**MATH 298 A1-Sem - Fall 2021**

**Problem solving seminar**

# Contents

**Lecture 1, Wednesday, September 1, 2021**

This course is not going to be as well structured as a standard undergraduate course in mathematics. There are a few reasons for this. One is the nature of the subject: there is not a well defined theory about problem solving, unlike, for instance, linear algebra, where it is quite clear what are the fundamental notions that should be covered in a first course on the subject. One can design such a course by presenting various problem solving techniques and illustrating them from different topics in mathematics; alternatively, one can present problems from algebra, calculus, number theory, combinatorics, etc., that can be solved using elementary theory and some problem solving techniques. In this course, we will do both: we will either spend a few consecutive weeks on a technique, or spend them instead studying problems from a specific area of mathematics.

Another reason is that the class may be quite heterogeneous: even though this problem solving seminar is listed as a 200-level course, it is open to students at all level who have the basic necessary background. In particular, a first course in calculus and a first course in linear algebra are preferable, but past experience with mathematical competitions can compensate for that.

# 1 The Box (Pigeonhole) Principle

The Box Principle is still more commonly known as the Pigeonhole Principle, but since pigeonholes are less common than they used to be, I'll call it the Box Principle. In its simplest version, it consists of the following observations:

If $n$ balls are placed in $m$ boxes and if $n > m$, then one box must contain at least two objects.

For instance, if you put four balls in three boxes, then there is a box with more than one ball. If you put six balls in four boxes, then one of the boxes must contain at least two balls.

There exists also a more general version of the Box Principle:

If more than $n$ balls are placed in $m$ boxes and $n > km$, then one box most contain at least $k + 1$ objects.

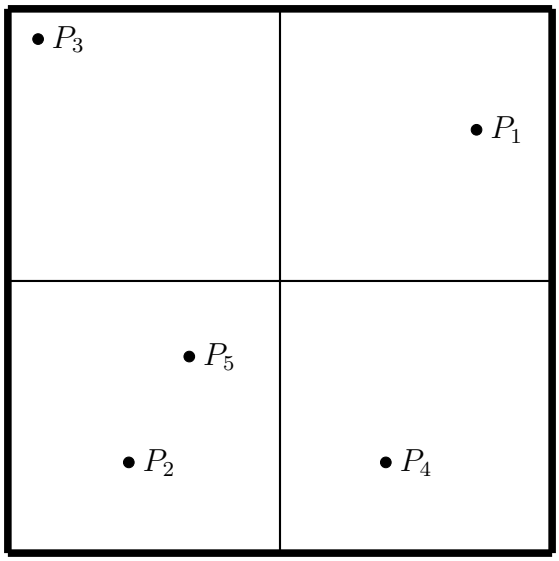
For instance, if you put five balls in two boxes (so $n = 5, m = 2, k = 2$), then there is a box with at least three balls. If you put seven balls in three boxes (so $n = 7, m = 3, k = 2$), then the same is true.

If you have $km$ balls and try to avoid putting $k + 1$ in any box, then the only way to achieve this is to put exactly $k$ balls in each of the $m$ boxes. After the $kn$ balls are distributed in this way, if you have one more ball to place in a box, then it will end up in a box with at least $k + 1$ balls because each box already contains $k$ balls.

The Box Principle does not require further explanations, but it is not always clear how to use it. To apply it to a mathematical problem, one has to determine what should play the role of the boxes and what should pay the role of the balls. Hopefully, a few examples will clarify this.

**Example 1**: Consider five points $P_1, P_2, P_3, P_4$ and $P_5$ located inside a square of side length 1. The points can be on the sides or strictly inside. Prove that at least two of those points are located at a distance $\leqslant \frac{\sqrt{2}}{2}$.

*Solution:* Divide the square into four smaller squares of the same size:




These smaller squares are the boxes and the five points are the balls. By the Box Principle, at least two of the points are in the same smaller square.

Since the large square has sides of length 1, the smaller squares have sides of length $\frac{1}{2}$ and a diagonal of length $\frac{\sqrt{2}}{2}$. Two points located in the same small square are at a distance of at most $\frac{\sqrt{2}}{2}$ from each other, with this upper bound being reached when the points at located at opposite corners. □

**Example 2**: If 11 distinct integers are selected from the set $\{1, 2, \ldots, 20\}$, show that two of those selected integers $a, b$ differ by 2: $|a - b| = 2$.

*Solution:* Let the balls be the 11 integers selected. The 10 boxes are labelled by the pairs

$$\{1,3\},\ \{2,4\},\ \{5,7\},\ \{6,8\},\ \{9,11\},\ \{10,12\},\ \{13,15\},\ \{14,16\},\ \{17,19\},\ \{18,20\}.$$

Note that the integers in each pairs differ by two. Place each integer selected into the box corresponding to the pairs that contains it: since the pairs are all disjoint, there is only one box into which each integer can be placed.

Since 11 integers are selected and placed into 10 boxes, some box contains at least two integers $a$ and $b$. By the way the boxes are labelled, these two integers differ by two. □

**Lecture 2, Wednesday, September 8, 2021**

Direct applications of the Box Principle allow us to draw the following conclusion:

- Among 13 people, at least two were born on the same month.

- Among 367 people, at least two were born on the same day of the year.

Here is another classic example of application of the Box Principle.

**Example 3**: $n$ people attend a meeting. Prove that at least two of them know the same number of people. (Here, it is assumed that if $X$ knows $Y$, then $Y$ knows $X$.)

*Solution:* Everyone knows between 1 and $n$ attendees, so a priori it seems that the Box Principle cannot be applied. One observation is actually needed before applying it: if someone knows everybody else, then everyone knows at least two people at the meeting: themselves and the person who knows everybody else. Thus, in this case, everyone knows between 2 and $n$ attendees. Otherwise, if no one knows everybody else, then everyone knows between 1 and $n-1$ attendees. Let's consider these two cases.

Case 1: Someone knows everybody else. Label the boxes from 2 to $n$ and label the balls by the name of the attendees. Put the ball label $X$ in box $m$ if person $X$ knows $m$ attendees. Since there are $n$ people present at the meeting, there are $n$ balls so, by the Box Principle, at least one box contains two balls. If box $m$ contains balls labelled $X$ and $Y$, then persons $X$ and $Y$ know exactly the same number of attendees, namely $m$ of them.

Case 2: No one knows everybody else. Then label the boxes from 1 to $n-1$ and label the balls again by the name of the attendees. The rest of the argument is as in the previous case. □

**Example 4**: The subset $\mathbb{Z}^2$ of $\mathbb{R}^2$ consisting of points $(a, b)$ with integral coordinates, so $a, b \in \mathbb{Z}$, is called the plane lattice. Five lattice points are chosen in $\mathbb{Z}^2$. Prove that two of these points are such that the segment joining these points passes through another lattice point.

*Solution:* Let's try to see when the midpoint of two of those lattice points can also belong to $\mathbb{Z}^2$. The midpoint of $(a, b)$ and $(c, d)$ is $\left(\frac{a+c}{2}, \frac{b+d}{2}\right)$. If $a, b, c, d \in \mathbb{Z}$, then this midpoint is on the lattice $\mathbb{Z}^2 \iff$ both $\frac{a+c}{2} \in \mathbb{Z}$ and $\frac{b+d}{2} \in \mathbb{Z} \iff$ both $a + c$ and $b + d$ are even.

$a + c$ is even $\iff a$ and $c$ have the same parity, so either both are even or both are odd. The same is true for $b + d$.

Is it possible to find two points $(a, b)$ and $(b, d)$ among those five lattice points for which $a$ and $c$ have the same parity, and similarly for $b$ and $d$?

There are four different possibilities for the parities of the coordinates of a lattice point $(a, b)$:

$$(\text{even}, \text{even}),\ (\text{even}, \text{odd}),\ (\text{odd}, \text{even}),\ (\text{odd}, \text{odd}).$$

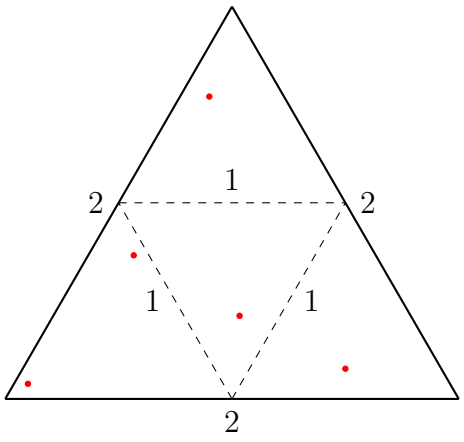
Consider four boxes labelled with these four possibilities and five balls labelled by the five lattice points. Put a ball labelled $(a, b)$ in the box labelled by the parities of $a$ and $b$.

By the Box Principle, one box contains at least two balls. If these are labelled by the lattice points $(a, b)$ and $(c, d)$, then the midpoint of the line segment connecting $(a, b)$ to $(c, d)$ is also on $\mathbb{Z}^2$ because $a + c$ is even and $b + d$ is also even. □

**Example 5**: Imagine that you throw darts at a target that has the shape of an equilateral triangle with sides of length 2. After throwing five darts, show that two of them are at a distance $\leqslant 1$ from each other.

*Solution:* In order to apply the Box Principle where the darts are the balls, we need to divide the equilateral triangle into four regions. In this type of problem, it is natural to try to find a subdivision into equal (congruent) parts.

An equilateral triangle of sides of length 2 can be divided into four smaller equilateral triangles, all with sides of length 1. By the Box Principle, one of these smaller triangles must contain at least two darts. Any two darts within one of these will be at a distance of at most 1. □



**Lecture 3, Wednesday, September 15, 2021**

**Example 6**: Prove that there is an integer whose decimal expansion consists only of 1's and which is a multiple of 2019.

*Solution:* Consider the integers

$$1,\ 11,\ 111,\ \cdots\ \underbrace{111\cdots1}_{2019\text{ digits}},\ldots$$

Label the balls with these integers. Here, there are infinitely many balls: this is fine because, for sure, there will be more balls than boxes.

Since this is a question about divisibility by 2019, it is natural to think that it may have to do with the remainders upon division by 2019. If you don't have much experience with this type of problem, this may not seem natural, but once you have more experience (and this topic will be discussed more in the last part of this course), you will see why this is reasonable. Therefore, let us label the boxes by the remainders $0, 1, 2, \ldots, 2018$ upon division by 2019.

Put ball $a$ in the box labelled $r$ if $a = 2019q + r$ and $0 \leqslant r \leqslant 2018$.

If one of those integers has remainder 0, the proof is finished. If not, by the Box Principle, at least two of those numbers $a$ and $b$ have the same remainder when they are divided by 2019:

$$a = 2019q_1 + r \text{ and } b = 2019q_2 + r.$$

The difference $a - b$ is divisible by 2019 since

$$a - b = 2019(q_1 - q_2).$$

Let us assume that $a > b$. (The same ideas work if $b < a$.) Then

$$a - b = 111\cdots100\cdots0 = \underbrace{111\cdots1}_{c}\cdot 10^k$$

for some $k$.

Since 10 and 2019 are relatively prime and 2019 divides $c\cdot 10^k$, it follows that 2019 divides $c$, so $c$ is a multiple of 2019 and its only digit is 1. □

This example can be generalized by replacing 2019 by any integer $n$ not divisible by 2 or 5: the proof above can be repeated verbatim with 2019 replaced by $n$.

**Example 7**: Show that if $n + 1$ numbers are selected from $\{1, 2, \ldots, 2n\}$, then one of them is divisible by another one.

*Solution:* One way for two such numbers to exist is if one of them is $k$ with $1 \leqslant k \leqslant n$ and the other one is $2k$, which must then be $\leqslant 2n$. If we can show that there exists a pair of integers of the form $k, 2k$ among that set of $n+1$ numbers, then this problem will be solved.

Since the are $n+1$ numbers selected, it is expected that the balls should be labelled by these integers, which we can denote by $a_1, a_2, \ldots, a_{n+1}$. Finding how to label the boxes requires some thinking.

We can factor each $a_i$ as

$$a_i = 2^{c_i} b_i$$

where $b_i$ is an odd integer in the set $\{1, 2, \ldots, 2n\}$ and $c_i \geqslant 0$. ($c_i = 0$ when $a_i$ is odd.) There are $n$ odd integers in the set $\{1, 2, \ldots, 2n\}$, namely $1, 3, 5, \ldots, 2n-1$. Let us label $n$ boxes using these integers and let us put ball $a_i$ in box $b_i$.

Since there are $n+1$ balls and $n$ boxes, by the Box Principle, there exists a box that contains two balls. In other words, there exist distinct integers $a_i$ and $a_j$ such that $b_i = b_j$. Assuming that $c_i < c_j$ (without loss of generality), we thus obtain

$$a_j = 2^{c_j} b_j = 2^{c_j - c_i} 2^{c_i} b_i = 2^{c_j - c_i} a_i.$$

This shows that $a_i$ divides $a_j$. □

**Example 8**: $n$ people sit at a round table to attend a meeting. They are all equally distributed around the table. There are name tags in front of each chair, but it happens so that no one took the chair with his or her name attached to it. Prove that it is possible to rotate the table so that at least two people are sitting with their name tags in front of them.

*Solution:* It was suggested in class that if we can first rotate the table so that one person is sitting in front of their name tag then, by some sort of application of the Box Principle, someone else must also have their name tag in front of them. This is not true and a counterexample was worked out after class. Here it is: imagine four people named $A, B, C, D$ sitting in the clockwise direction around a table and suppose that the name tags in front of them are, respectively, $C, A, D, B$. If the table is rotated by $90^\circ$ counter-clockwise, then the name tags in front of them become $A, D, B, C$, so $A$ has his or her own name tag, but this is not the case for $B, C$ and $D$.

Denote by $R_k$ the rotation of the table by an angle of $\frac{2\pi k}{n}$ for $k = 0, 1, \ldots, n-1$. Label $n$ boxes by the rotations $R_k$ for $k = 0, 1, \ldots, n-1$. Label the balls by the names of the people present. Put the ball labelled $X$ in box $R_k$ if, after rotating the table by $R_k$, $X$'s name tag is in front of them. By assumption, since no one took the chair with their name attached to it, no ball is in the box labelled $R_0$, so there are $n$ balls in the $n-1$ boxes labelled $R_1, \ldots, R_{n-1}$. Observe that, for each person $X$, there is exactly one rotation $R_k$ such that, after applying $R_k$, $X$'s name tag is in front of them.

By the Box Principle, one box contains at least two balls. If this is box labelled $R_k$ and the balls are labelled X and Y, then this means that, after rotating the table using $R_k$, the name tags of $X$ and $Y$ are in front of them. □

**Lecture 4, Wednesday, September 22, 2021**

**Example 9**: Let $X$ be a set consisting of $n$ distinct integers. Show that there is a non-empty subset $\widetilde{X}$ of $X$ such that the sum of the elements in $\widetilde{X}$ is divisible by $n$.

*Solution:* Let $x_1, x_2, \ldots, x_n$ be the integers in $X$. If we want to apply the Box Principle, then it is natural to take the $n$ congruence classes as the boxes. This is indeed what should be done, but an original idea is now needed.

For each subset $\widetilde{X}$ of $X$, we can consider the sum of its elements. $X$ has $2^n - 1$ non-empty subsets, so we obtain in this way at lot more than $n$ integers. However, there is no guarantee a priori that one of those is divisible by $n$.

We actually don't have to consider all the possible subsets of $X$. The original idea that is needed is to consider a chain of increasing subsets

$$X_1 \subset X_2 \subset X_3 \subset \cdots \subset X_n \subset X.$$

Namely, let $X_i = \{x_1, \ldots, x_i\}$. If

$$x_1 + x_2 + \cdots + x_i \equiv 0 \bmod n$$

for some $i$, then we are done: $\widetilde{X}$ can be taken to be $X_i$. If not, then the $n$ sums $x_1 + x_2 + \cdots + x_i$ (for $i = 1, 2, \ldots, n$) are all congruent to $1, 2, \ldots, n-2$ or $n-1$ modulo $n$.

By the Box Principle, two of those sums belong to the same congruence class, say

$$x_1 + x_2 + \cdots + x_j \equiv x_1 + x_2 + \cdots + x_i \bmod n$$

for some $1 \leqslant i < j \leqslant n$. Then it follows that

$$x_{i+1} + x_{i+2} + \cdots + x_j \equiv 0 \bmod n.$$

The subset $\widetilde{X}$ can then be taken to be $X_j \backslash X_i$ (the complement of $X_i$ in $X_j$), that is, the subset $\{x_{i+1}, x_{i+2}, \ldots, x_j\}$. □

There is a generalization of the Box Principle which will be used in the next two examples.

Generalized Box Principle: Let $k, m, n \in \mathbb{Z}_{\geqslant 1}$. If $n$ balls are placed in $m$ boxes and $n \geqslant mk+1$, then one box must contain at least $k+1$ balls.

For instance, if $m = 5, k = 3$ and $n = 16$, then you can put the first 15 balls into the 5 boxes with 3 balls per box, but then the $16^{th}$ must go into a box that already contains 3 balls, thus ending up with 4 balls in one box.

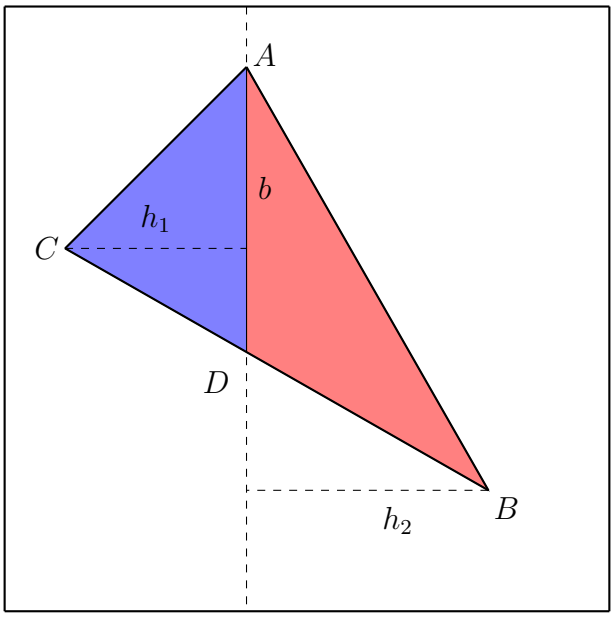
The original Box Principle is the case $k = 1$.

**Example 10**: Consider a square of side length 4. If 33 points are placed inside (or on the boundary) of this square, prove that 3 of them form a triangle of area $\leqslant \frac{1}{2}$.

*Solution:* Recalling the first example, we are lead to think about partitioning the given square into smaller squares and we would like to use the Generalized Box Principle to conclude that 3 points must be inside one of the small squares. This means that $k + 1$ should be 3, so $k$ should be 2. If the points are the balls and there are $m$ boxes, then we need to have $33 \geqslant 2m + 1$. This is true for $1 \leqslant m \leqslant 16$. In particular, if $m = 16$, that is, if the given square is divided into 16 smaller squares, then the Generalized Box Principle says that one of these smaller squares contains 3 points.

The large square can be divided into 16 squares of side length 1. The result now follows from the observation that any 3 points inside a square of unit area form a triangle of area $\leqslant \frac{1}{2}$. To see why this is true, observe that it three points $A, B, C$ are located inside a square, then it is possible to increase the area of the triangle $ABC$ if one vertex, say $A$, is not on one of the sides of the square, but moving $A$ towards a side of the square (following a line perpendicular to $BC$). Therefore, a triangle of maximum area is obtained when all three vertices $A, B, C$ are located on the square itself. It can then be seen that the maximum area is $\frac{1}{2}$: this happens, for instance, when $BC$ is one side of the square and $A$ is located on the side opposite to $BC$.

Here is a neat trick to show that the maximal area of $ABC$ is $\frac{1}{2}$.



Let $b$ be the length of the base common to the triangles $ABD$ and $DCA$.

$$\begin{aligned}\text{area}(ABC) &= \text{area}(ABD) + \text{area}(DCA)\\ &= \frac{bh_1}{2} + \frac{bh_2}{2}\\ &= \frac{b(h_1+h_2)}{2}\\ &\leqslant \frac{1\cdot 1}{2} = \frac{1}{2}\end{aligned}$$

The inequality follows from the observation that $b \leqslant 1$ and $h_1 + h_2 \leqslant 1$. □

**Lecture 5, Wednesday, September 29, 2021**

**Example 11**: Prove that any subset $S$ of 55 integers chosen from the set $\{1, 2, \ldots, 100\}$ must contain numbers differing by exactly 9.

*First solution:* Let the boxes be labelled by the congruences classes modulo 9 and let the balls be labelled by the 55 integers. Let's place ball $k$ into box $r$ if $r$ is the residue modulo 9 of $k$. By the Box Principle, one box contains at least two balls. This means that two numbers $x$ and $y$ in $S$ satisfy $x \equiv y \bmod 9$. However, being congruent modulo 9 does not mean differing by exactly 9: $x \equiv y \bmod 9$ means that $x - y$ is a multiple of 9, so it could be $\pm 9, \pm 18, \pm 27$, etc.

Therefore, something a bit more clever than a simple application of the Box principle is required. Actually, what is needed is the Generalized Box Principle. Since $55 = 9 \cdot 6 + 1$, there must be at least seven numbers in the set $S$ - denote them $x_1, x_2, \ldots, x_7$ - such that $x_i \equiv x_j \bmod 9$. Without loss of generality, we can assume that $x_1 < x_2 < \cdots < x_7$.

We have to see that two of them differ by exactly 9. Let's argue by contradiction, so let's suppose that this is not the case. Then $x_{i+1} - x_i \geqslant 18$ since $x_{i+1} \equiv x_i \bmod 9$ for $i = 1, 2, \ldots, 6$. Therefore,

$$x_7 \geqslant x_6 + 18 \geqslant x_5 + 2 \cdot 18 \geqslant x_4 + 3 \cdot 18 \geqslant \cdots \geqslant x_1 + 6 \cdot 18 \geqslant 1 + 108 = 109.$$

This is a contradiction because

$$\{x_1, x_2 \ldots, x_7\} \subset \{1, 2, \ldots, 100\}.$$

It follows that $x_{i+1} - x_i$ must equal 9 for some $i \in \{1, 2, \ldots, 6\}$. □

*Second solution:* Divide the set $\{1, 2, \ldots, 100\}$ into the following subsets:

$$\begin{gathered}\{1, 10\},\ \{2, 11\}, \ldots,\ \{9, 18\} \\ \{19, 28\},\ \{20, 29\}, \ldots,\ \{27, 36\} \\ \{37, 46\},\ \{38, 47\}, \ldots,\ \{45, 54\} \\ \{55, 64\},\ \{56, 65\}, \ldots,\ \{63, 72\} \\ \{73, 82\},\ \{74, 83\}, \ldots,\ \{81, 90\} \\ \{91, 100\},\ \{92\},\ \{93\}, \ldots,\ \{99\}\end{gathered}$$

The number of subsets in this list is $9 \cdot 5 + 1 + (99 - 92 + 1)$, that is, 54. Since the set $S$ contains 55 integers, by the Box Principle, one of those 54 subsets contains two integers from $S$. By the way those subsets are defined, it follows immediately that $S$ contains two integers that differ by exactly 9. □

A solution similar to the first one works for the same question, but with 9 replaced by 10. It actually shows that, in this case, 55 can be replaced by 51 and the same solution still applies.

We have seen applications of the Box Principle to problems in number theory, combinatorics and geometry. It can also be applied to problems that are more related to analysis or, in the next example, analytic number theory.

**Example 12**: Prove that there exist integers $a, b, c$, each less than $10^6$ in absolute value and not all 0, such that

$$|a + b\sqrt{2} + c\sqrt{3}| < 10^{-11}.$$

*Remark:* The same solution as the one below would show that there exist integers $a$ and $b$, each less than $10^6$ in absolute value, such that $|a + b\sqrt{2}| < 10^{-5}$.

*Solution:* Consider all the numbers of the form $r + s\sqrt{2} + t\sqrt{3}$ with integers $r, s, t$ such that $0 \leqslant r, s, t, \leqslant 10^6 - 1$. There are $10^{18}$ such integers and, for these values,

$$0 \leqslant r + s\sqrt{2} + t\sqrt{3} < (1 + \sqrt{2} + \sqrt{3})10^6 < 5 \cdot 10^6.$$

Partition the interval $[0, 5 \cdot 10^6]$ into $10^{18} - 1$ subintervals of the same length.

By the Box Principle, one of these subintervals must contain two of those numbers. (Here, the boxes are labelled by the subintervals and the balls are labelled by the numbers $r + s\sqrt{2} + t\sqrt{3}$.) If those two numbers are $r_1 + s_1\sqrt{2} + t_1\sqrt{3}$ and $r_2 + s_2\sqrt{2} + t_2\sqrt{3}$, set

$$a + b\sqrt{2} + c\sqrt{3} = (r_1 + s_1\sqrt{2} + t_1\sqrt{3}) - (r_2 + s_2\sqrt{2} + t_2\sqrt{3}).$$

In other words, set $a = r_1 - r_2$, $b = s_1 - s_2$ and $c = t_1 - t_2$. Then

$$|a + b\sqrt{2} + c\sqrt{3}| \leqslant \frac{5 \cdot 10^6}{10^{18} - 1} < \frac{10^7}{10^{18}} = 10^{-11}.$$

The first inequality follows from the fact that the subintervals all have length $\left|\frac{5 \cdot 10^6}{10^{18}-1}\right|$. $\square$

**Lecture 6, Wednesday, October 6, 2021**

It was mentioned in the remark above that there exist integers $a$ and $b$ such that $|a + b\sqrt{2}| < 10^{-5}$. It is actually possible to replace $10^{-5}$ by $10^{-k}$ for any $k \geqslant 1$ or by any $\epsilon > 0$. Even more generally, one can prove the following proposition.

**Example 13**: Let $\alpha \in \mathbb{R}$ be an irrational number. The line $y = \alpha x$ does not pass through any lattice point $(a, b)$ with $a, b \in \mathbb{Z}$ except $(0, 0)$, but it comes arbitrarily close to infinitely many of them.

*First proof:* This proof is more similar to the one used in Example 12. Since $\frac{b}{a} \neq \alpha$ for any $a, b \in \mathbb{Z}$ $(b \neq 0)$ because $\alpha$ is irrational, it follows that the line does not pass through the point $(a, b)$. It is enough to show that, for any $\epsilon > 0$, there exist integers $a$ and $b$ such that $|b - \alpha a| < \epsilon$, for then the point $(a, \alpha a)$ is within $\epsilon$ of the lattice point $(a, b)$.

Looking at the solution in the previous example (but with the roles of $a$ and $b$ interchanged), we need to look at integers in some interval $[0, N]$ and then obtain the inequalities

$$|b - \alpha a| \leqslant \frac{(1 + |\alpha|)N}{N^2 - 1} < \epsilon. \tag{1}$$

The last inequality is equivalent to $\frac{N^2-1}{(1+|\alpha|)N} > \frac{1}{\epsilon}$ and to

$$N^2 > \frac{(1 + |\alpha|)N}{\epsilon} + 1. \tag{2}$$

Since the function $x \mapsto x^2$ increases much faster than the linear function $x \mapsto \frac{(1+|\alpha|)x}{\epsilon} + 1$, there exists a positive integer $N$ for which the inequality (2) holds, hence the second inequality in (1) holds also.

The proof then goes on as follows. Without loss of generality, we can assume that $\alpha > 0$, for if $\alpha < 0$, then $-\alpha > 0$ and if $|b - (-\alpha)a| < \epsilon$ for some $a, b \in \mathbb{Z}$, then $|b - \alpha(-a)| < \epsilon$, so $a$ just needs to be replaced by $-a$.

With $N$ chosen such that $\frac{(1+\alpha)N}{N^2-1} < \epsilon$, subdivide the interval $[0, (1 + \alpha)N]$ into $N^2 - 1$ subintervals of equal length $\frac{(1+\alpha)N}{N^2-1}$. Consider the $N^2$ real numbers $s + \alpha r$ with $r, s$ integers

in the interval $[0, N-1]$. By the Box Principle, two of those numbers must be in the same subinterval, so if these two numbers are $s_1 + \alpha r_1$ and $s_2 + \alpha r_2$, then

$$|(s_1 + \alpha r_1) - (s_2 + \alpha r_2)| \leqslant \frac{(1+\alpha)N}{N^2 - 1}.$$

Setting $b = s_1 - s_2$ and $a = r_2 - r_1$, we obtain

$$|b - \alpha a| = |(s_1 + \alpha r_1) - (s_2 + \alpha r_2)| \leqslant \frac{(1+\alpha)N}{N^2 - 1} < \epsilon.$$

□

*Second proof:* Let $\epsilon > 0$ and pick a positive integer $n$ such that $\frac{1}{n} < \epsilon$. Consider the $n$ numbers $k\alpha$ with $k \in \{0, 1, \ldots, n-1\}$. Write each as

$$k\alpha = \lfloor k\alpha \rfloor + \{k\alpha\} \text{ where } 0 \leqslant \{k\alpha\} < 1 \text{ and } \lfloor k\alpha \rfloor \in \mathbb{Z}.$$

Label $n$ balls by the numbers $\{k\alpha\}$, $k = 0, 1, \ldots, n-1$.

Let's divide the interval $[0, 1]$ into $n$ sub-interval of equal length:

$$[0, 1) = \bigcup_{i=0}^{n-1} \left[ \frac{i}{n}, \frac{i+1}{n} \right).$$

If $0 \leqslant \{k\alpha\} < \frac{1}{n}$, then the distance between the points $(k, k\alpha)$ and $(k, \lfloor k\alpha \rfloor)$ is $k\alpha - \lfloor k\alpha \rfloor$, which equals $\{k\alpha\}$. Therefore, the distance is $< \frac{1}{n}$, hence is $< \epsilon$.

If no $\{k\alpha\}$ is in the interval $\left[0, \frac{1}{n}\right)$, then all the numbers $\{k\alpha\}$, $k = 0, 1, \ldots, n-1$ are in the $n-1$ intervals $\left[\frac{i}{n}, \frac{i+1}{n}\right)$ with $1 \leqslant i \leqslant n-1$. Label $n-1$ boxes by these intervals and put the ball labelled $\{k\alpha\}$ into the interval that contains it. By the Box Principle, one box contains at least two balls, which means that there is an interval $\left[\frac{i}{n}, \frac{i+1}{n}\right)$ that contains $\{k\alpha\}$ and $\{\ell\alpha\}$ for some distinct $k, \ell \in \{1, \ldots, n-1\}$. This means that $|\{k\alpha\} - \{\ell\alpha\}| < \frac{1}{n}$.

Therefore,

$$(k - \ell)\alpha = \lfloor k\alpha \rfloor - \lfloor \ell\alpha \rfloor + \{k\alpha\} - \{\ell\alpha\},$$

so

$$\big|\big(\lfloor \ell\alpha \rfloor - \lfloor k\alpha \rfloor\big) + (k - \ell)\alpha\big| = |\{k\alpha\} - \{\ell\alpha\}| < \frac{1}{n} < \epsilon.$$

The distance between the lattice point $(k - \ell, \lfloor \ell\alpha \rfloor - \lfloor k\alpha \rfloor)$ and the point $(k - \ell, (k - \ell)\alpha)$ on the line $y = \alpha x$ is thus $< \epsilon$. □

**Example 14** Prove that, for every set $X = \{x_1, x_2, \ldots, x_n\}$ of $n$ real numbers, there exists a non-empty subset $S$ of $X$ and an integer $m$ such that

$$\left| m + \sum_{s \in S} s \right| \leqslant \frac{1}{n+1}.$$

*Solution:* Let $S_i = \{x_1, x_2, \ldots, x_i\}$ and $\sigma_i = \sum_{s \in S_i} s$ for $i = 1, \ldots, n$.

Write each $\sigma_i$ as $\sigma_i = \lfloor \sigma_i \rfloor + \{\sigma_i\}$ where $0 \leqslant \{\sigma_i\} < 1$ and $\lfloor \sigma_i \rfloor \in \mathbb{Z}$. Consider the partition of the interval $[0, 1)$ by the $n+1$ sub-intervals $\left[\frac{i}{n+1}, \frac{i+1}{n+1}\right)$ with $0 \leqslant i \leqslant n$.

If $\{\sigma_i\} \in \left[0, \frac{1}{n+1}\right)$, then set $S = S_i$ and $m = -\lfloor \sigma_i \rfloor$. It follows that

$$|m + \sigma_i| = | - \lfloor \sigma_i \rfloor + \lfloor \sigma_i \rfloor + \{\sigma_i\}| = |\{\sigma_i\}| < \frac{1}{n+1}.$$

If $\{\sigma_i\} \in \left[\frac{n}{n+1}, 1\right)$, then set $S = S_i$ and $m = -\lceil \sigma_i \rceil = -\lfloor \sigma_i \rfloor - 1$. It follows that

$$|m + \sigma_i| = | - \lfloor \sigma_i \rfloor - 1 + \lfloor \sigma_i \rfloor + \{\sigma_i\}| = |\{\sigma_i\} - 1| \leqslant \frac{1}{n+1}.$$

In the other cases, $\{\sigma_i\} \in \left[\frac{k}{n+1}, \frac{k+1}{n+1}\right)$ with $1 \leqslant k \leqslant n-1$ for each $i = 1, \ldots, n$. By the Box Principle, since there are $n$ numbers $\{\sigma_i\}, 1 \leqslant i \leqslant n$, and $n-1$ possible intervals containing them, one subinterval contains $\{\sigma_i\}$ and $\{\sigma_j\}$ for some $1 \leqslant i < j \leqslant n$.

Set $S = S_j \backslash S_i = \{x_{i+1}, \ldots, x_j\}$. Then

$$\sum_{s \in S} s = \sum_{s \in S_j} s - \sum_{s \in S_i} s = \sigma_j - \sigma_i = \lfloor \sigma_j \rfloor + \{\sigma_j\} - \lfloor \sigma_i \rfloor - \{\sigma_i\}.$$

Thus, if we set $m = \lfloor \sigma_i \rfloor - \lfloor \sigma_j \rfloor$, then

$$\left| m + \sum_{s \in S} s \right| = |\{\sigma_j\} - \{\sigma_i\}| < \frac{1}{n+1}.$$

□

**Lecture 7, Wednesday, October 13, 2021**

**Example 15** Given any five points on a sphere, show that some four of them must lie on a closed hemisphere.

(Two identical hemispheres are obtained by cutting the sphere by a plane passing through its center. The intersection of such a plane with the surface of the sphere is a circle called a great circle as its has the largest diameter among all the circles on the surface of the sphere.)

*Solution:* Let's denote the five points by $P_1, P_2, P_3, P_4$ and $P_5$.

If you divide the sphere into two equal hemisphere and then place the five points on the sphere, then all you can say, by the Box Principle, is that one closed hemisphere contains at least three points.

The difference here is that a choice can be made about the hemisphere. Before applying the Box Principle, one good idea is needed: consider a plane passing through the center of the sphere and two of the five given points, say through $P_1$ and $P_2$. This plane divides the sphere into two equal closed hemispheres.

By the Box Principle, two of the three points $P_3, P_4$ and $P_5$ must lie in the same closed hemisphere, which must then contain four of the five given points. □

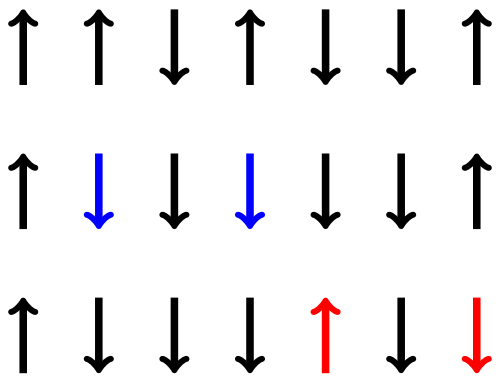
## 2 Invariants

One nice technique for solving mathematical problems is to seek quantities that do not change under certain transformations relevant to the problem in question. These quantities are called invariants. Of course, finding the proper invariant can be a challenging task. It can also happen that some quantity changes, but it does so always in the same way (e.g. it is always decreasing), in which case what is invariant is the way it changes and that quantity is then called a monovariant.

One basic invariant is the parity of an integer, that is, whether an integer is even or odd. The parity of the integer $N$ is essentially the same as its congruence class modulo 2. Talking about arithmetic modulo 2 may not be necessary when one is only interested in whether an integer is even or odd, but it suggests that replacing 2 by some other positive integer $n$ could perhaps, for some problems, lead to a new invariant, namely the congruence class of $N$ modulo $n$. Which integer $N$ to consider is not always obvious. Let us look at some examples to make this a bit more concrete.

**Example 1**: There are seven arrows drawn on a board, four pointing upwards and three pointing downwards. You can change the direction of the arrows, but only two at a time.

Is it possible to bring the seven arrows to all pointing upwards?

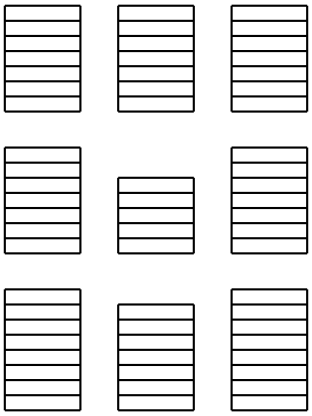


*Solution:* The answer is no. The reason is that the number $N$ of arrows pointing downwards is always odd: when changing the direction of two arrows, $N$ either increases by two, doesn't

change or deceases by two. For instance, if the direction of two arrows pointing upwards is changed, $N$ increases by two; if instead we change the direction of one arrow pointing upwards and one pointing downwards, then $N$ does not change.

It would also have been possible to take $N$ to be the number of arrows pointing upwards, which is always even. □

**Example 2**: Imagine now three piles of books with seven books in each pile. You can perform two operations: you can either remove two books from one pile, or you can add one book to each of two piles. Is it possible to remove all the books from the three piles?



*Solution:* Here, one could start by adding one book to each of the first two piles to make the number of books in each pile equal to eight. Then, by removing two books at a time from each pile, it will be possible to remove all those from the first two piles, but the third pile will remain with 7 books, which is odd. This doesn't prove that the answer to the question is no because there are other ways to proceed: one could start by removing books from the second column and then add one book to the second and the third column, etc.

The invariant to consider is the parity of the total number $N$ of books in the three piles. The first operation decreases $N$ by 2; the second operation increases it by 2. If $N$ is odd, then $N+2$ and $N-2$ are also odd; if $N$ is even, then $N+2$ and $N-2$ are also even. Since initially $N$ is odd ($N = 3 \cdot 7 = 21$), the total number of books in the three piles remains odd all the time. Therefore, it is impossible to reduce $N$ to zero. □

**Example 3**: The integers from 1 to 18 are written in a row on the board. Can you insert plus and minus signs between them in such a way as to get an expression that is equal to 0?

$$1 + 2 - 3 + 4 - 5 - 6 + \cdots + 16 - 17 + 18 = 0?$$

*Solution:* The answer is no. The invariant to consider here is the parity of the expression. It does not change whatever the signs are. Indeed, replacing $-a$ by $a$ changes the expression by $2a$, hence it does not change its parity (or just recall that $-a \equiv a \bmod 2$).

The parity of that expression is thus equal to the parity of the sum of all the integers from 1 to 18, which equals $\frac{18\cdot 19}{2}$, that is, 171:

$$1 + 2 + 3 + \cdots + 17 + 18 = \frac{18 \cdot 19}{2} = 171.$$

This number is odd, so the expression on the board is always odd, hence it can never equal zero. □

The following related problem was proposed and solved during class.

**Example 4**: Let $N$ be a positive integer and consider the sum

$$1 + 2 + 3 + \cdots + (N-1) + N$$

of all integers up to $N$. If this sum is odd, then the same argument as in Example 3 shows that it is not possible to change the signs to obtain a new expression equal to 0. If that sum is even, is it possible to change the signs as to obtain 0? The answer is yes. That sum is equal to $\frac{N(N+1)}{2}$, so if this number is even, then $\frac{N(N+1)}{2} = 2m$ for some $m \in \mathbb{Z}_{>0}$ and $N(N+1) = 4m$, so either $N$ is a multiple of 4 or $N+1$ is a multiple of 4. Let's consider these two cases separately.

Case 1: $N = 4k$ for some $k \in \mathbb{Z}_{>0}$. For any $j$ between 0 and $k-1$, consider the four consecutive integers $4j+1, 4j+2, 4j+3, 4j+4$ and the choice of signs

$$+(4j+1) - (4j+2) - (4j+3) + (4j+4).$$

Notice that this last expression is equal to 0. Therefore, so is the sum

$$\sum_{j=0}^{k-1}((4j+1) - (4j+2) - (4j+3) + (4j+4)),$$

which shows that it is possible to change the signs in $1 + 2 + 3 + 4 + \cdots + (N-3) + (N-2) + (N-1) + N$ to obtain 0.

Case 2: $N + 1 = 4k$ for some $k \in \mathbb{Z}_{>0}$. Then $N = 4k - 1 = 4(k-1) + 3$. As in Case 1, the signs in the sum $4 + 5 + \cdots + (N-1) + N$ can be changed so that the new sum equals 0: observe that the number of terms in this sum is $N - 3$, so equals $4(k-1)$ and is thus a multiple of 4. The following sum is zero:

$$4-5-6+7+\cdots+(N-3)-(N-2)-(N-1)+N = \sum_{j=0}^{k-1}(4j-(4j+1)-(4j+2)+(4j+3)) = 0.$$

As for the sum $1+2+3$, we can obtain 0 by changing the first two signs: $-1-2+3=0$. Therefore,

$$\begin{aligned}-1-2+3+4-5-6+7+\cdots+(N-3)-(N-2)-(N-1)+N \\ &= -1-2+3+\sum_{j=0}^{k-1}(4j-(4j+1)-(4j+2)+(4j+3)) \\ &= 0+0=0.\end{aligned}$$

**Lecture 8, Wednesday, October 20, 2021**

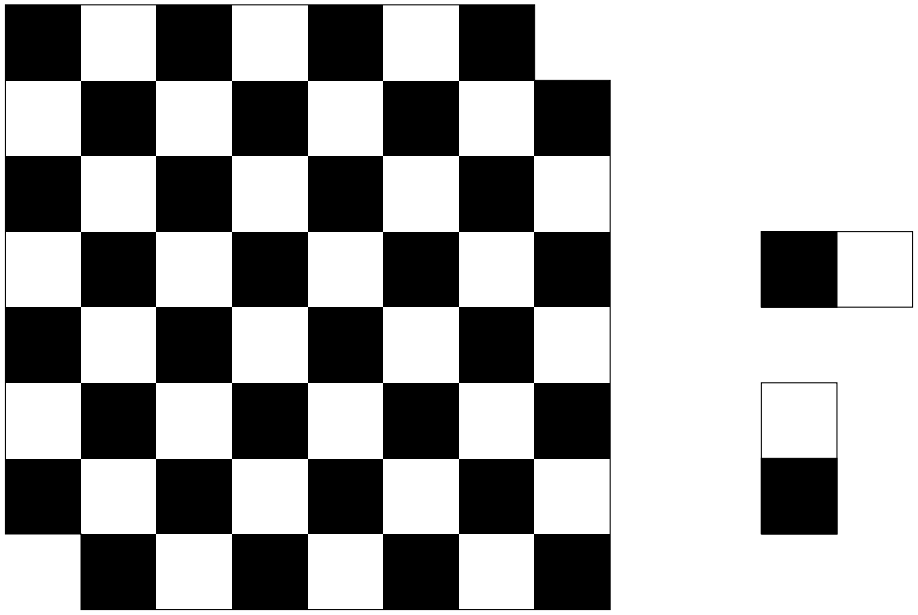
**Example 5**: The numbers 1, 2, . . . , 7 are written on a huge blackboard. A student has been condemned by his teacher to perform the following task: take any two numbers $a$ and $b$ and replace them by $a-b$. He has to repeat this until only one number remains on the blackboard. Can this last number be 3? If instead it's the integers $1, 2, \ldots, 13$ that are written on the board, can the last number be 2? If, initially, the numbers written on the blackboard are 1, 2, . . . , 2011, can the last number be 3?

*Solution:* The parity of the sum of all the numbers on the blackboard does not change, so the answer is no in all three cases. For instance, in the second case, the initial sum is equal to $\frac{13\cdot 14}{2}$, that is, 91, so it is odd and remains odd, hence it can never be equal to 2; in the third case, the initial sum is $\frac{2011\cdot 2012}{2}$, which equals $2011\cdot 1006$, and this last number is even because 1006 is even, so it can never equal 3. □

**Example 6**: Six stacks of coins are placed on a table. The first has 1 coin, the second 2 coins, and so on, until the last, which has 6 coins. You are allowed to select any two stacks and add one coin to each. Can you make all the stacks equal? You can repeat this operation as many times as you want.

*Solution:* The total number of coins on the six stacks is initially 21, hence odd. (Note that $1+2+3+4+5+6=\frac{6\cdot 7}{2}=21$.) Since adding two coins doesn't change the parity, the total number of coins is always odd. If the stacks are equal, since there are 6 of them, the total number of coins would have to be even, which is impossible. Therefore, the stacks can never become all equal. □

**Example 7**: Imagine that two opposite corner squares from a regular $8\times 8$ chessboard are removed. Explain why the remaining part cannot be covered by $2\times 1$ (or $1\times 2$) tiles (dominoes) of rectangular shape.



*Solution:* What can we say about the two squares which have been removed? They are of the same color. On a regular $8 \times 8$ chessboard, there are 64 squares, 32 white and 32 black. After removing two opposite corner squares, there will be left either 32 white and 30 black ones, or 30 white and 32 black ones.

How can this observation be used to answer the question? We need one more observation: wherever you place a $2 \times 1$ tile on the chessboard, whether it is horizontally or vertically, it always covers one white and one black square. If you place two tiles, they will cover two white and two black squares. In general, $n$ tiles will cover $n$ white squares and $n$ black squares.

To cover the remaining board, you need 31 tiles because there are 62 squares left. However, 31 tiles of size $2 \times 1$ will cover 31 white squares and 31 black squares, but the number of white and black squares which remain on the board is not the same. Therefore, it is impossible to cover the remaining chessboard using $2 \times 1$ tiles. If we want to use the language of invariants, we could argue in the following way: if $B$ is the number of black squares covered by $n$ tiles and $W$ is the number of white squares covered by $n$ tiles, then $B = W$ always; in other words, although $B$ and $W$ can change, the difference $B - W$ always equals 0. However, for the modified chessboard, the difference of the number of black and white squares is 2 (or $-2$). □

As a variation of the previous problem, consider the problem of covering by $2 \times 1$ or $1 \times 2$ rectangular tiles the shape obtained from a square of size $8\times$ by removing two $1 \times 1$ squares from two opposite corners. The solution is exactly the same, except that the first step would be to color that shape like a chessboard.

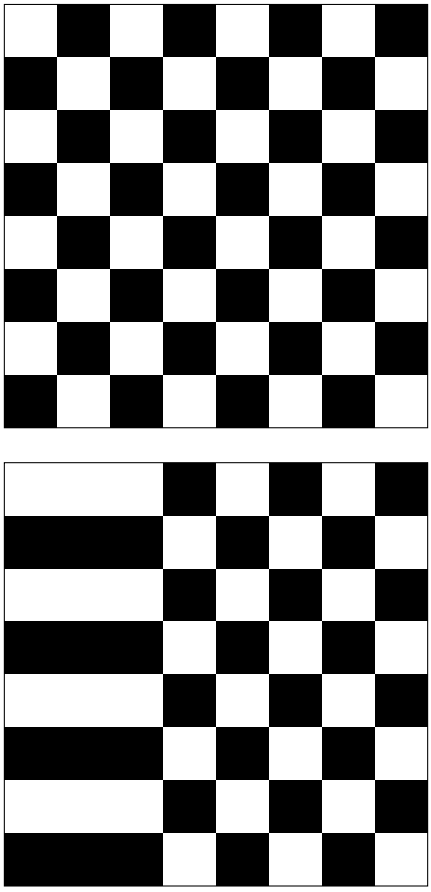
**Example 8**: Consider a regular $8 \times 8$ chessboard. Imagine a knight located at one corner

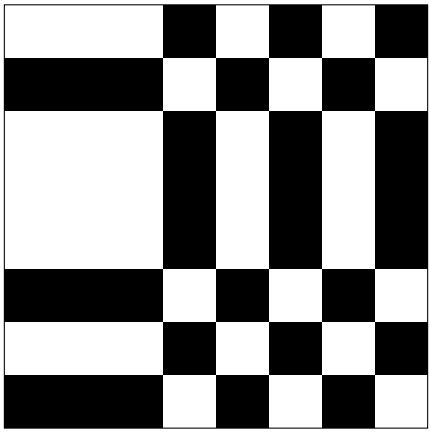
of a chessboard. Is it possible for the knight to move to the opposite corner of the board by passing once through all the squares?

*Solution:* If the knight starts on a white square and makes a move, it will land on a black square; if it starts on a black square, it will land on a white one. Therefore, the color of the square where the knight is located is not an invariant. However, what is always true is that, after an even number of moves, the knight will land on a square of the same color as the one he started on; after an odd number of moves, it will land on a square of a different color.

If it were possible for the knight to move from one corner to the opposite one by passing through all the squares only once, then this means that it would be able to reach the opposite corner after 63 moves, so the opposite corner would be of a color different from the initial one. However, this is not the case: opposite corners on a chessboard have the same color. □

**Example 9**: Consider a standard $8 \times 8$ chessboard. You are allowed to repaint all the squares on a row or column (so a black square becomes white and vice-versa), and you can repeat this operation. Can you obtain a chessboard with exactly one black square?





*Solution:* No, because the number of black squares is always even. If there are $B$ black squares and $W$ white squares on a given row (or column), then $B + W = 8$: this means that either $B$ and $W$ are both even or they are both odd. Therefore, after repainting all the squares on that row (or column), the number of black squares on that row (or column) will be $W$ instead of $B$, which have the same parity. This means that the parity of the total number of black squares on the whole chessboard does not change. Initially, there are 32 black squares on the chessboard, so there will always be an even number. □

**Lecture 9, Wednesday, October 27, 2021**

**Example 10**: A building is initially empty. Each minute, either one person enters the building or two people exit the building. Can there be 7 people in the building after 10 minutes? After 12 minutes? Can there be 10 people in the building after 18 minutes? Can there be $3^{2011} + 1$ people in the building after $3^{3000}$ minutes?

*Solution:* If 7 people enter the building, then two leaves, and afterwards two more enter, then there will be 7 people after 10 minutes. Or there could be 9 people entering the building during the first 9 minutes and 2 leaving at the $10^{th}$ minute.

The answer is no in the other cases. The change in the number of people in the building, from one minute to the next, is always congruent to 1 modulo 3. (It is either $+1$ or $-2$.) Therefore, after $t$ minutes, the number of people in the building is congruent to $t$ modulo 3. This implies that, after $3^{3000}$ minutes, the number of people in the building must be divisible by 3, hence cannot equal $3^{2011} + 1$.

Another way to say this is that if $N(t)$ is the number of people in the building after $t$ minutes, then $N(t) - t \equiv 0 \bmod 3$ for all $t \geqslant 0$, so the invariant is $N(t) - t$ modulo 3. □

A natural question related to the previous example is: what are the possible values for the number of people in the building at time $t$. This is a case where it is possible to list various possibilities for small values of $t$ and then make a conjecture about the answer to

that question. We always have $N(1) = 1$ and $N(2) = 2$, but $N(3)$ can be either 3 or zero. If $N(3) = 0$, then $N(4)$ can only be 1, but if $N(3) = 3$, then either $N(4) = 4$ or $N(4) = 1$. If $N(4) = 1$, then $N(5) = 2$, but if $N(4) = 4$, then either $N(5) = 5$ or $N(5) = 2$.

Continuing in this way suggests the following conjecture:

**Conjecture**: $N(t)$ can take any values of the form $t - 3k$ for some $k \in \mathbb{Z}_{>0}$ such that $0 \leqslant k \leqslant \lfloor \frac{t}{3} \rfloor$.

This conjecture can be proved by induction. From the paragraph above, we can see that it is true for a few small values of $t$. Assume that the conjecture is true after $t$ minutes. $N(t+1)$ either equals $N(t)+1$ or it equals $N(t)-2$. If $N(t) = t - 3k$ then, in the first case,

$$N(t+1) = N(t) + 1 = (t+1) - 3k;$$

in the second case,

$$N(t+1) = N(t) - 2 = t - 2 - 3k = (t+1) - 3(k+1).$$

This proves that $N(t+1)$ can take any values of the form $(t+1) - 3k$ for some $k \in \mathbb{Z}_{>0}$ such that $0 \leqslant k \leqslant \lfloor \frac{t+1}{3} \rfloor$.

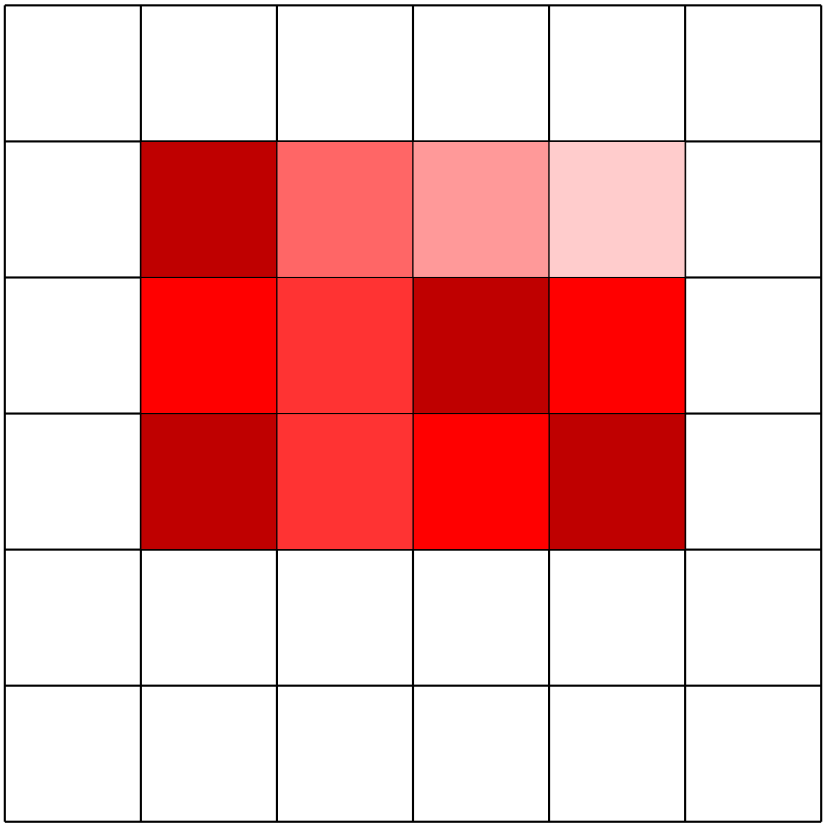
**Example 11**: In the parliament of Transoceania, each member has at most three enemies. Show how the house can be divided into two houses so that each member has at most one enemy in his or her own house.

*Solution:* Start with an arbitrary division and let $N$ be the total number of pairs of enemies which are in the same house. Perform the following operation: if member $A$ has at least two enemies in their own house, then $A$ switches to the other house where they have at most one enemy. After this operation, $N$ will have decreased by one, two or three. Since $N$ cannot be negative, we must reach a point when it is not possible anymore to perform that operation. This means that each member has at most one enemy in their own house. What is invariant here is the decreasing monotonicity of $N$. In other word, $N$ is a monovariant. □

**Lecture 10, Wednesday, November 3, 2021**

**Example 12**: (a) Imagine an array of $6 \times 6$ square cells. Initially, four cells are infected by some bacteria. After one minute, if a cell has exactly two infected neighbours, then it becomes infected also. (Two cells are neighbours if they have a side in common.) Can all the cells become infected?

*First solution:* When a new cell becomes infected, the perimeter of the infected area does not change: see the above diagram. Since initially this perimeter is at most 16, it can never become 24. □



*Second solution:* The left-most column that contains an infected cell is invariant, as so is the right-most column containing an infected cell. The same is true about rows. This means that, in order for all the cells to be infected, those rows and columns must be the first and last rows and columns of the $6 \times 6$ array. This can be achieved, for instance, with two infected cells at opposite corners. But then there should be a infected cells in the $2^{nd}$ and $5^{th}$ rows and columns, and one can see that the whole $6 \times 6$ array cannot become completely infected. There are a few cases to consider, but this argument can be made to work to show that the whole $6 \times 6$ array cannot become completely infected. □

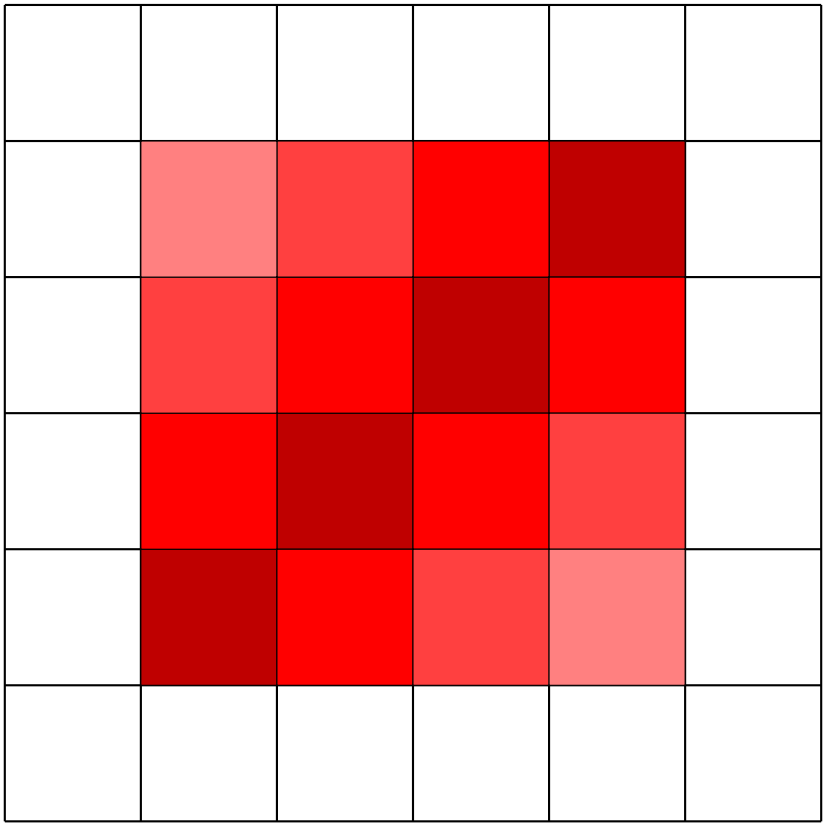
**Example 12**: (b) This problem is the same as in (a), but with "exactly two" replaced by "at least two".

*Solution:* When a new cell becomes infected, the perimeter of the infected area either does not change or decreases. It decreases when a cell has three or four neighbors, as can be seen on the diagram above. Since initially this perimeter is at most 16, it can never become 24. □

**Example 12**: (c) With the same rule as in either (a) or (b), what is the maximum number of cells that can become infected?

*Solution:* Let's assume that the infection process has stopped. Consider a connected component of the set of all infected cells: by connected, it is understood that each infected cell has a neighbor who is also infected. This connected component has to be a rectangle. Moreover, this rectangle has perimeter at most 16. The maximum number of infected cells occurs when the infected area is the largest. Given a fixed perimeter, the rectangle of maximal area with that perimeter is a square. This implies that the largest infected area of perimeter 16 is a $4 \times 4$ square. Therefore, the maximum number of infected cells is 16.

To complete the solution, we need to see if the maximum of 16 cells can be attained. This is indeed possible: start with 4 cells located on a diagonal, each cell sharing one or two corners with the other cells.



□

This example can be generalized: on a square array of $n \times n$ cells, with the same rule of infection as above, if there are initially $n-1$ infected cells, then there will always be at least one which remains uninfected. The same argument as above works since $4(n-1) = 4n-4 < 4n$. (The $6 \times 6$ grid above could thus be replaced by a $5 \times 5$ grid.)

**Example 13**: On the planet Functor lives a species of animals called eulers which can adopt one of three colors: red, blue and green. Initially, there are 7 red ones, 8 blue ones and 9

green ones. If two eulers of different colors meet, they both change to the third color. (If a red and a green one meet, they both become blue, etc.) Is it possible that, eventually, all the eulers will be of the same color? Is the answer the same if instead there are 9000 red ones, 9001 blue ones and 9002 green ones?

*First solution:* The answer is no in both cases. Let $R$ (respectively $B$, $G$) be the number of red (respectively, blue, green) eulers at a given time. The three possible colors for the eulers suggest that perhaps we should consider a certain number modulo 3. The values of $R$, $B$ and $G$ modulo 3 vary, but what does not change are the differences $R-B$, $R-G$ and $B-G$ modulo 3.

For instance, if a red and green eulers meet, then $B$ increases by 2 and $R$ and $G$ decrease by 1, so $R-B$ becomes $R-1-(B+2)$, that is, $R-B-3$, so $R-B$ does not change modulo 3. The same goes for $R-G$ and $B-G$. (In this case, $R-G$ does not change at all.) □

*Second solution:* The answer is no in both cases. Associate the number 0 to the red eulers, the number 1 to the blue ones and the number 2 to the green ones. Let $N$ be the sum of all the numbers associated to all the eulers, so $N = 0R + B + 2G$ where $R$ is the number of red eulers, $B$ is the number of blue ones and $G$ the number of green ones. When two eulers meet, the residue of $N$ modulo 3 does not change. Initially, $N \equiv 2 \bmod 3$, but if all the eulers were of the same color, then $N$ would have to be divisible by 3 because the total number of eulers is divisible by 3. □

**Example 14**: Consider the numbers $1, 2, \ldots, 100$ written on a blackboard. Every minute, a student erases any two numbers $a$ and $b$ and replaces them by $ab + a + b$. After 99 minutes, there will be only one number left. What is this number?

It is implicit in the statement of this problem that the last number does not depend on which numbers are erased and in which order. Let's see what happens when 100 is replaced by a smaller number $N$ and $N = 2, 3, 4, 5$.

Case $N = 2$: $1, 2 \rightsquigarrow 5$.

Case $N = 3$: $\underline{1}, 2, \underline{3} \rightsquigarrow 2, 7$; $\quad \underline{2}, \underline{7} \rightsquigarrow 23$.

Case $N = 4$: $1, \underline{2}, 3, \underline{4} \rightsquigarrow 1, 3, 14$; $\quad \underline{1}, \underline{3}, 14 \rightsquigarrow 7, 14$; $\quad \underline{7}, \underline{14} \rightsquigarrow 119$.

Case $N = 5$: $1, \underline{2}, 3, \underline{4}, 5 \rightsquigarrow 1, 3, 14, 5$; $\quad 1, \underline{3}, 14, \underline{5} \rightsquigarrow 1, 14, 23$; $\quad \underline{1}, 14, \underline{23} \rightsquigarrow 14, 47$; $\quad \underline{14}, \underline{47} \rightsquigarrow 719$.

From these cases, it if natural to conjecture that if 100 is replaced by $N$ and the same process as describe in Example 14 is applied, then the last number that remains is $(N+1)!-1$.

**Lecture 11, Wednesday, November 17, 2021**

*Solution:* The solution rests on the identity $ab + a + b = (a + 1)(b + 1) - 1$. Suppose that $a$ and $b$ have been replaced by $ab + a + b$. Now if $ab + a + b$ and $c$ are replaced by $(ab + a + b)c + (ab + a + b) + c$, notice that

$$(ab + a + b)c + (ab + a + b) + c = abc + ab + ac + bc + a + b + c = (a + 1)(b + 1)(c + 1) - 1.$$

What is an invariant is the general form of the new number written on the board: it is always of the form

$$(a_1 + 1)(a_2 + 1) \cdots (a_k + 1) - 1$$

where $\{a_1, a_2, \ldots, a_k\} \subset \{1, 2, \ldots, 100\}$.

It follows that the last remaining number is $101! - 1$. □

**Example 15**: Consider an $m \times n$ matrix $A$ with integral entries $a_{ij}$. You are allowed to change the signs of all the numbers in any row or column and you can repeat this operation as often as you want. Prove that you can reach a state where the sum of the entries in any row or column is non-negative.

*Solution:* Consider the sum $S$ of all the entries in the matrix. Apply the following operations in any order: if the sum of the entries in a row (or a column) is negative, change all the signs on that row (or column). Doing so will turn a negative sum along a row (or column) into a positive sum. Since $S$ is the sum of all the row sums (or column sums), the value of $S$ will then increase (by at least one since $S$ takes integral values). $S$ is thus a monovariant: it changes, but always in the same way.

Now the observation that is needed is that $S$ is bounded above by $\sum_{i=1}^{m} \sum_{j=1}^{n} |a_{ij}|$ (that is, $S \leqslant \sum_{i=1}^{m} \sum_{j=1}^{n} |a_{ij}|$) since, at any stage, it is equal to $\sum_{i=1}^{m} \sum_{j=1}^{n} (-1)^{?} a_{ij}$ for certains signs $(-1)^{?}$.

This implies that $S$ cannot always keep increasing. When this happens, the sum of the entries along any row or column of $A$ must be non-negative. □

**Example 16**: Consider 1000 integers written on a first row. The second row is obtained in the following way: under number $a$ in the first row is written $f(a)$, the number of times that $a$ occurs in the first row. The third row is then obtained in the same way, this time with the second row playing the role of the first. Prove that, eventually, all the rows become identical.

For instance, with 16 integers instead of 1000, we can obtain, for instance, the four rows below (and all those below the fourth one would be equal to the fourth one).

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 9 | 4 | 5 | 7 | 2 | 5 | 3 | 7 | 1 | 4 | 4 | 2 | 5 | 6 | 4 |
| 5 | 1 | 5 | 3 | 2 | 2 | 3 | 1 | 2 | 1 | 5 | 5 | 2 | 3 | 1 | 5 |
| 5 | 4 | 5 | 3 | 4 | 4 | 3 | 4 | 4 | 4 | 5 | 5 | 4 | 3 | 4 | 5 |
| 5 | 8 | 5 | 3 | 8 | 8 | 3 | 8 | 8 | 8 | 5 | 5 | 8 | 3 | 8 | 5 |

*Solution:* Consider the numbers $a_{1j}, a_{2j}, a_{3j}, \ldots$ in column $j$. Then $a_{2j} \leqslant a_{3j}$ and, in general, $a_{kj} \leqslant a_{k+1,j}$. The reason is that $a_{k-1,j}$ appears $a_{kj}$ times in row $k-1$, then $a_{kj}$ must appear at least the same number of times on the $k^{th}$-row. In follows that the numbers in column $j$ are non-decreasing, so they form a monovariant.

The second observation that is needed is that $1 \leqslant a_{ij} \leqslant 1000$ since no integer can occur more than 1000 times on a given row. It follows that, eventually, the numbers in each column must become constant. When this is true for all the columns, the rows do not change any more.

Although this is not needed for the solution, it can be observed that if the number $a$ appears $m$ times on the $k^{th}$-row with $k \geqslant 2$, then $m = ab$ for some integer $b \in \mathbb{Z}$. This is because if a column has entries $(c, a)$ in rows $k-1$ and $k$, then there is a total of $a$ columns with these same entries. This is also true if $c$ is replaced by another integer $d$. □

To end this section, here is a famous invariant which is useful to know for problem solving.

**Theorem 2.1** (Euler's Formula)**.** *Consider a connected graph drawn in the plane without any two edges intersecting except at a common vertex. Let $v$ be the number of vertices, $e$ the number of edges and $f$ the number of faces (including the infinite region outside of the graph). Then*

$$v - e + f = 2.$$

**Lecture 12, Wednesday, November 24, 2021**

# 3 Congruences modulo $n$

If you haven't seen congruences before and would like to learn a little bit about the subject, you can read about this topic and about $\mathbb{Z}_n$, the integers modulo $n$, in the document posted on eClass. Below is a little bit of information about them. What is needed to solve the problems in the example below will be added here.

**Definition 3.1.** *Let $a, b, n \in \mathbb{Z}$ and suppose that $n \geqslant 2$. $a \equiv b \bmod n$ means that $n$ divides $a - b$.*

**Definition 3.2.** *Given $a, n \in \mathbb{Z}$ with $n \geqslant 2$, the unique integer $r$ such that $0 \leqslant r \leqslant n-1$ and $a \equiv r \bmod n$ is called the residue of $a$ modulo $n$.*

**Theorem 3.3.** *If $a \equiv b \bmod n$ and $c \equiv d \bmod n$, then*

1. *$a + c \equiv b + d \bmod n$;*
2. *$ac \equiv bd \bmod n$.*

**Theorem 3.4.** *Let $a, b, n \in \mathbb{Z}, n > 1$ and set $d = \gcd(a, n)$. Then*

1. *The congruence equation $ax \equiv b \bmod n$ has solutions in $\mathbb{Z}$ if and only if $d \mid b$. (This notations means that $d$ divides $b$.)*
2. *If $d \mid b$, then the congruence equation $ax \equiv b \bmod n$ has $d$ distinct solutions in $0, 1, \ldots, n-1$.*

**Theorem 3.5** (Fermat's Little Theorem)**.** *$a^p \equiv a \pmod p$ if $p$ is prime.*

**Theorem 3.6** (Chinese Remainder Theorem)**.** *Suppose that $n_1, n_2, \ldots n_k$ are positive integers $> 1$ and $\gcd(n_i, n_j) = 1$ if $i \neq j$. For any integers $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, the system of congruence equations*

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \\ &\vdots \quad \vdots \qquad \vdots \\ x &\equiv a_k \bmod n_k \end{aligned}$$

*has a solution.*

**Lemma 3.7.** *If $x \in \mathbb{Z}$, then $x^2 \equiv 0$ or $1 \bmod 4$ and $x^2 \equiv 0, 1$ or $4 \bmod 8$.*

**Lemma 3.8.** *If $n \in \mathbb{N}$, then $n$ is congruent to the sum of its digits modulo 3 and modulo 9.*

**Definition 3.9** (Legendre symbol)**.** *Let $p$ be an odd prime number and $a \in \mathbb{Z}$, $a \neq 0$. If the congruence equation $x^2 \equiv a \bmod p$ has a solution, set $\left(\frac{a}{p}\right) = 1$; otherwise, set $\left(\frac{a}{p}\right) = -1$. It can be shown that*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

**Theorem 3.10** (Quadratic reciprocity)**.** *If $p$ and $q$ are distinct odd prime numbers, then*

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

Let's see some applications of congruences to answer questions from number theory.

**Example 1**: Prove that a multiple of 29 has 427 as its last three digits.

*Solution:* The last three digits of a multiple $29x$ of 29 is the residue modulo $1,000$ of $29x$. Indeed, if $29x = a_1 a_2 \cdots a_k 427$ where $a_1, a_2, \ldots, a_k$ are the other digits of $29x$, then

$$29x = a_1 a_2 \cdots a_k 000 + 427 = 1000b + 427$$

where $b = a_1 a_2 \cdots a_k$. The equality $29x = 1000b + 427$ shows that 427 is the residue modulo $1,000$ of $29x$.

Therefore, answering this question amounts to showing that the congruence equation

$$29x \equiv 427 \bmod 1,000$$

admits a solution. 29 does not divide 1,000 and is prime, so these two integers are relatively prime (that is, $\gcd(29, 1000) = 1$). It follows from Theorem 3.4 that the previous congruence equation admits a solution. □

**Example 2**: Give an explanation for why the equation $3x^2 - y^2 = 5$ does not admit a solution with $x, y \in \mathbb{Z}$.

*First solution:* If that equality holds in $\mathbb{Z}$, then the following congruence equation holds:

$$3x^2 \equiv y^2 \bmod 5.$$

Setting $x = 0, 1, 2, 3, 4$ shows that

$$3x^2 \equiv 0, 3 \text{ or } 2 \bmod 5$$

whereas setting $y = 0, 1, 2, 3, 4$ shows that

$$y^2 \equiv 0, 1 \text{ or } 4 \bmod 5.$$

(For instance, if $x = 3$, then $3x^2 \equiv 27 \equiv 2 \bmod 5$.) The congruence equation

$$3x^2 \equiv y^2 \bmod 5$$

can thus only hold when $3x^2 \equiv 0 \bmod 5$ and $y^2 \equiv 0 \bmod 5$, that is, when $x \equiv 0 \bmod 5$ and $y \equiv 0 \bmod 5$. This means that 5 divides both $x$ and $y$, hence 25 divides $x^2$ and $y^2$, but this is not possible since $3x^2 - y^2$ would then be a multiple of 25. □

*Second solution:* If the equality $3x^2 - y^2 = 5$ holds in $\mathbb{Z}$, then the following congruence equation holds:

$$3x^2 - y^2 \equiv 1 \bmod 4.$$

Equivalently, after multiplying by 3,

$$x^2 + y^2 \equiv 3 \bmod 4.$$

Setting $x, y = 0, 1, 2, 3$ shows that $x^2 \equiv 0$ or $1 \bmod 4$ and $y^2 \equiv 0$ or $1 \bmod 4$. (For instance, if $x = 2$, then $x^2 \equiv 4 \equiv 0 \bmod 4$.) The congruence equation

$$x^2 + y^2 \equiv 3 \bmod 4$$

does not have a solution since

$$x^2 + y^2 \equiv 0, 1 \text{ or } 2 \bmod 4.$$

□

**Example 3** ("Fermat's Very Little Theorem"): Show that if

$$x^3 + y^3 = z^3$$

for some integers $x, y, z$, then at least one of $x, y, z$ is a multiple of 7.

*Solution:* If the equality $x^3 + y^3 = z^3$ holds, then we also have the following congruence equation:

$$x^3 + y^3 \equiv z^3 \bmod 7.$$

Giving $x$ the value $0, 1, 2, 3, 4, 5, 6$ (or, equivalently, the values $0, 1, 2, 3, -3, -2, -1$), it can be checked that

$$x^3 \equiv 0, 1, -1 \bmod 7.$$

Case 1: $z^3 \equiv 0 \bmod 7$. This means that $z$ is a multiple of 7 and we are done.

Case 2: $z^3 \equiv 1 \bmod 7$. Then $x^3 + y^3 \equiv z^3 \equiv 1 \bmod 7$. Moreover, $x^3 \equiv 0, 1$ or $-1 \bmod 7$ and $y^3 \equiv 0, 1$ or $-1 \bmod 7$: the only combinations of these numbers that sum up to 1 modulo 7 are 1 and 0. Therefore, either

$$x^3 \equiv 0 \bmod 7 \text{ and } y^3 \equiv 1 \bmod 7$$

in which case $x$ is a multiple of 7, or

$$x^3 \equiv 1 \bmod 7 \text{ and } y^3 \equiv 0 \bmod 7,$$

in which case $y$ is a multiple of 7.

Case 3: $z^3 \equiv -1 \bmod 7$. This is entirely similar to case 2 with 1 replaced by $-1$. □

**Example 4**: Prove that an integer of the form $111\cdots1$ (that is, with all digits equal to 1) is never a square.

*Solution:* The idea here is to consider this number modulo 4 and use the fact that if $x \in \mathbb{Z}$, then $x^2 \equiv 0$ or $1 \bmod 4$.

If $k \geqslant 2$, then 4 divides $10^k$ since $2 \mid 10$. Therefore,

$$111\cdots1 = 10^n + 10^{n-1} + 10^{n-2} + \cdots + 100 + 10 + 1 \equiv 10 + 1 \equiv 3 \bmod 4.$$

Since $111\cdots1 \equiv 3 \bmod 4$, this number cannot be the square of an integer. □

**Example 5**: Prove that there is no power of 2 whose decimal expansion ends with 228.

*Solution:* Suppose that the decimal expansion of $2^n$ ends with 228. Then $2^n = 1000a + 228$ for some $a \in \mathbb{Z}$ and

$$2^n \equiv 228 \bmod 8.$$

This is a contradiction since $2^n \equiv 0 \bmod 8$ when $n \geqslant 3$ whereas

$$228 \equiv 200 + 28 \equiv 28 \equiv 4 \bmod 8.$$

□

**Lecture 13, Wednesday, December 1, 2021**

**Example 6**: The number $2^{29}$ consists of exactly 9 decimal digits and they are all distinct. This means that one of the digits $0, 1, 2, \ldots, 9$ is missing. What is this digit?

*Solution:* Denote by $x$ the missing digit. The sum of the digits of $2^{29}$ is thus

$$1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 - x = \frac{9 \cdot 10}{2} - x = 45 - x.$$

By Lemma 3.8, it follows that

$$2^{29} \equiv 45 - x \equiv -x \bmod 9. \tag{3}$$

To determine $x$, it is enough to determine $2^{29}$ modulo 9, as long as $x \neq 0, 9$.

$2^3 = 8 = 9 - 1$, so $2^3 \equiv -1 \bmod 9$ and

$$2^{27} = (2^3)^9 \equiv (-1)^9 \equiv -1 \bmod 9.$$

It follows that

$$2^{29} = 2^{27} \cdot 2^2 \equiv (-1) \cdot 4 \equiv -4 \bmod 9. \tag{4}$$

We can now conclude from (3) and (4) that $x = 4$. □

**Example 7**: Show that the equation

$$x^2 + y^2 + z^2 = 2xyz$$

has no solutions in $\mathbb{Z}$ except $x = 0$, $y = 0$ and $z = 0$.

*Solution:* Suppose that $x^2 + y^2 + z^2 = 2xyz$ and $x, y, z$ are not all 0. Then $x^2 + y^2 + z^2 \equiv 0 \bmod 2$. Therefore, either

- $x \equiv 0 \bmod 2$, $y \equiv 0 \bmod 2$ and $z \equiv 0 \bmod 2$, or

- one of $x, y, z$ is $\equiv 0 \bmod 2$ and the other two are $\equiv 1 \bmod 2$.

In the first case, $x = 2x_1$, $y = 2y_1$ and $z = 2z_1$ for some $x_1, y_1, z_1 \in \mathbb{Z}$. Substituting into $x^2 + y^2 + z^2 = 2xyz$ gives

$$4x_1^2 + 4y_1^2 + 4z_1^2 = 2 \cdot 8 \cdot x_1 y_1 z_1.$$

The previous equation simplifies to

$$x_1^2 + y_1^2 + z_1^2 = 4 \cdot x_1 y_1 z_1.$$

The same argument as above shows that either $x_1, y_1, z_1$ are all even, or one is even and the other two are odds. If they are all even, then $x_1 = 2x_2$, $y_1 = 2y_2$ and $z_1 = 2z_2$ for some $x_2, y_2, z_2$ and it follows that

$$4x_2^2 + 4y_2^2 + 4z_2^2 = 4 \cdot 8 \cdot x_2 y_2 z_2,$$

hence

$$x_2^2 + y_2^2 + z_2^2 = 8x_2 y_2 z_2.$$

Continuing to argue in the same way, we will eventually reach a point where we have integers $x_k, y_k, z_k$ such that

$$x_k^2 + y_k^2 + z_k^2 = 2 \cdot 2^k x_k y_k z_k$$

and one of $x_k, y_k, z_k$ is even while the other two are odd. (Here, the assumption that $x, y$ and $z$ are not all zero is needed.)

To simplify the notation, let's denote $x_k, y_k, z_k$ by $a, b, c$. We are thus reduced to showing that the equation

$$a^2 + b^2 + c^2 = 2^{k+1} abc$$

does not have a solution with $a, b, c \in \mathbb{Z}$, when only one of $a, b, c$ is even and $k \geqslant 0$.

Without loss of generality, suppose that $a$ is even and $b, c$ are odd. Then $a^2 \equiv 0 \bmod 4$, $b^2 \equiv 1 \bmod 4$ and $c^2 \equiv 1 \bmod 4$, so

$$a^2 + b^2 + c^2 \equiv 1 + 1 \equiv 2 \bmod 4.$$

However, if $a = 2\widetilde{a}$ with $\widetilde{a} \in \mathbb{Z}$, then

$$2^{k+1} abc \equiv 2^{k+1} \cdot 2\widetilde{a}bc \equiv 0 \bmod 4.$$

The last two congruences are in contradiction with $a^2 + b^2 + c^2 = 2^{k+1} abc$. Therefore, the initial assumption that $x, y, z$ are not all 0 must be rejected, so the only solution of the original equation $x^2 + y^2 + z^2 = 2xyz$ is the zero solution. □

**Example 8**: Imagine a square billiard table with sides of length 2 meters. A ball placed in the centre of the table is hit and starts travelling around the table, bouncing off the walls of the tables until it lands into one of the four cups located at the corners of the table.

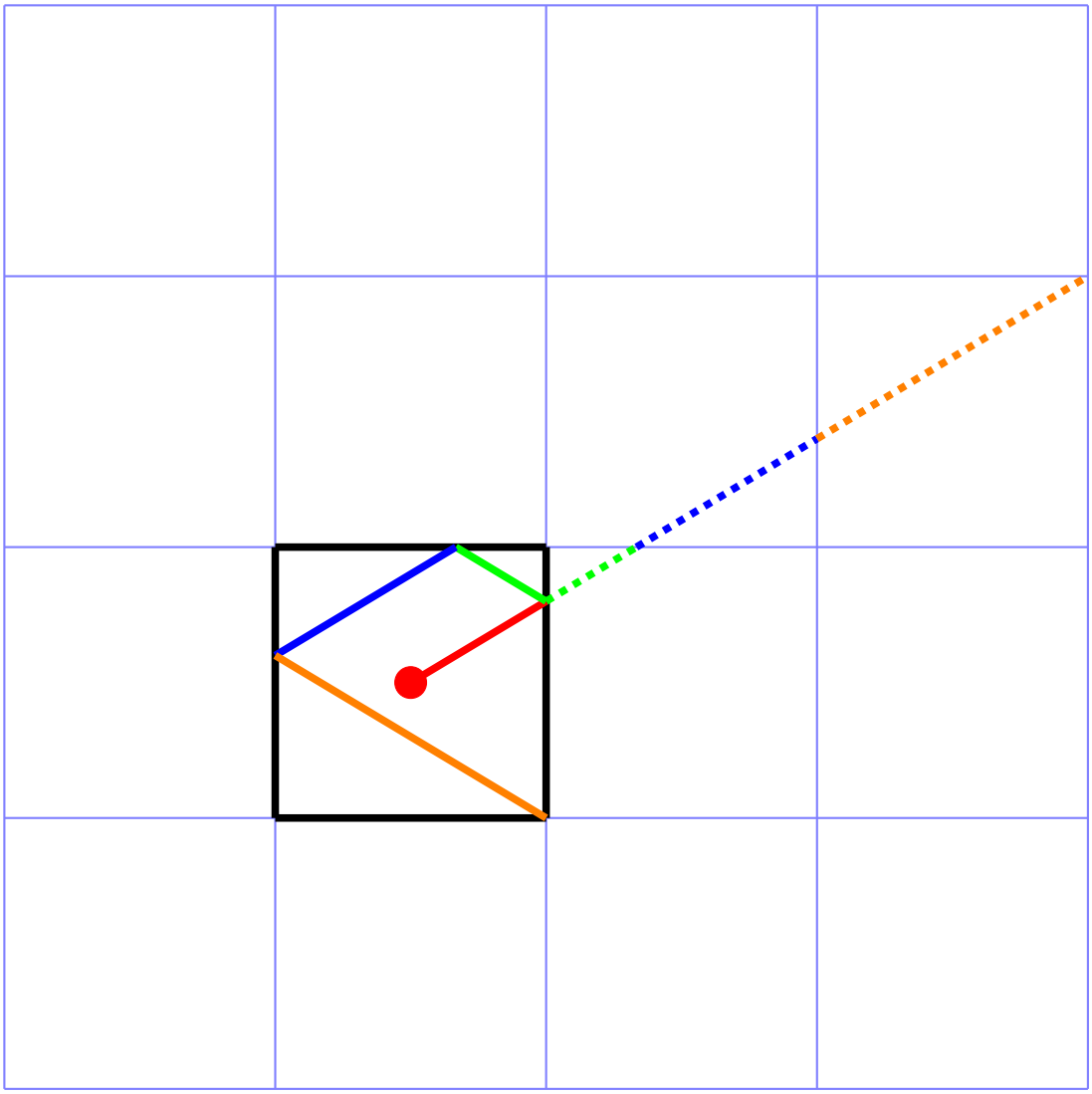
Prove that the distance travelled by that ball is not an integral number of meters.

*Solution:* This problem requires one truly original idea. It is also really intriguing that the answer to such a geometric question relies on congruences.

Imagine that the square billiard table is located in a very big room (as big as needed). This room has a standard coordinate system and the lines $x = a$ and $y = b$ are visible when $a$ and $b$ are odd. These lines form a grid in the room. Imagine that the center of the billiard table is the origin, so the sides of the tables are along the lines $x = 1, x = -1, y = 1$ and $y = -1$. See the diagram on the next page.

The original idea that is needed is the following. Imagine that, besides the physical ball that is bouncing off the walls of the table, there is also a ghost ball which starts travelling from the center of the table in the same direction as the physical ball but which simply goes through the walls of the table and continues travelling in the same direction. Assume that it travels at the same speed as the physical ball.

The physical ball hits a vertical side (respectively, a horizontal side) of the table exactly when the ghost ball reaches a line $x = a$ (respectively, $y = b$) because they travel at the same speed. It follows that the physical ball lands in one of the four cups exactly when the ghost ball reaches a visible point of intersections of the visible coordinate lines. Such a point has integral coordinates $(a, b)$ with $a$ and $b$ odd integers. The distance travelled by the physical ball is then the same as the distance travelled by the ghost ball between the center of the table located at $(0, 0)$ and the point $(a, b)$. This distance is $\sqrt{a^2 + b^2}$. However, since $a$ and $b$ are odd, $a^2 + b^2 \equiv 1 + 1 \equiv 2 \bmod 4$, so $a^2 + b^2$ is not equal to $c^2$ for any integer $c$ according to Lemma 3.7.



□