ARITHMETIC GEOMETRY, MOTIVES: COMPUTATIONAL ASPECTS

BAS EDIXHOVEN

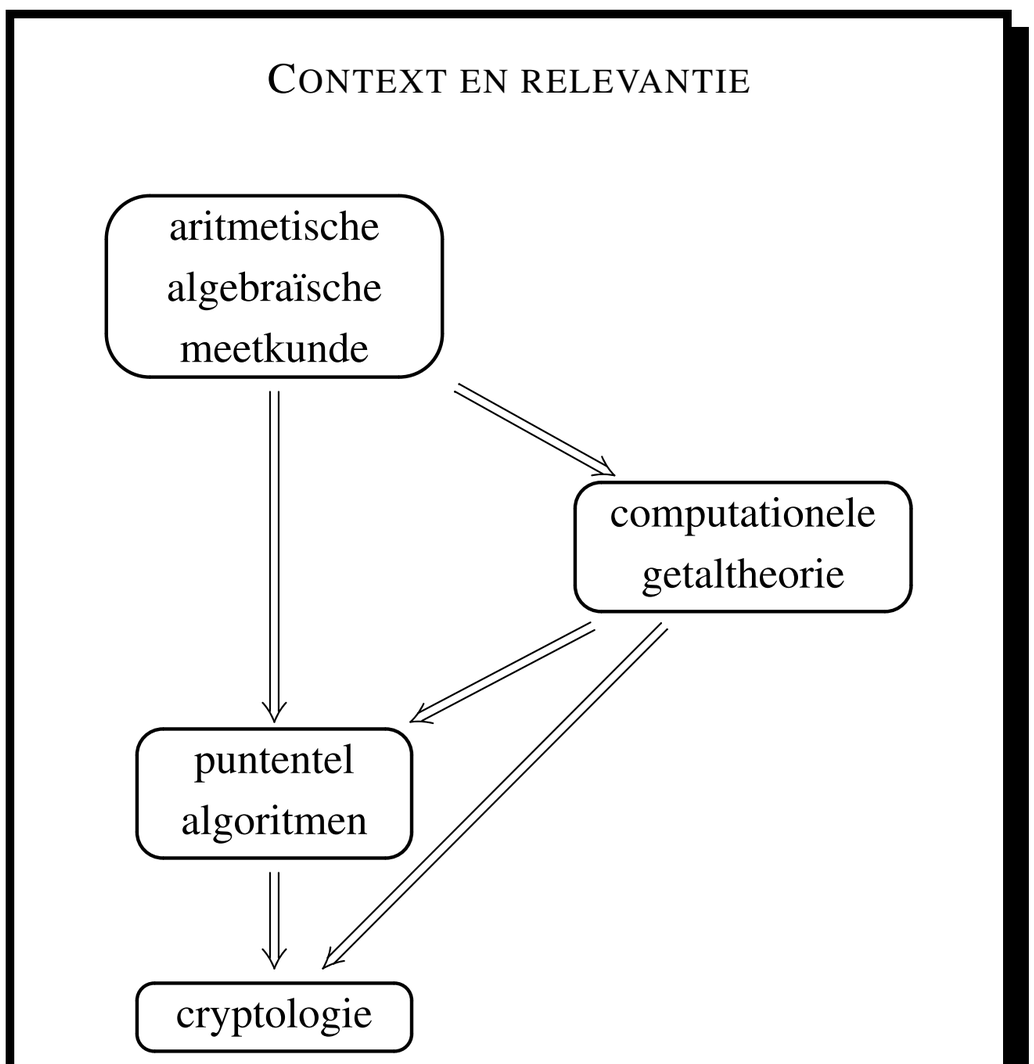
Overzicht van de presentatie:

1. Context en relevantie van het onderzoek;
2. Onderzoeksmethode;
3. Besteding van de subsidie;
4. Conclusies.

Dames en heren, allereerst mijn dank voor de uitnodiging voor dit interview.

De presentatie van mijn project, “aritmetische meetkunde, motieven, en computationele aspecten”, zal uit 4 onderdelen bestaan.

Ik zal achtereenvolgens ingaan op de “Context en relevantie van het onderzoek”, de “Onderzoeksmethode”, de “Besteding van de subsidie”, en ik zal enige “Conclusies” formuleren aan het eind.


aritmetische
algebraïsche
meetkunde
computationele
getaltheorie
puntentel
algoritmen
cryptologie

Dit schema geeft de relaties aan tussen de gebieden van de wiskunde en (theoretische) informatica die in het onderzoek een rol spelen.

Aan het ene uiterste zien we de aritmetische algebraïsche meetkunde, een deel van de wiskunde dat de reputatie heeft zeer abstract te zijn, en aan de andere kant cryptologie, d.w.z., de wetenschap van bescherming van elektronische gegevens, een gebied dat midden in de praktijk staat. De pijlen geven de richting van de toepassingen aan.

Ikzelf bevind mij in de aritmetische algebraïsche meetkunde, maar de toepassingen van het beoogde onderzoek op de andere gebieden zijn zeer duidelijk.

Ik zal nu kort ingaan op elk van de vier gebieden, te beginnen met wat we ons allemaal het makkelijkst kunnen voorstellen: de cryptologie.

CONTEXT EN RELEVANTIE: CRYPTOLOGIE

Doel: veilige communicatie via internet, elektronische handtekeningen, integriteit van documenten, elektronisch stemmen,...

Middelen: discrete wiskunde, met name computationele getaltheorie en algebraïsche meetkunde.

In de praktijk:

1. RSA, factoriseren is moeilijk.
2. ECC (elliptic curve cryptography), discrete logaritme op elliptische kromme is moeilijk.

Beoogde onderzoek:

1. mogelijke alternatieven voor ECC,
2. mogelijke vooruitgang in factoriseren en discrete log.

Zoals u weet is internet een publiek kanaal, waarop eigenlijk iedereen alles kan lezen. Vertrouwelijke berichten moeten dus versleuteld worden, terwijl nog bijna niemand dat doet. Als voorbeeld kunnen we de email van officier van justitie Tonino noemen.

ECC heeft het voordeel boven RSA dat het kan met kleinere chips.

CONTEXT EN RELEVANTIE: PUNTENTEL ALGORITMEN

Essentieel voor ECC: het *precieze aantal* oplossingen tellen van bepaalde vergelijkingen.

De veiligheid van ECC staat of valt met de grootte van de *grootste priemfactor* van zo'n aantal.

Voorbeeld van dit telprobleem. Laat p een priemgetal zijn (zeg van 100 of meer cijfers). Laat a en b gehele getallen zijn. Hoeveel paren (x, y) van gehele getallen met $0 \leq x, y < p$ zijn er waarvoor

$$-y^2 + x^3 + ax + b$$

deelbaar is door p? Hier is een goed algoritme voor (Schoof, 1985).

Beoogde onderzoek: generaliseert Schoof's algoritme.

Het is duidelijk dat men voor het tellen van de oplossingen niet alle p^2 paren (x, y) kan nagaan: er zijn minstens 10^{200} van die paren. Zelfs als we per x de mogelijke y tellen, moeten we nog minstens 10^{100} stappen doen. Daar kun je wel 10^{80} jaar gaan wachten, minstens.

Schoof's algoritme kost ongeveer $(\log p)^4$ stappen. Dat is zeer verbazend!

Hier zien we het verschil tussen exponentiële en polynomiale complexiteit van algoritmen.

CONTEXT EN RELEVANTIE: ARITMETISCHE ALGEBRAÏSCHE MEETKUNDE

De aritmetische algebraïsche meetkunde levert het middel dat het *theoretisch* mogelijk maakt snel oplossingen te tellen: *Weil cohomologie*.

In het geval van Schoof is deze cohomologie vrij gemakkelijk uit te rekenen.

Beoogde onderzoek: zal cohomologie algemener toepasbaar maken, door middel van snelle (polynomiale) algoritmen.

Eerste stap: van elliptische krommen naar algemene "motieven" van rang twee.

Dit is een cruciaal geval (hogere dimensies), ook voor de getaltheorie (Wiles).

Aritmetische algebraïsche meetkunde is de studie van systemen van veeltermvergelijkingen door middel van meetkundige technieken. Denkt u maar aan $x^2 + y^2 = 1$, dit is een veeltermvergelijking voor de cirkel.

Cohomologie bestaat uit vectorruimten met operatoren, d.w.z., matrices. Deze matrices leveren de aantallen punten.

Voorbeeld: elliptische kromme, $y^2 = x^3 + ax + b$, over $\mathbb{R}$ een "ei-kromme", over $\mathbb{C}$ een "zwemband met ventiel". Dit geeft $(\mathbb{R}, \mathbb{R}^2, 0)$ (in het algemeen: evenveel vectorruimten als de dimensie). Plaatjes!

Motieven zijn voor de algebraïsch meetkundigen wat quarks zijn voor de natuurkundigen: meetkundige objecten worden nog opgesplitst in hun cohomologie. In deze presentatie gebruik ik voor de eenvoudigheid het woord "motief" als synoniem voor "cohomologie".

Een motief van rang twee is dan een stuk cohomologie dat van dimensie twee is.

Wiles' bewijs van de laatste stelling van Fermat maakt essentieel gebruik van rang twee motieven. Tot Wiles werden alleen rang één motieven gebruikt (en dus lukte het niet).

CONTEXT EN RELEVANTIE: COMPUTATIONELE GETALTHEORIE

De computationele getaltheorie komt nu niet verder dan motieven van rang één (CFT, class field theory) en de simpelste motieven van rang twee (elliptische krommen).

Beoogde onderzoek: zal algemene motieven van rang twee, en in principe ook van hogere rang, bereikbaar maken. Doorbraak.

Een frappant concreet gevolg: voor priemgetallen p kan $\tau(p)$ in tijd polynomiaal in $\log p$ worden uitgerekend. Hier is τ de Ramanujan τ-functie, gedefinieerd door:

$$x\left(\prod_{n\geq 1}(1-x^n)\right)^{24}=\sum_{m\geq 1}\tau(m)x^m$$

Het gebruik van elliptische krommen heeft, via Lenstra, geleid tot snellere algoritmen voor factoriseren. Wie weet wat algemene motieven van rang twee zullen veroorzaken (ik geef toe, dit is wel speculatie!).

Hoe dan ook: volgend jaar scoor ik keihard in het doel van de computationele getaltheorie. Dit vind ik zelf de belangrijkste toepassing van mijn onderzoeksproject.

ONDERZOEKSMETHODE

De problemen worden gereduceerd tot het *exact* oplossen van bepaalde systemen veeltermvergelijkingen in een groot aantal variabelen.

Het aantal variabelen is te groot om dit met exacte methoden (computer algebra) te doen: de benodigde tijd is exponentieel in het aantal variabelen.

Innovatie: *benader* de oplossingen *numeriek*, met een zo grote precisie dat men er de exacte oplossing uit kan afleiden.

Voor dit laatste is een *bovengrens* nodig van de "complexiteit" van de oplossingen.

Gebruik alles wat er maar bestaat (onder andere "Arakelov theorie") om zo'n bovengrens te krijgen: dit is het moeilijkst van het hele project.

Ik kom nu toe aan het volgende onderdeel van de presentatie: de gebruikte onderzoeksmethode.

Via “standaard technieken” worden de problemen gereduceerd tot…

ONDERZOEKSMETHODE: VAN BENADERING NAAR EXACT

Een zeer eenvoudig voorbeeld.

Stel $x = a/b$ met a en $b \neq 0$ gehele getallen, en dat $|a| < 10^{100}$ en $|b| < 10^{100}$.

Dan kan ik x afleiden uit een benadering y met $|y - x| < 0.5{\cdot}10^{-200}$.

Namelijk: laat $x' = a'/b'$ net zo'n breuk zijn, met $x' \neq x$. Dan:

$$|x - x'| = \left|\frac{a}{b} - \frac{a'}{b'}\right| = \left|\frac{ab' - a'b}{bb'}\right| > \frac{1}{10^{200}}.$$

Conclusie: het is hier genoeg om met ongeveer 300 cijfers te rekenen.

In dit eenvoudige voorbeeld is 10^{100} de bovengrens voor de complexiteit van de oplossing.

BESTEDING VAN DE SUBSIDIE: SALARISKOSTEN

Salaris kosten (in k€):	
Kandidaat (0.4fte, 5 jaar)	276
Postdoc 1 (1.0 fte, 2 jaar)	97
Postdoc 2 (1.0 fte, 2 jaar)	97
Postdoc 3 (1.0 fte, 2 jaar)	97
OiO 1 (1.0 fte, 4 jaar)	155
OiO 2 (1.0 fte, 4 jaar)	155
OiO 3 (1.0 fte, 4 jaar)	155
Programmeur (0.2 fte)	30
Totaal	1062

BESTEDING VAN DE SUBSIDIE: OVERIGE KOSTEN

Overige kosten (in k€):	
Computers/software	38
Boeken/Tijdschriften	10
Buitenlandse bezoekers	25
Organisatie van int. workshops	40
Reis en verblijfskosten	50
Popularisering van wiskunde	25
Totaal	188

BESTEDING VAN DE SUBSIDIE: WIE DOET WAT?

Kandidaat: begeleidt het hele team.

Kandidaat en postdoc 1 (Robin de Jong): details 1ste stap (bepaalde motieven van rang 2, polynomiaal algoritme $\tau(p)$) uitwerken en publiceren, met Couveignes; generalisatie naar willekeurige motieven van rang 2.

OiO 1 (Johan Bosman): $\tau(p)$ uitrekenen voor p die nu totaal onbereikbaar zijn. Ook de "tussenresultaten" zijn zeer interessant.

Postdoc 2 en OiO 2: de complexiteit van de polynomiale algoritmes optimaliseren en zo goed mogelijk afschatten (meer gedetailleerde studie van de meetkunde, en van de de numerieke aspecten).

BESTEDING VAN DE SUBSIDIE: WIE DOET WAT?

Postdoc 3: meer algemene motieven, punten tellen op variëteiten die horen bij die motieven, toepassingen op cryptologie.

OiO 3: algemenere motieven over functielichamen bereikbaar maken voor computationele getaltheorie; gebruikt dezelfde aanpak, maar de meetkunde is eenvoudiger.

Programmeur: ondersteunen van vooral OiO 1, verder experimenteel werk voor het gehele team.

BESTEDING VAN DE SUBSIDIE: POPULARISERING

Edixhoven is voorzitter van het bestuur (met Henk Barendregt, Wim Berkelmans en Hendrik Lenstra) van de Stichting Vierkant voor Wiskunde.

Activiteiten van Vierkant: zomerkampen, en materiaal voor in de klas, voor leerlingen van lagere en middelbare school die meer willen.

Edixhoven coördineerde in 2003 en 2004 het wiskundig gedeelte van de wetenschapsdag in Leiden.

Het Web Interactive Multipurpose Server (WIMS) project. Interactieve wiskunde op internet: sommen, recreatieve puzzels, digitale klassen, maar ook moeilijke berekeningen.

Internationale workshops: in 2003-2004 heeft Edixhoven er drie ge(co)organiseerd (cryptologie, Shimura variëteiten, motieven), alle drie op het Lorentz Center te Leiden.

Hier wil ik aangeven met wat voor activiteiten ik bezig ben, en die kunnen worden voortgezet en uitgebreid als er subsidie is.

De kampen hebben evenveel deelnemers als het totaal aantal eerstejaars wiskunde studenten in Nederland. Vandaar het belang.

Opmerking over Freudenthal instituut: dat heeft goed werk gedaan om het wiskunde-onderwijs voor meer leerlingen bereikbaar te maken, maar het is daardoor niet meer interessant en uitdagend voor de betere leerlingen die wèl blij zouden zijn met meer abstractie, wat wel eens één van de oorzaken kan zijn dat er zo weinig eerste jaars wiskunde studenten zijn. Vierkant maakt materiaal dat wel interessant en uitdagend is voor geïnteresseerde leerlingen, zonder de onderwijsprogramma's in de weg te zitten.

Sindskort heb ik de eerste Nederlandse WIMS mirror hiervoor opgezet. Hier is nog veel werk te doen (vertalen naar Nederlands, bijvoorbeeld).

CONCLUSIES

De onderzoeksmethode werkt.

In 2005 zal er een doorbraak zijn.

Deze doorbraak maakt de subprojecten urgent.

Referee 5: “This will certainly be one of the (if not the) most important results in computational algebraic geometry in the last 50 years. . . for me this is THE most important work presently being done in explicit arithmetic geometry.”.

Het onderzoek is ook zeer relevant buiten de wiskunde (contract CELAR).

Na het project zal er een zeer goede en permanente algebraïsche meetkunde groep zijn in Leiden (één hoogleraar en twee u(h)d’s).

Laat ik eindigen met mijn conclusies.

In de inbeddingsgarantie bij mijn voorstel staat dat het vakgebied van mijn leerstoel één van de vier kerndisciplines van het Mathematisch Instituut van de universiteit Leiden is. Op termijn zijn er twee permanente medewerkers op ud of uhd niveau toegezegd.