

Cover Page



Universiteit Leiden



The handle <http://hdl.handle.net/1887/40676> holds various files of this Leiden University dissertation.

**Author:** Ciocanea Teodorescu, I.

**Title:** Algorithms for finite rings

**Issue Date:** 2016-06-22

# 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)

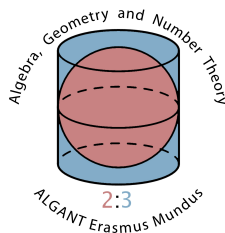
Prof. dr. Teresa Krick (Universidad de Buenos Aires)

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
TAEELMAN, Lenny	Professeur	Universiteit van Amsterdam	Rapporteur
BIESEL, Owen	Docteur	Universiteit Leiden	Examineur
DE SMIT, Bart	Professeur	Universiteit Leiden	Examineur
VAN DER KALLEN, Wilberd	Docteur	Universiteit Utrecht	Examineur



*“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  $P = NP$ , 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/](http://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

<b>Introduction</b>	<b>i</b>
<b>List of symbols</b>	<b>v</b>
<b>1 Background</b>	<b>1</b>
1.1 Algorithms and complexity . . . . .	1
1.2 Basic ring theory . . . . .	4
1.3 Basic module theory . . . . .	5
1.4 More ring theory . . . . .	7
1.5 Idempotents . . . . .	9
1.6 More module theory . . . . .	10
1.7 Quasi-Frobenius rings . . . . .	15
1.8 Frobenius algebras and symmetric algebras . . . . .	16
1.9 Duality . . . . .	17
<b>2 Linear algebra over <math>\mathbb{Z}</math>:</b>	
<b>basic algorithms for finite abelian groups</b>	<b>19</b>
2.1 Lattices . . . . .	20
2.2 Hermite and Smith normal forms . . . . .	22
2.3 Representing objects and basic constructions . . . . .	26
2.4 Homomorphism groups and tensor products . . . . .	33
2.5 Splitting exact sequences . . . . .	34
2.6 Torsion subgroups, exponents, orders, cyclic decompositions . . . . .	35
2.7 Homomorphism groups and tensor products reconsidered . . . . .	39
2.8 Projective $\mathbb{Z}/m\mathbb{Z}$ -modules . . . . .	40
<b>3 Linear algebra over <math>\mathbb{Z}</math>:</b>	
<b>basic algorithms for finite rings</b>	<b>45</b>
3.1 Representing objects and basic constructions . . . . .	46
3.2 Computations with ideals . . . . .	48
3.3 Computing the centre and the prime subring of a finite ring . . . . .	49
3.4 Computing the Jacobson radical . . . . .	50
3.5 Other known algorithms and open questions . . . . .	50



---

<b>4</b>	<b>The module isomorphism problem</b>	<b>53</b>
4.1	Introduction . . . . .	53
4.2	Context . . . . .	55
4.3	MIP via non-nilpotent endomorphisms . . . . .	56
4.4	MIP via an approximation of the Jacobson radical . . . . .	59
4.5	Remark on implementation and performance . . . . .	63
<b>5</b>	<b>A miscellaneous collection of algorithms</b>	<b>65</b>
5.1	Testing if a ring is a field . . . . .	65
5.2	Testing if a ring is simple . . . . .	66
5.3	Testing if a module is simple . . . . .	67
5.4	Testing if a module is projective . . . . .	67
5.5	Constructing projective covers . . . . .	68
5.6	Constructing injective hulls . . . . .	69
5.7	Testing if a module is injective . . . . .	70
5.8	Testing if a ring is quasi-Frobenius . . . . .	70
5.9	Constructive tests for existence of injective and surjective module homomorphisms . . . . .	70
<b>6</b>	<b>Approximating the Jacobson radical of a finite ring</b>	<b>75</b>
6.1	Introduction . . . . .	75
6.2	Separability . . . . .	76
6.3	An approximation of the Jacobson radical . . . . .	96
6.4	Computing the generalised prime subring . . . . .	111
	<b>Bibliography</b>	<b>115</b>
	<b>Index</b>	<b>123</b>
	<b>Abstract</b>	<b>125</b>
	<b>Résumé</b>	<b>126</b>
	<b>Samenvatting</b>	<b>127</b>
	<b>Acknowledgements</b>	<b>129</b>
	<b>CV</b>	<b>130</b>