Mathematics in Leiden, old and new

Bas Edixhoven

Universiteit Leiden

Cleveringa lecture
Erasmus Huis, Jakarta
2015/11/17

Abstract

Brief commemoration of Cleveringa's speech and its context.

200th anniversary of the faculty of Mathematics and Natural Sciences in Leiden, and the book 'Van Kabinet naar Science Park' that has been published on this occasion,

The recent opening of the website 'Leidse hoogleraren vanaf 1575'.

The speaker's work (in a not too technical way) in the areas of number theory and geometry.

Some examples of applications of these areas in daily life: secure internet banking (even if criminals have quantum computers), playing damaged cd's and dvd's, and fast computations with high precision and large numbers.

These notes will be available on my home page.

Background of the Cleveringa lectures

On Saturday November 23 of 1940, the jewish personnel of the dutch universities was removed from their positions by the ministery of education.

On Tuesday November 26, Rudolph Cleveringa, then dean of the faculty of law, held his famous protest speech.
He gave his speech at the time and place of the class of Eduard Maurits Meijers, one of the removed professors.
Also Ton Barge (anatomy and embryology) and Lambertus van Holk (theology) protested publicly.
The students went on strike, and the university was closed by the german authorities.

The university of Leiden during the occupation

The closure of the university was fortunate, because the german authorities had plans to reorganise the university according to nazi ideology.

These plans lead to a continuous struggle between the german authorities and the board and professors of the university.

After some professors were fired in March and April of 1942, 53 professors and 3 lectors collectively resigned from their positions. The university and the german plans came to a full stop.

Sources:
Mr. P.J. Idenburg, “De Leidse Universiteit 1928–1946”, Universitaire Pers, Leiden, 1978 (ISBN 90.6021.425.0);
Prof. dr. W. van der Woude’s lecture in “Kort Verhaal van de plechtige heropening der universiteit. . . ,” Universitaire Pers Leiden, 19??.
Cleveringa-reader LUF 2015.

What happened to Cleveringa?

Cleveringa was arrested and imprisoned in Scheveningen, but survived the war. Also Meijers, Barge and van Holk survived the war.

Telders did not survive the war, he died in Bergen-Belsen in April 1945. The “Teldersstichting” is named after him.

For so far about the history of the Universtiteit Leiden in World War 2.

Message from the rector, Carel Stolker.

Faculty of Mathematics and Natural Sciences 200 years, from old to new

Napoleon definitely defeated at Waterloo in June 1815, Faculty of Mathematics and Natural Sciences founded in August 1815 by king Willem Frederik (‘organiek besluit’).

At this occastion: the book ‘Van Kabinet naar Science Park’, by Otterspeer, van Delft and van Lunteren.
`http://leidenscience-200.leidenuniv.nl/lustrum-boek`

Cover

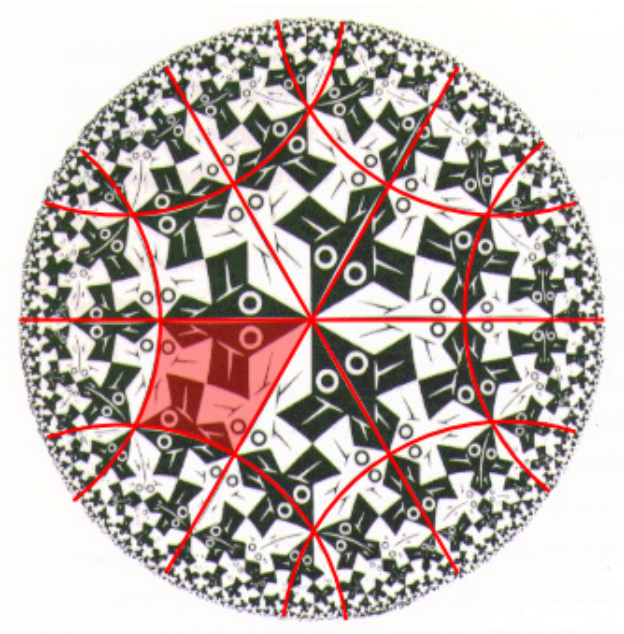
Bierens de Haan, Kloosterman (KNAW), Zoutendijk, Lenstra, Meulman, Edixhoven.

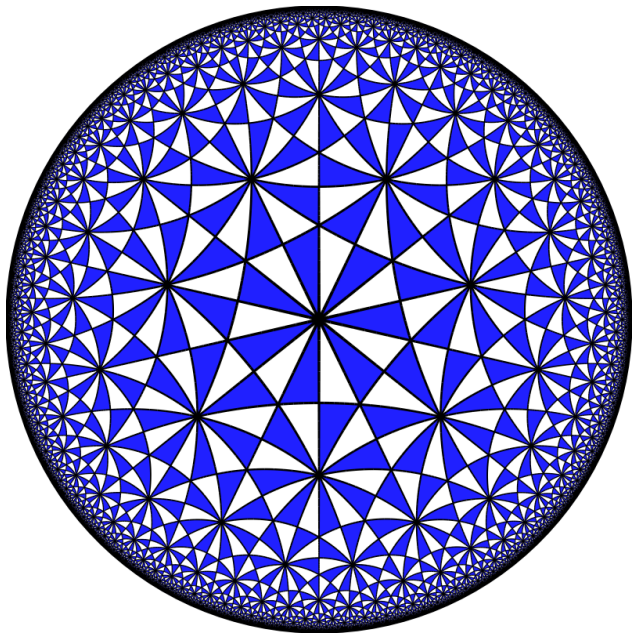
See also: `http://hoogleraren.leidenuniv.nl` for all Leiden professors since 1575.

My own work: on sums of squares

This work is mentioned as an example of recent research in the Netherlands on page 40 in the *Deltaplan voor de Nederlanse wiskunde*, to be submitted to the minister of Education, Culture and Science.

The concept behind this work: modular forms.





Langlands, Euler, Jacobi, Ramanujan, Deligne

Modular forms are an important special case of the "Langlands program", a series of conjectures, partly proved, concerning relations between notions of symmetry in geometry and analysis and of symmetry in number theory ($a+b\sqrt{2} \mapsto a-b\sqrt{2}$, etc.).

$$\prod_{n\geq 1}(1-q^n) = \sum_{m\in\mathbb{Z}}(-1)^m q^{(3m^2-m)/2}$$

$$\sum_{m\in\mathbb{Z}^4} q^{m_1^2+m_2^2+m_3^2+m_4^2} = 1 + \sum_{n\geq 1}\left(8\sum_{2\nmid d\mid m} d + 16\sum_{2\nmid d\mid m/2} d\right) q^n$$

$$q\prod_{n\geq 1}(1-q^n)^{24} = \sum_{m\geq 1}\tau(n)q^n, \quad \tau \text{ is Ramanujan's tau-function}$$

For p prime, $|\tau(p)| < 2\cdot p^{11/2}$.

Secure internet banking

When you communicate with your bank over internet, it is essential that only the intended receiver can read the messages.

This is achieved by mathematical constructions called encryption using the public key of the receiver. Only the receiver has the corresponding secret key to decrypt the encrypted message.

I will show you on our Leiden Sage server how it works in the case of RSA (invented in the 1970's):
`https://sage.math.leidenuniv.nl/`

Secure communication, also for terrorists

We can use such encryption for communication that even the NSA cannot break.

For that reason it is not so surprising that email is not encrypted by default, nowadays. NSA and the likes have apparently been able to prevent the most common computer and software producers from implementing it.

But terrorists and criminals, and also ordinary people who want privacy, use such encryption.

For electronic banking, strong cryptography is used, and is safe. Otherwise all our bank accounts would already have been emptied by criminals.

And now the quantumcomputer

A quantum computer does not compute with *bits* that can assume the values 0 and 1, but with *qubits* that can be superpositions of 0 and 1.

A quantum computer with input n qubits can run a computation on 2^n possible classical inputs simultaneously.

However, the output is only useful if it peaks at the desired solution. For certain *very specific* computations, such as finding the periodicity in a sequence, this possible by interference (technical tool: Fourier transform).

For example, quantumcomputers with at least 1000 qubits can break the RSA encryption in the example we gave.

But quantumcomputers do not yet exist (as far as we know). The idea was proposed by Benioff, Manin, Feynman and Deutsch in the beginning of the 1980's, and since then the situation is a lot like nuclear fusion reactors to produce energy.

Current research on quantum computers

The research group of Leo Kouwenhoven in Delft has obtained funding for a total of 150 ME for 10 years, see
`http://qt.tudelft.nl/2015/06/02/nederland-investeert-135-miljoen-in-quantumtechnologie`
to develop a quantum computer. A working prototype is promised already for 2013+6=2019. We will see!

The providers of the funds are: TU Delft, TNO, the departments EZ and OCW, NWO/STW/FOM and the topsector High Tech Systems and Materials (HTSM).

See also `http://www.onderzoeksgebieden.leidenuniv.nl/de-kwantumcomputer`
Here it is claimed that the quantum computer will solve the traveling salesman problem in polynomial time. This claim is unrealistic and unjustified: no polynomial time quantum algorithm is known for the traveling salesman problem.

Post quantum cryptography

Already at this moment, there are new methods of encryption that work on classical computers, for which no quantum algorithm is know, nor expected, for breaking it. See: `https://en.wikipedia.org/wiki/Post-quantum_cryptography`. Many of these methods are applications of the areas of mathematics where I work.

For the moment, the conclusion is: even when there will be quantum computers,

- we can still do our electronic banking securely with our old classical computers;
- everybody, including terrorists, can securely communicate over public channels such as internet, using just classical computers.

Playing damaged cd's and dvd's

Sound and images are recorded on cd's and dvd's as follows: the sound is sampled at 44.1 kHz and with a precision of 16 bits. This gives a stream of bits. Data to be stored on a cdrom already consists of bits.

The stream of bits is divided into blocks of 28 bytes. Each block encoded via a *Reed-Solomon error correcting code* to a block of 32 bytes. Sequences of 24 blocks are then encoded to 28 blocks. The resulting process is called Cross Interleaved Reed-Solomon Code. This added 1/3 of redundancy to the signal permits the correction of many errors, including scratches of 2.5 mm on the tracks.

Source: `https://en.wikipedia.org/wiki/Reed\OT1\textendashSolomon_error_correction`
See also:
`https://en.wikipedia.org/wiki/Kees_Schouhamer_Immink`

Leiden in snow

Thank you for your attention!

Let us watch
`https://www.youtube.com/watch?v=3ryBzWNhLxY`