. In the end there remains one fruit. Which fruit is it, if it is known how many bananas and pineapples were there initially?

[10] Comment: The possible numbers of acquaintances are 0,1,2,3,4. If 0 is among them, then 4 is not possible, so we have only 4 possibilities for 5 people. The same is true when there is no person with 0 acquaintances.

Solution. The parity of the number of bananas does not change, therefore, if the number of bananas was even, the remaining fruit is a pineapple, and if it was odd, then it is a banana.[11]

Example 2. In one cell of a 4×4 square table there is a minus sign, and in all the other cells there are pluses. It is allowed to change at once the signs in all cells of any one row or any one column. Prove that, no matter how many such changes of signs we perform, it is impossible to obtain a table consisting entirely of pluses.

Solution. Let us replace the sign "$+$" by the number 1 and the sign "$-$" by -1. Note that the *product of all numbers in the table* does not change when the signs in all numbers of any one row or column are flipped. In the initial position this product is -1, and in the table consisting entirely of pluses it is $+1$, which proves the impossibility of transition.[12]

Example 3. On a straight line there stand two chips: on the left a red one, on the right a blue one. It is allowed to perform either of two operations: insert two chips of the same color next to each other (between any two chips or at the edge), or remove a pair of neighboring chips of the same color (between which there are no other chips). Is it possible, by using such operations, to leave exactly two chips on the line, a blue one on the left and a red one on the right?

Solution. Consider the number of pairs of chips of different colors (not necessarily neighboring), where the left chip is red. Note that the parity of this number does not change. In the initial configuration this number is odd (equal to 1), but in the desired configuration it is even (0). Therefore it is impossible to reach the desired configuration.[13]

Example 4. On the island of Grey-Brown-Raspberry live chameleons: 13 grey, 15 brown, and 17 raspberry-colored ones. If two chameleons of different colors meet, then both change their color to the third one. Can it happen that at some moment all the chameleons on the island become of the same color?

Hint. Let us denote by B, G, and M the numbers of brown, grey, and raspberry chameleons, respectively. Prove that the remainders upon division by 3 of the

[11] Comment: The invariant is the parity of the number of bananas. The text implicitly assumes that the process continues until one fruit remains.

[12] Comment: The invariant here is the product of all entries in the table, equal to -1 at the start.

[13] Comment: The invariant is the parity of the number of red–blue pairs in that order.

differences $B-G$, $G-M$, and $M-B$ do not change.[14]

Example 6. Is it possible to cut a round disc into several parts and assemble from them a square? (The cuts are pieces of straight lines and arcs of the circle.)

Solution. Consider the invariant: the difference of the sums of the lengths of concave and convex boundary arcs of all the pieces. This quantity does not change when a piece is cut into two, nor when two pieces are joined together. For a unit round disc this invariant equals 2π, and for a square it equals 0. Therefore "squaring the circle" is impossible.[15]

1.2.4 :: :: problems for tutorial

1. Is it possible to connect five cities by roads so that each city is connected with exactly three others? [16]

2. Prove that there does not exist a polyhedron whose number of faces is odd and such that each face has an odd number of vertices. [17]

3. In each cell of an $m \times k$ rectangular array there is a number. The sum of the numbers in each row and in each column is 1. Prove that $m = k$. [18]

4. A class contains 25 students. It is known that among any three students there are two who are friends. Prove that there is a student who has at least 12 friends. [19]

[14] Comment: The invariant consists of the three residues modulo 3 of the color differences; since they cannot all become zero simultaneously, a single color for all chameleons is impossible.

[15] Comment: The invariant compares total curvature (arc excess vs. deficit) of the boundary. Since it is preserved under cutting and joining, the transition from circle to square is impossible.

[16] Comment: In graph–theoretic terms this asks for a five vertex 3–regular graph. The sum of degrees would be 15, which contradicts the handshaking lemma stating that the sum of degrees must be even.

[17] Comment: If F is the number of faces and each face has an odd number of edges, then the sum of the number of all edges in of faces is odd; however this sum also equals $2E$ (since each edge belongs to two faces), which is even. Therefore F must be even.

[18] Comment: Summing by rows gives a total of m, while summing by columns gives a total of k. Therefore $m = k$.

[19] Comment: In a graph on 25 vertices without an independent set of size 3 the average degree is more than $\frac{24}{2}$; hence some vertex has degree at least 12.

5. A committee of 60 people held 40 meetings. Exactly 10 committee members attended each meeting. Prove that some two members met at committee meetings at least twice. [20]

1.2.5 :: :: problems for workshop

1. Is there a convex polygon with more than three acute angles? [21]
2. Prove that there are infinitely many prime numbers of the forms
   (a) $4k+3$, [22]
   (b) $3k+2$, [23]
   (c) $6k+5$. [24]
3. Prove that if $(m-1)!+1$ is divisible by m, then m is a prime number. [25]
4. In a class of 30 pupils a test was written. Nikita made 13 mistakes and every other pupil made strictly fewer. Prove that there are three pupils who made the same number of mistakes. [26]
5. The Earth has more than six billion inhabitants and no person older than 150 years exists. Prove that there are two people on Earth who were born at exactly the same second. [27]

---

[20] Comment: Double count the pairs (meeting, {two participants}). There are $40 \times \binom{10}{2}$ such pairs, but there are only $\binom{60}{2}$ pairs of committee members. By the pigeonhole principle some pair must occur at least twice.

[21] Comment: The answer is no. In a convex n–gon the sum of the interior angles is $180(n-2)$ degrees. If all k angles are acute then their sum is less than $90k$, forcing $180(n-2) < 90k + 180(n-k)$; from this one sees that $k \leq 3$.

[22] Comment: Consider the number $4p_1p_2\cdots p_n + 3$ where the p_i run over all primes of the form $4k+3$.

[23] Comment: The same idea works by considering $3p_1p_2\cdots p_n + 2$.

[24] Comment: The argument is analogous; take $6p_1p_2\cdots p_n + 5$.

[25] Comment: This is a one direction form of Wilson's theorem. The converse is well known: if m is prime then $(m-1)! \equiv -1 \pmod{m}$.

[26] Comment: Excluding Nikita leaves 29 pupils making between 0 and 12 mistakes. There are 13 possible values and 29 pupils, so by the pigeonhole principle some value is taken by at least three pupils.

[27] Comment: The number of seconds in 150 years is approximately $150 \times 365 \times 24 \times 60 \times 60$, which is less than six billion. Therefore two of the more than six billion birth instants must coincide.

6. Twelve lines are drawn in the plane. Prove that some two of them form an angle of at most 15°. [28]

7. A drawer contains socks: 10 black, 10 blue and 10 white. What is the smallest number of socks one must draw without looking in order to guarantee that among the drawn socks there are

   (a) two of the same colour;[29]

   (b) two of different colours;[30]

   (c) two black socks?[31]

8. Thirty six stones were mined in a quarry. Their masses form an arithmetic progression $490, 495, 500, \ldots, 665$ kg. Is it possible to transport these stones using seven trucks, each of capacity 3 tonnes (3000 kg)?[32]

[28] Comment: Partition the 180° around a point into 12 intervals of length 15°. By the pigeonhole principle two of the directions of lines must lie in the same interval.

[29] Comment: Taking 4 socks guarantees at least two of the same colour, since 3 colours and 4 socks force a repetition.

[30] Comment: One could draw all 10 socks of one colour without yet having two colours. The eleventh sock guarantees at least one sock of a different colour.

[31] Comment: In the worst case one draws all 20 non black socks before drawing a black one. The next sock (the 22nd) must then be a second black.

[32] Comment: The total mass of the stones is $36 \times 577.5 = 20790$ kg. Seven trucks can carry 21000 kg, so sufficient capacity exists. But....

1.2.6 :: :: 2nd homework

Read:

Kenneth H. Rosen, Discrete Mathematics and Its Applications, p.313, 320-321. If you don't understand certain notation, just skip it for now (or find the explanation in the first chapter of this book), we will cover it later.

PRINCIPLE OF MATHEMATICAL INDUCTION To prove that $P(n)$ is true for all positive integers n, where $P(n)$ is a propositional function, we complete two steps:

BASIS STEP: We verify that $P(1)$ is true.

INDUCTIVE STEP: We show that the conditional statement $P(k) \rightarrow P(k+1)$ is true for all positive integers k.

To complete the inductive step of a proof using the principle of mathematical induction, we assume that $P(k)$ is true for an arbitrary positive integer k and show that under this assumption, $P(k+1)$ must also be true. The assumption that $P(k)$ is true is called the **inductive hypothesis**. Once we complete both steps in a proof by mathematical induction, we have shown that $P(n)$ is true for all positive integers, that is, we have shown that $\forall n\, P(n)$ is true where the quantification is over the set of positive integers. In the inductive step, we show that $\forall k(P(k) \rightarrow P(k+1))$ is true, where again, the domain is the set of positive integers.

Expressed as a rule of inference, this proof technique can be stated as

$$(P(1) \wedge \forall k(P(k) \rightarrow P(k+1))) \rightarrow \forall n P(n),$$

when the domain is the set of positive integers. Because mathematical induction is such an important technique, it is worthwhile to explain in detail the steps of a proof using this technique. The first thing we do to prove that $P(n)$ is true for all positive integers n is to show that $P(1)$ is true. This amounts to showing that the particular statement obtained when n is replaced by 1 in $P(n)$ is true. Then we must show that $P(k) \rightarrow P(k+1)$ is true for every positive integer k. To prove that this conditional statement is true for every positive integer k, we need to show that $P(k+1)$ cannot be false when $P(k)$ is true. This can be accomplished by assuming that $P(k)$ is true and showing that *under this hypothesis* $P(k+1)$ must also be true.

Remark: In a proof by mathematical induction it is *not* assumed that $P(k)$ is true for all positive integers! It is only shown that *if it is assumed* that $P(k)$ is true, then $P(k+1)$ is also true. Thus, a proof by mathematical induction is not a case of begging the question, or circular reasoning.

When we use mathematical induction to prove a theorem, we first show that $P(1)$ is true. Then we know that $P(2)$ is true, because $P(1)$ implies $P(2)$. Further, we know that $P(3)$ is true, because $P(2)$ implies $P(3)$. Continuing along these lines, we see that $P(n)$ is true for every positive integer n.

EXAMPLE 7 **An Inequality for Harmonic Numbers** The **harmonic numbers** H_j, $j = 1, 2, 3, \ldots$, are defined by

$$H_j = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{j}.$$

For instance,

$$H_4 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \frac{25}{12}.$$

Use mathematical induction to show that

$$H_{2^n} \geq 1 + \frac{n}{2},$$

whenever n is a nonnegative integer.

Solution: To carry out the proof, let $P(n)$ be the proposition that $H_{2^n} \geq 1 + \frac{n}{2}$.

BASIS STEP: $P(0)$ is true, because $H_{2^0} = H_1 = 1 \geq 1 + \frac{0}{2}$.

INDUCTIVE STEP: The inductive hypothesis is the statement that $P(k)$ is true, that is, $H_{2^k} \geq 1 + \frac{k}{2}$, where k is an arbitrary nonnegative integer. We must show that if $P(k)$ is true, then $P(k+1)$, which states that $H_{2^{k+1}} \geq 1 + \frac{k+1}{2}$, is also true. So, assuming the inductive hypothesis, it follows that

$$\begin{aligned}
H_{2^{k+1}} &= 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{2^k} + \frac{1}{2^k+1} + \cdots + \frac{1}{2^{k+1}} && \text{by the definition of harmonic number} \\
&= H_{2^k} + \frac{1}{2^k+1} + \cdots + \frac{1}{2^{k+1}} && \text{by the definition of } 2^k\text{th harmonic number} \\
&\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2^k+1} + \cdots + \frac{1}{2^{k+1}} && \text{by the inductive hypothesis} \\
&\geq \left(1 + \frac{k}{2}\right) + 2^k \cdot \frac{1}{2^{k+1}} && \text{because there are } 2^k \text{ terms each} \geq 1/2^{k+1} \\
&\geq \left(1 + \frac{k}{2}\right) + \frac{1}{2} && \text{canceling a common factor of } 2^k \text{ in second term} \\
&= 1 + \frac{k+1}{2}.
\end{aligned}$$

This establishes the inductive step of the proof.

We have completed the basis step and the inductive step. Thus, by mathematical induction $P(n)$ is true for all nonnegative integers n. That is, the inequality $H_{2^n} \geq 1 + \frac{n}{2}$ for the harmonic numbers holds for all nonnegative integers n. ◀

Remark: The inequality established here shows that the **harmonic series**

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \cdots$$

is a divergent infinite series. This is an important example in the study of infinite series.

Write:

1. A snail crawls in the plane at a constant speed and every 15 minutes turns 90° (sometimes left, sometimes right). Prove that it can return to its starting point only after an integer number of hours.

2. In the language of a certain tribe there are only two sounds (written here as **w** and **y**). Two words are considered the same if one can be obtained from the other by a sequence of operations of two types: deleting a consecutive occurrence of **wy** or **yyww** and inserting **yw** at any position. Do the words **ywy** and **wyw** represent the same word?

3. Three grasshoppers sit at three vertices of a square in the plane. They play a game of leapfrog: one grasshopper jumps to the point symmetric to another grasshopper across the third (a point A is symmetric to a point B with respect

to a point C if C is the middle of the interval AB, here A, B, C are points on the plane.) Can any grasshopper ever land on the fourth vertex of the square?

4. There is an island populated by knights and liars. Knights always tell truth, liars always lie. A stranger meets three local persons and asks everybody: "how many knights are among you three?". The first answered: no one. The second answered: one. What is the answer of the third person?

5. Automate can shred a piece of paper on 4 or 6 pieces. What number of pieces can be reached from one sheet?

6. Prove that among any 52 integers there exist two whose sum or difference is divisible by 100.

Just for fun, not a part of the homework: use AI, ask them to solve the following problem, then try to understand their solution, then check, if it is at all correct:

Four identical jars are filled to three quarters with paint, each containing a different colour. It is possible to pour any portion of the contents of one jar into another. Is it possible to perform a finite sequence of pourings so that each jar contains an identical mixture of the four colours?

Try to solve this problem by yourself.

Last, but not least. Read the next page for a short advice on how to write solutions with a good and bad example.

Example of bad and good writing

Five boys found nine mushrooms. Prove that at least two of them must have found the same number of mushrooms.

Bad solution	**Good solution**
It is not possible that they found different numbers of mushroom because in this case they will find at least 10 mushrooms[33], because in the worst[34] case the first[35] found 0, the second found 1 mushroom, etc, $0+1+2+3+4=10$.	Assume that the boys all found different numbers of mushrooms. Order them by increasing number of mushrooms. Then, the first boy picked at least 0 mushrooms, the second at least 1, the third at least 2, the fourth at least 3 and the fifth at least 4. Altogether they would have picked at least $0+1+2+3+4=10$ mushrooms, contradicting the fact that there were only nine mushrooms. Thus at least two boys must have collected the same number of mushrooms.

In a good solution each step is small and incremental, it might be

- an assumption (the first phrase states the proof strategy 'by contradiction'),
- an action ('Order them...'),
- introducing a notation ('Denote ... by ... '),
- a computation,
- or a conclusion derived from the preceeding steps.

Use single-action sentences: 'Assume this. Count that. Then A. Then B.' A solution is good (or formal) if it is easy to follow its logical structure and easy to check each step separately (assume that a reader has a limited amount of memory).

Instead of *'A, because of B'*, write *'B, therefore A'*.

Exercise: look at solutions of the problems across these notes and evaluate their quality, try to cut them into such elementary steps.

[33] Here the reader asks 'why'? It is better if, whenever it is possible, each next step immediately follows from the previous one, and explanations are given BEFORE a statement.

[34] Where is the definition of the worst case? And even if you give such a definition, then you need to show that the case 0,1,2,3,4 is indeed the worst case.

[35] What if the first found 3 and the second 0? Then you need to consider all these cases or convince the reader that these cases are all the same, i.e. as 'ordering' step in the good solution.

1.3 :: method of the extreme, counting in two ways, combinatorics

1.3.1 Method of the Extreme

Special or extreme objects often serve as a cornerstone of a solution. For example, one might look for the largest number, the nearest point, a corner point, a degenerate circle or a limiting case. It is therefore useful to consider such special objects.

In problems solvable by the method of the extreme one often uses the method of the minimal counterexample: assume that the statement is false. Then there exists a counterexample minimal in some sense. If one can show that this counterexample can be made smaller, one obtains the desired contradiction.

Example 1. *The plane is cut by $N \geq 3$ lines in general position. Prove that to each line there is a triangle adjacent to that line.*

Solution. Choose a line and consider all intersection points of the other lines. Among these points pick the one that is closest to the chosen line. The two lines passing through this closest point intersect the chosen line and form with it a triangle. No other lines can intersect the interior of this triangle (otherwise one would find a closer intersection point), so the triangle is indeed adjacent to the chosen line.

Example 2. *Prove that in any convex polyhedron there are two faces with the same number of edges.*

Solution. Consider the face G with the largest number n of edges. Each edge of G is adjacent to another face; there are n faces adjacent to G. The number of edges of each adjacent face lies between 3 and $n-1$, giving only $n-2$ possible values. Since there are more adjacent faces than possible values, by the pigeonhole principle two of them must have the same number of edges.

Example 3. *In each cell of a chessboard a number is written. It turns out that every number equals the arithmetic mean of the numbers in the neighbouring cells (by side). Prove that all the numbers are equal.*

Solution. Let M be the maximum of all the numbers. Since M equals the average of its neighbours, all neighbouring numbers must also equal M. Proceeding by connectivity of the board shows that all numbers are equal to M.

Example 4. *From a point inside a convex polygon perpendiculars are dropped to its sides or to their extensions. Prove that at least one of the perpendiculars falls on a*

side of the polygon.

Solution. Consider the perpendicular whose foot on the boundary of the polygon is closest to the original point. If that foot lay on the extension of a side, one could shift slightly in the direction of the polygon and produce a shorter perpendicular, a contradiction. Hence at least one perpendicular must land on an actual side.

Example 5. *Prove that the number*

$$1 + \tfrac{1}{2} + \tfrac{1}{3} + \cdots + \tfrac{1}{n}$$

is never an integer. (Here $n \geq 2$.)

Solution. Look at the denominators of the summands and identify the largest power of 2 appearing there. When the terms are written with a common denominator, the numerator will be odd, while the denominator is a multiple of that power of 2; hence the result cannot be an integer.

1.3.2 Counting in Two Ways

When setting up equations one often expresses some quantity—such as an area, a distance or a time—in two different ways. Sometimes one estimates a quantity in two different ways and obtains either an inequality or values with different parity. This idea is closely related to the notion of an invariant and is often a source of contradictions (see also the section on proof by contradiction).

Example 1. *Can one arrange numbers in a* 5×5 *square table so that the sum of the numbers in each row is positive and in each column is negative?*

Solution. Suppose such an arrangement were possible. If one sums all the numbers by rows, the total sum is positive. If one sums all the numbers by columns, the total sum is negative. This contradiction shows that no such arrangement exists.

Example 2. *In a class there are 27 pupils. Each boy is friends with four girls and each girl is friends with five boys. How many boys and how many girls are there?*

Solution. Let B be the number of boys and G the number of girls. Count the total number of friendships in two ways. On the one hand, each boy is friends with four girls, giving $4B$ friendships. On the other hand, each girl is friends with five boys, giving $5G$. Thus $4B = 5G$. Since $B + G = 27$, simple algebra yields $B = 15$ and $G = 12$.

Example 3. *Find the sum of the geometric progression*

$$S_n = 1 + 3 + 9 + \cdots + 3^n.$$

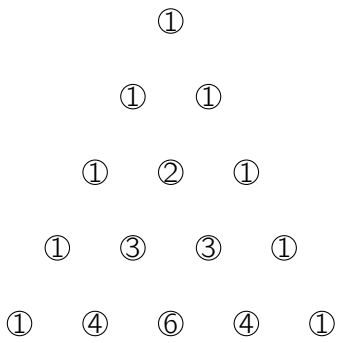
Solution. Observe that, given S_n, the next sum S_{n+1} can be obtained in two ways: either add 3^{n+1} to S_n or multiply all terms of S_n by 3 and then add 1. Hence $S_n + 3^{n+1} = 3S_n + 1$, which simplifies to $S_n = \frac{3^{n+1}-1}{2}$.

Example 4. *Can all faces of a convex polyhedron have six or more sides?*

Solution. No. Estimate in two ways the average of all the angles of all the faces. On the one hand, the average interior angle of an n–gon with $n \geq 6$ is at least $120°$. On the other hand, at each vertex of the polyhedron at least three faces meet and the sum of the angles meeting at a vertex is strictly less than $360°$. Therefore the average angle at each vertex is strictly less than $120°$. The contradiction shows that such a polyhedron cannot exist.

Example 5. A *binomial coefficient* $\binom{n}{k}$ (pronounced '*n choose k*') is the number of ways to choose k different numbers from the set $1, 2, \ldots, n$ of n numbers. Using the above definition of the binomial coefficients, prove (without any formulas) that

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



The picture on the left is called the Pascal triangle. Left and right sides are filled with ones. Then we fill rows one by one. Each interior entry equals the sum of the two entries above it: specifically, the entry in row n, position k is $\binom{n}{k}$.

Problem 1. Prove the **Newton binomial formula:** $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$, for example $(1+x)^4 = 1 + 4x + 6x^2 + 4x^3 + x^4$.

1.3.3 :: :: problems for tutorial

Before this tutorial read Section 5.1.

1. A football fan drew the positions of the players on a football field at the beginning of the first and the second halves. It turned out that some players had exchanged places, while the others remained in their positions. At the same time, the distance between any two players did not increase. Prove that all these distances in fact remained the same.[36]

2. A traveller leaves his home city A and goes to the city B in his country that is farthest from A. From that city he goes to the city C farthest from his current city B, and so on. Prove that if the city C does not coincide with A, then the traveller will never return home. (Distances between cities are assumed to be distinct.)[37]

3. One of the heads of a hundred headed dragon wants to arrange his heads so that each head lies strictly between two others. Can he do it? (You may regard the heads as points in space.)[38]

4. Show (hint: by induction) that a connected graph with n vertices and without cycles has exactly $n-1$ edge.

[36] Comment: An invariant argument: since no pairwise distance increases, the total sum of distances acts as a semi-invariant.

[37] Comment: Each step strictly increases the distance to the farthest city left behind. If one could return home, one would form a cycle of increasing distances, which is impossible.

[38] Comment: It is impossible for every point in a finite set to lie between two others on a straight line, because the extreme points on the convex hull of the configuration cannot be between two other points. Start solution by: consider the head with biggest z-coordinate. Among them consider the head with the biggest y-coordinate, among them...

1.3.4 :: :: problems for workshop

Exercise 1. In cafe, you can order green, red, or black soup and green, red, or black tea. How many different orders you can make if it is prohibited to order soup and tea of the same color?

Exercise 2. Five persons A, B, C, D, E visit a cafe every day and always seat on the same table with five chairs (chairs are numbered: $1, 2, 3, 4, 5.$). In how many different ways they can seat on these five chairs?[39]

Exercise 3. In cafe, the cook has a) 4, b) 8 ingredients. A dish is made of three different ingredients (their order is not important). How many different dishes the cook can cook? [40]

Exercise 4. How many four-digit numbers contain 7?

Exercise 5. In cafe, the cook has 9 ingredients. A dish is made of three different ingredients (their order is important). How many different dishes the cook can cook if the 3rd and 4th ingredients are not allowed to use together?

Problem 1. Find the coefficient behind x^3 in $(1+x)^{10}(1+2x)^7$.

Solution: we can choose x from three parenthesis of the first type $(1+x)$ and 1 from all parenthesis of the second type $(1+2x)$. We can do this in $10 \times 9 \times 8$ cases, but since it is not important in which order we choose the first type parenthesis, we divide by 6. So, this gives $\binom{10}{3}$. We also can choose x from two parenthesis of the first type and from one of the second type, this gives $2 \times \binom{10}{2}\binom{7}{1}$, etc. The answer[41]:

$$\binom{10}{3} + 2 \cdot \binom{10}{2}\binom{7}{1} + 4 \cdot \binom{10}{1}\binom{7}{2} + 8 \cdot \binom{10}{1}\binom{7}{3}.$$

Exercise 6. Find the coefficient behind x^4 in $(1+x)^{10}(1+2x)^7$.

[39] Recall the notation $n!$

[40] For the case a) one can list all dishes, then explain that it is $\frac{4 \cdot 3 \cdot 2}{3 \cdot 2 \cdot 1}$. Introduce the notation $\binom{n}{k}$, provide the formula for it, tell that the proof is exactly the same as in b).

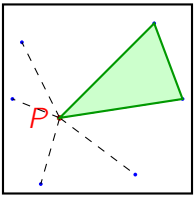
[41] You do not need to compute it numerically, the below answer is fine.

1.3.5 :: :: 3rd homework

Read:

Problem: In a unit square, 101 points are thrown in such a way that no three of them lie on one straight line. Prove that there exists a triangle with vertices at these points whose area does not exceed $\frac{1}{100}$.

Solution: Select a point P among 101 points and connect it with all the others — we obtain 100 segments. Choose a direction (say, clockwise) and successively connect the ends of these segments — we obtain 100 non-overlapping triangles whose total area does not exceed 1 (the total area of the square). By the pigeonhole principle, there exists at least one triangle among them whose area does not exceed $\frac{1}{100}$.



Write:

1. Find the mistake in the above solution, explain it in your homework.
2. One hundred numbers are arranged on a circle. Each number is equal to the arithmetic mean of its two neighbours. Prove that all the numbers are equal.
3. Prove that if a graph with n vertices has only $n-2$ edges, then it is disconnected.
4. Using the principle of mathematical induction, prove that

$$1\cdot 3+3\cdot 5+5\cdot 7+\cdots+(2n-1)\cdot(2n+1)=\frac{n(4n^2+6n-1)}{3}.$$

5. Each student in the class took part in at least one of two hikes. In each hike, the proportion of boys did not exceed 2/5. Prove that in the whole class, the proportion of boys does not exceed 4/7.
6. On a plane, N points are given. Some pairs of points are connected by segments. If two segments with different endpoints intersect, they may be replaced by two other non-intersecting segments with the same endpoints. Can this process continue indefinitely?

1.4 :: feedback

During the lectures we skipped some of the problems listed above and occasionally postponed others to the next class. For the easier problems we paused and gave students time to work on them.

After the first three weeks we ran a survey. Most of the respondents said that the material is interesting—difficult, but manageable. A few students (mainly those with a background in school math competitions) said the material was easy.

Several students said they especially liked the domino-and-chessboard problem. Many of them use AI tools to understand the wording of the problems and homework, and to clarify the lecture content (also, English is an issue). At the same time, many students struggle with what a *formal solution* is and how to write it properly. They do, however, enjoy the story-style settings of the problems (frogs, Martians, etc.).

Some students complained that we do not provide a template or model for writing up solutions.

2 Naive set theory

2.1 :: notation, union, intersection, Venn diagrams

Definition of a set, Euler-Venn diagrams, symbols $\cap, \cup, \forall, \exists, \wedge, \vee, \subset, \in, \notin, \Rightarrow, \Leftrightarrow, \varnothing, A \setminus B$, $\neg$ (negation), XOR, characteristic function (addition on the image is xor multiplications is AND, the same as multipication and addition for even and odd numbers) constructions such as

$$\mathbb{Q}_+ = \{q \in \mathbb{Q} | q > 0\}, \sum_{i=1..n} f(i), \sum_{a \in A} f(a).$$

When does $A \setminus B = B \setminus A$?

Problem 1. Translate into the plain English the following.

Def. $f : \mathbb{R} \to \mathbb{R}$ is continuous $\Leftrightarrow$

$\Leftrightarrow \forall x \in \mathbb{R}, \forall \varepsilon > 0, \exists \delta > 0,$ such that $\forall x' \in [x-\delta, x+\delta]$ we have $|f(x') - f(x)| < \varepsilon$.

Write a definition of a prime number without using words and using only mathematical notation.

Prove that for any three sets the inclusion (and give an example of three sets for which this inclusion is strict.)

$$(A \setminus B) \setminus C \subseteq A \setminus (B \setminus C)$$

Solution. The left-hand side of (i) consists of those $x \in A$ that do not belong to B and do not belong to C, is contained in $A \setminus B$. The right-hand side consists of those $x \in A$ that do not belong to $B \setminus C$ and, consequently, contains $A \setminus B$.

We can also express this in another way: the left-hand side consists of those x for which

$$x \in A \ \wedge \ x \notin B \ \wedge \ x \notin C,$$

while the right-hand side consists of those x for which

$$(x \in A \ \wedge \ x \notin B) \ \vee \ (x \in A \ \wedge \ x \in C).$$

Thus, to give an example of three sets for which a strict inclusion occurs here, it suffices to take any three sets for which $A \cap C$ is not contained in B, i.e. $A = C = A \cap C = \{x\}, B = \varnothing$.

The meaning of introducing operations $1 + 1 = 0 + 0 = 0, 0 + 1 = 1 + 0 = 1, 0 \cdot 0 = 0 \cdot 1 = 1 \cdot 0 = 0, 1 \cdot 1 = 1$ on the set $\{0, 1\}$ consists in the fact that now we can express Boolean operations on subsets of a set X in terms of operations on their characteristic functions.

Problem. Prove that for any two subsets $A, B \subseteq X$ the following equalities hold:

1. $\chi_{A \cap B} = \chi_A \chi_B$,
2. $\chi_{A \triangle B} = \chi_A + \chi_B$,
3. $\chi_{A \cup B} = \chi_A + \chi_B + \chi_A \chi_B$,
4. $\chi_{A \setminus B} = \chi_A + \chi_A \chi_B$.

The results of this problem serve as yet another argument in favor of considering $\cap$ as the *product* of sets, and $\triangle$ — rather than $\cup$ — as the *sum* of sets.

Problems on Intervals of the Real Line. *What is the intersection of two intervals on the real line?*

Answer. Let (a, b) with $a < b$ and (c, d) with $c < d$ be two intervals. If $b \leq c$ or $d \leq a$, their intersection is empty. If $b > c$ and $d > a$, then the intersection of these intervals is the interval

$$(\max(a, c), \min(b, d)).$$

Consider two intervals of the real line (a, b), $a < b$, and (c, d), $c < d$. When is their union again an interval? What is it equal to in this case?

Answer. The union is an interval if and only if (a, b) and (c, d) intersect, that is, when $c < b$ and $a < d$. In this case their union equals

$$(\min(a, c), \max(b, d)).$$

If three intervals of the real line have a common point, then at least one of them is contained in the union of the other two.

Solution. Let $I_i = (a_i, b_i)$, $a_i < b_i$, where $i = 1, 2, 3$, be the three intervals. By the condition, there exists a point $x \in \mathbb{R}$ such that $a_i < x < b_i$ for all $i = 1, 2, 3$. Applying twice the result of the previous problem, we obtain

$$I_1 \cup I_2 \cup I_3 = (\min(a_1, a_2, a_3), \max(b_1, b_2, b_3)).$$

Take an index i such that $\min(a_1, a_2, a_3) = a_i$. Next, take some $j \neq i$ such that $\max(b_1, b_2, b_3) = b_j$, or, if no such j exists (that is, if $b_i > b_j$ for all $j \neq i$), take any $j \neq i$. Then

$$I_i \cup I_j = (a_i, b_j) = I_1 \cup I_2 \cup I_3,$$

so if h is an index such that $\{i, j, h\} = \{1, 2, 3\}$, then $I_h \subset I_i \cup I_j$. □

2.1.1 :: :: problems for tutorial

1. Is it true that
$$(A \setminus B) \setminus C = (A \setminus C) \setminus B?$$
2. Is it true that
$$(A \setminus B) \setminus C = (A \setminus C) \setminus (B \setminus C)?$$
3. Prove the so-called **four sets identity:**
$$(A \cap B) \cup (C \cap D) = (A \cup C) \cap (A \cup D) \cap (B \cup C) \cap (B \cup D)$$
4. Express operations $\cup$ and $\setminus$ through the operations $\cap$ and $\triangle$
5. Express the operations $\cap$ and $\setminus$ through the operations $\cup$ and $\triangle$.

In fact, Boolean operations can be expressed through any two of them.

Expression through $\cap$ and $\triangle$. The operations $\cup$ and $\setminus$ are expressed through the operations $\cap$ and $\triangle$ as follows:

$$A \cup B = (A \triangle B) \triangle (A \cap B), \qquad A \setminus B = A \triangle (A \cap B).$$

Expression through $\cup$ and $\triangle$. The operations $\cap$ and $\setminus$ are expressed through the operations $\cup$ and $\triangle$. Since $\setminus$ is already expressed through $\triangle$ and $\cap$, it suffices to express $\cap$ through $\cup$ and $\triangle$. Such an expression is given by the following formula:

$$A \cap B = (A \cup B) \triangle (A \triangle B).$$

see also Section 5

2.1.2 :: :: problems for workshop

Exercise 7. Some of these expressions are grammatically or logically incorrect. Identify them and explain what is the fault. (In what follows, $f : \mathbb{R} \to \mathbb{R}$ is a real function and $A, B, C \subset \mathbb{R}$.)

$\{1+1\}$	$\{3\} \setminus \{\{3\}\}$	$1+1 \Rightarrow 2$
$\{1,2\} \Leftrightarrow \{2,1\}$	$\sqrt{2} \notin \mathbb{Q}$	$\mathbb{Z} \setminus (\mathbb{Z} \setminus \mathbb{N})$
$\mathbb{Z} \Rightarrow \mathbb{Q}$	$(\lvert x\rvert \in \mathbb{Z}) \Rightarrow (\lvert x\rvert \in \mathbb{Q})$	$(x \in A) \cup (x \in B)$
$(3 < 1) \Rightarrow \varnothing$	$A \leq (A \setminus B)$	$f(A) \in \{f(A)\}$
$(A \subset B) \cap C$	$A \subset (B \cap C)$	$A \subset B \subset A$
$(2,4,6,\ldots) \subset (1,2,3,\ldots)$	$\{A, \mathbb{Z}\}$	$\{\varnothing\} \cap \varnothing$
$f(1) \in \{2,3\}$	$f(\{1,2\}) \in \mathbb{N}$	$f(\mathbb{Q}) \subset \mathbb{Q}$
$\{x \in \mathbb{N} : -x\}$	$\{-x : x \in \mathbb{N}\}$	$\{x : x \Leftrightarrow 2\}$
$\{x \in \mathbb{Z} : x \notin \mathbb{Z}\}$	$\{\{x : \lvert x\rvert < 2\}\}$	$\{x \in \mathbb{Q} : 1 = 0\}$
$\{x \in \mathbb{Q} : x^2 \notin \mathbb{Z}\}$	$\{\{f(x)\} : x \in \mathbb{Q}\}$	$\{x : f(x) \in \mathbb{Q}\}$

Exercise 8. The following expressions define sets. Turn words into symbols.

1. The set of negative odd integers:
2. The set of natural numbers with three decimal digits:
3. The set of rational numbers which are the ratio of odd integers:
4. The set of rational numbers between 3 and π:
5. The set of real numbers at distance $\frac{1}{4}$ from an integer:
6. The complement of the unit circle in the Cartesian plane:
7. The set of lines tangent to the unit circle:

Exercise 9. Draw the Euler-Venn diagrams for $(A \cap B) \setminus C$ and $(A \setminus C) \cap (A \setminus B)$.

Exercise 10. Draw the Euler-Venn diagram for $\big((A \cap B) \cap (C \cup D)\big) \cup (A \setminus C)$.

Answers for tutorial:

$$\{\, n \in \mathbb{Z} : n < 0 \text{ and } n \text{ is odd} \,\} = \{\, n \in \mathbb{Z} : n < 0,\ n = 2k+1,\ k \in \mathbb{Z} \,\}.$$

$$\{\, n \in \mathbb{N} : 10^2 \leq n < 10^3 \,\}.$$

$$\left\{ \frac{p}{q} \in \mathbb{Q} : p, q \in \mathbb{Z},\ p, q \text{ odd},\ q \neq 0 \right\}.$$

$$\{\, q \in \mathbb{Q} : 3 < q < \pi \,\}.$$

$$\{\, x \in \mathbb{R} : |x - n| = \tfrac{1}{4} \text{ for some } n \in \mathbb{Z} \,\}.$$

$$\{\, (x, y) \in \mathbb{R}^2 : x^2 + y^2 \neq 1 \,\}.$$

$$\{\, ax + by = 1 : a^2 + b^2 = 1 \,\}.$$

2.1.3 :: :: 4th homework

1. A straight (finite) path in a park is completely illuminated by several lamps, each of which lights up a certain segment. Prove that it is possible to turn off some of the lamps so that the path remains completely illuminated, but no part of it is illuminated by three lamps at once.

2. Is it possible to cover an equilateral triangle with two smaller equilateral triangles?

3. Prove that the sum of the valencies (aka (also known as) the degrees) of the vertices of a graph is twice the number of the edges. (This is called **the handshaking lemma**)

4. Prove that every positive integer can be represented as a sum of different powers of two.

5. Draw the Euler-Wenn diagramm for $((A \setminus B) \cap (C \cup (D \setminus A))) \cup (D \cap B \cap A)$.

6. Let I be an index set, and $\{A_i\}_{i \in I}$ be a family of sets. Prove de Morgan laws without words, i.e. show that every element from the left set belongs to the right set and vice versa. It is prohibited to write words:

$$\left(\bigcup_{i \in I} A_i \right)^c = \bigcap_{i \in I} A_i^c$$

$$\left(\bigcap_{i \in I} A_i \right)^c = \bigcup_{i \in I} A_i^c$$

   where A^c is the complement to A in the "universal set".

7. **The Meticulous Job Applicant**

   A company requires that ideal candidates must satisfy **all** of the following conditions: speak English, have programming experience, possess a university degree, have at least 2 years of work experience. Describe in words the set of candidates who are **NOT** ideal for the position.

Solution

Let E: candidates who speak English, P: candidates with programming experience, D: candidates with a university degree, W: candidates with $\geq$ 2 years of work experience

The set of ideal candidates is:

$$I = E \cap P \cap D \cap W$$

Candidates who are **NOT** ideal form the complement:

$$I^c = (E \cap P \cap D \cap W)^c$$

Applying De Morgan's Law:

$$I^c = E^c \cup P^c \cup D^c \cup W^c$$

Verbal Interpretation: A candidate is **not ideal** if they **lack at least one** of the required qualifications.

2.2 :: functions, permutations, S_n

A function $f : A \to B$ (pronounced: "a function f from A to B", "a map f from A to B", "a mapping from A to B") is a rule that assigns to each element $a \in A$ an element $f(a) \in B$.

A function f is called an *injection* (we also say: f is *injective*, or f is *one-to-one*) if it sends different elements to different elements, i.e.

$$f(a_1) = f(a_2) \implies a_1 = a_2.$$

A function f is called a *surjection* (we also say: f is *surjective*, or f is *onto*) if for each $b \in B$ there exists an element $a \in A$ (not necessarily unique) such that

$$f(a) = b.$$

A function f is called a *bijection* (we also say: f is *bijective*, or f is a *one-to-one correspondence*) if f is both injective and surjective.

Examples.

- (*Inclusion map.*) If $A \subset B$, then there exists a map $\iota : A \to B$, called the *inclusion*, defined by
$$\iota(a) = a \quad \text{for all } a \in A.$$
- (*Identity map.*) The *identity map* $\mathrm{id}_A : A \to A$ is defined by
$$\mathrm{id}_A(a) = a \quad \text{for all } a \in A.$$
- (*Restriction map.*) Let $f : A \to B$ and let $X \subset A$. Then the *restriction* of f to X is the map
$$f|_X : X \to B, \qquad f|_X(x) = f(x) \quad \text{for all } x \in X.$$
This notation is useful to distinguish f and $f|_X$, because they are defined on different sets: f is defined on A, while $f|_X$ is defined on X.

The *composition* $g \circ f$ of two functions $f : A \to B$ and $g : B \to C$ is the function

$$g \circ f : A \to C, \qquad (g \circ f)(a) = g(f(a)) \quad \text{for all } a \in A.$$

Let $f : A \to B$ and $b \in B$. The *preimage* (or *inverse image*) of b is the set

$$f^{-1}(\{b\}) = \{\, a \in A \mid f(a) = b \,\}.$$

Often we write simply $f^{-1}(b)$ for this set. This set may be empty.

More generally, for $Y \subset B$ we define the preimage of Y as

$$f^{-1}(Y) = \{\, a \in A \mid f(a) \in Y \,\} = \bigcup_{b \in Y} f^{-1}(\{b\}).$$

The set $f(A) = \{f(a) | a \in A\} \subset B$ is called the *image* of A under f.

Problem 1. Let $f : A \to B$ be a function and let $Y \subset B$. Show that

$$f^{-1}(Y) = f^{-1}(Y \cap f(A)).$$

Conclude that the equality

$$Y = f(f^{-1}(Y))$$

holds if and only if $Y \subseteq f(A)$.

Solution. Recall that for $Z \subset B$,

$$f^{-1}(Z) = \{\, a \in A \mid f(a) \in Z \,\}.$$

First we show the equality of sets.

$\subseteq$: Let $a \in f^{-1}(Y)$. Then $f(a) \in Y$. But of course $f(a) \in f(A)$ for every $a \in A$. Hence $f(a) \in Y \cap f(A)$. Thus $a \in f^{-1}(Y \cap f(A))$. This proves

$$f^{-1}(Y) \subseteq f^{-1}(Y \cap f(A)).$$

$\supseteq$: Let $a \in f^{-1}(Y \cap f(A))$. Then $f(a) \in Y \cap f(A)$, so in particular $f(a) \in Y$. Hence $a \in f^{-1}(Y)$. Thus

$$f^{-1}(Y \cap f(A)) \subseteq f^{-1}(Y).$$

Combining the two inclusions we get

$$f^{-1}(Y) = f^{-1}(Y \cap f(A)).$$

For the second statement, recall that for any function f and set $Y \subset A$, we always have

$$f(f^{-1}(Y)) \subseteq Y,$$

because $f^{-1}(Y)$ consists exactly of those elements mapped into Y.

Now suppose $Y \subseteq f(A)$. Then every $y \in Y$ is equal to $f(a)$ for some $a \in A$. Since $y \in Y$, we have $a \in f^{-1}(Y)$, and thus $y = f(a) \in f(f^{-1}(Y))$. Hence

$$Y \subseteq f(f^{-1}(Y)).$$

Together with the always-true inclusion $f(f^{-1}(Y)) \subseteq Y$, this gives

$$Y = f(f^{-1}(Y)).$$

Conversely, if $Y = f(f^{-1}(Y))$, then every $y \in Y$ is of the form $y = f(a)$ for some $a \in f^{-1}(Y) \subseteq A$. Hence $y \in f(A)$, so $Y \subseteq f(A)$.

Thus

$$Y = f(f^{-1}(Y)) \quad \iff \quad Y \subseteq f(A).$$

Problem 2. Prove that if $f^{\circ n} = \mathrm{id}_X$ for some positive integer n, then f is a bijection.

Solution. Assume $f^{\circ n} = \mathrm{id}_X$, i.e.

$$\underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}} = \mathrm{id}_X.$$

Injectivity. Suppose $f(x_1) = f(x_2)$. Apply $f^{\circ(n-1)}$ to both sides:

$$f^{\circ(n-1)}(f(x_1)) = f^{\circ(n-1)}(f(x_2)).$$

The left-hand side is $f^{\circ n}(x_1) = \mathrm{id}_X(x_1) = x_1$, and similarly the right-hand side is x_2. Hence $x_1 = x_2$. So f is injective.

Surjectivity. Let $y \in X$ be arbitrary. We must find $x \in X$ such that $f(x) = y$. Consider

$$x := f^{\circ(n-1)}(y).$$

Then

$$f(x) = f\big(f^{\circ(n-1)}(y)\big) = f^{\circ n}(y) = \mathrm{id}_X(y) = y.$$

Thus every $y \in X$ has a preimage, so f is surjective.

Since f is both injective and surjective, it is bijective.

Permutations

Now let A be a finite set with n elements, i.e. $|A| = n$. (We denote the number of elements in a finite set A by $|A|$.)

All bijections $f : A \to A$ are called *permutations* of A. One may think of such a map as permuting the ordered list $1, 2, 3, \ldots, n$.

Examples of permutations

Let us work with the set

$$A = \{1, 2, 3, 4\}.$$

Some permutations in two-line notation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \qquad \pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

This means, for example, that $\sigma(1) = 2$, $\sigma(2) = 4$, $\sigma(3) = 1$, $\sigma(4) = 3$.

Composition of permutations

Given two permutations $\sigma, \tau : A \to A$, their composition $\tau \circ \sigma$ is the permutation defined by

$$(\tau \circ \sigma)(i) = \tau(\sigma(i)) \quad \text{for all } i \in A.$$

For our examples above, let us compute $\tau \circ \sigma$.

First compute $\sigma(i)$, then apply τ:

$$\begin{aligned} (\tau \circ \sigma)(1) &= \tau(\sigma(1)) = \tau(2) = 2, \\ (\tau \circ \sigma)(2) &= \tau(\sigma(2)) = \tau(4) = 1, \\ (\tau \circ \sigma)(3) &= \tau(\sigma(3)) = \tau(1) = 3, \\ (\tau \circ \sigma)(4) &= \tau(\sigma(4)) = \tau(3) = 4. \end{aligned}$$

So

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}.$$

In cycle notation this is

$$\tau \circ \sigma = (1\ 2),$$

because it swaps 1 and 2 and fixes 3, 4.

Decomposition into cycles: example 1

Take

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}.$$

To write σ in cycle notation, start from 1:

$$1 \mapsto 2, \quad 2 \mapsto 4, \quad 4 \mapsto 3, \quad 3 \mapsto 1.$$

So we return to 1, and we get one 4-cycle:

$$\sigma = (1\ 2\ 4\ 3).$$

A 4-cycle can be written as a product of **transpositions**:

$$(1\ 2\ 4\ 3) = (1\ 3)(1\ 4)(1\ 2).$$

Exercise. Any 4-cycle $(a\ b\ c\ d)$ can be written as $(a\ d)(a\ c)(a\ b)$.

Decomposition into cycles: example 2

Take

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

Start from 1:

$$1 \mapsto 3, \quad 3 \mapsto 4, \quad 4 \mapsto 1,$$

so we get the cycle $(1\ 3\ 4)$. What about 2? We have $\tau(2) = 2$, so 2 is a fixed point. Thus

$$\tau = (1\ 3\ 4),$$

with 2 omitted in cycle notation. As a product of transpositions,

$$(1\ 3\ 4) = (1\ 4)(1\ 3).$$

Product of two permutations and its cycle form

We have already computed

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (1\ 2).$$

This is already a transposition (a 2-cycle), so its decomposition into transpositions is just itself:

$$\tau \circ \sigma = (1\ 2).$$

If we reverse the order and compute $\sigma \circ \tau$, we get in general a different permutation:

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)).$$

Let us compute it explicitly:

$$\begin{aligned}
(\sigma \circ \tau)(1) &= \sigma(\tau(1)) = \sigma(3) = 1,\\
(\sigma \circ \tau)(2) &= \sigma(\tau(2)) = \sigma(2) = 4,\\
(\sigma \circ \tau)(3) &= \sigma(\tau(3)) = \sigma(4) = 3,\\
(\sigma \circ \tau)(4) &= \sigma(\tau(4)) = \sigma(1) = 2.
\end{aligned}$$

So

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}.$$

In cycle notation this is

$$\sigma \circ \tau = (2\ 4),$$

again a single transposition.

Thus, in these examples we saw:

- how to write a permutation in cycle notation;
- how to express a cycle as a product of transpositions;
- how to compose two permutations and then write the result in cycle form.

The set of all bijections of $\{1, 2, \ldots, n\}$ is denoted by S_n. As seen above, we can compose its elements, and one can check that S_n possesses the algebraic structure of a *group*, it is called the *symmetric group of degree n*. The symmetric group S_n is one of the most important groups in mathematics.

Theorem. Every permuation can be written as a product of cycles. Proof: follow the cycles.

Remark. $(a_1 a_2 \ldots a_k)(b_1 b_2 \ldots b_n) = (b_1 b_2 \ldots b_n)(a_1 a_2 \ldots a_k)$ if $a_i \neq b_j$ for all i, j.

Theorem. Every permutation can be written asa prroduct of transpositions.

Proof. Use the previous theorem and then $(1 a_1 a_2 \ldots a_k) = (1 a_k)(1 a_{k-1}) \ldots (1 a_1)$.

Remark:

$$(12)(23) = (123) \neq (132) = (23)(12), (12)(23)(12) = (23)(12)(23) = (13)$$

So if we denote $(ij) = \sigma_{ij}$ then $\sigma_{12}\sigma_{23}\sigma_{12} = \sigma_{23}\sigma_{12}\sigma_{23}$ but $\sigma_{12}\sigma_{23} \neq \sigma_{23}\sigma_{12}$. So the group S_n is not commutative but has another curious relations between uts elements!

2.2.1 :: :: problems for tutorial

1. Prove the following, using the Euler-Venn diagrams, and then only writing symbols, without any words and pictures.
   a) $(A \triangle B) \setminus C = (A \cup C) \triangle (B \cup C)$;
   b) $A \setminus (B \triangle C) = (A \setminus (B \cup C)) \cup (A \cap B \cap C)$.

2. Let $f : X \to Y$. Prove that for any subset $A \subseteq X$ and any subset $B \subseteq Y$ the inclusions hold:
   a) $A \subseteq f^{-1}(f(A))$, (the requirement that this turn into equality singles out the class of injective mappings)
   b) $B \supseteq f(f^{-1}(B))$. (the requirement that this turn into equality singles the class of surjective mappings.)
   c) Give examples showing that these inclusions can be strict.

3. Prove that if for a function $f : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ one has $f^{-1} = 1/f$, then $(f \circ f)(x) = 1/x$ for every $x \in \mathbb{R}_{>0}$. In particular, $f \circ f \circ f \circ f = \mathrm{id}$.

4. (if time permits, if not, it goes to the homework)Compute the n-th iterate of the mapping $x \mapsto \dfrac{x}{\sqrt{1+x^2}}$.

2.2.2 :: :: problems for workshop

Exercise 11. Let $A = \{1, 2, 3, 4\}, B = \{1, 2, 3, 4, 5\}$. Let

$$f : A \to B \text{ is given by } \begin{array}{l} 1 \to 3 \\ 2 \to 4 \\ 3 \to 2 \\ 4 \to 5 \end{array} \qquad g : B \to A \text{ is given by } \begin{array}{l} 1 \to 2 \\ 2 \to 1 \\ 3 \to 2 \\ 4 \to 3 \\ 5 \to 4 \end{array}$$

Find the compositions $f \circ g : B \to B, g \circ f : A \to A$. Are they injections, surjections, or bijections? Find $f^{-1}, g^{-1}, g^{-1} \circ f^{-1}, (f \circ g)^{-1}$.

It turns out that the complete preimage behaves very nicely with respect to set-theoretic Boolean operations.

Problem. Let $f : X \to Y$. Prove that for any two subsets $A, B \subseteq Y$ the following equalities hold (use only symbols, no words or pictures):

1. $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$,
2. $f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$,
3. $f^{-1}(A \setminus B) = f^{-1}(A) \setminus f^{-1}(B)$.

The behavior of the image is somewhat more complicated: some of the equalities listed above remain valid, but others turn into inclusions, which, generally speaking, can be strict.

Problem. Let $f : X \to Y$. Prove that for any two subsets $A, B \subseteq X$ the following relations hold (use only symbols, no words or pictures):

1. $f(A \cup B) = f(A) \cup f(B)$,
2. $f(A \cap B) \subseteq f(A) \cap f(B)$,
3. $f(A \setminus B) \supseteq f(A) \setminus f(B)$.

Give examples showing that the inclusions in points 2) and 3) can be strict, draw the corresponding pictures alike Euler-Venn diagramms.

2.2.3 :: :: 5th homework

Read:

Problem. Thirty boots stand in a row: 15 left and 15 right. Prove that among some ten consecutive boots there are equally many left and right ones.

Solution. Let L_i denote the number of left boots among the ten boots occupying positions $i, i+1, \ldots, i+9$. Then

$$L_1 + L_{11} + L_{21} = 15,$$

because these three disjoint blocks of ten boots together contain all 15 left boots.

If one of the numbers L_1, L_{11}, L_{21} equals 5, then we have already found the required block of ten boots with 5 left and 5 right.

Otherwise, one of these numbers is > 5 and another is < 5. When we shift the window $i, i+1, \ldots, i+9$ by one position, the number of left boots in it can change by at most 1, i.e.

$$|L_{i+1} - L_i| \leq 1.$$

Therefore, when we go from the block whose value is > 5 to the block whose value is < 5, we must pass through a block with value exactly 5. Thus, for some k we have $L_k = 5$, and the corresponding ten consecutive boots contain an equal number of left and right boots.

Write:

1. Find $|A|$ (the number of elements in the set A), where A is the set of natural numbers from a)1 to 30, b) 1 to 100 which are divisible by at least one number from the set $\{3, 5, 7, 9\}$.

2. Let A, B, C, D be four finite sets such that $A \cap B = C \cap D = \varnothing$. How to compute $|A \cup B \cup C \cup D|$ using numbers $|A|, |B|, |C|, |D|, |A \cap C|, |A \cap D|, |B \cap C|, |B \cap D|$? Hint: draw the Euler-Venn diagramm and then for each region write a variable expressing the number of elements there. Thus you may express $|X|$ for all sets X mentioned above.

3. Find the presentation of τ as a) a product of cycles b) as a product of transpositions
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}.$$

2.3 :: Cartesian products

People frequently write $X := Y$ ("is defined to be") when the object on the left is defined by the expression on the right.

Binary product. The Cartesian product of sets A and B is the set of ordered pairs where the first element is from A and the second is from B, i.e.

$$A \times B := \{(a, b) \mid a \in A,\ b \in B\}.$$

Example. If $A = \{1, 2\}$ and $B = \{a, b, c\}$, then

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}.$$

If A, B are finite sets, then $|A \times B| = |A| \cdot |B|$. We abbreviate $A^2 = A \times A$; thus $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$ is the plane, and in general the space $\mathbb{R}^n$ of dimension n consists of points, each of them having n coordinates

$$\mathbb{R}^n = \{(x_1, \ldots, x_n) \mid x_i \in \mathbb{R}\ (1 \le i \le n)\}.$$

Graphs and functions. For a function $f\colon A \to B$ its *graph* is

$$\Gamma_f := \{(a, f(a)) \mid a \in A\} \subseteq A \times B = \bigcup_{a \in A} \{(a, f(a))\}.$$

One says "a runs over A". Not every subset of $A \times B$ is a graph: for each $a \in A$ there must be *exactly one* pair in the subset whose first coordinate is a.

Definition 1. A function $f\colon A \to B$ is a subset $\Gamma \subseteq A \times B$ such that for every $a \in A$ there exists a unique $b \in B$ with $(a, b) \in \Gamma$. We then write $b = f(a)$ and $\Gamma = \Gamma_f$.

Examples. The identity $\mathrm{id}_A\colon A \to A$ has graph $\Gamma_{\mathrm{id}_A} = \{(a, a) \mid a \in A\} \subseteq A \times A$ (the diagonal).

Restriction. If $X \subseteq A$ and $f\colon A \to B$, the restriction $f|_X\colon X \to B$ has graph

$$\Gamma_{f|_X} := \Gamma_f \cap (X \times B).$$

Projections. The product $A \times B$ comes with projections

$$\pi_A\colon A \times B \to A,\ \ \pi_A(a, b) = a, \qquad \pi_B\colon A \times B \to B,\ \ \pi_B(a, b) = b.$$

Exercise. Express π_A, π_B using the graph definition of a function.

Finite sequences. Products of families. A finite sequence $(a_1, \dots, a_{100})$ of integers is an element of $\mathbb{Z}^{100}$.

Is it possible to define a direct product of an infinite family of sets? For example, we want to define an infinite sequence, what is the set of all infinite sequences $(a_1, a_2, \dots)$ on integer numbers?

We will give another definition of a direct product of two sets:

$$A_1 \times A_2 :=$$

$$\text{the set of all functions } f : \{1,2\} \to A_1 \cup A_2 \text{ such that } f(1) \in A_1, f(2) \in A_2$$

Then we can do the same for any family of sets! Let $\{A_i\}_{i \in I}$ be any family of sets parametrised by I. Define

The direct (Cartesian) product of this family is

$$\prod_{i \in I} A_i := \Big\{ f \colon I \to \bigsqcup_{i \in I} A_i \;\Big|\; f(i) \in A_i \text{ for all } i \in I \Big\},$$

i.e. the set of *choice functions* picking one element from each A_i. (For two sets this agrees with $A_1 \times A_2$ via $f \mapsto \big(f(1), f(2)\big)$.)

Restricted product over subsets of $\mathbb{Z}$ with basepoint 0. Let $\{S_i\}_{i \in I}$ be a family of subsets $S_i \subseteq \mathbb{Z}_{\geq 0}$ such that $0 \in S_i$ for all i. Define the (restricted) direct product with zero–basepoint by

$$\prod\nolimits^*_{i \in I} S_i \;:=\; \Big\{ (s_i)_{i \in I} \in \prod_{i \in I} S_i \;\Big|\; s_i = 0 \text{ for all but finitely many } i \Big\}.$$

Application: Fundamental Theorem of Arithmetic. Let $I = \mathcal{P}$ be the set of prime numbers and take $S_p = \mathbb{Z}_{\geq 0} = \{0, 1, 2, \dots\} \subset \mathbb{Z}$ for each $p \in \mathcal{P}$. For $n \in \mathbb{Z}_{\geq 1}$ write $v_p(n)$ for the exponent of p in the prime factorization of n. So,

$$n = 2^{v_2(n)} 3^{v_3(n)} 5^{v_5(n)} \cdots.$$

Then

$$\Phi : \; \mathbb{Z}_{\geq 1} \longrightarrow \prod\nolimits^*_{p \in \mathcal{P}} \mathbb{Z}_{\geq 0}, \qquad \Phi(n) = (v_p(n))_{p \in \mathcal{P}},$$

is a bijection with inverse

$$(e_p)_{p \in \mathcal{P}} \;\longmapsto\; \prod_{p \in \mathcal{P}} p^{\,e_p}.$$

Moreover, it behaves as the logarithm:

$$\Phi(nm) = \Phi(n) + \Phi(m) \quad \text{(componentwise addition)}.$$

Thus the Fundamental Theorem of Arithmetic can be expressed as the identification

$$(\mathbb{Z}_{\geq 1},\ \cdot)\ \cong\ \left(\prod\nolimits^{*}_{p\in\mathcal{P}} \mathbb{Z}_{\geq 0},\ +\right),$$

i.e. positive integers under multiplication correspond to finitely supported (i.e. only a finite number of non-zeros) exponent families (e_p) with values in $\mathbb{Z}_{\geq 0}$ and basepoint 0.

2.3.1 :: :: problems for tutorial

1. For a function $f : A \to B$ and $Y \subset B$ guess what is $\pi_A(\Gamma_f \cap (A \times Y))$
2. Guess what is $\pi_B(\Gamma_f \cap (X \times B))$ for $X \subset A$.
3. For functions $f : A \to B, g : B \to C$ express $\Gamma_{g \circ f}$ using set operations and Γ_f, Γ_g.

Projections and countable intersections Let $\pi_A : A \times B \to A$ be the projection $\pi_A(a, b) = a$.

1. Prove that for any family $\{E_i\}_{i \in I} \subseteq A \times B$,
$$\pi_A\left(\bigcup_{i \in I} E_i\right) = \bigcup_{i \in I} \pi_A(E_i).$$
2. Prove that for any family $\{E_i\}_{i \in I} \subseteq A \times B$,
$$\pi_A\left(\bigcap_{i \in I} E_i\right) \subseteq \bigcap_{i \in I} \pi_A(E_i),$$
and show that equality need not hold.
3. Give an explicit counterexample in $\mathbb{R}^2$: define a decreasing sequence of sets
$$E_1 \supseteq E_2 \supseteq E_3 \supseteq \cdots \subseteq \mathbb{R}^2$$
such that $\bigcap_{n \geq 1} E_n = \varnothing$ but
$$\bigcap_{n \geq 1} \pi_x(E_n) = \mathbb{R}.$$
4. (*Comment*) Parts (2)–(3) show that projection does not commute with countable intersections. A famous Lebesgue's paper said that they commute without proof; apparently, he considered it obvious. A counterexample to this "obvious" statement was discovered by Mikhail Suslin in 1916, which led Suslin and Luzin to the creation of the theory of analytic sets.

2.3.2 :: :: problems for workshop

Implication, DNF/CNF, and the set-theoretic analogue

(a) Two variables. Show that the truth table for $A \Rightarrow B$ coincides with

$$(\neg A \wedge \neg B) \ \vee \ (A \wedge B) \ \vee \ (\neg A \wedge B) \quad \text{and also with} \quad \neg A \vee B.$$

(b) Three variables (same idea, two representations). Consider the three-argument Boolean function

$$F(A, B, C) \ := \ (A \Rightarrow B) \ \wedge \ (B \Rightarrow C).$$

1. Compute its truth table.
2. Show that F has the *conjunctive normal form (CNF)*

$$F \equiv (\neg A \vee B) \ \wedge \ (\neg B \vee C).$$

3. Show that F has the *disjunctive normal form (DNF)*

$$F \equiv (\neg A \wedge \neg B) \ \vee \ (\neg A \wedge C) \ \vee \ (B \wedge C).$$

4. Conclude that the two formulas in (b.2) and (b.3) are logically equivalent by comparing with your truth table from (b.1).

(c) Sets (same two representations). Let X, Y, Z be subsets of a fixed universe U, and write complements as $X^c = U \setminus X$. Translate the Boolean equivalence from part (b) into a set identity:

$$(X^c \cup Y) \ \cap \ (Y^c \cup Z) \ = \ (X^c \cap Y^c) \ \cup \ (X^c \cap Z) \ \cup \ (Y \cap Z).$$

Prove this equality either by element-chasing (membership tables) or by distributive laws for $\cup, \cap$.

2.3.3 :: :: 6th homework

Read: Miklòs Laczkovich - Conjecture and Proof, pp. 49-52.

The Pigeonhole Principle

Suppose that several objects are distributed among some boxes (for example, letters among pigeonholes) such that the number of the objects is greater than the number of boxes. Then there must be a box that contains at least two objects. This simple observation is called the *pigeonhole principle*, and is used frequently in proofs of existence. In this section we shall give three examples. The first one is combinatorial, and deals with *Sidon sequences*.

A sequence $a_1 < \cdots < a_k$ of positive integers is called a *Sidon sequence* if the numbers $a_i + a_j$ $(1 \le i \le j \le k)$ are all different. Now the problem is the following: what is the length of the longest possible Sidon sequence satisfying $a_k \le n$?

Consider, for example, $n = 100$. If we want to find a long Sidon sequence, we may try the "greedy algorithm" that chooses at each step the first number that does not violate the Sidon property. In this way we obtain the numbers 1, 2, 4, 8, 13, 21, 31, 45, 66, 81, 97. But this is not the longest Sidon sequence up to 100; for example 1, 3, 7, 25, 30, 41, 44, 56, 69, 76, 77, 86 is a longer one. (This shows that the greedy algorithm need not give the best result.)

Let $s(n)$ denote the length of the longest Sidon sequence satisfying $a_k \le n$. Then we have $s(100) \ge 12$ and it can be shown by a computer search that, in fact, $s(100) = 12$. The value of $s(n)$ is not known in general. An upper bound can be obtained by using the pigeonhole principle, as follows.

Let $a_1 < \cdots < a_k$ be a Sidon sequence with $a_k \le n$. There are $\binom{k}{2} + k$ pairs of indices (i, j) satisfying $1 \le i \le j \le k$. Since $2 \le a_i + a_j \le 2n$ for every such pair, it follows that $\binom{k}{2} + k \le 2n - 1$. (Here the objects are the numbers $a_i + a_j$ and the boxes are the possible values $2, \dots, 2n$. If $\binom{k}{2} + k > 2n - 1$, that is, the number of objects is greater than the number of boxes, then there would be two objects in the same box, contradicting the Sidon property.) This gives $k(k-1) + 2k \le 4n - 2$, $k^2 < 4n$, $k < 2\sqrt{n}$ and thus $s(n) < 2\sqrt{n}$.

A better estimate is obtained if we also observe that the numbers $a_j - a_i$ $(i < j)$ are different. Since $1 \le a_j - a_i \le n-1$ for every $i < j$, the pigeonhole principle gives $\binom{k}{2} \le n - 1$ and $(k-1)^2 < 2 \cdot \binom{k}{2} \le 2(n-1) < 2n$; hence $s(n) < \sqrt{2} \cdot \sqrt{n} + 1$.

The best known upper bound is $\sqrt{n} + \sqrt[4]{n} + 1$. Paul Erdős conjectured that $|s(n) - \sqrt{n}|$ is bounded. Erdős considered this problem so important that he offered $1000 for the proof or disproof of this statement.

The next application is the following theorem: *If a and b are coprime integers, then every positive divisor of $a^2 + b^2$ is the sum of two squares.*

For example, the positive divisors of $10001 = 100^2 + 1^2$ are 1, 73, 137, and 10001 itself. Each of these numbers is the sum of two squares: $1 = 1^2 + 0^2$, $73 = 8^2 + 3^2$, and $137 = 11^2 + 4^2$.

To prove the general statement, let n be a positive divisor of $a^2 + b^2$. We may assume that n is not a perfect square. We shall prove that there are integers x, y, at least one of which is nonzero, such that n divides $x^2 + y^2$, and $|x|, |y| \le \lfloor \sqrt{n} \rfloor$. The last condition implies $x^2 + y^2 \le 2\lfloor \sqrt{n} \rfloor^2 < 2n$. Since $x^2 + y^2$ is a nonzero multiple of n, this gives $x^2 + y^2 = n$, which is to be proven.

Since $\gcd(a, b) = 1$, it follows that $\gcd(n, b) = 1$ (why?). Hence, n is a divisor of $x^2 + y^2$ if and only if n divides

$$b^2x^2 + b^2y^2 = b^2x^2 - a^2y^2 + (a^2 + b^2)y^2 = (bx - ay)(bx + ay) + (a^2 + b^2)y^2.$$

Therefore $n \mid x^2 + y^2$ will be satisfied if $n \mid bx - ay$.

Now consider the numbers $bx - ay$, where $0 \le x, y \le \lfloor \sqrt{n} \rfloor$. There are $(\lfloor \sqrt{n} \rfloor + 1)^2 > n$ such numbers. However, the possible remainders of these numbers when divided by n are $0, 1, \dots, n-1$, and thus, by the pigeonhole principle, there are distinct pairs (x_1, y_1) and (x_2, y_2) such that $bx_1 - ay_1$ and $bx_2 - ay_2$ give the same remainder. Let $x = x_1 - x_2$ and $y = y_1 - y_2$. Then $bx - ay = (bx_1 - ay_1) - (bx_2 - ay_2)$ is divisible by n. Also, $|x| \le \max(x_1, x_2) \le \lfloor \sqrt{n} \rfloor$, and similarly, $|y| \le \lfloor \sqrt{n} \rfloor$. Finally, x and y cannot be both zero, since the pairs (x_1, y_1) and (x_2, y_2) were distinct. This completes the proof.

As an important application, we obtain the following theorem of Fermat: *every prime of the form $4k + 1$ is the sum of two squares.*

next pages:

Indeed, by a basic theorem of number theory (the so-called Wilson theorem), p divides $(p-1)! + 1$. If $p = 4k + 1$, then it is easy to check that $(2k)!$ and $(2k+1)(2k+2)\cdots(4k)$ give the same remainder when divided by $4k + 1$. Therefore p divides $[(2k)!]^2 + 1$ and then, by the previous theorem, p is the sum of two squares.

For example, 1997 is a prime of the form $4k + 1$ and, accordingly, it is the sum of two squares: $1997 = 34^2 + 29^2$.

The next application of the pigeonhole principle deals with approximation by rationals. Every number can be approximated by rational numbers with an arbitrary small error. For example, if we want to approximate the number α with an error less than, say, 10^{-6} then we can proceed as follows: we find an integer p such that $p/10^6 \le \alpha < (p+1)/10^6$; then the error $|\alpha - (p/10^6)|$ will be smaller than 10^{-6}. Similarly, for every q there is a p such that $|\alpha - (p/q)| < 1/q$.

In general the error $|\alpha - (p/q)|$ is not much smaller than $1/q$. For example, if $\alpha = 1/3$ and if q is not divisible by 3, then for every p we have $|\alpha - (p/q)| = |q - 3p|/(3q) \ge 1/(3q)$. Or, if the decimal expansion of α does not contain the digits 0 and 9, then $|\alpha - (p/q)| \ge 1/(10q)$ whenever q is a power of 10 (why?). However, using other denominators, we can find much more effective approximations.

Consider for example $\alpha = \sqrt{2}$. In the fifth proof of the irrationality of $\sqrt{2}$ we remarked that $(\sqrt{2} - 1)^n = a_n + b_n\sqrt{2}$, where a_n, b_n are integers. Since $(\sqrt{2} - 1)^n \to 0$, $|b_n| \to \infty$ (why?). It follows from the binomial theorem that $(-\sqrt{2} - 1)^n = a_n - b_n\sqrt{2}$, and thus

$$(a_n + b_n\sqrt{2})(a_n - b_n\sqrt{2}) = (-1)^n.$$

Let $p_n = |a_n|$, $q_n = |b_n|$. Then

$$|p_n + q_n\sqrt{2}| \cdot |p_n - q_n\sqrt{2}| = 1,$$

from which $q_n|p_n - q_n\sqrt{2}| < 1$, and

$$\left|\sqrt{2} - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}.$$

That is, $|\sqrt{2} - (p/q)| < 1/q^2$ holds for infinitely many rationals p/q. Next we show that every irrational number has this property.

For every irrational α there are infinitely many rationals $\frac{p}{q}$ with

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}.$$

Proof. Let n be a natural number and consider the numbers $0, \{\alpha\}, \{2\alpha\}, \dots, \{n\alpha\}$, where $\{x\}$ denotes the fractional part of x; that is $\{x\} = x - [x]$.

These numbers define $n + 1$ points distributed among the n intervals $\left[\frac{i-1}{n}, \frac{i}{n}\right)$ $(i = 1, 2, \dots, n)$. There must be an interval which contains at least two of these points, and therefore there are numbers $0 \le k < m \le n$ such that $|\{m\alpha\} - \{k\alpha\}| < \frac{1}{n}$. Let $q_n = m - k$ and $p_n = [m\alpha] - [k\alpha]$. Then $0 < q_n \le n$ and $|q_n\alpha - p_n| < 1/n \le 1/q_n$, from which $|\alpha - (p_n/q_n)| < 1/q_n^2$.

In order to complete the proof we have to check that there are infinitely many different numbers among the quotients p_n/q_n. This is an immediate consequence of $0 < |q_n\alpha - p_n| < 1/n$.

Exercises

8.1. Prove that for every odd integer n there is a positive integer i such that $n \mid 2^i - 1$.

8.2. Let $a_1, a_2, \dots, a_{100}$ be a sequence of integers. Prove that there is a subsequence $a_{i_1}, a_{i_2}, \dots, a_{i_k}$ such that 100 divides $a_{i_1} + a_{i_2} + \cdots + a_{i_k}$.

8.3. Let $a_1, \dots, a_{51}$ be integers with $1 \le a_i \le 100$ $(i = 1, \dots, 51)$. Prove that $a_i \mid a_j$ holds for some $i \ne j$. (H)

8.4. The Fibonacci sequence u_n is defined as follows. Let $u_0 = 0$, $u_1 = 1$, and $u_n = u_{n-1} + u_{n-2}$ $(n = 2, 3, \dots)$. Prove that there is an $n > 0$ such that $1000 \mid u_n$.

8.5. Let p_n, q_n be as in Exercise 1.3, and let a_n, b_n be integers such that $(\sqrt{2} - 1)^n = a_n + b_n\sqrt{2}$. Prove that $a_n = p_n$ and $b_n = -q_n$.

8.6. Let $r_1 = 1$, $s_1 = 0$, and $r_{n+1} = 2r_n + 3s_n$, $s_{n+1} = r_n + 2s_n$ $(n = 1, 2, \dots)$. Prove that $|\sqrt{3} - (r_n/s_n)| < 1/s_n^2$. (H)

8.7. **a.** Let D be a positive integer, and let n be a positive divisor of $a^2 + Db^2$, where a and b are coprime integers. Prove that there are integers i, x, y such that $1 \le i \le D$ and $i \cdot n = x^2 + Dy^2$.

b. Prove that if $\gcd(a, b) = 1$, then every positive divisor of $a^2 + 2b^2$ is of the form $x^2 + 2y^2$ with integer x, y. Check the result on the divisors of $10002 = 100^2 + 2 \cdot 1^2$.

c. Prove that if $\gcd(a, b) = 1$, then every positive and odd divisor of $a^2 + 3b^2$ is of the form $x^2 + 3y^2$ with integer x, y. Check the result on the divisors of $10003 = 100^2 + 3 \cdot 1^2$.

2.4 :: power set, Cantor's theorem, Russel's paradox

Let A be a set. By 2^A we denote the set of all subsets of A, it is called the **power set** for A. Also it is frequently denoted as $\mathbb{P}(A)$ (the power set for A). Remember that 2^A is a set, it is not a number.

Example:

$$A = \{1, x, B\},$$

$$2^A = \{\varnothing, \{1\}, \{x\}, \{B\}, \{1, x\}, \{1, B\}, \{x, B\}, \{1, x, B\}\}$$

Theorem: 2^A can be identified with the set of all functions $A \to \{0, 1\}$.

Proof. Indeed, each subset $Y \subset A$ corresponds to the characteristic function of this subset, $\chi_Y : A \to \{0, 1\}$ and vice versa.

The set of all functions $f : A \to B$ is denoted by B^A. What is $\varnothing^A, A^\varnothing$?

Later in the Set theory course the number 2 will be **defined** as $\{0, 1\}$. This explains the notation 2^A for the set of maps $A \to \{0, 1\}$, i.e. the power set of A.

Problem 1. If $|A| < \infty$ (i.e. A is finite), then $|2^A| = 2^{|A|}$.

Indeed, for each element in A, we have two choices: include or not include it to a subset. So, $2^{|A|}$ possibilities.

Problem 2. For sets A, B with $A \cap B = \varnothing$, prove that $2^A \times 2^B = 2^{A \cup B}$.

Proof. We construct a **bijection** between $2^A \times 2^B$ and $2^{A \cup B}$. The first set is the set of pairs (a, b) where $a \subset A, b \subset B$. Given such a pair, consider the set $f(a, b) = a \cup b \subset A \cup B$, note that $a \cup b$ is an element of $2^{A \cup B}$, so we constructed a map $f : 2^A \times 2^B \to 2^{A \cup B}$. The map $g : 2^{A \cup B} \to 2^A \times 2^B$ in other direction is constructed as follows: let $c \in 2^{A \cup B}$, construct a pair $(c \cap A, c \cap B) \in 2^A \times 2^B$, this gives a map $g : 2^{A \cup B} \to 2^A \times 2^B$. Then check that $f \circ g$ and $g \circ f$ are both identity maps, so f, g are both bijections.

Theorem 1. For any sets A and B, there is a natural bijection

$$(2^A)^B \;\cong\; 2^{A \times B}.$$

In words: the set of all functions $B \to 2^A$ is the same as the set of all subsets of the Cartesian product $A \times B$.

Proof. An element of $(2^A)^B$ is a function

$$f : B \longrightarrow 2^A,$$

so for each $b \in B$ we have a subset $f(b) \subseteq A$.

Define a subset of $A \times B$ by

$$S_f := \{(a, b) \in A \times B \mid a \in f(b)\}.$$

This gives a map

$$\Phi : (2^A)^B \longrightarrow 2^{A \times B}, \qquad f \mapsto S_f.$$

Conversely, if $S \subseteq A \times B$, define a function

$$f_S : B \longrightarrow 2^A, \qquad f_S(b) := \{a \in A \mid (a, b) \in S\}.$$

This gives a map

$$\Psi : 2^{A \times B} \longrightarrow (2^A)^B, \qquad S \mapsto f_S.$$

It is immediate from the definitions that

$$\Psi(\Phi(f)) = f \qquad \text{and} \qquad \Phi(\Psi(S)) = S.$$

Thus Φ and Ψ are inverse bijections, proving the claim. □

Interpretation for $A = \{a_1, a_2, a_3\},\ B = \{b_1, b_2, b_3, b_4\}$

Elements of $A \times B$ are the 12 pairs

$$(a_i, b_j), \qquad 1 \le i \le 3,\ 1 \le j \le 4.$$

A subset $S \subseteq A \times B$ can be visualised as selecting some of these pairs. For each fixed $b_j \in B$, the *fiber*

$$S_{b_j} = \{\, a_i \in A : (a_i, b_j) \in S \,\}$$

is a subset of A. Therefore, from such an S we obtain a function

$$f_S : B \longrightarrow 2^A, \qquad f_S(b_j) = S_{b_j}.$$

Conversely, given any function

$$f : B \to 2^A,$$

for each b_j we choose a subset $f(b_j) \subseteq A$. These four subsets determine exactly which of the pairs (a_i, b_j) belong to the corresponding subset of $A \times B$:

$$(a_i, b_j) \in S_f \iff a_i \in f(b_j).$$

Thus specifying a subset of the grid

$$A \times B \;=\; \{a_1, a_2, a_3\} \times \{b_1, b_2, b_3, b_4\}$$

is equivalent to specifying, for each column b_j, a subset of A. This is exactly a function $B \to 2^A$.

Cantor's theorem: no injection $2^A \to A$

Lemma 1. Let A and B be sets. Then the following are equivalent:

1. There exists an injection $A \to B$.
2. There exists a surjection $B \to A$.

In particular:

- If no injection $A \to B$ exists, then no surjection $B \to A$ exists.
- If no surjection $B \to A$ exists, then no injection $A \to B$ exists.

Proof. (1) $\Rightarrow$ (2): Assume $f : A \to B$ is injective. Then f identifies A with the subset $f(A) \subseteq B$. Let $g : B \to A$ be defined by

$$g(b) = \begin{cases} a, & \text{if } b = f(a) \text{ for some } a \in A, \\ a_0, & \text{if } b \notin f(A), \end{cases}$$

where $a_0 \in A$ is fixed.

Every $a \in A$ has $f(a) \in B$ with $g(f(a)) = a$, so g is surjective.

(2) $\Rightarrow$ (1): Assume $g : B \to A$ is surjective. For each $a \in A$ choose one $b \in B$ with $g(b) = a$. Define $f : A \to B$ by sending each a to one of these chosen b's.

If $f(a) = f(a') = b$, then applying g gives

$$a = g(b) = a',$$

so f is injective.

The two "in particular" statements follow immediately: if (1) fails then (2) cannot hold, and if (2) fails then (1) cannot hold. □

Theorem 2 (Cantor)**.** For every set A there is no injective map

$$f : 2^A \longrightarrow A.$$

Equivalently, $|2^A| > |A|$ for every set A.

We first give a proof in the finite case, using an explicit construction, and then a more general argument that works for arbitrary sets.

Lemma 2 (Finite case)**.** Let A be a finite set. Then there is no injective map $f : 2^A \to A$.

Proof. Assume, for contradiction, that such an injective map $f : 2^A \to A$ exists.

Define inductively

$$X_0 := \varnothing, \quad x_1 := f(X_0), \quad X_1 := \{x_1\}.$$

Having defined $X_n \subseteq A$ and $x_{n+1} = f(X_n)$, put

$$X_{n+1} := X_n \cup \{x_{n+1}\}.$$

Claim: For every $n \geq 0$ we have $x_{n+1} \notin X_n$, and hence all elements $x_1, x_2, x_3, \ldots$ are pairwise distinct.

Indeed, suppose $x_{n+1} \in X_n$. Then $x_{n+1} = x_j$ for some $1 \leq j \leq n$. But by construction

$$x_{n+1} = f(X_n) \quad \text{and} \quad x_j = f(X_{j-1}).$$

Hence

$$f(X_n) = f(X_{j-1}).$$

Since $j - 1 < n$, we have $X_{j-1} \subsetneq X_n$, so $X_{j-1} \neq X_n$. This contradicts the injectivity of f.

Thus each step produces a new element $x_{n+1} \notin \{x_1, \ldots, x_n\}$, so A contains infinitely many distinct elements $x_1, x_2, \ldots$, which is impossible because A is finite.

Therefore no injective map $2^A \to A$ can exist when A is finite. □

For arbitrary sets we use a slightly different (and classical) argument. It is usually stated in terms of *surjections* $A \to 2^A$, but the two forms are equivalent.

Lemma 3 (Cantor's theorem in surjective form)**.** For every set A there is no surjective map

$$g : A \longrightarrow 2^A.$$

Proof. Assume, for contradiction, that $g : A \to 2^A$ is surjective.

Define a special subset $B \subseteq A$ by

$$B := \{\, a \in A \mid a \notin g(a) \,\}.$$

Since $B \subseteq A$, it is an element of 2^A. By surjectivity of g there exists some $b \in A$ such that

$$g(b) = B.$$

Now ask: does b belong to B?

Case 1: Suppose $b \in B$. By the definition of B this means $b \notin g(b)$. But $g(b) = B$, so this says $b \notin B$, a contradiction.

Case 2: Suppose $b \notin B$. Then, by the definition of B, we must have $b \in g(b)$. Since $g(b) = B$, this says $b \in B$, again a contradiction.

In both cases we reach a contradiction, so no such surjection g can exist (this idea is sometimes called "The Cantor diagonal argument"). □

Exercise: rewrite this proof to show that for each set A there exists no injective map $2^A \to A$.

Corollary 1. For every set A there is no injective map $f : 2^A \to A$.

Remark 1. The finite proof above can be viewed as a concrete version of the fact that $|2^A| > |A|$: assuming an injection $2^A \to A$ lets us construct an infinite sequence of distinct elements inside a finite set. The general diagonal argument shows that this phenomenon persists for *all* sets A, finite or infinite.

Russell's Paradox

Theorem 3 (Russell's paradox)**.** There is no set R such that

$$R = \{\, x \mid x \notin x \,\}.$$

In other words, the collection of all sets that do not contain themselves cannot be a set.

Proof. Assume, for contradiction, that such a set R exists.

Ask whether $R \in R$.

Case 1: Suppose $R \in R$. By the definition of R, a set belongs to R precisely when it does *not* belong to itself. Hence from $R \in R$ we must conclude $R \notin R$, a contradiction.

Case 2: Suppose $R \notin R$. Then by the defining condition of R, any set that does not belong to itself *must* be in R. Thus $R \in R$, again a contradiction.

Both possibilities lead to contradiction, so such a set R cannot exist. □

Remark 2. Russell's paradox shows that naive "comprehension" (forming a set of all objects satisfying a property $P(x)$) must be restricted. Modern set theory avoids the paradox by allowing only subsets of existing sets (separation), not arbitrary collections.

Countable and uncountable sets

Definition 2 (Countable, denumerable, uncountable)**.** A set A is called *countable* if there exists an injective map $A \to \mathbb{N}$.

A set A is called *denumerable* (or *countably infinite*) if there exists a bijection

$$f : \mathbb{N} \longrightarrow A.$$

A set is called *uncountable* if it is not countable.

Example 1. The sets $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{Q}$ are denumerable. In particular, $\mathbb{N}$ is denumerable via the identity map $n \mapsto n$.

We now show that uncountable sets actually exist.

Theorem 4. The power set $\mathcal{P}(\mathbb{N}) = 2^{\mathbb{N}}$ is uncountable.

Proof. Suppose, for contradiction, that $2^{\mathbb{N}}$ is countable. Then there exists an injective map

$$f : 2^{\mathbb{N}} \longrightarrow \mathbb{N}.$$

But this contradicts Cantor's theorem (proved above), which states that there is *no* injective map $2^A \to A$ for any set A, in particular for $A = \mathbb{N}$.

Hence $2^{\mathbb{N}}$ cannot be countable; it is uncountable. □

Corollary 2. There exists at least one uncountable set (namely $2^{\mathbb{N}}$).

2.4.1 :: :: tutorial/midterm solutions and common mistakes

In what follows we suppose that the two following propositions are true:

Proposition 1. The teaching team of Basic Concepts of Maths wants its student to do good in the course, including midterm, exams etc...

Proposition 2. Nikita sent an email claiming that in the midterm there will be 5 exercises covering: induction, pigeonhole principle, counting in two ways, proving of inclusion of two sets in a formal way (without words), presentation of a given permutation as a product of cycles and as a product of transpositions.

Combining the two above propositions we get the following corollary.

Corollary 3. There is a bijection between the questions of the midterm and the topics of the proposition (2)

We will try to find the bijection between exercises and topics!

Exercise 1. We draw an arrow on each side and each diagonal of a polygon. Show that there exists a vertex Z of this polygon such that any other vertex is reachable from Z if we are allowed to move along the arrows.

Solution. Here proving of inclusion of two sets in a formal way (without words), presentation of a given permutation as a product of cycles and as a product of transpositions don't make sense. Pigeonhole doesn't neither (what would we put in boxes?). Same for counting in two ways, what should we count? We are left with induction.

Label the vertices of the polygon by $1, 2, \ldots, n$. On each side and each diagonal we draw exactly one arrow between its two endpoints, so between any two distinct vertices there is exactly one directed edge (one arrow). Thus this is a directed graph[42] on n vertices.

We want to prove: **There exists a vertex Z such that every other vertex is reachable from Z by following arrows.**

We prove this by induction on n.

Base case $n = 3$. This is a direct verification. Draw a triangle with all possible directions of arrows and we are done. A remark, if we consider graphs and not polygons, we can even reduce to the case where $n = 1$.

[42] called a *tournament* in graph theory

Induction hypothesis. Assume that in every polygon where diagonals are drawn as well as arrows with n vertices, there exists a vertex from which all other vertices are reachable along directed paths.

Induction step: from n to $n+1$. Consider a such a polygon T on $n+1$ vertices. Pick one vertex and call it x, and remove it temporarily, as well as all the arrows/edges joining it. The remaining n vertices still form a polygon with the needed properties. By the induction hypothesis, there exists a vertex Z among these n vertices such that every other one of these n vertices is reachable from Z by a directed path.

Now look at the direction of the arrow between Z and x. There are two cases:

- **Case 1:** $Z \to x$.

  Then Z already has directed paths to all the other $n-1$ vertices (by the induction hypothesis), and there is a direct arrow from Z to x. Therefore, *every* vertex (including x) is reachable from Z. So in this case Z is the vertex we need.

- **Case 2:** $x \to Z$.

  Then from x we can go directly to Z, and from Z we can reach every other vertex among the remaining $n-1$ vertices (again by the induction hypothesis). Thus from x there is a directed path to every other vertex:

  $$x \to Z \to \cdots \to v$$

  for any vertex $v \neq x$. So in this case x is the vertex we need.

In either case, we have found a vertex (either Z or x) from which all other vertices of the $(n+1)$-vertex are reachable by following arrows.

This completes the induction, and hence in any orientation of all sides and diagonals of the polygon there exists a vertex Z from which every other vertex is reachable. □

Common mistakes: Many students supposed that they can choose the directions of the arrows. **We cannot** as we don't know these directions, they can be any. Some student wanted to split a vertex, it is not clear at all what this means. Students also tried to prove it by contradiction: Suppose there is no such vertex Z. Maybe it is possible to do so, but many details are needed to be taken cared of which was not done. Many times the induction was done on the **edges**, no! What we need is an induction on the **verticies**.

Exercise 2. Is it possible to divide a convex 17-gon into 14 triangles ?

Solution. We have already used the induction in the previous exercise. We are left with pigeonhole principle, counting in two ways, proving of inclusion of two sets in a formal way (without words), presentation of a given permutation as a product of cycles and as a product of transpositions. It is more or less clear that proving of inclusion of two sets in a formal way (without words), presentation of a given permutation as a product of cycles and as a product of transpositions is not what we need. We are left with pigeonhole or counting in two ways. The counting in two ways make more sense here.

Suppose a convex 17-gon is covered exactly by N triangles. Each triangle has angle sum 180°, so the sum of the angles of all triangles is

$$N \cdot 180^\circ.$$

We compute the same quantity in another way by grouping angles at each point where triangles meet.

Let

- $n = 17$ be the number of original vertices of the polygon,
- b be the number of additional *boundary* vertices created by subdividing edges,
- k be the number of *interior* vertices inside the polygon.

At each original vertex of the convex polygon, the sum of angles of all triangles meeting there equals the interior angle of the polygon at that vertex. Thus the total contribution from the original vertices is

$$(n-2) \cdot 180^\circ = (17-2) \cdot 180^\circ = 15 \cdot 180^\circ.$$

At each additional boundary vertex, the polygon boundary is straight, so the region inside the polygon forms a half-plane. The triangles that meet at such a point fill exactly that half-plane, so the sum of their angles there is

$$180^\circ.$$

Thus the b boundary subdivision points contribute $b \cdot 180^\circ$.

At each interior vertex, the triangles surround the point completely and fill a full circle, so the sum of the triangle angles at such a point is

$$360^\circ.$$

Hence the k interior points contribute $k \cdot 360^\circ$.

Summing all contributions, we obtain another expression for the total sum of triangle angles:

$$N \cdot 180^\circ = 15 \cdot 180^\circ + b \cdot 180^\circ + k \cdot 360^\circ.$$

Divide both sides by 180°:

$$N = 15 + b + 2k.$$

Since $b \geq 0$ and $k \geq 0$, we conclude that

$$N \geq 15.$$

Therefore a covering of a convex 17-gon by only 14 triangles is impossible. □

Common mistakes: A lot of students understood that they should provide an explicit division of the 17-gon and show that this division gives 15 triangles. No, the exercise should be read as follows, I give you 14 triangles, with absolutely no details about these triangle, is it possible with these 14 triangles to divide our 17-gon ? So we are not asking you to divide the 17-gon by taking all the diagonals starting from one vertex and prove that there are actually 15 triangles, or using other diagonals and show that we get again 15 triangles. These are fixed division that you constructed, and we are not interested by this. Other students thought about using counting in two ways, but doing it with the edges. Again the idea was with a fixed division coming from diagonals, so not what we need. Students also tried to use induction here, but again, this gave a fixed division of the 17-gon. Finally some students understood that it was about angles. But they forgot to speak about angles on the edges of the 17-gon, or angles inside the 17-gon, but this was already very good!

Exercise 3. Let A, B, C, D be sets. Prove or disprove that

$$(A \triangle C) \cap (B \triangle D) \subseteq (A \cup B) \triangle (C \cup D).$$

Solution. This is clearly about inclusion of sets. The claim is false. Indeed by taking $A = D = \{1\}$ and $C = B = \{\emptyset\}$ we get

$$(A \triangle C) \cap (B \triangle D) = \{1\} \tag{1}$$

whereas

$$(A \cup B) \triangle (C \cup D) = \{\emptyset\} \tag{2}$$

showing that the claim is false. □

Common mistakes: You need to remember this for the future, this is very important: *If you think that a statement is true, then you prove it. If you think that a claim is false then giving a* **counterexample is enough !** Many students tried to prove that the claim is false. You should not! It was almost impossible to understand the logic of what was written.

Exercise 4. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 3 & 1 & 2 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 3 & 4 \end{pmatrix}.$$

Present $\tau \circ \sigma$ as a product of cycles and as a product of transpositions.

Solution. We can all agree that this is about permutations.
By definition,

$$(\tau \circ \sigma)(i) = \tau\big(\sigma(i)\big).$$

Compute this for $i = 1, \ldots, 6$.

$$(\tau \circ \sigma)(1) = \tau(\sigma(1)) = \tau(6) = 4, \tag{3}$$
$$(\tau \circ \sigma)(2) = \tau(\sigma(2)) = \tau(4) = 5, \tag{4}$$
$$(\tau \circ \sigma)(3) = \tau(\sigma(3)) = \tau(5) = 3, \tag{5}$$
$$(\tau \circ \sigma)(4) = \tau(\sigma(4)) = \tau(3) = 1, \tag{6}$$
$$(\tau \circ \sigma)(5) = \tau(\sigma(5)) = \tau(1) = 2, \tag{7}$$
$$(\tau \circ \sigma)(6) = \tau(\sigma(6)) = \tau(2) = 6. \tag{8}$$

So in two-line notation,

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 3 & 1 & 2 & 6 \end{pmatrix}.$$

Now write as disjoint cycles: follow the images.

$$1 \mapsto 4 \mapsto 1 \quad \Longrightarrow \quad (1\ 4),$$
$$2 \mapsto 5 \mapsto 2 \quad \Longrightarrow \quad (2\ 5),$$

$$3 \mapsto 3, \qquad 6 \mapsto 6,$$

so 3 and 6 are fixed points.

Thus

$$\tau \circ \sigma = (1\ 4)(2\ 5)(3)(6),$$

where we usually omit the 1-cycles (3) and (6).

As a product of transpositions, we already have such a decomposition, since a 2-cycle is a transposition. Therefore

$$\tau \circ \sigma = (1\ 4)(2\ 5)(3)(6)$$

is the required expression as a product of cycles (disjoint cycles) and also as a product of transpositions.

□

Common mistakes: Not much to say here, be careful with the computations. We do not write things like $(3, 3)$ or $(6, 6)$, this should be just (3) or (6).

Exercise 5. During the last academic year, Raphael Laoshi solved at least one problem in mathematics every day. However, in any week (any 7 consecutive days) he solved no more than 12 problems. Prove that there exist some consecutive days during which he solved exactly 20 problems.

Solution. We are left with the last exercise. And we only have the pigeonhole left. Thus this exercise is about pigeonhole. This exercise is **HARD!** The hardest from the midterm. Because the problem is hard the solution will be very wordy to explain what we are doing.

Proof. Let a_i be the number of problems solved on day i. We know two things:

- Every day he solves at least one problem, so $a_i \geq 1$.
- In any 7 consecutive days he solves at most 12 problems.

Step 1: Look at the first 21 days. Split these 21 days into three blocks of 7 days each:

$$\{1, \ldots, 7\}, \quad \{8, \ldots, 14\}, \quad \{15, \ldots, 21\}.$$

Each block has at most 12 problems, so the total for all 21 days is at most 36. Since he solves at least one problem every day, the total is at least 21. Thus the number of problems solved in the first 21 days lies between 21 and 36.

Step 2: Prefix sums. Let

$$S_m = a_1 + a_2 + \cdots + a_m$$

be the total number of problems solved up to day m (and set $S_0 = 0$). Then

$$0 = S_0 < S_1 < S_2 < \cdots < S_{21} \leq 36.$$

So we now have 22 different numbers between 0 and 36.

Step 3: What we are looking for. If we want to find some consecutive days whose total is exactly 20, we are trying to find days $p+1$ through q such that

$$a_{p+1} + \cdots + a_q = 20.$$

But the left side is just a difference of prefix sums:

$$S_q - S_p = 20.$$

So our real goal is this:

Find two prefix sums that differ by exactly 20.

Step 4: Remainders and the pigeonhole. To find such a pair, take all the prefix sums $S_0, \ldots, S_{21}$. Look at the remainders of these numbers when we divide thm by 20. Since all possible remainders are $\{0, 1, 2, \ldots, 19\}$, by the pigeonhole principle we must have S_p, S_q with the same remainder. We may assume $q > p$. Then 20 divides $1 \leq S_q - S_p \leq 36$. Thus $S_q - S_p = 20$.

Thus the days $p+1$ through q have total

$$S_q - S_p = a_{p+1} + \cdots + a_q = 20.$$

Conclusion. There must be a block of consecutive days during which he solved exactly 20 problems. □

Common mistakes: There was a lot of hand-waving proofs, that were actually not proofs. On the other hand this exercise is hard, so nothing to worry about if you couldn't find the solution. Very few students mentioned that we should use the pigeonhole principle here.

2.4.2 :: :: problems for workshop: Even and Odd Permutations

Let S_n be the set of all permutations of $\{1, \ldots, n\}$. A *transposition* is a permutation that swaps two elements and fixes all others, it is written as $(i\ j)$.

• **[Definition of the parity via transpositions]** Every permutation $\sigma \in S_n$ can be written as a product of transpositions:

$$\sigma = \tau_1 \tau_2 \cdots \tau_k.$$

We say that σ is *even* if it can be written as a product of an even number of transpositions; σ is *odd* if it can be written as a product of an odd number of transpositions. This notion is well-defined (see the problems below).

• **[Definition of the parity via inversions]** For $\sigma \in S_n$, define an *inversion* to be a pair (i, j) with $1 \leq i < j \leq n$ and $\sigma(i) > \sigma(j)$. Let $\mathrm{inv}(\sigma)$ be the number of inversions. (cf. Problem on page 15)

Define $\varepsilon(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$. Show that $\varepsilon(\mathrm{id}) = 1$. Show that $\varepsilon(\sigma \circ (i\ j)) = -\varepsilon(\sigma)$. Conclude that $\varepsilon(\sigma) = \mathrm{sgn}(\sigma)$.

•**[All permutations in S_3]**

a) List all 6 permutations in S_3 in cycle notation.

b) Decompose each into transpositions and determine whether it is even or odd.

c) Check using the number of inversions.

•**[Computations in S_5]** Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Compute $\mathrm{inv}(\sigma)$.

•**[Sign of a cycle]** Let $c = (1\,2\,\ldots\,k)$ be a k-cycle.

a) Show that
$$(1\,2\,\ldots\,k) = (1\,k)(1\,k-1)\cdots(1\,3)(1\,2).$$

b) Deduce that $\mathrm{sgn}(c) = (-1)^{k-1}$.

c) Conclude that sgn of any permutation in disjoint cycle form is the product of the signs of its cycles.

Lemma 4. Let $\sigma \in S_n$ and let $\tau = (i\,j)$ with $i < j$, $\sigma' = \tau\sigma$. Then

$$\mathrm{inv}(\sigma') = \mathrm{inv}(\tau\sigma) \equiv \mathrm{inv}(\sigma) + 1 \pmod 2.$$

Proof. Recall that $\mathrm{inv}(\sigma) = \#\{(p,q) \mid p < q,\ \sigma(p) > \sigma(q)\}$.

(1) For indices less than i and bigger than j the inversion count for σ and σ' does not change at all.

(2) Middle indices $i < k < j$. For each k with $i < k < j$ look at triples (i,k,j). Before the transposition we compare $\sigma(i), \sigma(k), \sigma(j)$; after it, $\sigma(i)$ and $\sigma(j)$ swap places, and $\sigma(k)$ stays the same. Note that the pairity for the number of inversions in two pairs $\sigma(i)\sigma(k)$ and $\sigma(k)\sigma(j)$ does not change when we swap $\sigma(i)$ and $\sigma(j)$. Indeed, without loss of generality we may assume that $i = 1, k = 2, j = 3$ and $\sigma \in S_3$ and so check all six possible choices for σ to verify the statement.

(3) The pair (i,j). Here we compare $\sigma(i)$ with $\sigma(j)$, while in σ' we compare $\sigma'(i) = \sigma(j)$ with $\sigma'(j) = \sigma(i)$. So the pair $(\sigma(i), \sigma(j))$ changes from inversion to non-inversion or vice versa, contributing $+1$ modulo 2.

Therefore

$$\mathrm{inv}(\tau\sigma) \equiv \mathrm{inv}(\sigma) + 1 \pmod 2. \qquad \square$$

2.4.3 :: :: 7th homework

- Let

$$\sigma = (1\,7\,5\,3)\,(2\,6)\,(4\,9\,8) \in S_9.$$

a) Compute $\mathrm{sgn}(\sigma)$ using the fact that a k-cycle has sign $(-1)^{k-1}$.

b) Verify your answer by expressing σ as a product of transpositions.

c) Verify again by computing the number of inversions of σ.

- Let

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 7 & 3 & 2 & 8 & 4 & 6 \end{pmatrix} \in S_8.$$

a) Rewrite τ in disjoint cycle notation.

b) Compute $\mathrm{sgn}(\tau)$ using the formula for the sign of a cycle.

c) Check your answer by computing the parity of the number of inversions of τ.

- On the boundary of a convex polygon there grow hairs, in outside direction. Someone draws several non-intersection diagonals in the polygon, each such diagonal has hairs on one side. These diagonals dissect polygon into parts. Show that among these parts there exists a polygon with hairs outside. [Hint: induction]

2.5 :: infinite sequences, recursive definitions, Collatz conjecture

Definition 3 (Finite sequences)**.** Let A be a set and let $n \in \mathbb{N}$. A *finite sequence of length n* with values in A is a function

$$a : \{1, 2, \ldots, n\} \longrightarrow A.$$

We write such a sequence as

$$(a(1), a(2), \ldots, a(n)),$$

or, using subscript notation,

$$(a_1, a_2, \ldots, a_n).$$

Definition 4 (Infinite sequences)**.** An *infinite sequence* with values in A is a function

$$a : \mathbb{N} \longrightarrow A.$$

We usually denote it by

$$a(i), \qquad a_i, \qquad \text{or} \qquad (a_i)_{i \in \mathbb{N}},$$

all of which refer to the value of the sequence at index i.

Remark 3. Thus a sequence is simply a function with domain either $\{1, \ldots, n\}$ (finite case) or $\mathbb{N}$ (infinite case).

Componentwise operations

Let A be a set equipped with an operation. Typical example is $A = \mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$, with ordinary addition or multiplication.

Definition 5 (Componentwise sum)**.** Let $(a_i)_{i \in I}$ and $(b_i)_{i \in I}$ be two sequences in a set A equipped with a binary operation $+$. Their *componentwise sum* is the sequence

$$(a_i + b_i)_{i \in I}, \qquad \text{defined by} \qquad (a_i + b_i)(i) = a_i + b_i.$$

Definition 6 (Componentwise product)**.** If A has a multiplication $\cdot$, then the *componentwise product* of two sequences (a_i) and (b_i) is the sequence

$$(a_i \cdot b_i)_{i \in I}, \qquad \text{defined by} \qquad (a_i \cdot b_i)(i) = a_i \cdot b_i.$$

These operations are defined both for finite sequences and infinite sequences. They simply operate index-by-index. We also have the usual properties such as

$$a(b + c) = ab + ac, ab = ba, a(bc) = (ab)c, \text{etc.}$$

Second–order linear recurrences

Definition 7 (Second–order linear recurrence)**.** Let A be a set equipped with addition and scalar multiplication (e.g. $A = \mathbb{R}$ or $\mathbb{C}$). A sequence $(u_n)_{n\geq 0}$ satisfies a *second–order linear recurrence* if there exist constants c_1, c_2 such that

$$u_{n+2} = c_1 u_{n+1} + c_2 u_n \qquad \text{for all } n \geq 0.$$

Proposition 3 (Two initial values determine the sequence)**.** Let (u_n) satisfy

$$u_{n+2} = c_1 u_{n+1} + c_2 u_n.$$

Then the entire sequence is uniquely determined by the two initial values u_0 and u_1.

Proof. Knowing u_0 and u_1, the recurrence gives

$$u_2 = c_1 u_1 + c_2 u_0.$$

Once u_2 is known, the recurrence gives u_3, then u_4, and so on. Thus every term is determined inductively and uniquely. □

Characteristic polynomial

To such a recurrence we associate the *characteristic polynomial*

$$P(z) = z^2 - c_1 z - c_2.$$

Proposition 4 (Distinct roots give the general formula)**.** Suppose the characteristic polynomial

$$z^2 - c_1 z - c_2$$

has two distinct roots z_1 and z_2 (in $\mathbb{C}$). Then every solution of the recurrence has the form

$$u_n = A z_1^n + B z_2^n$$

for some constants A, B (determined by u_0 and u_1).

Moreover, for any given pair (u_0, u_1) there exists a unique pair (A, B) producing a sequence whose first two terms are exactly u_0 and u_1.

Proof. Since z_1 and z_2 satisfy the polynomial equation $z^2 - c_1 z - c_2 = 0$, we have

$$z_1^{n+2} = c_1 z_1^{n+1} + c_2 z_1^n, \qquad z_2^{n+2} = c_1 z_2^{n+1} + c_2 z_2^n.$$

Thus the sequences (z_1^n) and (z_2^n) both satisfy the recurrence.

Any linear combination

$$u_n = Az_1^n + Bz_2^n$$

also satisfies the recurrence (because the recurrence is linear).

To match initial conditions, solve the system

$$\begin{cases} u_0 = A + B, \\ u_1 = Az_1 + Bz_2. \end{cases}$$

Since $z_1 \neq z_2$, this 2×2 system has a unique solution

$$A = \frac{u_1 - u_0 z_2}{z_1 - z_2}, \qquad B = \frac{u_0 z_1 - u_1}{z_1 - z_2}.$$

Thus the coefficients are uniquely determined, and therefore the entire sequence is uniquely determined. □

Remark 4. The phrase *"then it is automatic"* refers to the fact that once the coefficients A and B have been chosen to make u_0 and u_1 correct, the formula

$$u_n = Az_1^n + Bz_2^n$$

automatically satisfies the recurrence for all $n \geq 0$, so no further verification is required.

Example: the Fibonacci sequence

The Fibonacci sequence $(F_n)_{n\geq 0}$ is defined by the second–order recurrence

$$F_{n+2} = F_{n+1} + F_n \qquad \text{with} \qquad F_0 = 0,\ F_1 = 1.$$

Thus it is an example of a recurrence of the form

$$u_{n+2} = c_1 u_{n+1} + c_2 u_n, \qquad c_1 = 1,\ c_2 = 1.$$

Characteristic polynomial. The associated characteristic polynomial is

$$z^2 - z - 1 = 0.$$

Its two distinct roots are

$$z_1 = \frac{1+\sqrt{5}}{2} = \varphi, \qquad z_2 = \frac{1-\sqrt{5}}{2} = \psi,$$

often called the golden ratio and its conjugate.

Explicit formula ("Binet's formula"). Since the roots are distinct, the general solution is

$$F_n = Az_1^n + Bz_2^n.$$

The constants A and B are determined from the initial conditions.

From $F_0 = 0$:

$$0 = A + B \quad \Rightarrow \quad B = -A.$$

From $F_1 = 1$:

$$1 = Az_1 + Bz_2 = Az_1 - Az_2 = A(z_1 - z_2).$$

Since

$$z_1 - z_2 = \frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2} = \sqrt{5},$$

we obtain

$$A = \frac{1}{\sqrt{5}}, \qquad B = -\frac{1}{\sqrt{5}}.$$

Hence the closed form is

$$\boxed{F_n = \frac{1}{\sqrt{5}}\left(\varphi^n - \psi^n\right).}$$

Why this works automatically. Because the formula

$$u_n = Az_1^n + Bz_2^n$$

satisfies the recurrence whenever z_1 and z_2 are roots of the characteristic polynomial, once the constants A and B are chosen to match u_0 and u_1, the whole sequence automatically satisfies

$$u_{n+2} = u_{n+1} + u_n \quad \text{for all } n.$$

First values.

$$F_0 = 0,\ F_1 = 1,\ F_2 = 1,\ F_3 = 2,\ F_4 = 3,\ F_5 = 5,\ F_6 = 8,\ \ldots$$

Fibonacci numbers thus give the simplest and most famous example of a second–order linear recurrence with two distinct characteristic roots.

Cassini's identity and other inductive properties

The Fibonacci sequence satisfies many remarkable identities that can be proved by simple induction once the recurrence

$$F_{n+2} = F_{n+1} + F_n$$

is known.

Theorem 5 (Cassini's identity)**.** For every integer $n \geq 1$,

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

Proof. We use induction on n.

Base case: For $n = 1$,

$$F_2F_0 - F_1^2 = 1 \cdot 0 - 1^2 = -1 = (-1)^1.$$

Induction step: Assume the identity holds for n:

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

Using the recurrence $F_{n+2} = F_{n+1} + F_n$, compute:

$$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= (F_{n+1} + F_n)F_n - F_{n+1}^2 \\ &= F_{n+1}F_n + F_n^2 - F_{n+1}^2 \\ &= -\big(F_{n+1}^2 - F_{n+1}F_n - F_n^2\big) \\ &= -\big(F_{n+1}(F_{n+1} - F_n) - F_n^2\big). \end{aligned}$$

A cleaner way: rewrite the LHS using the recurrence on the induction hypothesis:

$$\begin{aligned} F_{n+2}F_n - F_{n+1}^2 &= (F_{n+1} + F_n)F_n - F_{n+1}^2 \\ &= -\big(F_{n+1}^2 - F_{n+1}F_n - F_n^2\big) \\ &= -\big(F_{n+1}F_{n-1} - F_n^2\big) \qquad \text{(by the recurrence)} \\ &= -(-1)^n = (-1)^{n+1}. \end{aligned}$$

Thus the identity holds for $n+1$. By induction it holds for all n. □

Theorem 6 (Sum of the first n Fibonacci numbers)**.** For all $n \geq 0$,

$$F_0 + F_1 + F_2 + \cdots + F_n = F_{n+2} - 1.$$

Proof. We again use induction.

Base case: For $n = 0$,

$$F_0 = 0 = F_2 - 1 = 1 - 1.$$

Induction step: Assume the formula holds for n:

$$\sum_{k=0}^{n} F_k = F_{n+2} - 1.$$

Then for $n + 1$,

$$\sum_{k=0}^{n+1} F_k = \left(\sum_{k=0}^{n} F_k \right) + F_{n+1} = (F_{n+2} - 1) + F_{n+1} = F_{n+3} - 1,$$

using $F_{n+3} = F_{n+2} + F_{n+1}$. This completes the induction. □

Remark 5. Both identities illustrate a common phenomenon: many global properties of the Fibonacci sequence reduce to short calculations once the recurrence relation is known. The recurrence allows inductive proofs to extend "local" relations to all n.

The Thue–Morse sequence

Binary representations

Every nonnegative integer can be written uniquely in base 2.

Definition 8 (Binary representation)**.** For each integer $n \geq 0$ there exist unique digits $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_k \in \{0, 1\}$ such that

$$n \;=\; \varepsilon_0 2^0 + \varepsilon_1 2^1 + \cdots + \varepsilon_k 2^k \quad \text{and} \quad \varepsilon_k = 1 \text{ if } n > 0.$$

We write

$$n = (\varepsilon_k \varepsilon_{k-1} \ldots \varepsilon_1 \varepsilon_0)_2$$

and call this the *binary representation* of n.

The *binary digit sum* of n is

$$s_2(n) := \varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_k.$$

Example 2.

$$5 = (101)_2 = 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0, \qquad s_2(5) = 1+0+1 = 2;$$
$$13 = (1101)_2 = 1\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0, \quad s_2(13) = 1+1+0+1 = 3.$$

We now give four equivalent ways to define the Thue–Morse sequence.

Definition 9 (Thue–Morse sequence)**.** The *Thue–Morse sequence* is the infinite 0–1 sequence $(t_n)_{n\geq 0}$ which can be described in the following equivalent ways.

(a) **Recursion in base** 2**.**

$$t_0 = 0, \qquad t_{2n} = t_n, \qquad t_{2n+1} = 1 - t_n \quad \text{for all } n \geq 0.$$

(b) **Parity of the binary digit sum.** For each $n \geq 0$, write n in binary and let $s_2(n)$ be the sum of its binary digits. Then

$$t_n \equiv s_2(n) \pmod 2,$$

i.e. $t_n = 0$ if the number of 1's in the binary expansion of n is even, and $t_n = 1$ if it is odd.

(c) **Fixed point of a substitution.** Consider the substitution

$$\mu : 0 \mapsto 01, \quad 1 \mapsto 10.$$

Starting from the one-letter word $w_0 = 0$, define

$$w_{k+1} := \mu(w_k) \quad (k \geq 0).$$

where

$$\mu(\varepsilon_k\varepsilon_{k-1}\ldots\varepsilon_1\varepsilon_0) = (\mu(\varepsilon_k)\mu(\varepsilon_{k-1})\ldots\mu(\varepsilon_1)\mu(\varepsilon_0))$$

Thus

$$w_0 = 0, \quad w_1 = 01, \quad w_2 = 0110, \quad w_3 = 01101001, \quad \ldots$$

Each w_k is a prefix of w_{k+1}, so there is a unique infinite word $w = 01101001\ldots$ having all w_k as initial segments. Then t_n is the n-th symbol of this word.

(d) **Recursive block construction.** For a finite word $u = u_0 u_1 \dots u_{m-1}$ over $\{0,1\}$, let $\overline{u}$ be the word obtained by flipping all bits, i.e. replacing $0 \leftrightarrow 1$:

$$\overline{u} := (1-u_0)(1-u_1)\dots(1-u_{m-1}).$$

Define a sequence of finite words $(u_k)_{k\geq 0}$ by

$$u_0 := 0, \qquad u_{k+1} := u_k\,\overline{u_k} \quad (k \geq 0).$$

So

$$u_0 = 0, \quad u_1 = 01, \quad u_2 = 0110, \quad u_3 = 01101001, \quad \dots$$

Again, each u_k is a prefix of u_{k+1}, so there is a unique infinite word having all u_k as prefixes, and $(t_n)_{n\geq 0}$ is defined to be its sequence of symbols.

The first few terms are

$$(t_n)_{n\geq 0} = 0,1,1,0,1,0,0,1,1,0,0,1,0,1,1,0,\dots$$

Proposition 5. Descriptions (a), (b), (c), and (d) in Definition 9 all define the same sequence $(t_n)_{n\geq 0}$.

Proof. We prove a chain of equivalences.

(a) $\iff$ (b). Define a sequence $(u_n)_{n\geq 0}$ by

$$u_n := s_2(n) \pmod 2.$$

We show that (u_n) satisfies the recursion in (a) with $u_0 = 0$.

Write n in binary. Appending a 0 at the right corresponds to multiplying by 2, and appending a 1 at the right corresponds to multiplying by 2 and adding 1. Hence

$$s_2(2n) = s_2(n), \qquad s_2(2n+1) = s_2(n) + 1.$$

Reducing mod 2 gives

$$u_{2n} = u_n, \qquad u_{2n+1} = 1 - u_n,$$

and clearly $u_0 = s_2(0) = 0$. Thus (u_n) satisfies the recursion in (a).

Conversely, any sequence (t_n) satisfying (a) is uniquely determined by t_0: once t_0 is fixed, all t_n follow by repeatedly using the rules for t_{2n} and t_{2n+1}. Hence the sequence defined in (b) (which we have called (u_n)) coincides with the sequence defined in (a), and (a) and (b) are equivalent.

(b) $\Longrightarrow$ (d). For $k \geq 0$ let

$$T_k := t_0 t_1 \dots t_{2^k-1}$$

be the prefix of length 2^k of the infinite sequence (t_n) defined by (b). We claim that

$$T_0 = 0, \qquad T_{k+1} = T_k \, \overline{T_k}.$$

The first equality is immediate: T_0 has length 1 and $t_0 = s_2(0) \equiv 0$. Now fix $k \geq 0$ and $0 \leq m < 2^k$. Then $2^k + m$ has binary expansion obtained from that of m by adding a leading 1, so

$$s_2(2^k + m) = 1 + s_2(m).$$

Thus

$$t_{2^k+m} \equiv s_2(2^k + m) \equiv 1 + s_2(m) \equiv 1 - t_m \pmod 2,$$

i.e. $t_{2^k+m} = 1 - t_m$. This shows precisely that the block $(t_{2^k}, \dots, t_{2^{k+1}-1})$ is the bitwise complement of $(t_0, \dots, t_{2^k-1})$, so $T_{k+1} = T_k \, \overline{T_k}$. Hence the infinite sequence from (b) satisfies the block construction (d).

Conversely, the infinite word produced in (d) is uniquely determined by the rule $u_{k+1} = u_k \overline{u_k}$ and the starting word $u_0 = 0$, so (b) and (d) define the same sequence.

(c) $\Longleftrightarrow$ (d). Let μ be the substitution $0 \mapsto 01$, $1 \mapsto 10$ of (c), and let u_k be as in (d). We claim that

$$u_{k+1} = \mu(u_k) \quad \text{for all } k \geq 0.$$

Indeed, for a single letter $a \in \{0, 1\}$ we have

$$\mu(a) = a(1 - a),$$

so for a word $u = u_0 u_1 \dots u_{m-1}$ we obtain

$$\mu(u) = u_0(1 - u_0)\, u_1(1 - u_1) \dots u_{m-1}(1 - u_{m-1}) = u \, \overline{u}.$$

Therefore

$$u_{k+1} = u_k \, \overline{u_k} = \mu(u_k),$$

and by induction we get $u_k = \mu^k(0)$. Thus the sequence of words (u_k) in (d) coincides with the sequence (w_k) in (c), and the corresponding infinite words (and hence the sequences (t_n)) are the same.

(c) $\Longrightarrow$ (a). Let $(v_n)_{n \geq 0}$ be the sequence defined by (c), i.e. the n-th symbol of the unique infinite word w with $\mu(w) = w$ and w starting with 0. Each letter a of

w produces in $\mu(w)$ the two-letter block $a(1-a)$. Therefore, in positions $2n$ and $2n+1$ of w we see exactly the two letters generated from the letter in position n:

$$v_{2n} = v_n, \qquad v_{2n+1} = 1 - v_n.$$

Also $v_0 = 0$. Hence (v_n) satisfies the recursion in (a), and by the uniqueness argument above, (v_n) coincides with (t_n) from (a).

Combining (a)$\Longleftrightarrow$(b), (b)$\Longleftrightarrow$(d), and (c)$\Longleftrightarrow$(d), we conclude that all four descriptions define one and the same sequence $(t_n)_{n\geq 0}$, the Thue–Morse sequence. $\square$

Non-periodicity(without proofs)

Remark 6. The Thue–Morse sequence (t_n) is not eventually periodic. That is, there do not exist integers $N \geq 0$ and $p \geq 1$ such that

$$t_{n+p} = t_n \quad \text{for all } n \geq N.$$

Remark 7. In fact, the Thue–Morse sequence is much stronger: it contains no *overlaps* and in particular no substring of the form xxx where x is any nonempty finite word (it is *cube-free*). This deep property goes back to work of A. Thue and is a cornerstone of combinatorics on words.

Optional reading: Gauss's arithmetic–geometric mean iteration

Definition 10 (Arithmetic and geometric means)**.** For two positive real numbers $a, b > 0$ define their *arithmetic mean* and *geometric mean* by

$$A(a,b) = \frac{a+b}{2}, \qquad G(a,b) = \sqrt{ab}.$$

Definition 11 (Gauss (AGM) sequences)**.** Fix $a_0, b_0 > 0$. Define two sequences (a_n) and (b_n) by

$$a_{n+1} = \frac{a_n + b_n}{2}, \qquad b_{n+1} = \sqrt{a_n b_n}.$$

These are called the *arithmetic* and *geometric* mean iterations.

The following facts are classical and fundamental.

Proposition 6 (Monotonicity)**.** For all $n \geq 0$,

$$a_{n+1} \leq a_n, \qquad b_{n+1} \geq b_n.$$

Thus (a_n) is decreasing and (b_n) is increasing.

Proof. Since $a_n \geq b_n > 0$, the arithmetic–geometric mean inequality gives

$$\sqrt{a_n b_n} \leq \frac{a_n + b_n}{2}.$$

Thus

$$b_{n+1} \leq a_{n+1}.$$

But clearly

$$a_{n+1} = \frac{a_n + b_n}{2} \leq \frac{a_n + a_n}{2} = a_n,$$

and

$$b_{n+1} = \sqrt{a_n b_n} \geq \sqrt{b_n b_n} = b_n.$$

□

Proposition 7 (Squeezing)**.** For all n,

$$b_n \leq a_n.$$

Moreover, the difference $a_n - b_n$ tends to 0.

Proof. The inequality $b_n \leq a_n$ is preserved by the iteration:

$$a_{n+1} - b_{n+1} = \frac{a_n + b_n}{2} - \sqrt{a_n b_n} = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} \geq 0.$$

The right-hand side is 0 exactly when $a_n = b_n$.

Also,

$$a_{n+1} - b_{n+1} = \frac{(\sqrt{a_n} - \sqrt{b_n})^2}{2} \leq \frac{a_n - b_n}{2},$$

so the positive sequence $(a_n - b_n)$ is decreasing and is bounded below by 0, hence convergent. The last inequality shows that its only possible limit is 0. □

Theorem 7 (Convergence to a common limit: the AGM)**.** The sequences (a_n) and (b_n) converge to the same limit:

$$a_n \longrightarrow M(a_0, b_0), \qquad b_n \longrightarrow M(a_0, b_0),$$

where $M(a_0, b_0)$ is called the *arithmetic–geometric mean* of a_0 and b_0.

Proof. We already know:

- (a_n) is decreasing and bounded below by 0, hence convergent;
- (b_n) is increasing and bounded above by a_0, hence convergent;
- $a_n - b_n \to 0$.

Let

$$\lim_{n\to\infty} a_n = L_a, \qquad \lim_{n\to\infty} b_n = L_b.$$

Since $a_n - b_n \to 0$ we have $L_a = L_b$. Denote this common limit by

$$M(a_0, b_0).$$

□

Remark 8. Gauss showed that the AGM has deep connections with elliptic integrals:

$$\pi = 2\, M(1, \sqrt{1-k^2}) \cdot \int_0^{\pi/2} \frac{1}{\sqrt{1 - k^2 \sin^2\theta}}\, d\theta.$$

This relation lies at the heart of the fastest algorithms for computing π.

2.5.1 :: :: problems for tutorial: powers of $1 \pm \sqrt{2}$ and almost–integers

Problem 1 (Uniqueness of representation)**.** Let $a, b, c, d \in \mathbb{Q}$ and suppose

$$a + b\sqrt{2} = c + d\sqrt{2}.$$

Prove that $a = c$ and $b = d$.

Problem 2. For each $n \geq 0$ write

$$(1 - \sqrt{2})^n = a_n - b_n\sqrt{2}$$

with real numbers a_n, b_n.

1. Compute explicitly a_0, b_0, then a_1, b_1, then a_2, b_2.
2. Using the binomial theorem or induction on n, show that in fact $a_n, b_n \in \mathbb{Z}$ for all $n \geq 0$.
3. Show that the sequences (a_n) and (b_n) satisfy the same recurrence

   $$x_{n+2} = 2x_{n+1} - x_n$$

   with appropriate initial conditions.
4. Show that for all $n \geq 0$ the same integers a_n, b_n from the previous problem also satisfy

   $$(1 + \sqrt{2})^n = a_n + b_n\sqrt{2}.$$

Problem 3 (Integer part of the sum)**.** Let

$$u_n = (1 + \sqrt{2})^n + (1 - \sqrt{2})^n.$$

1. Express u_n in terms of a_n and deduce that $u_n \in \mathbb{Z}$ for all n.
2. Find a recurrence relation for u_n (it should again be order 2).
3. Compute the first several values of u_n (for example, for $n = 0, 1, 2, 3, 4$).
4. Let k be a positive integer. Show that if

   $$n > k \log_2 10,$$

   then $|(\sqrt{2} - 1)^n| < 10^{-k}$.
5. Show that for such even n the first k digits to the right of the decimal point in $(1 + \sqrt{2})^n$ are nines. Solutions are in Section 5.3

2.5.2 :: :: problems for workshop: second–order linear recurrences

Consider a second–order linear recurrence $u_{n+2} = c_1 u_{n+1} + c_2 u_n$. Its characteristic polynomial is $z^2 - c_1 z - c_2$, and knowledge of its roots gives a closed form for (u_n).

- If the characteristic polynomial has two distinct roots z_1, z_2, then

$$u_n = A z_1^n + B z_2^n$$

  for uniquely determined constants A, B (complex in general), obtained from u_0, u_1.

- If the characteristic roots are complex conjugates $re^{\pm i\varphi}$ and u_0, u_1 are real, then

$$u_n = r^n\big(A\cos(n\varphi) + B\sin(n\varphi)\big) \qquad (A, B \in \mathbb{R}).$$

- If the characteristic polynomial has a double root r, then

$$u_n = (A + Bn) r^n.$$

1. (Distinct complex roots; modulus–argument form) Solve the recurrence

$$u_{n+2} - 6u_{n+1} + 10u_n = 0, \qquad u_0 = 2,\ u_1 = 1,$$

and express the answer in the form

$$u_n = R \cdot \rho^n \cos(n\varphi - \theta).$$

2. (Repeated root)

Consider the recurrence

$$u_{n+2} - 2\lambda\, u_{n+1} + \lambda^2 u_n = 0, \qquad u_0 = \alpha,\ u_1 = \beta, \qquad \lambda \in \mathbb{C} \setminus \{0\}.$$

(a) Prove that $u_n = (A + Bn)\lambda^n$.

(b) Express A, B in terms of α, β, λ.

(c) Solve

$$u_{n+2} - 6u_{n+1} + 9u_n = 0, \qquad u_0 = 2,\ u_1 = 9.$$

Solution.

The characteristic equation is

$$z^2 - 6z + 10 = 0.$$

The roots are

$$z = 3 \pm i.$$

Write them in polar form:

$$3 + i = \rho e^{i\varphi}, \qquad \rho = \sqrt{3^2 + 1} = \sqrt{10}, \qquad \varphi = \arctan(1/3).$$

Hence

$$u_n = A(3+i)^n + B(3-i)^n = \rho^n\big(Ce^{in\varphi} + \overline{C}e^{-in\varphi}\big) = \rho^n\big(\alpha\cos(n\varphi) + \beta\sin(n\varphi)\big)$$

with real α, β.

Use initial conditions:

$$u_0 = 2 = \alpha, \qquad u_1 = 1 = \rho(\alpha\cos\varphi + \beta\sin\varphi).$$

Thus

$$1 = \sqrt{10}\big(2\cos\varphi + \beta\sin\varphi\big),$$

so

$$\beta = \frac{1}{\sqrt{10}\sin\varphi} - 2\cot\varphi = \frac{1}{1} - 2\cdot\frac{\cos\varphi}{\sin\varphi}$$

(using $\sin\varphi = \frac{1}{\sqrt{10}}$ and $\cos\varphi = \frac{3}{\sqrt{10}}$). Hence

$$\beta = 1 - 2\cdot 3 = -5.$$

Thus

$$u_n = (\sqrt{10})^n\big(2\cos(n\varphi) - 5\sin(n\varphi)\big).$$

Now rewrite in amplitude–phase form:

$$a\cos(n\varphi) + b\sin(n\varphi) = \sqrt{a^2+b^2}\,\cos(n\varphi - \theta), \quad \theta = \arctan\frac{b}{a}.$$

Here

$$R = \sqrt{2^2 + (-5)^2} = \sqrt{29}, \qquad \theta = \arctan\left(\frac{-5}{2}\right).$$

$$\boxed{u_n = \sqrt{29}\,(\sqrt{10})^n\cos\big(n\varphi - \theta\big), \qquad \varphi = \arctan(1/3).}$$

2.5.3 :: :: 8th homework

Definition 12 (Collatz map)**.** Define $T : \mathbb{N}_{\geq 1} \to \mathbb{N}_{\geq 1}$ by

$$T(n) \;=\; \begin{cases} \dfrac{n}{2}, & \text{if } n \text{ is even,} \\ 3n+1, & \text{if } n \text{ is odd.} \end{cases}$$

For $k \geq 0$, let T^k denote the k-fold iterate of T and the *trajectory* of n be $(n, T(n), T^2(n), \dots)$.

Very famous open Collatz (or $3n+1$) conjecture: For every $n \in \mathbb{N}_{\geq 1}$ there exists $k \geq 0$ such that $T^k(n) = 1$. Equivalently, every trajectory reaches the cycle $1 \mapsto 4 \mapsto 2 \mapsto 1$.

1. ~~Prove Collatz conjecture~~ Starting from 18, apply the Collatz map until you hit 1.

   (Complex conjugate roots with real data)] Let $u_{n+2} - 2u_{n+1} + 5u_n = 0$, with $u_0 = 0,\ u_1 = 1$.

   (a) Find a closed form for u_n using only real functions.

   (b) Show that for all $n \geq 0$,

   $$u_{n+1}^2 + 5u_n^2 - 2u_{n+1}u_n = 5^n.$$

   Hint: Either use the closed form, or consider $z_n = (1+2i)^n$ and relate $|z_n|^2 = 5^n$ to u_n.

2. (**Minimal polynomial from samples**) A sequence (u_n) satisfies a second–order linear homogeneous recurrence with constant coefficients and has values $u_0 = 1,\ u_1 = 2,\ u_2 = 5,\ u_3 = 12$.

   (a) Find the recurrence.

   (b) Decide whether it has a double root or distinct complex roots.

   (c) Solve for u_n.

Problem 1 (Complex conjugate roots with real data)**.** Let $(u_n)_{n\geq 0}$ satisfy

$$u_{n+2} - 2u_{n+1} + 5u_n = 0, \qquad u_0 = 0, \quad u_1 = 1.$$

1. Find a closed form for u_n using only real functions.
2. Show that for all $n \geq 0$,

$$u_{n+1}^2 + 5u_n^2 - 2u_{n+1}u_n = 5^n.$$

Proof. **(1) Closed form.** The characteristic polynomial is

$$r^2 - 2r + 5 = 0.$$

Its roots are

$$r_{1,2} = 1 \pm 2i.$$

Thus the general complex solution is

$$u_n = A(1+2i)^n + B(1-2i)^n,$$

for some constants $A, B \in \mathbb{C}$. Since the initial data u_0, u_1 are real and the roots are complex conjugate, we will get a real sequence for $B = \overline{A}$, but we can instead solve directly from u_0, u_1.

From $u_0 = 0$ we get

$$0 = u_0 = A + B \quad \Rightarrow \quad B = -A.$$

From $u_1 = 1$ we get

$$1 = u_1 = A(1+2i) + B(1-2i) = A(1+2i) - A(1-2i) = A\big((1+2i) - (1-2i)\big) = A($$

Hence

$$A = \frac{1}{4i}.$$

Therefore

$$u_n = \frac{(1+2i)^n - (1-2i)^n}{4i}.$$

Now write $1+2i$ in polar form. Its modulus is

$$\rho = |1+2i| = \sqrt{1^2+2^2} = \sqrt{5},$$

and we can choose an angle φ with

$$\cos\varphi = \frac{1}{\sqrt{5}}, \qquad \sin\varphi = \frac{2}{\sqrt{5}}, \qquad \varphi = \arctan 2.$$

Then

$$1 + 2i = \sqrt{5}\, e^{i\varphi}, \qquad 1 - 2i = \sqrt{5}\, e^{-i\varphi}.$$

Hence

$$(1+2i)^n = (\sqrt{5})^n e^{in\varphi}, \qquad (1-2i)^n = (\sqrt{5})^n e^{-in\varphi}.$$

Substituting into the formula for u_n,

$$\begin{aligned} u_n &= \frac{(\sqrt{5})^n e^{in\varphi} - (\sqrt{5})^n e^{-in\varphi}}{4i} = \frac{(\sqrt{5})^n}{4i}\big(e^{in\varphi} - e^{-in\varphi}\big) \\ &= \frac{(\sqrt{5})^n}{4i} \cdot 2i \sin(n\varphi) = \frac{(\sqrt{5})^n}{2} \sin(n\varphi), \end{aligned}$$

where $\varphi = \arctan 2$.

Thus a closed real form is

$$\boxed{u_n = \frac{(\sqrt{5})^{\,n}}{2} \sin\big(n \arctan 2\big).}$$

(2) Quadratic identity. We will prove

$$u_{n+1}^2 + 5u_n^2 - 2u_{n+1}u_n = 5^n \quad \text{for all } n \geq 0,$$

using a complex-number interpretation.

Define

$$z_n = (1+2i)^n.$$

Write z_n in terms of its real and imaginary parts:

$$z_n = a_n + ib_n, \qquad a_n, b_n \in \mathbb{R}.$$

Then

$$|z_n|^2 = a_n^2 + b_n^2 = |1+2i|^{2n} = 5^n.$$

On the other hand, from part (1) we have

$$u_n = \frac{(1+2i)^n - (1-2i)^n}{4i} = \frac{z_n - \overline{z_n}}{4i} = \frac{b_n}{2},$$

since $z_n - \overline{z_n} = 2ib_n$. Thus

$$b_n = 2u_n.$$

Next, compute z_{n+1}:

$$z_{n+1} = (1+2i)z_n = (1+2i)(a_n + ib_n) = (a_n - 2b_n) + i(2a_n + b_n).$$

Hence

$$b_{n+1} = 2a_n + b_n.$$

Using $u_{n+1} = b_{n+1}/2$ and $u_n = b_n/2$, we get

$$u_{n+1} = \frac{b_{n+1}}{2} = \frac{2a_n + b_n}{2} = a_n + \frac{b_n}{2} = a_n + u_n.$$

Thus

$$a_n = u_{n+1} - u_n.$$

Now plug a_n and b_n into $|z_n|^2$:

$$5^n = a_n^2 + b_n^2 = (u_{n+1} - u_n)^2 + (2u_n)^2.$$

Expanding,

$$5^n = u_{n+1}^2 - 2u_{n+1}u_n + u_n^2 + 4u_n^2 = u_{n+1}^2 + 5u_n^2 - 2u_{n+1}u_n.$$

This is exactly the desired identity:

$$\boxed{u_{n+1}^2 + 5u_n^2 - 2u_{n+1}u_n = 5^n \quad \text{for all } n \geq 0.}$$

This completes the proof. □

2.6 :: countable and uncountable sets, Cantor–Bernstein theorem

Simple shifts on countable sets. Define

$$f : \mathbb{N} \to \{2, 3, 4, \dots\}, \qquad f(n) = n + 1.$$

This is clearly a bijection: every integer $k \geq 2$ has a unique preimage $k - 1 \in \mathbb{N}$.

This illustrates a basic idea:

$$\mathbb{N} \sim \mathbb{N} \setminus \{1\}.$$

Here the notation "$A \sim B$" means: *there exists a bijection between A and B.*

A bijection between $(0, 1]$ and $(0, 1)$. We now construct an explicit bijection

$$(0, 1] \longrightarrow (0, 1).$$

Consider the countable set

$$S = \left\{ \frac{1}{n} : n \in \mathbb{N},\ n \geq 1 \right\} \subset (0, 1].$$

We will "shift" this set one step to the right.

Define $f : (0, 1] \to (0, 1)$ by

$$f(x) = \begin{cases} \dfrac{1}{n+1}, & \text{if } x = \dfrac{1}{n} \text{ for some } n \geq 1, \\ x, & \text{if } x \notin S. \end{cases}$$

- f is injective: If $x \notin S$, then $f(x) = x$, and these values are never equal to any $\frac{1}{n+1}$. If $x = \frac{1}{n}$ and $y = \frac{1}{m}$ with $n \neq m$, then $f(x) = \frac{1}{n+1} \neq \frac{1}{m+1} = f(y)$.
- f is surjective: Let $y \in (0, 1)$. If $y \notin \{1/(n+1) : n \geq 1\}$, then $y \notin f(S)$, so $f(y) = y$. If $y = \frac{1}{n+1}$, then $y = f\left(\frac{1}{n}\right)$.

Hence f is a bijection and

$$(0, 1] \sim (0, 1).$$

Homotheties and translations in the plane

Definition 13 (Homothety)**.** Let $\lambda > 0$. The *homothety* with center at the origin and ratio λ is the map

$$H_\lambda : \mathbb{R}^2 \to \mathbb{R}^2, \qquad H_\lambda(x) = \lambda x.$$

It is a bijection with inverse $H_{1/\lambda}$.

For example, if

$$D_r = \{x = (x_1, x_2) \in \mathbb{R}^2 : \|x\| = \sqrt{x_1^2 + x_2^2} < r\}$$

is the open disc of radius r centered at the origin, then

$$H_\lambda : D_r \longrightarrow D_{\lambda r}$$

is a bijection between discs of different radii.

Definition 14 (Parallel transport (translation))**.** For a fixed vector $v \in \mathbb{R}^2$, the *translation* by v is

$$T_v : \mathbb{R}^2 \to \mathbb{R}^2, \qquad T_v(x) = x + v.$$

This is a bijection with inverse T_{-v}.

Thus if D and D' are two discs of the same radius with different centers, a suitable translation T_v gives a bijection $D \to D'$. Similarly one constructs a bijection between two discs with arbitrarily radii and centers.

Disc with and without boundary

Let

$$D = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 < 1\}$$

be the open unit disc, and

$$\overline{D} = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leq 1\}$$

the closed unit disc (disc with boundary). We want a bijection

$$\overline{D} \longrightarrow D.$$

Idea: mimic the "shifting a countable set" trick using a countable family of concentric circles with radii $\{\frac{1}{n}\}$, $n = 1, 2, 3, \ldots$.

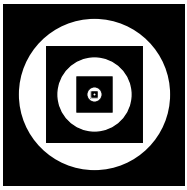
Cantor–Schröder–Bernstein theorem

Theorem 8 (Cantor–Bernstein (Schröder–Bernstein)). Let A, B be sets. Suppose there are injective maps

$$f : A \to B, \qquad g : B \to A.$$

Then there exists a bijection $h : A \to B$.

We will not prove this theorem in this course. The idea of the proof can be indicated on the example with a square and a disc. Fix injections, and apply them many times (see picture below). Now the bijection from the square to the disc is given by a constant map on the white parts and homothety shift inside of the black parts:



(A full proof will appear in the Set Theory course.) Instead we use it as a powerful tool:

To show that $|A| = |B|$, it suffices to construct injections both ways.

Example: $\mathbb{N}$ and $\mathbb{N} \times \mathbb{N}$

We show that

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

by constructing *two injections* and then applying the Cantor–Schröder–Bernstein theorem.

Injection $\mathbb{N} \to \mathbb{N} \times \mathbb{N}$. Define

$$f : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}, \qquad f(n) = (n, 1).$$

If $f(n) = f(m)$, then $(n, 1) = (m, 1)$, hence $n = m$. So f is injective.

Injection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Use the Fundamental Theorem of Arithmetic. For each pair $(m, n) \in \mathbb{N} \times \mathbb{N}$, set

$$g(m, n) = 2^m 3^n \in \mathbb{N}.$$

If $g(m, n) = g(m', n')$, then

$$2^m 3^n = 2^{m'} 3^{n'}.$$

By uniqueness of prime factorization, we must have $m = m'$ and $n = n'$. Thus g is injective.

Conclusion. We have constructed injections

$$f : \mathbb{N} \to \mathbb{N} \times \mathbb{N} \quad \text{and} \quad g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}.$$

By the Cantor–Schröder–Bernstein theorem, there exists a bijection

$$h : \mathbb{N} \longrightarrow \mathbb{N} \times \mathbb{N}.$$

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

Important corollary: So a countable union of countable sets is countable.

A bijection between $[0, 1]^2$ and $[0, 1]$

We now apply Cantor–Bernstein to show that

$$[0, 1]^2 \sim [0, 1].$$

Step 1: Injection $[0, 1] \to [0, 1]^2$. This is easy:

$$f : [0, 1] \to [0, 1]^2, \qquad f(x) = (x, 0).$$

Clearly injective.

Step 2: Injection $[0, 1]^2 \to [0, 1]$. We first build an injection $(0, 1)^2 \to (0, 1)$ by interleaving binary digits.

Write

$$x = 0.x_1x_2x_3\ldots, \qquad y = 0.y_1y_2y_3\ldots$$

in binary (avoiding the ambiguous expansions ending with repeating 1's). Define

$$\varphi(x, y) = 0.x_1y_1x_2y_2x_3y_3\ldots$$

(again in binary). Then $\varphi : (0,1)^2 \to (0,1)$ is injective.

To extend this to $[0,1]^2 \to [0,1]$, we can modify finitely or countably many special points (those with two binary expansions), or simply note:

- There is an injection $[0,1]^2 \to (0,1)^2$ (for instance, squeeze the square slightly into its interior).
- There is an injection $(0,1)^2 \to (0,1)$ (the map φ above).
- There is an injection $(0,1) \to [0,1]$ (inclusion).

Composing these, we obtain an injection

$$g : [0,1]^2 \to [0,1].$$

Step 3: Apply Cantor–Bernstein. We now have:

$$\text{an injection } [0,1] \to [0,1]^2 \quad \text{and} \quad \text{an injection } [0,1]^2 \to [0,1].$$

By Cantor–Bernstein, there exists a bijection

$$h : [0,1]^2 \longrightarrow [0,1].$$

Other examples

Using similar ideas and the Cantor–Bernstein theorem, one can show:

- $\mathbb{R} \sim (0,1) \sim (0,1)^2 \sim \mathbb{R}^2 \sim \mathbb{R}^n$ for any fixed $n \geq 1$.
- Any nonempty open interval $I \subset \mathbb{R}$ has the same cardinality as $\mathbb{R}$.
- Any open disc in the plane has the same cardinality as $\mathbb{R}$ and as the entire plane $\mathbb{R}^2$.

The key patterns to remember and practice in everyday life:

1. Removing or adding a finite or countable set (e.g. a boundary, a few special points) does not change cardinality.
2. Cantor–Bernstein allows us to turn *two* injections into a bijection.

Example 3. Let $I = \mathbb{N}$ and let all $A_i = \mathbb{Z}$, where $\mathbb{Z}$ is considered as a set with the distinguished point 0. Recall that the restricted direct product

$$\prod_i^* A_i$$

consists of all families $(a_i)_{i\in\mathbb{N}}$ such that $a_i = 0$ for all but finitely many i.

1. Verify that $\prod_i^* A_i$ is countable.
2. Verify that the full product $\prod_i A_i = \mathbb{Z}^{\mathbb{N}}$ has the cardinality of the continuum.

Proof. **(1) The restricted product is countable.**

By the definition of the restricted product with the distinguished point 0, we have

$$\prod_i^* A_i = \Big\{(a_i)_{i\in\mathbb{N}} \in \mathbb{Z}^{\mathbb{N}} \;\Big|\; a_i = 0 \text{ for all but finitely many } i\Big\}.$$

In other words, each element is a sequence of integers which is zero from some point on.

For each $k \geq 0$ define

$$S_k = \Big\{(a_i)_{i\in\mathbb{N}} \in \prod_i^* A_i \;\Big|\; a_i = 0 \text{ for all } i > k\Big\}.$$

Then every sequence with finite support belongs to some S_k, so

$$\prod_i^* A_i = \bigcup_{k\geq 0} S_k.$$

For fixed k, the set S_k is in bijection with $\mathbb{Z}^k$ via

$$(a_1, \dots, a_k, 0, 0, \dots) \longleftrightarrow (a_1, \dots, a_k).$$

Since $\mathbb{Z}$ is countable, so is every finite power $\mathbb{Z}^k$. Hence each S_k is countable.

Therefore $\prod_i^* A_i$ is a countable union of countable sets, so it is countable.

(2) The full product has the cardinality of the continuum.

The full product

$$\prod_i A_i = \mathbb{Z}^{\mathbb{N}}$$

is the set of all sequences of integers $(a_i)_{i\in\mathbb{N}}$.

First, we show that $\mathbb{Z}^{\mathbb{N}}$ is *uncountable*. Consider the subset

$$\{0,1\}^{\mathbb{N}} = \{(a_i)_{i\in\mathbb{N}} : a_i \in \{0,1\}\} \subset \mathbb{Z}^{\mathbb{N}}.$$

The set $\{0,1\}^{\mathbb{N}}$ is in bijection with the power set $\mathcal{P}(\mathbb{N})$ via characteristic functions:

$$E \subseteq \mathbb{N} \quad \longleftrightarrow \quad (\chi_E(i))_{i\in\mathbb{N}},$$

where $\chi_E(i) = 1$ if $i \in E$ and 0 otherwise. Thus

$$|\{0,1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})|.$$

By Cantor's theorem, $\mathcal{P}(\mathbb{N})$ is uncountable, so $\{0,1\}^{\mathbb{N}}$ is uncountable, and hence $\mathbb{Z}^{\mathbb{N}}$ is uncountable as well.

Next, we show that $\mathbb{Z}^{\mathbb{N}}$ has the cardinality of the continuum (the same as $\mathbb{R}$). Since $\mathbb{Z}$ is countable, there is a bijection $\mathbb{Z} \cong \mathbb{N}$, which induces a bijection

$$\mathbb{Z}^{\mathbb{N}} \cong \mathbb{N}^{\mathbb{N}}.$$

It is a standard result that

$$|\mathbb{N}^{\mathbb{N}}| = |\mathbb{R}|$$

(e.g. by encoding infinite sequences of natural numbers as real numbers in $(0,1)$ via base expansions, and conversely by sending (a_i) to $\sum_{n=1}^{\infty} 10^{-\sum_i^n a_i}$, then Cantor-Bernstein theorem).

Thus

$$|\mathbb{Z}^{\mathbb{N}}| = |\mathbb{N}^{\mathbb{N}}| = |\mathbb{R}|,$$

i.e. the full product $\prod_i A_i$ has the cardinality of the continuum. □

Theorem 9 (Cantor)**.** The set of real numbers in the interval $(0,1)$ is uncountable.

Proof. Suppose, for contradiction, that the set $(0,1)$ is countable. Then all real numbers in $(0,1)$ can be listed as a sequence

$$r_1, r_2, r_3, \ldots.$$

We will derive a contradiction by constructing a real number in $(0,1)$ that is not equal to any r_n.

Write each r_n in its decimal expansion:

$$r_1 = 0.d_{11}d_{12}d_{13}\ldots, \quad r_2 = 0.d_{21}d_{22}d_{23}\ldots, \quad r_3 = 0.d_{31}d_{32}d_{33}\ldots, \quad \ldots$$

where each $d_{nk} \in \{0,1,\ldots,9\}$ is the k-th digit of r_n after the decimal point.

We may assume that none of the r_n has a decimal expansion ending in infinitely many 9's (for example, we write $0.5000\ldots$ instead of $0.4999\ldots$). This is always possible, because every real number has at least one such expansion.

Now we construct a new real number $x \in (0,1)$ by specifying its decimal digits:

$$x = 0.c_1 c_2 c_3 \ldots,$$

where, for each $n \geq 1$, we define c_n by

$$c_n = \begin{cases} 1, & \text{if } d_{nn} \neq 1, \\ 2, & \text{if } d_{nn} = 1. \end{cases}$$

In particular, $c_n \in \{1,2\}$ and $c_n \neq d_{nn}$ for every n.

We claim that x is not equal to any r_n in the list. Fix $n \geq 1$. Then r_n has decimal expansion $0.d_{n1}d_{n2}\ldots$, while x has decimal expansion $0.c_1 c_2 \ldots$. By construction we have $c_n \neq d_{nn}$, so x and r_n differ at least in the n-th digit after the decimal point. Hence $x \neq r_n$.

Since n was arbitrary, x is a real number in $(0,1)$ that does not appear in the list $r_1, r_2, r_3, \ldots$. This contradicts our assumption that the list contains all real numbers in $(0,1)$.

Therefore $(0,1)$ is not countable; that is, it is uncountable. In particular, the set of all real numbers $\mathbb{R}$ is uncountable as well. $\square$

2.6.1 :: :: problems for tutorial: explicit bijections

Problem 1. Construct an explicit bijection

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

Idea: Arrange pairs (m, n) in a table and follow diagonals.

Problem 2. Construct an explicit bijection between $\mathbb{N}$ and the set of all finite sequences of natural numbers:

$$\mathcal{F} = \bigcup_{n \geq 0} \mathbb{N}^n.$$

Hint: Use prime factorizations: encode $(a_1, \ldots, a_k)$ as $2^{a_1+1}3^{a_2+1} \cdots p_k^{a_k+1}$, where p_k is the k-th prime.

Problem 3. Construct an explicit bijection between the open interval $(0, 1)$ and the real line $\mathbb{R}$.

Hint: First find a bijection $(0, 1) \to (0, \infty)$ (e.g. using a rational function), then $(0, \infty) \to \mathbb{R}$.

Solutions are in Section 5.4

2.6.2 :: :: problems for workshop: binary strings

Problem 1 (Vertices of the cube and subsets)**.** Show that the set of vertices of the n-dimensional unit cube $\{0,1\}^n$ is in bijection with the set of all subsets of $\{1,2,\ldots,n\}$. Give the bijection explicitly in both directions.

Problem 2 (Binary strings and lattice paths in a strip)**.** Show that the set of binary strings of length n with exactly k ones is in bijection with the set of lattice paths from $(0,0)$ to $(n-k,k)$ using steps $(1,0)$ and $(0,1)$.

Problem 3 (Lattice paths and binomial coefficients)**.** Consider lattice paths on the square grid from $(0,0)$ to (m,n) that only move one step right or one step up. Construct a bijection between such paths and m-element subsets of a set of size $m+n$. Deduce that the number of such paths is $\binom{m+n}{m}$.

Problem 4. Let $n \in \mathbb{N}$ have binary expansion

$$n = \sum_{k=0}^{m} \varepsilon_k 2^k, \qquad \varepsilon_k \in \{0,1\}.$$

Thus ε_0 is the least significant bit, ε_1 is the next bit, etc.

Fix $k \geq 0$ and consider the integer

$$q_k = \left\lfloor \frac{n}{2^k} \right\rfloor.$$

Prove that the $(k+1)$-st binary digit ε_k of n is determined by the parity of q_k:

$$\varepsilon_k \equiv q_k \pmod 2.$$

In other words, the $(k+1)$-st bit of n equals 1 if and only if $\lfloor n/2^k \rfloor$ is odd, and equals 0 if and only if $\lfloor n/2^k \rfloor$ is even.

2.6.3 :: :: homework

1. Prove that the union of a finite set and a countable set is countable.

2. A sequence $(s_n)_{n=0}^{\infty}$ of natural numbers is called *eventually constant* if there exist $n_0 \in \mathbb{N}$ and $s \in \mathbb{N}$ such that $s_n = s$ for all $n \geq n_0$. Show that the set of eventually constant sequences of natural numbers is countable.

3. A sequence $(s_n)_{n=0}^{\infty}$ of natural numbers is (eventually) *periodic* if there exist $n_0, p \in \mathbb{N}$ with $p \geq 1$ such that for all $n \geq n_0$ we have $s_{n+p} = s_n$. Show that the set of all periodic sequences of natural numbers is countable.

4. A sequence $(s_n)_{n=0}^{\infty}$ of natural numbers is called an *arithmetic progression* if there exists $d \in \mathbb{N}$ such that $s_{n+1} = s_n + d$ for all $n \in \mathbb{N}$. Prove that the set of all arithmetic progressions is countable.

3 Elementary number theory, equivalence relation, and real numbers

> I am able to discuss the series "If the liver is a mirror image of the sky" with capable scholars. I can solve convoluted reciprocals and calculations that do not come out evenly. I have read cunningly written text in Sumerian, obscure Akkadian, the interpretation of which is difficult.
>
> *Aššurbanipal*, Assirian king, 685–631 BC

3.1 :: remainders, congruences

We begin with the division algorithm.

Division with remainder. For any integer m and any natural number n, there exist unique integers k and r such that

$$m = kn + r, \qquad 0 \leq r < n.$$

The number r is called the *remainder* of m upon division by n.

Lemma. The remainder upon division by n of the sum and of the product of two integers m_1, m_2 depends only on the remainders of m_1 and m_2 upon division by n.

Proof. Write

$$m_1 = k_1 n + r_1, \qquad m_2 = k_2 n + r_2,$$

with $0 \leq r_1, r_2 < n$.

Then

$$m_1 + m_2 = (k_1 + k_2)n + (r_1 + r_2).$$

Thus the remainder of $m_1 + m_2$ upon division by n is the same as the remainder of $r_1 + r_2$.

Similarly,

$$m_1 m_2 = (k_1 n + r_1)(k_2 n + r_2) = k_1 k_2 n^2 + (k_1 r_2 + k_2 r_1)n + r_1 r_2.$$

Hence the remainder of $m_1 m_2$ upon division by n is the same as the remainder of $r_1 r_2$.

This proves the lemma. □

The lemma motivates the following fundamental notion.

Definition (congruence). Let n be a natural number. Two integers a and b are called *congruent modulo* n, written

$$a \equiv b \pmod{n},$$

if a and b have the same remainder upon division by n, that is, if $a - b$ is divisible by n.

Basic properties of congruences.

For all integers a, b, c and any natural number n:

1. $a \equiv a \pmod{n}$.
2. If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.
4. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
$$a + c \equiv b + d \pmod{n}.$$
5. If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then
$$ac \equiv bd \pmod{n}.$$

Proof. The first three properties follow directly from the definition.

For addition, write $a - b = kn$ and $c - d = \ell n$. Then

$$(a + c) - (b + d) = (k + \ell)n,$$

so $a + c \equiv b + d \pmod{n}$.

For multiplication,

$$ac - bd = a(c - d) + d(a - b),$$

and both terms on the right-hand side are divisible by n, hence so is $ac - bd$. □

Theorem 10 (Existence of a modular inverse)**.** Let n be a natural number and let d be an integer such that

$$\gcd(d, n) = 1.$$

Then there exists an integer u such that

$$du \equiv 1 \pmod{n}.$$

In other words, d has a multiplicative inverse modulo n.

Proof. Since $\gcd(d, n) = 1$, by Bézout's identity there exist integers u and v such that

$$du + nv = 1.$$

Rewriting this equality gives

$$du = 1 - nv.$$

The right-hand side differs from 1 by a multiple of n. Therefore,

$$du \equiv 1 \pmod{n}.$$

This shows that the residue class of u modulo n is a multiplicative inverse of d modulo n. □

Remark 9. The integer u is not unique, but its remainder modulo n is unique. Indeed, if u_1 and u_2 both satisfy

$$du_1 \equiv du_2 \equiv 1 \pmod{n},$$

then

$$d(u_1 - u_2) \equiv 0 \pmod{n}.$$

Since $\gcd(d, n) = 1$, this implies $u_1 - u_2$ is divisible by n, so $u_1 \equiv u_2 \pmod{n}$.

Decimal representation of integers.

Any nonnegative integer m can be written in base 10 as

$$m = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \cdots + a_k \cdot 10^k,$$

where $0 \leq a_i \leq 9$ are the digits of m.

We now apply congruences to divisibility tests.

Divisibility by 3 and 9.

Since

$$10 \equiv 1 \pmod{3} \qquad \text{and} \qquad 10 \equiv 1 \pmod{9},$$

we have

$$10^k \equiv 1 \pmod{3}, \qquad 10^k \equiv 1 \pmod{9}$$

for all k.

Therefore,

$$m \equiv a_0 + a_1 + \cdots + a_k \pmod{3},$$

and similarly modulo 9.

Hence:

- m is divisible by 3 if and only if the sum of its digits is divisible by 3;
- m is divisible by 9 if and only if the sum of its digits is divisible by 9.

Divisibility by 11**.**

Since

$$10 \equiv -1 \pmod{11},$$

we have

$$10^k \equiv (-1)^k \pmod{11}.$$

Thus

$$m \equiv a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^k a_k \pmod{11}.$$

Therefore, an integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11.

Divisibility by 37**.**

Since

$$1000 = 10^3 \equiv 1 \pmod{37},$$

we may group the decimal expansion of m into blocks of three digits:

$$m = b_0 + b_1 \cdot 1000 + b_2 \cdot 1000^2 + \cdots,$$

where each b_i is an integer between 0 and 999.

Then

$$m \equiv b_0 + b_1 + b_2 + \cdots \pmod{37}.$$

Hence, an integer is divisible by 37 if and only if the sum of its three-digit blocks is divisible by 37.

Divisibility rules for powers of 2 **and** 5

We first formulate simple divisibility rules for powers of 2 and 5.

Divisibility by powers of 2**.**

Let $k \geq 1$. An integer written in decimal form

$$m = a_0 + a_1 \cdot 10 + \cdots + a_r \cdot 10^r$$

is divisible by 2^k if and only if the integer formed by its last k decimal digits is divisible by 2^k.

Proof. We write

$$m = A \cdot 10^k + B,$$

where B is the number formed by the last k digits of m.

Since $10^k = 2^k \cdot 5^k$ is divisible by 2^k, the term $A \cdot 10^k$ is divisible by 2^k. Therefore, the divisibility of m by 2^k depends only on B. □

Divisibility by powers of 5**.**

Let $k \geq 1$. An integer m is divisible by 5^k if and only if the integer formed by its last k decimal digits is divisible by 5^k.

Proof. The proof is identical to the previous one, since

$$10^k = 2^k \cdot 5^k$$

is divisible by 5^k. □

Remark. These rules explain the familiar tests:

- divisibility by 2 depends on the last digit;
- divisibility by 4 depends on the last two digits;
- divisibility by 5 depends on the last digit;
- divisibility by 25 depends on the last two digits.

Existence of a power of 10 **congruent to** 1

We now prove a fundamental fact that leads to divisibility rules for many other numbers.

Theorem. Let n be a natural number such that $\gcd(n, 10) = 1$ (that is, n is not divisible by 2 or 5). Then there exists a natural number N such that

$$10^N \equiv 1 \pmod{n}.$$

Proof. Consider the sequence of remainders obtained by dividing

$$10^1,\ 10^2,\ 10^3,\ \ldots,\ 10^n$$

by n.

There are only $n-1$ possible nonzero remainders modulo n. Since $\gcd(10, n) = 1$, none of the powers 10^k is divisible by n, so all these remainders are nonzero.

By the pigeonhole principle, two of the numbers 10^i and 10^j with $1 \le i < j \le n$ have the same remainder modulo n. Thus

$$10^i \equiv 10^j \pmod{n}.$$

Subtracting,

$$10^i(10^{j-i} - 1) \equiv 0 \pmod{n}.$$

Since $\gcd(10^i, n) = 1$, we may cancel 10^i, obtaining

$$10^{j-i} \equiv 1 \pmod{n}.$$

Setting $N = j - i$ completes the proof. □

Divisibility rules derived from $10^N \equiv 1 \pmod{n}$

Assume now that n is not divisible by 2 or 5, and let N be a natural number such that

$$10^N \equiv 1 \pmod{n}.$$

Write a nonnegative integer m in decimal form and group its digits into blocks of length N:

$$m = b_0 + b_1 \cdot 10^N + b_2 \cdot 10^{2N} + \cdots,$$

where each b_i is an integer between 0 and $10^N - 1$.

Using the congruence $10^N \equiv 1 \pmod{n}$, we obtain

$$m \equiv b_0 + b_1 + b_2 + \cdots \pmod{n}.$$

Divisibility rule. An integer m is divisible by n if and only if the sum of its blocks of N digits is divisible by n.

Examples.

- For $n = 3$ and $n = 9$, we may take $N = 1$, recovering the rule for the sum of digits.
- For $n = 11$, we may take $N = 2$, leading to a rule based on two-digit blocks.
- For $n = 37$, we may take $N = 3$, leading to a rule based on three-digit blocks.

Example 4. Check the divisibility of the number

$$M = 987\,654\,321\,012\,345$$

by 1665, and compute the remainder of M upon division by 1665.

Note that

$$5 \cdot 9 \cdot 37 = 1665.$$

We compute the remainders of M modulo 5, 9, and 37, and then combine them.

Step 1. Remainder modulo 5.
The last digit of M is 5. Hence

$$M \equiv 0 \pmod 5.$$

Step 2. Remainder modulo 9.
Write M in decimal form and compute the sum of its digits:

$$9+8+7+6+5+4+3+2+1+0+1+2+3+4+5 = 60.$$

Since

$$60 = 9 \cdot 6 + 6,$$

we obtain

$$M \equiv 6 \pmod 9.$$

Step 3. Remainder modulo 37.
Since

$$1000 = 10^3 \equiv 1 \pmod{37},$$

we group the number into blocks of three digits:

$$M = 987 \cdot 10^{12} + 654 \cdot 10^9 + 321 \cdot 10^6 + 012 \cdot 10^3 + 345.$$

Using $10^3 \equiv 1 \pmod{37}$, we obtain

$$M \equiv 987 + 654 + 321 + 12 + 345 \pmod{37}.$$

Compute the sum:

$$987+654 = 1641, \quad 1641+321 = 1962, \quad 1962+12 = 1974, \quad 1974+345 = 2319.$$

Now divide:

$$2319 = 37 \cdot 62 + 25,$$

hence

$$M \equiv 25 \pmod{37}.$$

Step 4. Summary of remainders.

We have shown that

$$M \equiv 0 \pmod{5},$$
$$M \equiv 6 \pmod{9},$$
$$M \equiv 25 \pmod{37}.$$

Step 5. Computing the remainder modulo 1665**.**

We now find the unique integer r, $0 \leq r < 1665$, such that

$$r \equiv 0 \pmod{5}, \qquad r \equiv 6 \pmod{9}, \qquad r \equiv 25 \pmod{37}.$$

From $r \equiv 0 \pmod{5}$, write $r = 5k$. Then

$$5k \equiv 6 \pmod{9}.$$

Since $5 \cdot 2 = 10 \equiv 1 \pmod{9}$, the inverse of 5 modulo 9 is 2, and hence

$$k \equiv 6 \cdot 2 = 12 \equiv 3 \pmod{9}.$$

Thus

$$k = 9t + 3, \qquad r = 45t + 15.$$

Now impose the condition modulo 37:

$$45t + 15 \equiv 25 \pmod{37}.$$

Since $45 \equiv 8 \pmod{37}$, this becomes

$$8t + 15 \equiv 25 \pmod{37},$$

$$8t \equiv 10 \pmod{37}.$$

Because $8 \cdot 14 = 112 \equiv 1 \pmod{37}$, the inverse of 8 modulo 37 is 14, and therefore

$$t \equiv 10 \cdot 14 = 140 \equiv 29 \pmod{37}.$$

Hence

$$t = 37s + 29.$$

Substituting back,

$$r = 45(37s + 29) + 15 = 1665s + 1320.$$

The smallest nonnegative solution is

$$r = 1320.$$

Final result.

$$\boxed{987\,654\,321\,012\,345 \equiv 1320 \pmod{1665}.}$$

Thus the number is not divisible by $5 \cdot 9 \cdot 37$, and its exact remainder upon division by 1665 is 1320.

Remark. This method does not merely test divisibility: it allows one to compute the exact remainder of a very large number using only its decimal expansion and elementary congruence rules.

3.1.1 :: tutorial, method of the infinite descent

Every integer t can be written in exactly one of the three forms

$$t = 3k, \qquad t = 3k+1, \qquad t = 3k+2$$

for some integer k.

Problem 1 (Squares in the three cases)**.** Let k be an integer.

1. Expand $(3k)^2$ and show it is divisible by 3.
2. Expand $(3k+1)^2$ and show it has the form $3n+1$ for some integer n.
3. Expand $(3k+2)^2$ and show it has the form $3n+1$ for some integer n.

Conclude: every square integer is either divisible by 3 or has the form $3n+1$.

Lemma 5. If m^2 is divisible by 3, then m is divisible by 3.

Problem 2. Prove that the Diophantine equation

$$x^2 + y^2 = 3z^2$$

has no integer solutions other than $x = y = z = 0$.

Solution: Assume there is a nonzero solution. Among all nonzero solutions choose one with $|z|$ minimal.

1. Show that $z \neq 0$.
2. Show that $x^2 + y^2$ is divisible by 3, hence at least one of x^2, y^2 is not of the form $3n+1$. Deduce that *both* x^2 and y^2 are divisible by 3.
3. Use the lemma to conclude 3 divides x and y.
4. Write $x = 3x_1$, $y = 3y_1$ and substitute back to show 3 divides z as well.
5. Put $z = 3z_1$ and divide the equation by 9 to obtain a new solution

   $$x_1^2 + y_1^2 = 3z_1^2$$

   with $|z_1| < |z|$. Contradiction. This is another instance of the Method of Extreme from the beginning of this course.

Lemma 6. 1. If u^2 is even then u is even.

2. If u^2 is divisible by 4 then u is even.

3. If u^4 is even then u is even.

Lemma 7 (Warm up before Primitive Pythagorean triples)**.** Prove that if $xy = z^2$, with x, y, z positive integers, and $\gcd(x, y) = 1$ then x and y are both squares

Problem 3 (Primitive Pythagorean triples)**.** Suppose a, b, c are integers with

$$a^2 + b^2 = c^2,$$

$\gcd(a, b) = 1$, and a and b are not both odd. Prove that there exist integers $m > n \geq 1$ such that

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2$$

up to swapping a and b.

(Hint: Remark that if (a, b, c) are Primitive Pythagorean triples then a, b and c have no common factors. Try to understand why. If a is even, write $a^2 = (c - b)(c + b)$. You will also need to use the warm up lemma above.)

Problem 4 (Fermat's infinite descent for fourth powers)**.** We will most probably not have time to finish this exercise during the tutorial. You are highly encourage to try it! And if you have question, ask! Assume that there exists a nonzero integer solution of

$$x^4 + y^4 = z^4.$$

Among all such solutions, choose one with $z > 0$ minimal.

1. **Primitive reduction.** Show that $\gcd(x, y) = 1$.

2. **Parity.** Prove that x and y cannot both be odd. Deduce that one of x^2, y^2 is even and the other is odd.

3. **Primitive Pythagorean triple.** Rewrite the equation as

   $$(x^2)^2 + (y^2)^2 = (z^2)^2$$

   and show that (x^2, y^2, z^2) is a primitive Pythagorean triple.

4. **Parametrization.** Using the classification of primitive Pythagorean triples, show that—after possibly exchanging x and y—there exist coprime integers $m > n \geq 1$ of opposite parity such that

$$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad z^2 = m^2 + n^2.$$

5. **Square–factor structure.** Starting from the identity $y^2 = 2mn$, and using only coprimality and parity arguments, prove that exactly one of the following two cases holds:

$$\text{(A)} \quad m = r^2,\ n = 2s^2, \qquad \text{(B)} \quad m = 2r^2,\ n = s^2,$$

for some integers $r, s \geq 1$.

6. **Explicit factorization.** In Case (A), substitute $m = r^2$ and $n = 2s^2$ into

$$x^2 = m^2 - n^2$$

and show that

$$x^2 = (r^2 - 2s^2)(r^2 + 2s^2).$$

Prove that the two factors on the right-hand side are coprime.

7. **Forced squares.** Deduce that there exist integers $u, v > 0$ such that

$$r^2 - 2s^2 = u^2, \qquad r^2 + 2s^2 = v^2.$$

8. **Definition of the descended triple.** Define

$$x' := u, \qquad y' := v, \qquad z' := r.$$

9. **Verification.** By direct computation, verify that

$$x'^4 + y'^4 = z'^4.$$

10. **Descent.** Prove that $0 < z' < z$, contradicting the minimality of z.

11. **Conclusion.** Deduce that the equation $x^4 + y^4 = z^4$ has no integer solutions with $xyz \neq 0$.

3.1.2 :: workshop

[we do not use congruences here! congruences will be introduced later!]

Example 5. Prove that the number $n^3 - n$ is divisible by 6 for all integers n.

Solution. Factor the given expression:

$$n^3 - n = (n-1)n(n+1).$$

We obtain the product of three consecutive integers. One of them is divisible by 3, hence the product is divisible by 3. At least one of the three consecutive integers is even, so the product is even. A number divisible by both 2 and 3 is divisible by 6.

Example 6. Prove that there exist infinitely many integers that cannot be represented as the sum of three squares.

Solution. The square of an integer, when divided by 8, leaves a remainder of 0, 1, or 4. To verify this, it suffices to check the squares of all possible remainders modulo 8, namely the numbers from 0 to 7. Therefore, a sum of three squares cannot have remainder 7 when divided by 8.

Example 7. Prove that a number whose decimal representation consists of three ones and several zeros cannot be a square.

Solution. If such a number existed, it would be divisible by 3 but not divisible by 9 (by the divisibility tests for 3 and 9). However, if a number is divisible by 3 and is a perfect square, then it must be divisible by 9. This contradiction shows that such a number cannot be a square.

Prove:

1. If p is a prime number greater than 3, prove that $p^2 - 1$ is divisible by 24.
2. For which integers n is the number $2^n - 1$ divisible by 7?
3. It is known that the sum of several natural numbers is divisible by 6. Prove that the sum of the cubes of these numbers is also divisible by 6.
4. Prove that if an integer arithmetic progression contains a perfect square, then it contains infinitely many perfect squares.
5. A six-digit number is divisible by 7. Prove that if its last digit is moved to the front, the resulting number is also divisible by 7.
6. Find three pairwise coprime integers such that the sum of any two of them is divisible by the third.

3.1.3 :: :: homework

Egyptian Fractions

Definition 15. A *unit fraction* (or *Egyptian fraction*) is a fraction of the form $\frac{1}{n}$, where n is a positive integer. A representation of a rational number as a sum of distinct unit fractions is called an *Egyptian decomposition*.

Example 8. Consider dividing five loaves equally among eight people. Each person should receive $\frac{5}{8}$ of a loaf. Instead of cutting every loaf into eighths, one can note that

$$\frac{5}{8} = \frac{1}{2} + \frac{1}{8},$$

so it suffices to divide four loaves in half and the fifth loaf into eight parts. This exemplifies the efficiency of Egyptian decomposition.

The ancient egyptians expressed all other fractions as sums of distinct unit fractions. This problem is nontrivial because of the requirement that all denominators be distinct.

Lemma 8. For any positive integer n, the following identity holds:

$$\frac{1}{n} = \frac{1}{n+1} + \frac{1}{n(n+1)}.$$

Proof. Multiplying both sides by $n(n+1)$ gives $n+1 = n+1$, verifying the equality. □

Repeated application of this lemma allows one to expand a unit fraction into a sum of distinct unit fractions with successively increasing denominators. For instance:

$$\frac{3}{n} = \frac{1}{n} + \frac{1}{n} + \frac{1}{n+1} + \frac{1}{n(n+1)} = \frac{1}{n} + \frac{2}{n+1} + \frac{2}{n(n+1)} = \frac{1}{n} + \frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{(n+1)(n+2)} + \frac{1}{n(n+1)} + \frac{1}{n(n+1)+1} + \frac{1}{(n(n+1)+1)n(n+1)}.$$

However, the denominators in this procedure grow rapidly, making it impractical for general use.

The Fibonacci Algorithm

Definition 16. Given a proper fraction $\frac{k}{n}$ with $k < n$, the *Fibonacci algorithm* produces an Egyptian decomposition by setting

$$\frac{k}{n} = \frac{1}{\lceil \frac{n}{k} \rceil} + \frac{k\lceil \frac{n}{k} \rceil - n}{n\lceil \frac{n}{k} \rceil},$$

where $\lceil x \rceil$ denotes the smallest integer greater than or equal to x. The procedure is then applied recursively to the remaining fraction until a complete decomposition is obtained.

Theorem 11. The Fibonacci algorithm terminates after at most k steps and yields a decomposition into distinct unit fractions.

Proof. At each step, the numerator decreases while denominators strictly increase. Since the numerator is a positive integer, the process must terminate after finitely many steps, producing distinct denominators. □

Example 9. The fraction $\frac{5}{121}$ admits a Egyptian decomposition:

$$\frac{5}{121} = \frac{1}{33} + \frac{1}{121} + \frac{1}{363},$$

which is compact, whereas the Fibonacci algorithm yields a much longer expansion:

$$\frac{5}{121} = \frac{1}{25} + \frac{1}{757} + \frac{1}{763309} + \frac{1}{873960180193} + \frac{1}{152761279564209341884622 5}.$$

The inefficiency arises from the algorithm's *greedy* nature — it always selects the largest available unit fraction $\frac{1}{\lceil n/k \rceil}$. In this case, beginning with a bigger denominator (33 rather than 25) yields a shorter decomposition.

Open Problems

In 1985, M. Vose constructed an algorithm that expresses $\frac{k}{n}$ as a sum of at most $C\sqrt{\log n}$ unit fractions (where C is a constant independent of k and n). Lower estimates are of the order $\log(\log n)$. The exact bounds remain unknown. An even more elementary open question is the following:

Erdős–Straus Conjecture. For every integer $n \geq 2$, the fraction $\frac{4}{n}$ can be written as the sum of three disctinct unit fractions

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

Although this conjecture has been computationally verified for all $n \leq 10^{14}$, no general proof has yet been found.

How to Read Mathematical Texts

A general approach may be outlined as follows (apply instructions to the above example):

1. Focus on the Definitions

The most important part of any mathematical text is its *definitions*. Locate them first. Try to understand each definition and visualize some examples in your mind: what objects satisfy it, and what do not?

If the text provides examples (as it does for the *first definition*), study them carefully. If not (as for the *second definition*), create your own examples to clarify the meaning.

Exercise 1. Examine the definition of the *Fibonacci algorithm*. Apply it to the fraction a) $\frac{5}{13}$ b) $\frac{7}{19}$ and write down the sequence of unit fractions that you obtain.

2. Examine the Theorems

The next essential elements are the *theorems*. Find the theorem in the text and try to understand its *proof*.

How can you do this effectively?

Read the *first sentence* of the proof aloud. Check that you fully understand its meaning. Then try to question it — imagine disagreeing with the statement, and see if you can find a counterexample. Afterward, check how this sentence relates to the example you have already studied.

Continue with the *second sentence* in the same way: read, question, and test it against your example.

Finally, return to the statement of the theorem. Ask yourself: have we really proven what the theorem claims?

In our case the answer is **NO**. This often happens: mathematical proofs in textbooks or articles may be written concisely, leaving some

steps implicit. Treat the written proof as a *hint* or a guide, and try to reconstruct the argument on your own. Doing so will help you understand the logical structure of the reasoning.

Exercise 2. Write a full proof of Theorem 11 (i.e. prove that the process will terminate after at most k steps).

3. Read It Again

Once you have carefully examined the definitions, examples, and theorems, reread the entire text. You will likely find that what initially seemed complicated now appears as a connected and coherent narrative.

Reading mathematics is a skill developed through patience and active engagement. Always ask yourself: what is being defined, what is being claimed, and why is it true?

4. Look at the open problems.

Explore the open problems—they might have simple solutions that no one has noticed yet. Trying to solve them can be both fascinating and a lot of fun.

Exercise 3. For $n = 4, 5, 6, 7$ find the Egyptian decomposition

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}.$$

3.2 :: equivalence relations, partitions

Example 10. We call two integer numbers x, y equivalent if $x - y$ is divisible by 3. We denote this $x \sim y$. Note that if $x \sim y$ and $y \sim z$, then $x \sim z$. Also $x \sim x$. If $x \sim y$, then $y \sim x$. Then, all the integer numbers are divided in three groups: with remainder 0, remainder 1, and remainder 2, when we divide by 3. Similar things are called equivalence relations.

Binary relations. Let X be a set. A *binary relation* R on X is a subset

$$R \subseteq X \times X.$$

If $(x, y) \in R$, we write $x\,R\,y$.

Basic properties of relations. A relation R on X may have the following properties:

- *Reflexive*: for all $x \in X$, $x\,R\,x$ ($\forall x \in X$, $(x, x) \in R$)
- *Symmetric*: for all $x, y \in X$, if $x\,R\,y$ then $y\,R\,x$ (if $(x, y) \in R$, then $(y, x) \in R$).
- *Transitive*: for all $x, y, z \in X$, if $x\,R\,y$ and $y\,R\,z$, then $x\,R\,z$ (if $(x, y) \in R, (y, z) \in R$, then $(x, z) \in R$).
- *Antisymmetric*: for all $x, y \in X$, if $x\,R\,y$ and $y\,R\,x$, then $x = y$.

Definition. An *equivalence relation* on a set X is a reflexive, symmetric, and transitive binary relation R.

We shall denote equivalence as follows:

$$xRy \iff x \sim y$$

(read "x is equivalent to y"), but other symbols are often used as well: $\cong$, $\equiv$, and so on (the names of equivalence relations that will appear later, and the meanings of these symbols, will be clear from the context).

By definition:

1. $x \sim x$ (reflexivity);

2. $x \sim y \implies y \sim x$ (symmetry);

3. $x \sim y$ and $y \sim z \implies x \sim z$ (transitivity).

For each element $x \in X$, let $\bar{x}$ (or $[x]$) denote the corresponding *equivalence class*, defined as the set of all $y \in X$ equivalent to x:

$$\bar{x} = [x] = \{\, y \in X \mid y \sim x \,\}.$$

The element x itself is then called a *representative* of the class $\bar{x}$. Thus, by definition, if $\bar{x} = \bar{y} \iff x \sim y$, then $\bar{x}$ is uniquely determined by any of its representatives.

The conditions (a)–(c) can now be reformulated as:

1. $x \in \bar{x}$;

2. $y \in \bar{x} \iff x \in \bar{y}$;

3. $y \in \bar{x}$ and $z \in \bar{y} \implies z \in \bar{x}$.

On any set, there are two obvious equivalence relations:

- the *identity relation*, when $x \sim y \iff x = y$;
- the *universal relation*, when $x \sim y$ for all x, y.

Lemma 9 (Equivalence classes do not intersect or coincide)**.** Let R be an equivalence relation on a set X, and let $x, y \in X$. Then either

$$[x] = [y] \qquad \text{or} \qquad [x] \cap [y] = \varnothing.$$

Proof. Assume that $[x] \cap [y] \neq \varnothing$. Then there exists an element $z \in X$ such that

$$z \in [x] \quad \text{and} \quad z \in [y].$$

By definition of equivalence classes, this means

$$x\,R\,z \quad \text{and} \quad y\,R\,z.$$

Since R is symmetric, from $y\,R\,z$ we obtain $z\,R\,y$. By transitivity of R, from $x\,R\,z$ and $z\,R\,y$ we conclude

$$x\,R\,y.$$

Now let $u \in [x]$. Then $x\,R\,u$, and together with $x\,R\,y$ and symmetry we obtain

$$y\,R\,u,$$

so $u \in [y]$. Hence $[x] \subseteq [y]$. By symmetry of the argument, also $[y] \subseteq [x]$, and therefore $[x] = [y]$.

Thus, if two equivalence classes intersect, they must coincide. □

Example 11. We call two integer numbers x, y equivalent if $x - y$ is divisible by 3. We denote this by $x \sim y$.

Note that:

- $x \sim x$ for every integer x;
- if $x \sim y$, then $y \sim x$;
- if $x \sim y$ and $y \sim z$, then $x \sim z$.

Thus $\sim$ is an equivalence relation.

All integers are divided into three groups (equivalence classes):

$$\overline{0} = \{x | x \equiv 0 \pmod 3\}, \overline{1} = \{x | x \equiv 1 \pmod 3\}, \overline{2} = \{x | x \equiv 2 \pmod 3\}$$

These are the integers with remainder 0, 1, and 2 upon division by 3.

Arithmetic with equivalence classes.

We now observe that we can perform arithmetic operations directly with these equivalence classes.

For example:

- if $x \in \overline{2}$ and $y \in \overline{2}$, then $x+y \in \overline{1}$, since $2+2=4$ leaves remainder 1;
- if $x \in \overline{2}$ and $y \in \overline{1}$, then $x+y \in \overline{0}$;
- if $x \in \overline{2}$ and $y \in \overline{2}$, then $xy \in \overline{1}$, since $2 \cdot 2 = 4$ leaves remainder 1.

Thus we may write informally:

$$\overline{2}+\overline{2}=\overline{1}, \qquad \overline{2}+\overline{1}=\overline{0}, \qquad \overline{2}\cdot\overline{2}=\overline{1}.$$

Addition table modulo 3**.**

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Multiplication table modulo 3**.**

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Why we need equivalence relations.

In order for such tables to make sense, we must ensure that the result does *not depend on the chosen representatives*. For example, if $x \sim x'$ and $y \sim y'$, then we must have

$$x+y \sim x'+y', \qquad xy \sim x'y'.$$

This requirement is precisely guaranteed by working with *equivalence relations* and their associated *partitions into equivalence classes*.

Conclusion.

The set of equivalence classes

$$\mathbb{Z}/3\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}\}$$

together with the operations defined above forms a new mathematical object, obtained from the integers by identifying numbers that differ by a multiple of 3.

This construction will appear repeatedly in what follows.

Let us recall several other examples of equivalence relations that we shall encounter later:

- **Equivalence (isomorphism) of sets.** Consider some set X of sets, for example 2^Z for a fixed set Z. Then we set $A \sim B \iff |A| = |B|$, i.e., there exists a bijection between A and B.
- **Equality up to sign.** Let $X = \mathbb{Z}$, and define $m \sim n \iff m \mid n$ and $n \mid m$.
- **Congruence modulo** m**.** Let $X = \mathbb{Z}$ and m a fixed positive integer. We set $x \sim y \iff x \equiv y \pmod{m}$ (recall, this means that $x - y$ is divisible by m).

Many examples of equivalence relations appeared in elementary geometry. In addition to the already mentioned congruence, similarity, parallelism, etc., we can also give the following examples.

• **Equality of lengths.** Let X be the set of vectors in the plane or in three-dimensional space. We say that $x \sim y$ if the lengths of the vectors x and y coincide.

• **Equality of areas.** Let X be the "set of figures" on the plane. We shall say that two figures A and B are equivalent if they have the same area (or if the area is undefined for both).

Partitions

On the ancient pages of the Chinese encyclopedia "Heavenly Empire of Benevolent Knowledge" it is written that animals are divided into: a) belonging to the emperor, b) embalmed, c) tame, d) suckling pigs, e) sirens, f) fabulous, g) stray dogs, h) included in this classification, i) frenzied, j) innumerable, k) drawn with the finest brush of camel hair, l) others, m) that have just broken a flower vase, n) that resemble flies from afar. (*Jorge Luis Borges,* "The Analytical Language of John Wilkins".)

A *partition* of a set X is a representation of X as a disjoint union of some family of subsets:

$$X = \bigsqcup_{i \in I} X_i \quad (\text{i.e. } X_i \cap X_j = \varnothing \text{ for } i \neq j).$$

The notion of partition coincides essentially with that of an equivalence relation. Namely, to each partition one can associate an equivalence relation, for which $x \sim y$ if and only if $x, y \in X_i$ for some i. Conversely, every equivalence relation on X defines a partition of X into disjoint equivalence classes.

To choose one representative from each class X_i, let $\{x_i \mid i \in I\}$ be a *system of representatives* (*Vertretersystem, Repräsentantensystem*) of the equivalence relation $\sim$ (or a *transversal* to it).

Proposition. The set of equivalence classes forms a partition of X. In other words, X can be represented as a disjoint union

$$X = \bigsqcup_{i \in I} X_i, \quad i \in I,$$

of distinct classes.

Proof. First note that $X = \bigcup_i X_i$. Indeed, since we chose one x_i in each class, for any $x \in X$ there exists i such that $x \sim x_i$, and therefore $x \in X_i$. It remains to show that different classes do not intersect.

Indeed, if $x \in X_i$ and $x \in X_j$ for $i \neq j$, then $x \sim x_i$ and $x \sim x_j$, whence $x_i \sim x_j$, a contradiction. Thus the classes are disjoint, and the claim follows.

Definition. Let X be a set and let $\sim$ be an equivalence relation on X. The set

$$X/\sim = \{\, \bar{x} \mid x \in X \,\}$$

of all equivalence classes is called the *quotient set* of X by the equivalence relation $\sim$.

The map

$$\pi\colon X \longrightarrow X/\sim, \qquad x \longmapsto \bar{x},$$

is called the *canonical projection* (or *quotient map*).

By definition, the map π sends each element of X to the equivalence class to which it belongs.

Example 12 (Congruence modulo n)**.** Let $n \geq 1$ be a fixed integer. On the set $\mathbb{Z}$ we define an equivalence relation by

$$x \sim y \quad \Longleftrightarrow \quad x - y \text{ is divisible by } n.$$

This relation is called *congruence modulo n*.

The equivalence class of an integer k consists of all integers having the same remainder as k upon division by n:

$$\bar{k} = \{\, m \in \mathbb{Z} : m \equiv k \pmod{n} \,\}.$$

Every integer k can be written uniquely in the form

$$k = qn + r, \qquad 0 \leq r < n,$$

and therefore

$$\bar{k} = \bar{r}.$$

Thus there are exactly n distinct equivalence classes, namely

$$\bar{0}, \bar{1}, \ldots, \overline{n-1}.$$

The quotient set

$$\mathbb{Z}/n\mathbb{Z}$$

(or simply $\mathbb{Z}_n$) is the set of these equivalence classes.

The canonical projection

$$\pi\colon \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \qquad k \longmapsto \bar{k},$$

sends each integer to its remainder class modulo n.

:: tutorial: equivalence relations

Equivalence relation generated by a function.

Let A be a set and let $f\colon A \to A$ be a function. Consider its graph

$$\Gamma_f = \{(x, f(x)) : x \in A\} \subseteq A \times A.$$

We consider the *smallest equivalence relation on A that contains Γ_f*. That is, the intersection of all equivalence relations on A that contain Γ_f.

Description in simple words. Consider this equivalence relation $\sim$. From the definition we know that for each $x \in A$, we have $x \sim f(x)$. Two elements $x, y \in A$ are equivalent if and only if one can be obtained from the other by repeatedly applying the function f or its inverse relation, that is, if there exist nonnegative integers k, ℓ such that

$$f^k(x) = f^\ell(y).$$

Equivalence classes.

The equivalence class $[x]$ of an element $x \in A$ consists of all elements y whose forward orbits under f (i.e. $y, f(y), f^2(y), \ldots, f^k(y), \ldots$) eventually meet the forward orbit of x. In other words, two elements are equivalent if their iterates under f eventually coincide.

Example: remainders modulo n.

Let $f_n\colon \mathbb{Z} \to \mathbb{Z}$ be the function

$$f_n(x) = \text{the remainder of } x \text{ upon division by } n.$$

Then:

- For every integer x, the sequence $x, f_n(x), f_n(f_n(x)), \ldots$ stabilizes at a number between 0 and $n-1$ after the first step.
- Two integers x, y have the same eventual image under iteration of f_n if and only if they have the same remainder modulo n.

Therefore, the equivalence relation generated by Γ_{f_n} is exactly *congruence modulo n*, and the equivalence classes are the residue classes

$$\bar{r} = \{\, k \in \mathbb{Z} : k \equiv r \pmod{n} \,\}, \qquad r = 0, 1, \ldots, n-1.$$

Problem. Is the intersection of equivalence relations an equivalence relation? Is the union of equivalence relations an equivalence relation?

Solution.

Let $\{R_i\}_{i \in I}$ be a family of equivalence relations on a set X.

Intersection. Define

$$R = \bigcap_{i \in I} R_i.$$

Then:

- R is reflexive, since each R_i is reflexive;
- R is symmetric, since each R_i is symmetric;
- R is transitive, since each R_i is transitive.

Hence the intersection of equivalence relations is again an equivalence relation.

Union. Define

$$R = \bigcup_{i \in I} R_i.$$

In general, R is *not* transitive. Indeed, it may happen that

$$x \, R_1 \, y \quad \text{and} \quad y \, R_2 \, z,$$

but there is no index i such that both relations belong to the same R_i, so $x \, R \, z$ need not hold.

Therefore, the union of equivalence relations is *not* necessarily an equivalence relation. $\square$

:: workshop: Fundamental Theorem of Arithmetic as a problem sequence

Throughout this workshop, $\mathbb{N} = \{1, 2, 3, \dots\}$. We say that an integer $p > 1$ is *prime* (or *irreducible*) if its only positive divisors are 1 and p.

We will use the *minimal counterexample* principle several times: assume a statement (S) is false and choose a counterexample with the smallest possible value of some natural number parameter; then derive a strictly smaller counterexample. It contradicts to the choice of the initial counterexample, and this contradiction implies that the statement (S) is true.

Problem 1 (Division algorithm)**.** Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. Prove that there exist unique integers q, r such that

$$a = bq + r, \qquad 0 \leq r < b.$$

You need to prove a) existence, b) uniqueness.

Problem 2. Prove that every integer $n \geq 2$ can be written as a product of primes.

Hint (minimal counterexample in n). Assume not, and let $n \geq 2$ be the smallest integer that is not a product of primes. Show that n cannot be prime, so $n = ab$ with $1 < a < n$ and $1 < b < n$. Apply minimality to a and b and multiply their factorizations.

We want to prove the following theorem.

Theorem 12 (Fundamental Theorem of Arithmetic)**.** Every integer $n \geq 2$ can be written as a product of primes, and this factorization is unique up to the order of the factors.

We have already proven the existence of a factorization. Show that it is enough to prove the following:

Problem 3 (A prime dividing a product of primes)**.** Let p be a prime and suppose

$$p \mid q_1 q_2 \cdots q_k$$

where each q_i is prime. Prove that $p = q_i$ for some i.

(Hint: choose minimal n with two different factorizations $n = q_1 q_2 \cdots q_k = p_1 p_2 \cdots p_l$ (the minimal countexample), then apply the above problem to $p = p_1$ to obtain a smaller counterexample).

Now reduce the above problem to the following one.

Problem 4 (Cancellation from prime divisibility)**.** Let p be a prime and suppose $p \mid AB$ and $p \nmid A$. Prove that $p \mid B$.

(Hint: we can use this problem repeatedly: first apply it to $p \mid q_1(q_2 \cdots q_k)$, then continue...)

Thus we reduced the fundamental theorem of arithmetic to the following problem: (Euclid's lemma) Let p be a prime. We want to prove that for all integers A, B,

$$p \mid AB \quad \Longrightarrow \quad p \mid A \ \text{ or } \ p \mid B.$$

We will present here so called descent form proof of this statement.

Assume the statement is false for some prime p. Choose a counterexample with *minimal* prime p, and among those choose one with *minimal* product $AB > 0$ such that

$$p \mid AB, \qquad p \nmid A, \qquad p \nmid B.$$

Write $AB = pq$.

Problem 5. Show that one may assume $0 < A, B < p$. (Hint: if $A > p$, write $A = pk + r$ with $0 \le r < p$ and use that $p(q - kB) = rB$ which contradicts minimality.)

Problem 6. Assume now that $0 < A \le B < p$ and $AB = pq$. Prove that

$$1 \le q < p.$$

Hint. From $AB = pq$ and $A, B < p$, compare pq with p^2.

Problem 7. Assume $0 < A \leq B < p$ and $AB = pq$. Show that $q \neq 1$.

Problem 8 (A prime divisor of q yields a smaller counterexample)**.** Assume $q > 1$ and let q' be a prime divisor of q. Prove that q' does *not* divide A and does *not* divide B.

Hint. If $q' \mid A$ (or $q' \mid B$), divide the equality $AB = pq$ by q' and explain why this produces a counterexample with a smaller value of AB, contradicting the minimal choice of AB.

Problem 9 (Constructing a smaller prime counterexample)**.** Let q' be a prime divisor of q. Show that

$$q' \mid AB, \qquad q' \nmid A, \qquad q' \nmid B,$$

so (q', A, B) is a counterexample to Euclid's Lemma. *Hint.* Since $q' \mid q$ and $AB = pq$, we have $q' \mid AB$ and $q' < p$. This contradicts the minimality of p.

Remark (prime factorization may fail in other rings). The Fundamental Theorem of Arithmetic is special to the ring of integers $\mathbb{Z}$: in many other rings, a factorization into irreducible elements need not be unique. For example, in the ring

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\},$$

one can add, multiply elements and also give a definition of irreducible elements (coincides with the definition of prime elements that we have given above), but one has the identity

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}),$$

and each of the four factors $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ is irreducible in $\mathbb{Z}[\sqrt{-5}]$!

Moreover, they do not differ by multiplication by a unit (here the only units are ± 1), so these give genuinely different decompositions of the

same element. Thus, outside $\mathbb{Z}$ one must be careful: factorization into irreducibles may fail to be unique, and one should not expect the same proof strategy as in $\mathbb{Z}$.

One reason is that in $\mathbb{Z}[\sqrt{-5}]$ there is *no* division algorithm of the Euclidean type (no analogue of $a = bq + r$ with a remainder that is guaranteed to be "smaller" than b with respect to a Euclidean norm $|r| < |b|$). For instance, consider the usual norm

$$N(a + b\sqrt{-5}) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2.$$

Try to "divide" $1 + \sqrt{-5}$ by 2:

$$1 + \sqrt{-5} = 2 \cdot 0 + (1 + \sqrt{-5}) \qquad \text{and} \qquad 1 + \sqrt{-5} = 2 \cdot 1 + (-1 + \sqrt{-5}).$$

Both remainders have the same norm

$$N(1 + \sqrt{-5}) = 1^2 + 5 \cdot 1^2 = 6, \qquad N(-1 + \sqrt{-5}) = (-1)^2 + 5 \cdot 1^2 = 6,$$

while

$$N(2) = 4.$$

So neither remainder is "better" (smaller) than the other, and in fact *no* choice of $q \in \mathbb{Z}[\sqrt{-5}]$ makes the remainder $r = (1 + \sqrt{-5}) - 2q$ satisfy $N(r) < N(2)$. This illustrates that the familiar Euclidean-division mechanism behind many arguments in $\mathbb{Z}$ is not available in $\mathbb{Z}[\sqrt{-5}]$.

:: homework

1. A bus ticket with a six digit number is called *lucky* if the sum of its digits is divisible by 7. Can two consecutive tickets both be lucky?
2. Write the addition and multiplication tables for $\mathbb{Z}/n\mathbb{Z}$ for $n = 4, 5, 6, 7$.

3. Congruence modulo $\mathbb{Z}$. Let now $X = \mathbb{R}$. We shall say that two real numbers are congruent modulo $\mathbb{Z}$, and write $x \equiv y \pmod{\mathbb{Z}}$, if their fractional parts coincide. Recall that the fractional part $\{x\} \in [0, 1)$ of a real number $x \in \mathbb{R}$ is the difference $x - \mathrm{Ent}(x)$, where $\mathrm{Ent}(x)$ the largest integer n such that $n \leq x$. By definition, $x = \mathrm{Ent}(x) + \{x\}$. Thus,

$$x \equiv y \pmod{\mathbb{Z}} \iff \{x\} = \{y\}.$$

Show that this is an equivalence relation.

4. Consider two partitions $A = \bigsqcup_{i\in I} X_i = \bigsqcup_{j\in J} Y_j$ of the same set A. Show that the family of all *nonempty* pairwise intersections also forms a partition of A, namely

$$A = \bigsqcup_{k\in K} Z_k, \qquad K := \{(i,j) \in I \times J : \, X_i \cap Y_j \neq \varnothing\}, \qquad Z_{(i,j)} := X_i \cap Y_j.$$

This partition $\{Z_k\}_{k\in K}$ is called the *common refinement* of the partitions $A = \bigsqcup_{i\in I} X_i$ and $A = \bigsqcup_{j\in J} Y_j$.

5. Consider the partition $\mathbb{Z} = \bigsqcup_{i\in I} X_i$ induced by the equivalence relation $\pmod 2$. What are the sets X_i?

Consider the partition $\mathbb{Z} = \bigsqcup_{j\in J} Y_j$ induced by the equivalence relation $\pmod 3$. What are the sets Y_j?

Find the common refinement of these two partitions. To which equivalence relation does it correspond?

3.3 :: construction of natural, rational, real numbers

Axioms for the natural numbers

In mathematics, the natural numbers are not introduced as "obvious objects": they are characterized by axioms. The standard axiomatization is due to Peano.

Definition 17 (Peano axioms)**.** A *system of natural numbers* consists of a set $\mathbb{N}$, a distinguished element $0 \in \mathbb{N}$, and a map

$$S : \mathbb{N} \to \mathbb{N} \qquad \text{(the successor map)},$$

satisfying the following axioms:

(P1) 0 is not the successor of any natural number: for all $n \in \mathbb{N}$, $S(n) \neq 0$.

(P2) S is injective: if $S(m) = S(n)$, then $m = n$.

(P3) (*Induction axiom*) If $A \subseteq \mathbb{N}$ satisfies

$$0 \in A \quad \text{and} \quad (n \in A \Rightarrow S(n) \in A),$$

then $A = \mathbb{N}$.

Remark 10. Many texts use 1 instead of 0; this is only a change of notation. We will use 0 because it simplifies the definition of addition and multiplication.

Theorem 13 (Principle of induction)**.** Let $P(n)$ be a statement depending on $n \in \mathbb{N}$. Assume:

- $P(0)$ is true;
- for every $n \in \mathbb{N}$, $P(n) \Rightarrow P(S(n))$.

Then $P(n)$ is true for all $n \in \mathbb{N}$.

Proof. Let $A = \{n \in \mathbb{N} : P(n) \text{ is true}\}$. By assumption, $0 \in A$ and $n \in A \Rightarrow S(n) \in A$. By the induction axiom (P3), $A = \mathbb{N}$. □

Defining addition and multiplication on $\mathbb{N}$

Using induction, we can define operations recursively.

Definition 18 (Addition on $\mathbb{N}$)**.** Define addition $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by recursion on the second variable:

$$m + 0 := m, \qquad m + S(n) := S(m + n).$$

Definition 19 (Multiplication on $\mathbb{N}$)**.** Define multiplication $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by recursion on the second variable:

$$m \cdot 0 := 0, \qquad m \cdot S(n) := m \cdot n + m.$$

Remark 11. From these definitions one proves the familiar laws (associativity, commutativity of $+$ and $\cdot$, distributivity, etc.) by induction. We omit these proofs here, but they are an excellent exercise.

From natural numbers to integers

The natural numbers do not allow subtraction in general (e.g. $2 - 5$ is not in $\mathbb{N}$). To obtain a number system where subtraction is always possible, we construct the integers.

Definition 20 (Integers as equivalence classes)**.** Consider the set $\mathbb{N} \times \mathbb{N}$ of pairs (a, b). Define a relation $\sim$ on $\mathbb{N} \times \mathbb{N}$ by

$$(a, b) \sim (c, d) \quad \iff \quad a + d = b + c.$$

The set of integers is by definition the quotient (i.e. the set of equivalelnce classes)

$$\mathbb{Z} := (\mathbb{N} \times \mathbb{N}) / \sim .$$

We denote the class of (a, b) by $[(a, b)]$.

Remark 12. The class $[(a, b)]$ is intended to represent the formal difference $a - b$. For example, $[(5, 2)]$ corresponds to $+3$, and $[(2, 5)]$ corresponds to -3.

Definition 21 (Addition and multiplication in $\mathbb{Z}$)**.** Define

$$[(a,b)] + [(c,d)] := [(a+c,\ b+d)],$$

$$[(a,b)] \cdot [(c,d)] := [(ac+bd,\ ad+bc)].$$

Problem 1. Check that these operations are *well-defined*: if $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$, then the results of the above formulas define the same equivalence class.

Remark 13. The natural numbers embed into the integers via

$$\iota_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}, \qquad n \mapsto [(n,0)].$$

Under this embedding, the class $[(a,b)]$ behaves as $a-b$.

Construction of the rational numbers

The integers do not allow division in general (e.g. $1/2$ is not in $\mathbb{Z}$). To obtain a number system where division by a nonzero number is always possible, we construct the rational numbers.

Definition 22 (Rationals as equivalence classes of fractions)**.** Consider the set

$$\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$$

of pairs (a,b) with $b \neq 0$. Define a relation $\approx$ by

$$(a,b) \approx (c,d) \quad \iff \quad ad = bc.$$

The set of rational numbers is the quotient

$$\mathbb{Q} := \big(\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})\big) / \approx .$$

We denote the class of (a,b) by $\dfrac{a}{b}$.

Remark 14. The condition $ad = bc$ expresses the familiar equality of fractions:

$$\frac{a}{b} = \frac{c}{d} \quad \Longleftrightarrow \quad ad = bc.$$

For example, $(1, 2) \approx (2, 4)$ because $1 \cdot 4 = 2 \cdot 2$.

Definition 23 (Addition and multiplication in $\mathbb{Q}$)**.** Define

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd},$$

and

$$-\frac{a}{b} := \frac{-a}{b}.$$

Problem 2. Check that these operations are *well-defined*: if $(a, b) \approx (a', b')$ and $(c, d) \approx (c', d')$, then

$$\frac{ad + bc}{bd} \approx \frac{a'd' + b'c'}{b'd'} \quad \text{and} \quad \frac{ac}{bd} \approx \frac{a'c'}{b'd'}.$$

Definition 24 (Division in $\mathbb{Q}$)**.** If $\frac{c}{d} \neq 0$ (equivalently $c \neq 0$), define

$$\frac{a}{b} \Big/ \frac{c}{d} := \frac{a}{b} \cdot \frac{d}{c} = \frac{ad}{bc}.$$

Remark 15. The integers embed into the rationals via

$$\iota_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Q}, \qquad a \mapsto \frac{a}{1}.$$

Under this embedding, $\mathbb{Z}$ becomes a subset of $\mathbb{Q}$.

What we gain from the construction

- $\mathbb{N}$ is the basic structure governed by the Peano axioms.
- $\mathbb{Z}$ is obtained from $\mathbb{N}$ by formally allowing subtraction.

- $\mathbb{Q}$ is obtained from $\mathbb{Z}$ by formally allowing division by nonzero numbers.

These constructions are canonical: although one may build $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ in different ways, the resulting structures are the same up to a unique isomorphism.

The rational numbers $\mathbb{Q}$ are already rich, but they are not complete: there exist Cauchy sequences of rational numbers that do not converge to a rational limit (for example, rational approximations to $\sqrt{2}$). To obtain a complete number system, we construct the real numbers $\mathbb{R}$ from $\mathbb{Q}$.

Cauchy sequences in $\mathbb{Q}$

Definition 25 (Cauchy sequence)**.** A sequence $(a_n)_{n\geq 1}$ of rational numbers is called *Cauchy* if for every $\varepsilon \in \mathbb{Q}$ with $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $m, n \geq N$,

$$|a_n - a_m| < \varepsilon.$$

Remark 16. The absolute value $|x|$ for $x \in \mathbb{Q}$ is defined by

$$|x| = \begin{cases} x, & x \geq 0, \\ -x, & x < 0. \end{cases}$$

All inequalities above are inequalities of rational numbers.

Definition 26 (Null sequence)**.** A sequence $(a_n)_{n\geq 1}$ in $\mathbb{Q}$ is called a *null sequence* if for every $\varepsilon \in \mathbb{Q}$ with $\varepsilon > 0$ there exists $N \in \mathbb{N}$ such that for all $n \geq N$,

$$|a_n| < \varepsilon.$$

An equivalence relation on Cauchy sequences

Let $\mathcal{C}$ denote the set of all Cauchy sequences of rational numbers. This is a subset of $\mathbb{Q}^{\mathbb{N}}$.

Definition 27 (Equivalence of Cauchy sequences)**.** For two Cauchy sequences (a_n) and (b_n) in $\mathcal{C}$ we write

$$(a_n) \sim (b_n)$$

if the sequence of differences $(a_n - b_n)$ is a null sequence, i.e. if for every $\varepsilon \in \mathbb{Q}$ with $\varepsilon > 0$ there exists N such that for all $n \geq N$,

$$|a_n - b_n| < \varepsilon.$$

Problem 3. Prove that $\sim$ is an equivalence relation on $\mathcal{C}$: it is reflexive, symmetric, and transitive.

Definition of $\mathbb{R}$

Definition 28 (Real numbers)**.** The set of *real numbers* is the quotient set

$$\mathbb{R} := \mathcal{C} / \sim .$$

An element of $\mathbb{R}$ is an equivalence class of Cauchy sequences. If (a_n) is a Cauchy sequence, we denote its equivalence class by

$$[(a_n)] \in \mathbb{R}.$$

Remark 17. Two Cauchy sequences represent the same real number if and only if their difference tends to 0. Thus, each real number can be thought of as a "limit" of rational numbers, without assuming limits exist inside $\mathbb{Q}$.

Arithmetic operations on $\mathbb{R}$

We now define addition and multiplication by applying the operations termwise.

Definition 29 (Addition and multiplication)**.** Let $x = [(a_n)]$ and $y = [(b_n)]$ be real numbers. Define

$$x + y := [(a_n + b_n)], \qquad x \cdot y := [(a_n b_n)].$$

Define also

$$-x := [(-a_n)].$$

Problem 4 (Well-definedness)**.** Prove that these definitions do not depend on the choice of representatives: if $(a_n) \sim (a'_n)$ and $(b_n) \sim (b'_n)$, then

$$(a_n + b_n) \sim (a'_n + b'_n) \quad \text{and} \quad (a_n b_n) \sim (a'_n b'_n).$$

Order and absolute value

To compare real numbers we define an order relation in terms of sequences.

Definition 30 (Nonnegative real numbers)**.** A real number $x = [(a_n)]$ is called *nonnegative*, written $x \geq 0$, if there exists a Cauchy sequence (a_n) representing x such that $a_n \geq 0$ for all sufficiently large n (i.e. for all $n \geq N$ for some N).

Problem 5. Prove that the definition above is independent of the chosen representative of x.

Definition 31 (Order on $\mathbb{R}$)**.** For real numbers $x, y \in \mathbb{R}$, define

$$x \leq y \quad \iff \quad y - x \geq 0.$$

Definition 32 (Absolute value)**.** For $x \in \mathbb{R}$ define

$$|x| := \begin{cases} x, & x \geq 0, \\ -x, & x < 0. \end{cases}$$

Embedding of $\mathbb{Q}$ into $\mathbb{R}$

Definition 33 (Constant sequences)**.** For $q \in \mathbb{Q}$, consider the constant sequence $(q, q, q, \dots)$, which is Cauchy. Define

$$\iota_{\mathbb{Q}} : \mathbb{Q} \to \mathbb{R}, \qquad q \longmapsto [(q, q, q, \dots)].$$

Problem 6. Prove that $\iota_{\mathbb{Q}}$ is injective and preserves addition and multiplication:

$$\iota_{\mathbb{Q}}(q_1 + q_2) = \iota_{\mathbb{Q}}(q_1) + \iota_{\mathbb{Q}}(q_2), \qquad \iota_{\mathbb{Q}}(q_1 q_2) = \iota_{\mathbb{Q}}(q_1)\, \iota_{\mathbb{Q}}(q_2).$$

Completeness

The main advantage of $\mathbb{R}$ is that it is complete.

Theorem 14 (Completeness (Cauchy completeness))**.** Every Cauchy sequence of real numbers converges to a real number.

Remark 18. In this construction, a real number *is* an equivalence class of Cauchy sequences of rationals, so completeness is built into the definition: limits of Cauchy sequences exist by construction. A full proof requires checking that a Cauchy sequence of classes admits a representative Cauchy sequence in $\mathbb{Q}$ and that its class is the limit.

From Cauchy-sequence reals to decimal expansions

Recall that in our construction a real number is an equivalence class

$$x = [(a_n)]$$

of Cauchy sequences of rationals, where two Cauchy sequences represent the same real number if their difference is a null sequence.

Our goal is to define a map

$$\mathrm{Dec} : \mathbb{R} \longrightarrow \{\text{decimal expansions without an eventual tail of } 9\}$$

sending each real number to its (chosen) decimal representation.

A stability lemma

Lemma 10 (A Cauchy sequence cannot cross a point forever without converging to it)**.** Let (a_n) be a Cauchy sequence of rational numbers. Assume that there are infinitely many indices n with $a_n > 1$ and infinitely many indices m with $a_m < 1$. Then (a_n) represents the real number 1, i.e. the sequence $(a_n - 1)$ is a null sequence.

Proof. Fix any rational $\varepsilon > 0$. Since (a_n) is Cauchy, there exists N such that for all $n, m \geq N$,

$$|a_n - a_m| < \varepsilon.$$

By assumption, we can choose $n \geq N$ with $a_n > 1$ and $m \geq N$ with $a_m < 1$.

From $|a_n - a_m| < \varepsilon$ we get

$$a_n < a_m + \varepsilon < 1 + \varepsilon,$$

so $a_n < 1 + \varepsilon$. Similarly,

$$a_m > a_n - \varepsilon > 1 - \varepsilon.$$

Now take any $k \geq N$. Using $|a_k - a_n| < \varepsilon$ and $|a_k - a_m| < \varepsilon$ we obtain the two inequalities

$$a_k > a_n - \varepsilon > 1 - \varepsilon, \qquad a_k < a_m + \varepsilon < 1 + \varepsilon.$$

Hence for all $k \geq N$,

$$|a_k - 1| < \varepsilon.$$

This is exactly the definition that $(a_n - 1)$ is a null sequence. □

Step 1: the integer part

Lemma 11 (Integer part stabilizes)**.** Let (a_n) be a Cauchy sequence in $\mathbb{Q}$. Then there exists a unique integer $k \in \mathbb{Z}$ such that for all sufficiently large n,

$$k \leq a_n < k + 1.$$

Proof. Since (a_n) is Cauchy, there exists N such that for all $n, m \geq N$,

$$|a_n - a_m| < \frac{1}{2}.$$

Fix one index $n_0 \geq N$ and let k be the unique integer with

$$k \leq a_{n_0} < k + 1.$$

For any $n \geq N$ we have $|a_n - a_{n_0}| < \frac{1}{2}$, hence

$$a_n > a_{n_0} - \frac{1}{2} \geq k - \frac{1}{2} \qquad \text{and} \qquad a_n < a_{n_0} + \frac{1}{2} < k + \frac{3}{2}.$$

In particular, a_n cannot be $\leq k - 1$ and cannot be $\geq k + 2$, so for all $n \geq N$ we must have

$$k \leq a_n < k + 2.$$

If for infinitely many n we had $a_n < k + 1$ and for infinitely many m we had $a_m \geq k + 1$, then the Cauchy sequence would cross the point $k + 1$ infinitely often, hence (by applying the previous lemma to $a_n - (k + 1)$) it would represent exactly $k + 1$. To make the integer part unique, we adopt the standard convention that the interval is *right-open*: we choose k so that eventually $a_n < k + 1$ (not $a_n \leq k + 1$). With this convention, the integer k is unique. □

Definition 34 (Integer part)**.** For $x = [(a_n)] \in \mathbb{R}$, define its integer part $\lfloor x \rfloor$ as the unique integer k such that for some N,

$$k \leq a_n < k + 1 \qquad \text{for all } n \geq N.$$

Step 2: the first digit after the decimal point

Let $k = \lfloor x \rfloor$. For all sufficiently large n we have $a_n \in [k, k + 1)$.

Divide the interval $[k, k + 1)$ into 10 subintervals of equal length:

$$[k, k + 1) = \bigsqcup_{d=0}^{9} \left[k + \frac{d}{10},\ k + \frac{d + 1}{10} \right).$$

Lemma 12 (The first digit stabilizes)**.** There exists a unique digit $d_1 \in \{0, 1, \ldots, 9\}$ such that for all sufficiently large n,

$$k + \frac{d_1}{10} \leq a_n < k + \frac{d_1 + 1}{10}.$$

Proof. Let $\varepsilon = \frac{1}{20}$. Since (a_n) is Cauchy, there exists N such that for all $n, m \geq N$,

$$|a_n - a_m| < \varepsilon = \frac{1}{20}.$$

The distance between two *non-adjacent* subintervals in the above partition is at least $\frac{1}{10}$, and

$$\frac{1}{10} > \frac{1}{20}.$$

Therefore, all terms a_n with $n \geq N$ must lie in at most two *adjacent* subintervals. If they lie in two adjacent ones infinitely often, then the sequence crosses their common boundary $k + \frac{d}{10}$ infinitely often for some d, hence by the stability lemma it represents that boundary point. With the right-open convention, we then select the subinterval on the left and obtain a unique d_1. □

Step 3: inductive construction of all digits

Assume we have already chosen digits $d_1, \ldots, d_m$ and defined the rational truncation

$$t_m := k + \frac{d_1}{10} + \frac{d_2}{10^2} + \cdots + \frac{d_m}{10^m}.$$

Consider the interval of length 10^{-m}:

$$I_m := \left[t_m,\ t_m + \frac{1}{10^m} \right).$$

By construction, for all sufficiently large n we have $a_n \in I_m$.

Now subdivide I_m into 10 equal right-open intervals:

$$I_m = \bigsqcup_{d=0}^{9} \left[t_m + \frac{d}{10^{m+1}},\ t_m + \frac{d+1}{10^{m+1}} \right).$$

Exactly as for the first digit, the Cauchy property implies that eventually all a_n lie in one of these 10 subintervals, and if two adjacent subintervals occur infinitely often then the represented real number is their boundary point, resolved by the right-open rule. This determines a unique next digit d_{m+1}.

Thus we obtain a digit sequence $d_1, d_2, d_3, \ldots$ and define the decimal expansion

$$\mathrm{Dec}(x) = k.d_1 d_2 d_3 \cdots .$$

Why we forbid tails of 9 and how they correspond to terminating decimals

Decimal expansions are not unique because of the identity

$$0.9999\ldots = 1.0000\ldots$$

and its shifted variants. To obtain a *unique* representation, we forbid expansions that are eventually all 9.

Lemma 13 (Direct computation of a tail of 9)**.** For any integer $m \geq 1$,

$$\sum_{j=m+1}^{\infty} \frac{9}{10^j} = \frac{1}{10^m}.$$

Proof. This is a geometric series. We compute directly:

$$\sum_{j=m+1}^{\infty} \frac{9}{10^j} = \frac{9}{10^{m+1}} \left(1 + \frac{1}{10} + \frac{1}{10^2} + \cdots \right).$$

Let

$$S := 1 + \frac{1}{10} + \frac{1}{10^2} + \cdots .$$

Then

$$\frac{1}{10}S = \frac{1}{10} + \frac{1}{10^2} + \frac{1}{10^3} + \cdots,$$

so subtracting,

$$S - \frac{1}{10}S = 1 \quad \Longrightarrow \quad \frac{9}{10}S = 1 \quad \Longrightarrow \quad S = \frac{10}{9}.$$

Therefore

$$\sum_{j=m+1}^{\infty} \frac{9}{10^j} = \frac{9}{10^{m+1}} \cdot \frac{10}{9} = \frac{1}{10^m}.$$

□

Lemma 14 (If the algorithm produces $a999\ldots$, the number equals the terminating decimal)**.** Suppose a decimal expansion has the form

$$k.d_1 d_2 \cdots d_m 9999 \cdots.$$

Let

$$t_m = k + \frac{d_1}{10} + \cdots + \frac{d_m}{10^m}.$$

Then

$$k.d_1 d_2 \cdots d_m 9999 \cdots \;=\; t_m + \frac{1}{10^m},$$

which is exactly the terminating decimal obtained by increasing the m-th digit by 1 (with carrying if necessary) and then writing zeros:

$$k.d_1 d_2 \cdots d_m 9999 \cdots \;=\; k.d_1 d_2 \cdots (d_m + 1)0000 \cdots$$

(after performing carries).

Proof. Compute directly:

$$k.d_1 \cdots d_m 9999 \cdots = t_m + \sum_{j=m+1}^{\infty} \frac{9}{10^j} = t_m + \frac{1}{10^m},$$

using the previous lemma. But adding 10^{-m} to t_m is exactly the decimal operation "add 1 in the m-th place and replace the tail by zeros" (with carries). □

Remark 19. In our digit-extraction algorithm we use right-open intervals at every step. This convention forces boundary points to be represented by the terminating expansion (with zeros), and therefore the produced expansion is *never* eventually all 9. Equivalently: tails of 9 are forbidden because they duplicate terminating decimals, and the algorithm never outputs them.

Example: the real number $\sqrt{2}$

Consider a rational sequence (a_n) defined by truncating the decimal expansion of $\sqrt{2}$:

$$a_1 = 1,\ a_2 = 1.4,\ a_3 = 1.41,\ a_4 = 1.414,\ \ldots$$

This is a Cauchy sequence in $\mathbb{Q}$. It does not converge in $\mathbb{Q}$, but it defines a real number

$$[(a_n)] \in \mathbb{R}.$$

One can show that this real number satisfies $x^2 = 2$ in $\mathbb{R}$ and is positive; it is denoted by $\sqrt{2}$.

:: self-control, excellent:

Exercise 12. There is an island upon which a tribe resides. The tribe consists of 100 people, with various eye colours. Yet, their religion forbids them to know their own eye color, or even to discuss the topic; thus, each resident can (and does) see the eye colors of all other residents, but has no way of discovering his or her own (there are no reflective surfaces). If a tribesperson does discover his or her own eye color, then their religion compels them to commit ritual suicide at noon the following day in the village square for all to witness. All the tribespeople are highly logical and devout, and they all know that each other is also highly logical and devout (and they all know that they all know that each other is highly logical and devout, and so forth).

Of the 100 islanders, it turns out that n of them have blue eyes and $100 - n$ of them have brown eyes, although the islanders are not initially aware of these statistics (each of them can of course only see 99 of the 100 tribespeople).

One day, a blue-eyed foreigner visits to the island and wins the complete trust of the tribe.

One evening, he addresses the entire tribe to thank them for their hospitality.

However, not knowing the customs, the foreigner makes the mistake of mentioning eye color in his address, remarking "how unusual it is to see another blue-eyed person like myself in this region of the world".

What effect, if anything, does this *faux pas* have on the tribe? a) Consider the case $n = 1$. b) Consider the case $n = 2$. c) Consider the general case.

4 Order as a binary relation. Examples and lexicographic order

4.1 :: orders, lexicographic order, lexicographic induction

Order relations as binary relations

Recall that a *binary relation* on a set X is a subset $R \subseteq X \times X$. If $(x, y) \in R$, we write xRy.

Definition 35 (Partial order)**.** A binary relation $\leq$ on a set X is called a *partial order* if it satisfies:

1. **Reflexive:** for all $x \in X$, $x \leq x$.
2. **Antisymmetric:** for all $x, y \in X$, if $x \leq y$ and $y \leq x$, then $x = y$.
3. **Transitive:** for all $x, y, z \in X$, if $x \leq y$ and $y \leq z$, then $x \leq z$.

A set X equipped with a partial order is called a *partially ordered set* (or *poset*).

Definition 36 (Total (linear) order)**.** A partial order $\leq$ on X is called a *total order* (or *linear order*) if in addition it satisfies:

$$\text{for all } x, y \in X, \text{ either } x \leq y \text{ or } y \leq x.$$

This property is called *comparability*.

Example 13 (Standard orders)**.**

- The usual order on $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ is a total order.
- The subset relation $\subseteq$ on the power set $\mathcal{P}(X)$ is a partial order (usually not total).
- Divisibility on $\mathbb{N}$:
$$a \preceq b \quad \iff \quad a \mid b$$
is a partial order on $\mathbb{N}$ (again, not total).

Example 14 (Why some orders are not total)**.** On $\mathcal{P}(\{1,2,3\})$ with $\subseteq$, the sets $\{1\}$ and $\{2\}$ are not comparable:

$$\{1\} \not\subseteq \{2\} \quad \text{and} \quad \{2\} \not\subseteq \{1\}.$$

Thus $\subseteq$ is not a total order.

Lexicographic order

Lexicographic order is the mathematical version of the order used in dictionaries.

Definition 37 (Lexicographic order on pairs)**.** Let $(A, \leq_A)$ and $(B, \leq_B)$ be totally ordered sets. Define a relation $\leq_{\text{lex}}$ on $A \times B$ by:

$$(a, b) \leq_{\text{lex}} (a', b') \quad \iff \quad \big(a <_A a'\big) \text{ or } \big(a = a' \text{ and } b \leq_B b'\big).$$

Problem 1. Prove that if $\leq_A$ and $\leq_B$ are total orders, then $\leq_{\text{lex}}$ is a total order on $A \times B$.

Definition 38 (Lexicographic order on n-tuples)**.** Let $A_1, \ldots, A_n$ be totally ordered sets. For $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ in $A_1 \times \cdots \times A_n$, define

$$x \leq_{\text{lex}} y$$

if at the first position where x and y differ, the corresponding coordinate of x is smaller. Formally, $x <_{\text{lex}} y$ if there exists k such that

$$x_1 = y_1,\ x_2 = y_2,\ \ldots,\ x_{k-1} = y_{k-1}, \quad \text{and} \quad x_k < y_k.$$

Applications of lexicographic order

Example 15 (Sorting words)**.** Let A be the set of letters with the usual alphabetic order. A word is a finite sequence of letters. If we order words lexicographically, then we recover dictionary order. For example:

$$\texttt{cat} < \texttt{cater} < \texttt{dog}.$$

Example 16 (Sorting by two keys)**.** Suppose each student has a pair (grade, name), where grades are integers and names are ordered alphabetically. Lexicographic order on

$$(\text{grade}, \text{name})$$

sorts students primarily by grade, and among equal grades, by name.

Example 17 (Calendar order of dates)**.** A date can be represented by a triple

$$(\text{year}, \text{month}, \text{day}) \in \mathbb{N}^3.$$

Lexicographic order on these triples gives the usual chronological order: first by year, then by month, then by day.

Example 18 (Decimal expansions and order)**.** A nonnegative real number can be represented (after choosing a unique decimal expansion without an eventual tail of 9) by

$$(b_0, b_1, b_2, \dots), \qquad b_0 \in \mathbb{N}, \quad b_i \in \{0, 1, \dots, 9\}.$$

Comparing two such expansions digit by digit is a lexicographic comparison: the first digit where they differ determines which number is larger. This is exactly how we compare decimals in elementary school.

Example 19 (Minimal counterexample arguments)**.** Lexicographic order is often used to formalize "minimal counterexample" proofs when there are several parameters. For example, among counterexamples described by a pair (p, AB), one can choose a counterexample with minimal p, and among those with minimal AB. This is precisely choosing a minimal element with respect to lexicographic order on $\mathbb{N}^2$.

Exercises

Problem 2. Give an example of a partial order that is not a total order. Give an example of a total order.

Problem 3. On $\mathbb{N}^2$, compare the following two orders:

- lexicographic order;
- order by sum: $(a, b) \preceq (c, d)$ if $a + b \leq c + d$.

Which one is a total order? Which one is not? Give a counterexample where two elements are not comparable.

Problem 4. Let $(A, \leq_A)$ and $(B, \leq_B)$ be totally ordered sets. Prove that lexicographic order on $A \times B$ is a total order.

Problem 5. Let $A = \{0, 1, \ldots, 9\}$ with the usual order, and consider the set $A^{\mathbb{N}}$ of infinite digit sequences. Show that lexicographic order on $A^{\mathbb{N}}$ is not a total order if we allow arbitrary sequences, unless we impose an additional condition. What condition is needed to recover the usual order on nonnegative real numbers?

Lexicographic induction

Let two sequences of natural numbers be given

$$A = (a_1, \ldots, a_n), \qquad B = (b_1, \ldots, b_n).$$

We say that $A > B$ (that is, A is *lexicographically larger* than B) if either $a_1 > b_1$, or $a_1 = b_1$ and $a_2 > b_2$, or $a_1 = b_1$, $a_2 = b_2$ and $a_3 > b_3$, and so on.

1. Prove that:
   (a) if $A > B$ and $B > C$, then $A > C$;
   (b) any strictly decreasing sequence of strings (sequences) of length n is finite;
   (c) every nonempty set of strings (sequences) of length n has a smallest element.

2. Let $x > 1$ be a natural number. Every second Diego replaces it by the number

$$y = \frac{x}{p}(p-1)^k,$$

where p is some prime divisor of x, and the integer k is arbitrary (and may change from step to step). Prove that sooner or later Diego will obtain 1.

3. A businessman made a deal with the devil: every day the businessman gives the devil one banknote, and in return receives any number of banknotes he wants, but of strictly smaller denomination. The businessman has no other source of banknotes, and initially he has only finitely many. Prove that no matter how the businessman exchanges banknotes, at some moment he will go bankrupt.

4. A computer screen shows a certain finite sequence of zeros and ones. One may perform the following operation: replace the block of digits "01" by either

   (a) "1000",

   (b) "100...0", where the number of zeros is arbitrary and may change from step to step.

   Prove that no matter how we act, we cannot perform this operation infinitely many times.

5. Participants of some exam are seated one per desk arranged as a $10 \times 10 \times 10$ cube. The exam consists of one problem. After the first hour, some students solved and wrote down the solution. From this moment on, each minute one student either copies the solution from a neighbor, or discovers a flaw in an already written solution and crosses it out. The proctor tries to prevent copying, so copying from a neighbor on the left, above, or behind is impossible. It is known that every written solution will eventually be crossed out.

Prove that sooner or later all students will cross out all solutions in their notebooks, and thus all fail the exam.

6. Let $a_1 < a_2 < \cdots$ be an increasing sequence of natural numbers such that among the prime divisors of the numbers $a_1, \ldots, a_{100}$ there occur

   (a) only 2 and 5,

   (b) only 2, 3, and 5,

   and moreover, for every natural number $n > 100$, the number a_n is defined as the smallest natural number greater than a_{n-1} that is not divisible by any of the numbers $a_1, a_2, \ldots, a_{n-1}$. Prove that this sequence contains only finitely many composite numbers.

5 :: Materials

Comments to the arithmetic/geometri mean inequality. Notes from tutorial 1

In the tutorial, we proved that if $n = 2^k$ for some positive integer k, and $x_1, \ldots, x_{2^k}$ are positive numbers, then the inequality

$$(x_1 \cdots x_{2^k})^{\frac{1}{2^k}} \leq \frac{x_1 + \cdots + x_{2^k}}{2^k} \tag{9}$$

holds. In particular, equality occurs if and only if

$$x_1 = x_2 = \cdots = x_{2^k}.$$

We are left to show the case when n is not a power of 2, that is, we need to fill the gaps between powers of 2.

Let $x_1, \ldots, x_n$ be arbitrary positive numbers, and choose k such that $n \leq 2^k$. Define

$$\alpha_i := \begin{cases} x_i, & i \leq n, \\ A, & n+1 \leq i \leq 2^k, \end{cases} \qquad \text{where} \quad A := \frac{x_1 + \cdots + x_n}{n}.$$

We apply inequality (9) to

$$(\alpha_1 \alpha_2 \cdots \alpha_{2^k})^{\frac{1}{2^k}},$$

which yields (remark that $nA = x_1 + \cdots + x_n$)

$$\left(x_1 \cdots x_n A^{2^k - n}\right)^{\frac{1}{2^k}} \leq \frac{x_1 + \cdots + x_n + (2^k - n)A}{2^k} = A.$$

We obtain

$$(x_1 \cdots x_n)^{\frac{1}{2^k}} \leq A^{1 - \frac{2^k - n}{2^k}} = A^{\frac{n}{2^k}}.$$

Finally, raising both sides to the power $\frac{2^k}{n}$ gives

$$(x_1 \cdots x_n)^{\frac{1}{n}} \leq A = \frac{x_1 + \cdots + x_n}{n}.$$

This completes the proof.

Sufficiency of operations $\cup$ and $\triangle$

Exercise: Express $\cap$ and $\setminus$ using only the operations $\cup$ and $\triangle$.

Answer:

1. We prove that

$$A \cap B = (A \cup B) \triangle (A \triangle B).$$

First, we show that $(A \cap B) \subseteq (A \cup B) \triangle (A \triangle B)$.

Let $x \in (A \cap B)$. Then $x \in (A \cup B)$ and $x \notin (A \triangle B)$, so $x \in (A \cup B) \backslash (A \triangle B) \subseteq (A \cup B) \triangle (A \triangle B)$.

Next, we show that $(A \cup B) \triangle (A \triangle B) \subseteq (A \cap B)$.

Let $x \in (A \cup B) \triangle (A \triangle B)$. Then

$$x \in \big((A \cup B) \backslash (A \triangle B)\big) \cup \big((A \triangle B) \backslash (A \cup B)\big),$$

by the definition of the symmetric difference.

If $x \in (A \cup B) \backslash (A \triangle B)$, then $x \notin (A \triangle B)$, which implies $x \in (A \cap B)$. Moreover, it is clear that $(A \triangle B) \backslash (A \cup B) = \emptyset$. Thus, $(A \cup B) \triangle (A \triangle B) \subseteq (A \cap B)$, completing the proof.

2. We now prove that

$$A \backslash B = (A \cup B) \triangle B.$$

First, we show that $A \backslash B \subseteq (A \cup B) \triangle B$.

If $x \in A \backslash B$, then $x \in (A \cup B)$ and $x \notin B$, so $x \in (A \cup B) \backslash B \subseteq (A \cup B) \triangle B$.

Now, we show that $(A \cup B) \triangle B \subseteq A \backslash B$.

Let $x \in (A \cup B) \triangle B$. Then either $x \in (A \cup B) \backslash B$ or $x \in B \backslash (A \cup B)$, by definition of the symmetric difference.

If $x \in (A \cup B) \backslash B$, then $x \in A \backslash B$. On the other hand, $B \backslash (A \cup B) = \emptyset$. Therefore, $(A \cup B) \triangle B \subseteq A \backslash B$, completing the proof.

5.1 Basic Graph Theory: Trees, Paths, and Leaves

Graph. A *graph* $G = (V, E)$ consists of a set of *vertices* V and a set of *edges* $E \subseteq \{\{u, v\} : u, v \in V, u \neq v\}$.

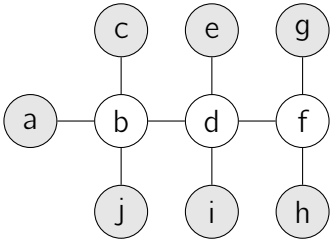
Path. A *path* is a sequence of distinct vertices $v_1, \ldots, v_k$ such that each consecutive pair (v_i, v_{i+1}) is an edge; its length is $k - 1$.

Tree. A *tree* is a connected graph with no cycles (acyclic). We will prove in tutorial that a tree on n vertices has exactly $n - 1$ edges.

A question before the tutorial

A *leaf* is a vertex of degree 1.
Why every tree has a leaf ?

Example tree with leaves highlighted



In the picture above, the light vertices a, c, e, g, h, i, j are *leaves* (each has degree 1). Vertices b, d, f have degree ≥ 2.

5.2 Corrections of students' homework

Student 1

1. **Solution:** Obviously, we cannot cut a 2×2 square without opposite corners into dominoes. Suppose we cannot cut a $2^n \times 2^n$ square with opposite corners removed into dominoes. A $2^{n+1} \times 2^{n+1}$ square can be cut into four $2^n \times 2^n$ squares. Even though it is obvious, you should show a picture showing what the cut is We place two dominoes at the center of this $2^{n+1} \times 2^{n+1}$ square so that they remove one corner from each of the four $2^n \times 2^n$ squares. In the case of two $2^n \times 2^n$ squares, their diagonals are effectively absent, meeting the above condition. The other two $2^n \times 2^n$ squares have one corner missing. here you should also show a picture Since the total grid count is even and dominoes cover an even number of cells, the coverable cells in the remaining squares are odd Here you are assuming that a domino should be contained in one of the four squares, which is not in the assumption. Hence the argument is wrong. Hence, we prove that a $2^{n+1} \times 2^{n+1}$ square with opposite corners removed cannot be tiled with dominoes.

2. **Solution:** According to Problem 1, we have proven by induction that a $2^n \times 2^n$ square without opposite corners cannot be cut into dominoes. Therefore, we cannot cut a $2^n \times 2^n$ square without opposite corners into dominoes.

3. **Solution:**

   - When $n = 7$, a large square is directly divided into four equal small squares, then one of these small squares is divided into four smaller squares, making a total of seven squares. You should show a picture
   - When $n = 8$, first divide the square into two rectangles, and then divide it into eight squares. Show a picture. I am afraid

you cannot obtain 8 squares in this form

- When $n = 9$, we can directly divide a square into nine squares. show a picture

We will prove this proposition by induction.

Suppose we can cut a square into n squares for each n. For a square that has been cut into n squares, cut one small square into four smaller squares. Then we prove we can cut a square into $n+3$ squares for each n. If you are going to apply induction, you could say: We already know that a square can be cut into 7,8 or 9 squares. Let $n \geq 9$ and suppose that a given square can be cut into k squares for any k between 7 and n. We are doing to cut the original square into $n+1$ small squares. Let $k = n+1-3$. Then k is between 7 and n so the original square can be cut into k squares by the inductive hypothesis. Choose one small square and cut it into four smaller squares. Then the original square has been cut into $k-1+4 = k+3 = n+1$ squares. By induction, we can say that the original square can be cut into n squares for any $n \geq 7$.

Alternatively, you coud also say: Note that if the given square can be cut into n squares then it can be also cut into $n+3$ squares. Indeed, for a square that has been cut into n squares, cut one small square into four smaller squares. Since any number $n \geq 10$ can be written as $7+3k$, $8+3k$ or $9+3k$ for $k \in \mathbb{N}$ and we know how to cut a square into 7, 8 and 9 squares, then we can cut a square into n square for any $n \geq 10$ too.

Hence, we prove it.

4. **Solution:** Totally, we have 51 odds, 50 evens, the sum of all numbers is odd (why?). Suggestion: At the beginning we have 51 odd numbers, 50 even numbers, and the sum of all the numbers

is $101 \times 102/2 = 101 \times 551$ We can do three operations: We analyze the 3 possible operations

- Odd minus even results in an odd, and the parity of the sum remains unchanged. you should give an explanation for this.
- Odd minus odd results in an even, and the parity of the sum remains unchanged. you should give an explanation for this.
- Even minus even results in an even, and the parity of the sum remains unchanged. you should give an explanation for this.

Hence, the parity of the sum is odd. (Suggestion: Hence the parity of the sum doesn't change after any sequence of these operations. Since at the beginning the sum is odd, it will be always odd.) When the last number is 0, the parity of the sum becomes even, leading to a contradiction. Thus, we prove it cannot be zero.

Student 2

Problem 1: Tiling a Square Without Opposite Corners

Suppose we don't have the corners $(1, 1)$ and $(4, 4)$.

- For row 1: We still have $(1, 1)$, $(1, 3)$, $(1, 4)$
- Let $(1, 2)$ and $(2, 2)$ be a domino (Explain why it is enough to consider this case). Then $(1, 3)$ and $(2, 3)$ should be a domino (why?, why can't $(1, 3)$ and $(1, 4)$ be covered by a domino instead?), $(4, 4)$ and $(5, 4)$ should be a domino.
- For row 2: We just have $(2, 1)$, then let $(2, 1)$ and $(3, 1)$ be a domino.
- For row 3: We have $(3, 2)$, $(3, 3)$, $(3, 4)$, let (. Let) $(3, 4)$ and $(4, 4)$, $(3, 5)$ and $(4, 5)$ be dominoes. Why do you consider these cases only? Then we still have $(3, 4)$.

- For row 4: We still have $(4, 1)$

But $(4, 1)$ and $(3, 4)$ can't be a domino. Thus, we cannot cut a square without opposite corners into dominoes.

Problem 2: Chessboard Coloring Argument

We can color the 8×8 square like a chessboard. Then a domino should cover one black square and one white square.

If we remove two black corners, then the removed cells are of the same color, and we can assume that they are black. Hence we have 30 black squares and 32 white squares. Thus, we can have 30 dominoes but still have 2 white squares left. Thus we can use at most 30 dominoes, leaving at least 2 white cells uncovered.

Therefore, we cannot cut an 8×8 square without opposite corners into dominoes.

Problem 3: Dividing a Square into Smaller Squares

- If $n = 7$, then we can cut a square into a square 2×2 and 6 squares 1×1. how? there are no pictures.
- If $n = 8$, then we can cut a square into a square 3×3 and a square 1×1. how? there are no pictures.
- If $n = 9$, then we can cut a square into 9 squares 1×1. how? there are no pictures.

For $n > 9$, if we can cut a square into k squares, then cut one of the squares into 4 smaller squares, thus we will get $k + 3$ squares.

- For $n = 7$, then we can get $n = 10 = 7 + 3$, $n = 13 = 10 + 3$, ...
- For $n = 8$, then we can get $n = 11 = 8 + 3$, $n = 14 = 11 + 3$, ...

- For $n = 9$, then we can get $n = 12 = 9 + 3$, $n = 15 = 12 + 3$, ...

In all, we can cut a square into 10 squares for each $n > 6$.

Problem 4: Parity Argument with Numbers

From 1 to 101, there are 51 odd numbers and 50 even numbers.

Since Note that:

- odd - odd = even
- even - odd = odd
- even - even = even
- odd - even = odd

Thus:

- If we remove two odd numbers, the count of odd numbers will decrease by 2
- If we remove an odd number and an even number, the counts will remain the same
- If we remove two even numbers, the counts will remain the same

Therefore, no matter what two numbers we remove, the count of odd numbers is always an odd number (at least 1).

Hence, this number cannot be zero.

Student 3

problem 1

You could begin by saying: Assume that it is possible and let us consider a covering. We write $(a, b) \to (c, d)$ to indicate that the cells (a, b) and (c, d) are covered by a domino.

The first line:
$(1,2) \to (1,3) \Rightarrow$ must $(1,4)$ y $(2,4)$ You could say. If $(1,2) \to (1,3)$ then necessarily $(1,4) \to (2,4)$

The second line:
$(2,3) \to (2,2) \Rightarrow$ must implies $(2,1) \to (3,1)$. Why do you assume $(2,3) \to (2,2)$?

The third line:
$(3,3) \to (3,4) \Rightarrow$ must $(3,2) \to (4,2)$ Same comment

So $(4,1)$ is solo is false However, it is now impossible to cover $(4,1)$

if $(3,2) \to (3,3)$ that $(3,4)$ must $\to (4,4)$

but $(4,4)$ is not exist so is false. is not exist doesn't exist in English. You may say: but then $(4,4)$ can not be covered.
It seems that you are considering two cases. Be more explicit.

Problem 2

Color the 8×8 grid in black and white like a chessboard
$8 \times 8 = 64$: it has 32 white cells and 32 black cells

reduce opposite corners $64 - 2 = 62$ After removing two opposite corners, there are 62 cells left

because the opposite corners have the same color

therefore it has 30 black (white) and 32 white (black)
Since two opposite corners have the same color, we may assume that

there are now 30 black cells and 32 white cells

because every domino have one black one-white color

but now the number (white and black) is not equal But every domino covers one black cell and one white cell and the number of white and black cells in the table are unequal; hence such a covering is impossible

so it is false . But every domino covers one black cell and one white cell and the number of white and black cells are unequal; hence such a covering is impossible

Problem 3

Let the large square cut into a 4 2×2 squares You might say: Let the large square be cut into four 2×2-squares. Include a figure

Let let one of the small squares be cut to into a 2×2 smaller squares like (figure)

it It totally has 7 squares and repeat . Repeat this process

We we can know what cut a square in $7 + 3n$ is correct. We therefore know how to cut a square into $7 + 3n$ squares

$n = 8$ like (figure) (The cut in the figure has only 7 squares

$n = 9$ like (figure)

so $9 + 3n$ is correct so $n > 6$ is correct. You probably want to say: Therefore, we can cut a square into $7 + 3n$, $8 + 3n$ and $9 + 3n$ for any non-negative integer n

Student 4

Problem 1

(figure) Establish a plane right angle coordinate system and each block can match a coordinate point.

Then we notice that $(1, 2)$ can only connect with $(1, 3)$ or $(2, 2)$ to create a domino.

(Case 1): $P(1, 2)$ connect with $(1, 3)$,
$\Rightarrow (1, 4)$ can only connect with $(2, 4)$
$\Rightarrow (3, 4)$ can only connect with $(3, 3)$
$\Rightarrow (2, 3)$ can only connect with $(2, 2)$
and $(4, 3)$ can only connect with $(4, 2)$
$\Rightarrow (3, 2)$ can only connect with $(3, 1)$
Then we find that $(2, 1)$ and $(4, 1)$ cannot create into a domino.
Therefore this case is invalid.

(Case 2): $P(1, 2)$ connect with $(2, 2)$
$\Rightarrow (2, 1)$ can only connect with $(3, 1)$
$\Rightarrow (4, 1)$ can only connect with $(4, 2)$
$\Rightarrow (3, 2)$ can only connect with $(3, 3)$
then we find that $(4, 3)$ cannot connect with anything. Therefore, this case is also invalid.

So we cannot cut a square without opposite corners into domino.

Problem 2

(figure: chess board)

We can cover some blocks with shadow to make sure that each block was surrounded by four blocks with shadow like the picture. Then we can find that a domino must be created by a white block and a shadowed block.

However, there exist $8 \times 8/2 = 32$ white blocks but only exist $8 \times 8/2 - 2 = 30$ shadowed blocks. Then there must exist two white blocks

that cannot be connected into a domino. Therefore, we cannot cut a square 8×8 without opposite corners into domino.

Problem 3

Assume that we can cut a square in

$$k \text{ squares }, k \in \mathbb{N}$$

Then we can choose one square from k squares and cut it into four 2×2 squares. Then we can get 3 more squares. Then we can cut a square in $k + 3$ squares

$$k \in \mathbb{N}$$

Then we only need to find that a square can be cut into $3n$ squares, $3n + 1$ squares and $3n + 2$ squares. $\exists n \in \mathbb{N}$. This phrase is badly written. You may want to say. Every $n \geq 7$ is of the form $9 + 3n$, $8 + 3n$ or $7 + 3n$.

1) cut a square in $3n$ squares Cut of a square into $9 + 3n$ squares

if $n = 3$, then $3n = 9$ By the above argument, it is enough to cut a square into 9 squares.

then we can cut it into a square 3×3 valid no figure is shown

2) cut a square in $3n + 1$ squares Cut of a square into $7 + 3n$ squares

if $n = 1$, then $3n + 1 = 4$ then we can cut it into a square 2×2 valid no figure is shown. Same comment as above

3) cut a square in $3n + 2$ squares if $n = 2$, then $3n + 2 = 8$ then we can cut it like the picture (figure) to get 8 squares, valid Same comment

Therefore, we can cut a square in n squares, $n > 6$ and $n \in \mathbb{N}$.

Problem 4

Assume that the remaining number is zero. There exist At the beginning there are 51 odd numbers and 50 odd (even)numbers and odd number will

not effect the parity (I don't understand this phrase), and the difference of odd numbers must be an even number.

So after repeating this operation to 50 odd numbers and 50 even numbers, the outcome must be an even number, then the difference between this even number and the last odd number must be an odd number. This part of the argument is unclear

However, zero is an even number Then contradiction This is a contradiction Then the number remained cannot be zero. The remaining number cannot be zero

Student 5

Problem 1

We assume first domino horizontal in row.

Row 1 has squares (1,1) removed, so possible dominoes are (1,2)–(1,3) or (1,3)–(1,4).

If (1,2)–(1,3)) Suppose that (1,2)–(1,3) is a domino. At this time Row 1 has (1,4) left - need to (2,4) so (1,4)–(2,4) should be a domino. Now Row 2 has (2,1)–(2,3) left. Placing force (2,1)–(2,2) force (2,3) left why do you assume that (2,1)–(2,2) is a domino?

(2,3) pair with (3,3) but (3,3)'s adjacent squares. You might say that (3,4) cannot be part of a domino.

Later create (3,3) unpaired square. this part is unclear

Others situation is similar to above. why?

Problem 2

(1) 8×8 has 32 black and 32 white squares. Removing 2 opposite corners. These corners are of the same color.

Thus the remain 30 black and 32 white. Thus we may assume that the remaining cells are 30 black cells and 32 white cells A domino always

covers 1 black cell and 1 white cell, but the number of white cells is not equal to the number of black cells.

Therefore It's impossible to tile an 8×8 square.

Problem 3

$n = 6$: Divide the original square into 1 large square (3/4 area) and 5 smaller equal square (1/16 area) in the remaining area. (figure) In the figure there are 8 squares. Besides 3/4+5/16 is not 1

$n = 7$: Divide the original square into 1 large square (2/3 area) and 6 smaller equal square (1/9) in the remaining area. No figure is shown and same problem as above

$n \geq 8$: start with $n = 6$ or $n = 11$ split one small square into 4 equal smaller squares. This argument is unclear

Problem 4

The sum of 1 to 101 is odd: $S = n(n+1)/2 = 101 \times 102/2 = 5151$ because $a + b$ and $|a - b|$ have same parity. Don't begin a sentence with because. You could say: Note that $a + b$ and $|a - b|$ have the same parity. By the way: Why this is true? after 100 operations the final number equals the total sum's parity (odd). Before saying this, you should say, since $a + b$ and $|a - b|$ have the same parity, the parity of the total sum is unchanged under any operation. Since it was odd at the beginning, it must be always odd; in particular, it can never be 0.

Since 0 is even so the final number cannot be 0.

Student 6

Problem 1

Solution: Assume that we can cut a square 4×4 without opposite corners into domino. Analyze the following programm (program: Why do you call it a program?):

(figure)

Number each grid cells, we can get that there is just one case, since the programmer is symmetry symmetric, then . Then 1-2, and could only be 3-4, 11-10, 12-13, 14-8, 7-6. Finally we can see that 5 and 9 are not covered which is contradiction. Therefore, we cannot cut a square 4×4 without opposite corners into domino.

Problem 2

Solution: Color the table 8×8 into black and white, like chess end a sentence with a period

then Then (the first word in a sentence should begin with a capital letter)each domino contains 1 white and 1 black cell

(figure) here 32 white cells 30 black cells

but a white cell needs to be paired with a black cell, thus the number of white cells and the number of black cells need to be equal. Therefore we cannot cut a square 8×8 without opposite corners into dominos.

Problem 3

Solution: Base step:

If $n = 7$, the result is true. proof: Start with a 2×2 square and divide one of the square into 4 smaller squares. This gives $\frac{1}{4} + 4 = 7$ squares.

If $n = 8$, the result is true. proof: Divide a 3×3 square into 9 smaller squares and merge 2 adjacent squares to form a 2×2 square. This gives $9 - 2 - 1 = 8$ squares. no figure. It seems that this is incorrect

If $n = 9$, the result is true. proof: Simply divide the square into 9 equal smaller squares. You should include a figure

Inductive step: Suppose the result is true for n ($n > 6$)

n.t.p. the result is true for $n + 3$. Since we already know that the result is true for $7, 8, 9$ we only need to prove that the result is true for $n + 3$

Proof: To get $n+3$ squares from n squares, take a configuration of n squares and divide one of the squares into 4 smaller squares. This increase the total count by 3. Therefore we can cut a square in n squares for each $n > 6$

Problem 4

Proof: Consider the sum modulo 2 of all numbers on the board. Initially, the numbers are 1, 2, ..., 101. The sum is $S = 101 \times 102/2 = 5151$

Since 5151 is odd, we have $S \equiv 1 (\text{mod } 2)$. Now, pick two numbers a and b, erase them, and write $|a-b|$.

If $a > b$, then $|a-b| = a-b$. The new sum $S = S-a-b+(b-a) = S-2b$

If $b \geq a$, then $|a-b| = b-a$. The new sum $S = S-a-b+(b-a) = S-2a$

Thus $S = S - 2 \cdot \min(a, b)$

That is, the sum changes by an even number. Therefore $S \equiv S (\text{mod } 2)$ What do you really want to say here? Maybe you want to say that if S' is obtained after any number of operations then $S' \equiv S \equiv 1$ mod 2. Suppose X remains. Thus the sum is X. That is, The sum is X and $X \equiv S \equiv 1 (\text{mod } 2)$

Hence X is odd, and in particular $X \neq 0$.

Student 7

Problem 1

Proof: Here is a square 4×4 with one corner. (figure)

Assume the top-left cell has the coordinate $(1, 1)$ and the bottom-right cell has the coordinate $(4, 4)$.

First case, we start to cover the $(1, 2)$ cell.

A. $(1, 2)$ cell covers the cell $(1, 3)$ (You want to say $(1, 2)$ and $(1, 3)$ are covered by the same domino. The same applies everywhere), then

the cell $(1,4)$ must cover $(2,4)$, then the cell $(3,4)$ covers the cell $(3,3)$, then the cell $(2,3)$ covers the cell $(2,2)$, then the cell $(2,1)$ covers the cell $(3,1)$, then the cell $(3,2)$ covers the cell $(4,2)$. Don't use too many commas in a row. Use perios instead Finally, we find that the cell $(4,1)$ and the cell $(4,3)$ can't be covered.

B. $(1,2)$ cell covers the cell $(2,2)$, then the cell $(2,1)$ covers the cell $(3,1)$, then the cell $(4,1)$ covers the cell $(4,2)$, then the cell $(4,3)$ covers the cell $(3,3)$, then the cell $(3,4)$ covers the cell $(4,4)$. Then we find that the cell $(3,3)$ and the cell $(4,3)$ can't be covered, so it is false. This last conclusion should be written in a separate paragraph.

You could finish the proof here by symmetry

Second case A, Cell (2,1) covers the cell (2,2), the cell (1,2) covers the cell (1,3), the cell (1,4) covers the cell (2,4), the cell (2,3) covers the cell (3,3). Then we find that the cell (3,4) can't be covered.

B cell (2,1) covers the cell (3,1): the cell (4,1) covers the cell (4,3), the cell (4,3) covers the cell (3,3), the cell (3,2) covers the cell (2,2), the cell (1,2) covers the cell (1,3), the cell (2,3) covers the cell (2,4). Then we find that the cell (1,4) and the cell (3,4) can't be covered.

In the two cases we find that this problem has no solution.

Problem 2

Proof: Color the 8×8 chessboard in a checkerboard pattern, where any two adjacent squares have different colors. Since squares at opposite corners are always of the same color, we may assume the squares at opposite corner are white, Use a period here. You could say: After removing them, we have .... then we remove them, then we have 32 black squares and 30 white squares.

When we place a 1×2 or 2×1 domino, we find that it must cover a black square and a white square. But the black squares is not equal to the white squares But the number of black squares ... after we removed the two white squares.

Thus, a complete tiling of the 8×8 chessboard with two opposite corners removed is impossible.

Problem 3

Proof: $n = 7$: we can cut the square then we have four squares, then we choose one square to cut, then we get $4 - 1 + 4 = 7$ squares. Use periods and figures: We first cut the square into 4 squares as shown in the figure. Then we pick one of the small squares and cut it in a similar fashion. We get $4 - 1 + 4 = 7$ squares

$n = 8$: we can cut the square like this picture (This is not a valid cut). Then we get 8 squares.

$n = 9$: we can cut the square like this picture. Then we get 9 squares.

Assume any element $K \geq 9$, the squares can be cut then we get K squares. Let $K \geq 9$ and assume that it is possible to cut a square into K squares. We can choose one squares to cut to get 4 squares Use a period then we get $K - 1 + 4 = K + 3$ squares.

Since we have proved it exist when $n = 7, 8, 9$. Then for all $n > 6$, $\Rightarrow n + 3$ when $n = 7$, $n = 10$, $n = 13$, $n = 16$, when $n = 8$, $n = 11$, $n = 14$, $n = 17$, when $n = 9$, $n = 12$, $n = 15$, $n = 16$. Thus for all $n > 6$ is exist. You may want to say: Since we have proved that it is possible to cut any square into 7,8 or 9 squares, the argument in the previous paragraphh says that it is also possible to cut a square into $7 + 3 = 10$, $10 + 3 = 13$, ..., squares, or $8 + 3 = 11$, $11 + 3 = 14$, ..., squares, or $9 + 3 = 12, 12 + 3 = 15, \ldots$. In other words, it is possible to cut a square into n squares for any $n \geq 7$

Problem 4

Proof: Firstly, we add all the numbers $1 + 2 + 3 + \ldots + 101 = \frac{101 \times 102}{2} = 5151$. When we choose two numbers such as a, b,

if $a+b$ is odd then $|a-b|$ is odd too because $|a-b| = |a+b-2b|$ odd-even=odd,

if $a+b$ is even, then $|a-b|$ is even too because $|a-b| = |a+b-2b|$ even-even=even. Don't use too many commas. Use periods instead.

Then we find that the parity of the total number remains the same after the change as it was before.

Assume the number is 0, then we find that the sum is even, but the initial total number 101×55 is odd because odd $\times$ odd = odd.

Thus the number is 0 that is false what do you want to express here, so the number isn't 0.

Student 8

Problem 1

Mark the horizontal and vertical coordinates from 1 to 4.

Case 1. Domino covers (1,3), (1,4)
(1,2) (2,2) ✓ since (1,1) is removed
consider (4,1)

1. 1-1 Domino covers (4,1) (4,2)
   sub (i) (4,3) - (3,3) ✓
   sub (ii) (2,4) ✓
   $(2,4) \to (2,3) \to (2,1) and (3,1)$ covered $(3,2)$ and $(3,4)$ isolated

   (2,4) $\to$ (3,4) $\to$ (2,3) isolated

   Above, it's contradiction in both subcases.

2. 1.2 covers (4,1) $\to$ (3,1) ✓
   $\to$ (4,2) ✓
   cover (4,3) $\Rightarrow$ (3,2) (3,3) ✓ leaving (2,1) $\times$
   cover (3,2) $\Rightarrow$ (4,3)(3,3) ✓ leaving (2,1) $\times$

Above, it's contradiction

Case 2 covers (1,4) (2,4) ✓
Then (1,3) ✓

2.1 covers (1,2) (1,3) ✓

Then (1,2) is covered. There are 3 cases (2,1) (3,1) (4,1)

(a) (4,1) (4,2) ✓
Then (4,3) covered with (3,3) ✓ and (2,1) must be covered
-(2,1) covered with (2,2) then (2,3) becomes isolated
-(2,1) If covered with (3,1) then (2,2), (2,3) (3,2) (3,4) remain but no domino can cover (2,3) and (3,4).

Contradiction

(b) covers (4,1) - (3,1)
(4,2) ✓
(4,2) $\rightarrow$ (4,3) ✓ $\rightarrow$ (3,2) covered with (3,3) leaving (2,1) $\times$
(4,2) $\rightarrow$ (3,2) $\Rightarrow$ (4,3) (3,3) ✓ leaving (2,1) $\times$

Contradiction

2.2 covers (1,3) - (2,3)

Then (1,2) - (2,2) ✓

(a) (4,1) - (4,2) covered
$\Rightarrow$ (4,3) covered with (3,3)
(2,1) must covered with (3,1) ✓
leaving (3,2) and (3,4) $\times$

Contradiction

(b) (3,1) - (4,1) ✓
Then (4,2) ✓
(4,2)→ (4,3) ⇒ (3,2)(3,3) ✓

(2,1) is isolated
(4,2)→(3,2) ⇒ (4,3) (3,3)
(2,1) is isolated.

Since all cases lead to contradiction, it's impossible. The proof us unnecessary long. It could be reduced to Case 1 by symmetry. Moreover, while it is possible to follow it, the language is imprecise

Problem 2

At the beginning there are... There are 64 squares. Black is 32 and White is 32. 32 black and 32 white

Since we remove the corners, hence the color of opposite corners are the same. Suppose the corners are both black, then black is 30, white is 32. This could be phrased as: Since we remove opposite cornes, and opposite cornes have the same colors, we may assume that there are now 30 black squares and 32 withe squares.

Since Remove 'since' each domino should cover 1 black and 1 white square, but the number of black squares $<$ the number of white squares.

Hence it can't be covered.

Conclusion: We can't cover a 8×8 square without opposite corners by dominoes.

Problem 3

Proof:

- For $n = 7$: This gives $4 - 1 + 4 = 7$ squares no figure is shown
- For $n = 8$: This gives $9 - 4 + 1 = 6$ squares no figure is shown

Induction:
Assume we can partition a square into k squares for some $k \geq 6$. Then we can partition into $k + 3$ by:

1. Select any one square
2. Divide it into 4 smaller squares
3. This increases the total count by 3

Hence, it's true. incomplete. You should also consider $n = 9$ as a base case

Problem 4

Proof:
Odd numbers: 51
Even numbers: 50

- Case 1: Erase 2 odd numbers $\Leftrightarrow$
  Their difference is even $\Leftrightarrow$ The count of odd numbers decreases by 2.
- Case 2: Erase 2 even numbers $\rightarrow$
  Their difference is ~~odd~~ even $\rightarrow$ The count of odd numbers remains unchanged.
- Case 3: Erase one odd and one even $\rightarrow$
  The difference is odd $\rightarrow$ The count of odd numbers remains unchanged.

We find no matter how you operate, the parity of odd count remains the same.

Therefore, the count of odd numbers is always odd.

If the last remaining number were 0, then the count of odd numbers would be 0.

This is a contradiction, hence it cannot be 0.

Student 9

Problem 1

Label the rows and columns of the 4×4 square from 1 to 4, suppose that the removed opposite corners are $(1,1)$, $(4,4)$.

For $(1,2)$, it has two situations: covered with $(1,3)$, or with $(2,2)$.

1. if covered with $(1,3)$ (Begin the sentence with capital I), so $(1,4)$ must be covered with $(2,4)$; $(3,4)$ must be covered with $(3,3)$; $(4,3)$ must be covered with $(4,2)$; $(4,1)$ must be covered with $(3,1)$; and $(2,1)$ must be covered with $(2,2)$;

   Eventually, there have $(2,3)$ and $(3,2)$ Eventually $(2,3)$ and $(3,2)$ are the only remaining cells, and they cannot be covered with a domino.

   So in this case, we cannot cut a square 4×4 without opposite corners into domino.

2. if covered with $(2,2)$ begin a sentence with capital I, so $(2,1)$ must be covered with $(3,1)$; $(4,1)$ must be covered with $(4,2)$; $(4,3)$ must be covered with $(3,3)$; $(3,4)$ must be covered with $(2,4)$; $(1,4)$ must be covered with $(1,3)$.

   Eventually, there have $(2,3)$ and $(3,2)$, and they cannot be covered with a domino.

   So in this case, we cannot cut a square 4×4 without opposite corners into domino.

Therefore, this proposition is true.

Problem 2

Color the 8×8 square in a checkerboard pattern (black and white alternatively). Each domino must cover one black and one white square. There are 64 squares in this square. After removing two opposite corners

(the same color) there are 30 black/white squares and 32 white/black squares left. Since each domino must cover one black square and one white square, ~~so~~ the number of black and white squares must be equal. So it is impossible to tile the space.

Problem 3

Proof: For $n = 7$, divide the square into three 2×2 squares and four 1×1 squares, totaling $3 + 4 = 7$ squares.

For $n = 8$, divide the square into one 3×3 square and seven 1×1 squares, totaling $1 + 7 = 8$ squares.

For $n = 9$, divide the square into nine 1×1 squares.

For $n \geq 7$, we can split one square into four smaller squares based on $n = 7$ (each operation increases the number of squares by 3). Thus, all integers $n > 6$ satisfy the situation. This argument is incomplete. The base cases are 7,8 and 9.

Problem 4

Proof: The initial sum $1 + 2 + \cdots + 101 = \frac{101 \times 102}{2} = 101x51$, which is odd. Each operation "erase two numbers a, b and write $|a - b|$" doesn't change the parity of the total sum why?. The remaining number must have the same parity as the initial sum, while 0 is even. Therefore, the remaining number cannot be 0.

1. A snail crawls in the plane at a constant speed and every 15 minutes turns 90 degrees (sometimes left, sometimes right). Prove that it can return to its starting point only after an integer number of hours.

   Solution: We introduce a system of orthogonal coordinates so that the starting point is $(0,0)$ and the snail moves either horizontally or vertically. In addition, we can assume that the snail turns precisely when it reaches a point with integer coordinates. For example, the initial path could be $(0,0) \to (0,1) \to (1,1) \to (1,2) \to (0,2) \to (1,1) \to (-1,1)$.

   Note that in each movement $(x,y) \to (x',y')$ the parity of the quantity $x+y$ will change. Hence the number of movements to return to the starting point must be even. In other words, the snail can return to its starting point only after an integer multiple of 30 minutes. However, any 30 minutes the parity of x changes. Hence, the snail can return to the starting point only after an even multiple of 30 minutes, in other words, only after an integer multiple of 60 minutes.

2. Prove that among any 52 integers there exist two whose sum or difference is divisible by 100.

   Solution: We partition the numbers $0, 1, 2, \ldots, 99$ into 51 groups: $\{0\}$, $\{1, 99\}$, $\{2, 98\}$, ..., $\{49, 51\}$ and $\{50\}$. There are 51 groups. Let S be a set of 52 integers. The reminder in the division by 100 of each of these integers is a number in one of these groups. Since we have 52 integers and 51 groups, there must be two integers $s_1, s_2 \in S$ in the same group. If s_1 and s_2 have the same reminder, say $s_1 = 100k_1 + r$ and $s_2 = 100k_2 + r$ then $s_1 - s_2 = 100(k_1 - k_2)$ is divisible by 100. If s_1 and s_2 have different remainders then the group containing these remainders is of the form $\{r, 100-r\}$ and we may assume that s_1 has remainder r and s_2 remainder $100-r$. Hence $s_1 = 100k_1 + r$ and $s_2 = 100k_2 + 100 - r$. Hence

$s_1 + s_2 = 100(k_1 + k_2 + 1)$ is a multiple of 100.

3. One hundred numbers are arranged on a circle. Each number is equal to the arithmetic mean of its neighbours. Prove that all the numbers are equal.

   Solution: Let L be the maximum of the numbers on the circle. We say that a number among the 100 numbers is maximal if it is equal to L. We want to show that every number is maximal. It is enough to show that if a number on the circle is maximal, then so are it two neighbours. Let a and b its neighbours. Then $a \leq L$ and $b \leq L$. We may assume $a \leq b$. Then $L = \frac{a+b}{2} \leq \frac{b+b}{2} = b \leq L$. Hence $b = L$. Now $L = \frac{a+L}{2}$, and from this we get $2L = a + L$ and so $a = L$.

4. Each student in the class took part in at least one of two hikes. In each hike, the proportion of boys did not exceed $2/5$. Prove that in the whole class, the proportion of boys does not exceed $4/7$.

   Solution:

Proof. Assume the snail moves at constant speed v, so each 15-minute segment covers distance $s = v \times 15$ minutes. Without loss of generality, scale units so $s = 1$.

The snail's path consists of unit-length moves, each perpendicular to the previous one due to the 90-degree turns. Thus, the moves alternate between horizontal (x-direction) and vertical (y-direction), assuming the initial move is horizontal; the case of initial vertical is symmetric.

After n moves: - If n is even, there are $n/2$ horizontal and $n/2$ vertical moves. - If n is odd, there are $(n+1)/2$ horizontal and $(n-1)/2$ vertical moves.

Each horizontal move is ± 1 in the x-direction, and each vertical move is ± 1 in the y-direction. For the snail to return to the origin, the net displacement in both x and y must be zero.

The net x-displacement is the number of $+1$ minus the number of -1 in horizontal moves. Let r be the number of $+1$ and ℓ the number of -1, so $r + \ell =$ number of horizontal moves, and net x = $r - \ell$. For net x = 0, $r = \ell$, so the number of horizontal moves must be even.

Similarly, the number of vertical moves must be even.

- If $n = 4k$, both are $2k$, even. - If $n = 4k + 1$, horizontal: $2k + 1$ (odd), vertical: $2k$ (even) — impossible. - If $n = 4k + 2$, both $2k + 1$ (odd) — impossible. - If $n = 4k + 3$, horizontal: $2k + 2$ (even), vertical: $2k + 1$ (odd) — impossible.

Thus, return is possible only if n is a multiple of 4.

The time elapsed is $n \times 15$ minutes = $n/4$ hours, which is an integer if and only if n is a multiple of 4. □

5.3 Notes from tutorial 8

Question 4. Show that if $n > k \log_2 10$, then

$$\left|(\sqrt{2}-1)^n\right| < 10^{-k}.$$

Solution. Since

$$\sqrt{2}-1 = \frac{1}{\sqrt{2}+1} < \frac{1}{2},$$

we have

$$0 < (\sqrt{2}-1)^n < \left(\frac{1}{2}\right)^n = 2^{-n}.$$

Now we explain why $n > k \log_2 10$ implies $2^{-n} < 10^{-k}$. Recall that $\log_2 10$ is *the number x such that* $2^x = 10$. Because the exponential function 2^x is strictly increasing, the inequality $n > k \log_2 10$ implies

$$2^n > 2^{k \log_2 10} = (2^{\log_2 10})^k = 10^k.$$

Taking reciprocals reverses the inequality (since all numbers are positive), giving

$$2^{-n} < 10^{-k}.$$

Combining with $(\sqrt{2}-1)^n < 2^{-n}$, we obtain

$$\boxed{\left|(\sqrt{2}-1)^n\right| < 10^{-k}}.$$

Question 5. Let n be even. Show that the first k digits after the decimal point of $(1+\sqrt{2})^n$ are equal to 9.

Solution. Define

$$u_n = (1+\sqrt{2})^n + (1-\sqrt{2})^n.$$

Since n is even, $(1-\sqrt{2})^n = (\sqrt{2}-1)^n > 0$, and $u_n \in \mathbb{Z}$. Set

$$\varepsilon = \left|(\sqrt{2}-1)^n\right| = (\sqrt{2}-1)^n.$$

By Question 4, if $n > k \log_2 10$ then $0 < \varepsilon < 10^{-k}$.

We write

$$(1+\sqrt{2})^n = u_n - (1-\sqrt{2})^n = u_n - \varepsilon.$$

Thus $(1+\sqrt{2})^n$ is an integer minus a positive number ε satisfying $0 < \varepsilon < 10^{-k}$. Hence the fractional part of $(1+\sqrt{2})^n$ is

$$\{(1+\sqrt{2})^n\} = 1 - \varepsilon.$$

Since $\varepsilon < 10^{-k}$, its decimal expansion begins with at least k zeros, so $1-\varepsilon$ begins with at least k nines. Therefore the first k digits after the decimal point of $(1+\sqrt{2})^n$ are all equal to 9.

For even $n > k \log_2 10$, the first k decimal digits of $(1+\sqrt{2})^n$ are 9.

5.4 Explaining the Diagonal Bijection $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$

Convention. $\mathbb{N} = \{0, 1, 2, \dots\}$.

1. The Diagonal Idea

Arrange all ordered pairs $(a, b) \in \mathbb{N} \times \mathbb{N}$ in a grid:

	$n=0$	$n=1$	$n=2$	$n=3$	$\cdots$
$m=0$	$(0,0)$	$(1,0)$	$(2,0)$	$(3,0)$	$\cdots$
$m=1$	$(0,1)$	$(1,1)$	$(2,1)$	$(3,1)$	$\cdots$
$m=2$	$(0,2)$	$(1,2)$	$(2,2)$	$(3,2)$	$\cdots$
$m=3$	$(0,3)$	$(1,3)$	$(2,3)$	$(3,3)$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

Instead of reading rows or columns, we read **diagonals** (top to bottom) of constant sum

$$a + b = 0,\ 1,\ 2,\ 3,\ \dots$$

For example:

$$\begin{aligned} a+b=0 &: (0,0) \\ a+b=1 &: (1,0),\ (0,1) \\ a+b=2 &: (2,0),\ (1,1),\ (0,2) \\ a+b=3 &: (3,0),\ (2,1),\ (1,2),\ (0,3) \\ &\vdots \end{aligned}$$

The idea is:

- First list all pairs on diagonal $a + b = 0$ - Then all pairs on diagonal $a + b = 1$ - Then all on diagonal $a + b = 2$, and so on.

This reading order goes through *every* pair exactly once, so it defines a bijection.

2. Counting How Many Pairs Come Before a Given Diagonal

Diagonal s (i.e. all pairs with $a+b=s$) contains exactly $s+1$ pairs.

The total number of pairs listed before diagonal s is therefore:

$$0+1+2+\cdots+s=\frac{s(s+1)}{2}.$$

This number is called the ***s*-th triangular number**, denoted

$$T_s=\frac{s(s+1)}{2}.$$

3. Locating (a,b) Along Its Diagonal

If a pair has sum

$$s=a+b,$$

then:

- there are T_s pairs on earlier diagonals, and - within the diagonal $a+b=s$, we move $**b$ steps** from the start (because the diagonal is listed as $(s,0),(s-1,1),(s-2,2),\ldots,(0,s)$).

Therefore the position (the natural number assigned to (a,b)) is

$$\boxed{\pi(a,b)=T_{a+b}+b=\frac{(a+b)(a+b+1)}{2}+b.}$$

4. Why This is a Bijection

First the following claim:
If m+n < m'+n', then $\pi(m,n)<\pi(m',n')$.
Proof: Subject to the constraint $m+n=k$, the maximum value of $\pi(m,n)$ is $\pi(0,k)=\frac{k(k+1)}{2}+k$ and the minimum value of $\pi(m,n)$

is $\pi(k,0) = \frac{k(k+1)}{2}$. Now if $k' \geq k+1$, then $\pi(k',0) = \frac{k'(k'+1)}{2} \geq \frac{(k+1)(k+2)}{2} = \frac{k(k+1)}{2} + k + 1 > \frac{k(k+1)}{2} + k = \pi(0,k)$.

Check that you understand why this is enough to prove the claim above.

Surjective. Given $n \in \mathbb{N}$, let $T_k = \frac{k(k+1)}{2}$ be the largest triangular number not exceeding n. Let $b = n - T_k$ and $a = k - b$, then $\pi(a,b) = n$.

Injective. It follows that the equality $\pi(a,b) = \pi(a',b')$ implies that $a+b = a'+b'$ But then $a = a'$ and $b = b'$, which gives the injectivity of $\pi(a,b)$.

5. Small Table

(a,b)	$\pi(a,b)$
$(0,0)$	0
$(1,0)$	1
$(0,1)$	2
$(2,0)$	3
$(1,1)$	4
$(0,2)$	5
$(3,0)$	6
$(2,1)$	7

	$n=0$	$n=1$	$n=2$	$n=3$	$\cdots$
$m=0$	0	1	3	6	$\cdots$
$m=1$	2	4	7		$\cdots$
$m=2$	5	8			$\cdots$
$m=3$	9				$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

6. Summary

The formula

$$\pi(a, b) = \frac{(a+b)(a+b+1)}{2} + b$$

is nothing more than:

1. Count all diagonals before the one containing (a, b): this gives T_{a+b}.

2. Then walk b steps along that diagonal.

This converts planar coordinates (a, b) into a single natural number by following the diagonal ordering.