Mahler Lecture 2003

Galois Theory and Primality Testing

Hendrik Lenstra Jr.
(AustMS Kurt Mahler Lecturer 2003)

Friday, June 20, 2pm

Carslaw 373, University of Sydney

Abstract: It was recognized in the mid−eighties, that several then current primality tests could be formulated in the language of Galois theory for rings. This made it possible to combine those tests for practical purposes. It turns out that the new polynomial time primality test due to Agrawal, Kayal, and Saxena can also be formulated in the Galois theory language. Whether the new formulation will allow the test to be combined with the older tests remains to be seen. It does lead to a primality test with a significantly improved guaranteed run time exponent. In this test, one makes use of Gaussian periods instead of roots of unity. The lecture represents joint work with Carl Pomerance (Bell Labs).

See also:	http://magma.maths.usyd.edu.au/~bruin/Workshop/mahler.html

Note: While featuring in the Workshop Computational Arithmetic Geometry (June 18 − 20, University of Sydney), this lecture is aimed at a general mathematical audience. Also people who do not participate in the workshop are invited to attend.

Contact:
Nils Bruin
School of Mathematics
University of Sydney, NSW 2006
AUSTRALIA

email:	bruin@maths.usyd.edu.au
telephone:	+61 (2) 9351 4010
fax:	+61 (2) 9351 4534