Congruence properties of linear recurring sequences

Nicholas Crouch B.Sc. (Hons)

Submitted for the degree of Master of Science in
the University of Adelaide

August 2006
# Contents

Abstract .............................. iv

Statement ................................ vi

Acknowledgements ......................... vii

1 Introduction ................................ 1
   1.1 Preliminaries ................................ 1
   1.2 Classical pseudoprimes and related ideas .......... 2
   1.3 Second order linear recurring sequences .......... 4
   1.4 The general case ................................ 7
   1.5 The cubic case ................................ 8
   1.6 Outline of thesis ............................. 9

2 Preliminaries ................................ 11
   2.1 Introduction .................................. 11
   2.2 Rings and modules .............................. 11
   2.3 Polynomials over a ring ....................... 14
   2.4 The Galois group, norm, trace and discriminant .... 19
   2.5 Finite fields .................................. 22
   2.6 Factorization into prime ideals .................. 24
   2.7 The Frobenius and Artin automorphisms .......... 27

3 Linear Recurring Sequences .................. 29
   3.1 Introduction .................................. 29
   3.2 Linear recurring sequences over a ring .......... 29
   3.3 The v-sequence ................................ 31
### Contents

3.4 The $U$-matrix and the $u$-sequences ........................................ 34
3.5 The family $\mathcal{F}(f)$ of linear recurring sequences ................. 36
3.6 Periodicity ......................................................... 40
3.7 The $u$-sequences and interpolation ........................................... 40

4 The Test Matrix .......................................................... 43
4.1 Introduction ......................................................... 43
4.2 The number of irreducible factors over $\mathbb{Z}_p$ ............................ 43
4.3 The test matrix over $\mathbb{Z}_p$ ....................................... 46
4.4 The test matrix modulo $n$ ............................................ 49
4.5 The vanishing of the test matrix modulo $n$ ................................ 52
4.6 The Szekeres Condition and Column Zero ................................ 53
4.7 Sums of algebraic integers related to the test matrix ....................... 55
4.8 Gurak's Condition ................................................. 58
4.9 Permutation conditions ............................................... 59

5 The Test Matrix of a Cubic ............................................... 63
5.1 Introduction ......................................................... 63
5.2 Third order linear recurring sequences in a ring $R$ ......................... 63
5.3 Addition formulae over a ring $R$ .................................... 65
5.4 Factorization and the Galois group of a cubic $f(x)$ over $\mathbb{Z}_p$ .... 66
5.5 The test matrix of a cubic over $\mathbb{Z}_n$ ................................ 67
5.6 The test matrix over $\mathbb{Z}_p$ ....................................... 68
5.7 The test matrix modulo $n$ ............................................ 71
5.8 Tests on the $3 \times 3$ test matrix .................................... 74
5.9 Computer investigation ............................................... 76
5.10 Signature conditions of Adams and Shanks. ............................... 82
   5.10.1 Definitions ..................................................... 83
   5.10.2 Characterisation via permutations .................................. 85
   5.10.3 Numerical investigation by Adams, Shanks and colleagues ......... 86
5.11 Subsequent computation using test matrix ................................... 87
5.12 Auxiliary results for relation between tests ................................ 87
5.13 The Concise Condition .............................................. 91
<table>
<thead>
<tr>
<th>CONTENTS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5.14 Conclusion</td>
<td>96</td>
</tr>
<tr>
<td>A Prime Program Results</td>
<td>98</td>
</tr>
<tr>
<td>B Column Zero Program</td>
<td>100</td>
</tr>
<tr>
<td>C Results of Main Investigation Program</td>
<td>103</td>
</tr>
<tr>
<td>References</td>
<td>109</td>
</tr>
</tbody>
</table>
Abstract

This thesis deals with the behaviour modulo $n$ of linear recurring sequences of integers with characteristic polynomial $f(x)$, where $n$ is a positive integer and $f(x)$ is a monic polynomial of degree $k$. Let $\alpha_1, \alpha_2, \ldots, \alpha_k$ be the zeros of $f(x)$ and $D(f) \neq 0$ its discriminant. We focus on the $v$-sequence $(v_j)$, defined by $v_j = \alpha_1^j + \alpha_2^j + \ldots + \alpha_k^j$ for $j \geq 0$. Our main interest is in algebraic congruences modulo $n$ which hold when $n$ is a prime and which involve only terms of the sequence and rational integers. For $k = 1, 2$ such results have been used extensively in primality testing and have led to the study of various types of pseudoprimes. For $k = 3$, such results have been studied by Adams and Shanks (1) under the further assumption $f(0) = -1$. For general $k$, quite different approaches have been taken by Gurak (2) and Szekeres (3).

The infinite test matrix modulo $n$ is the infinite matrix $M$ with rows and columns numbered $0, 1, 2, \ldots$ whose $(i, j)$ entry is $m_{i,j}$, the least residue modulo $n$ of

$$v_{i+j} - v_{i+j} \quad \text{for } i \geq 0 \text{ and } j \geq 0.$$ 

We study the congruence properties of $M$ and especially of the $k \times k$ submatrix $M^{(k)}$ determined by rows and columns $0$ to $k - 1$.

Chapters 1 and 2 introduce the thesis and summarise auxiliary results.

Chapter 3 presents background on linear recurring sequences with an emphasis on the matrix approach, including the $v$-sequence and the $k$ “$u$-sequences” (whose initial vectors are the rows of $I_k$).

Chapter 4 comprises theoretical study of the properties of $M$ for a general $k$, both when $n$ is a prime and for general $n$, together with investigation of the condition of Gurak (2). For $(n, k!D(f)) = 1$, we show that the condition of Szekeres is equivalent to the condition that $m_{i0} = 0$ for $1 \leq i \leq k$ and also to certain permutation conditions. Gurak's condition is then described using these conditions.

Chapter 5 assumes $k = 3$. For this case we study congruences modulo $n$ satisfied by the $m_{ij}$ when $n$ is a prime, and hence develop a combination of tests on $M^{(3)}$ which are passed by all primes. We report on extensive computer investigation of composites passing these tests. Such composites are found to be rare. Investigation of the relevant work of Adams and Shanks and colleagues, together with use of the permutation condition of Chapter 4, leads to a modification of the earlier tests on $M^{(3)}$. Under suitable assumptions we show that the new modified condition is equivalent to the basic condition of Adams and Shanks and also to that of Gurak but has significant advantages over both.

continued page v.
References


Statement

This thesis contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution and to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference is made in the text of the thesis.

I give consent to this copy of my thesis, when deposited in the University Library, being made available for loan and photocopy.

Nicholas Errol Crouch
Acknowledgements

I first wish to express my gratitude to my supervisor Dr Jane Pitman, for suggesting helpful ideas and providing careful criticism at all stages. Further, Sections 4.9, 5.12 and 5.13 are based on joint work with Dr Pitman. I would also like to thank Dr R.J. Clarke for his detailed comments on the final version of this thesis.

I wish to acknowledge the influence of the late Professor George Szekeres, for his advice and inspiration during the early stages of this thesis. Similarly my thanks go to Professor Hugh Williams for his helpful comments during his two visits to Adelaide.

I would like to thank Jason Whyte for his assistance and advice. In addition I would like to thank the following people for help with computing matters, David Beard, Paul McCann, Sue Gray, Jim Denier and Francis Vaughan.