Wiskunde in Leiden, oud en niew

Bas Edixhoven

Universiteit Leiden

Cleveringa lezing
Hollandse Club, Singapore
2015/11/19

Samenvatting

Korte herinnering aan Cleveringa's rede en de context ervan.

200 jaar faculteit Wiskunde en Natuurwetenschappen in Leiden, en het boek 'Van Kabinet naar Science Park' dat hierbij is uitgegeven,

De recente opening van de website 'Leidse hoogleraren vanaf 1575'.

Werk van de spreker (hopelijk zonder teveel technicaliteiten) in de getaltheorie en meetkunde.

Een paar voorbeelden van toepassingen van deze gebieden van de wiskunde in het dagelijks leven: veilig internetbankieren (zelfs als criminelen quantumcomputers hebben), afspelen van beschadigde cd's en dvd's.

Deze aantekeningen komen op mijn homepage.

Achtergrond van de Cleveringa lezingen

Op zaterdag 23 november 1940 werd het joodse personeel van de universiteiten ontheven van hun taak door het ministerie van onderwijs.

Op dinsdag 26 november hield Rudolph Cleveringa, decaan van de rechtenfaculteit, zijn beroemde protestrede.
Hij gaf deze rede op het tijdstip en de plaats van het college van Eduard Maurits Meijers, een van de joodse hoogleraren.
Maar ook Ton Barge (anatomie en embryologie) en Lambertus van Holk (theologie) protesteerden publiek.
De studenten gingen in staking, en de universiteit werd door de duitse autoriteiten gesloten.

De universiteit Leiden onder de bezetting

De sluiting kwam goed uit, want de duitse autoriteiten hadden plannen om de universiteit om te nazificeren.

Deze plannen leidden tot een voortdurende strijd tussen de duitse autoriteiten en het bestuur van de universiteit.

Nadat in maart en april 1942 enkele hoogleraren door de duitsers werden ontslagen dienden 53 hoogleraren en 3 lectoren collecief hun ontslag in. De universiteit, en ook de duitse plannen, kwamen tot een volledige stilstand.

Bronnen:
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 rede in “Kort Verhaal van de plechtige heropening der universiteit. . . ,” Universitaire Pers Leiden, 19??.
Cleveringa-reader LUF 2015.

Wat gebeurde uiteindelijk met Cleveringa?

Cleveringa werd gearresteerd en gevangen gezet in Scheveningen, maar overleefde de oorlog. Ook Meijers, Barge en van Holk overleefden de oorlog.

Telders overleefde niet, hij stierf in Bergen-Belsen in april 1945. De “Teldersstichting” is naar hem vernoemd.

Voor zover de geschiedenis van de Universtiteit Leiden in de WO2.

Boodschap van de rector, Carel Stolker.

Faculty W& N 200 jaar, van oud naar nieuw

Napoleon werd definitief verslagen bij Waterloo in juni 1815, de faculteit W& N werd opgericht in augustus 1815 door koning Willem Frederik (‘organiek besluit’).

Ter gelegenheid hiervan: het boek ‘Van Kabinet naar Science Park’, door Otterspeer, van Delft en van Lunteren.
`http://leidenscience-200.leidenuniv.nl/lustrum-boek`

Omslag

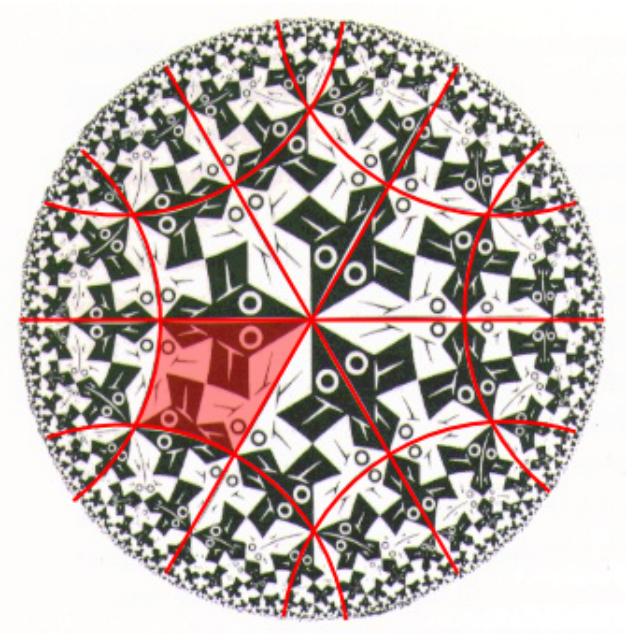
Bierens de Haan, Kloosterman (KNAW), Zoutendijk, Lenstra, Meulman, Edixhoven.

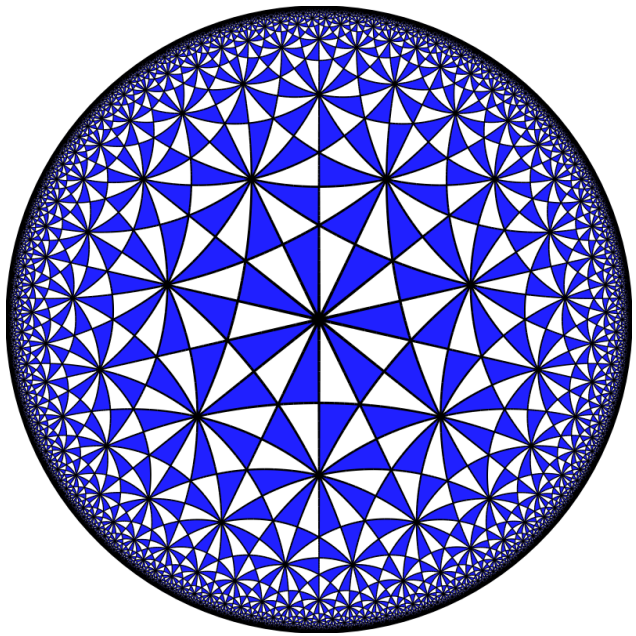
Zie ook: `http://hoogleraren.leidenuniv.nl` voor alle leidse hoogleraren sinds 1575.

Eigen werk: over sommen van kwadraten

Dit werk wordt beschreven als 1 van 12 voorbeelden van recent onderzoek in de wiskunde op pagina 40 van het *Deltaplan voor de Nederlanse wiskunde*, dat vandaag of morgen wordt overhandigd aan de minister van OCW.

Het concept achter dit werk: modulaire vormen.





Langlands, Euler, Jacobi, Ramanujan, Deligne

Modulaire vormen zijn een belangrijk speciaal geval van het "Langlands programma", een serie van vermoedens, gedeeltelijk bewezen, over verbanden tussen symmetrieën in de meetkunde, in de analyse, en in de getaltheorie ($a + b\sqrt{2} \mapsto a - b\sqrt{2}$, etc.).

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

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

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

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

Veilig internet bankieren

Wanneer je met je bank communiceert over internet, dan is het essentieel dat alleen de beoogde ontvanger de boodschappen kan lezen, weet van wie ze komen, weet dat de inhoud niet veranderd is, en dat hij de zender aan zijn verplichtingen kan houden.

Dit alles is mogelijk door wiskundige constructies als versleuteling, ontsleuteling, digitale handtekeningen, etc. Zowel de zender als de ontvanger maken een sleutelpaar aan: een publieke en een geheime sleutel. De zender gebruikt de publieke sleutel van de ontvanger. Voor de ontsleuteling is de geheime sleutel van de ontvanger nodig.

Laten we kijken hoe dit werkt op de leidse Sage server in het geval van RSA (uitgevonden in de jaren 1970):
`https://sage.math.leidenuniv.nl/`

Veilige communicatie, ook voor terroristen

Dergelijk versleutelde communicatie kan zelfs de NSA niet kraken.

Daarom is het ook niet verrassend dat zelfs nu email niet standaard versleuteld wordt. NSA en gelijken hebben kennelijk kunnen voorkomen dat de grootste computer- en softwarefabrikanten dit standaard leveren.

Maar terroristen en andere criminelen, en ook fatsoenlijke mensen die privacy wensen, gebruiken versleuteling.

Voor internetbankieren wordt versleuteling gebruikt, en die is veilig. Want anders zouden al onze bankrekeningen al zijn leeggehaald door criminelen.

En nu de kwantumcomputer

Een kwantumcomputer rekent niet met *bits* die de waarden 0 en 1 kunnen aannemen, maar met *qubits* die superposities zijn van 0 en 1.

Een kwantumcomputer met input n qubits kan simultaan een berekening doen op 2^n mogelijke klassieke inputs..

Maar de output is alleen bruikbaar als deze 'piekt' bij de gewenste uitkomst. Voor bepaalde *zeer speciale* berekeningen, zoals de periodiciteit vinden in een rij, is dit mogelijk door interferentie (technisch gereedschap: Fourier transformatie).

Bijvoorbeeld kunnen kwantumcomputers met minstens 1000 qubits de RSA versleuteling breken in het gegeven voorbeeld.

Maar kwantumcomputers bestaan (nog) niet, voor zover we weten. Het idee werd voorgesteld door Benioff, Manin, Feynman en Deutsch in het begin van de jaren 1980's, en sindsdien is het zoals met de kernfusie (veel beloftes, nog niets geleverd; wel, ITER wordt verwacht in 2018 energie te leveren).

Huidig onderzoek aan kwantumcomputers

De groep van Leo Kouwenhoven in Delft heeft 150 ME voor 10 jaar gekregen, zie `http://qt.tudelft.nl/2015/06/02/nederland-investeert-135-miljoen-in-quantumtechnologie` om een kwantumcomputer te ontwikkelen. Een werkend prototype is beloofd voor 2013+6=2019. We zullen zien!

De geldschieters zijn: TU Delft, TNO, EZ en OCW, NWO/STW/FOM, en de topsector High Tech Systems and Materials (HTSM).

Zie ook `http://www.onderzoeksgebieden.leidenuniv.nl/de-kwantumcomputer`
Daar wordt geclaimd dat de kwantumcomputer het handelsreizigersprobleem kan oplossen in polynomiale tijd. Dat is onrealistisch en niet geargumenteerd: geen polynomiaal kwantum algoritme is bekend voor dit probleem.

Postkwantum-cryptographie

Op dit moment zijn er al nieuwe methoden van versleuteling bekend, die op klassieke computers werken, waarvoor geen kwantum algoritme bekend is en ook niet verwacht wordt, om die te kraken. Zie: `https://en.wikipedia.org/wiki/Post-quantum_cryptography`. Veel van deze methoden zijn toepassingen van gebieden in de wiskunde waarin ik werk.

De conclusie is op dit moment: zelfs wanneer er kwantumcomputers zijn,

- dan kunnen we nog steends veilig internetbankieren met onze oude klassieke computers;
- iedereen, ook een terrorist, kan veilig communiceren over publieke kanalen zoals internet, alleen gebruik makend van klassieke computers.

Spelen van beschadigde cd's en dvd's

Geluid wordt opgeslagen op een cd als volgt: het geluid wordt gesampled op 44.1 kHz, met een precisie van 16 bits. Dat geeft een stroom van bits. Data voor opslag of een cdrom bestaat al uit bits.

De stroom van bits wordt opgedeeld in blokken van 28 bytes. Elk blok wordt gecodeerd vie een *Reed-Solomon error correcting code* naar een blok van 32 bytes. Rijen van 24 blokken worden vervolgens gecodeerd in rijen van 28 blokken. Het resulterend proces heet 'Cross Interleaved Reed-Solomon Code'. De toegevoegde 1/3 redundantie aan de data maakt het mogelijk om veel fouten te herstellen, bijvoorbeeld krassen van 2.5 mm in de sporen.

Bronnen: `https://en.wikipedia.org/wiki/Reed\OT1\textendashSolomon_error_correction`
Zie ook:
`https://en.wikipedia.org/wiki/Kees_Schouhamer_Immink`

Leiden in snow

Dank u voor uw aandacht!

Laten we kijken naar
`https://www.youtube.com/watch?v=3ryBzWNhLxY`