

Mathematical  
Surveys  
and  
Monographs

Volume 104

# Recurrence Sequences

Graham Everest  
Alf van der Poorten  
Igor Shparlinski  
Thomas Ward



American Mathematical Society

## EDITORIAL COMMITTEE

Jerry L. Bona  
Peter S. Landweber, Chair  
Michael P. Loss  
Tudor Stefan Ratiu  
J. T. Stafford

2000 *Mathematics Subject Classification*. Primary 11B37, 11B39, 11G05, 11T23, 33B10, 11J71, 11K45, 11B85, 37B15, 94A60.

---

For additional information and updates on this book, visit  
[www.ams.org/bookpages/surv-104](http://www.ams.org/bookpages/surv-104)

---

### Library of Congress Cataloging-in-Publication Data

Recurrence sequences / Graham Everest . . . [et al].  
p. cm. — (Mathematical surveys and monographs, ISSN 0076-5376 ; v. 104)  
Includes bibliographical references and index.  
ISBN 0-8218-3387-1 (alk. paper)  
1. Recurrent sequences (Mathematics) I. Everest, Graham, 1957- II. Series.

QA246.5.R43 2003  
512'.72—dc21

2003050346

---

**Copying and reprinting.** Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy a chapter for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, Rhode Island 02904-2294, USA. Requests can also be made by e-mail to [reprint-permission@ams.org](mailto:reprint-permission@ams.org).

© 2003 by the American Mathematical Society. All rights reserved.

The American Mathematical Society retains all rights  
except those granted to the United States Government.

Printed in the United States of America.

∞ The paper used in this book is acid-free and falls within the guidelines  
established to ensure permanence and durability.

Visit the AMS home page at <http://www.ams.org/>

10 9 8 7 6 5 4 3 2 1 08 07 06 05 04 03

# Contents

|   |                     |
|---|---------------------|
| <a href="#">Notation</a>  | <a href="#">vii</a> |
| Introduction  | ix                  |
| Chapter 1. Definitions and Techniques   | 1                   |
| 1.1. Main Definitions and Principal Properties  | 1                   |
| 1.2. $p$ -adic Analysis   | 12                  |
| 1.3. Linear Forms in Logarithms   | 15                  |
| 1.4. Diophantine Approximation and Roth's Theorem                                     | 17                  |
| 1.5. Sums of $S$ -Units   | 19                  |
| Chapter 2. Zeros, Multiplicity and Growth   | 25                  |
| 2.1. The Skolem–Mahler–Lech Theorem   | 25                  |
| 2.2. Multiplicity of a Linear Recurrence Sequence                                     | 26                  |
| 2.3. <a href="#">Finding the Zeros of Linear Recurrence Sequences</a>                 | <a href="#">31</a>  |
| 2.4. <a href="#">Growth of Linear Recurrence Sequences</a>                            | <a href="#">31</a>  |
| 2.5. Further Equations in Linear Recurrence Sequences                                 | 37                  |
| Chapter 3. Periodicity  | 45                  |
| 3.1. Periodic Structure   | 45                  |
| 3.2. Restricted Periods and Artin's Conjecture  | 49                  |
| 3.3. <a href="#">Problems Related to Artin's Conjecture</a>                           | <a href="#">52</a>  |
| 3.4. The Collatz Sequence   | 61                  |
| <a href="#">Chapter 4. Operations on Power Series and Linear Recurrence Sequences</a> | <a href="#">65</a>  |
| 4.1. <a href="#">Hadamard Operations and their Inverses</a>                           | <a href="#">65</a>  |
| 4.2. <a href="#">Shrinking Recurrence Sequences</a>                                   | <a href="#">71</a>  |
| 4.3. Transcendence Theory and Recurrence Sequences                                    | 72                  |
| <a href="#">Chapter 5. Character Sums and Solutions of Congruences</a>                | <a href="#">75</a>  |
| 5.1. <a href="#">Bounds for Character Sums</a>  | <a href="#">75</a>  |
| 5.2. <a href="#">Bounds for other Character Sums</a>                                  | <a href="#">83</a>  |
| 5.3. <a href="#">Character Sums in Characteristic Zero</a>                            | <a href="#">85</a>  |
| 5.4. Bounds for the Number of Solutions of Congruences                                | 86                  |
| <a href="#">Chapter 6. Arithmetic Structure of Recurrence Sequences</a>               | <a href="#">93</a>  |
| 6.1. <a href="#">Prime Values of Linear Recurrence Sequences</a>                      | <a href="#">93</a>  |
| 6.2. Prime Divisors of Recurrence Sequences   | 95                  |
| 6.3. Primitive Divisors and the Index of Entry  | 103                 |
| 6.4. Arithmetic Functions on Linear Recurrence Sequences                              | 109                 |
| 6.5. Powers in Recurrence Sequences   | 113                 |

|   |                     |
|---|---------------------|
| Chapter 7. Distribution in Finite Fields and Residue Rings        | 117                 |
| 7.1. Distribution in Finite Fields                                | 117                 |
| 7.2. Distribution in Residue Rings                                | 119                 |
| Chapter 8. Distribution Modulo 1 and Matrix Exponential Functions | 127                 |
| 8.1. Main Definitions and Metric Results                          | 127                 |
| 8.2. Explicit Constructions                                       | 130                 |
| 8.3. Other Problems   | 134                 |
| Chapter 9. Applications to Other Sequences                        | 139                 |
| 9.1. Algebraic and Exponential Polynomials                        | 139                 |
| 9.2. Linear Recurrence Sequences and Continued Fractions          | 145                 |
| 9.3. Combinatorial Sequences                                      | 150                 |
| 9.4. Solutions of Diophantine Equations                           | 157                 |
| Chapter 10. Elliptic Divisibility Sequences                       | 163                 |
| 10.1. Elliptic Divisibility Sequences                             | 163                 |
| 10.2. Periodicity   | 164                 |
| 10.3. Elliptic Curves   | 165                 |
| 10.4. Growth Rates  | 167                 |
| 10.5. Primes in Elliptic Divisibility Sequences                   | 169                 |
| 10.6. Open Problems   | 174                 |
| Chapter 11. Sequences Arising in Graph Theory and Dynamics        | 177                 |
| 11.1. Perfect Matchings and Recurrence Sequences                  | 177                 |
| 11.2. Sequences arising in Dynamical Systems                      | 179                 |
| Chapter 12. Finite Fields and Algebraic Number Fields             | 191                 |
| 12.1. Bases and other Special Elements of Fields                  | 191                 |
| 12.2. Euclidean Algebraic Number Fields                           | 196                 |
| 12.3. Cyclotomic Fields and Gaussian Periods                      | 202                 |
| 12.4. Questions of Kodama and Robinson                            | 205                 |
| Chapter 13. Pseudo-Random Number Generators                       | 211                 |
| 13.1. Uniformly Distributed Pseudo-Random Numbers                 | 211                 |
| 13.2. Pseudo-Random Number Generators in Cryptography             | 220                 |
| Chapter 14. Computer Science and Coding Theory                    | 231                 |
| 14.1. Finite Automata and Power Series                            | 231                 |
| 14.2. Algorithms and Cryptography                                 | 241                 |
| 14.3. Coding Theory   | 247                 |
| Sequences from the on-line Encyclopedia                           | 255                 |
| <a href="#">Bibliography</a>                                      | <a href="#">257</a> |
| <a href="#">Index</a>   | <a href="#">309</a> |

