

\*\*\*\*\*

MEDEDELINGEN VAN HET KONINKLIJK WISKUNDIG GENOOTSCHAP, 2015 nr. 12

19 juni 2015 (elektronische aflevering)

De eerstvolgende aflevering verschijnt omstreeks 3 juli 2015.

Kopij kan worden gestuurd naar [medwg@cwi.nl](mailto:medwg@cwi.nl); agenda-items kunnen ook worden aangeboden via de website [www.wiskgenoot.nl](http://www.wiskgenoot.nl)

Mededeling van het Bestuur

=====

Het verslag van de kascommissie aangaande het financiële jaarverslag van het KWG over 2014 is beschikbaar via

[www.wiskgenoot.nl/watbiedt/Jaarverslagen/ALV2015/VerslagKascie 2014.pdf](http://www.wiskgenoot.nl/watbiedt/Jaarverslagen/ALV2015/VerslagKascie%202014.pdf)

\*\*\*\*\*

1. Agenda
2. Colleges, voordrachten en cursussen
3. Personalia
4. Vacature

\*\*\*\*\*

1. Agenda

Van de met \* aangeduid activiteiten vindt men bijzonderheden in de rubriek Colleges, voordrachten en cursussen.

\*\*\*\*\*

22-6	UU: Talk by Paul Hovland (Argonne National Laboratories, USA) on: <i>Some combinatorial problems in derivative computation</i> 15.30-16.30 hr in HFG 611, Budapestlaan 6, De Uithof, Utrecht Abstract: We discuss some combinatorial problems arising in the efficient computation of derivatives. In one problem, given a directed acyclic graph (DAG) representation of a function, we seek to transform the DAG into an equivalent bipartite graph at minimal cost. In a related problem, we seek to transform the DAG into an equivalent DAG with the smallest possible number of edges. We describe heuristics and integer programming formulations for both problems. In both discrete and continuous adjoint methods for derivative computation, one must often trade recomputation for storage. We discuss some combinatorial problems arising from this tradeoff, focusing on the case where intermediate state might be written to both memory and disk.
24/26-6	Frankrijk: 26 <sup>th</sup> Rencontres arithmetiques de Caen: Geometry and Arithmetic over Local and Global Fields Location: Laboratoire de Mathématiques Nicolas Oresme <a href="#">Website</a>
25-6	UU: Stafcolloquium Spreker: Martijn Kool (Utrecht) <i>Enumerative geometry: from Ancient Greeks to Modern Physicists</i> 15.30-16.30 hr, room 611 (Hans Freudenthal building, formerly known as the Wiskunde/Maths building, campus De Uithof), Budapestlaan 6 The lecture is preceded by coffee, tea, and cookies from 15 to 15.30 hr, in the same room. <a href="#">Website</a>
3/15-7	Chiang Mai, Thailand: Internationale Wiskunde Olympiade <a href="#">Website</a>
6/10-7	VUA: European meeting of Statisticians The program consists of invited and contributed lectures, and posters, addressing a full range of subjects in statistics and its many applications.

Sponsored by the European Regional Committee of the Bernoulli Society. [Website](#)

- 17/20-8 \*Oxford, UK: Young Researchers in Mathematics Conference 2015 (YRM2015)
- 21/22-8 Amsterdam, CWI: Vakantiecursus 2015 - *Dit is triviaal*  
[Website](#), [e-mail](#)
- 28/29-8 Eindhoven: Vakantiecursus 2015 - *Dit is triviaal*  
[Website](#), [e-mail](#)
- 15/19-9 Hay-on-Wye, UK: LMS-CMI Research School "Diophantine Equations"  
The course will take the format of three 6-hour mini-courses,  
supported by exercise classes.  
[Website](#), [email](#)
- 18-9 Eindhoven: Finale Nederlandse Wiskunde Olympiade 2015  
Organisator: Nederlandse Wiskunde Olympiade.  
[Website](#), [email](#).
- 21/23-9 Warwick, UK: Workshop Non-Reversible Markov Chains for Monte-Carlo Sampling  
Organizers: Joris Bierkens and Gareth Roberts  
Workshop description:  
Markov Chain Monte Carlo (MCMC) methods are of fundamental importance to various scientific fields, such as statistics, statistical physics, molecular dynamics and machine learning.  
Keynote speakers:  
- Grigoris Pavliotis, Imperial College London, UK  
- Chii-Ruey Hwang, Academia Sinica, Taiwan  
- Marija Vucelja, The Rockefeller University Center, New York, USA  
- Ravi Montenegro, UML, USA  
- Luc Rey-Bellet, University of Massachusetts, USA  
- Natesh Pillai, Harvard University, USA  
- Alexandros Beskos, University College London, UK  
- Michael Betancourt, University of Warwick, UK  
- Tony Lelièvre, Ecole des Ponts ParisTech  
Registration is now open for the CRISM workshop.  
Those wishing to present a poster of their research, are welcome to submit a poster abstract [here](#).  
[Website](#), [email](#)
- 23/30-9 \*Bordeaux, France: ECC 2015
- 7/9-10 Zeist: Vooraankondiging 40-ste Woudschotenconferentie  
Keynote speakers:  
Margot Gerritsen (Stanford University, VS),  
Des Higham (University of Strathclyde, Engeland), Tamara G. Kolda (Sandia National Laboratories, VS), Cleve Moler (MathWorks, VS), Philip L. Roe (University of Michigan, VS), Gerhard Wanner (Université de Genève, Zwitserland).  
[Website](#)
- 22-10 Institut Henri Poincaré, Paris: Celebration of the 25th anniversary of the European Mathematical Society "Challenges for the next 25 years"  
Speakers: Hendrik Lenstra (Leiden, the Netherlands), Laure Saint-Raymond (ENS Paris, France), László Lovász (Budapest, Hungary), and Andrew Stuart (Warwick, UK).  
[Website](#)
- 28/30-10 TUD: Automatic sequences, number theory, aperiodic order  
Speakers include:  
Boris Adamczewski (Marseille), Michael Baake (Bielefeld), Henk Bruin (Vienna), Alan Haynes (York), Steve Hurder (Chicago),

Hendrik Lenstra (Leiden), Stefano Marmi (SNS Pisa), Robert Osburn (Dublin), Michel Rigo (Liege), Jeff Shallit (Waterloo), Joern Steuding (Wurzburg), Reem Yassawi (Trent U, Peterborough).  
[Website](#), [email](#).

- 12-11      Utrecht: Symposium Gerard Sleijpen 65  
Organisatoren: Rob Bisseling en Paul Zegeling (UU), Martin van Gijzen (TUD), Rob Stevenson (UvA)
- 13-11      Eindhoven: Prijsuitreiking Nederlandse Wiskunde Olympiade 2015  
Organisator: Nederlandse Wiskunde Olympiade  
[Website](#), [email](#).
- 13-11      Landelijk: Wiskunde B-dag  
Organisator: Freudenthal Instituut  
[Website](#), [e-mail](#).
- 22/23-3-2016    Amsterdam: BeNeLuxMC2016
- 8-4-2016       \*UvA: Congres Leve de Wiskunde!
- 6/16-7-2016     Hong Kong, China: Internationale Wiskunde Olympiade

\*\*\*\*\*

## 2. Colleges, voordrachten en cursussen

UvA

Leve de Wiskunde!

Datum: vrijdag 8 april 2016, Univ. van Amsterdam

Organisator: Universiteit van Amsterdam [e-mail](#).

Het jaarlijkse wiskundecongres van de Universiteit van Amsterdam geeft inzicht in actuele ontwikkelingen in het vakgebied. Wetenschappers vertellen over hun onderzoek in en rondom de wiskunde. Het congres betreft een gehele dag met korte lezingen.

Leve de Wiskunde! is kosteloos toegankelijk voor alle belangstellenden. In het bijzonder zijn wiskundedocenten en 5- en 6-vwo leerlingen van harte welkom. [Website](#).

Oxford, UK

Young Researchers in Mathematics Conference 2015 (YRM2015)

Date/location: August 17th-20<sup>th</sup>, 2015, Andrew Wiles Building- Mathematical Inst. Univ. Oxford, Oxford

The YRM2015 conference is primarily intended for PhD students in Mathematics and related disciplines (Statistics, Computer Science, Physics, etc.). Other early-career researchers are also very welcome (e.g. Master students with some research experience, Post-Docs, etc.).

There will be talks by young researchers, plenary and keynote talks by distinguished speakers across Mathematics, a poster competition, and a Quantitative Finance workshop from G-research.

All participants are invited to give a short (15 minutes + 5 minutes for questions) talk on their research. These talks will be organised into tracks which reflect different fields of research.

[Web page](#), [registration](#), [FAQs](#)

Bordeaux, France

ECC 2015 Elliptic Curve Cryptography 2015 (ECC 2015)

Dates: Summer school: [September 23-25](#)

Workshop: [September 28-30](#)

[Website](#), [email](#)

EARLY BIRD PREREGISTRATION ENDS THIS WEEK!

ECC 2015 is the 19th in a series of annual workshops dedicated to the study of elliptic curve cryptography and related areas. Over the past years the ECC conference series has broadened its scope beyond elliptic curve cryptography and now covers a wide range of areas within modern cryptography.

For instance, past ECC conferences included presentations on hyperelliptic curve cryptography, pairing-based cryptography, side-channel attacks, voting protocols, quantum key distribution, AES, hash functions and implementation issues. At the same time ECC continues to be the premier conference on elliptic curve cryptography. It is hoped that ECC 2015 will further our mission of encouraging and stimulating research on the security and implementation of elliptic curve cryptosystems and related areas, and that it will encourage collaboration between mathematicians, computer scientists and engineers in the academic, industry and government sectors.

There will be about fifteen invited lectures (and no contributed talks) delivered by internationally leading experts, giving both state-of-the-art survey lectures as well as presentations of latest research developments.

This year, there will also be a panel discussion on standardisation of elliptic curves for cryptography.

There will be a rump session at the conference on [Monday](#) evening, where participants can give short and entertaining presentations of recent results, work in progress, or make announcements of interest to attendees. A call for submissions for the rump session will be issued to registrants before the event.

The following invited speakers have already confirmed their participation:  
Léo Ducas (CWI, Netherlands): *Recovering Short Generators of Principal Ideals in Cyclotomic Rings*; Steven Galbraith (University of Auckland, New Zealand): *Algorithms for the ECDLP*, Christian Grothoff (INRIA Rennes-Bretagne-Atlantique, France): *Cryptography in GNUnet: Protocols for a Future Internet for Libre Societies*; Aurore Guillevic (École polytechnique and INRIA Saclay-Île-de-France, France): *Computing discrete logarithms faster in  $F_{p^n}$  with the Number Field Sieve algorithm*;

Michael Hamburg (Cryptography Research, USA), Michiel Kosters (Nanyang Technological University, Singapore), Juliane Krämer (Technische Universität Darmstadt, Germany), Enea Milio (INRIA Bordeaux-Sud-Ouest, France): *Computation of modular polynomials in dimension 2*;

Cécile Pierrot (CNRS, DGA and Sorbonne Universités, UPMC, France): *Discrete Logarithms in Medium Characteristic Finite Fields*;

Peter Schwabe (Radboud University, Netherlands): *Verifying ECC software*;

Katherine Stange (University of Colorado, USA), Arnaud Tisserand (CNRS, Université de Rennes and INRIA-Bretagne-Atlantique, France).

Abstracts are available on the conference web site.

The conference is preceded by a summerschool on elliptic curve cryptology and related areas of interest for the conference. Courses are intended for students preparing a master or doctoral degree.

Preregistration is now open at the conference web site. There are no registration fees for the summer school or the conference, but we have to limit the number of participants; so we will contact you after the preregistration to confirm whether your application has been accepted, and will ask you for a final confirmation of your participation.

Early bird preregistration: [June 19](#)

Early bird notification: [June 22](#)

Late preregistration: [August 12](#) (within the limits of available places)

Late notification: [August 14](#)

Andreas Enge and Damien Robert, for the local organising committee

\*\*\*\*\*

### 3. Personalia

Kobus Oosterhoff overleden

Op 27 mei 2015 is Jacobus Oosterhoff op de leeftijd van 82 jaar overleden.

Hij was van 1974 tot zijn emeritaat in 1996 hoogleraar Mathematische

Statistiek aan de VU.

Verschillende malen was hij hoofd van de afdeling Wiskunde van de VU, en decaan van de toenmalige Faculteit Wiskunde en Informatica.

Hij heeft een belangrijke bemiddelende rol gespeeld bij de overgang, eind 2005, van Uitgeverij Epsilon naar het KWG.

\*\*\*\*\*

### 4. Vacature

Dear Colleagues,

I will be joining the \*/School of Mathematical Sciences/ of /Monash University/\* (Melbourne, Australia) in [August 2015](#), as part of the School's expansion across broad areas of Mathematics, including computational mathematics.

I wanted to draw your attention to /\*several current openings for senior faculty positions (associate professor/full professor) in applied mathematics\*/ in the School:

<http://jobs.monash.edu.au/jobDetails.asp?sJobIDs=534771>

Outstanding candidates are sought in all areas of applied mathematics;

/\*numerical analysis and scientific computing are listed among the areas of specific interest/\*

(this includes numerical PDEs, numerical linear algebra, numerical optimization, computational finance, computational statistics, uncertainty quantification, data science, etc.).

Monash is a leading Australian research university that is globally ranked in the top 100, and Melbourne is recognized as being a great place to live.

/\*If you know of someone who may be interested, please forward them this message and the link above.\*/

Applications close Thursday 2 July 2015 (with apologies for the late notice...).

It is expected that several additional openings at more junior levels(Lecturer/Senior Lecturer, continuing appointments) will be advertised later this summer.

Thank you and best regards,

Hans De Sterck

Department of Applied Mathematics,  
University of Waterloo  
phone:[519-888-4567](tel:519-888-4567) ext 37550

\*\*\*\*\*

einde Mededelingen