ALGORITHMS FOR FINITE RINGS

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op woensdag 22 juni 2016
klokke 11:15 uur

door

Iuliana Ciocănea-Teodorescu
geboren te Boekarest, Roemenië
in 1990

Promotores: Prof. dr. Hendrik W. Lenstra (Universiteit Leiden)

Prof. dr. Karim Belabas (Université de Bordeaux)

Samenstelling van de promotiecommissie:

Dr. Owen Biesel (Universiteit Leiden)

Prof. dr. Bart de Smit (Universiteit Leiden)

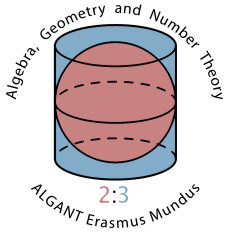
Prof. dr. Teresa Krick (Universidad de Buenos Aires)

Prof. dr. Lenny Taelman (Universiteit van Amsterdam)

Dr. Wilberd van der Kallen (Universiteit Utrecht)

Prof. dr. Aad van der Vaart (Universiteit Leiden)

This work was funded by Algant-Doc Erasmus Mundus and was carried out at Universiteit Leiden and l'Université de Bordeaux.



université de BORDEAUX

THÈSE

présentée à

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Iuliana CIOCĂNEA-TEODORESCU

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

Algorithmes pour les anneaux finis

Directeurs de recherche : Hendrik W. LENSTRA, Karim BELABAS

Soutenue le 22 juin 2016 à Leiden, devant la commission d'examen formée de :

LENSTRA, Hendrik W.	Professeur	Universiteit Leiden	Directeur
BELABAS, Karim	Professeur	Université de Bordeaux	Directeur
KRICK, Teresa	Professeur	Universidad de Buenos Aires	Rapporteur
TAELMAN, Lenny	Professeur	Universiteit van Amsterdam	Rapporteur
BIESEL, Owen	Docteur	Universiteit Leiden	Examinateur
DE SMIT, Bart	Professeur	Universiteit Leiden	Examinateur
VAN DER KALLEN, Wilberd	Docteur	Universiteit Utrecht	Examinateur

"Once [the reader] explicitly gives up all practical claims, he will realize that he can occupy himself with algorithms without having to fear the bad dreams caused by the messy details and dirty tricks that stand between an elegant algorithmic idea and its practical implementation. He will find himself in the platonic paradise of pure mathematics, where a conceptual and concise version of an algorithm is valued more highly than an ad hoc device that speeds it up by a factor of ten and where words have precise meanings that do not change with the changing world. (...) And in his innermost self he will know that in the end his own work will turn out to have the widest application range, exactly because it was not done with any specific application in mind."

H.W. Lenstra. Algorithms in Algebraic Number Theory (1992). *BAMS*, 26: 211–244

"If $\mathrm{P} = \mathrm{NP}$*, then the world would be a profoundly different place than we usually assume it to be. There would be no special value in creative leaps, no fundamental gap between solving a problem and recognizing the solution once it's found. Everyone who could appreciate a symphony would be Mozart; everyone who could follow a step-by-step argument would be Gauss (...)."*

Scott Aaronson. Personal blog: www.scottaaronson.com/blog/ (2006)

I died for beauty, but was scarce
Adjusted in the tomb,
When one who died for truth was lain
In an adjoining room.

Emily Dickinson. Fr 448, J 449 (1890)

Contents