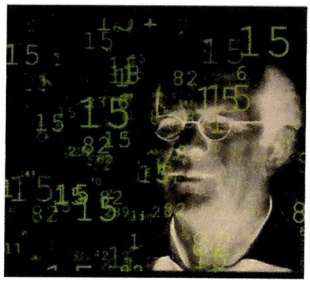
Workshop on Computational Number Theory

on the occasion of Herman te Riele's retirement from CWI Amsterdam



CWI Amsterdam, The Netherlands
December 1 - 2, 2011

Program

Thursday, December 1	
Location: **Turing room, WCW congress center (next to CWI), Science Park 125, Amsterdam**	
12:00	Lunch (provided)
13:20	Opening Remarks
Session: Factoring Large Numbers (Chair: Paul Zimmermann)	
13:30	Paul Leyland
14:00	Peter Montgomery
14:30	Joppe Bos
15:00	*Tea Break*
15:30	Jason Papadopoulos
16:00	Thorsten Kleinjung
16:30	Alexander Kruppa
17:00	*Closing*

Friday, December 2	
Location: **Turing room, WCW congress center (next to CWI), Science Park 125, Amsterdam**	
10:50	Welcome and opening
Session: Computations on Zeta and Other Functions (Chair: Herman te Riele)	
11:00	Joost Batenburg
11:30	Rob Tijdeman
12:00	Pieter Moree (1)
12:30	Lunch (provided)
14:00	Pieter Moree (2)
14:30	Andrew Odlyzko
Social Session	
15:00	*Farewell Speeches (by Herman himself and others)*
16:00	*Reception (ground floor of the new CWI building)*

Paul Leyland (Brnikat Ltd, Cambridge, UK)
A History of Factoring in the Real World

The integer factorization problem has been been of interest to mathematicians for well over two thousand years. For almost all of that time, it was of almost no interest to any other section of society and had almost no practical use whatsoever. In recent decades, integer factorization has transformed itself into being of interest to thousands, at least. It has also become of immense practical use and of great economic importance. In my talk I will describe how and why this remarkable change occurred. The emphasis will be on the economics, politics and social impact rather than the underlying mathematics, fascinating though that may be to mathematicians.

Peter Montgomery (Microsoft Research, Redmond, WA, USA, and CWI)

Early History of the Number Field Sieve

The Number Field Sieve (NFS) demonstrated its power in 1990, when it factored a cofactor of the ninth Fermat number $2^{512}+1$. I joined Oregon State University (OSU) 1992–1993 to research and implement NFS. The work continued at Centrum Wiskunde & Informatica (CWI) 1993–1994. In spring, 1994, we completed two big factorizations started at OSU a year earlier. Soon we were swamped with results other algorithm had missed.

Joppe Bos (EPFL, Switzerland)
Recent Developments in ECM

In this talk we outline how we obtained the 73-digit record factors using the fast parallel arithmetic designed to run on our PlayStation3 cluster inside a modified GMP-ECM implementation. Furthermore, we discuss some modifications to ECM when using Edwards curves on parallel architectures.

Jason Papadopoulos (3S Group Inc.)

High-performance optimization of GNFS polynomials

Modern algorithms that search for polynomials for use with the General Number Field Sieve now routinely generate candidates whose high-order coefficients are very highly skewed. This drastically increases the amount of work needed to further optimize both the size and root properties of each candidate. I will describe several techniques that can cope with the large search space and numerical difficulty that is a consequence of large skewness, as implemented in the Msieve factorization library. Examples will be given from a 2011 internet search for a substitute to the polynomial used to factor RSA768 in 2010.

Thorsten Kleinjung (EPFL, Switzerland)

Filtering and the matrix step in NFS

The matrix step is one of the main computational steps in NFS (number field sieve). It is more difficult to parallelise than the other main computational step (sieving), and its complexity depends on the outcome of the filtering step. For larger and larger numbers many matrix related problems arise. These will be addressed in the talk and strategies to reduce or circumvent them will be discussed.

Alexander Kruppa (CWI, Amsterdam)

Comparison of the Block Wiedemann with the Block Lanczos algorithm for the linear algebra step in NFS

We report on optimization efforts of the Block-Lanczos algorithm for the Power6-based Huygens supercomputer at SARA, compare its performance to Block-Wiedemann and evaluate its practical applicability to factorizations of size like RSA768 and possibly larger.

Joost Batenburg (Vision Lab, Univ. of Antwerp and CWI, Amsterdam)
Discrete tomography for lattice images: a journey through Mathematics

Tomography deals with the reconstruction of grey level images from their projections. In discrete tomography, it is assumed that the unknown image only contains grey levels from a small, discrete set. If one additionally assumes that the image is defined on a discrete domain, we arrive at the field of discrete tomography for lattice images.
Recently, tomography problems for lattice images have become of high practical relevance, due to their applicability to the reconstruction of nanocrystals at atomic resolution from projections obtained by electron microscopy.
Although the reconstruction problem for lattice images appears quite elementary at first sight, it turns out to be both elegant and complex. The problem has links with many different subfields of

mathematics, ranging from number theory and combinatorics to continuous optimization and analysis. In each of these directions, interesting and sometimes surprising results have been obtained during the past 10 years.
In this lecture I will illustrate the links of this tomography problem with different fields from mathematics and highlight some important results, followed by posing some new research questions that are currently unsolved.

Pieter Moree (Max Planck Institute for Mathematics, Bonn, Germany)

Talk 1: The Erdős-Moser conjecture

The conjecture claims that the Diophantine equation $1^k+...+(m-1)^k=m^k$ has only $1^1+2^1=3^1$ as solution. Moser showed by elementary arguments in 1953 that if (m,k) is a further solution, then $k>10^{10^6}$. By a completely different method involving the computation of log 2 with many digits of accuracy, Moser's result was improved in 2011 to $m>10^{10^9}$. This is joint work with Yves Gallot and Wadim Zudilin and depends crucially on earlier work by Herman te Riele.

Talk 2: Euler-Kronecker constants: from Ramanujan to Ihara

Given an L-series that has a series expansion around $s=1$ starting as $c_1(s-1)^\alpha+c_2+...$, one can define its Euler-Kronecker constant as c_2/c_1. Ramanujan in his `unpublished' manuscript on the Ramanujan tau-function made various conjectures on Euler-Kronecker constants. In case the L-series is the Dedekind zeta function, $\zeta_K(s)$, of a number field K (in which case $\alpha=-1$), this constant has been intensively studied by Ihara (of the Ihara zeta function) and his collaborators. We show amongst others that, assuming some widely believed conjectures, a conjecture made by Ihara in case $K=\mathbf{Q}(\zeta_q)$ is a cyclotomic field, q a prime, is false. We also deal with the analogue of Ramanujan's conjectures for these fields. (Joint work with Kevin Ford and Florian Luca.)

Andrew Odlyzko (University of Minnesota, USA)

Computation and the Riemann Hypothesis

Extensive computations of zeros of the Riemann zeta function started as soon as it was realized that the Riemann Hypothesis was an important and a difficult problem. But the meaning of "extensive" changed with improvements in algorithms and hardware, so the latest results cover 12 orders of magnitude more than the earliest ones. What have we learned? And what can we hope to learn?

Rob Tijdeman (Leiden University)

Smooth numbers

Smooth numbers are numbers composed of (relatively) small primes. They play an important part in many problems, for example with the factorization of large numbers. The number of positive integers at most x with all its prime factors less than y is usually denoted by the function Psi(x,y). Hardy and Littlewood and others gave formulas in case y is much smaller than x. Ramaswami and De Bruijn gave estimates in case y is a fixed power of x. De Bruijn further indicated how both cases fit together around y= ln x. I shall summarize the history and then go into later developments and variants to which former students of Herman te Riele and me have made some contributions.

CWI

Centrum Wiskunde & Informatica

Workshop on Computational Number Theory

on the occasion of Herman te Riele's retirement from CWI

Location: Turing room
Date: 1 – 2 december 2011

Program

Thursday, 1 December

12:00 Lunch
13:30 Opening

Session: Factoring large numbers

13:30 **Paul Leyland** (Brnikat Ltd., Cambridge)
14:00 **Peter Montgomery** (Microsoft US)
14:30 **Joppe Bos** (EPFL)
15:00 **Tea Break**
15:30 **Jason Papadopoulos** (3S Group Inc)
16:00 **Thorsten Kleinjung** (EPFL)
16:30 **Alexander Kruppa** (CWI)
17:00 **Closure**

Friday, 2 December

10:50 **Welcome**

Session: Computations on zeta and other functions

11:00 **Joost Batenburg** (CWI)
11:30 **Rob Tijdeman** (Universiteit Leiden)
12:00 **Pieter Moree (1)** (Max Planck Institute, Bonn)
12:30 **Lunch**
14:00 **Pieter Moree (2)**
14:30 **Andrew Odlyzko** (University of Minnesota)

Social session

15:00 **Farewell speeches** (by Herman himself and others)
16:00 **Reception** (ground floor new wing CWI building)