TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

E-320: Teaching Math with a Historical Perspective **O. Knill, 2010-2022**

Lecture 1: Mathematical roots

1.1. The organization of knowledge is a **taxonomy problem**. Early approaches to sort things out were the **canons of rhetoric** with memory, invention, delivery, style, and arrangement or the **liberal arts and sciences** which combined the **trivium**: grammar, logic and rhetoric with the **quadrivium**: arithmetic, geometry, music, and astronomy. Taxonomies are often historically grown and motivated.

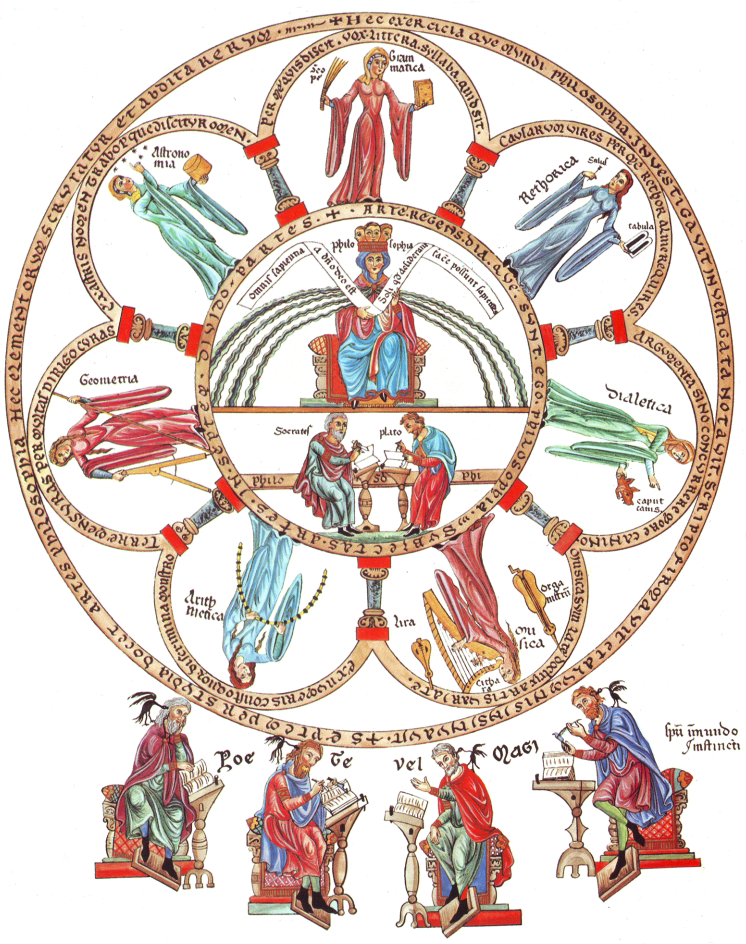


FIGURE 1. "Philosophia at septem artes liberales" (Philosophy within the seven liberal arts and sciences) by Herrad of Landsberg (1125-1195), an 12'th century abbess at the castle of Landsberg. The picture is in the public domain and part of her work "Hortus deliciarum" (Garden of delights).

1.2. A more human-centric approach appears in the **eight ancient roots of mathematics**. It is based on **practical tasks** from daily life. Each of the eight activities is paired with a key area

in mathematics:

counting and sorting	**arithmetic**
spacing and distancing	**geometry**
positioning and locating	**topology**
surveying and angulating	**trigonometry**
balancing and weighing	**statics**
moving and hitting	**dynamics**
guessing and judging	**probability**
collecting and ordering	**algorithms**

1.3. Modern mathematics has grown into a rather sophisticated building. Modern classification systems split math into about 100 subfields. To morph the above 8 roots into more modern mathematical areas, we complemented the ancient roots with calculus, numerics and computer science, merge trigonometry with geometry, separate arithmetic into number theory, algebra and arithmetic and turn statics into analysis. Let us call this more modern but still rather arbitrary adaptation the **12 modern roots of Mathematics**:

counting and sorting	**arithmetic**
spacing and distancing	**geometry**
positioning and locating	**topology**
dividing and comparing	**number theory**
balancing and weighing	**analysis**
moving and hitting	**dynamics**
guessing and judging	**probability**
collecting and ordering	**algorithms**
slicing and stacking	**calculus**
operating and memorizing	**computer science**
optimizing and planning	**numerics**
manipulating and solving	**algebra**

1.4. While relating **mathematical areas** with **human activities** is useful, it makes sense to also select specific topics in each of this area. Indeed, any of the subjects has grown itself to a large tree itself. For our course, we will select from each of the 12 topics to build a lecture.

Arithmetic	numbers and number systems
Geometry	invariance, symmetries, measurement, maps
Number theory	Diophantine equations, factorizations
Algebra	algebraic and discrete structures
Calculus	limits, derivatives, integrals
Set Theory	set theory, foundations and formalisms
Probability	combinatorics, measure theory, statistics
Topology	polyhedra, topological spaces, manifolds
Analysis	extrema, estimates, variation, measure
Numerics	numerical schemes, codes, cryptology
Dynamics	differential equations, iteration of maps
Algorithms	computer science, artificial intelligence

1.5. Like any classification, also this division is rather arbitrary and a matter of personal preferences. The **MCC 2020 AMS classification** distinguishes 63 main areas of mathematics. Many of them are broken off into even finer pieces. Additionally, there are fields which relate with other areas of science, like economics, biology or physics:

00 General
01 History and biography
03 Mathematical logic and foundations
05 Combinatorics
06 Lattices, ordered algebraic structures
08 General algebraic systems
11 Number theory
12 Field theory and polynomials
13 Commutative rings and algebras
14 Algebraic geometry
15 Linear algebra; matrix theory
16 Associative rings and algebras
17 Non-associative rings and algebras
18 Category theory, homological algebra
19 K-theory
20 Group theory and generalizations

22 Topological groups, Lie groups
26 Real functions
28 Measure and integration
30 Functions of a complex variable
31 Potential theory
32 Several complex variables, analytic spaces
33 Special functions
34 Ordinary differential equations
35 Partial differential equations
37 Dynamical systems and ergodic theory
39 Difference and functional equations
40 Sequences, series, summability
41 Approximations and expansions
42 Fourier analysis
43 Abstract harmonic analysis
44 Integral transforms, operational calculus
45 Integral equations
46 Functional analysis
47 Operator theory
49 Calculus of variations, optimization
51 Geometry
52 Convex and discrete geometry
53 Differential geometry
54 General topology
55 Algebraic topology
57 Manifolds and cell complexes
58 Global analysis, analysis on manifolds
60 Probability theory, stochastic processes
62 Statistics
65 Numerical analysis
68 Computer science
70 Mechanics of particles and systems

74 Mechanics of deformable solids
76 Fluid mechanics
78 Optics, electromagnetic theory
80 Classical thermodynamics, heat transfer
81 Quantum theory
82 Statistical mechanics, structure of matter
83 Relativity and gravitational theory
85 Astronomy and astrophysics
86 Geophysics
90 Operations research, Programming
91 Game theory, Economics
92 Biology and other natural sciences
93 Systems theory and control
94 Information, communication, circuits
97 Mathematics education

1.6. One can also try to dissect the body of mathematics alone property lines. A good start is to look at arcs which measure **fancy developments** in mathematics. Michael Atiyah identified in the year 2000 the following **six arcs**:

local	and	global
low	and	high dimension
commutative	and	non-commutative
linear	and	nonlinear
geometry	and	algebra
physics	and	mathematics

1.7. Also this choice is of course highly personal. One could easily add 12 other **polarizing** quantities which help to distinguish or parametrize different parts of mathematical areas. The use of ambivalent pairs can be used to slice through the different areas:

regularity	and	randomness
integrable	and	chaotic
invariants	and	perturbative
experimental	and	deductive
polynomial	and	exponential
applied	and	abstract

discrete	and	continuous
existence	and	construction
finite dim	and	infinite dim
topological	and	differential geometric
practical	and	theoretical
axiomatic	and	example based

1.8. An other possibility to refine the fields of mathematics is to **combine** different areas. Examples are **probabilistic number theory**, **algebraic geometry**, **numerical analysis**, **geometric number theory**, **numerical algebra**, **algebraic topology**, **geometric probability**, **algebraic number theory**, **dynamical probability = stochastic processes**. Almost every pair is has become an actual field.

1.9. Finally, let us try to give a short answer to the question: What is Mathematics?

Mathematics is the science of structure.

1.10. The simplicity of this definition is intended. As soon as we include more topics, we actually exclude other topics. "Structure" is a good word, because mathematics is built by them. Examples are algebraic structures, order structures, topological structures, measure theoretical structures or combinations of such structures. For example, one can let algebraic structures act on topological structures leading, a combination which appears in dynamical systems theory or in geometric group theory. Definitions, theorems and examples form a linguistic structure: the definitions fix the vocabulary, the theorems fix a grammar and examples are the novels written. The structure of all of mathematics is a structure too and today often described using language from category theory.

1.11. The goal is to illustrate some of these structures from a historical point of view. Each week, an other topic will be covered. Every week is a new start. Our focus is historical. By doing so we also learn a great deal about how mathematics is learned. One of the key insights we have in education is that the difficulties of the pioneers developing some new material is often mirrored today, when we learn the material. Understanding how learning works is not only important for teachers it is also important for students of mathematics. And history is not only fun, it provides key insight on how mathematics works and provides us with lessons how we might want to proceed and reevaluate.

1.12. This document has evolved over a decade now. It is the 11th time now, this course is taught here at the Harvard extension school.

Oliver Knill, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022

Lecture 1: The Mathematics of Mazes

0 In the first lecture, we discuss a topic with historical and artistic connections. It is the **mathematics of mazes**. Since 2010, when this course was run the first time, we have chosen for the first lecture a topic which is somehow connected to all of mathematics but also relates to research interests of myself at the time. This year, we look at the mathematics of mazes. [1]

1 Informally, a **maze** is a network G of **paths** in a background network K. The obstacles are **hedges** or **walls** G'. We also are given two points A, B in K. The problem is to get from A to B on G without crossing G'. A **labyrinth** is a maze in which G is not branched. The first figure shows an example of a maze. The background graph is a **grid path**. Take a square ruled paper and you have a grid graph! What we have first drawn out is G. The complement G' can be identified by line segments which can not be crossed. Try to find a way from A to B within G. The solution is shown in the second picture. The third picture shows that the complement G' of a maze. Instead of using the complementary edges G in K, we draw the walls perpendicular to them, forming so the obstacles. It is an amazing phenomenon that if you tie together all exits the of G' to a new node, you again get a maze.

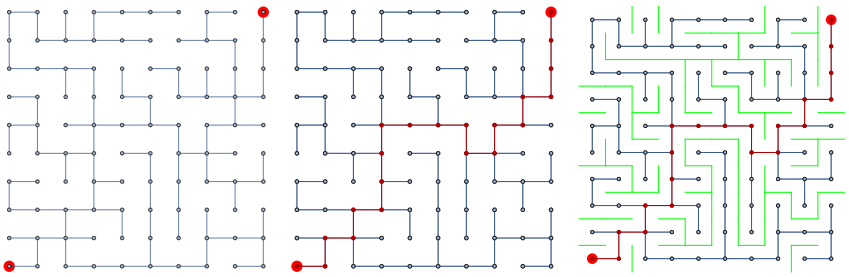


Figure 1: A 10×10 maze is a spanning tree G in a graph K. Here K is a 10×10 grid graph. The solution is a path from A to B. The third picture shows the dual G' consisting of hedges. If all exit paths are tied to a point, this is a again a tree.

2 Before getting to the **mathematics** of mazes, let us look a bit about the **history** and **culture** of mazes. The first "textbook maze" we know is a **Pylos clay tablet** created 1200 BC. Larger mazes have appeared earlier even, as they were used as **architectural tools**, for landscaping or decoration. In pure mathematics, mazes relate to rather serious topics. One principle is the **Jordan curve theorem** which tells that a closed curve in the plane has an interior and exterior. This theorem assures that if the complement of a planar maze contains a non-trivial closed loop, then the dual maze is not connected. Directly related to mazes is also the **Euler polyhedron formula** $V - E + F = 2$, relating the number of vertices, edges and faces of a **polyhedron**. I myself encountered mazes when looking at a quantity called **analytic torsion** which is a rational number defined by an arbitrary **network**.

[1] This document was last updated January 25th 2022.

3 The **lost labyrinth of Egypt** of **Hawara** is located about 80 km south of Cairo. It was built around 1800 BC by pharaoh **Amenemhet III**. The construction was completed by his daughter **Neferuptah**, whose sister **Sobekneferu** was one of the few women that ruled Egypt. According to **Herodots** (who lived 484-425 BC) the **Labyrinth of Minos** featured 3000 rooms in a funeral complex below the pyramid. Based on such descriptions, the Jesuit scholar **Athanasius Kircher** created in 1670 a copper plate picture of the now destroyed labyrinth. About 200 years ago, Egyptologist **Flinders Petrie** discovered the foundations and in 2008, the **Mathara expedition** found more evidence. Just because so much is still unknown, **Egypt's lost labyrinth** has remained an attractive mystery.

4 Labyrinths appear all over the world: examples are the **Labyrinth of the Chartres Cathedral** in France which dates back to 1205, the **11 circuit labyrinth** in San Francisco, the **Damme Priory** in Germany, **the Edge** in South Africa, the **Dunure Castle** in Scotland from the 13th century or the **Old Qing Dynasty Summer Palace** in Beijing or the Gardens shopping mall in Dubai. At Harvard, there is a maze at the **divinity school** located at 45 Museum street.

5 Why are mazes so attractive? It is not only the task of **solving puzzles** within architecture or landscaping, labyrinths were used for **contemplation** and **meditation**. In a religious setting, it a symbol for the human journey. The metaphor is that you can not get from A to B directly. Reaching a goal often happens with detours and passing through dead ends. Mazes also appear in **pop culture**. Early literature cameos are in Greek mythology with **Theseus killing the Minotaur**. You might remember also the **tri-wizard maze** in Harry Potter and the Goblet of Fire or the iconic last scene in Stanley Kubrics **Shining**. A more recent movie is the dystopian science fiction movie trilogy **Maze runner**.

6 The next figure shows a more challenging maze. Mathematically G was generated by producing a random spanning tree in a grid graph K. Only **one line of code** in a modern computer algebra system (here Mathematica) is needed to draw such a random maze:

```
n=30;K=GridGraph[{n,n}];G = Graph[FindSpanningTree[Graph[K,
    EdgeWeight->Table[Random[],{Length[EdgeList[K]]}]]]]
```

This allows us to randomly generate many mazes. By the way, we can exactly compute how many mazes there are of a given geometry. The **matrix tree theorem** gives us in the case of 10×10 mazes already 569431900407909779595721572576532837171200 0 different mazes! For 15×15 mazes already there are more than 10^{100} different mazes which can be realized. Also only **one line code** is needed to draw the solution from node 1 attached to $(1, 1)$ to node 1600 attached at $(40, 40)$. The second part of figure 1 was generated as such.

```
HighlightGraph[G,PathGraph[FindShortestPath[G,1,n^2]]]
```

7 Now try to solve the following maze in Figure 2. You might want to print it (or even better) load it onto an drawing app on a tablet or computer and search for the path. You can also solve the classical mazes shown in Figure 3, Figure 4 (we did that in class) or the central maze in Figure 5.

9 Mathematically, it is convenient to look at the maze as a finite structure. We define a maze G as a **spanning tree** embedded in a planar graph $K = (V, E)$. The **vertices** V are locations and E are the **edges** of the graph. For the mazes in Figure 1 or 2, the background graph is a rectangular grid like a square ruled paper. Since K is drawn on a plane it is called a **planar**

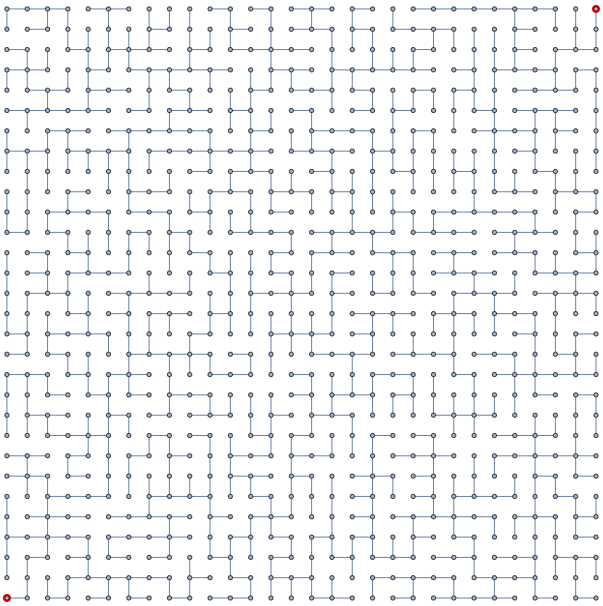


Figure 2: Solve this 30×30 maze by finding a path from A to B. It is now already more challenging to find a path.

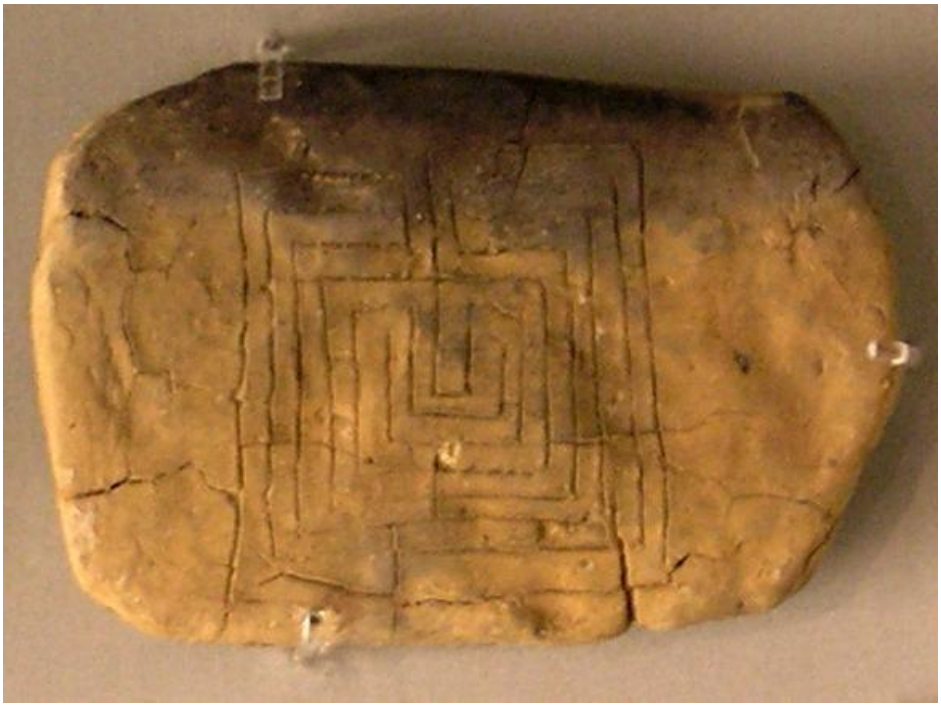


Figure 3: The clay tablet from King Nestor's palace of Pylos representing a classical labyrinth. The Mycenaean palace of Pylos was destroyed by fire around 1200 BC, which accidentally baked the tablet.

Figure 4: The Labyrinth in the Notre-Dames of Chartres was built in 1215. With a diameter of 12.85 meters, it is the largest church's labyrinth constructed in the middle ages. This is a labyrinth, not a maze. Its complement however is a maze.

graph. You can create the maze G by tracing out line segments in K making sure that you reach every crossing V but never produce a closed path. The mazes in Figures 1,2,3 are of this form.

10 It is a crucial assumption to have G a **tree**, meaning that we do not allow maze runners to run in circles. For the purpose of the **maze theorem** discussed below, this is needed. First, we proved the following in class by induction:

> **Tree lemma:** The number vertices minus the number of edges in a tree is 1.

To see this, we know it is true for a tree with two vertices and one edge. Now, whenever you add an other edge, we also add an other vertex. You can build a formal induction proof yourself. You can also see why it is wrong when we allow circles as then we have an opportunity to add an edge without adding an other vertex.

10 To see a planar maze as part of a sphere, just take the outside of the maze and consider it with an additional point. All the paths going to the outside of the maze are attached to this. Now G is a spanning tree in a graph K embedded in a sphere. The graph K divides the sphere into **faces**. In the case of your ruled paper, the faces are all squares. The dual graph K' has as vertices the faces of K. Two faces are connected if they intersect in an edge of K.

11 An important principle which has been seen already in antiquity is the **duality principle**. The dual of K is an other graph K' in which the facets are the vertices and two are connected if they intersect in an edge of K. One has seen that first for polyhedra. If K is the graph of the **cube**, then K' is the graph of the **octahedron**. If K is the graph of the **icosahedron**, then K' is the graph of the **dodecahedron**. Every polyhedron K has a dual polyhedron K' in which the faces F of K are the vertices and where two are connected if they intersected in an edge E.

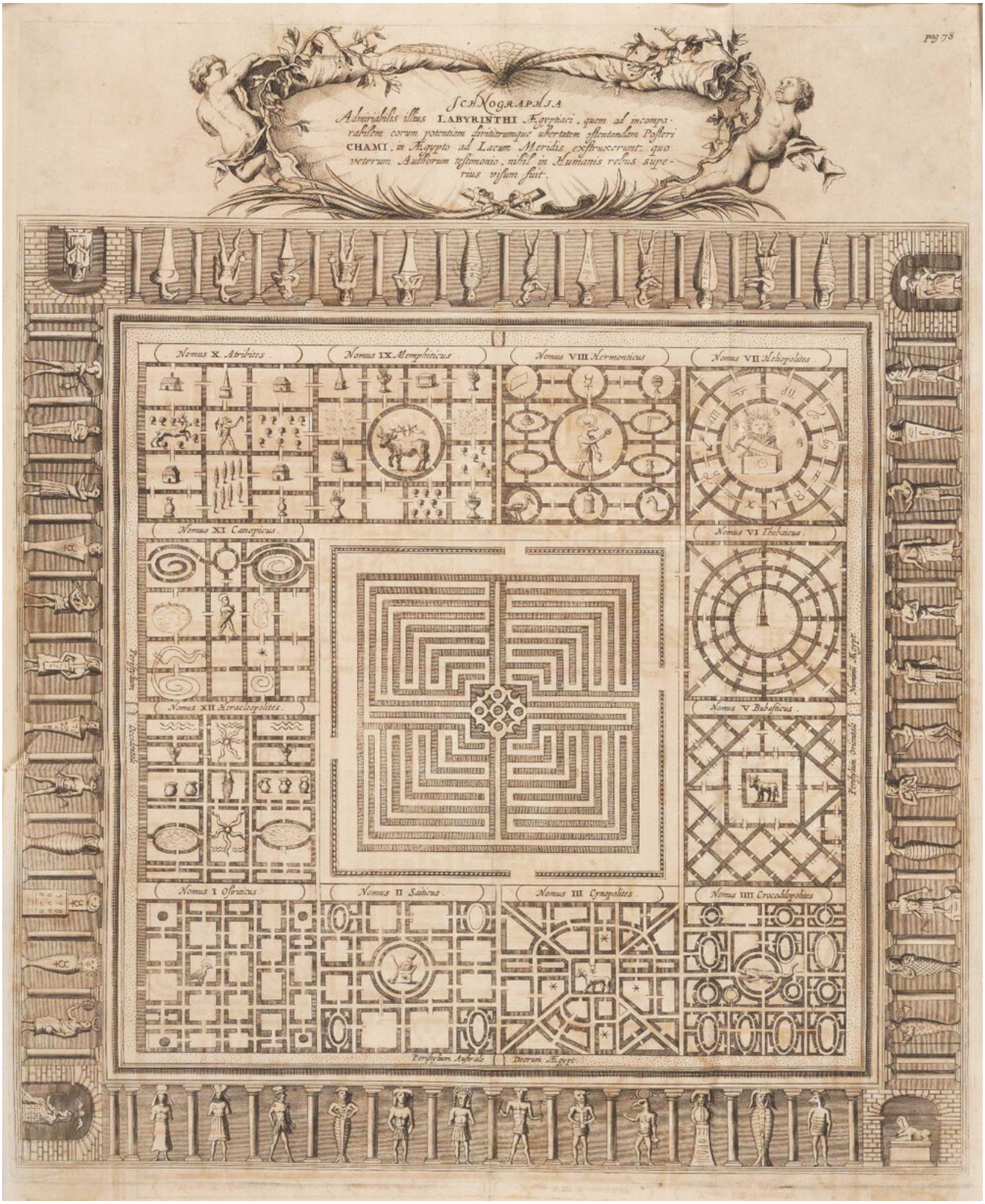


Figure 5: The Jesuit scholar **Athanasius Kircher** created in 1670 a copper plate picture of the lost Egyptian labyrinth. The central square maze is intriguing. We leave it to you to discover why.

10 The following theorem appears implicitly in a book of 1847 by Karl von Staudt who was a student of Gauss. Staudt did not use the language of mazes. But the content was there already.

Duality theorem: if G is a maze in K then G' is a maze in K'.

11 The reason is that G' is again a tree and by construction is spanning because it reaches every face. Why is it a tree? If there was a closed loop on a sphere, then this would divide the sphere into two disjoint regions and the maze G would be disconnected. (This is the Jordan Curve theorem.) But we have assumed that G is a tree which by definition is connected.

Figure 6: A labyrinth G at the Harvard divinity school. You walk on the bright part. The dual of this labyrinth can walked also by staying on the darker stones (the central point does not belong to it). Unlike G, this dual labyrinth G' is a maze and no more a Labyrinth. Try it out.

12 If V, E, F, the number of vertices, edges and faces of a planar K we have the

Euler polyhedron formula $V - E + F = 2$.

Proof: (von Staudt) Since $V(G) = E(G)+1$ and $F(G') = V(G') = E(G')+1$ and $E(G)+E(G') = E(K)$, we have we have $V - 1 + F - 1 = E$. Rearranging gives the formula.

13 By the duality theorem, we also know that the number of spanning trees in G is the same than the number of spanning trees in G'. For example, if G is an icosahedron, then G' is a dodecahedron. Indeed, we can count them. There are 5184000 mazes in both polyhedra.

Amazing Theorem: Number of mazes in K = Number of mazes in K'.

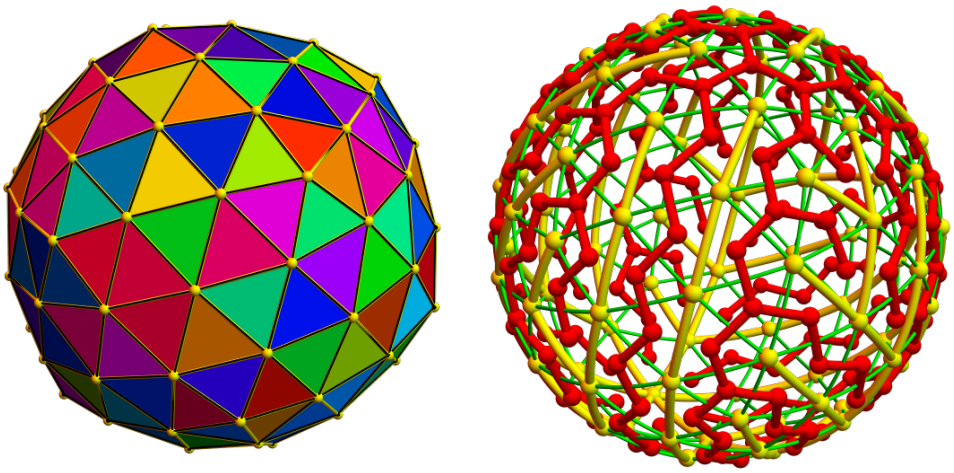


Figure 7: K is a refined Icosahedron. G (yellow) is a random maze. G' (red) is the dual maze in the dual network K'. There are 309942990509456533581461894804059712749399080000000000000000000 possible mazes on K. This is also the number of mazes in K'.

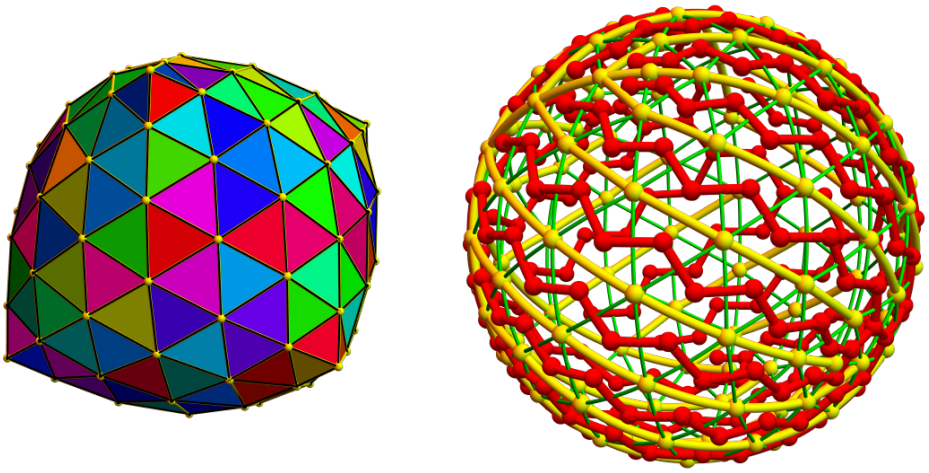


Figure 8: K is a refined Octahedron. G (yellow) is a random maze. G' (red) is the dual maze in the dual network K'. There are 899299297631504199387667566219148533377663103674658512321051081821913088000 possible mazes on K. This is also the number mazes in K'. This is about 10^{63}. **Archimedes** estimated this to be the number of grains of sand in the Aristarchian universe. Modern cosmology estimates the number of particles in the universe to be about 10^{80}. Contemplate about this the next time, you walk a maze.

TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

Lecture 2: Arithmetic

2.1. The oldest mathematical discipline is **arithmetic**. It deals with the construction and manipulation of **number systems**. Humans started doing mathematics by **counting**. **Tally sticks** or **pebbles** were the first memory tools. The earliest remnants of such devices have been found in **Africa**. The most notable examples are the **Lebombo bone** (44'000 BC) or the **Ishango bone** (20'000 BC). The first steps in building up number systems were initiated independently in various cultures. We have knowledge of early numerical structures erected by **Babylonian**, **Egyptian**, **South American**, **Chinese**, **Indian** or **Greek** thinkers.

FIGURE 1. Left: The four sides of the Ishango Bone. Source: Royal Belgian Institute of National Sciences, ""Have you heard of Ishango", 2010. Right: Clay tablet from 2041 BCE, from Umma, an ancient city in Sumer. Source: Spurlock Museum, University of Illinois.

2.2. The process of counting starts with the **natural numbers** $1, 2, 3, 4, \ldots$. They can be added as well as multiplied. While addition $+$ comes naturally by combining different objects, multiplication $*$ is more subtle: $3*4$ means to take 3 copies of 4 and get $4+4+4 = 12$ while $4*3$ means to take 4 copies of 3 to get $3+3+3+3 = 12$. The first factor counts the number of operations while the second factor counts the objects. Spacial insight shows $3*4 = 4*3$ as one can arrange the 12 objects in a rectangle. The earliest use of multiplication could have been been area computation. This was important as the amount of water to irrigate a field is proportional to its area.

2.3. Rules like **commutativity** $x + y = y + x, x * y = y * x$, **associativity** $(x + y) + z = x + (y + z), (x * y) * z = x * (y * z)$ or **distributivity** $x * (y + z) = x * y + x * z$ are guiding principles to extend the number systems. We can build negative numbers and fractions and introduce 0. This number **zero** appeared relatively late; even later than fractions. Negative numbers could first have become necessary in the context of **dept**. Dividing things up was more natural and lead to **fractions** and so the field of **rational numbers**, a preliminary culmination. The extension

from a **monoid** $\mathbb{N}$ to a **group** $\mathbb{Z}$ to a **ring** $\mathbb{Z}$ and its **field of fractions** $\mathbb{Q}$ is a prototype ladder to climb also when building other algebraic objects.

2.4. Geometry lead naturally to more general numbers. The diagonal of a square was a first example which was not quantified any more by fractions. It has been a puzzling moment for the Pythagoreans to realize that **irrational real numbers** do exist like the square root of 2. The are of a circle appeared soon not to be such a number rational. Today, we talk about the **real numbers** and use **limits** to define them. There are two major motivations to **to build new numbers**: we want to be able to **invert operations** and still get a number. Reverting the addition is subtraction for example, reverting multiplication is division, reverting taking the square is taking the square root. The second, related reason is the ability to **solve equations**.

2.5. In order to find an additive inverse of 3 we have to solve $x + 3 = 0$. The answer is the negative number $x = -3$. In order to solve solve $x * 3 = 1$ we need a rational number $x = 1/3$. To get a solution of $x^2 = 2$ a real number is needed. It does not stop there, in order to solve $x^2 = -2$ we need complex numbers. Finally, in calculus one deals with infinitesimal numbers. An other extension are **surreal numbers**. They in turn can be extended to **surreal complex numbers**.

Numbers	Operation to complete	Examples of equations to solve
Natural numbers	addition and multiplication	$5 + x = 9$
Positive fractions	addition and division	$5x = 8$
Integers	subtraction	$5 + x = 3$
Rational numbers	division	$3x = 5$
Algebraic numbers	taking positive roots	$x^2 = 2$, $2x + x^2 - x^3 = 2$
Real numbers	taking limits	$x = 1 - 1/3 + 1/5 - +...$,$\cos(x) = x$
Complex numbers	take any roots	$x^2 = -2$
Surreal numbers	transfinite limits	$x^2 = \omega$, $1/x = \omega$
Surreal complex	any operation	$x^2 + 1 = -\omega$

2.6. The development and history of arithmetic can be summarized as follows: humans started to count with natural numbers, dealt with positive fractions, reluctantly introduced negative numbers and zero to get the integers. They struggled to "realize" real numbers, were scared to introduce complex numbers, hardly accepted surreal numbers and most do not even know about surreal complex numbers. Ironically, as simple but impossibly difficult questions in number theory show, the modern point of view is the opposite to Kronecker's **"God made the integers; all else is the work of man"**. We would rather say the following: the **surreal complex** numbers are the most **natural** numbers; the **natural** numbers are the most **complex, surreal** numbers. Lets look a bit closer at various number systems.

2.7. Let us first look at **natural numbers** $\mathbb{N}$. Counting can be realized by sticks, bones, quipu knots, pebbles or wampum knots. The **tally stick** concept is still used when playing card games: bundles of fives are formed, maybe by crossing 4 "sticks" with a fifth. There is a "log counting" method in which graphs are used and vertices and edges count. An old stone age tally stick, the **wolf radius bone** contains 55 notches, with 5 groups of 5. It is probably more than 30'000 years old. The most famous paleolithic tally stick is the **Ishango bone**, the fibula of a baboon. It could be 20'000 - 30'000 years old. It was found in 1962 near Lake Edward in Congo Earlier counting could have been done by assembling **pebbles**, tying **knots** in a string, making **scratches** in dirt or bark but no such traces have survived the thousands of years. We have today still birk bark remnants from 1340 on.

2.8. The **Roman system** improved the tally stick concept by introducing new symbols for larger numbers like $V = 5, X = 10, L = 40, C = 100, D = 500, M = 1000$. in order to avoid bundling too many single sticks. The system is unfit for computations as simple calculations $VIII + VII = XV$ show. **Clay tablets**, some as early as 2000 BC and others from 600 - 300 BC are known. They feature **Akkadian arithmetic** using the base 60. The hexadecimal system with base 60 is convenient because of many factors. It survived: we use 60 minutes per hour. **The Egyptians**

used the base 10. The most important source on Egyptian mathematics is the **Rhind Papyrus** of 1650 BC. It was found in 1858 Hieratic numerals were used to write on papyrus from 2500 BC on. **Egyptian numerals** are hieroglyphics. The were found in carvings on tombs and monuments they are 5000 years old, from time of the pyramids.

1	stick
10	heel
100	monkey
1000	flower
10000	finger
1000000	frog
10000000	priest

Remember it as : "the priest points to a frog with his finger and the flower fears a monkey ending a stick."

2.9. The modern way to write numbers like 2022 is the **Hindu-Arab system** which diffused to the West only during the late Middle ages. It replaced the more primitive **Roman system**. Greek arithmetic used a number system with no place values: 9 Greek letters for $1, 2, \dots 9$, nine for $10, 20, \dots, 90$ and nine for $100, 200, \dots, 900$.

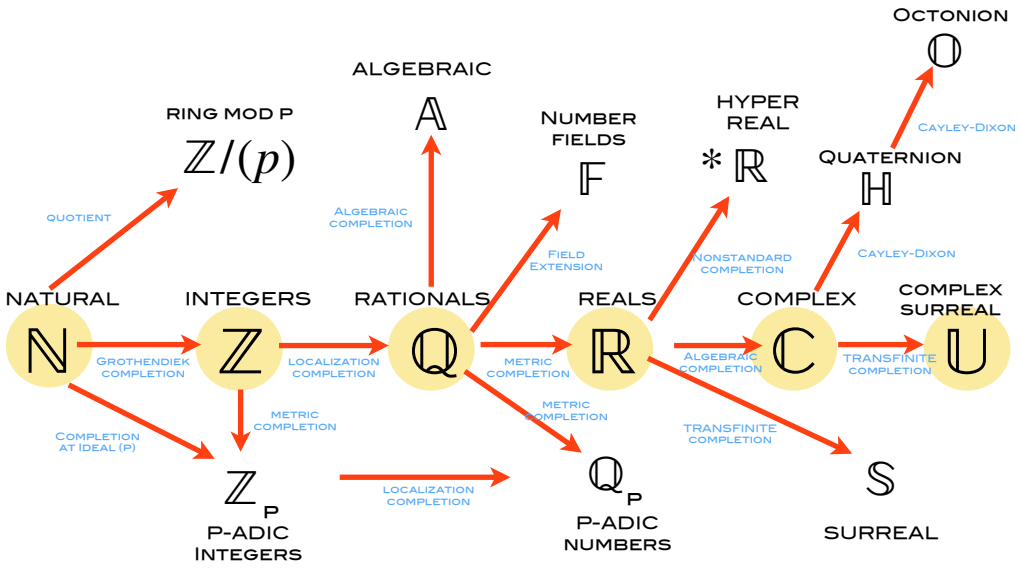


FIGURE 2. The structure of important number systems. The central bone is $\mathbb{N} \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{R} \to \mathbb{C} \to \mathbb{U}$, which starts with the natural numbers, goes to the integers, fractions, real numbers and finally the complex and surreal complex numbers. Paradoxically, $\mathbb{U}$ is the most natural since we can do anything there. Already solving equations in $\mathbb{N}$ is complex and surreal.

2.10. Now to the **Integers** $\mathbb{Z}$. **Indian Mathematics** morphed the **place-value system** into a modern method of writing numbers. Hindu astronomers used words to represent digits, but the numbers would be written in the opposite order. Independently, also the Mayans developed the **concept of** 0 in a number system using base 20. Sometimes after 500, the Hindus changed to a digital notation which included the symbol 0. Negative numbers were introduced around 100 BC in the **Chinese** text "Nine Chapters on the Mathematica art". Also the **Bakshali manuscript**, written around 300 AD subtracts numbers and carried out additions with negative numbers, where + was used to indicate a negative sign. In Europe, negative numbers were avoided until the 15'th century.

2.11. And now to **fractions** $\mathbb{Q}$ which is a natural **field**, a structure where one can add, subtract, multiply and divide by non-zero elements. Already the **Babylonians** could handle fractions. The **Egyptians** also used fractions, but wrote every fraction a as a sum of fractions with unit numerator and distinct denominators, like $4/5 = 1/2+1/4+1/20$ or $5/6 = 1/2+1/3$. Maybe because of such cumbersome computation techniques, Egyptian mathematics failed to progress beyond a primitive stage. The Egyptians used in the Rhind papyrus other conventions like $2/15 = 1/10 + 1/30$ and not $1/8 + 1/120$. There are still unsolved number theoretical problems involved with Egyptian fractions. And it also leads to puzzles. How do you write $11/17$ for example as a sum of fractions? A general method has been described by Fibonacci in his book "Liber Abaci". The answer is $1/2+1/7+1/238$. It is unknown for example whether whether Fibonnacci's process finishes after finitely many steps if we insist on odd fractions [**?**]. The example $11/17 = 1/3+1/5+1/9+1/383+1/292995$ shows that things get more complicated with when insisting of having odd fractions. The modern decimal fractions which are used today for numerical calculations were adopted only in 1595 in Europe.

2.12. An interesting transition comes when introducing **real numbers** $\mathbb{R}$ as one has to get a new concept, the concept of **limit** which is a topological or calculus like notion. As noted by the Greeks already, the diagonal of the square of length 1 has a length that is not a fraction. It first produced a crisis. Later, it became clear that "most" numbers are not rational. **Georg Cantor** saw first that the cardinality of all real numbers is much larger than the cardinality of the integers: while one can count all rational numbers but not enumerate all real numbers. One consequence is that most real numbers are **transcendental**: they do not occur as solutions of polynomial equations with integer coefficients. The number π is an example. The concept of real numbers is related to the **concept of limit**. Limits are involved when computing sums like $1 + 1/4 + 1/9 + 1/16 + 1/25 + \cdots$. The result is a number which is not rational.

2.13. The **complex numbers** $\mathbb{C}$ were introduced rather late. Rafael Bombelli introduced in 1572 a notation for $\sqrt{-1}$ and calls it "più di meno" (plus of minus). Gauss came up with the geometric picture of complex numbers in 1796 but only published it in 1931. He called them "complex numbers". Some polynomials have no real root. To solve $x^2 = -1$ for example, we need new numbers. One idea is to use pairs of numbers (a, b), where $(a, 0) = a$ are the usual numbers and extend addition and multiplication $(a, b)+(c, d) = (a+c, b+d)$ and $(a, b)\cdot(c, d) = (ac-bd, ad+bc)$. With this multiplication on pairs, the number $(0, 1)$ has the property that $(0, 1)\cdot(0, 1) = (-1, 0) = -1$. It is more convenient to write $a + ib$, where $i = (0, 1)$ satisfies $i^2 = -1$. One can now use the common rules of addition and multiplication. We can interpret the equation $x^2 = -1$ as the search transformation x in the plane which has the property that if one does the transformation twice, one gets the reflection $(a, b) \to -(a, b)$ at the origin. The transformation $(a, b) \to (-b, a)$, a rotation does the job. It satisfies the rule $i^2 = -1$. If we introduce complex numbers as $a + ib$, then multiplying with i gives indeed $i(a + ib) = ia + i^2b = -b + ia$. The algebra of real numbers can now be extended in a natural way to the set of all complex numbers $\{x + iy\}$. For example, $(3 + 4i)(1 - i) = 3 - 3i + 4i + 4 = 7 + i$. The multiplication with a complex number can be interpreted geometrically as a rotation scaling.

2.14. The **surreal numbers** are a construct which only appeared in the second half of the 20'th century. Similarly as real numbers fill in the gaps between the integers, the surreal numbers fill in the gaps between Cantors ordinal numbers. They are written as $(a, b, c, ...|d, e, f, ...)$ meaning that the "simplest" number is larger than $a, b, c...$ and smaller than $d, e, f, ...$ We have $(|) = 0, (0|) = 1, (1|) = 2$ and $(0|1) = 1/2$ or $(|0) = -1$. Surreals contain already transfinite numbers like $(0, 1, 2, 3, \dots |)$ or infinitesimal numbers like $(0|1/2, 1/3, 1/4, 1/5, \dots)$. They were introduced in the 1970'ies by John Conway. The late appearance confirms a pedagogical principle: **late human discovery manifests in increased difficulty to teach it**.
One of the reasons for introducing the surreal numbers is that one compute now for example $\sqrt{\omega}$. Different surreal numbers can mean the same, like $\{1|3\} = 2$. There are some things one has to

be careful about. For example: $x + y$ is not necessarily $y + x$. The number $\omega + 1$ is not the same as $1 + \omega = \omega$.

2.15. Geometry arithmetic: One can also compute with geometric objects like graphs. Our usual arithmetic is based on graphs without edges. Given two graphs, the addition is the disjoint union of the graphs. The multiplication takes the Cartesian product of the vertex sets and connects two if both projections either are vertices or edges. One can now repeat the construction of rational numbers, real numbers and complex numbers in a more general frame work.

2.16. Writing numbers: Geometric representations of numbers are actually already done when writing letters. Instead of carving 5 marks into a bone, one has a symbol 5 for that number. This is a geometric figure. Different cultures have introduced different ways to represent numbers. A big step was the **place value system**. Instead of having a number like 1 Million which the Egyptians wrote as a priest, one would write 1'000'000. But the base 10 system was not not the only one. The Mayan's used base 20, the Sumerians base 60. Modern computers use base 2 (binary), base 8 (octal) or base 16 (hexagesimal) systems.

2.17. Talking knots: Finally, we should mention that also knot representations have appeared in the form of **Khipu**. This also should be seen as a **geometric representation** of numbers. The use of geometry, in the form of protein structures storing information is part of the **generic code**. There are also

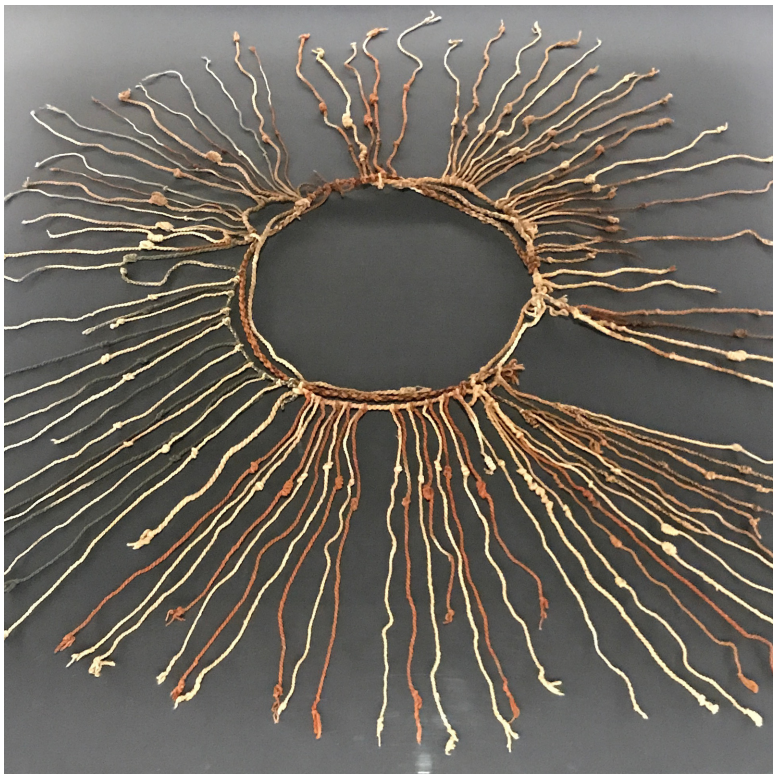


FIGURE 3. A khipu at the Boston museum of fine arts.

Work problems

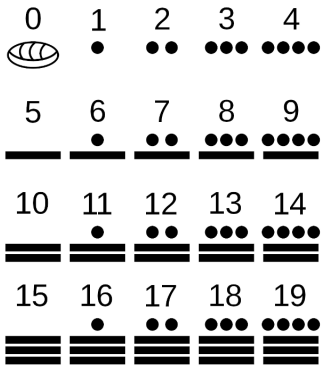
1) Here are example proofs: **Theorem:** $\sqrt{3}$ is irrational. **Proof:** $\sqrt{3} = p/q$ implies $3 = p^2/q^2$ or $3q^2 = p^2$. If we make a prime factorization, then on the left hand side contains an odd number of factors 3, while the right hand side contains an even number of factors 3.
Theorem: $\log_{10}(3)$ is irrational. **Proof.** If $\log_{10}(3) = p/q$ then $3 = 10^{p/q}$ or $3^q = 10^p$. This is not possible because the right hand side is not divisible by 3, while the left hand side is.
1a) Show that $\sqrt{17}$ is not rational, 1b) Prove that $\log_{10}(3)$ is irrational.

2) We have learned how to read hieroglyphs. Here are the symbols for 10, 100, 1000, 10000, 100000, 1000000:

Which integer does this **hieroglyph** represent? Remember: "The priest holds a frog in his finger. The flower fears a monkey bending a stick."

3) In 4000 BC, in the Mesopotamia region, cuneiform were imprinted on a wet clay tablets. An example is "Plimpton 322", a Clay tablet from 1800 BC. The Babylonians already contemplated the square root of 2. We have seen in the presentation the Clay tablet YBC 7289:

How would you write the number 1000 in the hexadecimal system?
4) The Mayan system is based on 20. Here are the first 20 numbers. Note that the Mayans have independently discovered and used zero and also had a place-valued system.



How would you write the number 401 in the Mayan system?

THE BABYLONIAN GRAPH

OLIVER KNILL

Abstract. The Babylonian graph B has the positive integers as vertices and connects two if they define a Pythagorean triple. Triangular subgraphs correspond to Euler bricks. What are the properties of this graph? Are there tetrahedral subgraphs corresponding to Euler tesseracts? Is there only one infinite connected component? Are there two Euler bricks in the graph that are disconnected? Do the number of edges or triangles in the subgraph generated by the first n vertices grow like of the order n W(n), where n is the product log? We prove here some simple results. In an appendix, we include a handout from a talk on Euler cuboids given in the year 2009.

1. Babylonian graphs

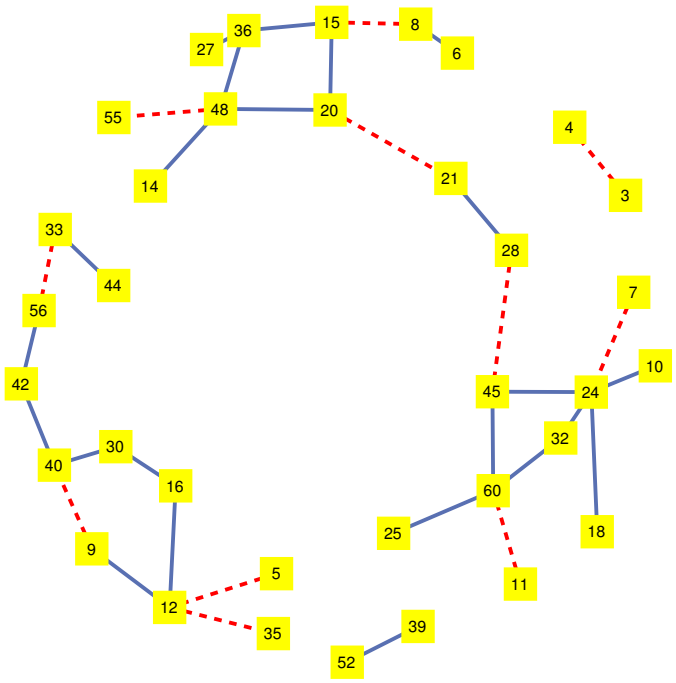


Figure 1. The graph B_{60} without isolated vertices like $\{1\}$ or $\{2\}$. The edges corresponding to primitive Pythagorean triples are dashed.

1.1. For every positive integer n, let **Babylon-n** denote the simple graph $B_n = (V_n, E_n)$ with vertex set $V_n = \{1, \ldots, n\}$ and edge set $E_n = \{(a, b), a^2 + b^2 \in \mathbb{N}, a, b \leq n\}$. We have a nested increasing sequence of graphs $B(n)$ which starts with $B_0 = K_1$ and leads to the **Babylonian graph** $B = (\mathbb{Z}^+, E)$ with **Pythagorean triples** (a, b) as edges is infinite. Triangles, complete subgraphs K_3 in B correspond to **Euler bricks** [4] (chapter XIX, see

Date: June 25, 2022.

Key words and phrases. Pythagorean triples, Euler bricks, Euler Tesseracts .

also [13]. The more extended notes [12] is attached here as an Appendix). A subclass of Euler bricks can be obtained by parametrizations like the **Saunderson parametrization** $a = u(4v^2 - w^2), b = v(4u^2 - w^2), c = 4uvw$. Triangles (a, b, c) for which additionally the sum $a^2 + b^2 + c^2$ is an integer correspond to **perfect Euler bricks**, an object which has not yet been found and which might not exist. The graphs B_n are the from $V_n = \{1, \ldots, n\}$ induced subgraph of B. Each B_n is a subgraph of B_{n+1} and the limit $B = (\mathbb{Z}^+, E)$ encodes all Pythagorean triples.

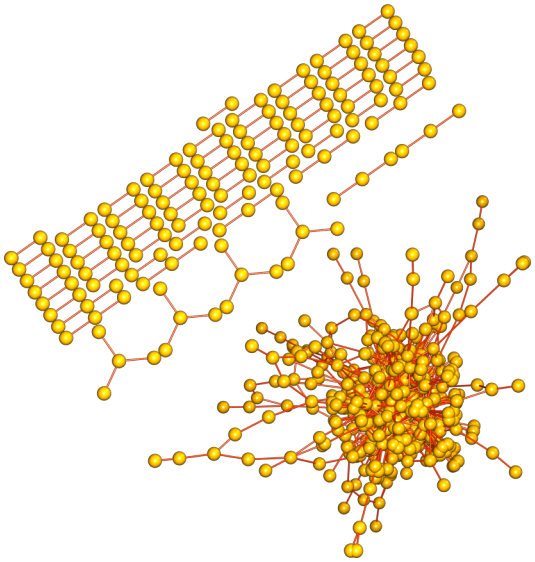


FIGURE 2. The graph B_{1000} without the 0-dimensional isolated points.

1.2. We are interested in the **largest connected component** B'_n of B_n and in the connectivity or symmetry properties of B. Are there K_4 subgraphs in B? What groups act as graph isomorphisms on B? While B has some small components like the single vertex $\{1\}$ or the single vertex $\{2\}$ or the isolated K_2 graph $\{3 \leftarrow 4\}$, we expect that B only has one large infinite connectivity component.

1.3. The question of existence of perfect Euler bricks appears to be difficult. The popularity of the problem persists. It is now also in a list of problems in [34] discussed beyond the Millenium problems. Euler bricks are triangles in B and correspond to points (x, y, z) in $\mathbb{R}^3$ located on three cylinders $x^2 + y^2 = a^2, y^2 + z^2 = b^2, z^2 + x^2 = c^2$ with integer radii a, b, c. In an Euler brick triangle, it is not possible that all three pairs are primitive. The graph induced by the primitive edges has no triangles. Figure illustrates the geometric problem to find integer points (x, y, z) on the intersection of three perpendicular main axes-centered cylinders with integer radius. The perfect Euler brick problem is to find such points which also have integer distance to the origin. Also the problem of **Euler tesseracts** can be seen geometrically. It is the problem to find the intersection of six perpendicular $3D$-cylinders $x_i^2 + x_j^2 = r_{ij}^2$, $1 \leq i < j \leq 4$ with integer radius r_{ij} in $\mathbb{R}^4$. It rephrases to find K_4 subgraphs of B. Whether this is possible is not clear.

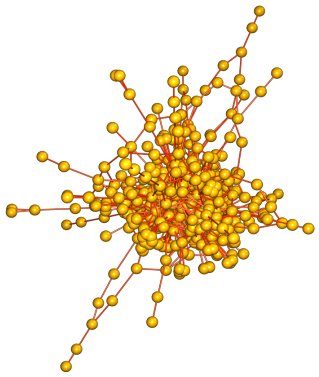


FIGURE 3. The main connected component B'_{1000} of the Babylonian graph B_{1000}. Its f-vector is $f = (480, 952, 10)$, its Euler characteristic is $\chi(B'_{1000}) = 480 - 952 + 10 = -462$ and its Betti vector is $b = (b_0, b_1) = (1, 463)$. The graph B_{10000} itself has f-vector $f = (1000, 1034, 10)$, Betti vector $b = (b_0, b_1) = (439, 463)$ and $\chi(B_{10000}) = f_0 - f_1 + f_2 = b_0 - b_1 = -24$.

1.4. There are quite many Diophantine problems using squares. One similar looking problem is the **Mengoli six square problem** of Mietro Mengoli who by the way also would suggest the **Basel problem**, to find the value of $\sum_{k=1}^{\infty} 1/k^2$. Mengoli asked for triples $x \leq y \leq z$ of integers such that the sum and difference of any two are squares. In other words, $x + y, y + z, x + z, y - x, z - y, z - x$ should all be squares. Euler found the smallest one. The solution found by Ozanam in 1691 is $(1873432, 2288168, 2399057)$. [24]

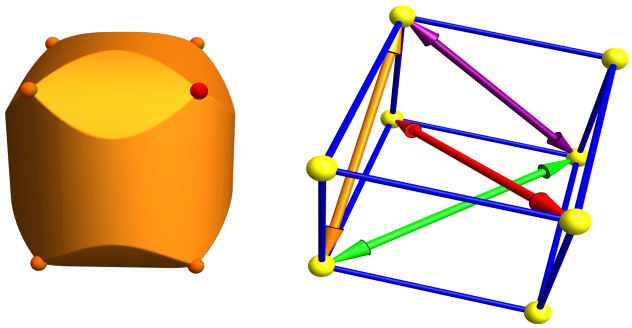


FIGURE 4. The intersection of three cylinders with integer radius defines Euler bricks. If the intersection point (x, y, z) also has integer distance to the origin, we have a perfect Euler brick. To the right we see an Euler brick.

2. FOUR QUESTIONS

2.1. Here are some natural questions. They can also be formulated as conjectures. Despite having this posted since February 2022, it is probably safer to still keep it as questions and not upgrade it to conjectures. One reason is that one or the other question could turn out to be obvious. When studying a problem for the first time, it is possible to miss something obvious. It can be that one or the other question are already answered in an other context or is a special case of a general theorem. We had looked a couple of years ago at the literature

of Euler bricks while preparing for a math circle talk. That handout in a treasure hunting theme [33] is here attached in an appendix.

2.2. First of all, we believe that there is only one largest connected component B'_n for all n and that it will end up to be a **single infinite component** in the Babylonian graph B. In principle, it is not yet excluded that there are several infinite disconnected components of B. Question Ⓐ asks whether such an "eternal maximal component" exists.

Question: Ⓐ Does B have only one infinite connected component?

2.3. Question Ⓑ is about the existence of **Hyper Euler bricks** or **Euler tesseracts**. It addresses the question about the **maximal dimension** of B. While unlikely, it would in principle be possible that the maximal dimension is infinity, meaning that there are complete subgraphs K_n of B for any integer n. Already the question of three dimensional complete subgraphs K_4 is unclear:

Question: Ⓑ Is there a K_4 sub-graph in B?

Euler tesseracts are hyper cubes $\{(x_1,x_2,x_3,x_4) \in \mathbb{R}^4, 0 \leq x_1 \leq x, 0 \leq x_2 \leq y, 0 \leq x_3 \leq z, 0 \leq x_4 \leq w\}$ with integer x,y,z,w side length for which all the 6 2D-face diagonals have integer length. One of the ways to show that a system of Diophantine equations has no solution is to look at the system modulo a prime p. If there is no solution modulo p, then there is no solution at all. In the **tesseract problem** we have to solve the system of Diophantine equations

$$x^2+y^2=a^2, y^2+z^2=b^2, z^2+w^2=c^2, w^2+x^2=d^2, x^2+z^2=e^2, y^2+w^2=f^2$$

for the 10 integer variables $x,y,z,w,a,b,c,d,e,f \in \mathbb{Z}^+ = \{1,2,3,\dots\}$. We have not started to look for solutions yet, but the strategy is similar than when looking for perfect Euler bricks: take a parametrization (x,y,z) of Euler bricks like the Saunderson parametrization, then we have a function $F_{x,y,z}(w) = d(\sqrt{x^2+w^2}) + d(\sqrt{y^2+w^2}) + d(\sqrt{z^2+w^2})$ where $d(t)$ is the distance to the nearest integer. Now, for large x,y,z and w, the dynamics $F_{x,y,z}(w) \to F_{x,y,z}(w+1)$ is by linear approximation close to a translation $t \to t+\alpha$ which then by a continued fraction expansion allows to find w for which $F_{x,y,z}(w)$ is very small and since the possible distances are quantized, once we are close enough, we hit a solution. This is how we have searched for perfect Euler bricks. A more sophisticated search using a multi-dimensional approach, leading to multi-variable Chinese remainder type problems [11].

2.4. Question Ⓒ asks about the maximal dimension of the non-major connected components. Example sub-graphs $\{1\},\{2\},\{3,4\}$ remain separated also in B. We have not yet seen any example, where a non-major connected component has maximal dimension larger than 1:

Question: Ⓒ Are there two connected components with triangles?

In other words, we look for pairs of Euler bricks, so that there is no connection from one brick to the other brick in B. We have also not seen any in any B_n. It could be possible that there exists a B_n with two disconnected K_3 subgraphs which however get reunited in a larger B_m for $m > n$. .

2.5. The fourth and last major question Ⓓ is a particular **growth rate question**. Let $W(x)$ denote the **product log** = **Lambert W-function** which is defined as the inverse of the function $y = x\log(x)$. This function naturally occurs in the **prime number theorem** which tells that the n'th prime p_n is of the order $p_n \sim n\log(n)$ meaning $W(p_n) \sim n$. Now the **number of primitive edges** in B_n grow like $C_1 n$, where C_1 is a concrete number expressible as an area of the parameters lattice points (u, v) in $[0, \sqrt{n}] \times [0, \sqrt{n}]$ such that $\Phi(u, v) = (u^2 - v^2, 2uv) \in [0, n] \times [0, n]$. Having a growth $C_1 n$ of primitive edges, we expect $C_1 n W(n)$ to be the growth of all edges.

Question: Ⓓ Does $f_1(B_n)/(nW(n))$ converge?

2.6. There are many other quantities one could look at. We can look at the **f-vector** $(f_0, f_1, f_2, \dots) = (n, f_1(B_n), f_2(B_n), \dots)$ or the Betti numbers $b_k(B_n) = \dim(\ker(L_k(B_n))$ where $L_k(B_n)$ is the k**-form Laplacian**. Of interest are the number of connected components $b_0(B_n)$, the number $b_1(B_n)$, a genus, which measures of the number of one dimensional "holes" in B_n, the maximal vertex degree, the distribution of the vertex degrees, the growth of the Euler characteristic $\chi(B_n) = f_0(B_n) - f_1(B_n) + f_2(B_n) - \cdots = b_0(B_n) - b_1(B_n) + b_2(B_n) - \dots$, the inductive dimension of B_n or B_n' with the ultimate goal to give lower and upper bounds. We looked first numerically at the diameter change up to $n = 10000$. The diameter goes to infinity because $\text{Diam}(B_1(5000)) = 18$, $\text{Diam}(B_1(10000)) = 29$. A logarithmic growth which is justified by scaled graphs $x_1, x_2, \dots, x_n = Mx_1, Mx_2, Mx_3, \dots, Mx_n$ etc.

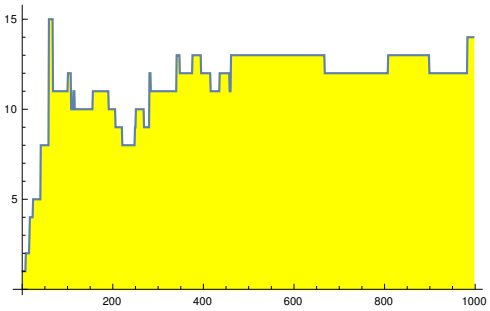


FIGURE 5. The diameter of B_n up to $n = 1000$.

2.7. Whenever we have a graph G, the **graph complement** $\overline{G}$ is of interest. The operation of taking graph complements is an **involution** on the class of all graphs. Even for very simple graphs, the graph complement can be interesting. See [17] for cyclic or linear graphs, where graph complements are either contractible or homotopic to spheres or wedge sums of spheres. What are the properties of the graph complement of B?

3. LOW HANGING FRUITS

3.1. One can wonder first whether there are **isolated vertices** that are not connected to anything else. These are zero dimensional connected components of the graph. There are exactly two vertices with this property. We know that $1 + b^2, 4 + b^2$ are never a square.

Remark: ① There are exactly two isolated single vertices $1, 2$ in B.

Proof: Already the **primitive Babylonian graph** B_p which connects only points a, b if $a, b, \sqrt{a^2 + b^2}$ is a primitive Pythagorean triple has no isolated points except $1, 2$: the reason

is that all odd numbers larger than 1 are of the form $u^2 - v^2$ and all even numbers larger than 2 are of the form $2uv$ for some positive distinct u, v.

3.2. There are other isolated connected components like $\{3, 4\}$ belonging to the primitive triple $3^2+4^2 = 5^2$. This can not be connected to anything else. If $9+b^2 = c^2$, then $c^2-b^2 = 9$ which is only possible for $b = 4, c = 5$. The relation $16 + b^2 = c^2$ is only possible for $b^2 = 9$.

3.3. One can wonder about the asymptotic distribution of the vertex degrees. When looking at the sequence B_n of graphs, there is an increasing part $C_n \subset B_n$ for which the vertex degrees do no more change when increasing n. The reason is that the monotone sequence $\deg(B_n)(x)$ converges:

Remark: ② $\deg_B(x)$ is finite for all $x \in V$.

Proof: every edge is a Pythagorean triple which is a multiple of a primitive Pythagorean triple and so of the form

$$(a, b) = (2pqc, (p^2 - q^2)c) ,$$

where p, q, c are integers. If we fix an integer like b, there are only finitely many solutions $(p^2 - q^2)c = b$ because both c and $p^2 - q^2$ have to be recruited from factors of b which is finite. For a fixed factor r of b the Diophantine equation $p^2 - q^2 = r$ has only finitely many solutions because both p, q have to be smaller than $\sqrt{r}$.

3.4. One can also wonder how many infinite connected components there are B. We do not know yet. We can get infinite connected components for a primitive $(a, b) = (2uv, u^2 - v^2)$ if it is connected to a multiple of itself. This can indeed happen and proves

Remark: ③ The diameter of B is infinite.

Proof: it is enough to construct a concrete path in B going to infinity: There is a connection from $n = 5$ to $n = 30$ given by $5 \to 12 \to 16 \to 30$. This scales. The path $30 \to 40 \to 96 \to 180$ for example extends the other path so that we have a connection from 5 to 180. We can continue like that and get an infinite path in B.

3.5. We could call a connected component in which a scaling $(a, b) \to m(a, b)$ exists a **component with scale symmetry**. We have just seen that such components are infinite. Are there components which are not scale invariant?

3.6. Since $a = u^2 - v^2, b = 2uv$ parametrizes all **primitive triples**, there is a constant C such that there are asymptotically $C * n$ primitive edges in the graph B_n. This limit can be computed explicitly as we can draw out the region in the parameter domain leading to triples $\leq n$. But then we have also non-primitive ones which come from scaled smaller primitive ones.

3.7. Here is an other simple observation about **leafs** in B. These are vertices x for which the unit sphere $S(x)$ (the subgraph generated by all vertices attached to x) contains only one point.

Remark: ④ If p is an odd prime, then p is a leaf in B.

Proof: We must have $p = u^2 - v^2$ so that p belongs to the primitive Pythagorean triple $2uv, u^2 - v^2$. Now, $u^2 - v^2 = p$ implies with $v = u - k$ that $p = u^2 - (u - k)^2 = 2uk - k^2$. Since p is prime, $k = 1$ meaning that we have only one choice to solve $u^2 - v^2 = p$ for u, v. The Pythagorean triple is not fixed.

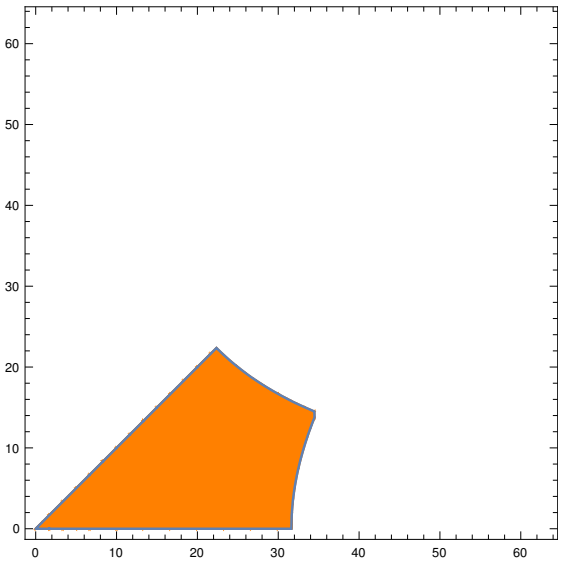


FIGURE 6. The uv-parameter region $- \leq u^2 - v^2 \leq n, 0 \leq 2uv \leq n, u \geq 0, v \geq 0$. For each lattice point (u, v) in that region, we get a Pythagorean triple $u^2 - v^2, 2uv, u^2 + v^2$ on $[0, 2\sqrt{n}] \times [0, 2\sqrt{n}]$ and so an edge in B_n.

3.8. By definition, the number of vertices $f_0(B_n) = n$. Let $W(x)$ denote the inverse of the function $x \to xe^x$. It is called the **Lambert W function**. Motivated from the prime number theorem telling that that n grows like $P(n)W(P(n))$, where $P(n)$ is the n'th prime number, it is likely that $\lim_{n\to\infty} f_1(B_n)/(nW(n)) = C_1$ and $\lim_{n\to\infty} f_2(B_n)/(nW(n)) = C_2$ exist:

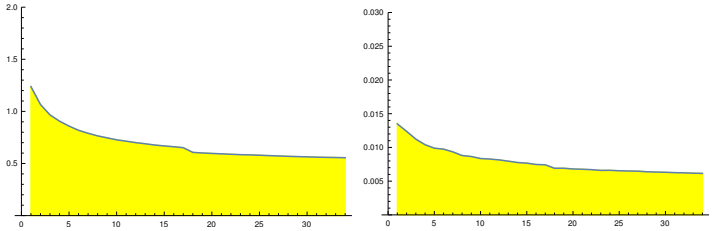


FIGURE 7. The number of edges and triangles for the main component. $f_1(B'_{n*1000})/(n*W(n)*1000)$ and $f_2(B'_{n*1000})/(n*W(n)*1000)$ for $n = 1, \ldots, 25$.

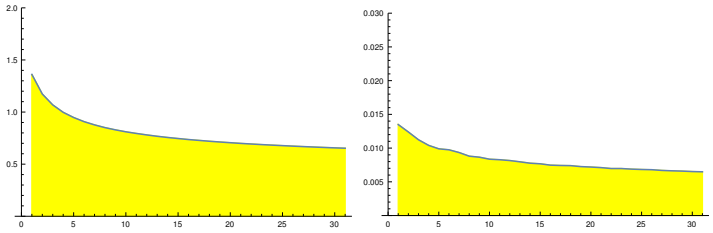


FIGURE 8. Number of edges and triangles for the full graph with all components: $f_1(B_{n*1000})/(n * W(n) * 1000)$ and $f_2(B_{n*W(n)*1000})/(n * 1000)$ for $n = 1, \ldots, 20$.

3.9. This would lead to a result that $C = \lim_{n\to\infty} \chi(B_n)/(nW(n)) = C_0 - C_1 + C_2 - C_3 + ...$ exists.

3.10. Here is a result which is somehow interesting. A graph can be defined to be planar if it does not contain a homeomorphic copy of K_5 or $K_{3,3}$. (There is also the traditional definition of planar using a topological embedding on a 2-sphere, but the just given one is equivalent by **Kuratowski's theorem**. The combinatorial definition has the advantage that is purely graph theoretical and does not refer to topology of Euclidean space.

Remark: ⑤ B_n is planar if and only if $n \leq 95$

Proof. Since B_{95} is planar all B_n with $n \leq 95$ are planar. Since B_{96} is non planar, all B_n with $n \geq 96$ are non-planar. □

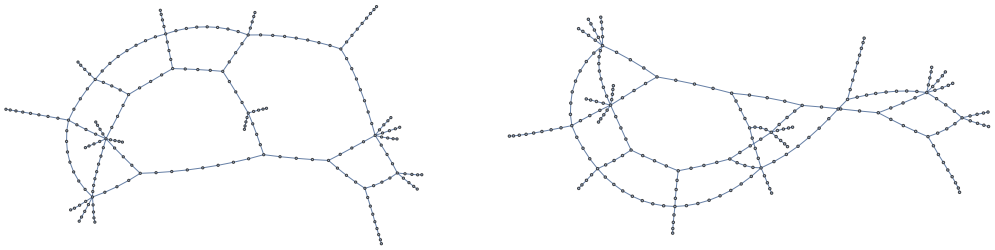


FIGURE 9. The graph B_{95} (looking like a piglet) is planar, the graph B_{96} (looking like a chicken) is not. We show here the second Barycentric refinements of the main connected components. The non-planar property of B_{96} is not well visible. We have to look closely at the crossing of edges. There is a crossing which is not a node.

4. Babylonian triplets and Pythagoras

4.1. Pythagorean triples appeared in Babylonians tablets. The most famous is Plimpton 322 [31, 21]. An other one is Si.427. We could call the examples of Pythagorean triples which appear in some Babylonian text a **Babylonian triplet**. The major known clay documents which list Babylonian triples appear all during the time 1900-1600 BC. Pythagorean triples also appear in ancient Egyptian mathematics like on the **Berlin Papyrus 6619**. It contains the non-primitive triple $6, 8, 10$ and which is a document dated at about a similar time than the clay tablets.

4.2. It has been speculated that experimental exploration of Pythagorean triples also had practical **engineering value** because the construction of right angles has architectural or irrigation area measurement applications. The interpretation that some of these clay tablets were school tablets indicate that the topic of Pythagorean triples must also have been of **educational value**. The Pythagorean triples also paved the way for the **Pythagorean theorem**, the statement that $a^2 + b^2 = c^2$ holds for the sides of a triangle if and only if the triangle has a right angle. In the remarkable tablet YBC 7289, an isosceles right angle triangle appears with a rather astounding approximation of $\sqrt{2}$. This was one of the first examples for the Pythagorean theorem with non-integer sides but it is also just an example.

4.3. Despite many speculations in that direction, there is **no evidence** that the Babylonians were aware of the Pythagorean theorem. We can **speculate** that they started to **suspect a general rule**. We see in the literature and even encyclopedias formulations like *"may suggest that the ancient Egyptians knew the Pythagorean theorem"*. Still, also for such a

claim, we lack any historical sources. We have no document on which any such conjecture is formulated. Formulations like "may suggest" are a bit reckless as they disregard the difficulty in mathematics to coming up with conjectures and general rules and then to prove them. There are countless many examples, where mathematical rules have been conjectured by looking at small examples and where later, the rule turned out to be false. Many examples are listed in [7]. Proto-Pythagorean themes have also appeared also in Chinese documents, including a proof of the Pythagorean theorem in the 3-4-5 triangle case which indicates that a general statement was in the air. As mathematicians, we know however that stating a fact like $3^2+4^2=5^2$ and visualizing it in a picture is not the same than claiming that $a^2+b^2=c^2$ holds in a triangle if one of the angles is a right angle triangle.

4.4. Jacob Bronowski took in his book [2] the old fashioned point of view about the discovery of Pythagoras. He of course was aware about the uncertainty of the sources. But it is the so far best guess that Pythagoras was the first who proved the theorem. Because of the lack of original documents of Pythagoras, we might never know who actually proved the Pythagorean theorem the first time. Bronowski tells: *Pythagoras had thus proved a general theorem: not just for the 3:4:5 triangle of Egypt, or any Babylonian triangle, but for every triangle that contains a right angle. He had proved that the square on the longest side or hypotenuse is equal to the square on one of the other two sides plus the square on the other if, and only if, the angle they contain is a right angle. For instance, the sides 3:4:5 compose a right-angled triangle. And the same is true of the sides of triangles found by the Babylonians, whether simple as 8:15:17, or forbidding as 3367:3456:4825, which leave no doubt that they were good at arithmetic. To this day, the theorem of Pythagoras remains the most important single theorem in the whole of mathematics. That seems a bold and extraordinary thing to say, yet it is not extravagant; because what Pythagoras established is a fundamental characterization of the space in which we move, and it is the first time that is translated into numbers. And the exact fit of the numbers describes the exact laws that bind the universe.*

4.5. The ability to make good conjectures and to get a **notion of proof** needed to evolve over time. Already the realization that there is a difference between **Examples**, **Conjectures**, **Hypothesis**, **Model** and **Theorems** is a cultural achievement. We see the process when watching students learning. When we learn mathematics we first confuse the process of proving a result in general or to just support a phenomenon by giving **anecdotal data evidence**. The ability of **asking questions** like **why** is what "makes us curious' [19] as it starts a scientific process. Because the object **Babylonian graph** seems historically not have appeared in the literature, we are in a realm, where we can also observe our own first steps and track misconceptions or mistakes.

4.6. Even wrong conjectures can be helpful as they illustrate our status of understanding for a subject. We also are interested in the Babylonian graph because we are here in a "data collection" and "forming conjecture" phase. Historians will have to find out whether the Babylonian graph has been mentioned earlier in the literature. In a hundred or thousand years, we might know a lot about this graph. Today in 2022, we seem to be in the "data collection" and "forming conjectures" phase. In a thousand years, there might be powerful theorems which answer all questions. It can of course also be that there is no interest in the object at all building up and that the topic will remain an obscure example.

4.7. The origins of the Pythagorean theorem itself is in mystery. Who was the first who conjectured it? This is already a major step going much beyond just listing examples. The next step is a giant one as it is way beyond conjecture. Who was the first who proved the

Pythagorean theorem? This is difficult as no authentic documents of Pythagoras himself are known. See [36, 35, 9, 29, 28, 22, 10]. Still, if we look at the text evidence, we have to give the Greek mathematicians (and especially Euclid from whom we have dated documents) the credit to formalize what a "theorem" and what a "proof" is and distinguish a "general statement" (which is always true) from a "statistical statement" (which is true in most cases or with a few exceptions only [the nonsensical "exceptions prove the rule" is even used in colloquial language]) and especially to distinguish from "anecdotal evidence" (which even in our modern times is often mistaken as "proof" by a mathematically untrained person, or then as a crude but effective tool for advertisement or propaganda.) The Babylonian triplets were **anecdotal evidence** for the theorem for Pythagoras, not more. It was still far from a conjecture about a general relation and even further away from a Pythagorean theorem which is a statement coming with a proof.

4.8. There have been a few headlines in the last couple of years claiming that the Babylonians invented trigonomety. There is no indication that Babylonians invented trigonometry. This statement depends on what "trigonometry" means. While trigonometry uses ratios of triangles for the definition of the trigonometric functions, looking at ratios of sides of triangles should not yet count as trigonometry. No school curriculum considers that nomenclature when talking about trigonometry. Looking at ratios of right angle triangles is **proto trigonometry at best**. To cite [31] about research theories in history: *"In general, we can say that the successful theory [in the history of mathematics] should not only be mathematically valid but historically, archaeologically, and linguistically sensitive too."* [21] for example has produced the **2021 controversy**: the paper has been picked up by media. Math historian Victor Blasjö formulated it nicely: 'it tricked news outlets into printing nonsense headlines".

5. Experimental explorations

5.1. Experimental explorations of a mathematical structure often have predated theorems considerably. Experiments can lead to **examples which suggest a theorem**. But there can be a long journey from experiments to theorems. It took a thousand years to get from **Pythagorean triple explorations** to the **Pythagorean theorem**. Otto Neugebauer already speculated that the parametrizations $a = u^2-v^2, b = 2uv, c = u^2+v^2$ could have been known thousands of years ago ([25] page 39). Bronowski for example gives the example of a pair $(3367, 3456)$ [2] which is the parametrization obtained with $u = 64, v = 27$. The largest number in Plimpton 322 is $(a, b) = (12709, 13500)$ which is obtained with $u = 125, v = 54$. Obtaining such large numbers without a parametrization is harder is not impossible. It needs a bit of patience and some luck. Such examples make it likely that the Euclid parametrization was known and used but it is still just a guess.

5.2. The fact that in the given examples on Plimpton 322, only a few "random" parameter values (u, v) appear and not a systematic list, ordered according to (u, v) speak against the knowledge of such a parametrization but it would be conceivable that some structure was seen like that one number is even and trying $b = 2uv$, where u, v are factors. All primitive triples can be obtained as such and also non-primitives like $6^2 + 8^2 = 10^2$ have been considered. Finding out what really happened is something for Sherlock Holmes [3], where we see the statement *We can begin by asking if numbers of the form $a^2 - b^2$ and $a^2 + b^2$ have any special properties. In doing so, we run the risk of looking at ancient Babylonia from the twentieth century, rather than trying to adopt the autochthonous viewpoint.*

5.3. Creighton Buck further writes: *"There is no independent information showing that these facts were known to the Babylonians at the time we conjecture that this tablet was inscribed."* Indeed, there is no known statement of a result $a^2 + b^2 = c^2$ for right angle triangles on clay tablets. Three thousand years ago, it had not been excluded that some **super large right triangle** with side length a, b, c would satisfy $a^2 + b^2 \neq c^2$. In most tablets, we only see integer side triangles. There is the triple $(1, 1, \sqrt{2})$ in YBC 7289 which contains a non-integer side length. We can only imagine how puzzling this must have been.

5.4. In the context of finding historical clues, we also can gain insight by looking at what children do. Looking at early learners is like pointing a telescope to the past. The early steps in mathematics resemble the first steps of the pioneers developing the topic. This prompted a historian to claim [6] **"A student should be taught a subject pretty much in the order in which the subject developed over the ages."** It is a good rule of thumb but of course not universal. Many secrets from geometry can be appreciated much faster for example when using algebra. The fact that mathematics has evolved for many thousands of years and in an accelerated way requires a modern student also to pass to the modern topics faster and taking shortcuts and bypass times of stagnation.

5.5. In the context of pedagogy, there is an anecdote of the teacher letting students construct right angle triangles using paper and ask them measure $a^2 + b^2 - c^2$. One student group reported in their presentation that they found a remarkable rule: $a^2 + b^2 - c^2$ was always small but never zero! This **anti-Pythagorean theorem** is **academically honest** because every measurement comes with errors. The students reported **what they measured** and did not report what they **wanted to see**. It is the most common sin in science to fall into **wishful thinking**. It is a powerful source of motivation, but it is dangerous. We know that error measurements have a continuous distribution so that without prejudice, it is correct that in experiments, $a^2 + b^2 - c^2 \neq 0$ with probability 1. The students doing the measurements of course had not been exposed to statistics and data science. A more sophisticated approach would be to build a statistical model for the **possible errors**, to make a **hypothesis** and determine the **p-value**, the evidence against a null hypothesis. A good scientist tries to make the p-value as small as possible and so give **data evidence** for the Pythagorean theorem. This theorem would then be a **mathematical model**. The scientist then decides whether the measurements support the model. This is still far from proving the theorem. To prove the theorem one has to place the statement into a particular frame work, like planar Euclidean geometry. This requires to make some **idealizations** and **assumptions**.

5.6. Also the process of **building a model** or placing a statement in a **particular axiomatic frame work** is an achievement of Greek mathematics which should not be underestimated. I myself was not taught about **methods of science** in mathematics but in a philosophy classes. First in high school and later in college in a lecture series of Paul Feyerabend. Let me mention the high school part: I have been lucky to have a year of philosophy in the Schaffhausen highschool with Markus Werner (1944-2016) who was also a successful writer who won a dozen prestigious prizes like the Herman Hesse literature prize. He started one of the lessons with "What is the color red?" which led to interesting discussions about what color is, and whether it is something we can understand. What happens if we mix colors when drawing with a yellow and blue crayons what happens if we illuminate an object with blue and yellow lights simultaneously. An other of these philosophy lesson started with "What is the sum of the angles in a triangle?". A student would answer 180 degrees. Werner would ask to prove it. An other student would prove it on the board. The class

would discuss then what kind of assumptions went into the proof. Werner would then draw a triangle on a sphere, where the theorem fails. How could we go wrong? What was wrong with the proof? On a sphere, there are triangles where the sum of the three angles is 270 degrees. There are 8 triangles on a sphere which partition the sphere up like that. In these 90 degree triangles, the Pythagorean result $a^2 + b^2 = c^2$ fails. Actually, for those special 90-90-90 triangles, one has $a^2 = b^2 = c^2$. They are equilateral right angle triangles. Why did the proof which everybody agreed upon fail? What assumptions went into the proof?

FIGURE 10. Markus Werner (1944-2016), a writer and high school teacher.

5.7. An even more sophisticated picture appeared since Einstein. Sphere or non-Euclidean geometries are just one of many Riemannian geometries and Riemannian geometry is a more accurate model of our physical space than Euclidean space. [1] The Pythagorean theorem is well known to fail in our **three dimensional physical space**: it is an **idealization** dealing with **flat Euclidean space**. In a linear algebra setting, assuming a linear flat space, the subject can be dealt with quickly: define two vectors to be perpendicular if $u \cdot v = 0$ and define the length as $\sqrt{u \cdot u}$, then check $|u-v|^2 = (u-v) \cdot (u-v) = u \cdot u + v \cdot v = |u|^2 + |v|^2$. We make a lot of assumptions although, the result assumes that space is continuous and in particular that there are perpendicular objects. Then we assume that space has an algebraic structure in that we can add and scale.

5.8. But we know since more than 100 years now from general relativity that every mass bends space and that right angle triangles only satisfy $x^2+y^2 = c^2$ in the **complete absence of matter** or under very special circumstances of the curvature. But even if we assume total absence of matter and ignore the presence of virtual particles (which are confirmed by phenomena like the Casimir effect), we still do not know because we have no access to any **Planck scale features** of space. We have no idea what happens if we take a right angle triangle of side length a, b, c if a, b, c are of the order 10^{-35}. Our notions of distance based on measurements using electromagnetic waves do not make sense any more.

5.9. On a computer small physical distances are no problem- up to some reasonable scale. We can for example enjoy looking at features of the Mandelbrot set on a scale of say 10^{-200}. It is not difficult for a computer to show us topological features of that mathematical object on such a small scale. But we can also with a computer not explore scales like $10^{-10^{200}}$. If the structure of space on the Planck scale would be understood, one can always ask what happens on an even smaller scale. Once the atom was considered the smallest unit, then protons, now we suspect quarks to be part of the smallest ingredients. There was a long way

[1] By the way, Einstein lived 1901/1902 in Schaffhausen for a few months, and lived a few hundred meters from the highschool in Schaffhausen, working as a tutor.

from speculations by philosophers like Democritus to the current standard model of particle physics.

6. About the question

6.1. We mentioned the Babylonian graph in our first lecture of Math 22 in the spring of 2022. It was aimed as an illustration of the fact that mathematics is not only **eternal**, but also **infinite**. If you solve one problem, ten more problems pop up. Having seen in January, the movie "The eternals" in a movie theater, I called the Babylonian graph problem there the **"Eternals" problem**, because it had been communicated to us by the eternal Ajak from the Marvel comics universe. We also used the Babylonian graph as an example in the computer science lecture on May 1st, 2022 Math E 320 to illustrate the process of **experimental mathematics**. A related graph is the graph in which one takes pairs a, b for which $a + ib$ is a Gaussian prime. We have played with graphs related to number theory also in [15].

6.2. In [16] we looked at the graph G_n with vertex set $V = \{1, 2, \dots n\}$, where two are connected if their sum is a square. So, the connecting rule is $a + b = c^2$, (not $a^2 + b^2 = c^2$). This graph had as a motivation a puzzle posed by Anna Beliakova of the University of Zürich and Dmitrij Nikolenkov of Trogen, a high school in Switzerland: *Write down the numbers* $1 - 16$ *in a row so that the sum of two arbitrary neighbors is a square number.* This means we have to find a Hamiltonian path in G_{16}. Historically, the use of graph theory is closely tied to puzzles. William Rowan Hamilton came up with the idea of Hamiltonian paths in the context of the **Icosian game**, the problem to find a Hamiltonian cycle on the dodecahedron graph. All questions asked for the Babylonian graph can be asked for this **Baliankova-Nikolenkov graph**.

6.3. An other class of natural graphs G_n appears on square free integers by connecting two such integers if one divides the other [14]. It has the Euler characteristic $\chi(G_n)) = 1 - M(n)$ relates to the **Mertens function** $M(x) = \sum_{k=1}^{n} \mu(k)$ with the Möbius function μ. The value $-\mu(k)$ is the **Poincaré-Hopf index** of the vertex k using the Morse function $f(k) = k$. Adding a new integers is part of a **Morse build-up** because every critical point either has index 1 or -1 and **"counting" is a Morse theoretical process**, during which more and more 'handles" in the form of topological balls are added, building an increasingly complex topological structure. I would see later that this structure has already been studied earlier in [1].

6.4. In February 2022, we already looked numerically at the growth of the graph diameter of the main connected component B'_n of Babylon B_n. The diameter does not grow monotonically as some parts reconnect. But the experiments suggested already then that the diameter might increase indefinitely. While easy to see, it has not been visible to me at first and I asked it as a question. Only when noticing that there are connections from integers to a multiple of an integer, the infinite diameter of B became clear and obvious. In retrospect it now would have been ridiculous to formulate an infinite diameter conjecture.

6.5. It might well be that one or the other of the questions Ⓐ,Ⓑ,Ⓓ, Ⓓ mentioned here are not difficult to answer. When you look at a new problem the first time, a lot of things which later appear "obvious", are still obscured. It might also be that some Diophantine problems like the problem of the existence of K_4 or K_5 subgraphs in B are difficult. The **perfect Euler brick problem** turned out to be hard and evidence that it is really hard is the fact that it has remained open for so long. It is well possible that the K_4 problem is

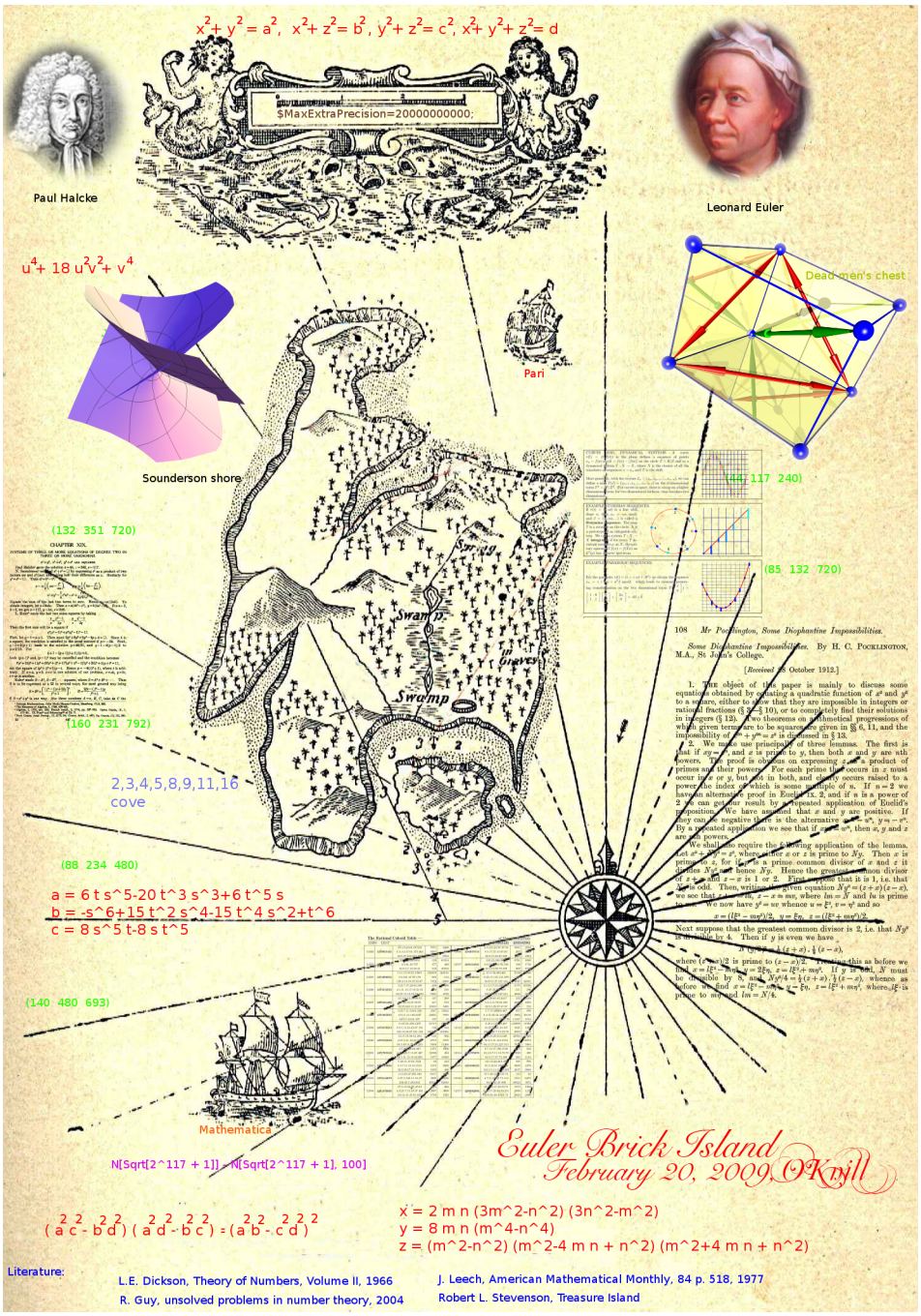
easy and that it could be answered by just looking at the problem from the right angle or by having a sufficiently strong computer and patience to find one.

Appendix: A talk on Euler bricks

Math table, February 24, 2009, Oliver Knill

Treasure Hunting Perfect Euler bricks

An Euler brick is a cuboid with integer side dimensions such that the face diagonals are integers. Already in 1740, families of Euler bricks have been found. Euler himself constructed more families. If the space diagonal of an Euler brick is an integer too, an Euler brick is called a perfect Euler brick. Nobody has found one. There might be none. Nevertheless, it is an entertaining sport to go for this treasure hunt for rational cuboids and search - of course with the help of computers. We especially look in this lecture at the Saunderson parametrization and give a short proof of a theorem of Spohn [32] telling that the any of these Euler bricks is not perfect. But there are other parameterizations.



Introduction: the map of John Flint

An **Euler brick** is a cuboid of integer side dimensions a, b, c such that the face diagonals are integers. If u, v, w are integers satisfying $u^2 + v^2 = w^2$, then the Saunderson parametrization

$$(a, b, c) = (|u(4v^2 - w^2)|, |v(4u^2 - w^2)|, |4uvw|)$$

leads to an Euler brick.

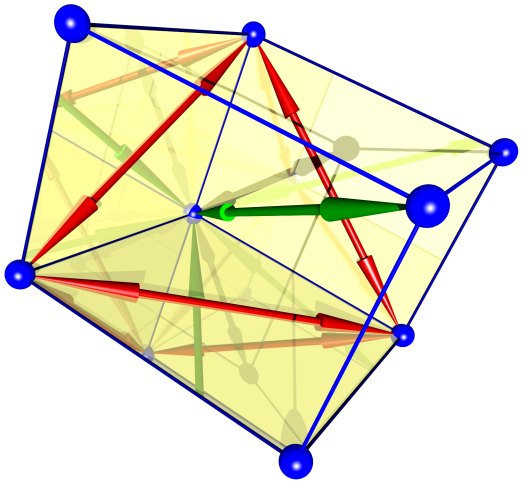


Fig 1. An Euler brick has integer face diagonals. It is perfect if the long diagonal is an integer too.

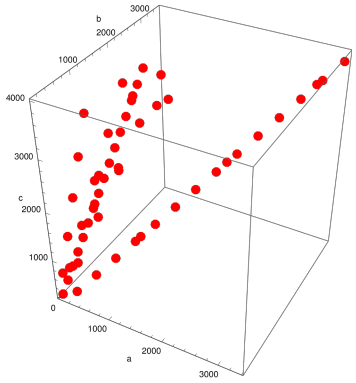


Fig 2. The smallest Euler bricks (a, b, c) with $a \leq b \leq c$ plotted in the parameter space.

The cuboid with dimensions $(a, b, c) = (240, 117, 44)$ is an example of an Euler brick. It is the smallest Euler brick. It has been found in 1719 by Paul Halcke (- 1731) [4].
If also the space diagonal is an integer, an Euler brick is called a **perfect Euler brick**. In other words, a cuboid has the properties that the vertex coordinates and all distances are integers.

It is an open mathematical problem, whether a perfect Euler bricks exist. Nobody has found one, nor proven that it can not exist. One has to find integers (a, b, c) such that

$$\sqrt{a^2 + b^2}, \sqrt{a^2 + c^2}, \sqrt{b^2 + c^2}, \sqrt{a^2 + b^2 + c^2}$$

are integers. This is called a system of Diophantine equations. You can verify yourself that that the Saunderson parametrization produces Euler bricks.
If we parametrize the Pythagorean triples with $u = 2st, v = s^2 - t^2, w = s^2 + t^2$, we get $a = 6ts^5 - 20t^3s^3 + 6t^5s$, $b = -s^6 + 15t^2s^4 - 15t^4s^2 + t^6$, $c = 8s^5t - 8st^5$. This defines a parametrized surface

$$r(s, t) = \langle 6ts^5 - 20t^3s^3 + 6t^5s, -s^6 + 15t^2s^4 - 15t^4s^2 + t^6, 8s^5t - 8st^5 \rangle$$

which leads for integer s, t to Euler bricks.

Indeed, one has then: $a^2 + b^2 = (s^2 + t^2)^6$, $a^2 + c^2 = 4(5s^5t - 6s^3t^3 + 5st^5)^2$ $b^2 + c^2 = (s^6 + 17s^4t^2 - 17s^2t^4 - t^6)^2$.
A perfect Euler brick would be obtained if $f(t, s) = a^2 + b^2 + c^2 = s^8 + 68 * s^6 * t^2 - 122 * s^4 * t^4 + 68 * s^2 * t^6 + t^8$ were a square.

Brute force search: yo-ho-ho and a bottle of rum!

There are many Euler bricks which is not parametrized as above:
A brute force search for $1 \leq a, b, c \leq 300$ gives $a = 44, b = 117, c = 240$ and $a = 240, b = 252 c = 275$ as the only two Euler bricks in that range. In the range $1 \leq a < b < c \leq 1000$ there are 10 Euler bricks:

a	b	c
44	117	240
85	132	720
88	234	480
132	351	720
140	480	693
160	231	792
176	468	960
240	252	275
480	504	550
720	756	825

In the $1 \leq a < b < c \leq 2000$, there are a 15 more, totalling 25.

a	b	c
170	264	1440
187	1020	1584
220	585	1200
264	702	1440
280	960	1386
308	819	1680
320	462	1584
352	936	1920
480	504	550
720	756	825
960	1008	1100
1008	1100	1155
1200	1260	1375
1440	1512	1650
1680	1764	1925

Searching $1 \leq a < b < c \leq 4000$, we get 54 Euler cuboids, in $1 \leq a < b < c \leq 8000$ there are 120:

44	117	240	528	5796	6325	968	2574	5280	1680	1764	1925
85	132	720	560	1920	2772	980	3360	4851	1755	4576	6732
88	234	480	561	3060	4752	1008	1100	1155	1920	2016	2200
132	351	720	572	1521	3120	1012	2691	5520	2016	2200	2310
140	480	693	595	924	5040	1056	2808	5760	2160	2268	2475
160	231	792	616	15	3360	1100	2925	6000	2400	2520	2750
170	264	1440	640	924	3168	1120	1617	5544	2496	2565	7920
176	468	960	660	1755	3600	1120	3840	5544	2640	2772	3025
187	1020	1584	680	1056	5760	1144	3042	6240	2880	3024	3300
195	748	6336	700	2400	3465	1155	6300	6688	3024	3300	3465
220	585	1200	704	1872	3840	1188	3159	6480	3120	3276	3575
240	252	275	720	756	825	1200	1260	1375	3360	3528	3850
255	396	2160	748	1989	4080	1232	3276	6720	3600	3780	4125
264	702	1440	748	4080	6336	1260	4320	6237	3840	4032	4400
280	960	1386	765	1188	6480	1276	3393	6960	4032	4400	4620
308	819	1680	780	2475	2992	1280	1848	6336	4080	4284	4675
320	462	1584	792	2106	4320	1287	2640	7020	4320	4536	4950
340	528	2880	800	1155	3960	1320	3510	7200	4560	4788	5225
352	936	1920	828	2035	3120	1364	3627	7440	4800	5040	5500
374	2040	3168	832	855	2640	1400	4800	6930	5040	5292	5775
396	1053	2160	836	2223	4560	1408	3744	7680	5040	5500	5775
420	1440	2079	840	2880	4158	1440	1512	1650	5280	5544	6050
425	660	3600	850	1320	7200	1440	2079	7128	5520	5796	6325
429	880	2340	858	1760	4680	1452	3861	7920	5760	6048	6600
440	1170	2400	880	2340	4800	1540	5280	7623	6000	6300	6875
480	504	550	924	2457	5040	1560	2295	5984	6048	6600	6930
480	693	2376	935	1452	7920	1560	4950	5984	6240	6552	7150
484	1287	2640	935	5100	7920	1600	2310	7920	6480	6804	7425
510	792	4320	960	1008	1100	1656	4070	6240	6720	7056	7700
528	1404	2880	960	1386	4752	1664	1710	5280	6960	7308	7975

The number of Euler bricks appears to grow with respect to the box size because if (a, b, c) is an Euler brick, then (ka, kb, kc) is an Euler brick too. It would be interesting to know how primitive Euler bricks are distributed.

Modular considerations: pieces of eight! Pieces of eight!

If we take a Diophantine equation and consider it modulo some number n, then the equation still holds. Turning things around: if a Diophantine equation has no solution modulo n, then there is no solution in the integers. By checking all possible solutions in the finite space of all possible cases, we can also determine some conditions, which have to hold.

Example: $5x^4 = 3 + 7y^4$ has no integer solutions because modulo 8, we have no solution because modulo 8 we have $x^4, y^4 \in \{0, 1\}$.

To use this idea, lets assume we deal with prime Euler bricks, bricks for which the greatest common divisor of a, b, c is 1.

For $n \in \{2, 3, 5, 11\}$ as well as $n \in \{2^2, 3^2, 4^2\}$, there exists at least one side of an Euler brick which is divisible by n.

Proof. The case $n = 2, 4, 16$ follows directly from properties of Pythagorean triples, for $n = 9$, use that if two (say x, y) are divisible by 3, then $x^2 - y^2 = a^2 - b^2$ is divisible by 9 and $a = b \pmod 3$ showing that also z has to be divisible by 3 and the cube is not prime.

Searching using irrational rotation: on a dead man's chest

The problem of solving Diophantine equations has a dynamical system side to it. Take one of the variables x as time, solve with respect to an other variable say y then write $y = (f(x))^{1/n}$ where f is a polynomial. We can study the dynamical system $(f(x))^{1/k} \to f(x+1)^{1/k} \bmod 1$ and look for n to reach 0. If there are several parameters, we have a dynamical system with multidimensional time.

For the problem to find s, t for which

$$\sqrt{s^8 + 68t^2s^6 - 122t^4s^4 + 68t^6s^2 + t^8}$$

is close to an integer, we can change the parameter s, t along a line and get incredibly close. Unfortunately, we can not hit a lattice point.

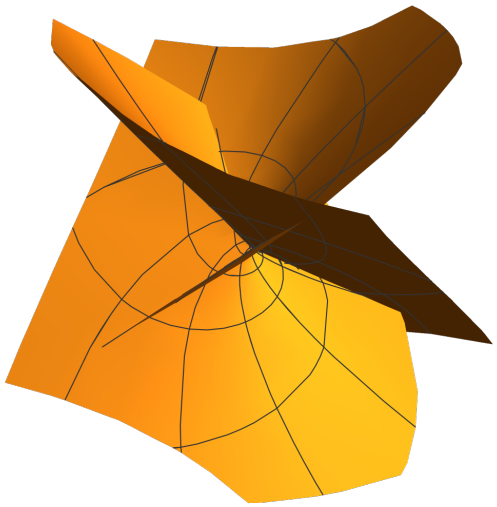


Fig 1. The Saunderson surface: a parametrized surface $r(s,t) = (a(s,t), b(s,t), c(s,t))$ of Euler bricks.

The treasure is not there: ney mate, you are marooned

Spohn is the "Ben Gunn" of the Euler brick treasure island. He has moved the treasure elsewhere. But maybe it does not exist. Anyway, Spohn [32] proved in 1972:

Theorem (Spohn): There are no perfect Euler bricks on the Saunderson surface of Euler bricks.

Proof. With $a = u(4v^2 - w^2)$, $b = v(4u^2 - w^2)$, $c = 4uvw; w^2 = u^2 + v^2$, we check $a^2+b^2+c^2 = w^2(u^4+18u^2v^2+v^4)$. Pocklington [27] has shown first in 1912 that $u^4+18u^2v^2+v^4$ can not be be square. His argument is more general. We can prove this more easily however:

Lemma (Pocklington): Unless $xy = 0$, the Diophantine equation $x^4 + 18x^2y^2 + y^4 = z^2$ has no solution.

Proof: x, y can not have a common factor, otherwise we could divide it out and include it to z. Especially, there is no common factor 2. If $x^4 + 18x^2y^2 + y^4 = (x^2 + y^2)^2 + 4^2x^2y^2 = z^2$ then we have Pythagorean triples which can be parametrized.
a) Assume first the triples are primitive, there is no common divisor among the triple $(x^2 + y^2)^2, 4^2x^2y^2, z^2)$.

(i) If x, y are both odd, we must have

$$\begin{aligned} x^2 + y^2 &= 2uv \\ 4xy &= u^2 - v^2 \ . \end{aligned}$$

The first equation proves that $x^2 + y^2 = 2 \bmod 4$. If $2uv = 2 \bmod 4$, both u, v must be odd. The second equation can now not be solved modulo 8. If $u = 4n \pm 1$, $v = 4m \pm 1$, then $u^2 - v^2$ is divisible by 8. But the left hand side of the equation is congruent to 4 modulo 8.
(ii) If x is odd and y is even, the Pythagorean triple representation is

$$\begin{aligned} x^2 + y^2 &= u^2 - v^2 \\ 2xy &= uv \ . \end{aligned}$$

Because y is even, the second equation shows that uv is divisible by 4 and because u, v have no common divisor, wither u is divisible by 4 or v is divisible by 4. If u is divisible by 4, the first equation can not be solved modulo 4. If v is divisible by 4, the first equation has no solution modulo 16: the right hand side is $0, 1, 4, 9$ modulo 16 while the left hand side is congruent to $5, 13$ modulo 16.

b) If there is a common divisor p among $(x^2 + y^2)^2$ and $4^2x^2y^2$ then it has to be 2, because any other factor p would be a factor of either x or y as well as of $x^2 + y^2$ and so of both x and y, which we had excluded at the very beginning. With a common factor 2, we have a Pythagorean triple parametrization

$$\begin{aligned} x^2 + y^2 &= 4uv \\ 4xy &= 2(u^2 - v^2) \ . \end{aligned}$$

but since x, y are both odd, $x^2 + y^2$ is congruent 2 modulo 4 contradicting the first equation.

This finishes the proof of the lemma and so the theorem of Spohn. It is remarkable that the result of Pocklington does not use infinite decent in this case. By the way, the article of Pocklington of 1912 has been checked out many times at Cabot library since this volume almost falls to dust.
Side remark: quartic Diophantine equations of this type form an old topic [23] (section 4). Fermat had shown using infinite descent that u^4+v^4 is never a square so that $u^4+v^4=z^4$ has no solution. As is well known, he concluded a bit hastily that he has a proof that $x^p+y^p=z^p$ has no solution for all $p>2$ but that the margin is not large enough to hold it.

Large numbers: shiver my timbers!

There are more parametrizations to be explored. Euler got

$$\begin{aligned} a &= 2mn(3m^2-n^2)(3n^2-m^2) \\ b &= 8mn(m^4-n^4) \\ c &= (m^2-n^2)(m^2-4mn+n^2)(m^2+4mn+n^2) \end{aligned}$$

for which $x^2+y^2=4m^2n^2(5m^4-6m^2n^2+5n^4)^2$, $^2+z^2=(m^2+n^2)^6$, $y^2+z^2=(m-n)^2(m+n)^2(m^4+18m^2n^2+n^4)^2$.
In that case, we have $x^2+y^2+z^2=(m^2+n^2)^2(m^8+68m^6n^2-122m^4n^4+68m^2n^6+n^8)=(m^2+n^2)^2[(m^4+n^4)^2+2m^2n^2(17m^4-31m^2n^2+17n^4)]$.

Computer algebra systems like to compute as long as possible in algebraic fields. For example:

```
Expand[(5 + Sqrt[5])^6]
```

produces the result

```
72000+32000 Sqrt[5]
```

This is a much more valuable result than a numerical value like 143554.1753.... The evaluation of numerical values in Mathematica is quite mysterious: sometimes, it works quite well:

```
N[Sqrt[2^171 + 1]] - N[Sqrt[2^171 + 1], 100]
```

Sometimes, it does not

```
N[Sqrt[2^117 + 1]] - N[Sqrt[2^117 + 1], 100]
```

which gives in this case a value of -64. Even increasing the accuracy like with

```
$\$$MaxExtraPrecision=20000000000;
```

Wolfram research promised to fix this problem.
By the way, this issue is much better in Pari. How to compute with large accuracy in the open source algebra system Pari/GP? Pari projects algebraic integers correctly, even with millions of digits:

```
\p 1000000
a=sqrt(2^117+1)
```

It can compute up to 161 million significant digits (you have to increase the stack size to do so), like defining

```
parisize = 800M
```

in the .gprc file. It still can produce an overflow depending on your machine. But working a million digits or so is ok.

History: Captain Flints logbook

In 1719 by **Paul Halcke**, a German accountant, who would also do astronomical computations, found the smallest solution [4]. Nothing earlier seems to be known.

N. Saunderson found in 1740 the parametrization with two parameters mentioned above. Only in 1972, it was established by Spohn that the parametrization does not lead to that these parametrizations do not lead to perfect Euler bricks. Jean Lagrange gave an other argument in 1979 also.

Leonard Euler found in 1770 a second parametrization and in 1772 a third parametrization. After his death, more parametrizations were found in his notes.

Modern considerations: the black spot

The topic has appeared several times in American Mathematical Monthly articles and was even a topic for a PhD theses in 2000 in Europe and 2004 in China. Because of its simplicity, it is certainly of great educational value. The topic appears for example in a journal run by undergraduates similar to HCMR [26].

Noam Elkies told me:

"The alebraic surface parametrizing Euler bricks is the intersection in P^5 of the quadrics $x^2+y^2=c^2$, $z^2+x^2=b^2$, $y^2+z^2=a^2$ which happens to be a K3 surface of maximal rank, so quite closely related to much of my own recent work in number theory. Adding the condition $x^2+y^2+z^2=d^2$ yields a surface of general type, so it might well have no nontrivial rational points but nobody knows how to prove such a thing."

Noam also remarked that Euler's parametrization would only lead to a finite number of perfect Cuboids as a consequence of Mordell's theorem. There seems however no reason to be known which would tell whether there are maximally finitely many primitive perfect cuboids.

There are also relations with elliptic curves since a system of quadratic equations often define an elliptic curve. See [20]. The article [18] which mentions also relations with rational points on plane cubic curves.

The problem appeared also in articles for the general public. In 1970 Martin Gardner asked to find solutions for which 6 of the 7 distances in the cuboid are integers. If the large diagonal

is an integer, these are no more Euler bricks, unless we would have a perfect brick.

As for any open problem, it is also interesting to look more fundamental questions. As with many open problems, the problem to find a perfect Euler brick could be undecidable: we would not be able to find a proof that there exists no Euler brick. This is possible only if there is indeed no Euler brick. You can read an amusing story about Goldbach conjecture in "Uncle Petros and the Goldbach conjecture", where the perspective of such an option blew all motivation of poor uncle Petros to search for the Goldbach grail. [5]

Treasure problems: scatter and find 'em!

Many unsolved problems like the Goldbach conjecture, the Riemann hypothesis, the problem to find perfect numbers, or the problem of finding perfect Euler bricks, finding dense sphere packings in higher dimensions, are mathematical tasks which could in principle be solved quickly: by finding an example - if it should exist:

- Writing down an integer which can not be written as a sum of two primes would settle the Goldbach conjecture.
- Finding an integer for which the sum of the proper divisors is the number itself.
- Find a root of the zeta function with $Re(z) \neq 1/2$. Just one lucky punch would be needed to solve the problem.

But like treasure hunting, aiming to catch such a treasure is not a good business plan or a way to make a living: the treasure simply does not need to be there. If it does not exist, the most skillful treasure hunter can not be successful.

But it is the search which is interesting, not the prospect of finding anything.

By the way, numerical searches for the grail of a perfect cuboid have been done. Randal Rathbun has found no perfect cuboid with least edge larger than 333750000. The greatest edge is larger than 10^9. See [8]. Treasure hunters all over the world have probably gone even further. See [30] on ArXiv.

Update, May 20 2022: Robert Matson (Matson, Robert D. "Results of a Computer Search for a Perfect Cuboid" (PDF). unsolvedproblems.org. Retrieved May 23, 2022.) reports that *there are no perfect cuboids with odd side less than 25 trillion, and no perfect cuboids with minimum side less than 500 billion.*

References

[1] A. Björner. A cell complex in number theory. *Advances in Appl. Math.*, 46:71–85, 2011.
[2] J. Bronowski. *The Ascent of Man.* BBC, 1973.
[3] R.C. Buck. Sherlock Holmes in Babylon. *American Mathematical Monthly*, 87:335–345, 1980.
[4] L.E. Dickson. *History of the theory of numbers.Vol.II:Diophantine analysis.* Chelsea, New York, 1966.
[5] A. Doxiadis. *Uncle Petros and Goldbach's Conjecture.* Bloomsbury, USA, New York, 2000.
[6] H. Eves. *Great moments in mathematics (I and II.* The Dolciani Mathematical Expositions. Mathematical Association of America, Washington, D.C., 1981.
[7] R. Guy. The strong law of small numbers. *Amer. Math. Monthly*, 95:697–712, 1988.
[8] R. K. Guy. *Unsolved Problems in Number Theory.* Springer, Berlin, 3 edition, 2004.
[9] C.H. Kahn. *Pythagoras and the Phythagoreans, A brief history.* Hackett Publishing Company, 2001.
[10] V. Katz. *Mathematics of Egypt, Mesopotamia, China, India and Islam.* Princeton Univ. Press, 2007.
[11] O. Knill. A multivariable chinese remainder theorem. https://arxiv.org/abs/1206.5114, 2005-2012.
[12] O. Knill. Hunting for Perfect Euler Bricks. *The Harvard College Mathematics Review*, 2, no 2, 2008.
[13] O. Knill. Treasure Hunting Perfect Euler Bricks. Mathtable talk, February 24, 2009, 2009.

[14] O. Knill. On primes, graphs and cohomology. https://arxiv.org/abs/1608.06877, 2016.
[15] O. Knill. Some experiments in number theory. https://arxiv.org/abs/1606.05971, 2016.
[16] O. Knill. Exploring creativity through computer algebra. *Tech-Based Teaching: Computational Thinking in the Classroom*, 2018. https://medium.com/tech-based-teaching/exploring-creativity-through-computer-algebra-c3788d1a06b7.
[17] O. Knill. Graph complements of circular graphs. https://arxiv.org/abs/2101.06873, 2021.
[18] J. Leech. The rational cuboid revisited. *American Mathematical Monthly*, 84:518–533, 1977.
[19] M. Livio. *Why? - What makes us Curious*. Schuster, 2017.
[20] Allen J. MacLeod. Parametric expressions for a nearly-perfect cuboid. maths.paisley.ac.uk/allanm/PDFILES/Newside.pdf.
[21] D.F. Mansfield. Plimpton 322: A study of rectangles. *Foundations of Science*, 26:977–1005, 2021.
[22] E. Maor. *The Pythagorean Theorem: A 4000 year history*. Princeton University Press, 2007.
[23] L.J. Mordell. *Diophantine Equations*, volume 30 of *Pure and Applied Mathematics*. Academic Press, London and New York, 1969.
[24] P. Nastasi and A. Scimone. Pietro mengoli and the six-square problem. *Historia Mathematica*, 21:10–27, 1994.
[25] O. Neugebauer. *The exact Sciences in Antiquity*. Dover Publications, second edition, 1969.
[26] A. Ortan and V. Quenneville-Bélair. Euler's brick. *The Delta-Epsilon: Mc Gills Undergraduate Mathematics Magazine*, Issue 2006. http://sums.mcgill.ca/delta-epsilon/issue06.html.
[27] H.C. Pocklington. Some Diophantine impossibilities. *Proceedings Cambridge Philosophical Society*, 18:110–118, 1912.
[28] A.S. Posamentier. *The Pythagorean Theorem: The Story of its Power and Beauty*. Prometheus, 2010.
[29] E. Kaplan R. Kaplan. *Hidden Harmonies*. Bloomsbury, 2011.
[30] R. L. Rathbun. The rational cuboid table of Maurice Kraitchik. *http://arxiv.org/abs/math.HO/0111229*, 2001.
[31] E. Robson. Words and Pictures: New Light on Plimpton 322. *Amer. Math. Monthly*, 109:105–120, 2002.
[32] W. Spohn. On the integral cuboid. *American Mathematical Monthly*, 79:57–59, 1972.
[33] R.L Stevenson. *Treasure Island*. Cassell and Co., 1883.
[34] I. Stewart. *Visions of Infinity*. Basic Books, 2013.
[35] P. Strathern. *The big idea: Pythagoras and his theorem*. Arrow books, 1997.
[36] F.J. Swetz and T.I. Kao. *Was Pythagoras Chinese?* Pennsylvania State University Press, 1988.

Department of Mathematics, Harvard University, Cambridge, MA, 02138

THE INKA QUIPU ENIGMA

OLIVER KNILL

1. Introduction

1.1. The history, mathematics and database technology of the **quipu** [1], the "talking knots" of the Inka empire is a fascinating subject. Quipu are an original approach to number systems, database structures. Unlike marks on bones, tally sticks or clay tablets, ink on wood, papyrus or paper, it is a topological encoding, similarly in nature than genetic code is woven from protein knots. The first scientific study of quipus began by **L. Leland Locke**. His important article [11] documented in a very clear way how knots were used for recording numbers. In his introduction, Locke also pointed out that also in other parts of the world, like China, knot records have preceded the knowledge of writing.

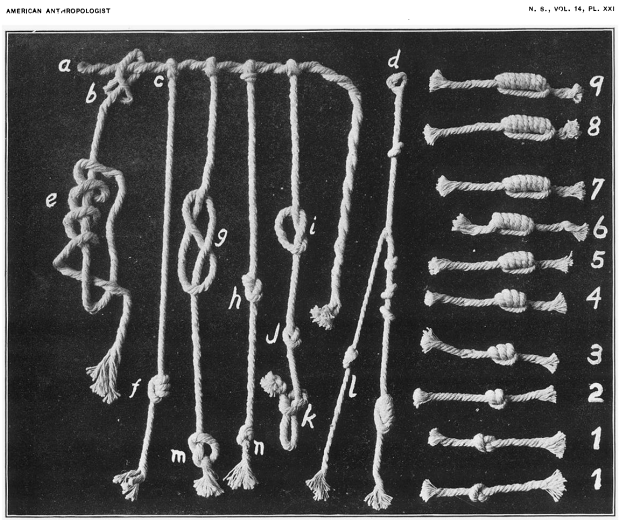


FIGURE 1. A page from [11].

Date: 10/22/2018, updated 1/31/2022 for Math E 320.

[1]Quipu and Khipu are equivalent spelling variations

1.2. Recent research pointed to **Rosetta stone break-through discoveries** leading to publications for a general audience like [6, 14, 5, 20]. In 2018, when this document started, there there was also quipu exhibit at the Boston museum of fine arts. Naturally, these popularizations or reports hide the work which is needed to investigate the topic. There is the field work of digging out, cleaning, reading and then cataloging the information, then to place the data into the context of the history, linguistic, and culture of the time and finally to translate interpret and cross referencing the data. In the quest to decode the quipu cypher, there has been spectacular progress for post-colonial quipus [7, 13] and progress in better understanding non-numerical pre-conquest quipus [4].

2. Knots, Links and Graphs

2.1. Strictly speaking, for a mathematician, a quipu is neither a **knot** (a closed loop in space) nor a **link**, a collection of non-intersecting knots in space. But they are links in a generalized sense in that they would be links if the ends of the individual ropes were connected. It is not so much the topology of quipu which is of interest for researchers but the information content which is encoded topologically. Because only three different type of knots appear in Inka style data (simple knots, figure eight knots and long knots) (whose topology is well understood), these entities could be replaced by symbols like $L4, S, E$ standing for a long knot with 4 turns, a single knot or a figure eight knot. A quipu can be described as a graph on which scalar and vector data are attached. The scalar data assign to a node the knot type or the attachment type, if the node is branching off there. The vector data which describe the connecting strings are determined by ply and spin direction, attachment type, color and the material of the knot. For a computer scientist a quipu is an example of a **graph database**.

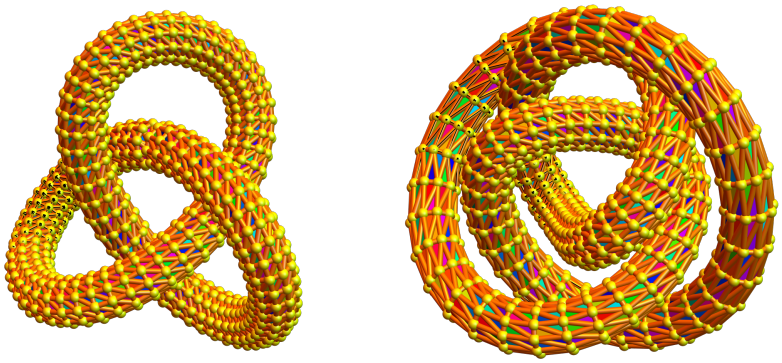


Figure 2. The trefoil knot and a figure eight knot.

3. Crypto riddles

3.1. The **Inca code** is a cypher which has not yet cracked. While the numerical data encoding are quite well understood, the problem lies in understanding non-numerical signs. Crypto riddles have always attracted the interest of the general public. Examples are the **Maya code**, the **Egyptian hieroglyphs**, the **German Enigma** during the second world war or the fictional alien pictorial language which is at the center of the movie "**Arrival**". An other example of an outstanding riddle is the **"Antikythera" instrument** which is believed to be an early **analogue computer** used for astronomical computations. More riddles have presented themselves when trying to decode texts from **Palimpsests**, texts which are hidden beneath other texts. An example is the Archimedes Palimpsest. In those cases, reading the text requires first to reveal the structure as the text had been erased and written over.

Figure 3. The Anticitera, the Maya and the Rosetta stone.

4. Rosetta stone moments

4.1. Also in the case of the German enigma code which was cracked at Bletchley Park, the problem was not entirely mathematical. One had to wait for Rosetta stone moments, clues like knowledge of the **weather code**, or rely on **planted information** which allowed the cryptographers to attack the code using **crib-based decryption** techniques. In the case of the quipu, the task is harder because there are no known cribs (at least from the pre-colonial time) and many of these documents were destroyed in the wake of the colonial conquest and because quipu from regions with high precipitation deteriorated rapidly if not preserved as they are made of organic material like wool.

4.2. There are less than 1000 quipu known today. The **Berlin collection** contains about a third. The decoding problem has linguistic, historical and anthropological context. Understanding the content of a coded text or new language needs "Rosetta stone moments" like in the case of the hieroglyphs, where Champoleon and Young have been able to crack the code of the hieroglyphs. The quipu form a cryptological riddle in which plain text information is missing. Since the information is believed

to be non-phonetic, the problem is harder than in the case of hieroglyphs, the cuneiforms or the Maya code.

FIGURE 4. Some quipu researchers: Leland Locke, Marcia and Robert Ascher, Sabine Hyland.

5. Algebra with strings attached

5.1. For a mathematician, quipu can be fascinating in various ways. One knows already quite a bit about the numerical aspects [2]. But mathematics can be understood as a more general concept, not only as the science of numbers, or the quest to understand algebraic or geometric objects but more generally as a **science of structure**. For a mathematician, a **language** is a mathematical structure, usually a subset of a monoid of words, in which a grammar and axiom systems define what is meaningful in this language. [10].

5.2. In formal language theory, a language is a set of strings over some finite alphabet A. There is an operation on the set of string, which is concatenation. This is associative. Together with the zero element, the empty string, one has a **monoid**. A linear order on A defines a lexicographical ordering on the language. If we look at language encoded on a quipu however, then the monoid structure is gone. There are algebraic operations on graphs, like disjoint union or joins (which both can serve as additions) or product operations which complement them rendering the category of finite simple graphs into rings, but these structures have no meaning in language. The addition of strings to a quipu needs more information as strings can be attached in different ways.

5.3. Communicating with knots is a completely different approach to writing. The sentences are not elements in a monoid because there is a spacial **nonlinear approach**. One can encode a quipu as a weighted graph, where the nodes are the knots, which are labeled by the value of the knot, the spin or attachment direction.

The edges can be equipped with color, ply direction and hierarchy data too. Numbers are encoded using three different type of knots, but they can also be arranged in different ways leading to more information content than anticipated.

6. Nonlinear languages

6.1. But having content written down in a linear narrative way is not unique. This has also be developed by other cultures. We use pictures for example to represent mathematical statements, we use tables represent data, we use graphs to represent relations, mind maps are examples of graph information containers which are non-linear. In our time of electronic documents, we can add a parameter "detail" to a mathematical text. Varying the detail level allows then to zoom in and out in the knowledge landscape, similarly as we do when we look at a map of the earth. A map is a highly non-linear representation of data.

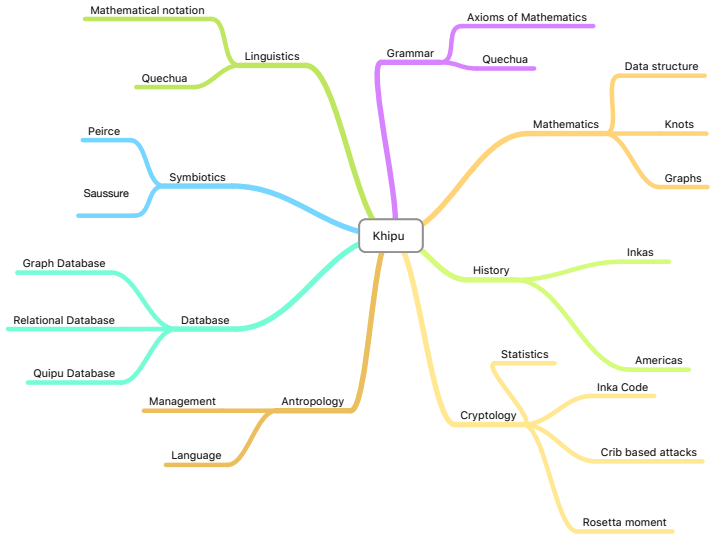


Figure 5. A **mind map** as an example of a non-linear language.

7. Popular culture

7.1. Intersections of linguistic and mathematics appear frequently in **pop culture**. The reason is that mathematics related to linguistics is more approachable than mathematics related to algebraic structures. We can mention the novels of Dan Brown, in which a Harvard symbiologist Robert Langdon is the hero. The field of

Symbology does not exist. We should also mention the movie "Contact", in which an alien language is broadcast from an other planetary system to us. The decoding of the language needed spacial insight as it was a three-dimensional document. Also remarkable is the movie "Arrival" in which a linguist and physicist work together to get access to a strange smoke ring based language spoken by two aliens "Abbot and Castello".

FIGURE 6. Linguistic in pop culture: Arrival and the Dan Brown story, Inferno and Contact.

8. Topological writing

8.1. First of all, the mathematical approach of the quipu is unique. It is a three dimensional writing, dealing with topological objects known as knots and links which are of interest to mathematicians, and physicists. For a computer scientist it is a **graph database**. Using spacial, material and color information, the Inkas have placed information onto the strings. An introduction about this fascinating topic is [20].

9. Seeing real samples

9.1. The museum of fine arts in Boston currently has an exhibit showing off some of the quipus from the Peabody museum at Harvard. While quipu are always mentioned in the context of the origins of number systems, there had been much progress recently in understanding more about these Inka code. This and some art installation must have prompted the exhibit at the museum.

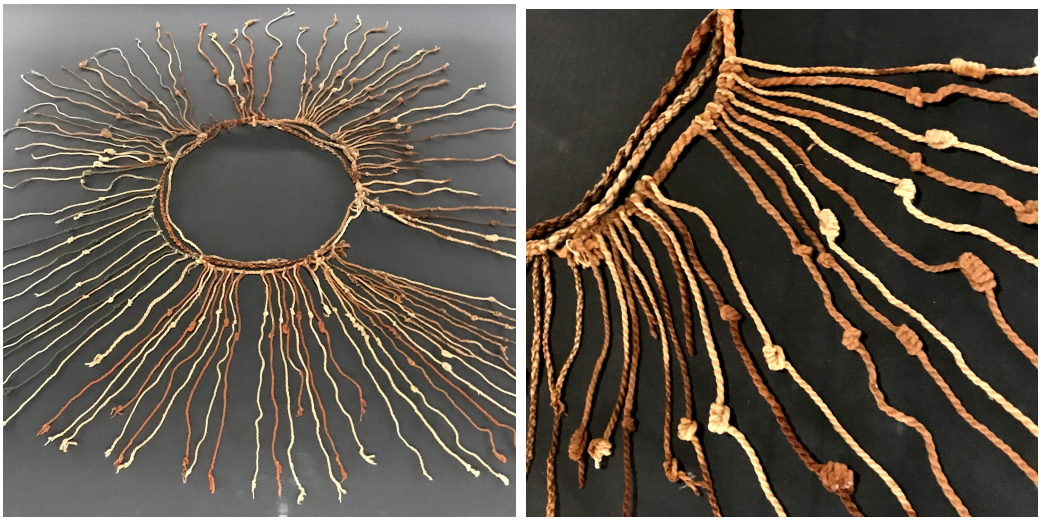


FIGURE 7. Photos of quipus from the exhibit at the Boston museum of fine arts.

10. Mathematical notation

10.1. The quipu research sheds light onto the origins of mathematical notation, the origins of number systems and even the philosophy of mathematics [17]. Talking knots are a highly original approach to language and naturally are of extreme interest in linguistics, semiotics, sociology and anthropology. There are also relations to **education** because the way human cultures develop mathematics is similar to how students acquire it. Recent battles about notation syntax (the PEMDAS wars) illustrate how "antropological" mathematical notation is: computers and humans empirically disagree with reading mathematical content like $6/2(1+2)$. Most humans get 1 while computers get 9. The syntax laws are ambiguous [3]. The PEMDAS wars are silly because it is a battle in a realm where no consensus has been built by authority. It is a heated battle because there are some, who religiously defend their own interpretation of mathematical syntax.

11. Management

11.1. An efficient **record keeping system** was necessary for building the Inca empire. Engineering projects involved calculations, recording of data, calculating ratios and proportions. As the largest empire in the pre-Columbian new world between Ecuador and Columbia, it stretched 5000 km along the Andes. The **Tawantinsuyu**, "the four parts divided together" or "land of the four quarters" as it was called covered a complex environment reaching deserts, the Andes or the Amazon.

11.2. The quipu story leads to insight in management and organization theory [20]. The Inka empire which lasted only for a short time (1400-1532) was able to develop and run effectively because of technology. (Of course also using military force but it appears that the power of organization can complement military conquests. This has been proven to be true even up to very recent times. Failed military adventures failed at providing management.) The quipu technology was essential for management and administration of such a complex structure. In some sense it must have enabled progress similarly as the **modern internet** now does: the Inka road network [19, 1] compares to the internet backbone and the quipu are the files.

11.3. To conclude, the story of the Inkas is an **allegory** for our time: investement in infrastructure, in language, in organization can be as powerful as military power. It is modern because in our time, power is also more and more established by entities which know how to gather process and understand information.

12. Genetic code

12.1. Interestingly, the Inkas stored information similarly than our **genetic code** is stored, on knots: our DNA consists of strands of twisted **DNA molecules** while quipus use twisted rods. It appears that modern bioinformatics is getting inspired by quipus [16]. Color encodings of electronic parts like resistors encode numbers in colors.

12.2. Mind-boggling is also that the Inkas used binary encoding [18] using spinning, plying and knot directionality and the markednes theory in linguistic. Binary steps were also done in Chinese hexagrams where the binary encoding had six bits ($2^6 = 64$).

12.3. Binary symmetries appear also in biology and modern physics, where chirality and parity are important. In physicist it is the weak force which shows an asymmetry, in biology it is the orientation of the DNA, which is dominant. There is also a left handed Z-DNA. In the Urton terminology of markedness, this would be the marked version.

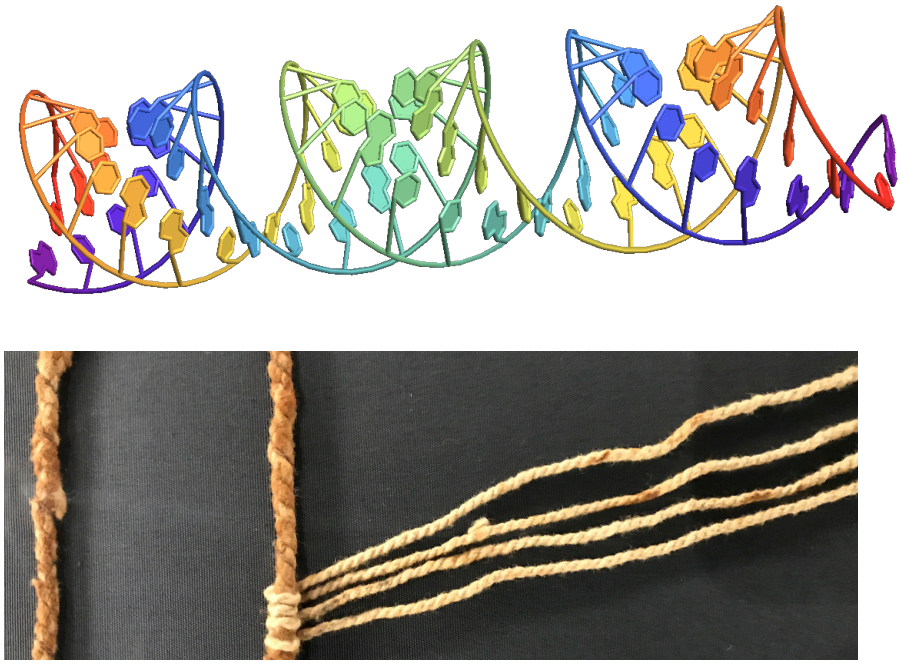


FIGURE 8. DNA and Quipu both have orientations.

13. Graph Database

13.1. Organization through inka decimal administration, required time accounting, census data to be organized on quipu by **quipukamayuq** (professional quipu writers), who had an **information technology** (IT) structure with a consolidated database in **Cuzco**, a prerunner of the "cloud". The cloud is just a modern word for a decentralized "main frame". If one would compare the quipu with files of modern computing, the analogue of the internet was realized by **Chaskis**, the quipu runners.

13.2. In our time of information technology, we deal a lot with three dimensional physical space: we have **augmented reality**, **computer vision**, **3D scanning** or **3D printing** technologies. Usual writing is two dimensional. The quipu system therefore appears very modern. Our own genetic code is encoded on knotted devices, the DNA, we use **graph based** databases, like Neo4J. Graph databases are an alternative to **relational databases**. They appear to be superior if the data structures are complicated.

14. The Unix philosophy

14.1. But one does not have to go far. One of the most popular databases used is the **Unix file system**, which organizes information in a **tree**. This technology allows comfortably to work with a half a dozen tera bytes of data at the finger tips and split different things into different tree branches (**directories**). This smaller quipu project (which occupied me over a few weeks) is an independent tree in my Unix database. Like every course, every website I maintain, my library with thousands of electronic documents, programming parts etc, they are all comfortably separated and organized like on a quipu.

14.2. One of the most important insights could be that **Like the Unix file system, the quipu database system is a paradigm**. It is a **gem in simplicity** and efficiency and very close to the **UNIX idea**. This principle was adopted also for our AI experiment of 2003 [9], where the AI bot was just a Unix file system and the intelligent agent just parses a sentence the travels the file system to do things as the nodes of the file system can be programs or little scripts which look things up. One advantage of this **quipu way** is that it is highly scalable. The industry uses it even with peta bytes of data while any conventional data base would get challenged. Extending a quipu data base is very easy, just add an other strang of nodes or produce more subsidary nodes. Similarly, a Unix file system can virtually have unbounded capacity.

15. The problem of backup

15.1. The only limitation in scale is the size of the harddrives. I personally currently have my files on 5TBytes external drives which are then stored in a frozen and of course encrypted form also in different locations (as the Inkas did). There are currently about 8million files there. They can be tiny text or program fragments, or larger documents like books, pictures or movies. But I would not store this in the cloud as one can also learn from history. The most obvious one is that services and companies die or change their focus, cutting off things which are no more profitable. Companies are no charity. The Inkas saved things in the "cloud" which was then their main capital "Cusco". And we all know what happened when the Spaniards invaded the place. Many major databases were destroyed and less than 1000 quipus survived.

15.2. My own data would even survive if Boston would be annihilated by a nuclear catastrophe (the analogue of a colonialization disaster) or all cloud services would have bit the dust. [One can easily imagine scenarios in which they could disappear in the near future. Examples are CPU leaking concerns, lawsuits due to copy rights or then that companies running the business will simply die or forced by some rogue government to make things accessible.] In the past, the surviving quipu were stored

and backed up in hidden decentralized places. Unfortunately for us, we can not read most of the non-numerical data. The Inkas somehow used to encrypt things (even so this had not been the main intention it had the advantage of some privacy as the quipus contained what we would call today bank information or services owned). Also this is a lesson: never store information in a form which is not accessible by simple tools for which public domain or at least open source tools exist to read it.

15.3. My own small quipu project is a small branch in a bigger Unix tree of my work stations (which are synced regularly). My "quipu pendant string" contains only 500 MBytes of data currently but it includes scanned books, documents, the Harvard khiup database, articles and pictures as well as texts about quipu. If in future, more things should appear, I would add it as "subsidiaries" as the Inkas did when adding more information to a primary cord. I have absolutely no problem to find things like that as it is in of of the 3 major project branches in my Unix file hierarchy. It is nice to see that this simple but efficient storage paradigm is actually Inka technology.

16. Reversed Polish Notation

16.1. An important feature of the Quechua language is **agglutination**, which allows that operators often can be found at the end. Like "ni=I" appears at the end of **Runasimi-ta yacha-ku sa-ni**. (People language, learn, now, I) or **Oliver, Wasi-Ta ruwan** which translates as Oliver house builds. [8]. Despite that linguists call Quechua a SOV language (Subject, Object, Verb), the aggultinative part makes it possible to put a subject suffix and have the subject at the end.

16.2. This reminds of the reverse polish notation RPN (still used in stack oriented programming languages like **Poscript** or **Bibtex**). One sees also reverse order in numbers like Quepchua: 13, "ten, possessor of three", while we say "thirteen". In a **stack oriented language**, you say $23x$ **rather than** $2x3 =$. We don't need the equal sign. Operators come to the end, which is more efficient and does not need equal signs. So, it appears that at least for addition and multiplication, no computing device is needed. And unlike for pebbles (bad for transportation) and tally sticks (we can not subtract), the computation with knots can do that.

16.3. The advantage of RPN is also that no brackets are needed. We use the RPN often when doing quick computations. For example, to compute the sum of the squares of the square roots of the first 100 primes, one can use the RPN notation in Mathematica: **Range[100] // Prime //Sqrt //N // Total** which has the advantage that I see in each step what has been computed. The traditional (written way) is to write: **Total[N[Sqrt[Prime[Range[100]]]]]** which gives just the end result but requires to write a nested sequence of brackets.

FIGURE 9. Non-RPN and RPN calculators.

17. SEMIOTICS

17.1. The Swiss **Ferdinand de Saussure** (1857-1913) was a pioneer in linguistic and semiotics. Saussure was eclipsed vastly both in scope and originality by his contemporary **Charles Sanders Peirce** (1939-1914) who only later would be recognized as one of the greatest thinkers and philosophers of his time. Frank Salomon suggests the quipus reference system to be a general purpose semasiography [15]. Semasiographic signs were present in multiple Andean systems.

17.2. Highly successful and persistent non-phonetic scripts are not only used in math notation (figures or combinatorial diagrams like Dynkin or Ferrers diagrams or commutative diagrams) but also in physics (Feynman diagrams for example), they also are common in music notation, programming flow charts, chemical formulas, choreographic notation, and knitting and weaving codes.

17.3. Notation is important in mathematics and it is linked to mathematics itself: Barry Mazur was cited in "Enlightening Symbols" [12] that *A seemingly modest change of notation may suggest a radical shift in viewpoint. Any new notation may ask new questions.* This also applies to the quipu language. It is a completely new angle to the origin of mathematical language and illustrates the richness and diversity with which the art of expressing mathematical thought has begun.

FIGURE 10. Two pioneers in linguistics: Ferdinand de Saussure (1857-1913) and Charles Sanders Peirce (1839-1914).

REFERENCES

[1] M. Anderson. 5 reasons the inka road is one of the greatest achievements in engineering. *In Anthropology, History and Culture*, 20, 2015.

[2] M. Ascher and R. Ascher. *Mathematics of the Incas: Code of the Quipu*. Dover Publications, 1981.

[3] F. Cajori. *A history of Mathematical Notations*. The Open Court Company, London, 1928.

[4] J. Clindaniel. Toward a grammar of the inka khipu: Investigating the production of non-numerical signs. Harvard dissertation, department of Anthropology, 2018.

[5] A. Shapiro (Host). Harvard student cracks incan code. https://www.npr.org/2017/12/28/574314933/harvard-student-cracks-incan-code.

[6] S. Hyland. Unraveling an ancient code written in strings. *Scientific American, Sapiens*, November 11 2017, 2017.

[7] S. Hyland. Writing with twisted cords: The inscriptive capacity of Andean khipus. *Current Anthropology*, 58(3):412–419, 2017.

[8] P. Jorgensen. Quechua - the living language of the incas. https://www.youtube.com/watch?v=KlXj28dXPAU, 2017.

[9] O. Knill, J. Carlsson, A. Chi, and M. Lezama. An artificial intelligence experiment in college math education. http://www.math.harvard.edu/knill/preprints/sofia.pdf, 2003.

[10] M. Kracht. *The Mathematics of Language*, volume 63 of *Studies in Generative Grammar*. Mouton De Gruyter, 2003.

[11] L.L. Locke. The ancient quipu, a peruvian knot record. *American Anthropologist*, 14:325–332, 1912.

[12] J. Mazur. *Enlightening Symbols, A short history of Mathematical notation and its hidden powers*. Princeton University Press, 2014.

[13] M. Medrano and G. Urton. Toward the decipherment of a set of mid-colonial khipus from the santa valley, coastal peru. *Ethnohistory*, 65:1–23, 2018.

[14] J. Radsken. Undergrad deciphers meaning of knots, giving native south american people a chance to speak. *Harvard Gazette*, August 25, 2017.

[15] F. Salomon. *The Cord Keepers, Khipus and Cultural Life in a Peruvian Village*. Duke University Press, 2004.
[16] A. Stasiak. Much like the khipu system, dna knots contain precious information. https://www.sib.swiss.
[17] G. Urton. *The Social Life of Numbers*. University of Texas Press, 1997.
[18] G. Urton. *Signs of the Inka Khipu*. University of Texas Press, Austin, 2003.
[19] G. Urton. Engineering a world with strings attached. Smithonian Institute Symposium, 2013.
[20] G. Urton. *Inka History in Knots*. University of Texas Press, 2017.

TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

Lecture 3: Geometry

3.1. Geometry is a science of **shape, size and symmetry**. It is one of the oldest mathematical disciplines. It appears in some of the earliest documents of human kind like the Rhind papyrus from 1600 BC. As shapes have aesthetic value, geometry also relates to art and design. While arithmetic focuses on numerical structures, geometry builds, relates and describes metric structures. It is far from limited to shapes that we can physically realize in our world; geometry can also describe objects of large, fractional or infinite dimension. In geometry, not even the sky is the limit.

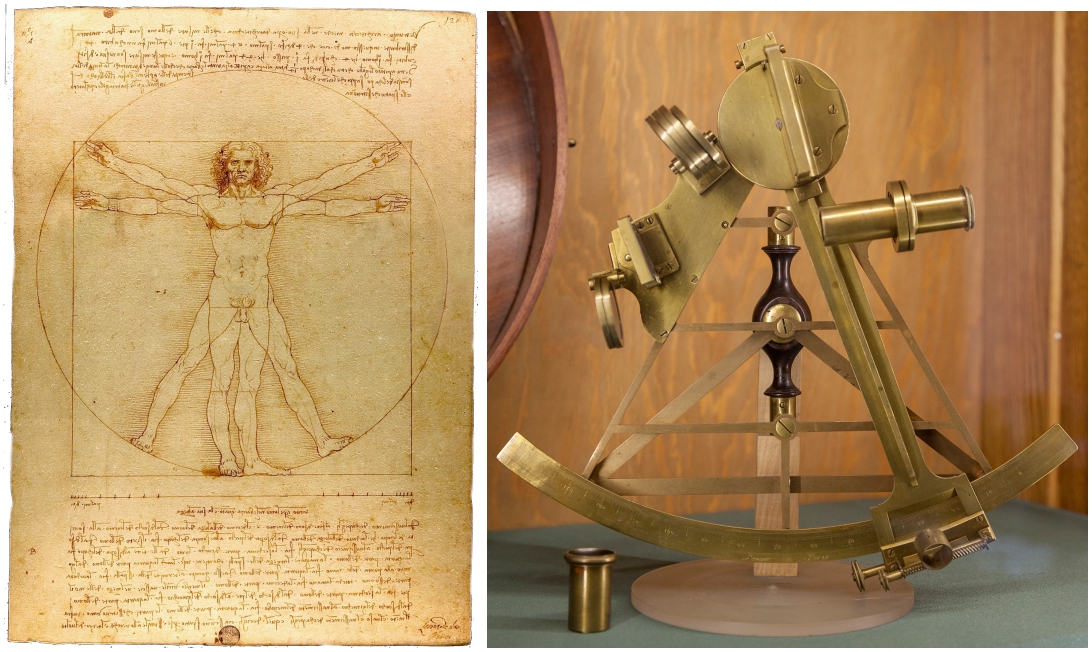


FIGURE 1. The Vitruvian man (1490) by Leonardo da Vinci not only features basic geometric features like angles, proportion, squares and circle, it also relates to art. The sextant (Collegium Matopolski Instytut Kultury) is a symbol for measurements on earth like to determine the position on earth.

3.2. Already the first geometric drawings have relations with arithmetic: the multiplication of two numbers as an **area** of a **shape** that is invariant under a physical **symmetry** rotating the rectangle from a $n \cdot m$ to $m \cdot n$ and so justify a naive commutativity assumption for multiplication. Non-commutative or quantum geometries later generalized geometries even further. A guide is Felix Klein's **Erlanger program** used symmetries to distinguish geometries. Symmetries links geometry also with algebra an other core pillar of mathematics.

3.3. One of the earliest connections between number systems and geometry came through identities like the **Pythagorean triples** $3^2 + 4^2 = 5^2$ which were interpreted and drawn geometrically. It is related to the concept of **right angle** which is the most symmetric angle besides 0. **Symmetry** manifests itself in quantities which are **invariant**. Invariants are most central aspects

of geometry and often numerical like Euler characteristic. Generalizing the realm of symmetries leads then to other related fields like topology.

3.4. In this lecture, we first look at a few results related to the first discoveries in geometry. We will start with a few smaller miracles happening in triangles as well as a couple of gems: **Pythagoras**, **Thales**,**Hippocrates**, **Feuerbach**, **Pappus** or **Morley**, **Butterfly**. They all illustrate the importance of symmetry and also extremely approachable as we can realize and see even build the objects.

3.5. Much of geometry is based on our ability to measure **length**, the **distance** between two points. Indeed, the etymology of the word geometry comes from measuring distances on the earth. Geometric thinking became more and more important when human extended their horizon. Discovering new worlds required to travel more efficiently, first by ship. Also modern global positioning systems (GPS) are built on simple geometric ideas like that enough differences between distances between various satellites to you determine your positions. It does not stop with space, because light travels with a universal speed, distances are related to time spans.

3.6. Having a notion of distance $d(A, B)$ between any two points A, B, we can look at the next more complicated object, a **triangle** which is a set A, B, C of 3 points. Given a triangle ABC, are there relations between the three possible distances $a = d(B, C), b = d(A, C), c = d(A, B)$? If we fix the scale by $c = 1$, then $a + b \geq 1, a + 1 \geq b, b + 1 \geq a$. For any pair of parameters (a, b) in this region, there is a triangle. A triangle also defines angles leading to **triangulations**, for example using sextants.

3.7. The concept of distance leads to the notion of **spheres**, the set of points with fixed distance r from a point. In the plane, the sphere is called a **circle**. A natural problem is to find the circumference $L = 2\pi$ of a unit circle, or the **area** $A = \pi$ of a unit disc, the **surface area** $S = 4\pi$ of a unit sphere and the **volume** $V = 4 = \pi/3$ of a unit sphere. Measuring the length of segments on the circle leads to **angle** or **curvature**. Because the circumference of the unit circle in the plane is $L = 2\pi$, angle questions are tied to the number π, which Archimedes already has approximated with rational numbers.

3.8. **Volumes** were among the first quantities, Mathematicians wanted to measure and compute. A problem on **Moscow papyrus** dating back to 1850 BC explains the formula $h(a^2 + ab + b^2)/3$ for a truncated pyramid with base length a, roof length b and height h. Archimedes achieved to compute the **volume of the sphere** by seeing that it is the volume the complement of the cone inside the cylinder which has at height z a slice of area $\pi - \pi z^2$. The volume of the half sphere therefore is volume of the complement of the cone inside the cylinder which is $\pi - \pi/3 = 2\pi/3$. Later, using calculus and analysis even stronger tools to compute volumes became available.

3.9. The first geometric explorations were done in flat two-dimensional space. Highlights are **Pythagoras theorem**, **Thales theorem**, **Hippocrates theorem**, and **Pappus theorem**. Discoveries in planimetry have been made later on: an example is the Feuerbach nine-point theorem from the 19th century. Ancient Greek Mathematics is closely related to history. It starts with **Thales** goes over Euclid's era at 500 BC and ends with the threefold destruction of Alexandria 47 BC by the Romans, 392 by the Christians and 640 by the Muslims.

3.10. Geometry was also a place, where, in the hands of Euclid, the **axiomatic method** entered mathematics. More rigorous deductive proofs appeared at the same time also in number theory, especially in the context of prime numbers. The Pythagorean theorem leads naturally to Pythagorean triples, integers satisfying a Diophantine equation $x^2 + y^2 = z^2$. With axioms and proofs, mathematics became more organized and reliable. The first axioms of geometry were the five axioms of Euclid:

1. Any two distinct points A, B determines a line through A and B.
2. A line segment $[A, B]$ can be extended to a straight line containing the segment.
3. A line segment $[A, B]$ determines a circle containing B and center A.
4. All right angles are congruent.
5. If lines L, M intersect with a third so that inner angles add up to $< \pi$, then L, M intersect.

3.11. **Euclid** wondered whether the fifth postulate can be derived from the first four and called theorems derived from the first four "absolute geometry". Only much later, with **Karl-Friedrich Gauss**, **Janos Bolyai** and **Nicolai Lobachevsky** in the 19'th century, one has realized that for a **hyperbolic space** the 5'th axiom does not hold any more. This was just the beginning for many new geometries. Geometry can be generalized to non-flat, or even much more abstract situations.

3.12. Basic examples of **non-Euclidean geometries** are geometry on a sphere leading to **spherical geometry**. Then there is the geometry on the Poincare disc, an example of a **hyperbolic space**. These geometries are still rather limited. **Riemannian geometry**, which is essential for **general relativity theory** generalizes both concepts to a great extent. An example is the geometry on an arbitrary surface. Curvatures of such spaces can be computed by measuring length alone, which is how long light needs to go from one point to the next. Also Riemannian geometries have been generalized to geometries allowing for rather arbitrary metric spaces.

3.13. An important moment in mathematics was the **merge of geometry with algebra**. This step is often attributed to **René Descartes**. Together with algebra, the subject exploded to an enormous building called **algebraic geometry**. It is a geometry that can also can make use of computer algebra systems.

3.14. Here are some examples of geometries which are determined from the amount of symmetry which is allowed:

Euclidean geometry	Properties invariant under a group of rotations and translations
Affine geometry	Properties invariant under a group of affine transformations
Projective geometry	Properties invariant under a group of projective transformations
Spherical geometry	Properties invariant under a group of rotations
Conformal geometry	Properties invariant under angle preserving transformations
Hyperbolic geometry	Properties invariant under a group of Möbius transformations

3.15. We finally show four pictures about the 4 special points in a triangle. They will be the starting point of our lecture. We will see why in each of these cases, the 3 lines intersect in a common point. It is a manifestation of a **symmetry** present on the space of all triangles. **size** of the distance of intersection points is constant 0 if we move on the space of all triangular **shapes**. It's Geometry!

Beautiful theorems

3.16. The existence of the **centroid** (the intersection of medians) B, the **orthocenter** (the intersection of altitudes) O , the **circumcenter** (the center of the circumcircle) C and the **incenter** (the center of the incircle) I are already not completely obvious. We can show their existence algebraically. The points B, O, C are on a line, the **Euler line**.

3.17. The **Pythagorean theorem** does not need any introduction. Like $E = mc^2$, it is a famous quadratic law: for all right angle triangles of side length a, b, c, the quantity $a^2 + b^2 - c^2$ is zero.

3.18. The **3D Pythagoras theorem** tells that areas of the three sides of the pyramid add up to the base area. It is also called the **Faulhaber extension** or **de Gua theorem**. We can verify it by computing the area of the triangle $A = (a, 0, 0), B = (0, b, 0), C = (0, 0, c)$ which is $|\langle a, -b, 0\rangle \times \langle 0, b, -c\rangle|/2 = |\langle bc, ac, ab\rangle| = (bc^2 + ac^2 + ab^2)/4$.

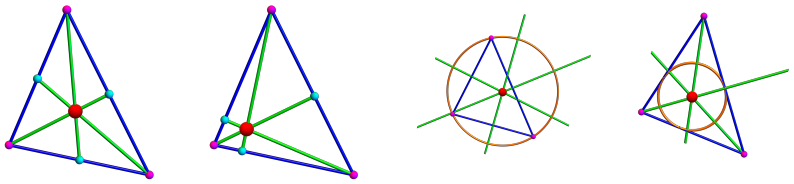


FIGURE 2. The existence of centroid B, orthocenter O, circumcenter C and incenter I are four little miracles for triangles. The points B, O, C are located on a line.

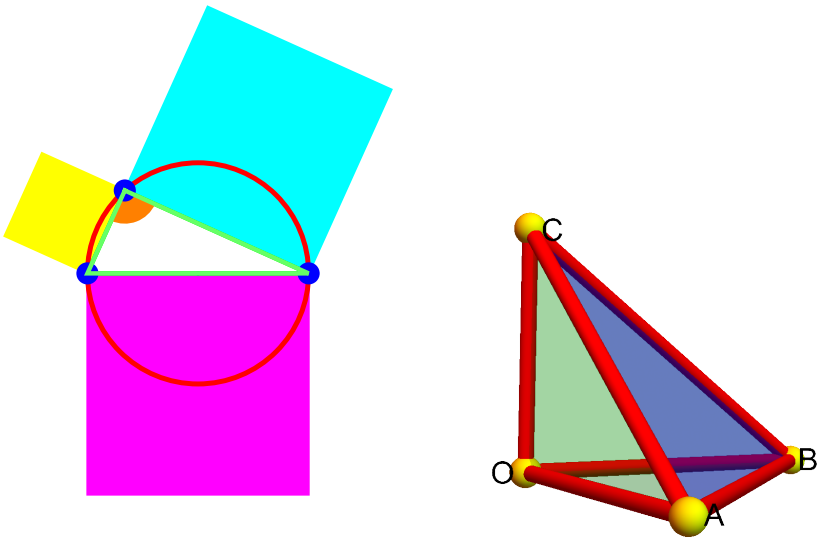


FIGURE 3. The two and three dimensional Pythagoras theorem.

3.19. Thales of Miletus (625 BC -546 BC) showed that if a triangle inscribed in a fixed circle is deformed by moving one of its points on the circle, then the angle at this point does not change.

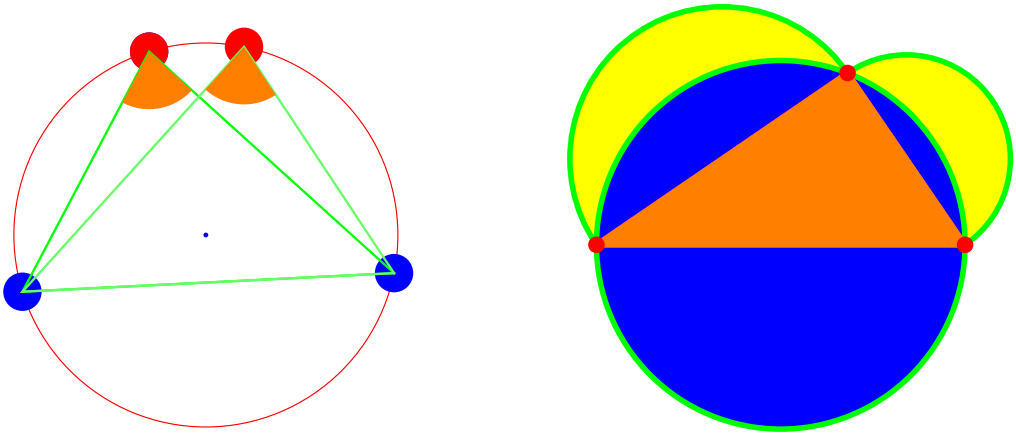


FIGURE 4. Thales theorem assures that the angle does not change when moving the point point on the circle. The Hippocrates theorem equates the areas of the "lunes" (moon shaped figures) with the triangle area.

3.20. The quadrature of the Lune is due to **Hippocrates of Chios** (470 BC - 400 BC). It is the first rigorous quadrature of a curvilinear area. The sum $L + R$ of the area L of the left moon and the area R of the right moon is equal to the area T of the triangle.

3.21. The proof of Morley's miracle we can decompose the triangle with 7 triangles.

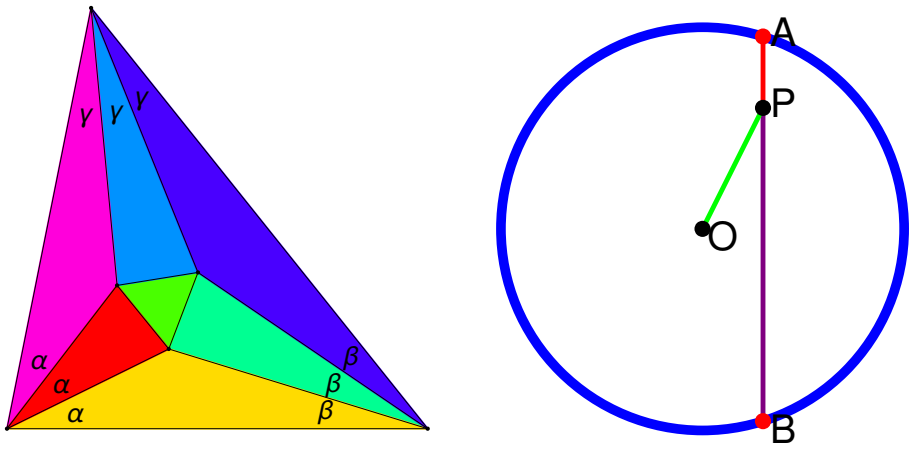


FIGURE 5. Morley's theorem produces an equilateral triangle from angle trisectors of an arbitrary triangle. The Fasskreis theorem assures $1 - |PO|^2 = |PA||PB|$.

3.22. Given a circle of radius 1 and a point P inside the circle. For any line through P which intersects the circle at points A, B we have $1 - |PO|^2 = |PA||PB|$. Proof with Pythagoras. By scaling, translation and rotation we can assume the circle is the unit circle and that the line through the point $P = (a, b)$ is vertical. The intersection points with the circle are then $A = (a, -\sqrt{1-a^2}), B = (a, \sqrt{1-a^2})$. Now

$$|PA||PB| = (\sqrt{1-a^2} - b)(\sqrt{1-a^2} + b) = 1 - a^2 - b^2 = 1 - |PO|^2 \ .$$

3.23. The **Butterfly theorem** in a triangle is determined by two intersecting line segments in the circle. This defines 5 points, where 4 are on the circle and one point is the intersection point M. The configuration now defines two congruent triangles which intersect in M and which look like the wings of a butterfly. Now draw an additional segment through M. The theorem tells that this segment cuts intervals through the wings which have equal length. It looks like a simple theorem but it is surprisingly hard to prove.

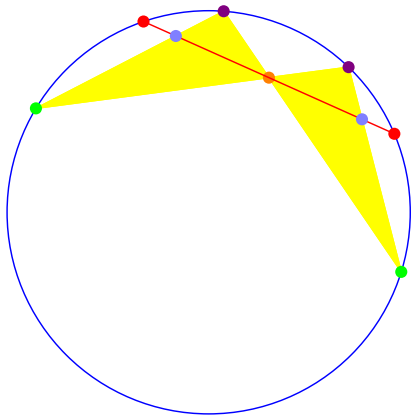


FIGURE 6. The butterfly theorem.

OLIVER KNILL

Lecture 4: Number Theory

4.1. Number theory studies the structure of **prime numbers** and equations involving integers. Gauss called it the **"Queen of Mathematics"**. We look here at a few theorems as well as some open problems in this field.

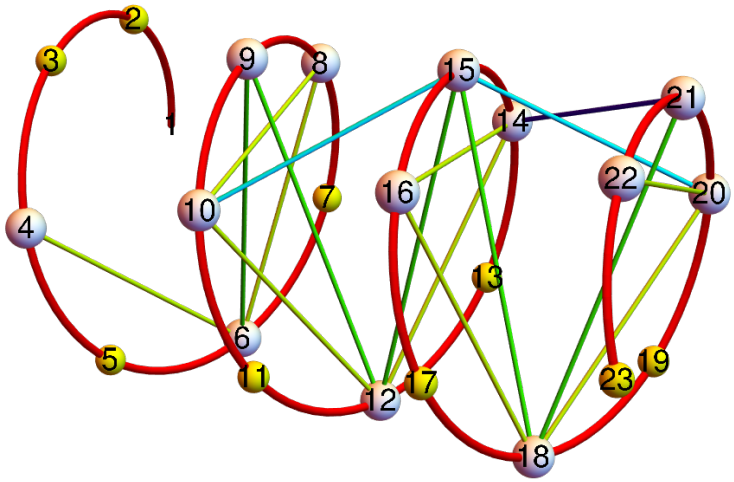


FIGURE 1. The **Eratosthenes sieve** can be visualized by aligning the number line on a spiral, then knocking out multiplies of 2, then all multiplies of 3, all multiplies of 5 etc. What remains after this sieving process are the prime numbers.

4.2. An integer larger than 1 that is divisible only by 1 and itself is called a **prime number**. We sometimes just say "prime". As of today, the number $2^{82589933}-1$ is the so far largest known prime number. It has 24862048 digits. **Euclid** proved that there are infinitely many primes: his proof was by **contradiction**: assume there are only finitely many primes $p_1 < p_2 < \cdots < p_n$. Then $n = p_1 p_2 \cdots p_n + 1$ is not divisible by any $p_1, \ldots, p_n$. Therefore, it must be a prime or be divisible by a prime larger than p_n.

4.3. Primes become less frequent as larger as they get. An important result is the **prime number theorem** which tells that the n'th prime number has approximately the size $n\log(n)$. [1] For example the $n = 10^{13}$'th prime is $p(n) = 133472665317708923$ and $p(n)/(n\log(n)) = 1.07323\ldots$. Many questions about prime numbers are unsettled. Some of these questions are listed below.

[1] One usually stats that $\pi(n)$ the number of primes smaller or equal to n is about $n/\log(n)$.

4.4. If the sum of the proper divisors of an integer n is equal to n, then n is called a **perfect number**. The smallest perfect number is 6. Indeed, the proper divisors $1, 2, 3$ of 6 sum up to 6. The next one is $28 = 1+2+4+7+14$. All currently known perfect numbers are even. The question whether **odd perfect numbers** exist is probably the oldest open problem in mathematics and is not settled. Perfect numbers were familiar to Pythagoras and his followers already. Calendar coincidences like that we have 6 work days and that the moon needs "perfect" 28 days to circle the earth might have helped to increase the fascination with perfect number.

4.5. Euclid of Alexandria (300-275 BC) was the first to realize that if $2^p - 1$ is prime then $k = 2^{p-1}(2^p - 1)$ is a perfect number. The proof is as follows: let $\sigma(n)$ be the sum of **all** factors of n, including n. It has the general property $\sigma(nm) = \sigma(n)\sigma(m)$. Now $\sigma(2^p - 1)2^{p-1}) = \sigma(2^p - 1)\sigma(2^{p-1}) = 2^p(2^p - 1) = 2 \cdot 2^{p-1}(2^p - 1)$ shows $\sigma(k) = 2k$ and verifies that k is perfect.

4.6. Around 100 AD, **Nicomachus of Gerasa** (60-120) introduced in his work "Introduction to Arithmetic" of perfect numbers and lists four perfect numbers. He also defines **superabundant numbers**, for which the sum of proper factors is larger than n and **deficient numbers** for which it is smaller than n. Also the Greek philosopher **Theon of Smyrna** (70-135) distinguished around 130 AD between **perfect**, **abundant** and **deficient numbers**. Only much later it became clear that Euclid already got all the even perfect numbers: Euler showed that all even perfect numbers are of the form $(2^n - 1)2^{n-1}$, where $2^n - 1$ is prime. The factor $2^n - 1$ is called a **Mersenne prime**. The proof is as follows: assume $N = 2^k m$ is perfect where m is odd and $k > 0$. Then $2^{k+1}m = 2N = \sigma(N) = (2^{k+1} - 1)\sigma(m)$. This gives $\sigma(m) = 2^{k+1}m/(2^{k+1} - 1) = m(1 + 1/(2^{k+1} - 1)) = m + m/(2^{k+1} - 1)$. Because $\sigma(m)$ and m are integers, also $m/(2^{k+1} - 1)$ is an integer. It must also be a factor of m. The only way that $\sigma(m)$ can be the sum of only two of its factors is that m is prime and so $2^{k+1} - 1 = m$.

4.7. The first 39 **known Mersenne primes** are of the form $2^n - 1$ $n = 2$, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917. There are 12 more known. But for those, the rank of the corresponding Mersenne prime is not known as there might be some between. The list as of now is n = 20996011, 24036583, 25964951, 30402457, 32582657, 37156667, 42643801,43112609,57885161, 74207281,77232917,82589933. The last was found in January 2018. It is unknown whether there are infinitely many.

4.8. A polynomial equations for which all coefficients and variables are integers is called a **Diophantine equation**. The first Diophantine equation studied already by the Babylonians is $x^2 + y^2 = z^2$. A solution (x, y, z) of this equation in positive integers is called a **Pythagorean triple**. For example, $(3, 4, 5)$ is a Pythagorean triple. Since 1600 BC, it is known that all solutions to this equation are of the form $(x, y, z) = (2st, s^2 - t^2, s^2 + t^2)$ or $(x, y, z) = (s^2 - t^2, 2st, s^2 + t^2)$, where s, t are different integers. Here is the Proof: either x or y has to be even because if both are odd, then the sum $x^2 + y^2$ is even but not divisible by 4 but the right hand side is either odd or divisible by 4. Move the even one, say x^2 to the left and write $x^2 = z^2 - y^2 = (z - y)(z + y)$, then the right hand side contains a factor 4 and is of the form $4s^2t^2$. Therefore $2s^2 = z - y, 2t^2 = z + y$. Solving for z, y gives $z = s^2 + t^2, y = s^2 - t^2$, $x = 2st$.

4.9. Analyzing Diophantine equations can be difficult. Only in 1994, Andrew Wiles has proven that the **Fermat equation** $x^n + y^n = z^n$ has no solutions with $xyz \neq 0$ if $n > 2$. The **last theorem of Fermat** has become a true theorem. It has been a dramatic work with Wiles having announced the result in 1993. In 1994, a gap was found which was in the same year then filled. Fermat's last theorem was not the last of all open problems in number theory.

4.10. Here are some **open problems** for Diophantine equations. Are there nontrivial solutions to the following Diophantine equations?

$x^6+y^6+z^6+u^6+v^6=w^6$	$x,y,z,u,v,w>0$
$x^5+y^5+z^5=w^5$	$x,y,z,w>0$
$x^k+y^k=n!z^k$	$k\geq 2, n>1$
$x^a+y^b=z^c, a,b,c>2$	$\gcd(a,b,c)=1$

The last equation is called the **Super Fermat** or **Beals equation**. A Texan banker **Andrew Beals** once sponsored a prize of 100′000 dollars for a proof or counter example to the statement: "If $x^p+y^q=z^r$ with $p,q,r>2$, then $\gcd(x,y,z)>1$."

4.11. Given a prime like 7 and a number n we can add or subtract multiples of 7 from n to get a number in $\{0,1,2,3,4,5,6\}$. We write for example $19=12 \bmod 7$ because 12 and 19 both leave the remainder 5 when dividing by 7. Or $5*6=2 \bmod 7$ because 30 leaves the remainder 2 when dividing by 7. Probably the most useful theorem in elementary number theory is **Fermat's little theorem** which tells that if a is an integer and p is prime then a^p-a is divisible by p. For example $2^7-2=126$ is divisible by 7. [Proof: use induction. For $a=0$ it is clear. The binomial expansion shows that $(a+1)^p-a^p-1$ is divisible by p. This means $(a+1)^p-(a+1)=(a^p-a)+mp$ for some m. By induction, a^p-a is divisible by p and so $(a+1)^p-(a+1)$.]

4.12. An other beautiful theorem is **Wilson's theorem** which allows to characterize primes: It tells that $(n-1)!+1$ is divisible by n if and only if n is a prime number. For example, for $n=5$, we verify that $4!+1=25$ is divisible by 5. [Proof: assume n is prime. There are then exactly two numbers $1,-1$ for which x^2-1 is divisible by n. The other numbers in $1,\dots,n-1$ can be paired as (a,b) with $ab=1$. Rearranging the product shows $(n-1)!=-1$ modulo n. Conversely, if n is not prime, then $n=km$ with $k,m<n$ and $(n-1)!$ is divisible by $n=km$ so that $(n-1)!+1$ can not be divisible by n.]

4.13. The solution to **systems of linear equations** like $x=3 \pmod 5, x=2 \pmod 7$ is given by the **Chinese remainder theorem**. To solve it, continue adding 5 to 3 until we reach a number which leaves rest 2 to 7: on the list $3,8,13,18,23,28,33,38$, the number 23 is the solution. Because 5 and 7 have no common divisor, the system of linear equations has a solution.

4.14. For a given n, how do we solve $x^2-yn=1$ for the unknowns y,x? A solution produces a square root x of 1 modulo n. For prime n, only $x=1, x=-1$ are the solutions. For composite $n=pq$, more solutions $x=r\cdot s$ where $r^2=-1 \bmod p$ and $s^2=-1 \bmod q$ appear. Finding x is equivalent to factor n, because the greatest common divisor of x^2-1 and n is a factor of n.

4.15. Factoring is difficult if the numbers are large. This helps to produce **encryption algorithms**. The mathematical difficulty makes surethat bank accounts and communications stay safe. Number theory, once the least applied discipline of mathematics has become one of the most applied one.

Twin prime conjecture

There are infinitely many prime twins $p, p+2$.

The first twin prime is $(3,5)$. The largest known prime twins $(p, p+2)$ have been found in 2011. It is $3756801695685 \cdot 2^{666669} \pm 1$. There are analogue problems for **cousin primes** $p, p+4$, **sexy primes** $p, p+6$ or **Germaine** primes, where $p, 2p+1$ are prime. Progress on prime gaps has been done recently: $p_{n+1} - p_n$ is smaller than 600 eventually. The largest known gap is $p_{n+1} - p_n = 1550$ appears at $p_n = 18361375334787046697$. Bertrand's postulate assures that $p_{n+1} - p_n < p_n$.

Goldbach

Every even integer $n > 2$ is a sum of two primes.

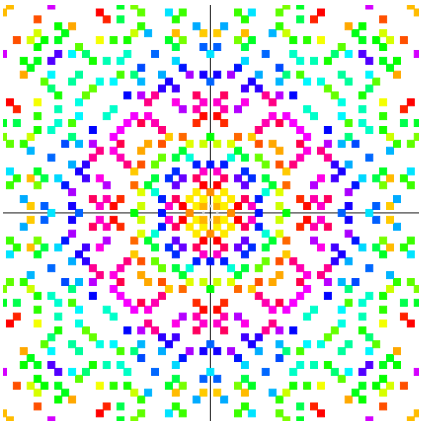
The Goldbach conjecture has been verified numerically until $4 \cdot 10^{18}$. It is known that every odd number larger than 5 is the sum of 3 primes (Helfgott 2013). This was called the "weak Goldbach conjecture".

Andrica

The prime gap estimate $\sqrt{p_{n+1}} - \sqrt{p_n} < 1$ holds.

For example $\sqrt{p_{1000}} - \sqrt{p_{999}} = \sqrt{7919} - \sqrt{7907} = 0.067....$ An other prime gap estimate conjectures is **Polignac's conjecture** claiming that there are infinitely many prime gapdf for every even number n. It is stronger than the twin prime conjecture. It includes for example the claim that there are infinitely many cousin primes or sexy primes. **Legendre's conjecture** claims that there exists a prime between any two perfect squares. Between $16 = 4^2$ and $25 = 5^2$, there is the prime 23 for example.

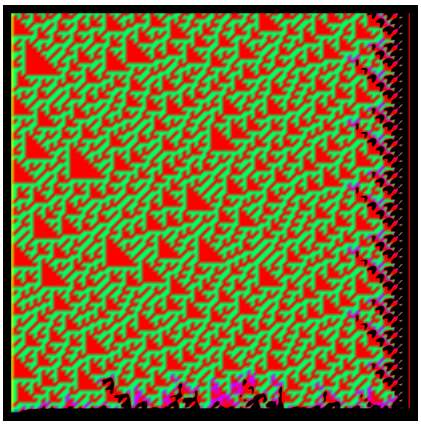
Landau



There are infinitely many primes of the form $p = n^2 + 1$.

This conjecture is one of the most astonishing ones. It restates the question whether there are infinitely many Gaussian primes $a + i$ in the complex plane. A complex integer $p = a + ib$ is prime if and only if $a^2 + b^2$ is prime or $ab = 0$ and $|a|$ is a rational prime of the form $4k+1$. Hardy and Littlewood conjectured that the ratio of primes of the form $p = n^2 + 1$ with $p \leq N$ and primes of the form $p = 4k + 3$ with $p \leq N$ converges to a constant 1.3728.... Hardy and Littlewood statement is much stronger than the Landau problem.

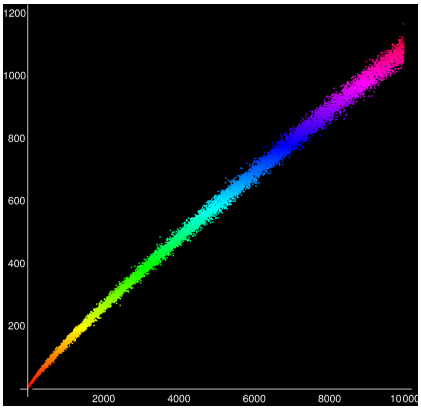
Gilbreath



If p_n is the n'th prime, then $(\Delta^k p)_1 = 1$ for all $k > 0$

This uses the notation $(\Delta a)_n = |a_{n+1} - a_n|$ for the absolute difference. For example: $\Delta^2(1, 4, 9, 16, 25, \dots) = \Delta(3, 5, 7, 9, 11, \dots) = (2, 2, 2, 2, \dots)$.

Legendre



Between successive squares there is always a prime.

In formulas, for every n there exists a prime between n^2 and $(n + 1)^2$. The numerical computation of the number of primes between n^2 and $(n + 1)^2$ shows even an increasing comet.

Odd perfect numbers

Probably the oldest open problem in mathematics is the claim:

There is an odd perfect number.

A **perfect number** has the property that it is equal to the sum of all its proper positive divisors. Like $28 = 1 + 2 + 4 + 7 + 14$. The search for perfect numbers is related to the search of large prime numbers. The largest prime number known today is $p = 2^{77232917} - 1$. It is called a Mersenne prime. Euler proved that every even perfect number is of the form $2^{n-1}(2^n - 1)$, where $2^n - 1$ is prime.

Diophantine equations

Many problems about Diophantine equations, meaning equations with integer solutions are unsettled. Here is an example:

Solve $x^5 + y^5 + z^5 = w^5$ for $x, y, z, w \in \mathbb{N}$.

Also $x^5 + y^5 = u^5 + v^5$ has no nontrivial solutions yet. Probabilistic considerations suggest that there are no solutions. The analogue equation $x^4 + y^4 + z^4 = w^4$ has been settled by Noam Elkies in 1988 who found the identity $2682440^4 + 15365639^4 + 18796760^4 = 20615673^4$.

ABC Conjecture

Let s define $\mathrm{rad}(n)$ to be the product of all the distinct prime factors of n. One special version of the ABC conjecture is

If $a + b = c, \gcd(a, b, c) = 1$, then $c \leq \mathrm{rad}(n)^2$.

One could replace the power 2 by $1 + \epsilon$ for any $\epsilon > 0$. For example, for $10 + 21 = 31$, the prime factors of $abc = 6510$ are $2, 3, 5, 7, 31$ and indeed $31 \leq (2 * 3 * 5 * 7 * 31)^2$. The ABC-conjecture implies Fermat's theorem for $n \geq 6$: assume $x^n + y^n = z^n$ with coprime $x < y < z$. Take $a = x^n, b = y^n, c = z^n$. The ABC-conjecture gives $c = z^n \leq \mathrm{rad}(abc)^2 \leq (xyz)^2 < z^6$ establishing Fermat for $n \geq 6$. The cases $n = 3, 4, 5$ have been known to Fermat already. A claimed proof of the ABC conjecture by Shinichi Mochizuki is still highly controversial.

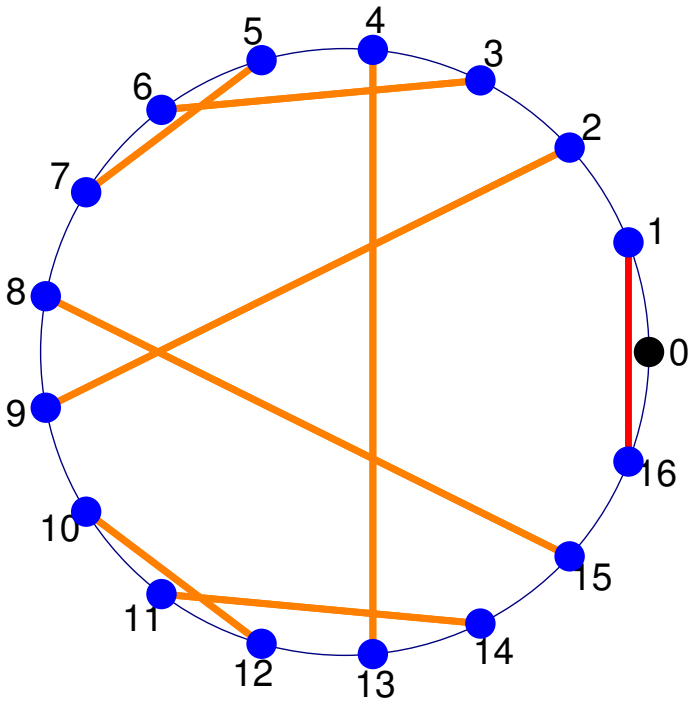
Work problems

4.16. 1) Modify Euclid's proof to show that For every n, there exist consecutive primes which differ by at least n. Do that by verifying that all integers $n! + 2, \ldots, n! + n$ are composite.

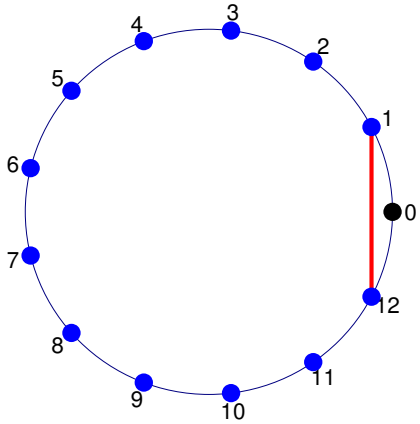
4.17. 2) Wilson's theorem assures:

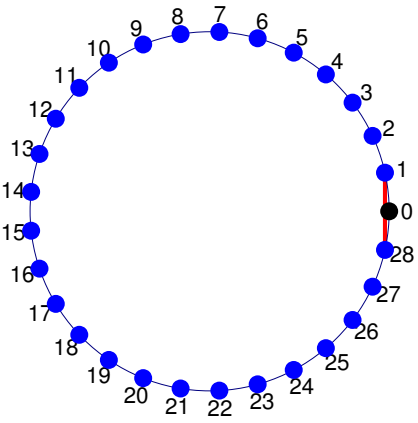
n is a prime if and only if $(n-1)! + 1$ is divisible by n.

4.18. The proof of the theorem has two directions:
If n is a prime, then the equation $xy = 1 \bmod n$ with different x, y has exactly one pair of solution. For $x^2 = 1$, there is only the solution $1, -1$.



Wilson's theorem in the case $p = 17$. We find all pairs which multiply to 1 Like $2 * 9 = 18, 3 * 6 = 18, 4 * 13 = 52, 8 * 15 = 120$ which all leave rest 1 when dividing by 17. Only the numbers 1 and -1 do not pair. The product $(n-1)!$ multiplies all the numbers together and gives $(-1) \cdot 1(2 * 9)(3 * 6)(4 * 13)(5 * 7)(8 * 15)(10 * 12)(11 * 14) = -1$.
Verify the proof either in the case $p = 13$ or $p = 29$.





4.19. Lets look at the reverse If $n = pq$ is not a prime and larger than 4, then $(n-1)!$ is divisible by n because it is a multiple of p and q.

Verify this in the concrete case of $n = 15$. Why is

$$15! = 1 * 2 * 3 * 4 * 5 * 6 * 7 * 8 * 9 * 10 * 11 * 12 * 13 * 14$$

a multiple of 15?

Fermat's little theorem

4.20. 3) Fermat's little theorem is:

$a^p - a$ is divisible by p for all prime p.

4.21. The **binomial formula** is

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + ... + \binom{n}{n-1} ab^{n-1} + b^n$$

In the case $b = 1$ it means

$$(a+1)^n = a^n + \binom{n}{1} a^{n-1} + \binom{n}{2} a^{n-2} + ... + \binom{n}{n-1} a + 1$$

4.22. a) Check that Fermat's theorem is true for $a = 0$ and $a = 1$.

b) Verify that the induction step from a to $a+1$ is equivalent to show that

$$(a+1)^p - a^p - 1$$

is divisible by p if p is a prime.

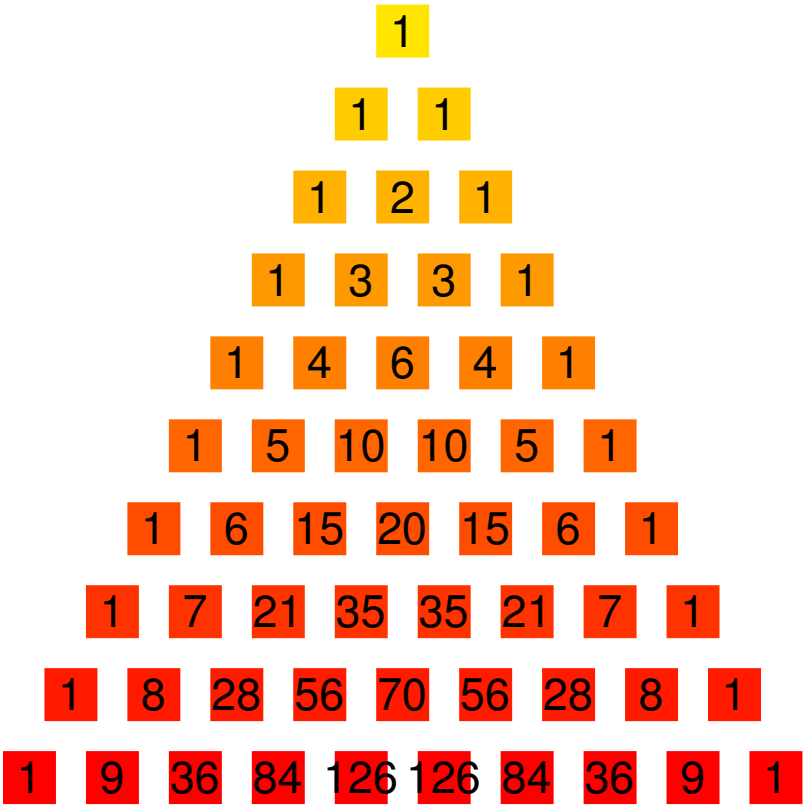
c) Verify that $(a+1)^p - a^p - 1$ is divisible by p if all all binomial coefficients

$$\binom{p}{m} = \frac{p!}{m!(p-m)!} = \frac{p \cdot (p-1)... \cdot (p-m+1)}{m \cdot (m-1) \cdot ... \cdot 1}$$

are divisible by p.

d) Verify that $\frac{p \cdot (p-1)... \cdot (p-m+1)}{m \cdot (m-1) \cdot ... \cdot 1}$ divisible by p if p is prime.

This is illustrated by the **Pascal triangle**. For rows which are prime, the interior entries are all divisible by the row number. For example, for $p = 5$, the middle entries $5, 10, 10, 5$ are all divisible by 5.



Oliver Knill, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022

TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

Lecture 5: Algebra

5.1. Algebra studies **structures** like "groups" in which one can add and "rings" in which one can add and multiply. The theory allows to solve polynomial equations like the **cubic equation** $x^3+bx^2+cx+d=0$, characterize objects by its **symmetries** like all symmetries of an equilateral triangle and is the heart and soul of many puzzles like the **Rubik cube**. Lagrange claims **Diophantus** to be the inventor of Algebra, others argue that the subject started with solutions of **quadratic equation** by **Mohammed ben Musa Al-Khwarizmi** in the book Al-jabr w'al muqabala of 830 AD. Solutions to equation like $x^2+10x=39$ are solved there by the method of **completing the squares**: add 25 on both sides go get $x^2+10x+25=64$ and so $(x+5)=8$ so that $x=3$.

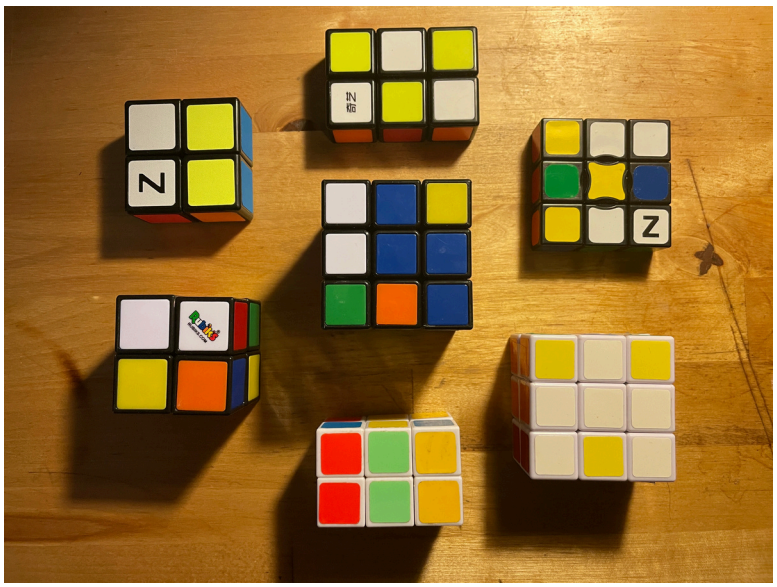


FIGURE 1. Rubik type puzzles.

5.2. **Variables** we use today in **elementary algebra** were introduced only in the 16th century. Ancient texts dealt with particular examples of equations and calculations were done with concrete numbers in the realm of **arithmetic**. It was **Francois Viete** (1540-1603) who first used letters like A,B,C,X for variables. Equations like the **quadratic equation** $x^2+bx+c=0$ was only written as such since 1637 with René Descartes.

5.3. The search for formulas for polynomial equations of degree 3 and 4 lasted 700 years. In the 16'th century, the cubic equation and quartic equations were solved. **Niccolo Tartaglia** and **Gerolamo Cardano** reduced the **cubic equation** $x^3+bx^2+cx+d=0$ to the quadratic: first translate $X=x-b/3$ so that X^3+aX^2+bX+c is a **depressed cubic** x^3+px+q. Now substitute $x=u-p/(3u)$ to get a quadratic equation $(u^6+qu^3-p^3/27)/u^3=0$ for u^3.

5.4. **Lodovico Ferrari** shows that the quartic equation $x^4+bx^3+cx^2+dx+e=0$ can be reduced to the cubic by writing it as a product $(x^2+px+q)(x^2+ux+v)$ and solving this for p,q,u,v. For the **quintic** $x^5+bx^4+cx^3+dx^2+ex+f$ no formulas could be found. It was **Paolo Ruffini**, **Niels Abel** and **Évariste Galois** who independently realized that there are no formulas in terms of roots which allow to "solve" such equations in general. This was an amazing achievement and the birth of "group theory".

5.5. In a **group** G one has an operation $*$, an inverse a^{-1} and a **one-element** 1 such that $a*(b*c)=(a*b)*c, a*1=1*a=a, a*a^{-1}=a^{-1}*a=1$. For example, the set $\mathbb{Q}^*$ consisting of fractions p/q with non-zero p,q and multiplication operation $*$ and inverse $1/a$ form a group. The integers $\mathbb{Z}$ with addition and inverse $a^{-1}=-a$ and one-element 0 form a group too. Group operations are sometimes written in an additive way $x+y$ or in a multiplicative way $x*y$. Especially in **commutative settings**, where $a+b=b+a$, one usually uses the additive writing.

5.6. A **ring** R comes with two operations, addition and multiplication $+$ and $*$. The plus operation is a group satisfying the commutativity law $a+b=b+a$ in which the one-element is called 0. The multiplication operation $*$ is required to be associative. The two operations $+$ and $*$ are glued together by the **distributive law** $a*(b+c)=a*b+a*c$. An example of a ring are the **integers** $\mathbb{Z}$ or the **rational numbers** $\mathbb{Q}$ or the **real numbers** $\mathbb{R}$. The last two are actually **fields**, rings for which the multiplication on nonzero elements is a group too.

5.7. Why is the theory of groups and rings not part of arithmetic? First of all, a crucial ingredient of algebra is the appearance of **variables** and computations with these algebras without using concrete numbers. Second, the algebraic structures are not restricted to "numbers". Groups and rings are general structures and extend for example to objects like the set of all possible symmetries of a geometric object.

5.8. Groups appear often as **symmetries** in a geometry. The set of all **similarity transformations** on the plane for example form a group. An other important ring is the **polynomial ring** of all polynomials in a variable x. Given any ring R and a variable x, the set $R[x]$ consists of all polynomials with coefficients in R. The addition and multiplication is done like in $(x^2+3x+1)+(x-7)=x^2+4x-7$.

5.9. The problem to factor a given polynomial with integer coefficients into polynomials of smaller degree: x^2-x+2 for example can be written as $(x+1)(x-2)$ have a number theoretical flavor. Because symmetries of some structure form a group, the algebra of groups has intimate connections with geometry. The importance of this manifests also in physics, where groups explain the structure of elementary particles.

5.10. Symmetries are not the only connection with geometry. Here is a link to more modern geometry. If we look at polynomial rings of several variables, we get geometric objects with shape and symmetry which sometimes even have their own algebraic structure. They are called **varieties** and are studied in **algebraic geometry**. An example of a variety is the lemniscate of Gerono given by $(x^2-1)^2+y^2=1$. Algebraic objects given by polynomial equations in have in the last century been generalized further to **schemes**, **algebraic spaces** or **stacks**. Commutative algebra continue to play a crucial role in such constructs.

5.11. Arithmetic introduces addition and multiplication of numbers. Both form a group. The operations can be written additively or multiplicatively. Lets look at this a bit closer: for integers $\mathbb{Z}$, fractions $\mathbb{Q}$ and reals $\mathbb{R}$ and the addition $+$, the one-element 0 and the inverse is $-g$, we have a group. Many groups are written multiplicatively, where the one-element is 1. In the case where we have both addition and multiplication, the number 0 is not part of the multiplicative group. It is not possible to divide by 0. But the nonzero fractions or the nonzero real numbers form a group. In all these examples $\mathbb{Z},\mathbb{Q},\mathbb{R}$, the groups satisfy the commutative law $g*h=h*g$.

5.12. Groups are in general not commutative. The set of all rotations in space is an example of a group where it matters in which order we turn things. Rotate a cube by 90 degrees around the x-axes, then by 90 degrees around the y-axes is different from doing things with the opposite order. It contains the subgroup of all rotations which leave the unit cube invariant. There are $3 * 3 = 9$ rotations around each major coordinate axes, then 6 rotations around axes connecting midpoints of opposite edges, then $4 * 2$ rotations around diagonals. Together with the identity we have a group with 24 elements. This is the group of symmetries of the cube.

5.13. An other example of a group is S_4, the set of all permutations of four numbers $(1, 2, 3, 4)$. If $g : (1, 2, 3, 4) \to (2, 3, 4, 1)$ is a permutation and $h : (1, 2, 3, 4) \to (3, 1, 2, 4)$ is an other permutation, then we can combine the two and define $h * g$ as the permutation which does first g and then h. We end up with the permutation $(1, 2, 3, 4) \to (1, 2, 4, 3)$.

5.14. The rotation symmetry group of the cube turns out to be the same than the group S_4. To see this "isomorphism", label the 4 space diagonals in the cube by numbers $1, 2, 3, 4$. Given a rotation, we can look at the induced permutation of the diagonals. Every rotation corresponds to exactly one permutation. The symmetry group can be introduced for any geometric object. For shapes like the triangle, the cube, the octahedron or tilings in the plane. Symmetry groups describe geometric shapes by algebra.

5.15. Many **puzzles** are groups. A popular puzzle is the **15-puzzle**. It was invented in 1874 by **Noyes Palmer Chapman** in the state of New York. If the hole is given the number 0, then the task of the puzzle is to order a given random start permutation of the 16 pieces. To do so, the user is allowed to transposes 0 with a neighboring piece. Since every step changes the signature s of the permutation and changes the taxi-metric distance d of 0 to the end position by 1, only situations with even $s + d$ can be reached. It was **Sam Loyd** who suggested to start with an impossible solution and as an evil plot to offer 1000 dollars for a solution. The group of the 15 puzzle has $16!/2$ elements. Strangely enough the "God number" of the puzzle is not known exactly. It is between 152 and 208.

5.16. The **Rubik cube** is an other famous puzzle, which is a group. Exactly 100 years after the invention of the 15 puzzle, the Rubik puzzle was introduced in 1974. It still popular and some can solve it in 5 seconds. For the $3x3x3$ cube, the **God number**, is is now known to be 20: this means that one can always solve it in 20 or less moves, in principle.

5.17. A small Rubik type game is the $3 \times 3 \times 1$ Rubik cube called the "floppy" which is a third of the Rubik and which has only 192 elements.

5.18. The smallest Rubik cube of interest is the $2 \times 2 \times 1$ Rubik. If we allow all the cubes to move, then this group has 24 elements. It is again the same group than the rotation symmetry group of the cube. It is also the symmetry group the roots of the quartic equation $x^4+bx^3+cx^2+dx+e = 0$.

Work problems

5.19. The solution of the **quadratic equation** $x^2+bx+c=0$ is one of the major achievements of early algebra. It relies on the method of **completion of the square** and is due to the Persian mathematician **Al Khwarizmi**. The **completion of the square** is the idea to add $b^2/4$ on both sides of the equation and move the constant to the right. Like this $x^2+bx+b^2/4$ becomes a square $(x+b/2)^2$. Geometrically, one has added a square to a region to get a square. From $(x+b/2)^2 = -c+b^2/4$ we can solve x and get the famous formula for the solution of the quadratic equation

$$x = \pm\sqrt{\frac{b^2}{4}-c} - \frac{b}{2} \; .$$

There are two solutions. An other point of view is to plug in $x = y - b/2$. **Problem 1)** Write down the solution in the more general case $ax^2+bx+c=0$.

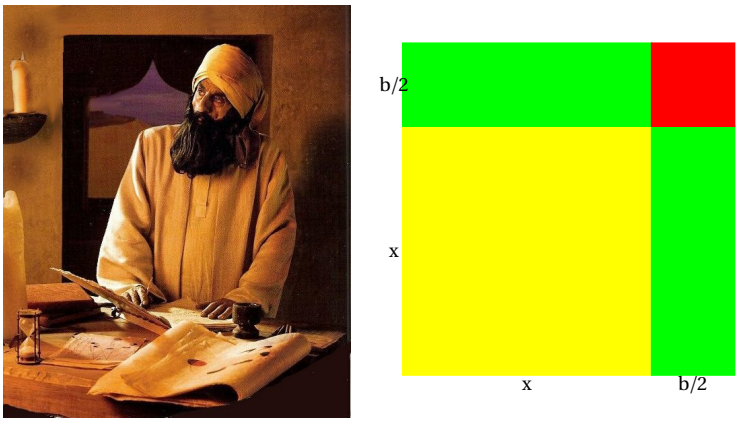


FIGURE 2. Al Kharizmi and the completion of the square.

5.20. Here are some SAT tricks. Why do they work?
Problem 2)
a) If x_1, x_2 are the two solutions to $x^2+bx+c=0$, then the sum of the two solutions is $x_1+x_2=-b$.
b) If x_1, x_2 are the two solutions of x^2+bx+c, then the product of the solutions is $x_1x_2=c$.

5.21. Problem 3) Find the solutions to the following equations

a) $x^4-4x^2+3=0$? b) $x^6-4x^4+3x^2=0$.

5.22. Problem 4) Sometimes we can find the solution of a equation by guessing.

a) Can you find the solutions to the cubic equation x^3-7x+6? b) Can you find the solution to the equation $x^4+4x^3+6x^2+4x+1$? c) What are the solutions to $x^4-2x^2+1=0$?

5.23. Problem 5) Verify that if a, b, c are solutions to a cubic equation and $a+b+c=0$, then it is depressed: $x^3+px+q=0$. Hint: Write $(x-a)(x-b)(x-c)$.

5.24. We look at all the **rotational symmetries** of a square and realize it as a group. Given a square in the plane centered at the origin. We can rotate the square by 90, 180 or 270 degrees and get the same shape. Given two such rotations, we can perform one after the other and get an other rotation. All the rotations leaving the square invariant form a **group**: one can "add" these operations and get a new operation. here is the **multiplication table**:

+	0	90	180	270
0	0	90	180	270
90	90	180	270	0
180	180	270	0	90
270	270	0	90	180

Problem 6) For the equilateral triangle, there are 3 rotations and 3 reflections. Can you write the multiplication table of the symmetries of the equilateral triangle?

5.25. If we look at all rotations and reflections which leave the square invariant, there are 8 group elements. Beside the four rotations, we have 2 reflections at the diagonals and 2 reflections at the main axes.
Problem 7: Can you write down the multiplication table of the symmetries of the square? This is a large 8×8 multiplication table.

The 15 puzzle

5.26. The **15 puzzle** was invented by **Noyes Palmer Chapman** in 1874. Chapman was a postmaster from Canastota in New York. From there the puzzle moved over to Syracuse, Watchhill, Hartfort and was first seriously sold in Boston. **Sam Loyd** offered a 1000 dollar prize for the solution of the case, when two pieces are switched.

FIGURE 3. The 15 puzzle.

5.27. It is a bit harder to see that there are exactly 16!/2 group elements with the whole at the end. It is better to not assume that the hole as to be at the end since otherwise, one has no group. The god number is still not known. It between 152 and 208 for single tile moves.

Problem 8: Find and write down the argument why there we can not solve the 15 puzzle if two elements are switched.

The floppy

5.28. The **floppy cube** was designed by Katsuhiko Okamoto. With 192 possible positions, it is much less complex than the Rubik cube. We will learn how to solve it in class.

The Rubik's cube

FIGURE 4. The Floppy

5.29. The **Rubik's cube** is quite a large puzzle. Argue that the Rubic cube has less than $8! \cdot 12! \cdot 3^8 \cdot 2^{12}$ group elements.

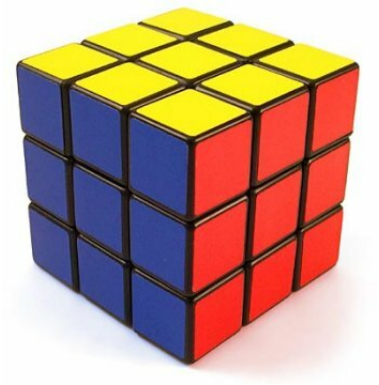


FIGURE 5. The Rubik cube

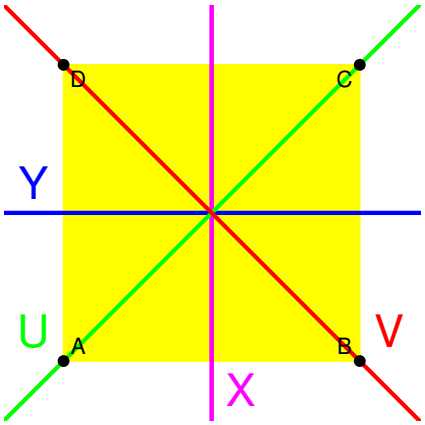
OLIVER KNILL, KNILL@MATH.HARVARD.EDU MATH E-320, HARVARD EXTENSION SCHOOL, 2010-2022

Lecture 5: Multiplication table and Sudoku

The symmetry group of a square

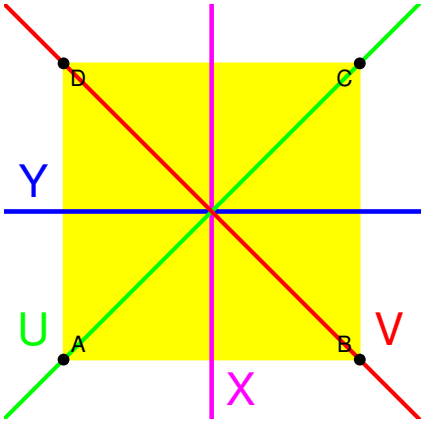
The symmetry group of the square has 8 elements. There are four rotations $0, 90, 180, 270$, a reflection $X : (x, y) \to (-x, y)$ switching the sign of the x-coordinate, a reflection $Y : (x, y) \to (x, -y)$ switching the sign of the y-coordinate, a reflection $U : (x, y) \to (y, x)$ at the diagonal and a reflection $V : (x, y) \to (-y, -x)$ at the anti diagonal. In order to build the multiplication table, perform the operation on the left first then do the operation on the top. Make a picture or build a model so that you can do the operations. Here is the table without any entries:

$*$	0	90	180	270	X	Y	U	V
0								
90								
180								
270								
X								
Y								
U								
V								



1. Step. First fill in the rotation part. All rotations are counter clockwise. For example, rotating by 180 and then rotating by 270 gives you a rotation by $180 + 270 = 450 = 90$. You can use in this part that rotation in two dimensions is commutative and also use the **Sudoku rule** that all of the rotations have to appear in all of the rows and columns.

$*$	0	90	180	270	X	Y	U	V
0	0	90	180	270				
90	90	180	270	0				
180	180	270	0	90				
270	270	0	90	180				
X								
Y								
U								
V								

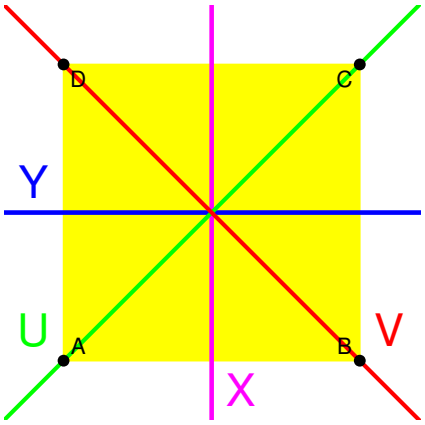


2. Step. Now fill in products of reflections. For example, $X * X = 0$, $X * Y = 180$,$X * V = 90$, $V * X = 270$. For example, in order to see $X * V = 90$, look what happens with the points A,B,C,D of the square. Do this for each multiplication. For example:

$$X * V : A \to B \to B, B \to A \to C, C \to D \to D, D \to C \to A \; .$$

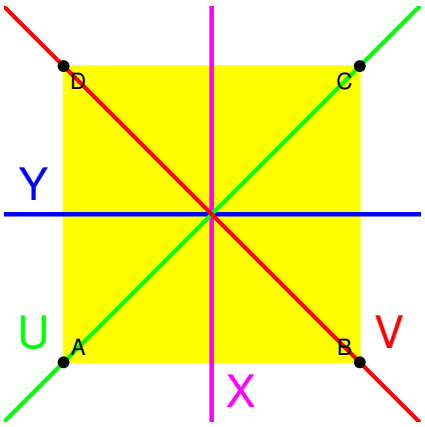
This means $ABCD$ goes to $BCDA$, which is a 90 degree rotation. You should reach something like

$*$	0	90	180	270	X	Y	U	V
0	0	90	180	270				
90	90	180	270	0				
180	180	270	0	90				
270	270	0	90	180				
X					0	180	270	
Y					180	0	90	
U						270	0	
V								0



2. Step continue. **Sudoku!** If you reach a stage like this, you can use Sudoku rules. Two reflections give a rotation and all rotations have to appear. You can now fill the rest without having to do the computations!

$*$	0	90	180	270	X	Y	U	V
0	0	90	180	270				
90	90	180	270	0				
180	180	270	0	90				
270	270	0	90	180				
X					0	180	270	90
Y					180	0	90	270
U					90	270	0	180
V					270	90	180	0

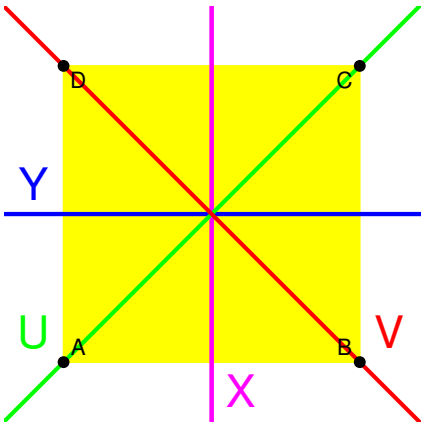


3. Step. Now combine rotations with reflections. That is the upper right part. For example $90 * X$. In order to see this look what happens with the square:

$$A \to B \to A, B \to C \to D, C \to D \to C, D \to A \to B$$

We see that $ABCD$ goes to $ADCB$ which means $90 * X = V$.

$*$	0	90	180	270	X	Y	U	V
0	0	90	180	270	X	Y	U	V
90	90	180	270	0	V			
180	180	270	0	90				
270	270	0	90	180				
X					0	180	270	90
Y					180	0	90	270
U					90	270	0	180
V					270	90	180	0



In a 4. Step, fill in the lower left cases like $X * 0 = X$. Continue filling and do not forget to use Sudoku rules when having enough info. In each row and each column, all the entries $0, 90, 180, 270, X, Y, U, V$ should appear. In the upper 4×4 block, only reflections should X, Y, U, V appear. These are mini Sudoku blocks. Reflect also a bit after having finished: You might notice for example for two reflections $X * Y = -Y * X$, where $-90 = 270, -180 = 180$.

TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

Lecture 6: Calculus

6.1. Calculus generalizes the process of **taking differences** and **taking sums**. Differences measure **change**, sums explore how quantities **accumulate**. The procedure of taking differences has a limit called **derivative**. The activity of taking sums leads to the **integral**. Sum and difference are dual to each other and related in an intimate way. In this lecture, we look first at the simplest possible setup, where functions are evaluated on integers and where we do not take any limits.

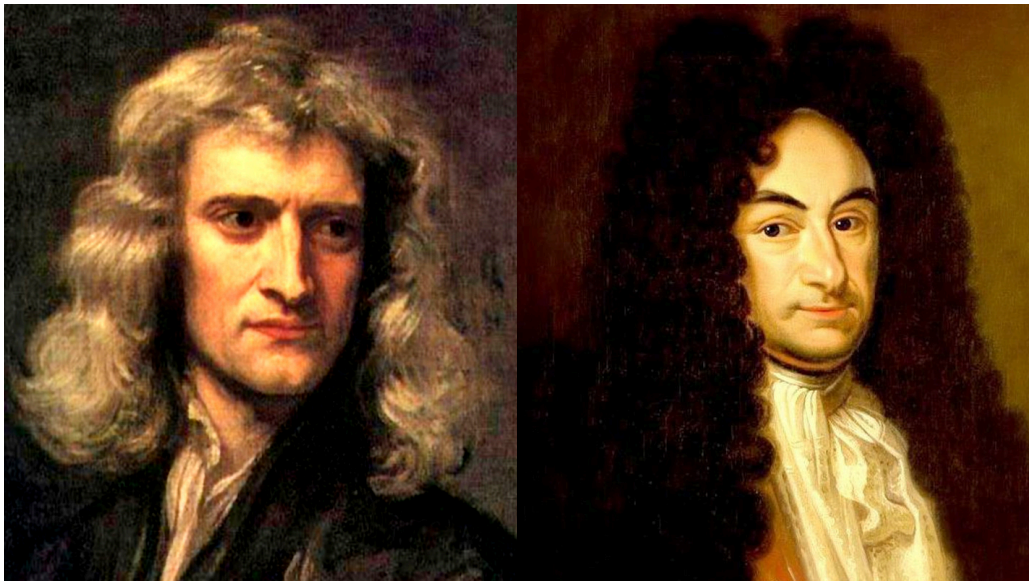


FIGURE 1. Newton and Leibniz

6.2. We have seen in the arithmetic lecture that numbers were first represented by units like

$$1, 1, 1, 1, 1, 1, \dots \ .$$

for example carved in the Ishango bone. It took thousands of years until numbers were represented with symbols like

$$0, 1, 2, 3, 4, \dots \ .$$

Using the modern concept of **function**, we can say $f(0) = 0, f(1) = 1, f(2) = 2, f(3) = 3$ and mean that the **function** f assigns to an **input** like 1001 an **output** like $f(1001) = 1001$. Define $Df(x) = f(x+1) - f(x)$, the **difference** between two function values. We see that the function $f(x) = x$ satisfies $Df(x) = 1$ for all x. We can also formalize the summation process. If $g(x) = 1$ is the function which is constant 1, then $Sg(x) = g(0) + g(1) + \cdots + g(x-1) = 1 + 1 + \cdots + 1 = x$. We see that $Df = g$ and $Sg = f$.

6.3. If we start with $f(x) = x$ and apply **summation** on that function we get

$$Sf(x) = f(0) + f(1) + f(2) + \cdots + f(x-1) \; .$$

In our example, we get the values:

$$0, 1, 3, 6, 10, 15, 21, \ldots \; .$$

The new function $g(x) = Sf(x)$ satisfies $g(1) = 1, g(2) = 3, g(2) = 6$, etc. These numbers are called **triangular numbers**. From g we can get back f by taking difference:

$$Dg(x) = g(x+1) - g(x) = f(x) \; .$$

For example $Dg(5) = g(6) - g(5) = 15 - 10 = 5$ which indeed is $f(5)$. Finding a formula for the sum $Sf(x)$ is not so easy. Can you do it? When **Karl-Friedrich Gauss** was a 9 year old school kid, his teacher, a Mr. Büttner gave the class the task to sum up the first 100 numbers $1+2+\cdots+100$. Gauss found the answer immediately by pairing things up: to add up $1+2+3+\cdots+100$, he would write this as $(1+100) + (2+99) + \cdots + (50+51)$, leading to 50 terms of 101 to get for $x = 101$ the value $g(x) = x(x-1)/2 = 5050$. Taking differences again is easier $Dg(x) = g(x+1) - g(x) = x(x+1)/2 - x(x-1)/2 = x = f(x)$.

6.4. Lets add now the triangular numbers up compute $h = Sg$. We get the sequence

$$0, 1, 4, 10, 20, 35, \ldots$$

called the **tetrahedral numbers**. One can stack $h(x)$ balls to build a tetrahedron of side length x. For example, $h(4) = 20$ golf balls are needed to build a tetrahedron of side length 4. The formula which holds for h is $\boxed{h(n) = n(n-1)(n-2)/6}$. Here is the fundamental theorem of calculus, which is the core of calculus:

$$\boxed{SDf(n) = f(n) - f(0), \qquad DSf(n) = f(n) \; .}$$

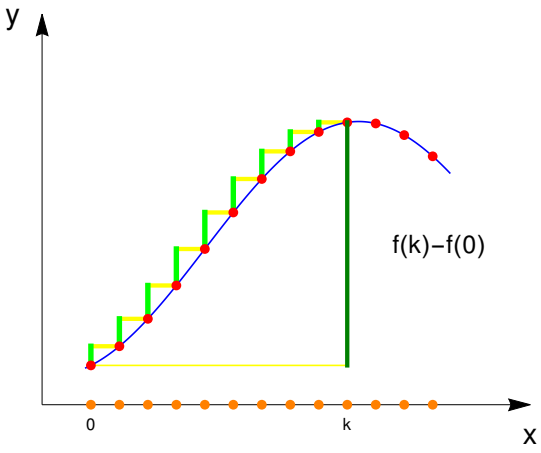
Proof.

$$SDf(n) = \sum_{k=0}^{n-1} [f(k+1) - f(k)] = f(n) - f(0) \; ,$$

$$DSf(n) = [\sum_{k=0}^{n-1} f(k+1) - \sum_{k=0}^{n-1} f(k)] = f(n) \; .$$

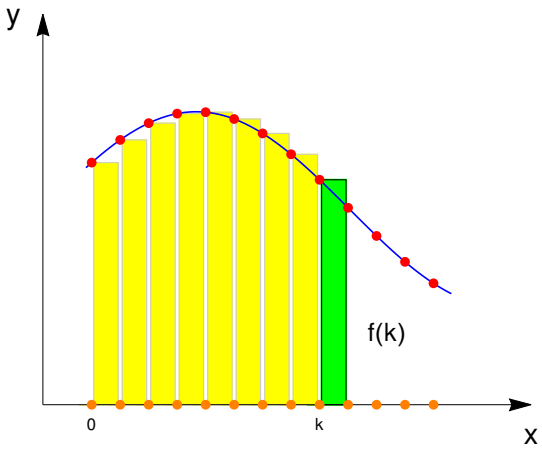
The process of adding up numbers will lead to the **integral** $\boxed{\int_0^x f(x)\, dx}$. The process of taking differences will lead to the **derivative** $\boxed{\frac{d}{dx} f(x)}$.

$$\boxed{\int_0^x \frac{d}{dt} f(t)\, dt = f(x) - f(0), \qquad \frac{d}{dx} \int_0^x f(t)\, dt = f(x)}$$



Theorem: Sum the differences and get

$$SDf(kh) = f(kh) - f(0)$$



Theorem: Difference the sum and get

$$DSf(kh) = f(kh)$$

6.5. If we define the functions $[x]^0 = 1, [x]^1 = n, [x]^2 = x(x-1)/2, [x]^3 = x(x-1)(x-2)/6$ then $D[x] = [1], D[x]^2 = 2[x], D[x]^3 = 3[x]^2$ and in general

$$\boxed{\frac{d}{dx}[x]^n = n[x]^{n-1}}$$

The calculus we have just seen, contains the essence of single variable calculus. A major **core idea** is present which will become more powerful and natural if it is used together with the concept of limit.

6.6. Problem: The **Fibonnacci sequence** $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ satisfies the rule $f(x) = f(x-1) + f(x-2)$. It defines a function on the positive integers. For example, $f(6) = 8$. What is the function $g = Df$, if we assume $f(0) = 0$? We take the difference between successive numbers and get a new sequence of numbers

$$0, 1, 1, 2, 3, 5, 8, \ldots$$

which is the same sequence again. We can deduce from this recursion that f has the property that $\boxed{Df(x) = f(x-1)}$.

6.7. Problem: Take the same function f given by the sequence $1, 1, 2, 3, 5, 8, 13, 21, ...$ but now compute the function $h(x) = Sf(x)$ obtained by summing the first x numbers up. It gives the sequence $1, 2, 4, 7, 12, 20, 33, \ldots$. What sequence is that?
Solution: Because $Df(x) = f(x-1)$ we have $f(x) - f(0) = SDf(x) = Sf(x-1)$ so that $Sf(x) = f(x+1) - f(1)$. Summing the Fibonnacci sequence produces the Fibonnacci sequence shifted to the left with $f(2) = 1$ is subtracted. It has been relatively easy to find the sum, because we knew what the difference operation did. This example shows:

$$\boxed{\text{We can study differences to understand sums.}}$$

The next problem illustrates this too:

6.8. Problem: Find the next term in the sequence
2 6 12 20 30 42 56 72 90 110 132 . **Solution:** Take differences

2	6	12	20	30	42	56	72	90	110	132
2	4	6	8	10	12	14	16	18	20	22
2	2	2	2	2	2	2	2	2	2	2
0	0	0	0	0	0	0	0	0	0	0

.

Now we can add an additional number, starting from the bottom and working us up.

2	6	12	20	30	42	56	72	90	110	132	156
2	4	6	8	10	12	14	16	18	20	22	24
2	2	2	2	2	2	2	2	2	2	2	2
0	0	0	0	0	0	0	0	0	0	0	0

6.9. Problem: The function $f(n) = 2^n$ is called the **exponential function**. We have for example $f(0) = 1, f(1) = 2, f(2) = 4, \ldots$. It leads to the sequence of numbers

n=	0	1	2	3	4	5	6	7	8	...
f(n)=	1	2	4	8	16	32	64	128	256	...

We can verify that f satisfies the equation $\boxed{Df(x) = f(x)}$ because $Df(x) = 2^{x+1} - 2^x = (2-1)2^x = 2^x$.
This is an important special case of the fact that

$$\boxed{\text{The derivative of the exponential function is the exponential function itself.}}$$

The function 2^x is a special case of the exponential function when the Planck constant is equal to 1. We will see that the relation will hold for any $h > 0$ and also in the limit $h \to 0$, where it becomes the classical exponential function e^x which plays an important role in science.

Calculus has many applications: computing areas, volumes, solving differential equations. It even has applications in arithmetic. Here is an example for illustration. It is a proof that π is irrational. The theorem is due to Johann Heinrich Lambert (1728-1777):

Theorem of Lambert Pi is irrational.

The proof by Ivan Niven is given in a book of Niven-Zuckerman-Montgomery. It originally appeared in 1947 (Ivan Niven, Bull.Amer.Math.Soc. 53 (1947),509). The proof illustrates how calculus can help to get results in arithmetic.

Proof. Assume $\pi = a/b$ with positive integers a and b. For any positive integer n define

$$f(x) = x^n(a - bx)^n/n! \ .$$

We have $f(x) = f(\pi - x)$ and

$$0 \leq f(x) \leq \pi^n a^n/n! (*)$$

for $0 \leq x \leq \pi$. For all $0 \leq j \leq n$, the j-th derivative of f is zero at 0 and π and for $n <= j$, the j-th derivative of f is an integer at 0 and π.

The function

$$F(x) = f(x) - f^{(2)}(x) + f^{(4)}(x) - ... + (-1)^n f^{(2n)}(x)$$

has the property that $F(0)$ and $F(\pi)$ are integers and $F + F'' = f$. Therefore, $(F'(x)\sin(x) - F(x)\cos(x))' = f\sin(x)$. By the fundamental theorem of calculus, $\int_0^\pi f(x)\sin(x)\,dx$ is an integer. Inequality (*) implies however that this integral is between 0 and 1 for large enough n. For such an n we get a contradiction.

Work problems

6.10. We stack two dimensional disks building n layers and count the number of discs. The number sequence we get are called **triangular numbers**.

1	3	6	10	15	21	36	45	...

This sequence defines a **function** on the natural numbers. For example, $f(4) = 10$. Can you find $f(200)$? The task to find this number was given to Carl Friedrich Gauss in elementary school. The 7 year old came up quickly with an answer. How?

FIGURE 2. Carl-Friedrich Gauss, 1777-1855

6.11. We stack spheres onto each other building n layers and count the number of spheres. The numbers which appear are called **tetrahedral numbers**.

1	4	10	20	35	56	84	120	...

Also this sequence defines a **function**. For example, $g(3) = 10$. But what is $g(100)$? Can we find a formula for $g(n)$? Verify that $g(n) = n(n+1)(n+2)/6$, satisfies $Dg(n) = g(n) - g(n-1) = n(n+1)/2$.

6.12. Problem: Given the sequence $1, 1, 2, 3, 5, 8, 13, 21, \ldots$ which satisfies the rule $f(x) = f(x-1) + f(x-2)$. It defines a function on the positive integers. For example, $f(6) = 8$. What is the function $g = Df$, if we assume $f(0) = 0$?

6.13. Problem: Take the same function f given by the sequence $1, 1, 2, 3, 5, 8, 13, 21, ...$ but now compute the function $h(n) = Sf(n)$ obtained by summing the first n numbers up. It gives the sequence $1, 2, 4, 7, 12, 20, 33, ...$ What sequence is that?

6.14. Problem: Find the next term in the sequence
2 6 12 20 30 42 56 72 90 110 132 .

6.15. Problem: Find the next term in the sequence

$$3, 12, 33, 72, 135, 228, 357, 528, 747, 1020, 1353... .$$

To do so, compute successive derivatives $g = Df$ of f, then $h = Dg$ until you see a pattern.

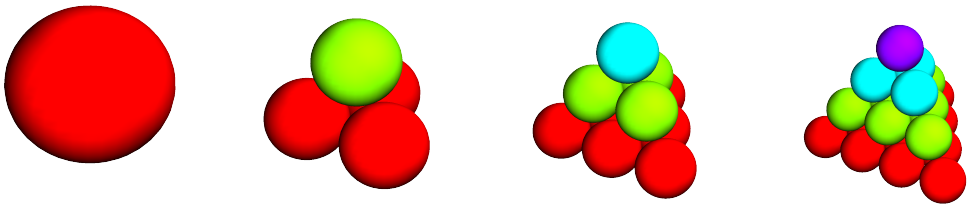


FIGURE 3. Tetrahedral numbers

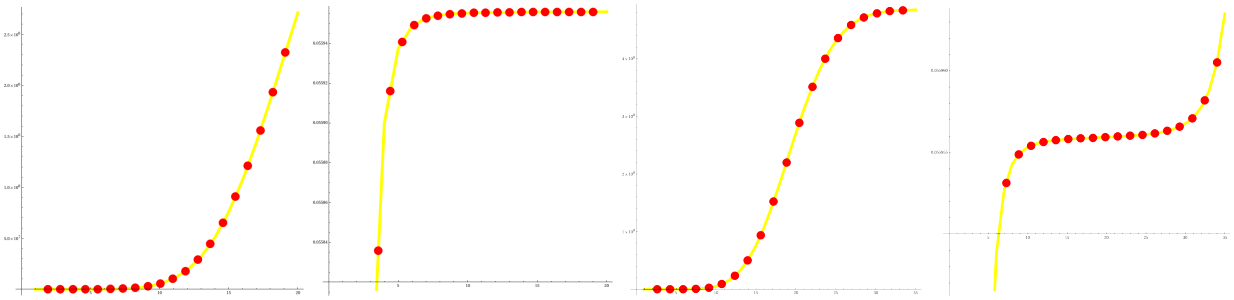
6.16. Henri Poincaré mentions in his "New Methods of Celestial Mechanics" the two sums

$$S_n = \sum_{n=0}^{\infty} \frac{1000^n}{n!}$$

and

$$S_n = \sum_{n=0}^{\infty} \frac{n!}{1000^n} .$$

Why does the first one have a limit? Can you give its value? You might have to look up the series for the exponential function. Why does the second series not have a limit? Just take some large n and see what the terms are you are summing up. Experimental evidence would rule the first to be divergent and the second to be convergent. The experiments would be too extreme in Poincaré's example. Therefore, we replace 1000 with 20. Lets look at the first 20 values of S_n



6.17. The harmonic series

$$\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+...$$

does not converge. Lets see why.

a) Why is the third and forth therm together larger than 1/2?

$$\frac{1}{3}+\frac{1}{4}\ .$$

b) Why is the sum of the fifth up to eighth term larger than 1/2?

$$\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\ .$$

c) How do we continue the argument?
Experimentally, the series seems to stay bounded. To get to 100, we would need $e^{100} = 10^{43}$ steps. But the universe is only 10^{17} seconds old.

6.18. Here are three of the **Zeno paradoxa**.
1) "In a race, the quickest runner can never overtake the slowest, since the pursuer must first reach the point whence the pursued started, so that the slower must always hold a lead."
2) "That which is in locomotion must arrive at the half-way stage before it arrives at the goal."
3) "If everything when it occupies an equal space is at rest, and if that which is in locomotion is always occupying such a space at any moment, the flying arrow is therefore motionless." Can you reformulate and resolve these paradoxa?

6.19. How would you summarize calculus in one paragraph? What are the 10 most important results for you in calculus? **Eli Maor** expresses it well in his book "The facts on file: Calculus Handbook, 2003":

"Over the past 25 years or so, the typical college calculus textbook has grown from a modest 350-page book to a huge volume of some 1,200 pages, with thousands of exercises, special topics, interviews with career mathematicians, 10 or more appendixes, and much, much more. But as the old adage goes, more is not always better. The enormous size and sheer volume of these monsters (not to mention their weight!) have made their use a daunting task. Both student and instructor are lost in a sea of information, not knowing which material is important and which can be skipped. As if the study of calculus is not a challenge already, these huge texts make the task even more difficult."

6.20. *Here are some pioneers of single variable calculus and calculus teaching. here are some important mathematicians for single variable calculus. Can you find more?*
Zeno of Elea *490-430 Notion of derivative*
Democritus *460-370 Cone and Pyramid. Atomic structure of matter*
Eudoxus *408-355 BC method of exhaustion*
Archimedes *287-212 BC area of disc, volume of sphere*
Johannes Kepler *1571-1630, velocity and acceleration*
Rene Descartes *1596-1650, tangents, rule of signs*
Bonaventura Cavalieri *1598-1647 Cavalieri principle*

Pierre de Fermat *1601-1665 Maxima, Integral of power function*
John Wallis *1616-1703 integral calculus with x^a, infinite series*
Christiaan Huygens *1629-1695 Waves, gravity,*
Blaise Pascal *1623-1662, expectation, Pascal triangle*
Isaac Barrow *1630-1677 Calculating tangents*
James Gregory *1638-1675 Fundamental theorem of calculus*
Robert Hooke *1635-1703 Inverse square law*
Isaac Newton *1643-1727 Fluxions = Derivatives*
Gottfried Leibniz *1646-1716 Modern version of calculus*
Michel Rolle *1652-1719 Critic of calculus, Roles theorem*
Guillaume de L'Hospital *1661-1704 Textbook, Hospitals law*
Johann Bernoulli *1667-1748 First textbook (written with L'Hospital)*
Brook Taylor *1685-1731 Taylor series, Difference calculus*
Leonard Euler *1707-1783 Basel problem, analytic geometry*
Maria Agnesi *1718-1799 Textbook in calculus*
Bernard Bolzano *1781-1848 Rigor, intermediate and extremal value theorem*
Augustin Cauchy *1789-1857, continuity, complex calculus*
Karl Weierstrass *1815-1897 Rigorous foundation of calculus*
Bernhard Riemann *1826-1866 Riemann integral, Zeta functions*
Henri Lebesgue *1875-1941 Modern integration*

Oliver Knill, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022

TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

Lecture 7: Set Theory and Logic

7.1. Sets are fundamental building blocks of mathematics. While **logic** provides a language and the rules for doing mathematics, set theory is the building material for all mathematical structures. Set theory is not the only possible framework. More recently one has used **category theory** as a foundation. It has been seen that **Cantorian set theory** is also quite accessible for younger minds. We have the set of plants, the set of animals, the set of food for example. We can then ask about the relation between these. Are the plants which are animals are there animals which are food etc. What belongs to the set of plants and food which are not both? During the "new math" revolution the language has been introduced to younger kids. Primary school students (including me) had to learn the concept of **Venn diagrams**, long before being exposed to fractions for example. One can argue also that category theory can also be introduced early as it can be seen as some sort of graph theory. But category theory really becomes useful only if one is acquainted with a few mathematical structures. Set theory gives immediate results. By introducing the clever notion of "cardinality", Cantor could prove that there are different scales of "infinities". The diagonal argument can be understood long before one can grasp other frame works like calculus and has a "Wow!" effect: we can have different infinities!

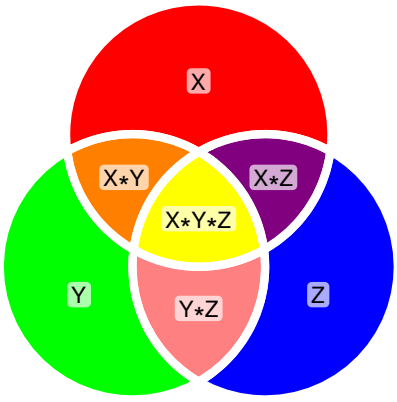


FIGURE 1. The intersection $*$ is the multiplication in the Boolean ring. The symmetric difference $+$ is the addition.

7.2. One can compute with subsets of a given set X ="universe" like with numbers. There are two basic operations: the **addition** $A+B$ of two sets is defined as the set of all points which are in exactly one of the sets. The **multiplication** $A \cdot B$ of two sets contains all the points which are in both sets. With this **symmetric difference** $\Delta = +$ as addition and the **intersection** $\cdot = \cap$ as multiplication, the subsets of a given set X become a **ring**. It is called a **Boolean ring**. It has the property $A + A = 0$ and $A \cdot A = A$ for all sets. The **zero element** is the **empty set** $\emptyset = \{\}$. The additive inverse (the negative) of A is the complement $-A$ of A in X. The multiplicative 1-element is the full universe X under consideration because $X \cdot A = A$. As in the ring of integers, the addition and multiplication on sets is **commutative** and multiplication does not have an inverse in general. In class and homework we will play with this ring.

7.3. Two sets A, B have the **same cardinality**, if there exists a **one-to-one map** from A to B. For finite sets, this means that they have the same number of elements. Sets which do not have finitely many elements are called **infinite**. Do all sets with infinitely many elements have the same cardinality? The integers $\mathbb{Z}$ and the natural numbers $\mathbb{N}$ for example are infinite sets which have the same cardinality: $f(2n) = n, f(2n+1) = -n$ establishes a bijection between $\mathbb{N}$ and $\mathbb{Z}$. Also the rational numbers Q have the same cardinality than $\mathbb{N}$. To see this, associate a fraction p/q with an integer lattice point (p, q) in the plane, cut out the column $q = 0$ and run the Ulam spiral on the modified plane. This gives us an explicit enumeration of the rationals. We say that sets which can be counted are called of cardinality $\aleph_0$.

7.4. Does an interval $[0, 1]$ have the same cardinality than the real number line $\mathbb{R}$? Even so an interval like $(-\pi/2, \pi/2)$ has finite length, one can bijectively map it to the real lines with the tan map. Similarly one can see that any two intervals of positive length have the same cardinality. It was a great moment of mathematics, when **Georg Cantor** realized in 1874 that the interval $(0, 1)$ does not have the same cardinality than the natural numbers $\mathbb{N}$. His argument is ingenious: assume, we could count the points $a_1, a_2, \dots$ in $[0, 1]$. If $0.a_{i1}a_{i2}a_{i3}...$ is the decimal expansion of a_i, define the real number $b = 0.b_1b_2b_3...$, where $b_i = a_{ii} + 1 \bmod 10$. Because this number b does not agree at the first decimal place with a_1, nor at the second place with a_2 and so on, the number b does not appear in that enumeration of all reals. It has positive distance at least 10^{-i} from the i'th number (and any representation of the number by a decimal expansion which is equivalent). This is a contradiction. The new cardinality, the **continuum** is also denoted $\aleph_1$. The reals are **uncountable**. This gives elegant proofs like the existence of **transcendental number**, numbers which are not algebraic, the root of any polynomial with integer coefficients: algebraic numbers can be counted.

7.5. Similarly as one could establish a bijection between the natural numbers N and the integers Z, there is a bijection f between the interval I and the unit square: if $x = 0.x_1x_2x_3\dots$ is the decimal expansion of x then $f(x) = (0.x_1x_3x_5\dots, 0.x_2x_4x_6\dots)$ is a bijection between I and $I \times I$. Are there cardinalities above $\aleph_1$? Cantor answered also this question. He showed that for an infinite set, the set 2^X of all subsets of the set X has a larger cardinality than the set X itself. How does one see this? Assume there is a bijection $x \to A(x)$ which maps each point to a set $A(x)$. Now look at the set $B = \{x \mid x \notin A(x)\}$ and let b be the point in X which corresponds to B. If $y \in B$, then $y \notin B(x)$. On the other hand, if $y \notin B$, then $y \in B$. The set B does appear in the "enumeration" $x \to A(x)$ of all sets. The set of all subsets of $\mathbb{N}$ has the same cardinality than the continuum: $A \to \sum_{j \in A} 1/2^j$ provides a map from $P(\mathbb{N})$ to $[0, 1]$. The set of all **finite subsets** of $\mathbb{N}$ however can be counted. The set of all subsets of the real numbers has cardinality $\aleph_2$, etc.

7.6. Is there a cardinality between $\aleph_0$ and $\aleph_1$? In other words, is there a set which can not be counted and which is strictly smaller than the continuum in the sense that one can not find a bijection between it and $\mathbb{R}$? This was the first of the 23 problems posed by Hilbert in 1900. The answer is surprising: one has a choice. One can accept either the "yes" or the "no" as a new axiom. In both cases, mathematics is still fine. The nonexistence of a cardinality between $\aleph_0$ and $\aleph_1$ is called the **continuum hypothesis** and is usually abbreviated CH. It is independent of the other axioms making up mathematics. This was the work of **Kurt Gödel** in 1940 and **Paul Cohen** in 1963. For most mathematical questions, it does not matter whether one accepts CH or not. The story of exploring the consistency and completeness of axiom systems of all of mathematics is exciting. Euclid gave axioms for Euclidean geometry, Hilbert's goal was much more ambitious, to find a set of axiom systems for all of mathematics. The challenge to prove Euclid's 5'th postulate is paralleled by the quest to prove the CH. But the later is much more fundamental and striking because it deals with **all of mathematics** and not only with a particular field of geometry. Here are the **Zermelo-Frenkel Axioms** (ZFC) including the Axiom of choice

(C) as established by **Ernst Zermelo** in 1908 and **Adolf Fraenkel** and **Thoral Skolem** in 1922.

7.7.

Extension	If two sets have the same elements, they are the same.
Image	Given a function and a set, then the image of the function is a set too.
Pairing	For any two sets, there exists a set which contains both sets.
Property	For any property, there exists a set for which each element has the property.
Union	Given a set of sets, there exists a set which is the union of these sets.
Power	Given a set, there exists the set of all subsets of this set.
Infinity	There exists an infinite set.
Regularity	Every nonempty set has an element which has no intersection with the set.
Choice	Any set of nonempty sets leads to a set which contains an element from each.

7.8. The **axiom of choice (C)** has a nonconstructive nature which can lead to seemingly paradoxical results like the **Banach Tarski paradox**: one can cut the unit ball into 5 pieces, rotate and translate the pieces to assemble two identical balls of the same size than the original ball. Gödel and Cohen showed that the axiom of choice is logically independent of the other axioms ZF. Other axioms in ZF have been shown to be independent, like the **axiom of infinity**. A **finitist** would refute this axiom and work without it. It is surprising what one can do with finite sets. The **axiom of regularity** excludes Russellian sets like the set X of all sets which do not contain themselves. The **Russell paradox** is: does X contain X? It has also been popularized as the **Barber riddle**: a barber in a town only shaves the people who do not shave themselves. Does the barber shave himself?

7.9. A complete axiom system for mathematics is not possible because of **Gödel's theorems** of 1931. They deal with **mathematical theories**. They are assumed to be sufficiently strong meaning that one can do at least basic arithmetic in them and call it simply **a theory**:
First incompleteness theorem:
In any theory there are true statements which can not be proved within the theory.
Second incompleteness theorem:
In any theory, the consistency of the theory can not be proven within the theory.
The proof uses an encoding of mathematical sentences which allows to state liar paradoxical statement "this sentence can not be proved". While the later is an odd recreational entertainment gag, it is the core for a theorem which makes striking statements about mathematics. These theorems are not limitations of mathematics; they illustrate how wast it is. Wouldn't it be terrible if we could build axiom system and enumerate mechanically all possible truths from it?

7.10. The work of **George Cantor** and **Kurt Gödel** changed the way we think and teach about mathematics. In both cases, the mathematics community needed time to absorb the implications of the revolutions. Hilbert said about Cantor "Nobody will drive us from the paradise that Cantor has created for us". Cantor clarified the term "cardinality" is, showed that certain infinities like that the cardinality of points in the plane or points in space are the same and most importantly showed that different infinities exist. Gödel's theorems show that mathematics and knowledge in general can not be exhausted by listing a sequence of basic truths from which everything follows. Whenever we make such a list, there are statements which are independent of the system. It would be a mistake to take this as a limitation of mathematics, in contrary it shows that mathematics is inexhaustible: there is always something more to explore.

7.11. We first demonstrate that one can compute with sets like with numbers. There is an addition, the symmetric difference and a multiplication, the intersection. With these two operations, we prove the familiar rules of arithmetic

$$A + B = B + A, A \cdot B = B \cdot A, A \cdot (B + C) = A \cdot B + A \cdot C$$

hold. This is called a **Boolean algebra**. There is a set which plays the role of 0. Which one is it? There is also a set which plays the role of 1. Which one is it? One can calculate with sets as with numbers. They form a "Boolean ring".
Addition: $A + B = A \Delta B$ with the zero element $\emptyset$
Multiplication: $A \cdot B = A \cap B$ with the one element Ω.
All the rules of the real numbers apply but there are additional consequences which appear a bit strange $A + A = 0$ and $A^2 = A \cdot A = A$. This means that A is its own additive inverse. We will visualize the laws of this algebra with **Venn diagrams**.

7.12. Hilbert's hotel is located on route 8. It has countably many rooms numbered $1, 2, 3, \ldots$. The hotel is fully booked. As a newcomer arrives. David, the hotel manager is mortified. David has an idea and moves guest in room i to room $i + 1$ and gives the newcomer the first room 1.
An other day, the hotel is empty but a large group arrives. They are the "fractions" on their way to a cardinal match with the "squares". Can David accommodate them? He thinks hard and finally manages.
In the summer, the "reals" appear. David is not there but has George, the apprentice is in the office. The group consists of all real numbers between 0 and 1. Can George accommodate them? As much as he tries to shift and renumber, he can not do it.

7.13. Paradoxa like the **Liars paradox** "I never tell the truth", the **barbers paradox** "the barber is the person who shaves everybody who does not shave himself" the **surprise exam problem** "it is impossible to make a surprise exam problem", the **heap problem** "take a grain away from a heap keeps it a heap", the **biographer's problem** "who needs one year to write one day of his biography", Here is an other, the **Berry paradox** which comes somehow close to the Goedel numbering: **The smallest integer not definable in less than 11 words.** The problem is that this number is defined in 10 words. This looks like a stupid example but it illustrates that there are properties of numbers like "the shortest way to describe the number" which is not computable.

7.14. The **axiom of choice (C)** has a nonconstructive nature which can lead to seemingly paradoxical results like the **Banach Tarski paradox**: one can cut the unit ball into 5 pieces, rotate and translate the pieces to assemble two identical balls of the same size than the original ball. Cohen showed that the axiom of choice is logically independent of the other axioms ZF.

Work problems

7.15. 1) We have defined addition as $A + B = A \Delta B$ and **multiplication** as $A \cdot B = A \cap B$.
a) How can we write the union of two sets $A \cup B$ using addition and multiplication?
b) Verify that $A = -A$. The set A is the unique set which satisfies $A + A = \emptyset$.

c) Draw the Venn diagram of $A - B = A + (-B)$.
d) How can we write the set difference $A \setminus B$ using addition and multiplication. (Note that this is not the difference $A - B$.
e) Draw a diagram which illustrates the associativity property $A + (B + C) = (A + B) \cdot A + C$ for addition.

f) Draw a diagram which illustrates the associativity property $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ for multiplication.

g) Draw a diagram which illustrates the distributive property $A \cdot (B + C) = A \cdot B + A \cdot C$.

h) Which sets have an inverse A^{-1} in the sense that $A \cdot A^{-1} = 1 = X$?

7.16. 2) The **Russell paradox** defines the set$X$ of all sets which do not contain themselves as elements.

a) Verify that if X contains itself as an element then X contains itself as an element.
b) Verify that if X does not contain itself as an element then X does not contain itself as an element. c) A barber in Cambridge only shaves people who do not shave themselves. Does the barber shave himself? There is an elegant (non mathematical) solution to this paradox. Can you find it? d) The first version of the Liar Paradox seems have been found in the fourth century BC by Greek philosopher **Eubulides**, successor of Euclid. Somebody tells "I'm always lying". Does the person tell the truth? The paradox is attributed to the Cretan philosopher **Epimenides** who said "All Cretans are liars."

7.17. 3) We explore some cardinality questions. We look at a continuous map from the unit interval onto the unit square. And explore whether it is a bijection.
a) What is the cardinality of the prime numbers?
b) What is the cardinality of the set of linear functions $ax + b$, where a, b are real numbers? c) A number is called **algebraic** if it is a solution to a polynomial equation

$$p(x) = 0 \ ,$$

where the polynomial has integer coefficients Can we count all the polynomials? This would establish that one can count all the algebraic numbers and therefore that there are numbers which are not algebraic.

Oliver Knill, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022

TEACHING MATHEMATICS WITH A HISTORICAL PERSPECTIVE

OLIVER KNILL

Lecture 8: Probability theory

8.1. Probability theory is the science of chance. It starts with **combinatorics** and leads to a theory of **stochastic processes**. Historically, probability theory initiated from gambling problems, as in **Girolamo Cardano's** gamblers manual in the 16th century. A great moment of mathematics occurred, when **Blaise Pascal** and **Pierre Fermat** jointly laid a foundation of mathematical probability theory.

8.2. It took mathematicians longer to formalize "randomness" precisely. Here is the setup as which it had been put forward by **Andrey Kolmogorov**: all possible experiments of a situation are modeled by a set Ω which is the **laboratory**. A measurable subset of experiments is called an **event**. A probability function P gives the proability $P[A]$ of an event. Measurements are done by real-valued functions X. These functions are called **random variables** and are used to **observe the laboratory**. [1]

FIGURE 1. Probability theory started with gambling (Cardano).

[1] If Ω is finite, then every subset of Ω can be an event and every function X can be random variable. In general, there can be subsets of Ω which can not be assigned a probability in a reasonable way.

8.3. As an example, let us model the process of throwing a coin 5 times. An **experiment** is a word like $httht$, where h stands for "head" and t represents "tail". The laboratory consists of all possible 32 words. We could look for example look the event A where the first two coin tosses are tail. It is the set $A = \{ttttt, tttth, tttht, ttthh, tthtt, tthth, tthht, tthhh\}$. The most natural probability function is $P[A] = |A|/|\Omega|$, in this case $P[A] = 8/32 = 1/4$. We could also look at the random variable X which assigns to a word w the number of heads in w. For every experiment, we get a value, like for example, $X[tthht] = 2$.

8.4. In order to make precise statements about randomness, the specification of the **probability measure** is important. This is a function P from the set of all events to the interval $[0, 1]$. It should have the property that $P[\Omega] = 1$ and $P[A_1 \cup A_2 \cup \dots] = P[A_1] + P[A_2] + \cdots$, if A_i are disjoint events.

8.5. The most natural probability measure on a finite set Ω is $P[A] = \|A\|/\|\Omega\|$, where $\|A\|$ stands for the number of elements in A. It is the ""number of good cases" divided by the "number of all cases". For example, to count the probability of the event A that we throw 3 heads during the 5 coin tosses, we have $|A| = 10$ possibilities. Since the entire laboratory has $|\Omega| = 32$ possibilities, the probability of the event is $P[A] = 10/32$. In order to study these probabilities, **combinatorics** helps:

How many ways are there to:	**The answer is:**
rearrange or permute n elements	$n! = n(n-1)...2 \cdot 1$
choose k from n with repetitions	n^k
pick k from n if order matters	$\frac{n!}{(n-k)!}$
pick k from n with order irrelevant	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

8.6. The **expectation** $\mathrm{E}[X]$ of a random variable X is defined as the sum $m = \sum_{\omega \in \Omega} X(\omega) P[\{\omega\}]$. In our coin toss experiment, this is $5/2$. The **variance** of X is the expectation of $(X - m)^2$. In our coin experiments, it is $5/4$. Its square root is called the **standard deviation**. This is the expected deviation from the mean. An event happens **almost surely** if the event has probability 1.

8.7. An important case of a random variable is $X(\omega) = \omega$ on $\Omega = R$ equipped with probability $P[A] = \int_A \frac{1}{\sqrt{\pi}} e^{-x^2} \, dx$, the **standard normal distribution**. Analyzed first by **Abraham de Moivre** in 1733, it was studied by **Carl Friedrich Gauss** in 1807 and therefore also called **Gaussian distribution**.

8.8. Two random variables X, Y are called **decorrelated**, if $E[XY] = E[X] \cdot E[Y]$. If for any functions f, g also $f(X)$ and $g(Y)$ are decorrelated, then X, Y are called **independent**. Two random variables are said to have the same distribution, if for any $a < b$, the events $\{a \leq X \leq b\}$ and $\{a \leq Y \leq b\}$ are independent. If X, Y are decorrelated, then the relation $\mathrm{Var}[X] + \mathrm{Var}[Y] = \mathrm{Var}[X + Y]$ holds. This is just the **Pythagorean theorem**, because decorrelated can be understood geometrically: $X - E[X]$ and $Y - E[Y]$ are orthogonal.

8.9. A common problem is to study the sum of independent random variables X_n with identical distribution. One abbreviates this with **IID**. Here are the three important theorems which we formulate in the case, whee all random variables are assumed to have expectation 0 and standard deviation 1. Let $S_n = X_1 + \cdots + X_n$ be the n'th sum of the IID random variables. It is also called a **random walk**.

LLN **Law of Large Numbers** assures that S_n/n converges to 0.

CLT **Central Limit Theorem**:$S_n/\sqrt{n}$ approaches the Gaussian distribution.

LIL **Law of Iterated Logarithm:** $S_n/\sqrt{2n \log\log(n)}$ accumulates in $[-1, 1]$.

(For LLN and LIL, one should say that the converges happens with probability 1. For the CLT, the convergence is in the sense of distributions.)

8.10. The LLN shows that one can find out about the expectation by averaging experiments.
The CLT explains why one sees the standard normal distribution so often.
The LIL gives us a precise estimate how fast S_n grows.
Things become interesting if the random variables are no more independent. Generalizing LLN,CLT,LIL to such situations is part of ongoing research.

8.11. Here is an open questions in probability theory:

Are $\pi, e, \sqrt{2}\cdots$ normal in the following sense: do all digits appear with the same frequency?

8.12. **Statistics** is the science of modeling random events in a probabilistic setup. Given data points, we want to find a **model** which fits the data best. This allows to **understand the past**, **predict the future** or **discover laws of nature**. The most common task is to find the **mean** and the **standard deviation** of some data. The mean is also called the **average** and given by $m = \frac{1}{n}\sum_{k=1}^{n} x_k$. The variance is $\sigma^2 = \frac{1}{n}\sum_{k=1}^{n}(x_k - m)^2$ with standard deviation σ.

8.13. A sequence of random variables X_n produce a **stochastic process**. Continuous versions of such processes are where X_t is a curve of random random variables. An important example is **Brownian motion**, which is a model of a random particles.

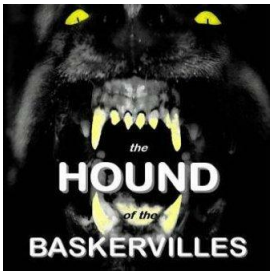
8.14. Besides gambling and analyzing data, also **physics** has been an important motor to develop probability theory. An example is statistical mechanics where laws of nature are studied with probabilistic methods. A famous physical law is **Ludwig Boltzmann's** relation $S = k\log(W)$ for entropy, a formula which decorates Boltzmann's tombstone. The **entropy** of a probability measure $P[\{k\}] = p_k$ on a finite set $\{1, ..., n\}$ is defined as $S = -\sum_{i=1}^{n} p_i \log(p_i)$. Today, we would reformulate Boltzmann's law and say that it is the expectation $S = E[\log(W)]$ of the logarithm of the "Wahrscheinlichkeit" random variable $W(i) = 1/p_i$ on $\Omega = \{1, ..., n\}$.

8.15. Entropy is important because nature tries to maximize it In the simplest situations, if a system has n states, the $W = n$. If each state has an energy E_i and the free energy $S - E$ is minimized, the probability distribution $p_i = e^{-E_i}/Z$ is the **Boltzman distribution**.

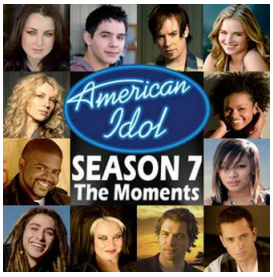
Here are the most important combinatorics problems:

How many ways are there to:	**The answer is:**
permute n elements	$n! = n(n-1)...2 \cdot 1$
choose k from n with repetitions	n^k
pick k different from n if order matters	$\frac{n!}{(n-k)!}$
pick k different from n where order does not matter	$\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Problem 1: You play "scrabble". You are stuck with the letters $STORY$. How many single words of length 5 can you write?



Problem 2: the "Hound of Baskervilles" has 338'787 letters. How many novels are there with this number of letters? You can assume an alphabet of 30 including space and punctuations.



Problem 3: How many ways are there to chose 3 people from a contestant group of 12 if the order does not matter?

Problem 4: A combination lock has 40 numbers $0-39$. A lock combination consists of 3 different numbers, where the order matters. How many different lock combinations are there?

Work problems

8.16. 1) We want to understand the famous **Monty Hall problem**

You have to choose from three doors. Behind one door is a car and behind the others are goats. You pick a door. The host, who knows what's behind the doors, opens an another door, one which has a goat. You have the choice to choose the door or to switch. What is better?

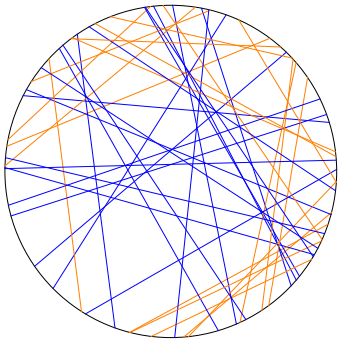
The problem became sensation and controversy in 1991. Intuitive argumentation can lead to the conclusion that it does not matter whether to change the door or not. When asked, a large

majority of test persons tell that it does not matter. a) We first assume that we decide not to switch.
You choose a door. Note that the revelation of the host does not affect your choice.
What is the probability that you win in this case?
b) Now we switch. We look at three possibilities now.
What happens if you initially chose the door with the car? Do you win or lose in this case?
c) What happens if you initially chose the door with the goat? Do you win or lose in this case?
d) What do you conclude

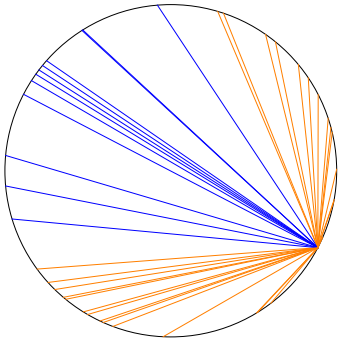
8.17. 2) For the following question, most people would say 1/2.

Dave has 2 kids. One of them is a boy. What is the probability that the other kid is a girl?

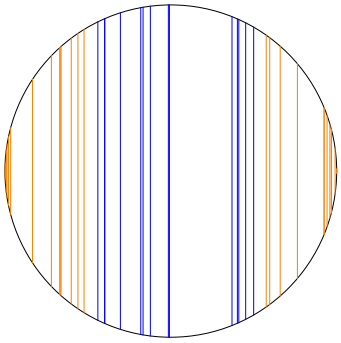
8.18. The **Bertrand paradox** illustrates that one has to be clear on how to setup a probabilistic model in a concrete situation.



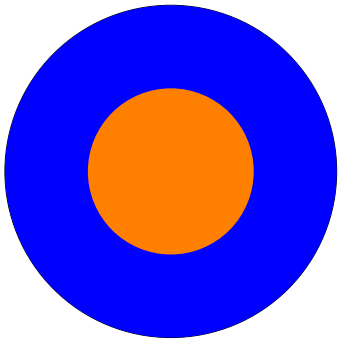
We throw random lines onto the unit disc. What is the probability that the line intersects the disc with a length $\geq \sqrt{3}$, the length of the inscribed equilateral triangle?



Problem 1) Take an arbitrary point on the boundary of the disc. The set of all lines through that point are parameterized by an angle ϕ. For which midpoints is the length of the chord longer than the equilateral triangle length? By comparing angles, what is the probability?



Problem 2) Take now all lines perpendicular to a fixed diameter. The entire diameter has length 2. Where do the chords hit the diameter so that it is longer than $\sqrt{3}$? By comparing lengths, what is the probability?



Problem 3) Look at the midpoints of the chords. Where does such a midpoint have to be so that the chord is longer than $\sqrt{3}$? By comparing areas, what is the probability now?

8.19. The origins of probability was in gambling. We look here closely at the Petersburg paradox, which had been devised by Daniel Bernoulli in 1738. You pay a fixed entrance fee C and you get the prize 2^T, where T is the number of times, the casino flips a coin until "head" appears.
For example, you enter 10 dollars. If the sequence of coin experiments would give "tail, tail, tail, head", you win $2^3 - 10 = 8 - 10 = -2$ dollars. This means you have lost 2 dollars in this game.

a) Build groups of 2-4. One is the casino, the others play the casino. Choose an entrance fee which you think is fair and play as many times as time allows. In the end, record your winning.
b) What is the probability that you lose your entire winning? That is, what is the chance that we have "head" the first time? Note that $T = 0$ in this case. c) What is the probability that we have "head" the second time? Note that $T = 2$ in this case. How much do we win or lose in this case?
d) What is the probability that "head" appears the third time? Note that $T = 3$ in this case. How much did you win or lose in this case?
e) What is the probability that "head" appears at time $T = n$ the first time? How much did you win or lose in this case?
Fair would be an entrance fee which is equal to the expectation of the win, which is $1 \cdot P[T = 0] + 2 \cdot P[T = 1] + 5 \cdot P[T = 2] + ...$ What does "fair" mean? For example, the situation $T = 20$ is so improbable that it never occurs in the life-time of a person. Therefore, for any practical reason, one has not to worry about large values of T. This, as well as the finiteness of money resources is the reason, why casinos do not have to worry about the following bullet proof **martingale strategy** in roulette: bet c dollars on red. If you win, stop, if you lose, bet $2c$ dollars on red. If you win, stop. If you lose, bet $4c$ dollars on red. Keep doubling the bet. Eventually after n steps, red will occur and you will win $2^n c - (c + 2c + \cdots + 2^{n-1}c) = c$ dollars.

8.20. Here is some additional information. How does one solve the Petersburg paradox? What would be a reasonable entrance fee in "real life"? Bernoulli proposed to replace the expectation $\mathrm{E}[G]$ of the profit $G = 2^T$ with the expectation $(\mathrm{E}[\sqrt{G}])^2$, where $u(x) = \sqrt{x}$ is called a **utility function**. This would lead to a fair entrance

$$(\mathrm{E}[\sqrt{G}])^2 = (\sum_{k=1}^{\infty} 2^{k/2} 2^{-k})^2 = \frac{1}{(\sqrt{2}-1)^2} \sim 5.828... \, .$$

Similar effects appear in political situations as in **voting systems**, where different voting systems can produce different winners. The following example is by Donald Saari:

"Consider 15 people deciding what beverage to serve at a party. Six prefer milk first, wine second, and beer third; five prefer beer first, wine second, and milk third; and four prefer wine first, beer second, and milk third. In a plurality vote, milk is the clear winner. But if the group decides instead to hold a runoff election between the two top contenders milk and beer, then beer wins, since nine people prefer it over milk. And if the group awards two points to a drink each time a voter ranks it first and one point each time a voter ranks it second, suddenly wine is the winner."

OLIVER KNILL

Lecture 9: Topology

9.1. **Topology** is rubber geometry. It studies properties of geometric objects that do not change under continuous invertible deformations. For a topologist, a coffee cup with a single handle is the same as a doughnut. One can deform one into the other without punching any holes or ripping things apart. Similarly, a plate and a croissant are the same. But a croissant is not equivalent to a doughnut. On a doughnut, there are closed curves which can not be pulled together to a point. For a topologist, the letters O and P are the same but they both are different from the letter B.

9.2. The mathematical setup is beautiful: a **topological space** is a set X with a set O of subsets of X containing both $\emptyset$ and X such that finite intersections and arbitrary unions in O are in O. Sets in O are called **open sets** and O is called a **topology**. The complement of an open set is called **closed**. Examples of topologies are the **trivial topology** $O = \{\emptyset, X\}$, where no open sets besides the empty set and X exist or the **discrete topology** $O = \{A \mid A \subset X\}$, where every subset is open. But these are in general not interesting.

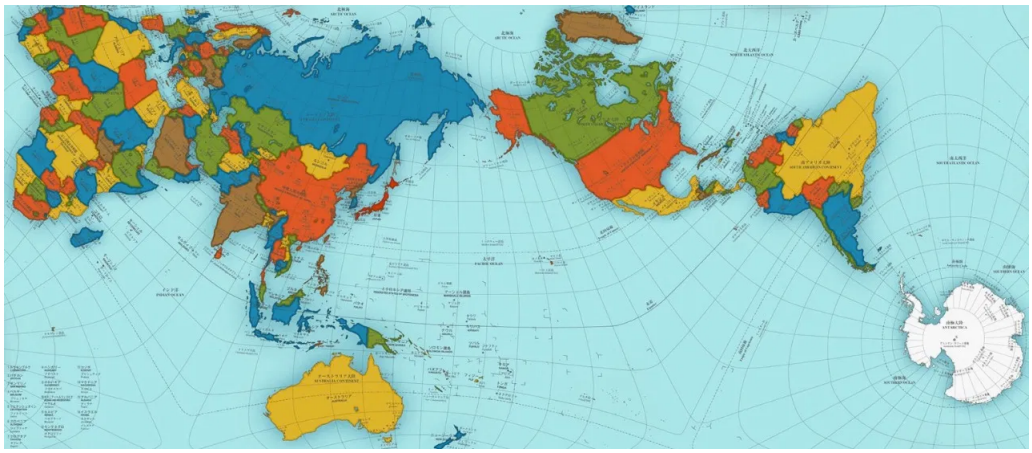


FIGURE 1. To map the spherical earth we need an atlas. An example is the authagraph. It maps the earth onto a tetrahedron then unfolds that to a rectangle and preserves area at about 100 parts of the earth. You can see why it has appeared in Japan (1999) and is not so popular yet in places like Europe.

9.3. For example, let X be the set of points of your paper and $\mathcal{O}$ the set of sets generated by open balls. For the of $\mathcal{O}$ one can use arbitrary unions and finite intersections. Special class of topological spaces are **metric spaces**. These are sets X that are equipped with a **distance function** $d(x, y) = d(y, x) \geq 0$ satisfying the **triangle inequality** $d(x, y) + d(y, z) \geq d(x, z)$ and which has the property that $d(x, y) = 0$ if and only if $x = y$. A set U in a metric space is open, if to every x in U, there is a **ball** $B_r(x) = \{y | d(x, y) < r\}$ of positive radius r contained in U. The set of open sets defines then a topology.

9.4. A substantial part of topology deals with spaces which locally look like our space. An example is the **sphere** for which our earth is an example. At a fixed location on earth the geometry looks like part of a plane but we need an **atlas** to cover all of X. The charts are then glued together with identification maps on the intersection. This gives what one calls a **manifold**. An other example of such a space is the **torus** or the **Klein bottle**. Topological spaces X, Y are "topologically equivalent" if there is an invertible map from X to Y so that this also induces an invertible map on the corresponding topologies.

9.5. A basic task is to decide whether two spaces are equivalent in this sense or not. The surface of the coffee cup for example is equivalent in this sense to the surface of a doughnut but it is not equivalent to the surface of a sphere. In an informal sense, two spaces are equivalent, if one can deform one into an other without changing quantities like connectivities, dimension or the collection of closed non-contractible loops in the space. Punching a hole into a paper for example changes the topology of the space. Gluing together left and right of a rectangular paper changes its topology to a cylinder. If the upper and lower parts are identified too, one has the "pacman space" which is a doughnut and called a torus.

9.6. Many properties of geometric spaces X can be understood by replacing them with **finite networks**. The points and connections then form a skeleton of the space. Networks are also called **graphs**. A finite simple graph (V, E) is a finite collection of vertices V paired with a finite set of edges E, where each edge in E connects two different points in V. For example, the set V of cities in the US form a network if one takes as edges are pairs of neighboring cities connected by a street. Two cities x, y are neighboring if there is a direct street from x to y not passing through an other city.

9.7. Graph theory is the birth crib of topology. The **Königsberg bridge problem** was a trigger for the study of graph theory. Also **Polyhedra**, objects already studied by the Greeks has led to graphs. The study of polyhedra is loosely related to the analysis of surfaces. The reason is that one can see polyhedra as discrete versions of surfaces. In computer graphics for example, surfaces are rendered as networks of triangulations.

9.8. The **Euler characteristic** of a convex polyhedron is a remarkable topological invariant. For two dimensional convex polyhedra, it is

$$V - E + F = 2 \ ,$$

where V is the number of vertices, E the number of edges and F the number of **faces**. This formula for the Euler characteristic is also called **Euler's gem**. It comes with a rich history. **René Descartes** seems have stumbled upon it and written it down in a secret notebook. It was Leonard Euler in 1752 was the first to proved the formula for convex polyhedra. There was a long sequence of proofs of refutations which however all boil down to how general one assumes the notion of polyhedron to be. Removing the assumption of convex for example can completely change the story. There are non-convex polyhedra which have not Euler characteristic 2. Kepler has found some. The story has been woven into a dialog written by Lacatos: "Proofs and Refutations". It is a tale of caution to use precise definitions.

9.9. A convex polyhedron is called a **Platonic solid**, if all vertices are on the unit sphere, all edges have the same length and all faces are congruent polygons. A theorem of **Theaetetus** states that there are only five platonic solids: [Proof: Assume the faces are regular n-gons and m of them meet at each vertex. Beside the Euler relation $V + E + F = 2$, a polyhedron also satisfies the relations $nF = 2E$ and $mV = 2E$ which come from counting vertices or edges in different ways. This gives $2E/m - E + 2E/n = 2$ or $1/n + 1/m = 1/E + 1/2$. From $n \geq 3$ and $m \geq 3$ we see that it is impossible that both m and n are larger than 3. There are now nly two possibilities: either $n = 3$ or $m = 3$. In the case $n = 3$ we have $m = 3, 4, 5$ in the case $m = 3$ we have $n = 3, 4, 5$. The five possibilities $(3, 3), (3, 4), (3, 5), (4, 3), (5, 3)$ represent

the five platonic solids.] The pairs (n, m) are called the **Schläfly symbol** of the polyhedron:

Name	V	E	F	V-E+F	Schläfli
tetrahedron	4	6	4	2	$\{3,3\}$
hexahedron	8	12	6	2	$\{4,3\}$
octahedron	6	12	8	2	$\{3,4\}$

Name	V	E	F	V-E+F	Schläfli
dodecahedron	20	30	12	2	$\{5,3\}$
icosahedron	12	30	20	2	$\{3,5\}$

9.10. The Greeks proved the classification result geometrically: Euclid showed in the "Elements" that each vertex can have either 3,4 or 5 equilateral triangles attached, 3 squares or 3 regular pentagons. (6 triangles, 4 squares or 4 pentagons would lead to a total angle which is too large because each corner must have at least 3 different edges). **Simon Antoine-Jean L'Huilier** refined in 1813 Euler's formula to situations with holes: $V - E + F = 2 - 2g$, where g is the number of holes. For a doughnut with one hole we have $V - E + F = 0$. . Cauchy first proved that there are exactly 4 non-convex regular **Kepler-Poinsot** polyhedra. Their Euler characteristic can be different.

Name	V	E	F	V-E+F	Schläfli
small stellated dodecahedron	12	30	12	-6	$\{5/2,5\}$
great dodecahedron	12	30	12	-6	$\{5,5/2\}$
great stellated dodecahedron	20	30	12	2	$\{5/2,3\}$
great icosahedron	12	30	20	2	$\{3,5/2\}$

If two different face types are allowed but each vertex still look the same, one obtains 13 **semi-regular polyhedra.** They were first studied by **Archimedes** in 287 BC. Since his work is lost, **Johannes Kepler** is considered the first person since antiquity to describe the whole set of thirteen in his "Harmonices Mundi". The Euler characteristic $\chi = 2 - 2g$ is also useful for surfaces. One can reduce the question to graphs, triangularizations of the surface.

9.11. It turns out that the Euler characteristic completely characterizes smooth compact surfaces if they are orientable. A non-orientable surface, the **Klein bottle** can be obtained by gluing ends of the Möbius strip. Classifying higher dimensional manifolds is more difficult and finding good invariants is part of modern research. Higher analogues of polyhedra are called **polytopes** (Alicia Boole Stott). **Regular polytopes** are the analogue of the platonic solids in higher dimensions. Here they are for the first few dimensions:

dimension	name	Schläfli symbols
2:	Regular polygons	$\{3\}, \{4\}, \{5\}, ...$
3:	Platonic solids	$\{3,3\}, \{3,4\}, \{3,5\}, \{4,3\}, \{5,3\}$
4:	Regular 4D polytopes	$\{3,3,3\}, \{4,3,3\}, \{3,3,4\}, \{3,4,3\}, \{5,3,3\}, \{3,3,5\}$
≥ 5:	Regular polytopes	$\{3,3,3,\ldots,3\}, \{4,3,3,\ldots,3\}, \{3,3,3,\ldots,3,4\}$

9.12. Ludwig Schläfly found in 1852 that there are exactly six convex regular convex 4-polytopes or **polychora**. The expression "choros" is Greek for "space". Schlaefli's polyhedral formula tells that for any **convex polytope** in four dimensions, the relation

$$V - E + F - C = 0$$

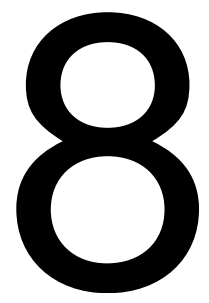
holds, where C is the number of 3-dimensional **chambers**. In dimensions 5 and higher, there are only 3 types of polytopes: the higher dimensional analogues of the tetrahedron, octahedron and the cube. A general formula $\sum_{k=0}^{d-1}(-1)^k v_k = 1 - (-1)^d$ gives the Euler characteristic of a convex polytop in d dimensions with k-dimensional parts v_k.

Work problems

9.13. 1) The digits 0-9:
a) The numbers $0, 4, 6, 9$ are topologically equivalent.

b) The numbers $1, 2, 3, 5, 7$ are topologically equivalent.

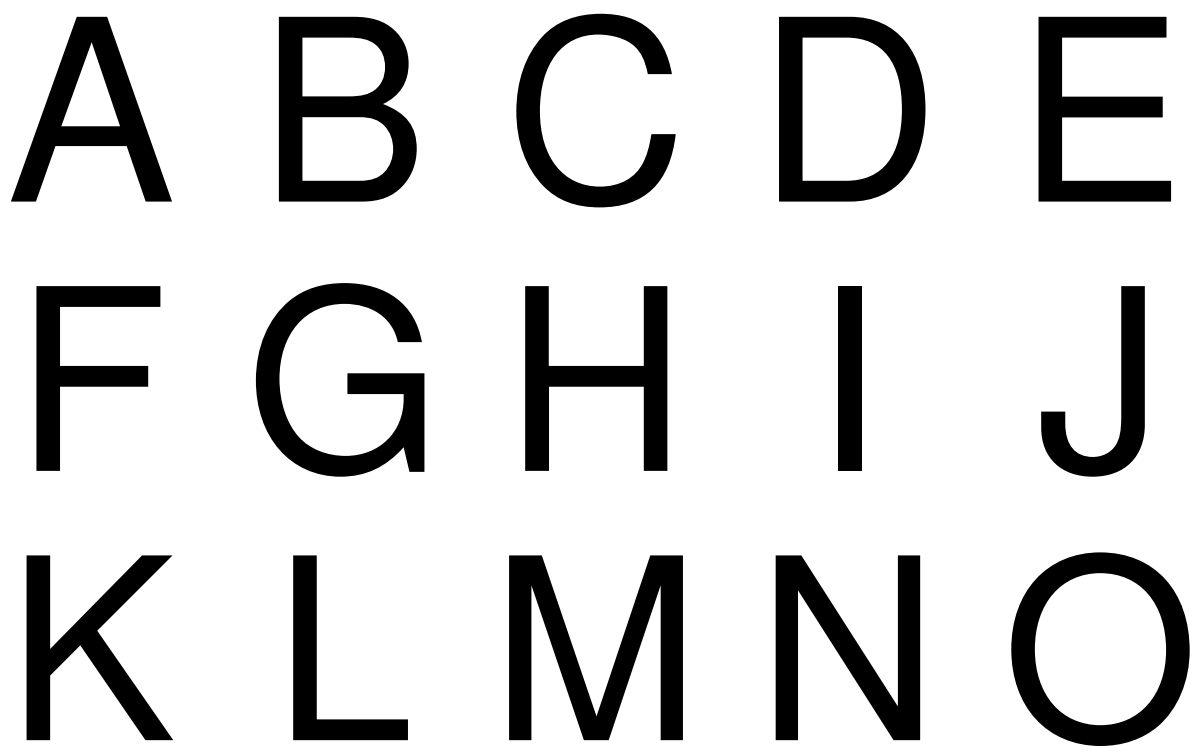
c) The number 8 is not topologically equivalent to any other digit.



d) Are there any numbers which are disconnected?

e) Which numbers are simply connected?

9.14. 2) The letters:

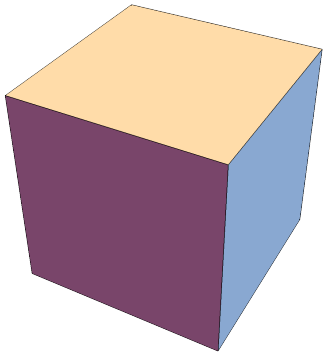


P Q R S T

U V W

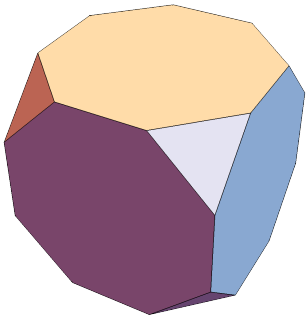
X Y Z

9.15. 3. Euler Characteristic



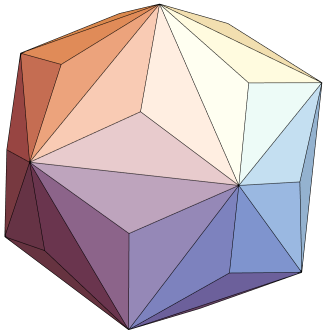
a) Compute the Euler Characteristic $V - E + F$ for the cube

Vertices V	Edges E	Faces F



b) Cutting the corners of the cube produces 8 new faces and renders the old faces octagonal. Count the Euler characteristic of the new object which is now a semi-regular polyhedron.

Vertices V	Edges E	Faces F



c) Start again with the cube, but now cut each of the faces into 4 faces by drawing the diagonals in the squares. If the midpoints are lifted up a bit so that all triangles become equilateral, the new object is called a **stellation** of the cube. It is an other semi-regular polyhedron.

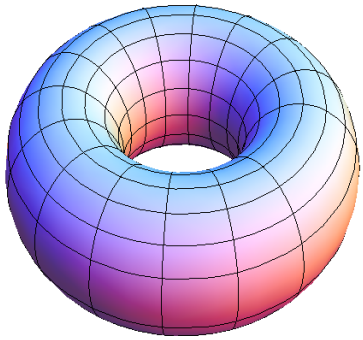
Vertices V	Edges E	Faces F

9.16. 3) Which of the following pieces of cloth are topologically equivalent?

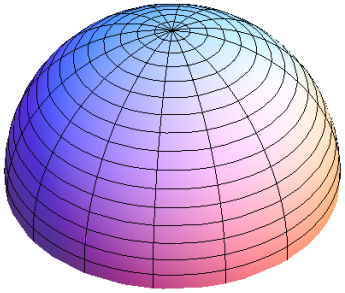
9.17. 4) By identifying sides of a square we obtain models of compact surfaces: the **sphere**, the **torus**, the **projective plane** and the **Klein bottle**. We want to explore here the topology of

these spaces, especially the simply conntectedness: can one pull any closed rope in this space to a point? Only the sphere is simply connected.

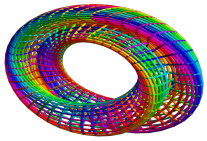
a) Draw some curves on the torus, which can not be pulled together to a point.



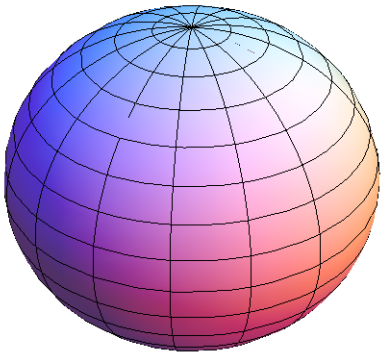
b) Draw a curve on the projective plane, which can not be pulled together to a point.



c) Move a letter R around on the Klein bottle, what happens with the letter as it moves over the boundary to the right and appears to the left?



d) Draw a curve on the sphere. Visualize that you can pull it together to a point.



e) By triangulating a space, we are also able to compute the Euler characteristic of these spaces. The Euler characteristic of the sphere is 2, the Euler characteristic of the torus is 0, the Euler characteristic of the projective plane is 1, the Euler characteristic of the Klein bottle is 0. Can you show this in the examples?

Oliver Knill, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022

OLIVER KNILL

Lecture 10: Analysis

10.1. **Analysis** is the science of measure and optimization. As contains a rather diverse collection of mathematical fields, it contains **real and complex analysis**, **functional analysis**, **harmonic analysis** and **calculus of variations**. Analysis also has close relations to calculus, geometry, topology, probability theory and dynamical systems.

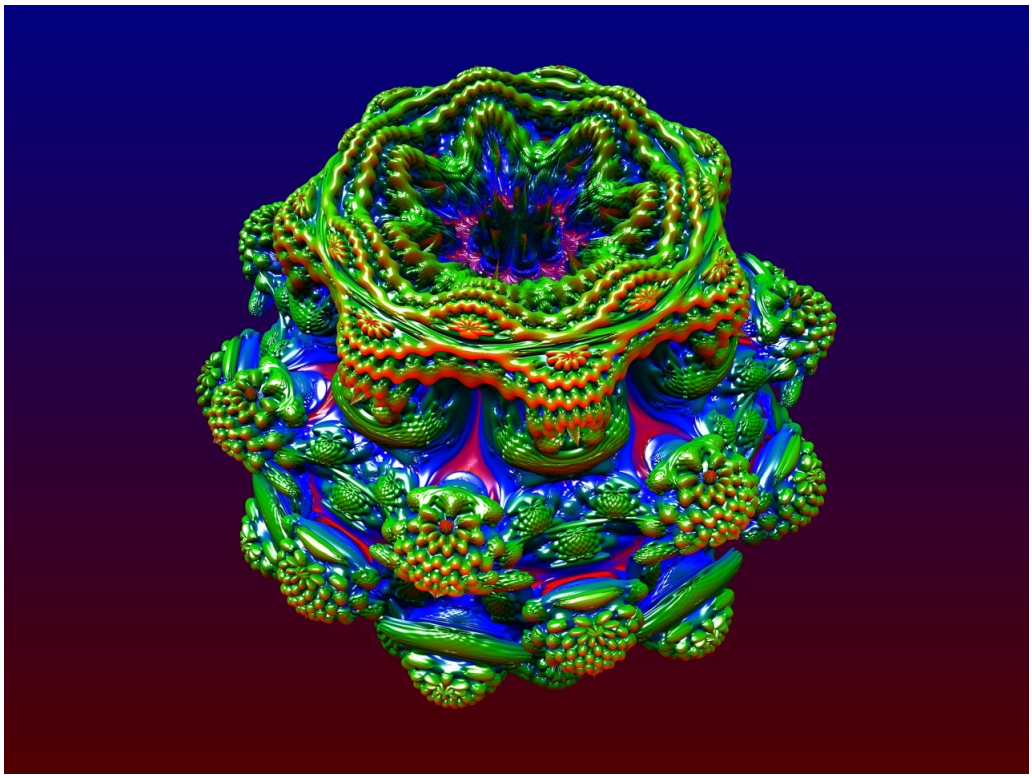


FIGURE 1. The mysterious Mandelbulb was rendered with Mandelbulb3D under Wine in Linux. It is a fractal type shape with properties which are still completely mysterious.

10.2. We focus here mostly on "the geometry of fractals" which can be seen as part of **dimension theory**. Examples are Julia sets which belong to the sub-field of "complex analysis" of "dynamical systems". The subject of "Calculus of variations" could be illustrated by the Kakeya needle set in "geometric measure theory", "Fourier analysis" appears when looking at functions which have fractal graphs, "spectral theory" as part of functional analysis is represented by the "Hofstadter butterfly". We somehow try to illustrate the vast field of analysis using "pop icons", being aware that it is very much worn out. Being labeled as **mathematical kitsch** should however not disqualify the subject.

10.3. A **fractal** is a set with non-integer dimension. An example is the **Cantor set**, as discovered in 1875 by Henry Smith. Start with the unit interval. Cut the middle third, then cut the middle third from both parts then the middle parts of the four parts etc. The limiting set is the Cantor set. The mathematical theory of fractals belongs to **measure theory** and can also be viewed of a playground for real analysis or topology.

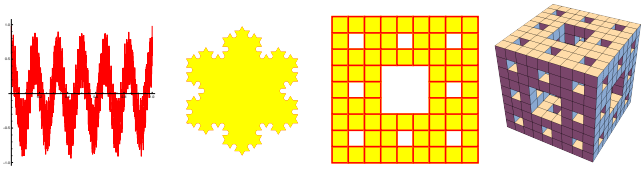
10.4. The term **fractal** had been introduced by Benoit Mandelbrot in 1975, with his book "The fractal geometry of nature". Very important is the notion of **Dimension**. It can be defined in different ways. The simplest is the **box counting definition** which works for most "household fractals": if we need n squares of length r to cover a set, then

$$d = -\log(n)/\log(r)$$

converges to the dimension of the set with $r \to 0$. A curve of length L for example needs L/r squares of length r so that its dimension is 1. A region of area A needs A/r^2 squares of length r to be covered and its dimension is 2. The Cantor set needs to be covered with $n = 2^m$ squares of length $r = 1/3^m$. Its dimension is $-\log(n)/\log(r) = -m\log(2)/(m\log(1/3)) = \log(2)/\log(3)$.

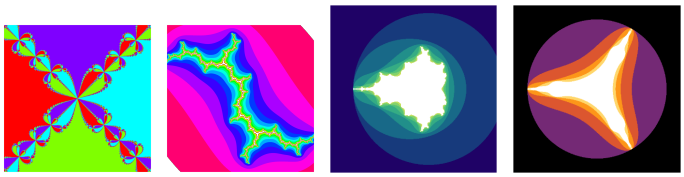
10.5. Examples of fractals (for the first, the dimension is

Weierstrass function	1872
Koch snowflake	1904
Sierpinski carpet	1915
Menger sponge	1926



Complex analysis extends calculus to the complex. It deals with functions $f(z)$ defined in the complex plane. Integration is done along paths. Complex analysis completes the understanding about functions. It also provides more examples of fractals by iterating functions like the **quadratic map** $f(z) = z^2 + c$:

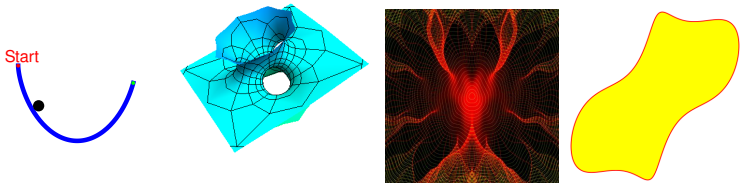
Newton method	1879
Julia sets	1918
Mandelbrot set	1978
Mandelbar set	1989



10.6. Particularly famous Julia sets are the **Douady rabbit** and the **dragon**, the **dendrite**, the **airplane**.

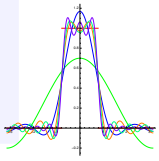
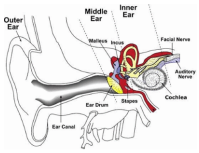
10.7. Calculus of variations is calculus in infinite dimensions. Taking derivatives is called taking "variations". Historically, it started with the problem to find the curve of fastest fall leading to the **brachistochrone** curve $\vec{r}(t) = (t - \sin(t), 1 - \cos(t))$. In calculus, we find maxima and minima of functions. In calculus of variations, we extremize on much larger spaces. Here are some examples of problems:

Brachistochrone	1696
Minimal surface	1760
Geodesics	1830
Isoperimetric problem	1838
Kakeya Needle problem	1917



10.8. Fourier theory decomposes a function into basic trigonometric parts of various frequencies $f(x) = a_1\sin(x) + a_2\sin(2x) + a_3\sin(3x)...$. The numbers a_i are called Fourier coefficients. Our ear does such a decomposition, when we listen to music. By distinguish different frequencies, our ear produces a Fourier analysis.

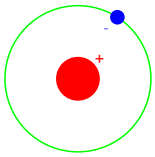
Fourier series	1729
Fourier transform (FT)	1811
Discrete FT	Gauss?
Wavelet transform	1930

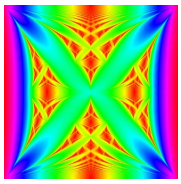
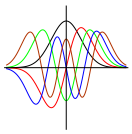




10.9. The Weierstrass function mentioned above is given as a series $\sum_n a^n \cos(\pi b^n x)$ with $0 < a < 1, ab > 1 + 3\pi/2$. The dimension of its graph is believed to be $2 + \log(a)/\log(b)$ which is confirmed for some ranges.

10.10. Spectral theory analyzes linear m.pdf L. The **spectrum** are the real numbers E such that $L - E$ is not invertible. A Hollywood celebrity among all linear m.pdf is the **Matthieu operator** $L(x)_n = x_{n+1} + x_{n-1} + (2 - 2\cos(cn))x_n$: if we draw the spectrum for for each c, we see the **Hofstadter butterfly**. For fixed c the map describes the behavior of an electron in an almost periodic crystal. An other famous system is the **quantum harmonic oscillator**, $L(f) = f''(x) + f(x)$, the **vibrating drum** $L(f) = f_{xx} + f_{yy}$, where f is the amplitude of the drum and $f = 0$ on the boundary of the drum.

Hydrogen atom	1914
Hofstadter butterfly	1976
Harmonic oscillator	1900
Vibrating drum	1680




10.11. All these examples in analysis look unrelated at first. Fractal geometry ties many of them together: spectra are often fractals, minimal configurations have fractal nature, like in solid state physics or in **diffusion limited aggregation** or in other critical phenomena like **percolation** phenomena, **cracks** in solids or the formation of **lighting bolts**

10.12. In Hamiltonian mechanics, minimal energy configurations are often fractals like **Mather theory**. And solutions to minimizing problems lead to fractals in a natural way like when you have the task to turn around a needle on a table by 180 degrees and minimize the area swept out by the needle. The minimal turn leads to a Kakaya set, which is a fractal.

10.13. Finally, lets mention some unsolved problems in analysis. The firs problem is also a problem in number theory: does the **Riemann zeta function** $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ have all nontrivial roots on the axis $\mathrm{Re}(s) = 1/2$? This question is called the **Riemann hypothesis** and is the most important open problem in mathematics. It is an example of a question in **analytic number theory** which also illustrates how analysis has entered into number theory. Some mathematicians think that spectral theory might solve it.

10.14. Also the Mandelbrot set M is not understood yet: the "holy grail" in the field of complex dynamics is the problem whether it M is locally connected. About the Hofstadter butterfly one knows that it has measure zero. What is its dimension?

10.15. An other open question in spectral theory is the "can one hear the sound of a drum" problem which asks whether there are two convex drums which are not congruent but which have the same spectrum.
In the area of calculus of variations, just one problem: how long is the shortest curve in space such that its convex hull (the union of all possible connections between two points on the curve) contains the unit ball.

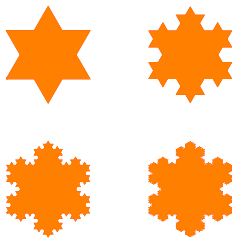
10.16. Here is a shorter summary: as Analysis reaches a lot of different areas in mathematics, it is also harder to define. Analysis often extends calculus to areas where traditional calculus does no more apply, like to infinite dimensions or to functions which are not continuous. Sometimes also, it deals with rather strange objects, like fractal geometries or generalized functions. Our goal is to understand **fractals** as they make an appearance in many parts of analysis: spectral theory, complex analysis, harmonic analysis, calculus of variations or functional analysis. Because these fields need some time to learn and explain, the analysis of fractals looks like a nice entry point as it can be seen and the need for a new mathematics is evident. Our story will be mostly pictorial. There is one single formula, we want to understand:

$$\dim(X) = \frac{-\log(n)}{\log(r)} .$$

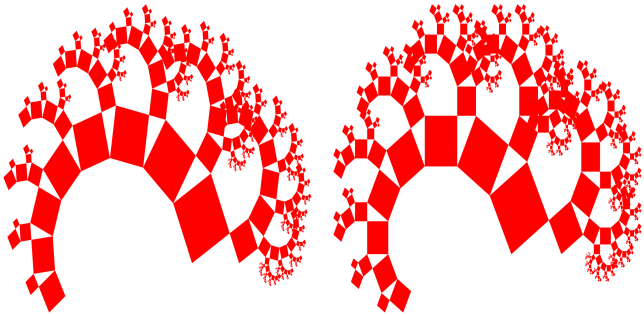
It tells that if we want to find the dimension of an object, we cover it with boxes of size $r > 0$ and count how many boxes we need. Assume this number is n. Dimension is what happens if r goes to zero. The prototype of a fractal is the **Cantor set** which was discovered in 1875 by **Henry Smith**. Start with the unit interval. Cut the middle third, then cut the middle third from both parts then the middle parts of the four parts etc. What is left in the end is the Cantor set for which the dimension is log(2) log(3).

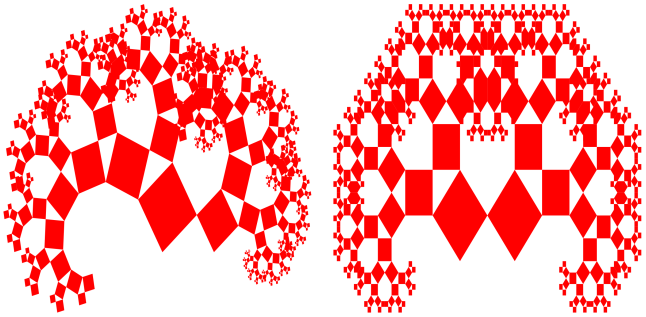
10.17. Here are again pictures of the more famous fractals: first the Cantor set

The **Koch snowflake** is an example of a fractal with dimension located strictly between 1 and 2. It was first described by the Swedish mathematician **Helge von Koch** (1870-1924) who described it in 1904. It is a simple model for a **snowflake**. There is a simplified version which just is defined over an interval. It is called the **Koch curve**.

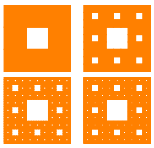


The tree of Pythagoras:

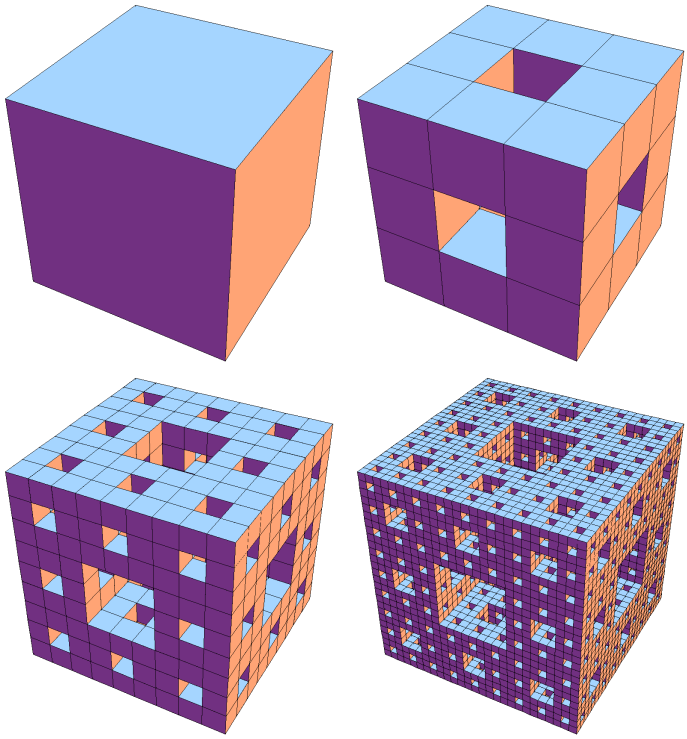




The **tree of Pythagoras** is an example of a fractal with dimension between 1 and 2. We have seen it in our first lecture. The tree of Pythagoras inspired antenna designs for small devices.



The **Sierpinski carpet** is a fractal in the plane. Its dimension is $\log(8)/\log(2)$. It was described by **Waclav Sierpinski** in 1916.



The **Menger sponge** is a fractal in space. Its dimension is between 2 and 3. It was first described by Karl Menger (1902-1985). Its dimension is $\log(20)/\log(3)$ which is about 2.7.

10.18. In order to understand the Mandelbrot set we need to look at complex numbers $z = a+ib$ and define complex multiplication

$$(a + ib)(u + iv) = au - bv + (av + bu)i \ .$$

Now look at the function $f(z) = z^2 + c$, where c is a fixed complex number. Start with $z = i$ for example, we get $f(z) = i + c$ and $f^2(z) = f(f(z)) = (i + c)^2 + c$ etc. The **Mandelbrot set** is the set of complex numbers $c = a+ib$ for which $f^n(0)$ stays bounded. The **filled in Julia set** J_c of c is the set of z such that $f^n(z)$ stays bounded. The **Julia set** is the boundary of the filled in Julia set.

For example, for $c = 0$, the map is $f_0(z) = z^2$. Since $|z^n| = |z|^n$ we see that the disc $\{|z| \leq 1\}$ is the filled in Julia set for $c = 0$ and the unit circle $\{|z| = 1\}$ is the Julia set.

10.19. A three dimensional version of the Mandelbrot set is called the **Mandelbulb**. It uses spherical coordinates which have been introduced by Euler.

10.20. The **Hofstadter butterfly** is an example of a fractal which appears in spectral theory. It was first described in 1976 and was popularized in Hofstadters book "Goedel-Escher-Bach".

Work problems

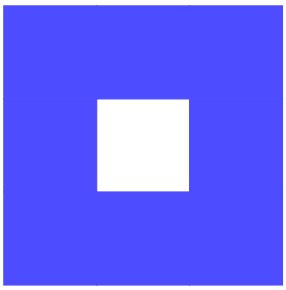
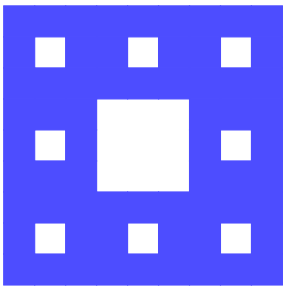
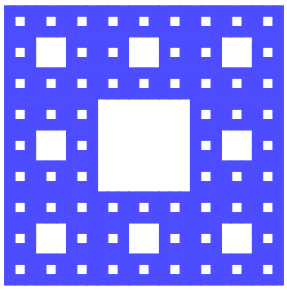
10.21. 1) We want to compute the dimension of various objects in the plane. If we need n squares of side length r to cover an object X. the dimension is defined as

$$d = \frac{-\log(n)}{\log(r)} \text{ when } r \text{ gets zero.}$$

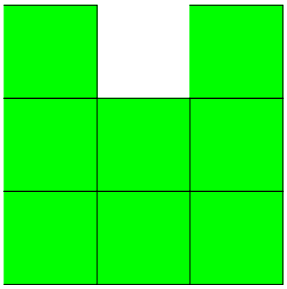
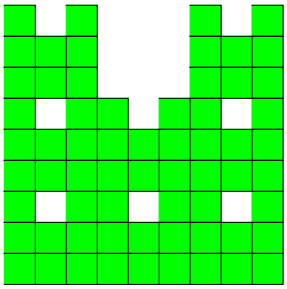
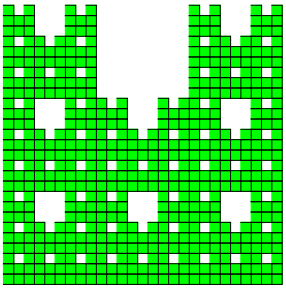
a) Assume a curve is given as the boundary of the unit square. How many squares of length $r = 1/10$ do we need to cover the curve? If we call n this number, what is $-\log(n)/\log(r)$?

b) Assume a region is the unit square. How many squares of length $r = 1/10$ do we need to cover the square? If we call n this number, what is $-\log(n)/\log(r)$?

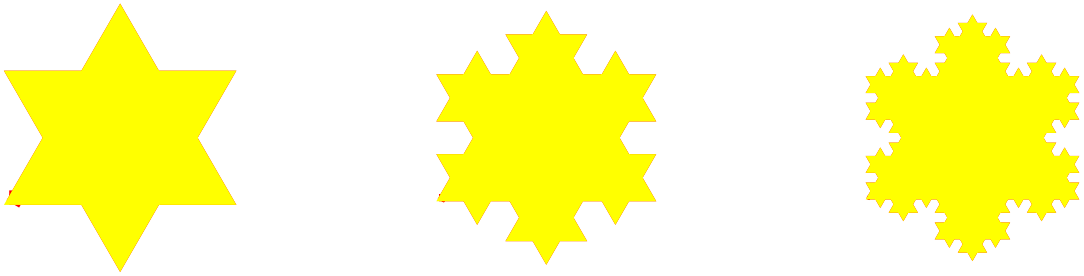
c) The **Sirpinski carpet** is constructed recursively by dividing a square in 9 equal squares and cutting away the middle one, repeating this procedure with each of the squares etc. At the k'th step, we need $n = 8^k$ squares of length $r = 1/3^k$ to cover the carpet. What is the dimension?

d) What is the dimension of the following fractal from which we see the first levels of construction?

e) What is the dimension of the Koch snowflake? How large is n, the number of squares we need to covert the flake if the square has size $1/3^k$ assuming that the first triangle has side length 1.



10.22. 2) We want to understand the definition of the Julia sets and the Mandelbrot set. Define

$$T(z) = z^2 + c \ ,$$

where c is a fixed parameter. The **filled in Julia set** J_c is the set of points z for which the orbit $z, T(z), T(T(z))...$ stays bounded. The **Mandelbrot set** M is the set of c for which the point 0 is in the filled in Julia set J_c. It is the set of c such that $0, T(0) = c, T(T(0)) = c^2 + c, T(T(T(0))) = (c^2 + c)^2 + c...$ stays bounded. The **Julia set** finally is the boundary of the filled in Julia set.
a) What is the square root of -9?
b) Add $2 + 6i$ with $6 + 8i$.

c) Multiply $2 + 6i$ with $6 + 8i$.

d) What is the length of the complex number $3 + i4$?

e) Assume $c = 2$. Compute the first 3 st.pdf of the orbit of $z = 1$ of the quadratic map.

f) Verify that 0 is inside the Mandelbrot set. Verify that -1 is inside the Mandelbrot set. Verify that i is inside the Mandelbrot set.

g) Verify that 2 is outside the Mandelbrot set. Verify that 1 is outside the Mandelbrot set.

h) Can you verify that $1/4$ is the largest real number in the Mandelbrot set and -2 the smallest real number in the Mandelbrot set?

OLIVER KNILL

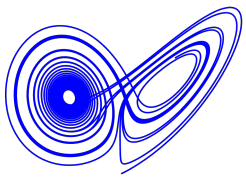
E-320: Teaching Math with a Historical Perspective **O. Knill, 2010-2022**

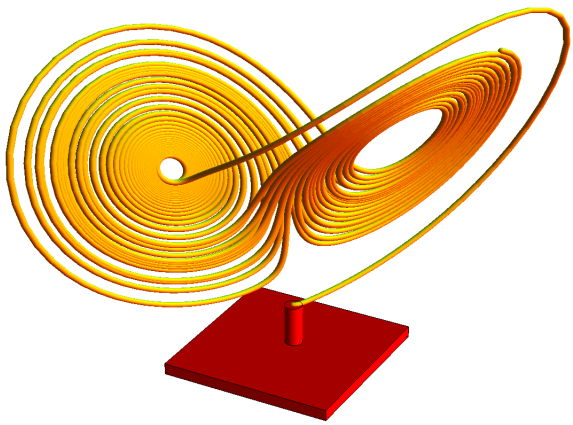
Lecture 11: Dynamical systems

11.1. **Dynamical systems theory** is the science of time. If time is **continuous**, the evolution is defined by a **differential equation** $\dot{x} = f(x)$. If time is **discrete**, then we look at the **iteration of a map** $x \to T(x)$. Here is the prototype of a differential equation in three dimensions:

$$\begin{aligned} \dot{x} &= \sigma(y-x) \\ \dot{y} &= rx - y - xz \\ \dot{z} &= xy - bz \ . \end{aligned}$$

the **Lorenz system**. There are three parameters σ, r, b. For $\sigma = 10, r = 28, b = 8/3$, one observes a **strange attractor** with fractal shape.





11.2. The goal is to **predict the future** of the system when the present state is known. A **differential equation** is an equation of the form $d/dtx(t) = f(x(t))$, where the unknown quantity is a path $x(t)$ in some "phase space". We know the **velocity** $d/dtx(t) = \dot{x}(t)$ at all times and the initial configuration $x(0)$), we can to compute the **trajectory** $x(t)$. What happens at a future time? Does $x(t)$ stay in a bounded region or escape to infinity? Which areas of the phase space are visited and how often? Can we reach a certain part of the space when starting at a given point and if yes, when. An example of such a question is to predict, whether an asteroid located at a specific location will hit the earth or not. An other example is to predict the weather of the next week.

11.3. An example of a dynamical systems in one dimension is the differential equation

$$x'(t) = x(t)(2 - x(t)), x(0) = 1 \ .$$

It is called the **logistic system** and describes population growth. This system has the solution $x(t) = 2e^t/(1 + e^{2t})$ as you can see by computing the left and right hand side.

11.4. A **map** is a rule which assigns to a quantity $x(t)$ a new quantity $x(t + 1) = T(x(t))$. The state $x(t)$ of the system determines the situation $x(t+1)$ at time $t+1$. An example is is the **Ulam map** $T(x) = 4x(1 - x)$ on the interval $[0, 1]$. This is an example, where we have no idea what happens after a few hundred iterates even if we would know the initial position with the accuracy of the Planck scale. We will experiment with that in class.

11.5. Dynamical system theory has applications in all fields of mathematics. We can use dynamical systems for example to find roots of equations. The **Newton map**

$$T(x) = x - f(x)/f'(x)$$

is such a procedure. If we are close enough to the fixed point, applying T again and again will have us converge very fast to the fixed point.

11.6. Dynamical systems also appear in number theory. For large primes p, nonlinear maps like $T(x) = x^2 + c \mod p$ or $T(x) = a^x \mod p$ behave rather erratically. And this is good so as the maps can be used for encryption.

11.7. A rather curious system of number theoretical nature is the **Collatz map**

$$T(x) = \frac{x}{2} \text{ (even x)}, 3x + 1 \text{ else} \ .$$

A system of geometric nature is the **Pedal map** which assigns to a triangle the pedal triangle.

11.8. Lets look a bit at the history of chaos: about 100 years ago, **Henry Poincaré** was able to deal with **chaos** of low dimensional systems. While **statistical mechanics** had formalized the evolution of large systems with probabilistic methods already, the new insight was that simple systems like a **three body problem** or a **billiard map** can produce very complicated motion. It was Poincaré who saw that even for such low dimensional and completely deterministic systems, random motion can emerge.

11.9. While physicists have dealt with chaos earlier by assuming it or artificially feeding it into equations like the **Boltzmann equation**, the occurrence of stochastic motion in simple systems like double penduli, geodesic flows or billiards or restricted three body problems was a surprise. These findings needed half a century to sink in and only with the emergence of computers in the 1960ies, the awakening happened. Icons like Lorentz helped to popularize the findings and we owe them the **"butterfly effect"** picture: a wing of a butterfly can produce a tornado in Texas in a few weeks.

11.10. The reason for this statement is that the complicated equations to simulate the weather reduce under extreme simplifications and truncations to a simple differential equation $\dot{x} = \sigma(y - x), \dot{y} = rx - y - xz, \dot{z} = xy - bz$, the **Lorenz system**. For $\sigma = 10, r = 28, b = 8/3$, Ed Lorenz discovered in 1963 an interesting long time behavior and an aperiodic "attractor". Ruelle-Takens called it a **strange attractor**. It is a **great moment** in mathematics to realize that attractors of simple systems can become fractals on which the motion is chaotic. It suggests that such behavior is abundant. What is chaos? If a dynamical system shows **sensitive dependence on initial conditions**, we talk about **chaos**. We will experiment with the two maps $T(x) = 4x(1 - x)$ and $S(x) = 4x - 4x^2$ which starting with the same initial conditions will produce different outcomes after a couple of iterations.

11.11. The sensitive dependence on initial conditions is measured by how fast the derivative dT^n of the n'th iterate grows. The exponential growth rate γ is called the **Lyapunov exponent**. A small error of the size h will be amplified to $he^{\gamma n}$ after n iterates. In the case of the Logistic map with $c = 4$, the Lyapunov exponent is $\log(2)$ and an error of 10^{-16} is amplified to $2^n \cdot 10^{-16}$. For time $n = 53$ already the error is of the order 1. This explains the above experiment with the different maps. The maps $T(x)$ and $S(x)$ round differently on the level 10^{-16}. After 53 iterations, these initial fluctuation errors have grown to a macroscopic size.

11.12. Here is a famous open problem which has resisted many attempts to solve it: Show that the map

$$T(x, y) = (c\sin(2\pi x) + 2x - y, x)$$

with $T^n(x, y) = (f_n(x, y), g_n(x, y))$ has sensitive dependence on initial conditions on a set of positive area. More precisely, verify that for $c > 2$ and all n $\frac{1}{n}\int_0^1 \int_0^1 \log|\partial_x f_n(x, y)|\, dxdy \geq \log(\frac{c}{2})$. I have tried over a decade to prove this using methods from quantum mechanics, calculus of variations and complex analytic methods. The problem is open.

11.13. The left hand side converges to the average of the Lyapunov exponents which is in this case also the **entropy** of the map. For some systems, one can compute the entropy. The logistic map with $c = 4$ for example, which is also called the **Ulam map**, has entropy $\log(2)$. The **cat map**

$$T(x, y) = (2x + y, x + y) \bmod 1$$

has positive entropy $\log|(\sqrt{5} + 3)/2|$. This is the logarithm of the larger eigenvalue of the matrix implementing T.

11.14. While questions about simple maps look artificial at first, the mechanisms prevail in other systems: in astronomy, when studying planetary motion or electrons in the van Allen belt, in mechanics when studying coupled pendulum or nonlinear oscillators, in fluid dynamics when studying vortex motion or turbulence, in geometry, when studying the evolution of light on a surface, the change of weather or tsunamis in the ocean.

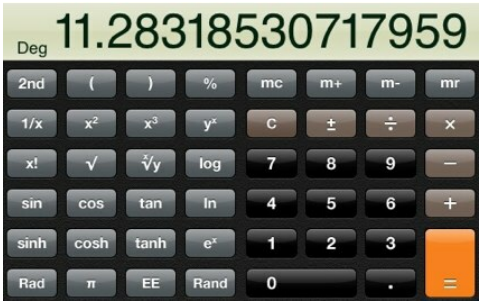
11.15. Dynamical systems theory historically started with the problem to understand the **motion of planets**. Newton realized that this is governed by a differential equation, the **n-body problem**

$$x_j''(t) = \sum_{i=1}^{n} \frac{c_{ij}(x_i - x_j)}{|x_i - x_j|^3} \ ,$$

where c_{ij} depends on the masses and the gravitational constant. If one body is the sun and no interaction of the planets is assumed and using the common center of gravity as the origin, this reduces to the **Kepler problem** $x''(t) = -Cx/|x|^3$, where planets move on **ellipses**, the radius vector sweeps equal area in each time and the period squared is proportional to the semi-major axes cubed. A great moment in astronomy was when Kepler derived these laws empirically. An other great moment in mathematics is Newton's theoretically derivation from the differential equations.

Work problems

1) We experiment with simple transformations can produce chaotic outcome. Make sure your calculator is in the "Rad" mode. Remember that 2π radians is equal to 360 degrees. You can check whether your calculator is in Radian mode, by computing $\cos(\pi)$ and get the result -1. Make sure your calculator is in rad mode. Use a scientific calculator. In the iphone calculator for example, turn the device to get to the scientific mode.



The Scientific Calculator built in by default in the Iphone/Ipod/Ipad appears when you turn the device.

a) Take a calculator, and pushing repetitively the button cos. What do you observe?

b) Now repeat pushing the sin button. What do you observe?

c) Now push x^2 repetitively.

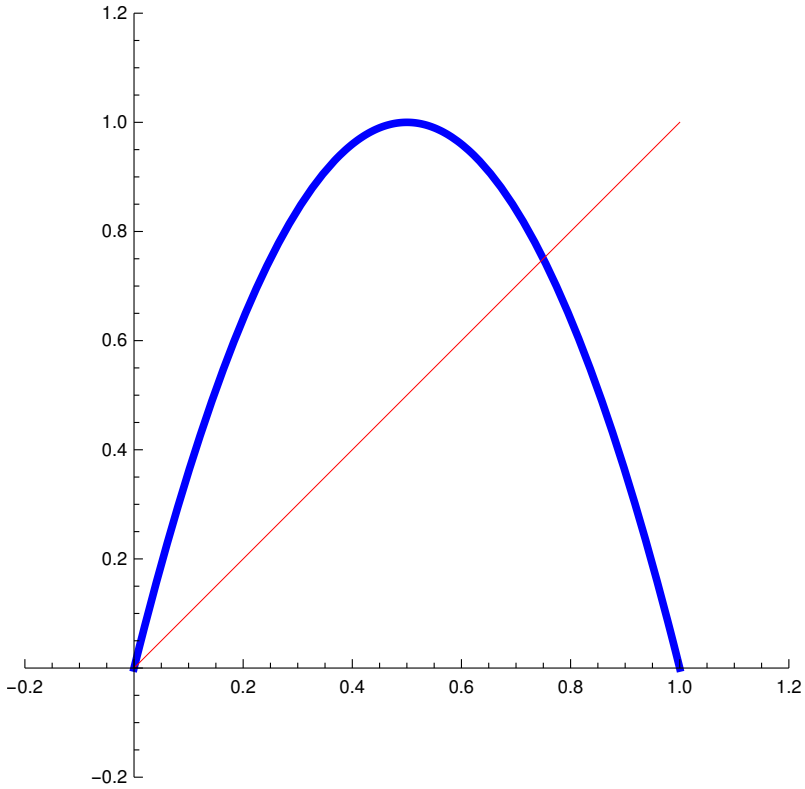
d) Now push $\sqrt{x}$ repetitively.

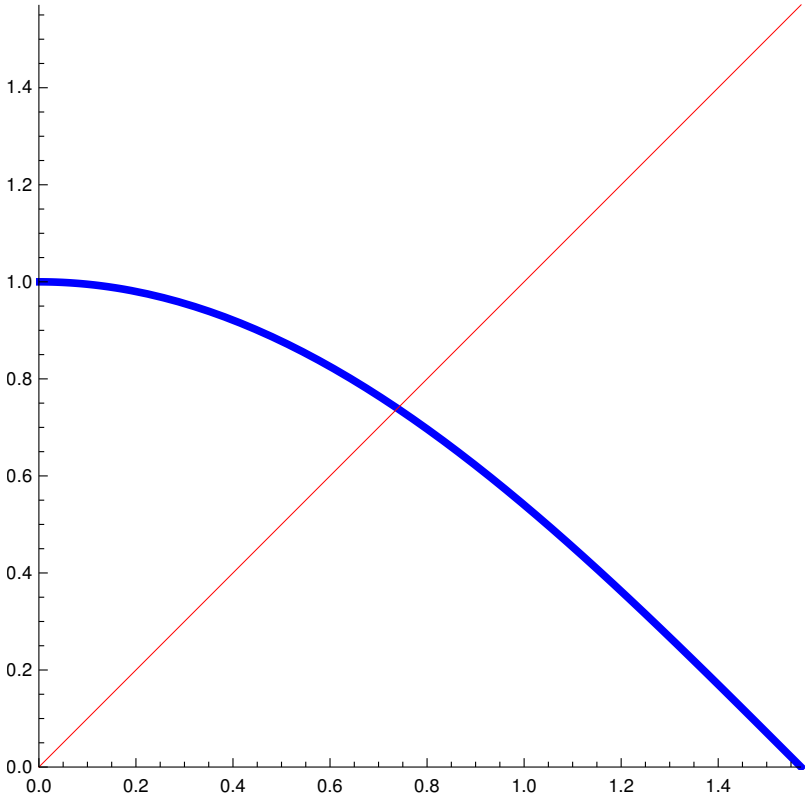
e) What do you see if you push the buttons sin, then type $1/x$ and repeat this process again and again?

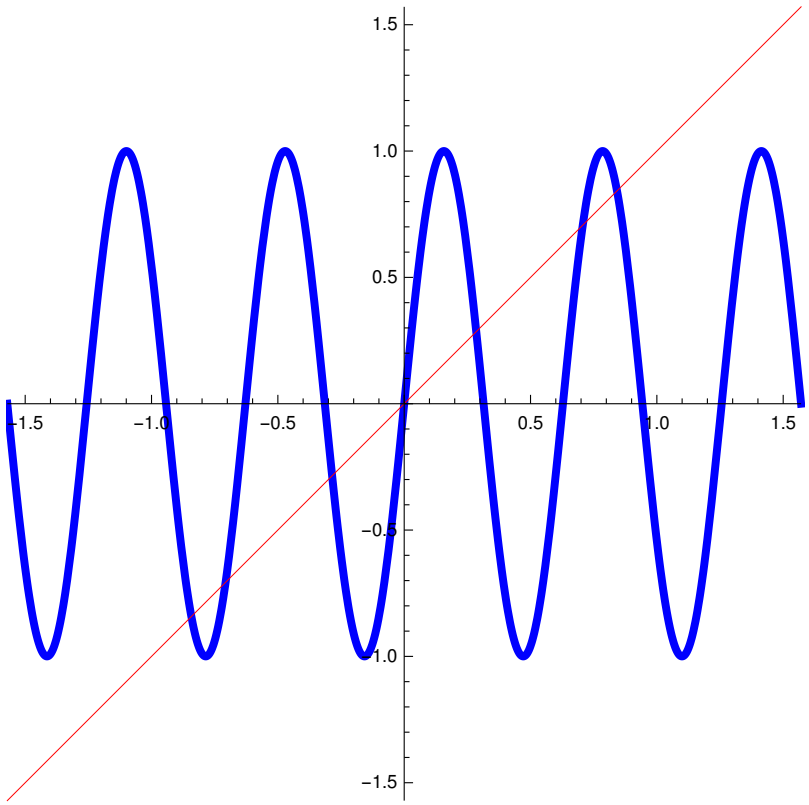
f) Experiment with the button tan. Also here, change from tan and cot (in the cot case, you might have to hit tan and $1/x$ buttons after each other).

g) Look for other "chaotic" key combinations? Experiment also with Deg and Rad changes and try especially the log functions.

2) We graphically compute a few iterates of one dimensional maps. This can be done on paper. One produces a so called cobweb.







3) We look at a dynamical system of number theoretical nature. In the **Collatz system**, we start with an integer and map it with the following rule:

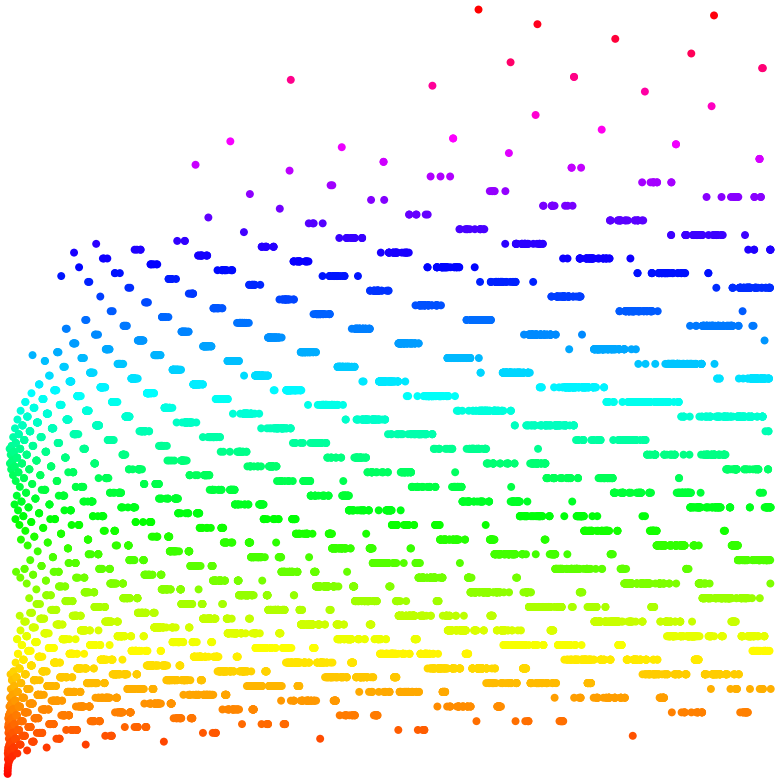
$$T(x) = \begin{cases} x/2 & x \text{ even} \\ 3x+1 & x \text{ odd} \end{cases}$$

The question is whether the orbit always ends up with 1. For example: $x = 7$ produces $7, 22, 11, 34, 17$.
a) Start with the initial condition 26:
b) Start with the initial condition 9:
c) Start with the initial condition 2048:
d) What is wrong with the following proof of the Collatz conjecture?

Proof. Consider only the odd numbers in the Collatz sequence. We show that each odd number is in average 3/4 times smaller than the previous one:

> With probability 1/2 the number $3x+1$ is divisible by 2 and not 4: this increases x by 3/2
> With probability 1/4 the number $3x+1$ is divisible by 4 and not 8: this decreases x by 3/4
> With probability 1/8 the number $3x+1$ is divisible by 8 and not 16: this decreases x by 3/8

To compute the probability, we take logarithms and compute $a = \sum_{n=1}^{\infty} \frac{1}{2^n} \log(3/2^n)$. The average decay rate of the size of a number is the factor $e^a = 3/4$.

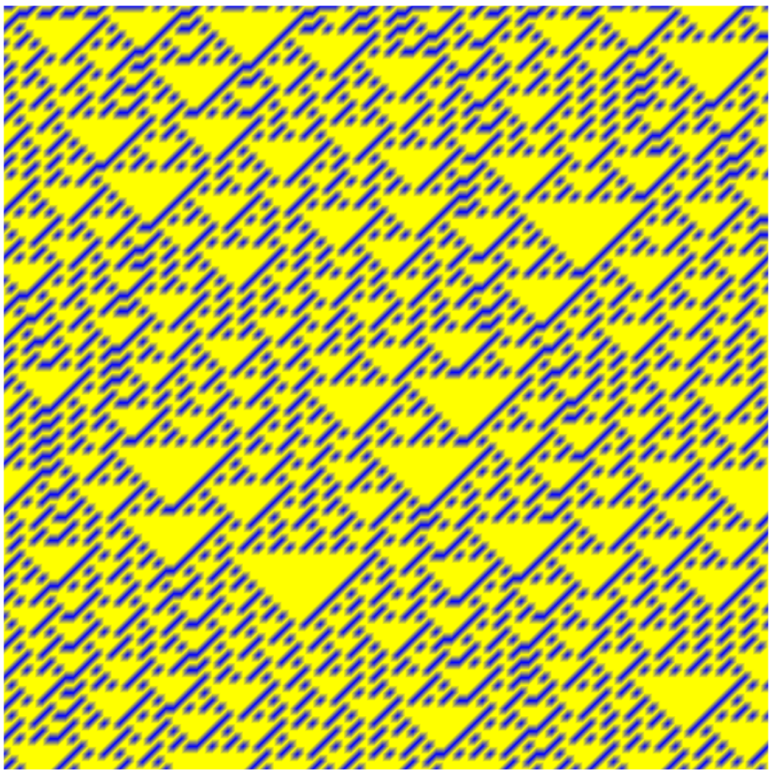


e) The Collatz system certainly can be modified. Can you find one, for which there is a nontrivial loop?

4) We look at a dynamical systems called Cellular automata. These are continuous maps on sequence spaces in which the evolution rule is translational invariant.

neighborhood	new middle cell
111	0
110	0
101	0
100	1
011	0
010	0
001	1
000	0

to an offspring 1, we and $100 = 4, 001 = 1$ in binary, we have $2^4 + 2^1 = 18$.



a) run it:

1	0	1	0	0	0	1	0	0	1	0	1	1	0	1	0

Cellular Automata Offer New Outlook on Life, the Universe, and Everything

What kind of world do we live in? The question has been bandied about for thousands of years by philosophers, theologians, and politicians. More recently, a spectrum of talk show hosts have weighed in on the subject. So far, no one's come up with an answer that everyone can agree on.

Mathematicians have considered the same question. But where others worry over the blurred boundaries of Good and Evil, mathematicians ponder a sharper dichotomy: the Continuous versus the Discrete.

Continuous mathematics, exemplified by calculus and differential equations, has long dominated mathematical descriptions of the world. But discrete mathematics is making a bid for primacy. With modern computers, researchers have discovered astonishingly complex behavior in seemingly simple, finite systems. The results have led some theorists to speculate that discrete models, which lend themselves to digital computation, are the "right" way to study nature.

Erica Jen, a mathematician at Los Alamos National Laboratory in Los Alamos, New Mexico, is one of a growing number of researchers who believe that discrete mathematics can mirror many aspects of physical reality fully as well as the more customary continuous theories. Jen has been studying mathematical properties of discrete systems known as cellular automata. These systems, she says, are useful models for many types of complex physical, chemical, or biological systems. They also have an amazing life of their own.

Cellular automata "exhibit an extremely rich and diverse range of pattern formation," Jen says. Among the most interesting are "self-organizing" patterns: highly structured features that seem to emerge spontaneously from a "primordial soup" of random binary

Erica Jen. *(Photo courtesy of Erica Jen.)*

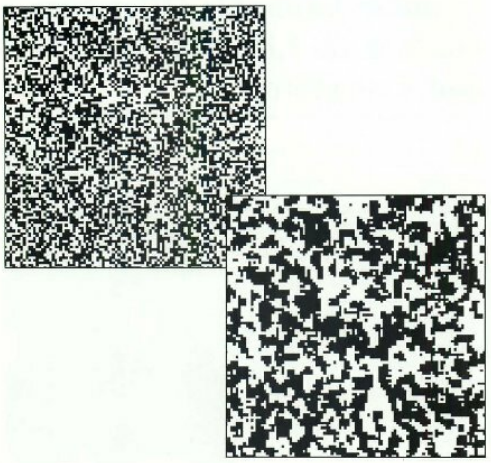


Figure 2. A 100 × 100 "majority vote" cellular automaton proceeds from a random initial state (top) to a final state (bottom right, facing page). On each ballot, every cell looks at the cells around it, and changes color value if its current value is in the minority. Most cells have 8 neighbors, but cells on the edges have 5 neighbors, and corner cells only 3. Some features of the final state take shape with the first round of voting (middle).

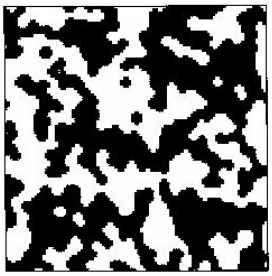
digits. Jen and her colleagues hope to understand exactly how these patterns arise and precisely what properties they possess. By studying cellular automata with mathematical tools from areas such as abstract algebra and number theory, Jen hopes to bring theoretical rigor to a subject that is often as much art as science.

Jen hopes to bring theoretical rigor to a subject that is often as much art as science.

Loosely speaking, a cellular automaton is a "polyhedron" of space and time. Instead of varying continuously from point to point and moment to moment, cellular automata consist of discrete "cells" with discrete values that change instantaneously at discrete intervals, much like frames in a movie. The crucial feature, moreover, is a *rule* that prescribes exactly how each cell's value changes depending on the values of nearby cells.

One possible rule, for example, is a "majority vote": Each cell in a system of black and white squares could be programmed to switch color if the majority of its immediate neighbors are of the opposite color (see Figure 2). Another rule might specify that the value of each cell change to the sum of the values of the cells surrounding it—or, reducing things to black and white again, to the *parity* of the sum (black could be odd and white even).

"The essential features of cellular automata are that they are deterministic and discrete in space, time, and state values; they evolve according to local interaction rules; and these rules apply



Computer technology was not really up to the job of exploring cellular automata until the 1980s.

synchronously and homogeneously across the system." Jen explains. These features accord well with standard physical assumptions about the uniformity of space and time (the laws of physics are the same everywhere) and the impossibility of instantaneous action at a distance (nothing travels faster than the speed of light). They also lend themselves to modeling complex systems consisting of a large number of simple components that are locally connected. Perhaps most important, these features are tailor-made for digital computation.

Cellular automata were first dreamt of in the early 1950s by John von Neumann and Stanislaw Ulam, as tools for studying biological systems. In the late 1960s, John Conway, then at Cambridge University (now at Princeton), invented rules for a cellular automaton he called the Game of Life, which Martin Gardner popularized in his column for *Scientific American*. But computer technology was not really up to the job of exploring cellular automata until the 1980s, when color graphics workstations replaced the clattering teletype machines that trailed alphanumeric symbols with a room-sized mainframe in another building.

With today's high-speed machines (dated, no doubt, to seem painfully slow in another few years), researchers can glimpse the complex patterns that often arise from the repeated application of the simple rules that define cellular automata. Fast computers allow experiments with relatively large systems: Automata with thousands of cells can be followed for hundreds of time steps on a personal computer; workstations and supercomputers can track systems with millions of cells for thousands of time steps.

Jen's research focuses on a class of one-dimensional systems called "elementary" cellular automata. Each state of such a system is represented by a row of black and white pixels, corresponding to a string of 1's and 0's, and the update rule uses only the value of a given cell and the values of its two adjoining cells. (To simplify the description, researchers often work with a "wrap around" model, in which the two ends are joined, so that all cells are treated alike.) The evolution of a one-dimensional automaton is conveniently displayed in a two-dimensional format, each new row below its predecessor. (Researchers also often "colorize" their elementary systems to highlight key features.) The result can be as richly textured as a Navajo weaving.

In the early 1980s, Stephen Wolfram, then at the Institute for Advanced Study in Princeton, roughed out a classification scheme

OLIVER KNILL

Lecture 11: Cryptography

11.1. **Cryptology** is the science of constructing and breaking codes. It consist of **cryptography**, the creation of codes and **cryptanalysis**, the theory of cracking codes. Related in information theory is the construction of **error correcting codes**. The purpose of the later is the building of protocols allowing the transmission of information to be more secure. The goal is data corruption or data loss can be reversed by adding redundant information. Already the DNA, encoding the blueprints of life have redundancy built in.

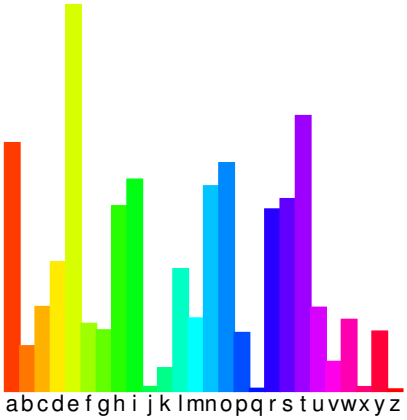
FIGURE 1. Some gadgets related to cryptology.

11.2. What kind of mathematics is involved? The theory has ties with **probability theory**. Especially in the code breaking part **statistical methods** are useful. Many codes are based on **number theory** like RSA and Diffie-Hellman. **Combinatorial** considerations come into play for example, when looking at the complexity of codes. Especially in code breaking like with plain text attacks. **Algebraic geometry** has entered through examples like **elliptic curve cryptosystems**. In general, **algebra** enters if algebraic objects like number fields are used. New branches like **quantum cryptology** use **analysis** like **Fourier theory**.

11.3. The **Caesar cipher** permutes the letters of the alphabet. We can for example replace every letter A with B, every letter B with C and so on until finally Z is replaced with A. The word "mathematics" becomes so encrypted as "nbuifnbujdt". Caesar would shift the letters by 3. The right shift just discussed was used by his Nephew Augustus. **Rot13** shifts by 13, and **Atbash cipher** reflects the alphabet, switch A with Z, B with Y etc. The last two examples are involutions: encryption is decryption. Here are examples:

Cesar:	shift three to the left	F becomes C for example
Augustus:	shift to the right	F becomes G.
Atbash:	reflect	B becomes Y and Y becomes B.
Rot13:	move to middle	A Becomes N and N becomes A.

11.4. More general ciphers are obtained by permuting the alphabet. Because of the $26! = 403291461126605635584000000 \sim 10^{27}$ permutations, it appears first that a brute force attack is not possible. But Cesar ciphers can be cracked very quickly using **statistical analysis**. If we know the frequency with which letters appear and match the frequency of a text we can figure out which letter was replaced with which.



11.5. The **Trithemius cipher** prevents this simple analysis by changing the permutation in each step. It is called a polyalphabetic substitution cipher. Instead of a simple permutation, there are many permutations. After transcoding a letter, we also change the key. Lets take a simple example. Rotate for the first letter the alphabet by 1, for the second letter, the alphabet by 2, for the third letter, the alphabet by 3 etc. The word "Mathematics" becomes now "Ncwljshbrmd". Note that the second "a" has been translated to something different than a. A frequency analysis is now more difficult. The **Viginaire cipher** adds even more complexity: instead of shifting the alphabet by 1, we can take a key like "BCNZ", then shift the first letter by 1, the second letter by 3 the third letter by 13, the fourth letter by 25 the shift the 5th letter by 1 again. While this cipher remained unbroken for long, a more sophisticated frequency analysis which involves first finding the length of the key makes the cipher breakable. With the emergence of computers, even more sophisticated versions like the German **enigma** had no chance.

Alberti	Random change of alphabet indicating switch
Trithemius	Deterministic change of alphabet
Viginere	Using key telling which alphabet to use
Enigma	Using key and deterministic alphabet change overlapped with Cesar
Hill Cipher	Use matrices to permute

11.6. Block ciphers cut text into larger chunks and scramble them. Examples are

DES	Data Encryption Standards 1973
Triple DES	Used for some electronic payments, 1998

11.7. Public key systems are based number theoretical mathematical principles like the problem of factoring integers. This has lots of relations with number theory, computer science as well as seemingly unrelated topics like algebraic geometry.

11.8. Diffie-Hellman key exchange allows Ana and Bob want to agree on a secret key over a public channel. The two palindromic friends agree on a prime number p and a base a. This information can be exchanged publicly. Ana chooses now a secret number x and sends $X = a^x$ modulo p to Bob over the channel. Bob chooses a secret number y and sends $Y = a^y$ modulo p to Ana. Ana can compute Y^x and Bob can compute X^y but both are equal to a^{xy}. This number

is their common secret. The key point is that eves dropper Eve, can not compute this number. The only information available to Eve are X and Y, as well as the base a and p. Eve knows that $X = a^x$ but can not determine x. The key difficulty in this code is the **discrete log problem**: getting x from a^x modulo p is believed to be difficult for large p.

11.9. The **Rivest-Shamir-Adleman public key system** uses a **RSA public key** (n, a) with an integer $n = pq$ and $a < (p-1)(q-1)$, where p, q are prime. Also here, n and a are public. Only the factorization of n is kept secret. Ana publishes this pair. Bob who wants to email Ana a message x, sends her $y = x^a \bmod n$. Ana, who has computed b with $ab = 1 \bmod (p-1)(q-1)$ can read the secrete email y because $y^b = x^{ab} = x^{(p-1)(q-1)} = x \bmod n$. But Eve, has no chance because the only thing Eve knows is y and (n, a). It is believed that without the **factorization** of n, it is not possible to determine x. The message has been transmitted securely.

11.10. The core difficulty is that **taking roots** in the ring $Z_n = \{0, \ldots, n-1\}$ is difficult without knowing the factorization of n. With a factorization, we can quickly take arbitrary roots. If we can take square roots, then we can also factor: assume we have a product $n = pq$ and we know how to take square roots of 1. If x solves $x^2 = 1 \bmod n$ and x is different from 1, then $x^2 - 1 = (x-1)(x+1)$ is zero modulo n. This means that p divides $(x-1)$ or $(x+1)$. To find a factor, we can take the greatest common divisor of $n, x-1$. Take $n = 77$ for example. We are given the root 34 of 1. ($34^2 = 1156$ has reminder 1 when divided by 34). The greatest common divisor of $34 - 1$ and 77 is 11 is a factor of 77. Similarly, the greatest common divisor of $34 + 1$ and 77 is 7 divides 77. Finding roots modulo a composite number and factoring the number is equally difficult.

Cipher	Used for	Difficulty	Attack
Cesar	transmitting messages	many permutations	Statistics
Viginere	transmitting messages	many permutations	Statistics
Enigma	transmitting messages	no frequency analysis	Plain text
Diffie-Helleman	agreeing on secret key	discrete log mod p	Unsafe primes
RSA	electronic commerce	factoring integers	Factoring

11.11. The simplest **error correcting scheme** just uses 3 copies of the same information. A single error can be corrected. With 3 watches for example, you know the time, even if one of the watches fails. Cockpits of airplanes have three copies important instruments. But this basic error correcting code is not efficient. It can correct single errors by tripling the size. Its efficiency is only 33 percent. A cheap way to make it more efficient is to compress the data first and then make three copies. **Data compression** is a topic by itself. Here is a simple example, the **dictionary compression**. Take dictionary with $65'536 = 2^{16}$ words for example. Every word can be encoded by two bytes. Assuming an average word length of 6, we can encode every word with 2 bytes instead of 6. There are better error correcting codes using linear algebra or algebraic geometry.

Work problems

1) We crack the Caesar cypher using statistical analysis:

Letter	Percentage	Letter	Percentage
E	11.16	M	3.01
A	8.50	H	3.00
R	7.58	G	2.47
I	7.54	B	2.07
O	7.16	F	1.81
T	6.95	Y	1.78
N	6.65	W	1.29
S	5.74	K	1.10
L	5.49	V	1.01
C	4.54	X	0.29
U	3.63	Z	0.27
D	3.38	J	0.20
P	3.17	Q	0.20

The frequency of letters is relevant for designing keyboards. The Qwerty keyboard for example has ESER and OI in prominent places.
The 'top twelve' letters help with about 80 percent of the text. You can remember the first 8 with the memonic

"A SIN TO ERR".

An other thing to look for: The **top pairs** which appear are

TH HE AN RE ER IN ON AT ND ST ES EN OF TE ED OR TI HI AS TO

The most frequent **double letters** are

"LL EE SS OO TT FF RR NN PP CC"

Example

We aim to decrypt the following text:
xf uif qfpqmf pg uif vojufe tubuft,
jo psefs up gpsn b npsf qfsgfdu vojpo,
ftubcmjti kvtujdf, jotvsf epnftujd usborvjmjuz,
qspwjef gps uif dpnnpo efgfodf,
qspnpuf uif hfofsbm xfmgbsf,
boe tfdvsf uif cmfttjoht pg mjcfsuz
up pvstfmwft boe pvs qptufsjuz,
ep psebjo boe ftubcmjti uijt dpotujuvujpo gps uif
vojufe tubuft pg bnfsjdb
Decoding:
Count the number of letters which occur. Since we have not much time, the 8 most frequent letters are listed in this text. Can you figure out the text?

f	appears	39 times
u	appears	29 times
p	appears	25 times
t	appears	20 times
s	appears	20 times
j	appears	20 times
o	appears	17 times
b	appears	14 times

2) Decrypt the following text. It belongs to a famous novel.

"ny nx f ywzym zsnajwxfqqd fhpstbqjilji, ymfy f xnslqj rfs ns utxxjxxnts tk f ltti ktwyzsj, rzxy gj ns bfsy tk f bnkj. mtbjajw qnyyqj pstbs ymj kjjqnslx tw anjbx tk xzhm f rfs rfd gj ts mnx knwxy

jsyjwnsl f sjnlmgtzwmtti, ymnx ywzym nx xt bjqq kncji ns ymj rnsix tk ymj xzwwtzsinsl kfrnqnjx, ymfy mj nx htsxnijwji ymj wnlmykzq uwtujwyd tk xtrj tsj tw tymjw tk ymjnw ifzlmyjwx.:"

3) We have seen how to encrypt messages using the Vigenère Cipher. This encryption was used for a long time and should be seen as an important marker in the development of substitution ciphers:

Julius Caesar	-70
Ahmad al-Qalqashandi	1400
Leon Battista Alberti	1467
Johannes Trithemius	1508
Blaise de Viginère	1586
Charles Babbage	1854
Friedrich Kasiski	1863
Arthur Scherbius	1920

Blaise de Vigenère was not really the inventor of the cypher.

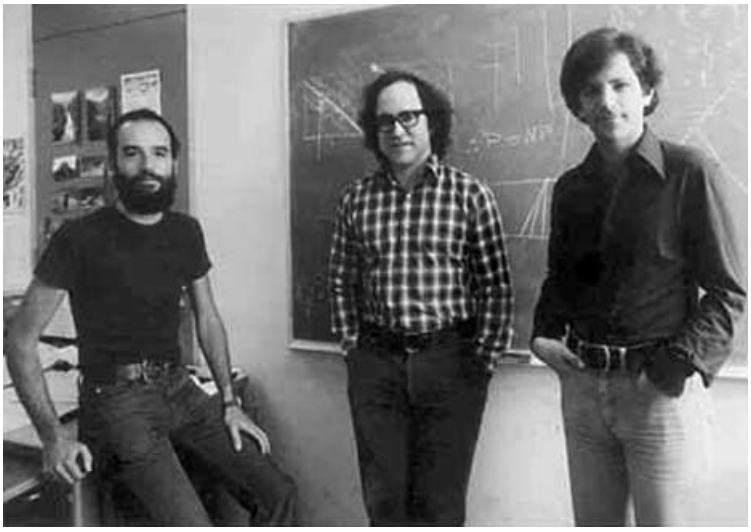
Assume we have a secret key like "ENIGMA". Given a text like "HARVARD IS COOL", we encrypt it using the following table: for the first letter, we use the line starting with E, for the second letter, we use the line starting with N etc.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Now it is your turn

HARVARD IS COOL

3) We want to understand the basic mechanism for RSA encryption.



Ron Rivest, Adi Shamir and Len Adleman.

An **RSA public key** is a pair (n, a) where n is an integer with secret factorization $n = pq$ and where $a < (p-1)(q-1)$ is such that there exists b with $ab = 1 \bmod (p-1)(q-1)$. Ana publishes this pair. If Bob wants to send a secrete message to Ana, he transmits to Ana the message

$$y = x^a \bmod n \ .$$

Ana can read the email by computing

$$y^b \bmod n \ .$$

Why does it work? We use the **Fermat's little theorem** which tells that $x^{p-1} - 1$ is is divisible by p and $x^{q-1} - 1$ is divisible by q. But this assumes p, q to be prime. For $n = pq$, we have $x^{(p-1)(q-1)} - 1$ divisible by pq.
For example take $p = 3$ and $q = 5$ Verify that $2^{(p-1)(q-1)} - 1$ is divisible by $n = pq$.

11.12. Because $y^b = x^{ab} = x \bmod n$, because $ab-1$ is divisible by $(p-1)(q-1)$ and $x^{(p-1)(q-1))} = 1 \bmod n$ we have $x^{ab} = x \bmod n$.
Ana gets the message, Bob has sent. But Eve has no chance to read it, because the only thing Eve can see is y and (n, a). It is believed that without the factorization of n, the message can not be read.

Let $(55, 13)$ be the public key of Ana. Assume Ana has the message $x = 4$ to submit. She computes $y = 4^{13} \bmod 55 = 9$. Because $55 = 11 * 5 = pq$, Ana knows $(p-1)(q-1) = 40$ and can obtain $b = 37$. With $x = 9^{37} \bmod 55$ she gets back 4.

11.13. Problem a) Assume the public key of Ana is $(n, a) = (15, 2)$. You are Bob. Send the message $x = 7$ to Ana.
Problem b) You are now Ana and have received the message from Bob. Decipher it.

Oliver Knill, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022

OLIVER KNILL

Lecture 13: Computing

13.1. **Computing** deals with algorithms and the practice of programming. While the subject intersects with computer science, information technology, the theory is by nature rather mathematical. New aspects have emerged. Computers have opened the field of **experimental mathematics** and serve now as the **laboratory** for new mathematics. Computers are not only able to **simulate** more and more of our physical world, they allow us to **explore** new worlds. They have become important parts of our **senses** and interfaces between measuring devices and sensors and our brains.

13.2. A mathematician pioneering new grounds with computer experiments does similar work than an experimental physicist. Computers have blurred the boundaries between physics and mathematics. There are some mathematicians who do much more experiments than some theoretical physicists working in domains where access to measurements are absent. According to Borwein and Bailey, experimental mathematics consists of:

Gain insight and intuition.	Explore possible new results
Find patterns and relations	Suggest approaches for proofs
Display mathematical principles	Automate lengthy hand derivations
Test and falsify conjectures	Confirm already existing proofs

13.3. Computers can also assist us in proofs. If all the source code for the computation can be inspected and all computations are done symbolically or with integers, one can verify that the proof is correct and there is no fundamental difference between a computer assisted proof or a proof done on paper. There are aspects which need to be considered however. There is a trust required in that the computer does the right thing, that the programs are correct. But this is no different with our brains. We have to trust that we do not forget things when doing a proof or that previous work is correct. The layers of trust we have in humanly produced proofs are already wide. A theorem which has been proven in many different ways is more reliable than a theorem for which the proof is thousands of pages long and been done by dozens of mathematicians.

13.4. We have seen examples in this course, where the computer has proven geometric theorems. Algebraic computations or integral computations, or solving differential equations, this all gets done swiftly with computers. When using computers to prove things, reading and verifying the computer program is part of the proof. If Goldbach's conjecture would be known to be true for all $n > 10^{18}$, the conjecture should be accepted because numerical verifications have been done until $2 \cdot 10^{18}$ until today. The first famous theorem proven with the help of a computer was the "4 color theorem" in 1976. The theorem tells that any finite simple planar graph admits a function on the nodes taking 4 values so that neighboring nodes do not have the same color.

13.5. It would be unreasonable to ask a human to manually verify the finitely many cases not covered by the theory. A mathematician would like to insist that software which is used open source. But even that would not be enough for a purist. It is possible for example that the CPU produces errors. Commercial computer algebra software without insight into the source code does not qualify because there could be bugs. Mathematics is eternal. A once established fact is true

for ever. With more openness in CPU architecture as well as insistence of open source compilers and tools one might accept computer assisted proofs more. Still, one also wants to understand "why" a result is true and hope that a proof produces "insight".

13.6. Besides assisting in experiments and proofs, also the visualization and illustration aspect is important in mathematical activities. And that is where computers shine. It is possible these days to record a lecture with various cameras, cut the material together, enhance it with multimedia like pictures, movies, graphics and so generate a **virtual reality environment** which would not be possible without the computer. This is not only valuable for pedagogical reason. A good visualization can lead to new result and a good illustration can help to increase the global understanding of the subject and to pass it on to future generations.

13.7. Here are some pointers in the history of computing. It is best done by looking at computing devices. The conceptual development of computing is much more subtle. There is dispute for example whether the Sumerian Abacus is real and should count as a computing device. Writing on clay and so moving physically matter around is the same already than counting with pebbles without having them be formally attached to a device.

2700BC	Sumerian Abacus	1935	Zuse 1 programmable	1973	Windowed OS
200BC	Chinese Abacus	1941	Zuse 3	1975	Altair 8800
150BC	Astrolabe	1943	Harvard Mark I	1976	Cray I
125BC	Antikythera	1944	Colossus	1977	Apple II
1500	Khipus	1946	ENIAC	1981	Windows I
1300	Modern Abacus	1947	Transistor	1983	IBM PC
1400	Yupana (Inkas)	1948	Curta Gear Calculator	1984	Macintosh
1600	Slide rule	1952	IBM 701	1985	Atari
1623	Schickard computer	1958	Integrated circuit	1988	Next
1642	Pascal Calculator	1969	Arpanet	1989	HTTP
1672	Leibniz multiplier	1971	Microchip	1993	Webbrowser, PDA
1801	Punch cards	1972	Email	1998	Google
1822	Difference Engine	1972	HP-35 calculator	2007	iPhone, Android
1876	Mechanical integrator	1972	first digital watch	2015	Apple watch
				2021	desktop quantum computer

13.8. We live in a time of exponentially exploding technology measures. **Moore's law** from 1965 predicted that semiconductor technology doubles in capacity and overall performance every 2 years. This has happened since. Some futurologists like Ray Kurzweil conclude from this technological singularity in which artificial intelligence might take over.

13.9. In 1937, **Alan Turing** introduced the idea of a **Turing machine**, a theoretical model of a computer which allows to quantify complexity. It has finitely many states $S = \{s_1, ..., s_n, h\}$ and works on an tape of $0-1$ sequences. The state h is the "halt" state. If it is reached, the machine stops. The machine has rules which tells what it does if it is in state s and reads a letter a. Depending on s and a, it writes 1 or 0 or moves the tape to the left or right and moves into a new state. Turing showed that anything we know to compute today can be computed with Turing machines. For any known machine, there is a polynomial p so that a computation done in k steps with that computer can be done in $p(k)$ steps on a Turing machine.

13.10. What can be computed? The Church's thesis of 1934 states that everything which can be computed can be computed with Turing machines. This almost certainly will remain a thesis as we never know whether we have understood all fundamental mechanisms of nature. It could be possible in principle that a time machine is possible allowing a computer to look ahead what happens and do so "computations" which are not possible by a Turing machine. The Church thesis is a sound assumption as it removes possibilities like unnatural phenomenons or computations done by some sort of religion, like asking a deity for help with some computation.

13.11. Similarly as in mathematics itself, there are limitations of computing. Turing's setup allowed him to enumerate all possible Turing machine and use them as input of an other machine. Denote by TM the set of all pairs (T, x), where T is a Turing machine and x is a finite input. Let $H \subset TM$ denote the set of Turing machines (T, x) which halt with the tape x as input. Turing looked at the decision problem: is there a machine which decides whether a given machine (T, x) is in H or not. An ingenious Diagonal argument of Turing shows that the answer is "no". [Proof: assume there is a machine $HALT$ which returns from the input (T, x) the output HALT(T, x) = true, if T halts with the input x and otherwise returns HALT(T, x) = false.

13.12. Turing constructs a Turing machine DIAGONAL, which does the following:
1) Read x. 2) Define Stop=HALT(x,x) 3) While Stop=True repeat Stop:=True; 4) Stop
Now, DIAGONAL is either in H or not. If DIAGONAL is in H, then the variable Stop is true which means that the machine DIAGONAL runs for ever and DIAGONAL is not in H. But if DIAGONAL is not in H, then the variable Stop is false which means that the loop 3) is never entered and the machine stops. The machine is in H.]
Lets go back to the problem of distinguishing "easy" and "hard" problems: One calls **P** the class of decision problems that are solvable in polynomial time and **NP** the class of decision problems which can efficiently be tested if the solution is given. These categories do not depend on the computing model used.

13.13. An important aspect of computing is the question how to decide whether a computation is "easy" or "hard". The question "N=NP?" is the most important open problem in theoretical computer science. It is one of the seven **millenium problems** and it is widely believed that $P \neq NP$.

13.14. If a mathematical task is such that every other NP problem can be reduced to it, it is called **NP-complete**. Popular games like **Minesweeper** or **Tetris** are known to be NP-complete. If it were true that $P \neq NP$ (which is what most computer scientists believe to be the case), then there are no efficient algorithm to beat the game. An example of a rather accessible NP-complete problem is the task to find the largest complete subgraph in a finite simple graph. While for many classes of graphs like networks triangulating a surface this is not a big deal, in general, this is computationally hard.

13.15. An other example of an NP-complete problem is the **balanced number partitioning problem**: given n positive integers, divide them into two subsets A, B, so that the sum in A and the sum in B are as close as possible. A first shot: chose the largest remaining number and distribute it to alternatively to the two sets.

13.16. We all feel that it is harder to **find a solution to a problem** rather than to **verify a solution**. If $N \neq NP$ there are one way functions, functions which are easy to compute but hard to verify.
For some important problems, we do not even know whether they are in NP. Here are two examples: 1) **the integer factoring problem**: given n find the factors 2) **the merit factor problem**: minimize $\sum_{k=-n}^{n} c_k^2$, where $c_k = \sum_{j=0}^{n-k} a_j a_{j+k}$ An efficient algorithm for the first one would have enormous consequences for our modern lives. Watch the intellectual thriller movie "Traveling Salesman (2012)" to appreciate this.

13.17. Finally, lets look at some mathematical problems in artificial intelligence AI:

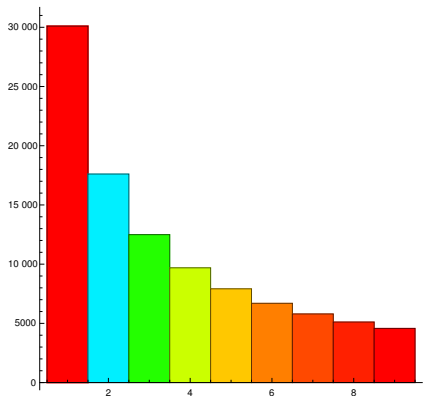
problem solving	playing games like chess, performing algorithms, solving puzzles
pattern matching	speech, music, image, face, handwriting, plagiarism detection, spam
reconstruction	tomography, city reconstruction, body scanning
research	computer assisted proofs, discovering theorems, verifying proofs
data mining	knowledge acquisition, knowledge organization, learning
translation	language translation, porting applications to programming languages
creativity	writing poems, jokes, novels, music pieces, painting, sculpture
simulation	physics engines, evolution of bots, game development, aircraft design
inverse problems	earth quake location, oil depository, tomography
prediction	weather prediction, climate change, warming, epidemics, supplies

We had started with basic human activities defining mathematical fields, we end the course with mathematical activities defining some aspects of computing. Our journey through math is over.

Work problems

13.18. 1) Experimental mathematics uses a method used a lot in other natural sciences sciences: we experiment! This can happen on paper, but also with the help of a computer. We will look at examples illustrating this. with **Benford's law** which deals with the statistics of the first significant digit in data. Simon Newcomb found the law in 1881 and Frank Benford made significant progress on it in 1938. Here is an example where one can prove things. Look at the first digits of the sequence 2^n. One can prove that the digit k appears with probability $p_k = \log_{10}(1 + 1/k)$. The digit 1 for example occurs with about $\log_{10}(2) = 0.30$ which is 30 percent. Lets experiment and look at 2^n for $n = 1$ to $n = 100'000$ and determine the first digit:

```
data = Table[First[IntegerDigits[2^n]], {n, 1, 100000}];
S = Histogram[data, 10, ColorFunction -> Hue]
```



13.19. How does one compute the probability? If we look at the logarithms, then $\log(2^n) = n\log(2)$. The first digit is 1 if the rest of $[n\log(2)]$ modulo 1 is between 0 and $\log(2)$. The first digit is 2 if it is between $\log(2)$ and $\log(3)$ etc. The probability that the letter is k is $\log_{10}(k+1) - \log_{10}(k)$.

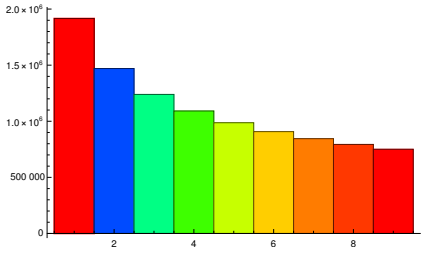
13.20. One can look at the first significant digit problem on other sequences like squares $1, 4, 9, 1, 2, 3, 4, 6, 8,$ Here is an experiment:

```
data = Table[First[IntegerDigits[n^2]], {n, 1, 10000000}];
S = Histogram[data, 10, ColorFunction -> Hue]
```

It is interesting because we want to see what the distribution of $2\log(n)$ is modulo 1. It looks as if we have a similar Benford law here. Indeed it is a generalized Benford law with $p_k = \frac{\int_k^{k+1} x^{-\alpha}\, dx}{\int_1^{10} x^{-\alpha}\, dx} =$

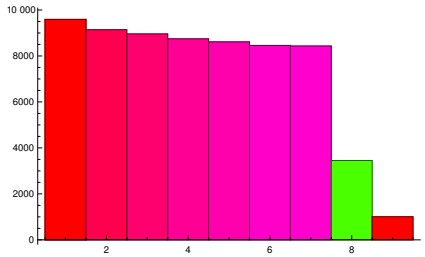
$[(k+1)^{1-\alpha}-k^{1-\alpha}]/(10^{1-\alpha}-1)$. It interpolates the Benford law $\alpha = 1$ with the uniform distribution $\alpha = 0$.

We have the digit 1, if $\log(n) \in k + [0, \log(2)]$. How many cases are in 1000 and 2000. It is $\sqrt{2000}-\sqrt{1000} = \sqrt{1000}(\sqrt{2}-1)$. How many cases are in 2000 and 3000. It is $\sqrt{3000}-\sqrt{2000} = \sqrt{1000}(\sqrt{3}-\sqrt{2})$.



a) Experiment to find the What is the first significant digit of the prime numbers?

```
data = Table[First[IntegerDigits[Prime[n]]], {n, 1, 664000}];
S = Histogram[data, 10, ColorFunction -> Hue]
```



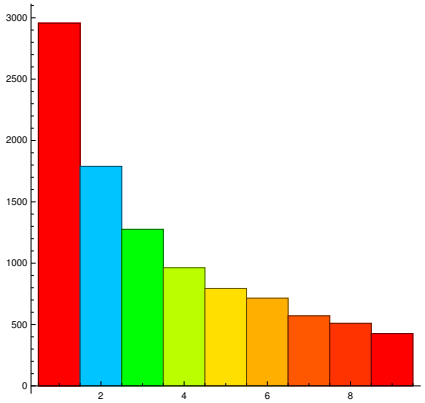
How many primes are there in 1000 and 2000. We expect $1000/Log[1000]$ primes in there and $1000/Log[2000]$ with first significant digit 2.

S1=ListPlot[Table[PrimePi[k],k,10000]]; S2=ListPlot[Table[k/Log[k],k,10000]]; Show[S1,S2]

We expect the distribution to be $a/\log(k)$, where $a = \sum 1/\log(k)$.

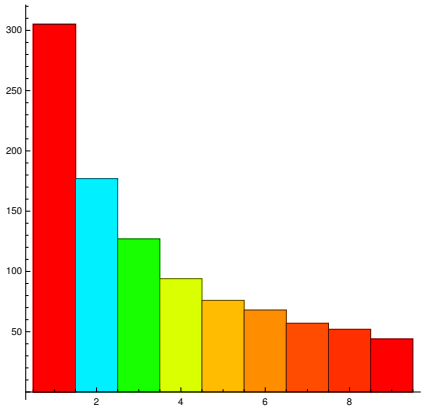
For factorials, the limiting distribution is known to be the Benford distribution. There is no reason why $\log_{10}(n!) mod 1$ should not be uniformly distributed.

```
data = Table[First[IntegerDigits[n!]], {n, 1, 10000}];
S = Histogram[data, 10, ColorFunction -> Hue]
```



b) Also for the partition numbers, $p(n)$, which give the number of possibilities in which the number n can be written as a sum of integers, we measure that the Benford distribution takes place. As far as we know this is not known.

```
data = Table[First[IntegerDigits[PartitionsP[n]]], {n, 1, 10000}];
S = Histogram[data, 10, ColorFunction -> Hue]
```



2) We look at an other problems where computers could play a role for the solution. Usually, in the case a counter example exists.
Goldbach's conjecture tells that every even number larger than 2 is the sum of two primes. While it is unlikely that a computer search will find a counter example, it might be that computer search finds the solution to the problem. How? Here is a complex analytic approach which is a caricature of much more sophisticated methods developed since 90 years. Search for function $f(x) = \sum_p a_n x^p$ with a_p positive so that f can be written in terms of functions for which integration theory works well (trig functions, exponentials, polynomials, hypergeometric functions etc). Then check (theoretically) that the Taylor coefficients of $f(x)^2$ are positive. One can do that by integration in the complex plane. This approach is a long shot since it is unlikely that a closed form for $f(x)$ can be found which works. More likely is that one can approximate things well enough to push the threshold higher above which counter examples must appear. The task is now to find coefficents a_n such that $f(x)$ is an explicit function we can compute with.
3) **Euler cuboid** It is not known whether there exists a cuboid with integer side length such that all face diagonals are integers and additionally, also the large diagonal is an integer. Computer searches have found nothing. One can search on parametrized families of Euler cubes but the **perfect Euler cuboid** - if it exists - could be so large that no computer could find it by brute force search. There are ways to explore large Euler cuboids. One is to look for families of Euler cuboids and in this space of Euler cuboids use linear analysis to predict large parameters for which we are close to **perfect cuboids**. Maybe such an approach could lead to an example. By a lucky punch. It is however still also possible that there are no perfect Euler cuboid.
4) **The Riemann hypothesis** is a prototype problem, where experiments led to more and more support that the Riemann hypothesis is true. One approach looks numerically for roots of the Riemann zeta function on the critical line. One approach is called the **Merten's approach**. Define the **Möbius function** $\mu(n) = 1$ if n is the product of an even number of different primes and -1 if n is the product of an odd number of different primes. In all other cases, that is if n has a square factor larger than 1, we have $\mu(n) = 0$. Is μ sufficiently random so that $S_n = \sum_{k=1}^n \mu(k)$ grows like the iterated law of logarithm? While it looks as if the $\mu(n)$ behave like a random sequence, there are some correlations.
5) **Billiards** One does not know whether there are triangular billiards without periodic points. One also does not know whether there are smooth convex billiards besides the ellipse for which one has **integrability** in the sense that all points are either periodic, asymptotic to a periodic point or almost periodic in the sense that the dynamics is equivalent to a translation on a finite or infinite dimensional torus. Integrability implies that one can compute the future orbit arbitrarily well without running into the sensitive dependence on initial condition problems.
5) **Standard map**. Verify that for $c > 2$ and all n $\frac{1}{n}\int_0^1 \int_0^1 \log|\partial_x f_n(x,y)|\ dxdy \geq \log(\frac{c}{2})$. I myself have tried over a decade to prove this using methods from quantum mechanics, calculus of variations and complex analytic methods. The problem is open. The left hand side converges to the average of the Lyapunov exponents which is in this case also the **entropy** of the map.

6) **prime twins**. This is a problem, which can first of all be investigated statistically. Similarly as Gauss looked numerically for a law describing the frequency of the prime numbers, one can first see, hoe many prime twins one has to expect in a certain interval and then see whether this expectation is confirmed. Furthermore one can look whether there are any patterns on arithmetic subsequences. Maybe there are some unexpected sequences along which there are more prime twins. Related to the twine prims problem is the problem to estimate the minimal distance between two Gaussian primes in the complex plane.

7) **Normality of π. This is an example where one can have fun with statistics. Are there any statistical tests which indicate that the digits of π are not normal? The decimal digits of π appear random enough so that every digit appears with the same frequency.**

8) Odd perfect numbers. While a brute force search is unlikely, there are other approaches which are more likely to find an odd perfect number. Any perfect number satisfies $\sigma(n)/n = 2$, where $\sigma(n)$ is the sum of all the divisors of n including n. Take a large set $B = \{p_1, ..., p_s\}$ of primes. For every $k = (k_1, ..., k_s)$, form the number $n = p_1^{k_1} p_2^{k_2} ... p_s^{k_l}$. We have $\sigma(p^k) = (1+p+p^2+...p^k)/p^k = (p-p^{-k})/(p-1)$. Let $a(p,k) = \log(\sigma(p^k))$. The goal is to find $(k_1, ..., k_s)$ such that

$$\log(a(p_1, k_1)) + ... + \log(a(p_l, k_l)) - k_1 \log(p_1) - ...k_s \log(p_s) = \log(2) \ .$$

The idea is to keep first the primes and change only the "dials" k_j in a controlled way. Certain dial changes will produce a very small net change of the left hand side. For large primes and large n the first order change will dominate and methods from Diophantine geometry could be used and linear algebra to get close to the right hand side. If lucky (provided of course there is an odd perfect number), one could hit it like this. If we would take 1000 primes each 1000 digits long and deal with exponents of the order of 1000, we would investigate numbers with billions of digits.

9) Turing machines. We see a concrete Turing machine and evolve it a few steps to see what it does. The machine is initially in state $\boxed{1}$ and starts with an empty tape.

	-3	-2	-1	0	1	2	3	···
···	0	0	0	0	0	0	0	···

Here is the definition of a machine with three states:

Input 0

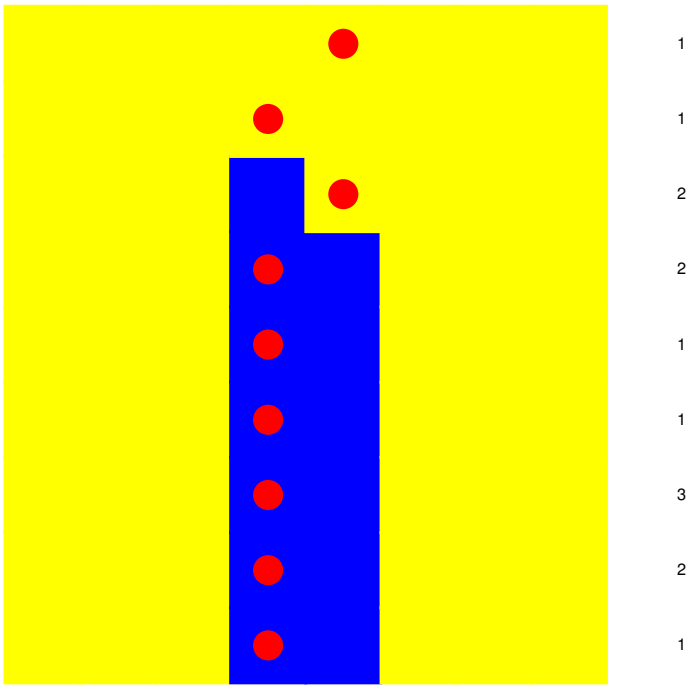
State	New state	Write	move to
1	2	0	left
2	3	1	right
3	1	1	left

Input 1

State	New state	Write	move to
1	2	1	left
2	1	0	right
3	3	0	right

a) We run this machine a few steps and mark the number, where the machine reads the tape. This place will move with time.

	-3	-2	-1	0	1	2	3	···	State=1
···	0	0	0	0	0	0	0	···	State=1
···	0	0	0	0	0	0	0	···	State=2
···	0	0	0	0	0	0	0	···	State=3
···	0	0	0	0	0	0	0	···	State=1
···	0	0	0	0	0	0	0	···	State=1



b) Here is the definition of a new machine with three states:

Input 0

State	New state	Write	move to
1	2	1	right
2	3	1	right
3	3	0	left

Input 1

State	New state	Write	move to
1	2	1	left
2	1	0	right
3	3	0	left

c) Run it!

···	0	0	0	0	0	0	0	···	State=1
···								···	State=
···								···	State=
···								···	State=

10) The following problem is known to be NP-complete. This means that if it could be solved in polynomial time, then all NP problems would be polynomial and P=NP. In other words, if you can design a method, which solves the problem in a manner which is polynomial in n, you win a Million dollars and you would have solved the most important problem in computer science.

Given n positive integers $a_1, \ldots, a_n$, divide them up into two subsets, so that the sum of these numbers in one set and the sum of numbers in the other set are as close together as possible.

For example, let

$$A = \{2, 3, 5, 7, 11, 13, 17\} .$$

We can apply the "cruel school selection" algorithm: the largest two elements are the team leaders of a team, who alternatively select the best remaining candidate. What do you get?

a. Can you do better than that? How well can you divide up the numbers better?

11) One does not know how to factor integers of 200 digits efficiently. Can we find some factors fast?

b) There is a simple method to decide whether a number is divisible by 9. What is it? For example: is

$$121212121212121212$$

divisible by 9?

c) There is a simple method to decide whether a number is divisible by 11. What is it? 4) For example is

$$1212121212121212121212$$

divisible by 11?

d) Which factors can be detected by looking at the last decimal digit of a number only?

e) The 1,-3,2 method for divisibility by 7 is to split the number into groups of 6, then multiply in each group the three pairs by 1,-3,2, then add up all results. For example $11111111111114 = (000011)(111111)(111114)$ leads to $2 * 11 + 1 * 11 - 3 * 11 + 2 * 11 + 1 * 11 - 3 * 11 + 2 * 14 = 28$ which is divisible by 7.

Is

$$111111111111111111111111111111111111111111111111$$

divisible by 7 (48 digits of 1).

Oliver Knill, knill@math.harvard.edu Math E-320, Harvard Extension School, 2010-2022