CO380: History of Mathematics
Spring 2017
Lecture 8/9

Alain Gamache
agamache@uwaterloo.ca
Phone ext: 38041

May 29, 2017

The Problem

"On raconte que, dans le grand temple de Bénarès, au-dessous du dôme qui marque le centre du monde, on voit plantées dans une dalle d'airain trois aiguilles de diamant hautes d'une coudée et grosses comme le corps d'une abeille. Sur une de ces aiguilles, Dieu enfila au commencement des siècles 64 disques d'or pur, le plus large reposant sur l'airain, et les autres, de plus en plus étroits superposés jusqu'au sommet. C'est la tour de Brahma. Nuit et jour, les prêtres se succèdent, occupés à transporter la tour de la première aiguille de diamant sur la troisième sans écarter des règles fixes et immuables imposées par Brahma. Le prêtre ne peut déplacer qu'un seul disque à la fois; il ne peut poser ce disque que sur une aiguille libre ou au-dessus d'un disque plus grand. Lorsque'en suivant strictement ces reccomandations, les 64 disques auront été transportés de l'aiguille où Dieu les a placés sur la troisième. la tour et les brahmes tomberont en pussière et ce sera la fin du monde."

The Problem

"In the great temple of Benares, beneath the dome which marks the centre of the world, rests a brass plate in which there are fixed three diamond needles, each a cubit high and as thick as the body of a bee. On one of these needles, at the creation, God placed 64 discs of pure gold, the largest disc resting on the brass plate, and the others getting smaller and smaller up to the top one. This is the Tower of Bramah. Day and night unceasingly the priests transfer the discs from one diamond needle to another according to the fixed and immutable laws of Bramah, which require that the priest on duty must not move more than one disc at a time and that he must place this disc on a needle so that there is no smaller disc below it. When the 64 discs have been thus transferred from the needle on which at the creation God placed them to one of the other needles, tower, temple, and Brahmins alike will crumble into dust, and with a thunderclap the world will vanish."

Today

Édouard Lucas and The Tower of Hanoi

- The Place: France in the Second Half of the Nineteenth Century
- The Person: Édouard Lucas
- The Problem : Primality Testing from The Tower of Hanoi to the Mersenne Primes

The Place

France in the Second Half of the Nineteeth Century

- The Political Turmoils
- The French Academics

France in the Second Half of the Nineteenth Century

The Political Turmoils

From 1830 to 1914, France will undergo several political periods: the July Monarchy, the Second Republic, the Second Empire and finally the Third Republic. Each of these different regimes ended by a violent event: the French Revolution of 1848, the French coup of 1851, the defeat in the French-Prussian War of 1870 and finally the Paris Commune.

France in the Second Half of the Nineteenth Century

The Political Turmoils

- The Second Republic (1848-1852)
- The Second Empire (1852-1870)
- The End of the Second Empire and the Beginning of the Third Republic (1871-1914)

France in the Second Half of the Nineteenth Century

The Second Republic (1848-1852): The Uprising

- Followed the July Monarchy which saw the last French monarchy fall in 1848.
- The king at the time : King Louis-Phillipe, also named the *The Citizen King*.
- A refusal by the government at the time to meet with representatives of the working class led to an uprise in the streets that caused a full-blown revolution and forced King Louis-Phillipe into exile in England.
- Instability ensues.

France in the Second Half of the Nineteenth Century

The Second Republic (1848-1852): The calm... before the storm

- Louis-Napoléon Bonaparte (Napoleon III), nephew of Napoleon I, took the role of head of the state.
- The first years of the Second Empire were relatively positive and witnessed change in favour of the population:
  - abolition of slavery
  - reinstitution of universal suffrage
  - introduction of new social programs
  - improvement in the freedom of speech for the press
- Legislation returns to a more conservative and Napoleon III organized a coup which leads to the dissolution of the Legislative.

France in the Second Half of the Nineteeth Century

The Second Empire (1852-1870): The Growth

- Napoleon III is at the helm of the Second Empire.
- Authoritarian, the government of Napoleon III established a line of conduct that disallowed for any type of misconduct
- This very strict approach allowed France to focus on its economic development and growth (ex: expansion of railroads).
- Paris is the focus of Napoleon III
- Napoleon III, trying to battle his loss in popularity, started loosening his tight grip on France.
  - more liberal approach
  - commercial treaty with Great Britain (seen as a vulnerability by both republicans and monarchists)

France in the Second Half of the Nineteeth Century

The Second Empire (1852-1870): The War and...more War

- Napoleon III has an obsessive desire to extend the Empire as his uncle, Napoleon I, had done before him.
- Allied France with the United Kingdom and the Ottoman Empire to declare war on Russia in the Crimea War of 1854-1856. War that is quickly won.
- France becomes a power in Europe, Developed colonies in Africa and in Asia.
- Napoleon III foreign policies are weak.
- Protests and insults toward the Prussian Empire left him with little support.
- Left with few options, he declared war on Prussia on July 19th 1870.

France in the Second Half of the Nineteeth Century

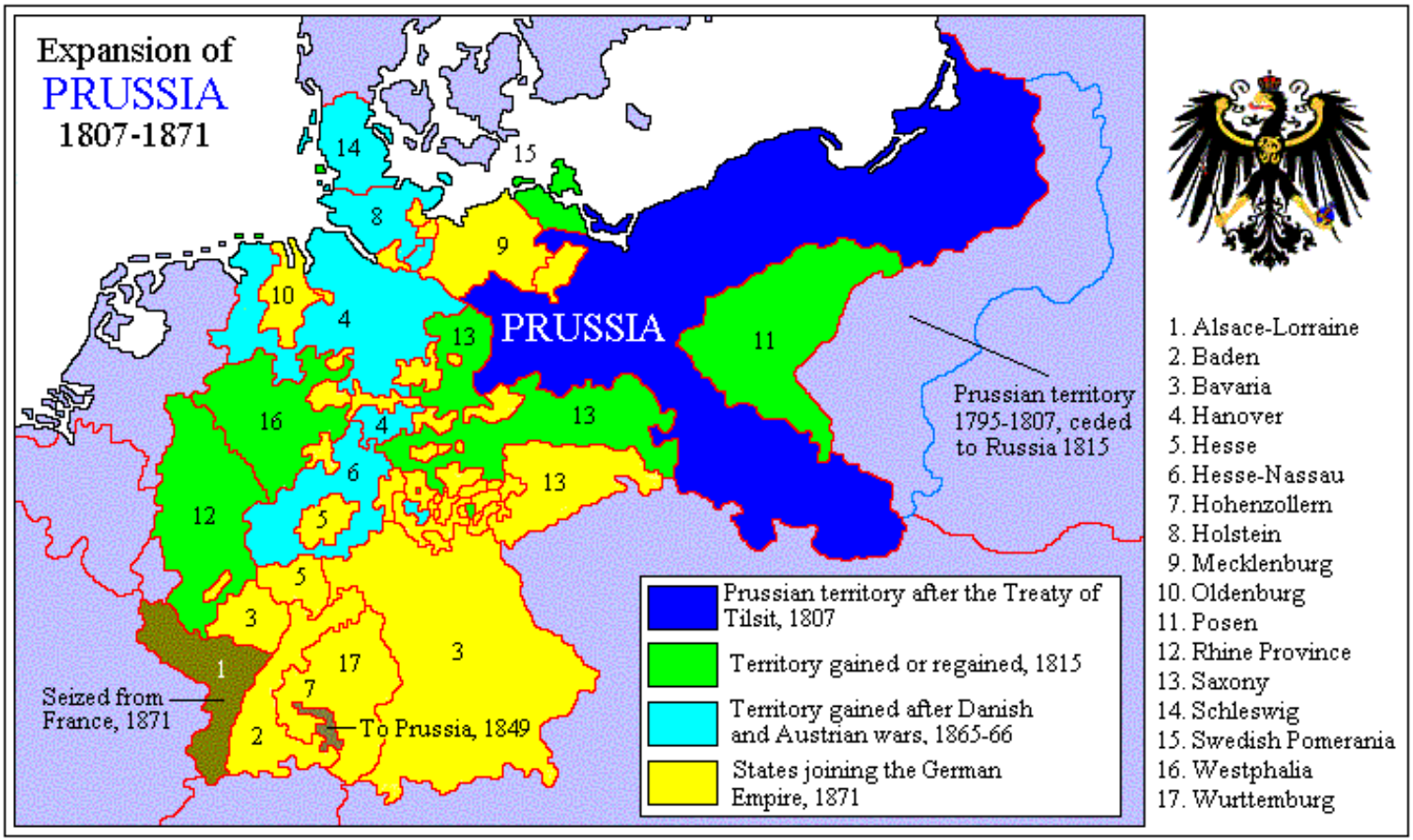


Figure: The Empire of Prussia: Wikipedia

France in the Second Half of the Nineteeth Century

The End of the Second Empire and the Beginning of the Third Republic: The Franco-Prussia war

- The Franco-Prussian war was a disaster for the French.
- The French were ill-prepared, devoid of allies and fell quickly.
- The French lost Alsace and their Emperor would became a prisoner of the Prussian army by September 2nd in Sedan.
- Finally, Paris fell after a long siege in January.

France in the Second Half of the Nineteenth Century

The End of the Second Empire and the Beginning of the Third Republic: The Aftermath

- Following the defeat, the Third Republic, with Adolphe Thiers at its head, was created by a vote at the French National Assembly in March 1871.
- While maintaining peace with the Prussian Empire, the new government created a new enemy from within.
- The Paris Commune was elected in Paris and opposed the new government whom they considered too conservative.
- The opposition became violent when Thiers ordered the removal of the cannons present across Paris.
- The Paris Commune considered that action as a way of rendering the population defenseless.

France in the Second Half of the Nineteenth Century

The End of the Second Empire and the Beginning of the Third Republic: Yet another conflict

- The French army and the Paris Commune clashed for a week in May, named The Bloody Week, which left almost thirty thousand casualties.
- The Paris Commune was defeated on May 28th and from there the Third Republic ruled until the start of WWI.

France in the Second Half of the Nineteenth Century

The French Academics

- The Imperial Lycée during the Second Empire
- L'École Normale Supérieure (E.N.S.)
- The Scientific Research in France

France in the Second Half of the Nineteenth Century

The French Academics: The Imperial Lycée during the Second Empire

- Science teaching was a problem.
- The lack of equipment and professors willing to invest time into research and teaching were the primary reasons for this tendancy of the French education system to abandon sciences.
- Instauration of reforms that transformed the teaching sequences of the mathematics and latin courses taught (sciences return to the former currcula) and that create a branching system.
- It was difficult to attract a stable clientele, as students mostly chose the language study path where little science was taught.
- As a result, the students were inadequately prepared for continued studies at the École Polytechnique (doctors and engineers)

France in the Second Half of the Nineteeth Century

The French Academics: L'École Normale Supérieure (E.N.S.)

- The E.N.S. resulted from the first imperial regime under Napoleon I.
- By the beginning of the second half of the nineteenth century, the E.N.S. was an institution where professors did not offer in-depth schooling that allowed major advancements in science.
- In 1857, Louis Pasteur was appointed as administrator in charge of directing studies at the E.N.S.
- Pasteur's intervention aimed to raise the quality of education in science and to increase student population at the E.N.S.
- Soon after his involvement, students registered for doctoral studies; His intervention prevailed.

France in the Second Half of the Nineteenth Century

The French Academics: The Scientific Research in France

- Despite Pasteur's efforts, scientific progress in France was slow and quickly fell far behind that of its two main rivals: England and Germany.
- The latter of these countries enjoyed a rich, decentralized life compared to France, where the greater majority of its activities took place in Paris.
- France was content during this time with scientific research based on discovery.
- The Imperial government only granted them minimal attention.

France in the Second Half of the Nineteenth Century

The French Academics: Scientific Research in France - The Awakening

- The defeat during the Franco-Prussian war awoke the French authorities.
- The French armies losses were due not only to the war but also to the propagation of smallpox, for which the Prussian had a vaccine but the French did not.
- This showed the scientific superiority of Germany over France.

France in the Second Half of the Nineteenth Century

The French Academics: Scientific Research in France - Catching-up

- The post-war years marked an intense catching-up period through methods such as translating foreign works.
- Finally, when the Third Republic was well implemented, Pasteur's efforts in refurbishing science facilities and giving more credibility enabled results.
- The E.N.S., whose principal mandate was to produce professors for the French lycées, celebrated numerous young, brilliant scientists who developed innovative theses and reputed chairs in Parisian universities.
- This increase in knowledge from the ENS provoked a competition with the École Polytechnique, which improved the quality of its education as a result.

The Person

Édouard Lucas

- His Education
- The "Observatoire de Paris" Episode
- Lucas' Return to Normal Life
- Lucas' Teaching
- Lucas' Work

The Person

Figure: Édouard Lucas

Édouard Lucas

His Education- The Early Years

- François-Édouard Anatole Lucas, the oldest in a family of eight children, was born in Amiens in 1842.
- His primary studies took place in a school run by monks.
- He then registered at the Imperial lycée in Amiens to follow his secondary studies at a time another reform was taking place in the Imperial education system. Allow him to take a large selection of science courses.
- High academic achievement in both language and science won him a full scholarship which allowed him to pursue his studies.
- His skills in mathematics and sciences were underlined and he was given the opportunity to write the entrance test to the E.N.S. despite being too young; he was 16 at the time.
- He was accepted at both the École Polytechnique and the E.N.S.

Édouard Lucas

His Education

- For Lucas, the choice of program is obvious; his attraction towards science and the pressure Pasteur used to rebuild the scientific department at the E.N.S. were sufficient in convincing him to pursue his studies in science.
- His mathematics courses were offered, among others, by Joseph Bertrand and Charles Hermite, two eminent French figures in mathematics at the time.
- The nomination of these two professors was a direct link with Pasteur's initiative to rebuild the E.N.S.'s coat of arms.
- In his third year, Lucas moved on, concentrating solely on physics and mathematics.

Édouard Lucas

The "Observatoire de Paris" Episode

- With Pasteur's help in his efforts to bring France back to the forefront of European science, Lucas is granted a position as joint astronomer in 1864.
- The observatory was, at the time, under the direction of Urbain Le Verrier, and under his command, the past decade had been tense and led to several astronomers leaving the observatory.
- Two years after joining the observatory, Lucas also confronted the authority of Le Verrier, who refused him a holiday as long as he did not finish the computations correction for the current year's observations (computation instruments were not acceptable at the observatory)
- Lucas used a doctor's note justifying his actions and decided to disobey and leave the observatory to return to Amiens.

Édouard Lucas

The "Observatoire de Paris" Episode

- Le Verrier tried to discredit Lucas' work in the eyes of the "Ministre de l'instruction publique" and tried to get him fired.
- Pasteur led an aggressive intervention where, trying to defend his former student, he pointed out the rigidity of the observatory's director and his incapability to work with young astronomers.
- Le Verrier continued to find fault in Lucas and to try to force him to leave his position.
- The battle between Lucas and Le Verrier, moderated by different political figures, lasted until 1869, the year in which Lucas returned to teaching while receiving financial aid from the government.
- Le Verrier was dismissed in 1870 after an investigation during which most of the observatory's astronomers resigned and signed a bill describing Le Verrier's behaviour.

Édouard Lucas

Lucas' Return to Normal Life

- Before Lucas obtained any teaching position, the French declared war on the Prussian so Lucas' next destination was the front, where he briefly participated in the war as a volunteer.
- The problem: "find a way to stack a square of cannonballs laid out on the ground into a square pyramid" was imagined by Lucas during his time served at the front.
- Incapable of finding a job as a teacher in a lycée, he moved to Moulins.
- Before the end of his stay at Moulins, Lucas submitted two papers on number theory.
- Unfortunately, neither of his theses were sustained, despite positive critiques.

The Cannonballs Problem

The Cannonballs Problem

Solve the following Diophantone Equation:

$$\frac{1}{6}k(k+1)(1+2k) = n^2$$

where k is the height of the pyramid.

Édouard Lucas

The Cannonballs Problem

The Cannonballs Problem

Solution : $k = 24, n = 70$

Édouard Lucas

Lucas' Teaching

- In 1876, Lucas obtained a position at the Charlemagne Lycée, where he taught for three years.
- He was recognized as a good teacher who used original methods that allowed the best students to blossom but left behind the students who experienced difficulties. Based on recognition, Lucas got a position at a school of higher importance: Lycée Saint-Louis.
- Balancing his teaching and research was probably his biggest challenge.

Édouard Lucas

Lucas' Teaching

- These conciliation problems caused the minister to send Lucas back to the Charlemagne Lycée where he would still participate in numerous mathematics associations.
- During a banquet with one of these associations, in 1891, Lucas suffered a cut to the cheek from a piece of a broken dish. The injury did not heal and Lucas died of blood poisoning a few days later, at the age of 49.

Édouard Lucas

Lucas' Work

- Lucas was a prolific mathematician (184 published works)
- Concept of proofs was a recurring problem in Lucas' work
- Lucas' first thesis was written about textile geometry. It is during this work that he produced a new definition on the law of quadratic reciprocity, in 1890.
- The second of Lucas' important works was his first tome of *Théorie des nombres*.
  - His themes, inspired by a vast array of works, including Gauss' *Disquisitiones arithmeticae* and Tchebychev's *Théorie des congruences*.
  - Three major elements were explored: integers, rational numbers and divisibility.
  - Second volume that discussed divisibility and algebraic irreductibility, binomial congruences and primitive roots was not published.

Édouard Lucas

Lucas' Work - *Sur la théorie des fonctions simplement périodiques*

- Studied the properties of recurrent sequences such as the Fibonacci sequence.
- He generalized them and obtained what we now call Lucas' functions.
  - It was on these functions that he based the majority of the primality tests that were first elaborated around the Fibonacci sequence before being generalized to all prime numbers of the form $2^n - 1$.

Édouard Lucas

Lucas' Work - *Les Récréations Mathématiques*

- Collection of problems and puzzles showed a less academic side of Lucas.
  - The cannonball pyramid
  - The Tower of Hanoi
  - Dots and Boxes

The Problem

Primality Testing: from The Tower of Hanoi to the Mersenne Primes

- The Tower of Hanoi
- Lucas Functions
- Prime Numbers $2^n - 1$
- Lucas and the Mersenne Primes
- Return to the Tower of Hanoi

Primality Testing: from The Tower of Hanoi to the Mersenne Primes

The Tower of Hanoi

- The history behind this puzzle is not always clear.
- One of the first editions was presented by Professor N. Claus (de Siam) of the Collège Li-Sou-Stian in 1883, an anagram for Professor Édouard LUCAS (D'AMIENS).
- Rules of the game: The game consists of demolishing the tower level by level, and reconstructing it in a neighboring place, conforming to the rules given:
  1. At each turn, we can only move one disc located at the top of one pile.
  2. We can place a disc on an empty needle without restriction.
  3. We can only move a disc on top of another disc that is bigger than the disc moved.

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

The States in TH

The TH can be divided into two categories of presentation: regular state and irregular state. In a regular state, the discs are always placed following the rules given. Moreover, the regular state can be divided in two: the perfect regular state, when all the discs are placed on one peg, and the non-perfect regular state. In the irregular state, a bigger disc can be placed on top of a smaller disc which breaks the Divine Rule).

- In a regular state, the discs are always placed following the rules given.
  - Perfect regular state : all the discs are placed on one peg
  - Non-perfect regular state
- In the irregular state, a bigger disc can be placed on top of a smaller disc which breaks the Divine Rule).

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

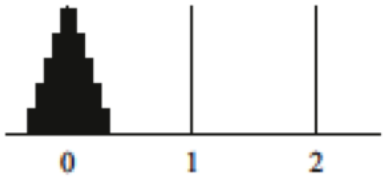


Figure: Regular perfect state

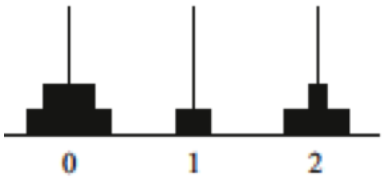


Figure: Regular non-perfect state

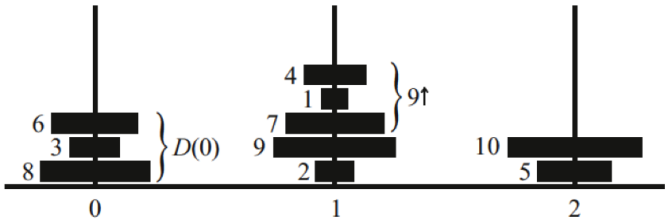
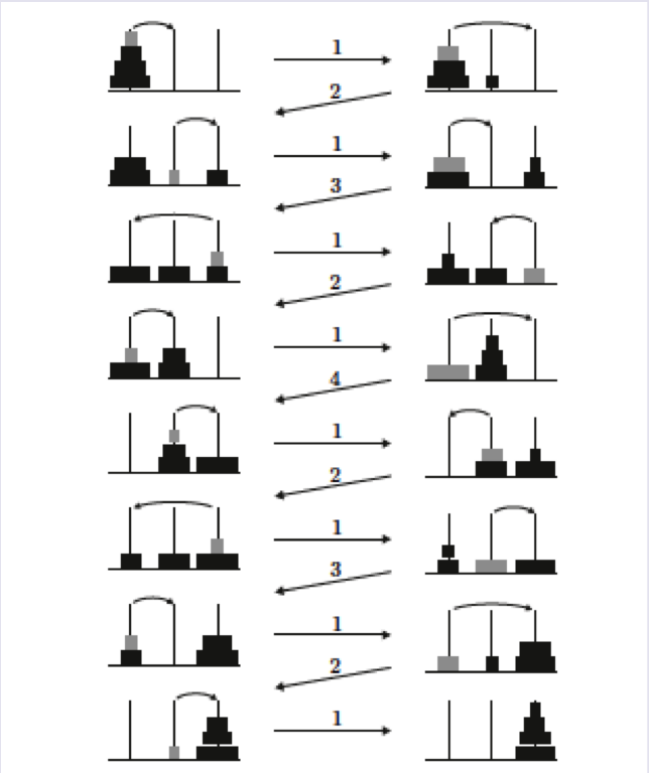


Figure: Irregular state

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

Solution of the Four-Disc TH

Solving TH for 4 discs is relatively easy and straightforward when you see the recursion existing in it.



Representing Tower of Hanoi and the Recursive Nature of the Puzzle

The Hanoi Graph

The Hanoi Graph, noted H_k^n where k represents the number of pegs and n the number of discs. In that graph, two vertices are connected if you can, by a legal move, go from one state to the other. The labeling at each vertex is done using n spaces (which represents the number of discs) and in each space you can use numbers from 0 to $k-1$; the labeling of peg starts at 0. To clarify this, here are a few examples using H_3^4:

- Vertex (0000): All discs on peg 0.
- Vertex (0021): Disc 1 is on peg 1, disc 2 is on peg 2, and discs 3 and 4 are on peg 0.
- Vertex (1202): Disc 1 on peg 2, disc 2 on peg 0, disc 3 on peg 2 and disc 4 on peg 1.

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

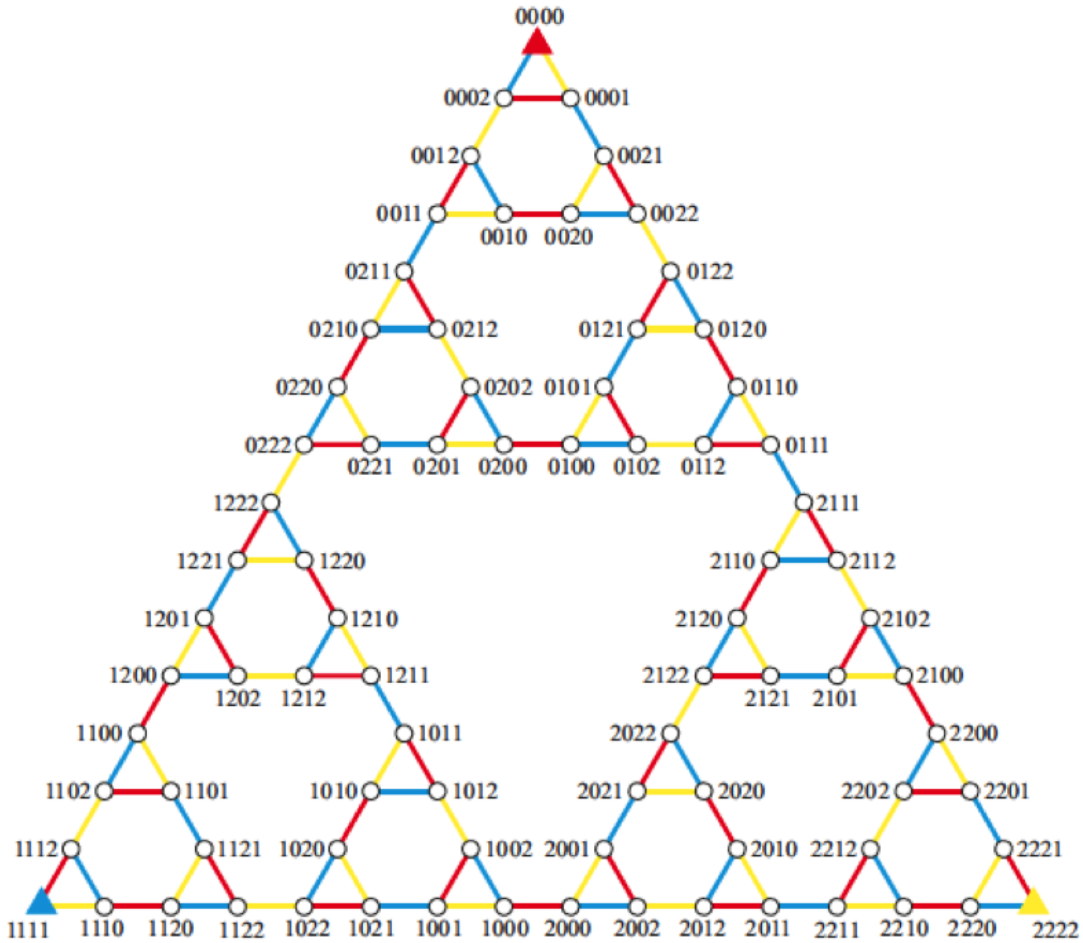


Figure: The graph H_4^3

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

Optimizing the Solution

The recursive solution $T_n = 2T_{n-1} + 1$ is not satisfactory when one wants to know how many moves the poor monk in the Temple de Bénarès needed to accomplish in order to move the 64 golden discs.

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

Optimizing the Solution

The recursive solution $T_n = 2T_{n-1} + 1$ is not satisfactory when one wants to know how many moves the poor monk in the Temple de Bénarès needed to accomplish in order to move the 64 golden discs.

Theorem

The shortest solution to the Tower of Hanoi with n discs and 3 pegs from one perfect state to another perfect state is $2^n - 1$

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

Proof

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

Proof

So the number of moves for a tower with 64 discs is $2^{64} - 1 = 18446744073709551615$.

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

From regular state to regular state

The solution from perfect state, (0,0,0,0), to perfect state (2,2,2,2) is relatively easy. Adding more discs does not really change the solution, being recursive. But a more difficult problem is to start from any regular position, non-perfect state, to any other regular position, non-perfect state. An interesting result is to find the "maximum number" of moves to start from a randomly regular position, non-perfect state, to a different randomly selected position.

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

From regular state to regular state

The solution from perfect state, (0,0,0,0), to perfect state (2,2,2,2) is relatively easy. Adding more discs does not really change the solution, being recursive. But a more difficult problem is to start from any regular position, non-perfect state, to any other regular position, non-perfect state. An interesting result is to find the "maximum number" of moves to start from a randomly regular position, non-perfect state, to a different randomly selected position.

Theorem

It takes at most $2^n - 1$ moves to solve the Tower of Hanoi with 3 pegs and n discs from any random regular state to a different randomly selected regular state.

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

Proof

We will again proceed by induction.
For $n = 1$, the puzzle is solved with one move since all position on H_1^3 are one move away from any other position.
We will suppose that it holds for $n = k$ and show that it also holds for $n = k + 1$. So that the number of moves is at most $2^{k+1} - 1$.
Let a and b represent the starting and finishing positions in H_{k+1}^3 and $l(a, b)$ the function representing the shortest distance between a and b on H_{k+1}^3. Reminder: H_{k+1}^3 consists of three copies of H_k^3.

Representing Tower of Hanoi and the Recursive Nature of the Puzzle

Proof

Let's consider two cases:

Case one: a and b both lay inside the same copy of H_k^3. The hypothesis states that $I(a,b) \leq 2^k - 1 \leq 2^{k+1} - 1$.

Case two: a and b are located in two different copies of H_k^3. We know by our hypothesis that the maximal number of moves in H_k^3 to pass from a to the vertex sharing the edge between the two copies is at most $2^k - 1$. Then we have to move once to get to the vertex of the second copy. We repeat the same argument from that vertex to b in at most $2^k - 1$ using our hypothesis. Therefore:

$$I(a,b) \leq 2^k - 1 + 1 + 2^k - 1 \leq 2(2^k - 1) + 1 \leq 2^{k+1} - 2 + 1 = 2^{k+1} - 1$$

Prime Numbers $2^n - 1$

Historical note

Marin Mersenne was a French monk who lived in the 17th century. Along with his profound religious beliefs, Mersenne showed an unusual interest in mathematics. Mersenne had incredible amounts of correspondence with mathematicians and scientists. He was known to steer scientists in the right direction, advising them on the next step to take.

Mersenne Primes

Theorem

If $a^n - 1$ is prime, then a must be 2 and n must be prime.

Proposition

$$x^n - 1 = (x - 1)\left(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1\right)$$

Mersenne Primes

Proof

Mersenne Primes

Definition

$2^n - 1$ primes are called Mersenne primes and we use the notation M_n.

Mersenne's Conjecture

In the *Praefatio generalis* of his *Cogita physico-mathematica* of 1644 Mersenne wrote that M_n was prime only for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ with $n \leq 257$.

Mersenne Primes

Mersenne's conjecture is shown to be fasle

Euler proved that for $n = 31$ was prime, then Lucas proved that for $n = 127$ was also prime (which will be further investigated). Then Pervushin showed that for $n = 61$ was also prime, making Mersenne's list officially incorrect, and at the beginning of the 20th century Powers proved two prime numbers Mersenne also missed $n = 89, 107$. By 1947, the correct list of primes $n \leq 258$ was : $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127$.

As of May 30th

Today: We have found every Mersenne Primes between $2^2 - 1$ and $2^{37156667} - 1$. However, we know that $2^{74207281} - 1$ is prime. We have yet to verify that there does not exist Mersenne Primes between these last two.

Mersenne Primes

Perfect Numbers

A perfect number is a positive integer n that is equal to the sum of its positive divisors less than n.

6 is a perfect number since $6 = 3 \times 2 \times 1$ and $6 = 3 + 2 + 1$. The next perfect number is 28.

Sum of divisors

$\sigma(n)$, $n \in \mathbb{Z}+$, is the sum of the positive divisors of n.

Furthermore, $\sigma(mn) = \sigma(n)\sigma(m)$ if $\gcd(m, n) = 1$. We say that it is a multiplicative function.

Mersenne Primes

Euclid-Euler Theorem

$2^{k-1}(2^k - 1)$ is an even perfect number if and only if $2^k - 1$ is prime.

Proof

A note on perfect numbers

In Proposition 36 of Book IX of Euclid's *Elements* we find the first part of the previous proof; Euler then proved the second part, making the one-on-one correlation very clear and showing that every perfect number is even (due to the form with factor 2^{k-1} which will always be even). It is not yet known if there exists any odd perfect number.

Mersenne Primes

Interesting problems

1. Show that if n is a perfect number, then $8n + 1$ is a perfect square.
2. Show that n is a perfect square if and only if n has an odd number of divisors and then use that result to show that there are no perfect square that are perfect numbers.
3. Show that the sum of the reciprocals of all the positive divisors of a perfect number is 2.
4. Show that if you sum the digits of any even perfect number (except 6), and then sum the digits of the resulting number, and then repeat this process until you get a single digit, that digit will be one.

Lucas Functions

Definition

Lucas started by defining a and b the roots of the following equation:

$$x^2 = Px - Q$$

We then have that :

$$a + b = P \qquad\qquad ab = Q$$

Lucas then defined the following functions:

$$U_n = \frac{a^n - b^n}{a - b} \qquad\qquad V_n = a^n + b^n$$

Lucas Functions

Simplest example

Here is the simplest example of a Lucas function: For $P = 1$ and $Q = -1$, we have:

$$a = \frac{1+\sqrt{5}}{2} \qquad b = \frac{1-\sqrt{5}}{2}$$

$$u_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}} \qquad v_n = \frac{(1+\sqrt{5})^n + (1-\sqrt{5})^n}{2^n}$$

We can then create the following sequences:

n	0	1	2	3	4	5	6	7	8	9
$U(1,-1)$	0	1	1	2	3	5	8	13	21	34
$V(1,-1)$	2	1	3	4	7	11	18	29	47	76

We recognize the first series as the Fibonacci sequence. The second one was named the Lucas sequence, for obvious reasons.

Lucas Functions

Exercise

Finally, Lucas showed his functions were also recurrent using the binomial theorem. Both the algebraic work and the final result are not clear in terms of showing the recurrence. Show that:

$$U_{n+1} = PU_n - QU_{n-1}, V_{n+1} = PV_n - QV_{n-1}$$

Lucas and the Mersenne Primes

- Lucas' first step in developing primality testing was to study the Fibonacci sequence $0, 1, 1, 2, 3, 5, 8, 13, \ldots$ named series of Lamé at the time.
- He then produced a table of the first 60 numbers with their factorization, where u_n would be the n^{th} number in the Fibonacci sequence.
- Used that table, the concept of proper divisor (primitive divisor) and other number theory results to show how he found that $u_{29} = 514229$ was a prime number.

Lucas and the Mersenne Primes

The first test

Let F_k be the kth term of the Fibonacci sequence. If $n \equiv \pm 3 \pmod{10}$ and n is a proper divisor of F_{n+1}, then n is prime. If $n \equiv \pm 1 \pmod{10}$ and n is a proper divisor of F_{n-1}, then n is prime.

(d is a proper divisor of F_n if $d \nmid F_r$ for any r such that $1 < r < n$).

The test was not presented with a valid proof, which, as we will see, seems to be a common theme for some of the tests Lucas would propose. The first proof of that test would be given by Carmichael in 1913.

Lucas and the Mersenne Primes

Example

Let's look at $n = 31$. $31 \equiv 1 \pmod{10}$. If we find 31 to be a proper divisor of $u_{31-1} = 832040$, then 31 is prime. Looking at the tables of Fibonacci Numbers, we find that $31 \nmid u_r$ for $1 < r < 31$, so 31 is a proper divisor of 832040, making 31 a prime.

Lucas and the Mersenne Primes

Lucas' Work on M_{127}

- The proof of M_{127} prime is nothing short of incredible.
- At the end of the nineteeth century, the largest Mersenne prime proved was M_{61} by Pervushin and the next two Mersenne primes, M_{89}, M_{107} were proven by Powers in the 1910's.
- To add to the impressive feat, M_{127} is still the largest prime proven without the help of a computer. How did Lucas manage to prove that a 39-digit number is a prime number?

Lucas and the Mersenne Primes

Lucas' Work on M_{127}

- The proof of M_{127} prime is nothing short of incredible.
- At the end of the nineteeth century, the largest Mersenne prime proved was M_{61} by Pervushin and the next two Mersenne primes, M_{89}, M_{107} were proven by Powers in the 1910's.
- To add to the impressive feat, M_{127} is still the largest prime proven without the help of a computer. How did Lucas manage to prove that a 39-digit number is a prime number?

  Lucas' clever use of modular arithmetic, binary notation and a chessboard made it possible.

Lucas and the Mersenne Primes

Defining a recurrence sequence

His idea was to use the sequence $S_0 = 1, S_1 = 3, S_{n+1} = S_n^2 - 2$. M_{127} would be prime if the least value of k such that $M_{127} \mid S_k$ is 126. This test was then reduced to squaring and substracting two and then dividing by a 39-digit number 126 times.

Useful result

If $M_n = 2^n - 1$, then $2^{m+n} \equiv 2^m \mod M_n$.

Proof

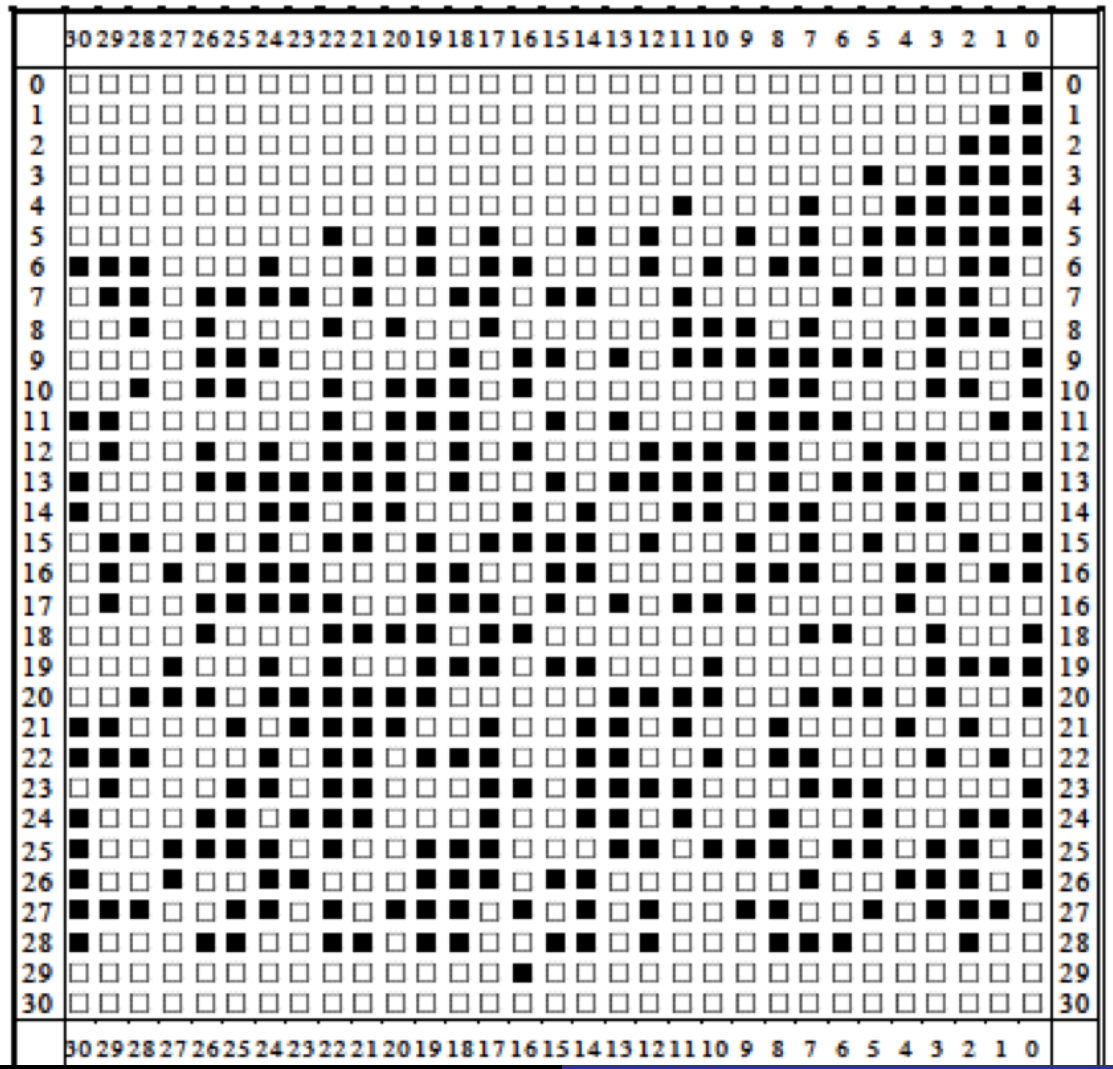
Lucas and the Mersenne Primes

Showing M_7 is prime

So for M_7 to be prime we need to show that $S_6 \equiv 0 \pmod{M_7}$. We have that $S_0 = 1, S_1 = 3, S_2 = 7, S_3 = 47$ and here comes Lucas' brilliant idea. Instead of squaring S_3, he would write it first in binary which is 101111.

Lucas and the Mersenne Primes

The arithmetic piano



Lucas' Major Works on Primality Testing

Lucas First Test

Let $M_n = 2^n - 1$, where n is prime and $n \equiv 3 \pmod 4$. Form the sequence $r_1 = 3, r_2 = 7, r_3 = 47, r_4 = 2207, ...,$ where $r_{i+1} = r_i^2 - 2$. M_n is a prime when $M_n \mid r_{n-1}$; M_n is composite if $M_n \nmid r_k$ for k= 1, 2, 3,...,n-1; and if $\alpha[\leq n-1]$ is the least value of k such that $M_n \mid r_k$, then the prime divisors of M_n must be of the form $2^{\alpha+1}m \pm 1$ and must also be divisors of the quadratic form $x^2 - 2y^2$.

Lucas' Major Works on Primality Testing

Lucas Second Test

Let $M_n = 2^n - 1$, where n is prime and $n \equiv 1(\mod 4)$. Form the sequence $r_1 = 4, r_2 = 14, r_3 = 194, r_4 = 37634, ...,$ where $r_{i+1} = r_i^2 - 2$. The number M_n is composite if $M_n \nmid r_k$ for k=1, 2, 3, ..., n-1; M_n is prime if the least value of α of k such that $M_n \mid r_k$ is such that $\frac{n+1}{2} \leq \alpha \leq n$. If $\alpha < \frac{n-1}{2}$, then the prime divisors of M_n must have the form $2^\alpha m \pm 1$.

Lucas' Major Works on Primality Testing

A word on proof

Both of Lucas tests were presented without a complete proof. Various tests, not only those for primality, must prove two aspects: the necessity of the test, meaning that the test will guarantee the wanted result and sufficiency of the test, meaning doing the test is enough to guarantee the condition is met.

Lucas' Major Works on Primality Testing

Putting it all together

Following those two tests, Lucas put together a few more tests. He even presented some tests with both conditions proved!.
Nonetheless, the next leap in the race for proving bigger and bigger prime numbers was taken by D.H. Lehmer in 1930 in his paper *An Extended Theory of Lucas' Functions*.

The Lucas-Lehmer Primality Test

The number $N = 2^n - 1$ is a prime if and only if it divides the $(n-1)$st term of the series

$$4, 14, 194, 37634, \ldots, S_k, S_k^2 - 2, \ldots$$

The Great Internet Mersenne Prime Search (G.I.M.P.S.)

The Idea

The G.I.M.P.S. is a project on the Internet that uses the computing power of a collective of users to find Mersenne Primes. The software used utilizes the Lucas-Lehmer test and the programmation for that test is incredibly simple. The G.I.M.P.S. was created in 1996 and since then they have found 15 new Mersenne primes. To this date the largest prime found is the 49th Mersenne $M_{74207281}$ a 22338618-digit number (close to 900 pages of digits!).

The Great Internet Mersenne Prime Search (G.I.M.P.S.)

The Pseudo Code for the Lucas-Lehmer Test:

Lucas Lehmer Test(p):
$s := 4$;
for i from 3 to p do $s := s^2 - 2 \mod 2^p - 1$;
if $s == 0$ then
$2^p - 1$ is prime
else
$2^p - 1$ is composite

The New Mersenne Conjecture

NMC

Following the proof that Mersenne original conjecture was false, Bateman, Selfridge, and Wagstaff proposed this New Mersenne conjecture:
Let p be any odd natural number. If two of the following conditions hold, then so does the third:

- $p = 2^k \pm -1$ or $p = 4^k \pm -3$
- $2^p - 1$ is a prime
- $\frac{(2^p+1)}{3}$ is a prime. (Prime of that form are named Wagstaff prime)

The only numbers that could have been verified are :
$3, 5, 7, 13, 17, 19, 31, 61, 127$. The interesting question to ask is if this is enough evidence to consider this statement a conjecture.

Return to the Tower of Hanoi

The *devil's peg*

A variation not yet mentioned is what happens if we add another peg. Adding a fourth peg, *the devil's peg*, defines a whole new problem. TH with four pegs is also called the Reve puzzle, which first appeared in a paper by Dudeney in 1907: *The Canterbury Puzzles*.

Return to the Tower of Hanoi

The *devil's peg*

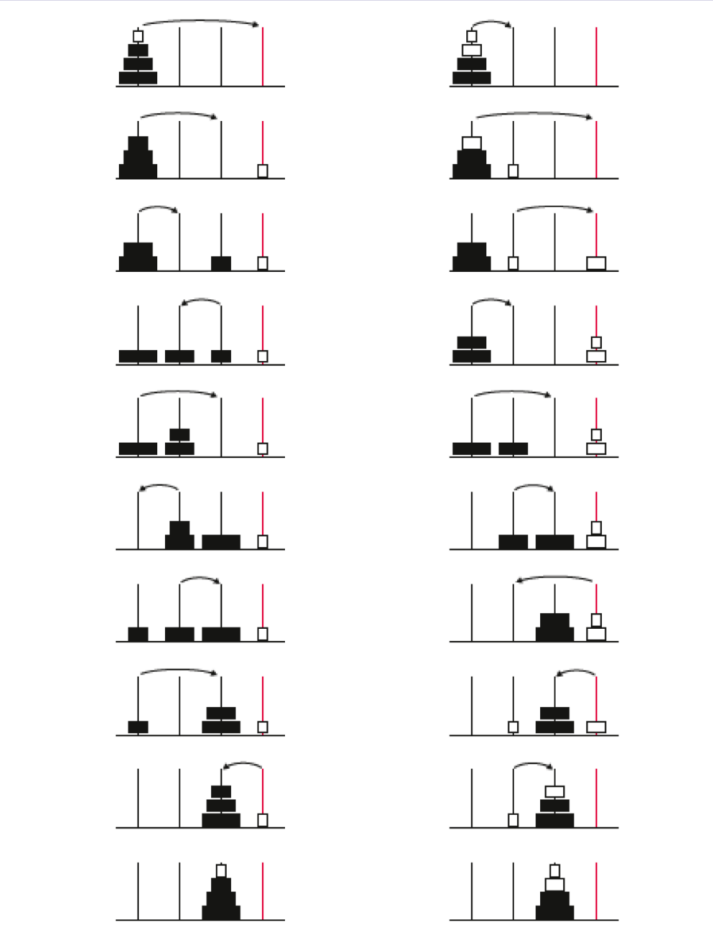


Figure: Solution to TH with 4 discs and 4 pegs

Return to the Tower of Hanoi

The *devil's peg*

The number of moves required to solve the puzzle can be found using the following recurrence:

$$M(n) = 2M(n-k) + 2^k - 1$$

In this process, k is the variable that must be picked to minimize the number of moves. The problem of solving the Reve Puzzle is ~~still an open problem~~solved (2014). This shows how a very simple problem can become very difficult by changing only one parameter.