Mathematical
Surveys
and
Monographs

Volume 104

Recurrence Sequences

Graham Everest
Alf van der Poorten
Igor Shparlinski
Thomas Ward

American Mathematical Society

http://dx.doi.org/10.1090/surv/104

Recurrence Sequences

Mathematical
Surveys
and
Monographs

Volume 104

Recurrence Sequences

Graham Everest
Alf van der Poorten
Igor Shparlinski
Thomas Ward

American Mathematical Society

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

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

∞ 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

Notation

Particular notation used is collected at the start of the index; some general notation is described here.

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}_+$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the natural numbers, integers, non-negative integers, rational numbers, real numbers, and complex numbers, respectively;
- $\mathbb{Q}_p$, $\mathbb{Z}_p$, $\mathbb{C}_p$ denote the p-adic rationals, the p-adic integers, and the completion of the algebraic closure of $\mathbb{Q}_p$, respectively;
- $\operatorname{ord}_p z$ is the p-adic order of $z \in \mathbb{C}_p$;
- $\mathbb{P}$ is the set of prime numbers;
- $\mathcal{R}$ is a commutative ring with 1;
- $\mathbb{F}_q$ is a field with $q = p^r$ elements, $p \in \mathbb{P}$, $r \in \mathbb{N}$, and $\mathbb{F}_q^*$ is its multiplicative group;
- $\mathbb{F}_p$, $p \in \mathbb{P}$ is identified with the set $\{0, 1, \dots, p-1\}$;
- given a field $\mathbb{F}$, $\overline{\mathbb{F}}$ denotes the algebraic closure of $\mathbb{F}$; thus $\overline{\mathbb{Q}}$ is the field of all algebraic numbers;
- for any ring $\mathcal{R}$, $\mathcal{R}[X]$, $\mathcal{R}(X)$, $\mathcal{R}[[X]]$, $\mathcal{R}((X))$ denote the ring of polynomials, the field of rational functions, the ring of formal power series, and the field of formal Laurent series over $\mathcal{R}$, respectively;
- $\mathbb{Z}_{\mathbb{K}}$ denotes the ring of integers of the algebraic number field $\mathbb{K}$;
- $H(f)$ denotes the naïve height of $f \in \mathbb{Z}[x_1, \dots, x_m]$, that is, the greatest absolute value of its coefficients;
- $\gcd(a_1, \dots, a_k)$ and $\operatorname{lcm}(a_1, \dots, a_k)$ respectively denote the greatest common divisor and the least common multiple of $a_1, \dots, a_k$ (which may be integers, ideals, polynomials, and so forth);
- ε denotes any fixed positive number (for example, the implied constants in the symbol O may depend on ε);
- δ_{ij} denotes Kronecker's δ-function: $\delta_{ij} = 1$ if $i = j$, and $\delta_{ij} = 0$ otherwise;
- $\mu(k)$, $\varphi(k)$, $\tau(k)$, $\sigma(k)$ respectively denote the Möbius function, the Euler function, the number of integer positive divisors of k, and the sum of the integer positive divisors of k, where k is some non-zero integer;
- $\nu(k)$, $P(k)$, $Q(k)$ respectively are the number of distinct prime divisors of k, the greatest prime divisor of k, and the product of the prime divisors of k; thus, for example: $\nu(12) = 2$, $P(12) = 3$, and $Q(12) = 6$;
- for a rational $r = k/\ell$ with $\gcd(k, \ell) = 1$, $P(r) = \max\{P(k), P(\ell)\}$ and $Q(r) = \max\{Q(k), Q(\ell)\}$;
- $\pi(x)$ is the number of prime numbers not exceeding x;
- $|X|$ denotes the cardinality of the set X;
- $\log x = \log_2 x$, $\ln x = \log_e x$;
- $\operatorname{Log} x = \log x$ if $x > 2$, and $\operatorname{Log} x = 1$ otherwise;

- a constant is *effective* if it can be computed in a finite number of steps from starting data;
- $C(\lambda_1, \lambda_2, \dots)$ or $c(\lambda_1, \lambda_2, \dots)$ denotes a constant depending on the parameters $\lambda_1, \lambda_2, \dots$. Such constants may be supposed to be effective, unless it is pointed out explicitly that they are not;
- a statement $S(x)$ is true for almost all $x \in \mathbb{N}$ if the statement holds for $N + o(N)$ values of $x \leq N$, $N \to \infty$. Similarly, a statement $S(p)$ is true for almost all $p \in \mathbb{P}$ if it holds for $\pi(N) + o(\pi(N))$ values of $p \leq N$, $N \to \infty$;
- the symbol $\Box$ denotes the end of a proof.

Introduction

The importance of recurrence sequences hardly needs to be explained. Their study is plainly of intrinsic interest and has been a central part of number theory for many years. Moreover, these sequences appear almost everywhere in mathematics and computer science. For example, the theory of power series representing rational functions [**1026**], pseudo-random number generators ([**935**], [**936**], [**938**], [**1277**]), k-regular [**76**] and automatic sequences [**736**], and cellular automata [**780**]. Sequences of solutions of classes of interesting Diophantine equations form linear recurrence sequences — see [**1175**], [**1181**], [**1285**], [**1286**]. A great variety of power series, for example zeta-functions of algebraic varieties over finite fields [**725**], dynamical zeta functions of many dynamical systems [**135**], [**537**], [**776**], generating functions coming from group theory [**1110**], [**1111**], Hilbert series in commutative algebra [**788**], Poincaré series [**131**], [**287**], [**1110**] and the like — are all known to be rational in many interesting cases. The coefficients of the series representing such functions are linear recurrence sequences, so many powerful results from the present study may be applied. Linear recurrence sequences even participated in the proof of Hilbert's Tenth Problem over $\mathbb{Z}$ ([**786**], [**1319**], [**1320**]). In the proceedings [**289**], the problem is resolved for many other rings. The article [**998**] by Pheidas suggests using the arithmetic of bilinear recurrence sequences to settle the still open rational case.

Recurrence sequences also appear in many parts of the mathematical sciences in the wide sense (which includes applied mathematics and applied computer science). For example, many systems of orthogonal polynomials, including the Tchebychev polynomials and their finite field analogues, the Dickson polynomials, satisfy recurrence relations. Linear recurrence sequences are also of importance in approximation theory and cryptography and they have arisen in computer graphics [**799**] and time series analysis [**136**].

We survey a selection of number-theoretic properties of linear recurrence sequences together with their direct generalizations. These include non-linear recurrence sequences and exponential polynomials. Applications are described to motivate the material and to show how some of the problems arise. In many sections we concentrate on particular properties of linear recurrence sequences which are important for a variety of applications. Where we are able, we try to consider properties that are particularly instructive in suggesting directions for future study.

Several surveys of properties of linear recurrence sequences have been given recently; see, for example, [**215**], [**725**, Chap. 8], [**822**], [**827**], [**899**], [**914**], [**1026**], [**1181**], [**1202**], [**1248**], [**1285**], [**1286**]. However, they do not cover as wide a range of important features and applications as we attempt here. We have relied on these surveys a great deal, and with them in mind, try to use the 'covering radius 1' principle: For every result not proved here, either a direct reference or a pointer to an easily available survey in which it can be found is given. For all results, we try to recall the original version, some essential intermediate improvements, and — up to the authors' limited knowledge — the best current form of the result.

Details of the scope of this book are clear from the table of contents. In Chapters 1 to 8, general results concerning linear recurrence sequences are presented. The topics include various estimates for the number of solutions of equations, inequalities and congruences involving linear recurrence sequences. Also, there are estimates for exponential sums involving linear recurrence sequences as well as results on the behaviour of arithmetic functions on values of linear recurrence sequences. In Chapters 9 to 14, a selection of applications are given, together with a study of some special sequences. In some cases, applications require only the straightforward use of results from the earlier chapters. In other cases the technique, or even just the spirit, of the results are used. It seems almost magical that, in many applications, linear recurrence sequences show up from several quite unrelated directions. A chapter on elliptic divisibility sequences is included to point out the beginning of an area of development analogous to linear recurrence sequences, but with interesting geometric and Diophantine methods coming to the fore. A chapter is also included to highlight an emerging overlap between combinatorial dynamics and the theory of linear recurrence sequences.

Although objects are considered over different rings, the emphasis is on the conventional case of the integers. A linear recurrence sequence over the integers can often be considered as the trace of an exponential function over an algebraic number field. The coordinates of matrix exponential functions satisfy linear recurrence relations. Such examples suggest that a single exponential only *seems* to be less general than a linear recurrence sequence. Of course that is not quite true, but in many important cases links between linear recurrence sequences and exponential functions in algebraic extensions really do play a crucial role. Michalev and Nechaev [**827**] give a survey of possible extensions of the theory of linear recurrence sequences to a wide class of rings and modules.

For previously known results, complete proofs are generally not given unless they are very short or illuminating. The underlying ideas and connections with other results are discussed briefly. Filling the gaps in these arguments may be considered a useful (substantial) exercise. Several of the results are new; for these complete proofs are given.

Some number-theoretic and algebraic background is assumed. In the text, we try to motivate the use of deeper results. A brief survey of the background material follows. First, some basic results from the theory of finite fields and from algebraic number theory will be used. These can be found in [**725**] and [**909**], respectively. Also standard results on the distribution of prime numbers, in particular the Prime Number Theorem $\pi(x) \sim x/\ln x$, will be used. All such results can easily be found in [**1049**], and in many other textbooks. Much stronger results are known, though these subtleties will not matter here. The following well-known consequences of the Prime Number Theorem,

$$k \geq \varphi(k) \gg k/\operatorname{Log}\log k, \qquad \nu(k) \ll \operatorname{Log} k/\operatorname{Log}\log k$$

and

$$P(k) \gg \nu(k)\operatorname{Log}\nu(k), \qquad Q(k) \geq \exp\left((1+o(1))\nu(k)\right)$$

will also be needed.

A second tool is p-adic analysis [**29**], [**131**], [**620**]; in particular Strassmann's Theorem [**1261**], sometimes called the p-adic Weierstrass Preparation Theorem. Section 1.2 provides a basic introduction to this beautiful theory. At several points in the text, results about recurrence sequences will be given where the most natural proofs seem to come from p-adic analysis. We can offer no explanation for this phenomenon. For example, in Section 1.2, we give a simple proof of a special case of the Hadamard quotient problem using p-adic analysis. The general case has now been resolved and the methods are still basically p-adic. Similarly, when it is applicable, p-adic analysis produces very good estimates for the *number* of solutions of equations; compare the estimate of [**1123**] based on new results on S-unit equations with that of [**1038**] obtained by the p-adic method. On the other hand, a disadvantage of this approach is its apparent non-effectiveness in estimating the *size* of solutions.

The simple observation that any field of zero characteristic over which a linear recurrence sequence is defined may be assumed to be finitely generated over $\mathbb{Q}$ will be used repeatedly. Indeed, it is enough to consider the field obtained from $\mathbb{Q}$ by adjoining the initial values and the coefficients of the characteristic polynomial. Then, using specialization arguments [**1026**] and [**1037**], we may restrict ourselves to studying sequences over an algebraic extension of $\mathbb{Q}_p$ or even just over $\mathbb{Q}_p$, using a nice idea of Cassels [**213**]. Cassels shows that given any field $\mathbb{F}$, finitely generated over $\mathbb{Q}$, and any finite subset $M \in \mathbb{F}$, there exist infinitely many rational primes p such that there is an embedding $\varphi : \mathbb{F} \longrightarrow \mathbb{Q}_p$ with $\operatorname{ord}_p \varphi(\mu) = 0$ for all $\mu \in M$. A critical feature is that the embedding is into $\mathbb{Q}_p$, rather than a 'brute force' embedding into an algebraic extension of $\mathbb{Q}_p$. The upshot is that for many natural problems over general fields of zero characteristic, one can expect to get results that are not worse than the corresponding one in the algebraic number field case, or even for the case of rational numbers. Moreover, there are a number of examples in the case of function fields where even stronger results can be obtained, see [**128**], [**160**], [**167**], [**171**], [**548**], [**781**], [**871**] [**920**], [**1002**], [**1041**], [**1162**], [**1308**], [**1309**], [**1324**], [**1373**].

Thirdly, many results depend on bounds for linear forms in the logarithms of algebraic numbers. Section 1.3 gives an indication of the connection between the theory of linear recurrence sequences and linear forms in logarithms by considering the apparently simple question: How quickly does a linear recurrence sequence grow? After the first results of Baker [**50**], [**51**], [**52**], [**53**], [**54**], [**55**], and their p-adic generalizations, for example those of van der Poorten [**1017**], a vast number of further results, generalizations and improvements have been obtained; appropriate references can be found in [**1324**]. For our purposes, the modern sharper bounds do not imply any essentially stronger results than those relying on [**55**] and [**1017**]. In certain cases more recent results do allow the removal of some logarithmic terms; [**1369**] is an example. We mostly content ourselves with consequences of the relatively old results.

Fourthly and finally, several results on growth rate estimates or zero multiplicity are based upon properties of sums of S-units. Specifically, linear recurrence sequences provide a special case of S-unit sums. Section 1.5 gives a basic account of the way results about sums of S-units can be applied to linear recurrence sequences. This does not do justice to the full range of applicability of results about sums of S-units — applications will reverberate throughout the text.

In surveys such as this, it is conventional to attach a list of open questions. Rather than doing this, the best current results known to the authors are presented; if a generalization is straightforward and can be done in the framework of the same arguments that is noted. Other generalizations or improvements should be considered implicit research problems. We do however mention attempts at improvements which seem hopeless in the light of today's knowledge.

Finally, we add several words about what we do not deal with. First, it is striking to note that the binary recurrence $u(n+2) = u(n+1)+u(n)$, one of the simplest linear recurrences whose solutions are not geometric progressions, has been a subject of mathematical scrutiny certainly since the publication of Leonardo of Pisa's *Liber abaci* in 1202 [**1212**]. Indeed, this recurrence has an entire journal devoted to it [**113**]. This volume is more egalitarian; with a few exceptions, no special properties of individual recurrences will be discussed. Several specific sequences arise as examples; the most important of these are listed with their identifying numbers in Sloane's Online Encyclopedia of Integer Sequences [**1222**] in an Appendix on page 254.

Second, one could write an enormous book devoted to one particular case of linear recurrence sequences — polynomials. We do not deal with polynomials *per se*; extensive treatments are in [**1116**] and [**1120**]. Nonetheless, this case alone justifies the great interest in general linear recurrence sequences. Therefore, we give several applications to polynomials but such applications are obtained using partially hidden — although not too deep — links between polynomials and linear recurrence sequences.

Third, a huge book could be written dealing with exponential polynomials as examples of entire functions and therefore, ultimately, with analytic properties of those functions. We barely consider any analytical features of exponential polynomials, though we mention some relevant results about the distribution of their zeros. We do not deal with analytical properties of iteration of polynomial mappings. Thus the general field of complex dynamics, and the celebrated Mandelbrot set, is outside our scope. (Recall that the Mandelbrot set is the set of points $c \in \mathbb{C}$ for which the sequence of polynomial iterations $z(k) = z(k-1)^2 + c$, $z(0) = 0$, is bounded; for details we refer to [**154**].) However, in Chapter 3 we do consider some simple periodic properties of this and more general mappings.

Fourth, as we mentioned, general statements about the behaviour — both Archimedean and non-Archimedean — of sums of S-units lie in the background of important results on linear recurrence sequences. Nonetheless, we do not deal with sums of S-units or their applications systematically. On the topic generally, we first recommend the pioneering papers [**376**] and [**1037**] which appeared independently and contemporaneously (the latter as a preprint [**1019**] of Macquarie University in 1982). We point particularly to the book [**1181**] and the excellent survey papers [**378**], [**380**], [**381**], [**382**], [**503**], [**1128**], [**1175**], [**1285**], [**1286**].

On the other hand, we do present some less well-known results about finitely generated groups, such as estimates of the size of their reduction modulo an integer ideal in an algebraic number field, and on the testing of multiplicative independence of their generators. When results on S-unit sums are applied to linear recurrence sequences, an induction argument usually allows the conditions on non-vanishing proper sub-sums to be eliminated (such conditions are unavoidable in the general study of S-unit sums).

Despite the large number of references, no systematic attempt has been made to trace the history of major results that have influenced the subject. No single book on the history of this huge topic could hope to be definitive. However — Leonardo of Pisa notwithstanding — it is reasonable to view the modern study of the arithmetic of recurrence sequences as having been given essential impetus by the remarkable work of François Édouard Anatole Lucas (1842–1891); many of the themes developed in this book originate in his papers (see [**283**] and [**1354**] for some background on his life and work, and [**517**] for a full list of his publications and some of his unpublished work).

The bibliography reflects the interests and biases of the authors, and some of the entries are to preliminary works. The authors extend their thanks to the many workers whose contributions have given them so much pleasure and extend their apologies to those whose contributions have not been cited. The authors also thank many people for help with corrections and references, particularly Christian Ballot, Daniel Berend, Keith Briggs, Sheena Brook, Susan Everest, Robert Laxton, Pieter Moree, Patrick Moss, Władysław Narkiewicz, James Propp, Michael Somos, Shaun Stevens, Zhi-Wei Sun and Alan Ward.

Alf van der Poorten & Igor Shparlinski
Centre for Number Theory Research
Macquarie University
Sydney
`alf@math.mq.edu.au`
`igor@comp.mq.edu.au`

Graham Everest & Thomas Ward
School of Mathematics
University of East Anglia
Norwich
`g.everest@uea.ac.uk`
`t.ward@uea.ac.uk`

Sequences from the on-line Encyclopedia

Sequences mentioned in the text that appear in Sloane's Online Encyclopedia of Integer Sequences [**1222**] are listed here, together with the pages on which they appear. In some cases the entry here reflects a specific sequence satisfying a recurrence relation in the text.

Bibliography

1. N. Adachi, *An application of Frey's idea to exponential Diophantine equations*, Proc. Japan Acad. Ser. A Math. Sci. **70** (1994), no. 8, 261–263. MR **95i:**11022
2. R. Adler, M. Keane, and M. Smorodinsky, *A construction of a normal number for the continued fraction transformation*, J. Number Theory **13** (1981), no. 1, 95–105. MR **82k:**10070
3. L. Afflerbach and R. Weilbächer, *The exact determination of rectangle discrepancy for linear congruential pseudorandom numbers*, Math. Comp. **53** (1989), no. 187, 343–354. MR **90h:**65009
4. M. Agrawal, N. Kayal, and N. Saxena, *Primes is in* **P**, `www.cse.iitk.ac.in/news/primality.pdf`, 2002.
5. S. D. Ahlgren, *Polynomial-exponential equations in two variables*, J. Number Theory **62** (1997), no. 2, 428–438. MR **97k:**11044
6. ______, *The set of solutions of a polynomial-exponential equation*, Acta Arith. **87** (1999), no. 3, 189–207. MR **99m:**11031
7. S. Akiyama, *A new type of inclusion exclusion principle for sequences and asymptotic formulas for $\zeta(k)$*, J. Number Theory **45** (1993), no. 2, 200–214. MR **94k:**11027
8. ______, *A criterion to estimate the least common multiple of sequences and asymptotic formulas for $\zeta(3)$ arising from recurrence relation of an elliptic function*, Japan. J. Math. (N.S.) **22** (1996), no. 1, 129–146. MR **97f:**11021
9. R. Ž. Aleev, *Higman's central unit theory, units of integral group rings of finite cyclic groups and Fibonacci numbers*, Internat. J. Algebra Comput. **4** (1994), no. 3, 309–358. MR **95h:**16042
10. W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2) **139** (1994), no. 3, 703–722. MR **95k:**11114
11. J.-P. Allouche, *Automates finis en théorie des nombres*, Exposition. Math. **5** (1987), no. 3, 239–266. MR **88k:**11046
12. ______, *The number of factors in a paperfolding sequence*, Bull. Austral. Math. Soc. **46** (1992), no. 1, 23–32. MR **93f:**11020
13. ______, *Sur la complexité des suites infinies*, Bull. Belg. Math. Soc. Simon Stevin **1** (1994), no. 2, 133–143. MR **96d:**68167
14. J.-P. Allouche, A. Arnold, J. Berstel, S. Brlek, W. Jockusch, S. Plouffe, and B. E. Sagan, *A relative of the Thue-Morse sequence*, Discrete Math. **139** (1995), no. 1-3, 455–461. MR **96c:**11029
15. J.-P. Allouche and M. Bousquet-Mélou, *On the conjectures of Rauzy and Shallit for infinite words*, Comment. Math. Univ. Carolin. **36** (1995), no. 4, 705–711. MR **97e:**68103
16. J.-P. Allouche, P. Hajnal, and J. Shallit, *Analysis of an infinite product algorithm*, SIAM J. Discrete Math. **2** (1989), no. 1, 1–15. MR **90f:**68073
17. J.-P. Allouche and P. Liardet, *Generalized Rudin-Shapiro sequences*, Acta Arith. **60** (1991), no. 1, 1–27. MR **92k:**11080
18. J.-P. Allouche, M. Mendès France, and A. J. van der Poorten, *An infinite product with bounded partial quotients*, Acta Arith. **59** (1991), no. 2, 171–182. MR **92k:**11074
19. J.-P. Allouche, P. Morton, and J. Shallit, *Pattern spectra, substring enumeration, and automatic sequences*, Theoret. Comput. Sci. **94** (1992), no. 2, 161–174. MR **93i:**11030
20. J.-P. Allouche and J. Shallit, *Infinite products associated with counting blocks in binary strings*, J. London Math. Soc. (2) **39** (1989), no. 2, 193–204. MR **90g:**11013
21. ______, *The ring of k-regular sequences*, Theoret. Comput. Sci. **98** (1992), no. 2, 163–197. MR **94c:**11021

22. ______, *Complexité des suites de Rudin-Shapiro généralisées*, J. Théor. Nombres Bordeaux **5** (1993), no. 2, 283–302. MR **95d:**11030

23. ______, *Sums of digits, overlaps, and palindromes*, Discrete Math. Theor. Comput. Sci. **4** (2000), no. 1, 1–10. MR **2001c:**11009

24. J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, A. Petersen, and G. Skordev, *Automaticity of double sequences generated by one-dimensional linear cellular automata*, Theoret. Comput. Sci. **188** (1997), no. 1-2, 195–209. MR **98j:**68116

25. J.-P. Allouche, F. von Haeseler, H.-O. Peitgen, and G. Skordev, *Linear cellular automata, finite automata and Pascal's triangle*, Discrete Appl. Math. **66** (1996), no. 1, 1–22. MR **97b:**11033

26. N. Alon, O. Goldreich, J. Håstad, and R. Peralta, *Simple constructions of almost k-wise independent random variables*, Random Structures Algorithms **3** (1992), 289–304, Addendum: **4** (1993), 119–120. MR **93k:**94006a

27. J. Althaler and A. Dür, *Finite linear recurring sequences and homogeneous ideals*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 5, 377–390. MR **99e:**94026

28. A. S. Ambrosimov, *On the distribution of the frequencies of multigrams in linear recurrent sequences over a residue ring*, Uspekhi Mat. Nauk **48** (1993), no. 5(293), 157–158. MR **95a:**11008

29. Y. Amice, *Les nombres p-adiques*, Presses Universitaires de France, Paris, 1975. MR 56 #5510

30. V. S. Anashin, *Uniformly distributed sequences over p-adic integers*, Number-theoretic and algebraic methods in computer science (Moscow, 1993), World Sci. Publishing, River Edge, NJ, 1995, pp. 1–18. MR **96m:**11107

31. M. Anderson and D. W. Masser, *Lower bounds for heights on elliptic curves*, Math. Z. **174** (1980), no. 1, 23–34. MR **82g:**10049

32. Ş. Andrei, M. Kudlek, and R. Ş. Niculescu, *Some results on the Collatz problem*, Acta Inform. **37** (2000), no. 2, 145–160. MR **2002c:**11022

33. Ş. Andrei and C. Masalagiu, *About the Collatz conjecture*, Acta Inform. **35** (1998), no. 2, 167–179. MR **99d:**68097

34. D. Applegate and J. C. Lagarias, *Density bounds for the $3x + 1$ problem. I. Tree-search method*, Math. Comp. **64** (1995), no. 209, 411–426. MR **95c:**11024

35. ______, *Density bounds for the $3x + 1$ problem. II. Krasikov inequalities*, Math. Comp. **64** (1995), no. 209, 427–438. MR **95c:**11025

36. ______, *The distribution of $3x + 1$ trees*, Experiment. Math. **4** (1995), no. 3, 193–209. MR **97e:**11033

37. ______, *Lower bounds for the total stopping time of $3x+1$ iterates*, Math. Comp. **72** (2003), no. 242, 1035–1049 (electronic). MR 1 954 983

38. F. Arnault, *The Rabin-Monier theorem for Lucas pseudoprimes*, Math. Comp. **66** (1997), no. 218, 869–881. MR **97f:**11009

39. D. K. Arrowsmith and F. Vivaldi, *Geometry of p-adic Siegel discs*, Phys. D **71** (1994), no. 1-2, 222–236. MR **95d:**11162

40. M. Artin and B. Mazur, *On periodic points*, Ann. of Math. (2) **81** (1965), 82–99. MR 31 #754

41. M. Ayad, *Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques*, Ann. Inst. Fourier (Grenoble) **43** (1993), no. 3, 585–618. MR **94f:**11009

42. M. Ayad and D. L. McQuillan, *Irreducibility of the iterates of a quadratic polynomial over a field*, Acta Arith. **93** (2000), no. 1, 87–97, Erratum: **99** (2001), 97. MR **2001c:**11031

43. L. Babai, R. Beals, J.-Y. Cai, G. Ivanyos, and E. M. Luks, *Multiplicative equations over commuting matrices*, Proceedings of the Seventh Annual ACM-SIAM Symposium on Discrete Algorithms (Atlanta, GA, 1996) (New York), ACM, 1996, pp. 498–507. MR 1 381 955

44. E. Bach, *Realistic analysis of some randomized algorithms*, J. Comput. System Sci. **42** (1991), no. 1, 30–53. MR **92b:**11090

45. ______, *Toward a theory of Pollard's rho method*, Inform. and Comput. **90** (1991), no. 2, 139–155. MR **92a:**11151

46. ______, *Efficient prediction of Marsaglia-Zaman random number generators*, IEEE Trans. Inform. Theory **44** (1998), no. 3, 1253–1257. MR **99b:**65007

47. E. Bach and L. Huelsbergen, *Statistical evidence for small generating sets*, Math. Comp. **61** (1993), no. 203, 69–82. MR **93k:**11089

48. E. Bach, R. Lukes, J. Shallit, and H. C. Williams, *Results and estimates on pseudopowers*, Math. Comp. **65** (1996), no. 216, 1737–1747. MR **97a:**11161

49. E. Bach and J. Shallit, *Factoring with cyclotomic polynomials*, Math. Comp. **52** (1989), no. 185, 201–219. MR **89k:**11127

50. A. Baker, *Linear forms in the logarithms of algebraic numbers. I*, Mathematika **13** (1967), 204–216.

51. ———, *Linear forms in the logarithms of algebraic numbers. II*, Mathematika **14** (1967), 102–107.

52. ———, *Linear forms in the logarithms of algebraic numbers. III*, Mathematika **14** (1967), 220–228. MR 36 #3732

53. ———, *Linear forms in the logarithms of algebraic numbers. IV*, Mathematika **15** (1968), 204–216. MR 41 #3402

54. ———, *Transcendental number theory*, Cambridge University Press, London, 1975. MR 54 #10163

55. ———, *The theory of linear forms in logarithms*, Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), Academic Press, London, 1977, pp. 1–27. MR 58 #16543

56. ———, *Logarithmic forms and the abc-conjecture*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 37–44. MR **99e:**11101

57. M. Baker, *Lower bounds for the canonical height on elliptic curves over abelian extensions*, Int. Math. Res. Not. (2003), no. 29, 1571–1589.

58. R. Balasubramanian and M. Ram Murty, *Elliptic pseudoprimes. II*, Séminaire de Théorie des Nombres, Paris 1988–1989, Birkhäuser Boston, Boston, MA, 1990, pp. 13–25. MR **92f:**11076

59. R. Balasubramanian and S. V. Nagaraj, *Density of Carmichael numbers with three prime factors*, Math. Comp. **66** (1997), no. 220, 1705–1708. MR **98d:**11110

60. ———, *The least witness of a composite number*, Lect. Notes in Comp. Sci. **1396** (1997), 66–74.

61. C. Ballot, *Density of prime divisors of linear recurrences*, Mem. Amer. Math. Soc. **115** (1995), no. 551, viii+102. MR **95i:**11110

62. ———, *Group structure and maximal division for cubic recursions with a double root*, Pacific J. Math. **173** (1996), no. 2, 337–355. MR **97k:**11018

63. ———, *The density of primes p, such that −1 is a residue modulo p of two consecutive Fibonacci numbers, is* 2/3, Rocky Mountain J. Math. **29** (1999), no. 3, 749–761. MR 1 733 067

64. ———, *Strong arithmetic properties of the integral solutions of* $X^3 + DY^3 + D^2Z^3 - 3DXYZ = 1$*, where* $D = M^3 \pm 1, M \in \mathbb{Z}^*$, Acta Arith. **89** (1999), no. 3, 259–277. MR **2001d:**11012

65. W. Banks, F. Griffin, D. Lieman, and I. E. Shparlinski, *Non-linear complexity of the Naor-Reingold pseudo-random function*, Lect. Notes in Comp. Sci. **1787** (2000), 53–59.

66. G. Barat and P. J. Grabner, *Distribution of binomial coefficients and digital functions*, J. London Math. Soc. (2) **64** (2001), no. 3, 523–547. MR 1 865 548

67. E. Barone, *A heuristic probabilistic argument for the Collatz sequence*, Ital. J. Pure Appl. Math. **4** (1998), 151–153 (1999). MR **2000d:**11033

68. D. Barsky, J.-P. Bézivin, and A. Schinzel, *Une caractérisation arithmétique de suites récurrentes linéaires*, J. Reine Angew. Math. **494** (1998), 73–84. MR **99j:**11011

69. T. Bass, *The Reach Tee Shirt Site*, `www.math.harvard.edu/~propp/reach/shirt.html`.

70. N. L. Bassily, I. Kátai, and M. Wijsmuller, *Number of prime divisors of* $\phi_k(n)$*, where* ϕ_k *is the k-fold iterate of* ϕ, J. Number Theory **65** (1997), no. 2, 226–239. MR **2000c:**11159

71. ———, *On the prime power divisors of the iterates of the Euler-*ϕ *function*, Publ. Math. Debrecen **55** (1999), no. 1-2, 17–32. MR **2000g:**11092

72. A. Batra and P. Morton, *Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. I*, Rocky Mountain J. Math. **24** (1994), no. 2, 453–481. MR **95d:**11163

73. ———, *Algebraic dynamics of polynomial maps on the algebraic closure of a finite field. II*, Rocky Mountain J. Math. **24** (1994), no. 3, 905–932. MR **95j:**11114

74. E. Bavencoffe and J.-P. Bézivin, *Une famille remarquable de suites récurrentes linéaires*, Monatsh. Math. **120** (1995), no. 3-4, 189–203. MR **97a:**11027

75. A. F. Beardon, *Iteration of rational functions*, Springer-Verlag, New York, 1991. MR **92j:**30026

76. P.-G. Becker, *k-regular power series and Mahler-type functional equations*, J. Number Theory **49** (1994), no. 3, 269–286. MR **96b:**11026

77. P.-G. Becker and T. Töpfer, *Transcendency results for sums of reciprocals of linear recurrences*, Math. Nachr. **168** (1994), 5–17. MR **95d:**11089

78. W. Beckner and A. Regev, *Asymptotics and algebraicity of some generating functions*, Adv. in Math. **65** (1987), no. 1, 1–15. MR **88h:**05008

79. E. G. Belaga and M. Mignotte, *Embedding the* $3x + 1$ *conjecture in a* $3x + d$ *context*, Experiment. Math. **7** (1998), no. 2, 145–151. MR **2000d:**11034

80. B. Benzaghou and J.-P. Bézivin, *Propriétés algébriques de suites différentiellement finies*, Bull. Soc. Math. France **120** (1992), no. 3, 327–346. MR **93m:**12006

81. D. Berend and M. D. Boshernitzan, *On a result of Mahler on the decimal expansions of* $(n\alpha)$, Acta Arith. **66** (1994), no. 4, 315–322. MR **95f:**11051

82. ———, *Numbers with complicated decimal expansions*, Acta Math. Hungar. **66** (1995), no. 1-2, 113–126. MR **95m:**11073

83. C. A. Berenstein and A. Yger, *Exponential polynomials and $\mathcal{D}$-modules*, Compositio Math. **95** (1995), no. 2, 131–181. MR **95m:**32004

84. F. Bergeron and C. Reutenauer, *Combinatorial resolution of systems of differential equations. III. A special class of differentially algebraic series*, European J. Combin. **11** (1990), no. 6, 501–512. MR **91m:**05010

85. E. R. Berlekamp, *Algebraic coding theory*, McGraw-Hill Book Co., New York, 1968. MR 38 #6873

86. D. J. Bernstein and J. C. Lagarias, *The* $3x + 1$ *conjugacy map*, Canad. J. Math. **48** (1996), no. 6, 1154–1169. MR **98a:**11027

87. J. Berstel and M. Mignotte, *Deux propriétés décidables des suites récurrentes linéaires*, Bull. Soc. Math. France **104** (1976), no. 2, 175–184. MR 54 #2576

88. V. Berthé, *Automates et valeurs de transcendance du logarithme de Carlitz*, Acta Arith. **66** (1994), no. 4, 369–390. MR **95h:**11068

89. ———, *Combinaisons linéaires de* $\zeta(s)/\Pi^s$ *sur* $\mathbb{F}_q(x)$*, pour* $1 \leq s \leq q-2$, J. Number Theory **53** (1995), no. 2, 272–299. MR **97c:**11075

90. A. Bertrand-Mathis, *Nombres normaux dans diverses bases*, Ann. Inst. Fourier (Grenoble) **45** (1995), no. 5, 1205–1222. MR **97m:**11103

91. ———, *Nombres normaux*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 397–412. MR **98c:**11073

92. ———, *Ensembles normaux relatifs à des matrices non-commutantes*, J. Number Theory **63** (1997), no. 1, 180–190. MR **98f:**11079

93. F. Beukers, *The multiplicity of binary recurrences*, Compositio Math. **40** (1980), no. 2, 251–267. MR **81g:**10019

94. ———, *The zero-multiplicity of ternary recurrences*, Compositio Math. **77** (1991), no. 2, 165–177. MR **92a:**11014

95. ———, *Recurrent sequences and p-adic spectra*, Math. Z. (to appear).

96. F. Beukers and H. P. Schlickewei, *The equation* $x + y = 1$ *in finitely generated groups*, Acta Arith. **78** (1996), no. 2, 189–199. MR **97k:**11051

97. F. Beukers and R. Tijdeman, *On the multiplicities of binary complex recurrences*, Compositio Math. **51** (1984), no. 2, 193–213. MR **85i:**11017

98. J.-P. Bézivin, *Factorisation de suites récurrentes linéaires et applications*, Bull. Soc. Math. France **112** (1984), no. 3, 365–376. MR **86j:**11017

99. ———, *Diviseurs premiers de suites récurrentes linéaires*, European J. Combin. **7** (1986), no. 3, 199–204. MR **88d:**11014

100. ———, *Sur les diviseurs premiers des suites récurrentes linéaires*, Ann. Fac. Sci. Toulouse Math. (5) **8** (1986/87), no. 1, 61–73. MR **88j:**11007

101. ———, *Diviseurs premiers de suites récurrentes non linéaires*, Collect. Math. **38** (1987), no. 1, 37–55. MR **90a:**11022

102. ———, *Suites récurrentes linéaires en caractéristique non nulle*, Bull. Soc. Math. France **115** (1987), no. 2, 227–239. MR **89d:**11009

103. ———, *Plus petit commun multiple des termes consécutifs d'une suite récurrente linéaire*, Collect. Math. **40** (1989), no. 1, 1–11 (1990). MR **92f:**11022

104. ———, *Une généralisation du théorème de Skolem-Mahler-Lech*, Quart. J. Math. Oxford Ser. (2) **40** (1989), no. 158, 133–138. MR **90g:**11021

105. ———, *Les suites q-récurrentes linéaires*, Compositio Math. **80** (1991), no. 3, 285–307. MR **93d:**11014

106. ———, *Fractions continues et suites récurrentes*, C. R. Acad. Sci. Paris Sér. I Math. **318** (1994), no. 11, 991–994. MR **95e:**11015

107. ———, *Fonctions multiplicatives et équations différentielles*, Bull. Soc. Math. France **123** (1995), no. 3, 329–349. MR **97d:**11009

108. ———, *Sur les suites récurrentes à coefficients polynômes*, J. Number Theory **66** (1997), no. 2, 282–290. MR **98h:**11027

109. ———, *Sur les suites presque-périodiques*, Arch. Math. (Basel) **70** (1998), no. 6, 447–454. MR **99d:**11091

110. J.-P. Bézivin and V. Laohakosol, *On the theorem of Skolem-Mahler-Lech*, Exposition. Math. **9** (1991), no. 1, 89–96. MR **92c:**11140

111. J.-P. Bézivin, A. Pethő, and A. J. van der Poorten, *A full characterisation of divisibility sequences*, Amer. J. Math. **112** (1990), no. 6, 985–1001. MR **91k:**11017

112. J.-P. Bézivin and P. Robba, *Rational solutions of linear differential equations*, J. Austral. Math. Soc. Ser. A **46** (1989), no. 2, 184–196. MR **90c:**12009

113. M. Bicknell-Johnson, *A short history of The Fibonacci Quarterly*, Fibonacci Quart. **25** (1987), no. 1, 2–5.

114. H. Bilharz, *Primdivisoren mit vorgegebener Primitivwurzel*, Math. Ann. **114** (1937), 476–492.

115. Y. Bilu, *Catalan's conjecture (after Mihăilescu)*, Preprint, 2002.

116. Y. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122, With an appendix by M. Mignotte. MR **2002j:**11027

117. S. R. Blackburn, *Fast rational interpolation, Reed-Solomon decoding, and the linear complexity profiles of sequences*, IEEE Trans. Inform. Theory **43** (1997), no. 2, 537–548. MR **98c:**94012

118. ———, *Linear cellular automata as stream cipher components*, Preprint, 1997.

119. ———, *Orthogonal sequences of polynomials over arbitrary fields*, J. Number Theory **68** (1998), no. 1, 99–111. MR **98m:**11013

120. ———, *The linear complexity of the self-shrinking generator*, IEEE Trans. Inform. Theory **45** (1999), no. 6, 2073–2077. MR **2000f:**94025

121. S. R. Blackburn, T. Etzion, and K. G. Paterson, *Permutation polynomials, de Bruijn sequences, and linear complexity*, J. Combin. Theory Ser. A **76** (1996), no. 1, 55–82. MR **97h:**94004

122. R. E. Blahut, *Theory and practice of error control codes*, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. MR **85f:**94001

123. R. Blecksmith, M. Filaseta, and C. Nicol, *A result on the digits of a^n*, Acta Arith. **64** (1993), no. 4, 331–339. MR **94d:**11005

124. D. Bleichenbacher, *Efficiency and security of cryptosystems based on number theory*, Ph.D. thesis, Zurich, 1996.

125. D. Bleichenbacher, W. Bosma, and A. K. Lenstra, *Some remarks on Lucas-based cryptosystems*, Advances in cryptology—CRYPTO '95 (Santa Barbara, CA, 1995), Springer, Berlin, 1995, pp. 386–396. MR **97m:**94012

126. V. D. Blondel and N. Portier, *The presence of a zero in an integer linear recurrent sequence is* **NP***-hard to decide*, Linear Algebra Appl. **351-352** (2002), 91–98. MR 1 917 474

127. L. Blum, M. Blum, and M. Shub, *A simple unpredictable pseudorandom number generator*, SIAM J. Comput. **15** (1986), no. 2, 364–383. MR **87k:**65007

128. E. Bombieri, J. Mueller, and M. Poe, *The unit equation and the cluster principle*, Acta Arith. **79** (1997), no. 4, 361–389. MR **98a:**11037

129. E. Bombieri and A. J. van der Poorten, *Continued fractions of algebraic numbers*, Computational algebra and number theory (Sydney, 1992), Kluwer Acad. Publ., Dordrecht, 1995, pp. 137–152. MR **96g:**11079

130. E. Borel, *Les probabilités denombrables et leurs applications arithmetiques*, Rend. Circ. Math. Palermo **27** (1909), 247–271.

131. A. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966. MR 33 #4001

132. W. Bosma and C. Kraaikamp, *Metrical theory for optimal continued fractions*, J. Number Theory **34** (1990), no. 3, 251–270. MR **91d:**11095

133. ———, *Optimal approximation by continued fractions*, J. Austral. Math. Soc. Ser. A **50** (1991), no. 3, 481–504. MR **92f:**11093

134. J. Bourgain, *On triples in arithmetic progression*, Geom. Funct. Anal. **9** (1999), no. 5, 968–984. MR **2001h:**11132

135. R. Bowen and O. E. Lanford, III., *Zeta functions of restrictions of the shift transformation*, Global Analysis (Proc. Sympos. Pure Math., Vol. XIV, Berkeley, Calif., 1968), Amer. Math. Soc., Providence, R.I., 1970, pp. 43–49. MR 42 #6284

136. G. E. P. Box and G. M. Jenkins, *Times series analysis. Forecasting and control*, Holden-Day, San Francisco, Calif., 1970. MR 42 #7019

137. J. Boyar, *Inferring sequences produced by a linear congruential generator missing low-order bits*, J. Cryptology **1** (1989), no. 3, 177–184. MR **90g:**94012

138. ———, *Inferring sequences produced by pseudo-random number generators*, J. Assoc. Comput. Mach. **36** (1989), no. 1, 129–141. MR **91g:**68035

139. D. W. Boyd, *Reciprocal polynomials having small measure*, Math. Comp. **35** (1980), no. 152, 1361–1377. MR **82a:**30005

140. ———, *Speculations concerning the range of Mahler's measure*, Canad. Math. Bull. **24** (1981), no. 4, 453–469. MR **83h:**12002

141. ———, *Reciprocal polynomials having small measure. II*, Math. Comp. **53** (1989), no. 187, 355–357, S1–S5. MR **89m:**30013

142. ———, *Salem numbers of degree four have periodic expansions*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 57–64. MR **90j:**11071

143. ———, *Irreducible polynomials with many roots of maximal modulus*, Acta Arith. **68** (1994), no. 1, 85–88. MR **95i:**11119

144. ———, *On beta expansions for Pisot numbers*, Math. Comp. **65** (1996), no. 214, 841–860. MR **96g:**11090

145. ———, *On the beta expansion for Salem numbers of degree* 6, Math. Comp. **65** (1996), no. 214, 861–875, $S29$–$S31$. MR **96g:**11091

146. ———, *The beta expansion for Salem numbers*, Organic mathematics (Burnaby, BC, 1995), Amer. Math. Soc., Providence, RI, 1997, pp. 117–131. MR **98k:**11146

147. ———, *Mahler's measure and special values of L-functions*, Experiment. Math. **7** (1998), no. 1, 37–82. MR **99d:**11070

148. ———, *Mahler's measure and special values of L-functions—some conjectures*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 27–34. MR **2000f:**11139

149. ———, *Mahler's measure and invariants of hyperbolic manifolds*, Number theory for the millennium, I (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 127–143. MR 1 956 222

150. D. W. Boyd, J. Cook, and P. Morton, *On sequences of* ± 1*'s defined by binary patterns*, Dissertationes Math. (Rozprawy Mat.) **283** (1989), 64. MR **91c:**11006

151. M. Boyle and D. Handelman, *The spectra of nonnegative matrices via symbolic dynamics*, Ann. of Math. (2) **133** (1991), no. 2, 249–316. MR **92d:**58057

152. ———, *Algebraic shift equivalence and primitive matrices*, Trans. Amer. Math. Soc. **336** (1993), no. 1, 121–149. MR **93e:**58050

153. G. Braga, G. Cattaneo, P. Flocchini, and C. Quaranta Vogliotti, *Pattern growth in elementary cellular automata*, Theoret. Comput. Sci. **145** (1995), no. 1-2, 1–26. MR **96h:**68137

154. B. Branner, *The Mandelbrot set*, Chaos and fractals (Providence, RI, 1988), Amer. Math. Soc., Providence, RI, 1989, pp. 75–105. MR 1 010 237

155. J. J. Brennan and B. Geist, *Analysis of iterated modular exponentiation: the orbits of* x^α mod N, Des. Codes Cryptogr. **13** (1998), no. 3, 229–245. MR **99b:**11086

156. B. Brent, $3x + 1$ *dynamics on rationals with fixed denominator*, `arXiv:math.DS/0204170`, 2002.

157. R. P. Brent, *On the periods of generalized Fibonacci recurrences*, Math. Comp. **63** (1994), no. 207, 389–401. MR **94i:**11012

158. L. Brenton and R. R. Bruner, *On recursive solutions of a unit fraction equation*, J. Austral. Math. Soc. Ser. A **57** (1994), no. 3, 341–356. MR **95i:**11024

159. J. Brillhart, P. Erdős, and P. Morton, *On sums of Rudin-Shapiro coefficients. II*, Pacific J. Math. **107** (1983), no. 1, 39–69. MR **85i:**11080

160. B. Brindza, *Zeros of polynomials and exponential Diophantine equations*, Compositio Math. **61** (1987), no. 2, 137–157. MR **88d:**11029

161. ———, *On the generators of S-unit groups in algebraic number fields*, Bull. Austral. Math. Soc. **43** (1991), no. 2, 325–329. MR **92m:**11124

162. B. Brindza, K. Győry, and R. Tijdeman, *On the Catalan equation over algebraic number fields*, J. Reine Angew. Math. **367** (1986), 90–102. MR **87g:**11041

163. B. Brindza, K. Liptai, and L. Szalay, *On products of the terms of linear recurrences*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 101–106. MR **99e:**11015

164. B. Brindza, Á. Pintér, and W. M. Schmidt, *Multiplicities of binary recurrences*, Canad. Math. Bull. **44** (2001), no. 1, 19–21. MR **2002a:**11010

165. S. Brlek, *Enumeration of factors in the Thue-Morse word*, Discrete Appl. Math. **24** (1989), no. 1-3, 83–96. MR **90i:**20071

166. S. Brocco, *A note on Mignosi's generalization of the* $(3X+1)$*-problem*, J. Number Theory **52** (1995), no. 2, 173–178. MR **96d:**11025

167. J. Browkin, *The abc-conjecture*, Number theory, Birkhäuser, Basel, 2000, pp. 75–105. MR **2001f:**11053

168. J. Browkin, M. Filaseta, G. Greaves, and A. Schinzel, *Squarefree values of polynomials and the abc-conjecture*, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), Cambridge Univ. Press, Cambridge, 1997, pp. 65–85. MR **99d:**11101

169. G. Brown and W. Moran, *Schmidt's conjecture on normality for commuting matrices*, Invent. Math. **111** (1993), no. 3, 449–463. MR **94c:**11064

170. T. C. Brown, D.-Y. Pei, and P. J.-S. Shiue, *Irrational sums*, Rocky Mountain J. Math. **25** (1995), no. 4, 1219–1223. MR **96m:**11055

171. W. D. Brownawell and D. W. Masser, *Vanishing sums in function fields*, Math. Proc. Cambridge Philos. Soc. **100** (1986), no. 3, 427–434. MR **87k:**11080

172. T. Brox, *Collatz cycles with few descents*, Acta Arith. **92** (2000), no. 2, 181–188. MR **2001a:**11032

173. L. Le Bruyn and M. Van den Bergh, *Algebraic properties of linear cellular automata*, Linear Algebra Appl. **157** (1991), 217–234. MR **92k:**68086

174. Y. Bugeaud, *Linear forms in p-adic logarithms and the Diophantine equation* $(x^n-1)/(x-1)=y^q$, Math. Proc. Cambridge Philos. Soc. **127** (1999), no. 3, 373–381. MR **2000h:**11029

175. ———, *Fundamental systems of S-units with small height and their applications to Diophantine equations*, Publ. Math. Debrecen **56** (2000), no. 3-4, 279–292, Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday. MR **2001d:**11037

176. ———, *On some exponential Diophantine equations*, Monatsh. Math. **132** (2001), no. 2, 93–97. MR **2002c:**11026

177. ———, *On the Diophantine equation* $a(x^n-1)/(x-1)=y^q$, Number theory (Turku, 1999), de Gruyter, Berlin, 2001, pp. 19–24. MR **2002b:**11042

178. ———, *Linear mod one transformations and the distribution of fractional parts* $\{\xi(p/q)^n\}$, Preprint, 2002.

179. ———, *Nombres de Liouville et nombres normaux*, C. R. Math. Acad. Sci. Paris **335** (2002), no. 2, 117–120. MR **2003e:**11081

180. Y. Bugeaud, P. Corvaja, and U. Zannier, *An upper bound for the G.C.D. of* a^n-1 *and* b^n-1, Math. Z. **243** (2003), no. 1, 79–84. MR 1 953 049

181. Y. Bugeaud, G. Hanrot, and M. Mignotte, *Sur l'équation diophantienne* $(x^n-1)/(x-1)=y^q$*. III*, Proc. London Math. Soc. (3) **84** (2002), no. 1, 59–78. MR **2002h:**11027

182. Y. Bugeaud and M. Mignotte, *On integers with identical digits*, Mathematika **46** (1999), no. 2, 411–417. MR **2002d:**11035

183. ———, *L'équation de Nagell-Ljunggren* $\frac{x^n-1}{x-1}=y^q$, Enseign. Math. (2) **48** (2002), no. 1-2, 147–168. MR 1 923 422

184. ______, *On the Diophantine equation $(x^n - 1)/(x - 1) = y^q$ with negative x*, Number Theory for the Millennium, Vol.I, A. K. Peters, Natick, MA, 2002, pp. 145–151. MR 1 956 223

185. Y. Bugeaud, M. Mignotte, and Y. Roy, *On the Diophantine equation $(x^n - 1)/(x - 1) = y^q$*, Pacific J. Math. **193** (2000), no. 2, 257–268. MR **2001f:**11049

186. P. Bundschuh, *Irrationalitätsmaße für e^a, $a \neq 0$ rational oder Liouville-Zahl*, Math. Ann. **192** (1971), 229–242. MR 44 #3962

187. D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3) **12** (1962), 179–192. MR 24 #A2569

188. D. A. Burgess and P. D. T. A. Elliott, *The average of the least primitive root*, Mathematika **15** (1968), 39–50. MR 38 #5736

189. R. J. Burthe, Jr., *The average least witness is* 2, Acta Arith. **80** (1997), no. 4, 327–341. MR **98h:**11118

190. ______, *Upper bounds for least witnesses and generating sets*, Acta Arith. **80** (1997), no. 4, 311–326. MR **98h:**11117

191. R. N. Buttsworth and K. R. Matthews, *On some Markov matrices arising from the generalized Collatz mapping*, Acta Arith. **55** (1990), no. 1, 43–57. MR **92a:**11016

192. J.-Y. Cai, W. H. Fuchs, D. Kozen, and Z. Liu, *Efficient average-case algorithms for the modular group*, 35th Annual Symposium on Foundations of Computer Science (Santa Fe, NM, 1994), IEEE Comput. Soc. Press, Los Alamitos, CA, 1994, pp. 143–152. MR 1 489 243

193. J.-Y. Cai, R. J. Lipton, and Y. Zalcstein, *The complexity of the ABC problem*, SIAM J. Comput. **29** (2000), no. 6, 1878–1888. MR **2001f:**68045

194. J.-Y. Cai and Z. Liu, *The bounded membership problem of the monoid* $\mathrm{SL}_2(\mathbb{N})$, Math. Systems Theory **29** (1996), no. 6, 573–587. MR **98b:**68054

195. E. Çakçak, *A remark on the minimal polynomial of the product of linear recurring sequences*, Finite Fields Appl. **4** (1998), no. 1, 87–97. MR **99b:**11009

196. C. Calude and H. Jürgensen, *Randomness as an invariant for number representations*, Results and trends in theoretical computer science (Graz, 1994), Springer, Berlin, 1994, pp. 44–66. MR **96f:**11100

197. C. Calude, S. Marcus, and I. Ţevy, *The first example of a recursive function which is not primitive recursive*, Historia Math. **6** (1979), no. 4, 380–384. MR **80i:**03053

198. R. Canetti, J. B. Friedlander, S. V. Konyagin, M. Larsen, D. Lieman, and I. E. Shparlinski, *On the statistical properties of Diffie–Hellman distributions*, Israel J. Math. **120** (2000), 23–46. MR **2001k:**11258

199. R. Canetti, J. B. Friedlander, and I. E. Shparlinski, *On certain exponential sums and the distribution of Diffie–Hellman triples*, J. London Math. Soc. (2) **59** (1999), no. 3, 799–812. MR **2000g:**11079

200. E. R. Canfield and N. C. Wormald, *Ménage numbers, bijections and P-recursiveness*, Discrete Math. **63** (1987), no. 2-3, 117–129. MR **88d:**05007

201. L. Cangelmi and F. Pappalardi, *On the r-rank Artin conjecture. II*, J. Number Theory **75** (1999), no. 1, 120–132. MR **2000i:**11149

202. A. Canteaut, P. Charpin, and H. Dobbertin, *Binary m-sequences with three-valued cross-correlation: a proof of Welch's conjecture*, IEEE Trans. Inform. Theory **46** (2000), no. 1, 4–8. MR **2001e:**94011

203. D. G. Cantor, *On arithmetic properties of coefficients of rational functions*, Pacific J. Math. **15** (1965), 55–58. MR 31 #1245

204. ______, *On arithmetic properties of the Taylor series of rational functions.*, Canad. J. Math. **21** (1969), 378–382. MR 39 #422

205. ______, *On arithmetic properties of the Taylor series of rational functions. II*, Pacific J. Math. **41** (1972), 329–334. MR 46 #5286

206. ______, *On the continued fractions of quadratic surds*, Acta Arith. **68** (1994), no. 4, 295–305. MR **96c:**11079

207. W. Carlip and E. Jacobson, *A criterion for stability of two-term recurrence sequences modulo 2^k*, Finite Fields Appl. **2** (1996), no. 4, 369–406. MR **97h:**11012

208. ______, *Unbounded stability of two-term recurrence sequences modulo 2^k*, Acta Arith. **74** (1996), no. 4, 329–346. MR **97b:**11021

209. ______, *Stability of two-term recurrence sequences with even parameter*, Finite Fields Appl. **3** (1997), no. 1, 70–83. MR **98b:**11014

210. W. Carlip, E. Jacobson, and L. Somer, *A criterion for stability of two-term recurrence sequences modulo odd primes*, Applications of Fibonacci numbers, Vol. 7 (Graz, 1996), Kluwer Acad. Publ., Dordrecht, 1998, pp. 49–60. MR 1 638 430

211. W. Carlip and L. Somer, *Bounds for frequencies of residues of regular second-order recurrences modulo p^r*, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 691–719. MR **2000e:**11012

212. G. Carter, *Enumeration results on linear complexity profiles*, Cryptography and coding, II (Cirencester, 1989), Oxford Univ. Press, New York, 1992, pp. 23–34. MR **93b:**94018

213. J. W. S. Cassels, *An embedding theorem for fields*, Bull. Austral. Math. Soc. **14** (1976), no. 2, 193–198, Addendum: **14** (1976), 479–480. MR 54 #10213a

214. ______, *Local fields*, Cambridge University Press, Cambridge, 1986. MR **87i:**11172

215. L. Cerlienco, M. Mignotte, and F. Piras, *Suites récurrentes linéaires: propriétés algébriques et arithmétiques*, Enseign. Math. (2) **33** (1987), no. 1-2, 67–108. MR **88h:**11010

216. U. Cerruti and F. Vaccarino, *R-algebras of linear recurrent sequences*, J. Algebra **175** (1995), no. 1, 332–338. MR **96e:**11030

217. J. S. Chahal, *Topics in number theory*, Plenum Press, New York, 1988. MR **89m:**11001

218. M. Chamberland, *A continuous extension of the $3x + 1$ problem to the real line*, Dynam. Contin. Discrete Impuls. Systems **2** (1996), no. 4, 495–509. MR **97m:**11028

219. D. G. Champernowne, *The construction of decimals normal in the scale of ten*, J. London Math. Soc. **8** (1933), 254–260.

220. A. H. Chan and R. A. Games, *On the linear span of binary sequences obtained from finite geometries*, Advances in cryptology—CRYPTO '86 (Santa Barbara, Calif., 1986), Springer, Berlin, 1987, pp. 405–417. MR **88i:**94025

221. A. H. Chan, M. Goresky, and A. Klapper, *On the linear complexity of feedback registers*, IEEE Trans. Inform. Theory **36** (1990), no. 3, 640–644.

222. Agnes H. Chan and R. A. Games, *On the quadratic spans of de Bruijn sequences*, IEEE Trans. Inform. Theory **36** (1990), no. 4, 822–829. MR **91i:**11014

223. A. Chang, P. Gaal, S. W. Golomb, G. Gong, T. Helleseth, and P. V. Kumar, *On a conjectured ideal autocorrelation sequence and a related triple-error correcting cyclic code*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 680–687. MR **2001d:**94035

224. D. X. Charles, *A note on the subgroup membership problem for* $\mathrm{PSL}(2,p)$, Electronic Colloq. on Comp. Compl., Report 2001-0029 (2001), 1–6.

225. G. Chassé, *Combinatorial cycles of a polynomial map over a commutative field*, Discrete Math. **61** (1986), no. 1, 21–26. MR **87k:**12001

226. I. Chen, *On Siegel's modular curve of level 5 and the class number one problem*, J. Number Theory **74** (1999), no. 2, 278–297. MR **2000b:**11065

227. Y.-G. Chen, *On integers of the form $k2^n + 1$*, Proc. Amer. Math. Soc. **129** (2001), no. 2, 355–361. MR **2003a:**11004

228. ______, *On integers of the forms $k - 2^n$ and $k2^n + 1$*, J. Number Theory **89** (2001), no. 1, 121–125. MR **2002b:**11020

229. J. Cheon and S. Hahn, *The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve*, Acta Arith. **88** (1999), no. 3, 219–222. MR **2000i:**11084

230. B. P. Chisala, *Cycles in Collatz sequences*, Publ. Math. Debrecen **45** (1994), no. 1-2, 35–39. MR **95h:**11019

231. V. Chothi, G. R. Everest, and T. Ward, *S-integer dynamical systems: periodic points*, J. Reine Angew. Math. **489** (1997), 99–132. MR **99b:**11089

232. W. S. Chou, *On inversive maximal period polynomials over finite fields*, Appl. Algebra Engrg. Comm. Comput. **6** (1995), no. 4-5, 245–250. MR **96h:**11126

233. W.-S. Chou, *The period lengths of inversive congruential recursions*, Acta Arith. **73** (1995), no. 4, 325–341. MR **97d:**11118

234. W. S. Chou, *The period lengths of inversive pseudorandom vector generations*, Finite Fields Appl. **1** (1995), no. 1, 126–132. MR **96i:**11087

235. W.-S. Chou and S. D. Cohen, *The dynamics of linearized and sublinearized polynomials in finite fields*, Preprint, 2001.

236. W. S. Chou and G. L. Mullen, *Generating linear spans over finite fields*, Acta Arith. **61** (1992), no. 2, 183–191. MR **93d:**11125

237. W.-S. Chou and H. Niederreiter, *On the lattice test for inversive congruential pseudorandom numbers*, Monte Carlo and quasi-Monte Carlo methods in scientific computing (Las Vegas, NV, 1994), Springer, New York, 1995, pp. 186–197. MR **97k:**65017

238. D. V. Chudnovsky and G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math. **7** (1986), no. 4, 385–434. MR **88h:**11094

239. ———, *Computer assisted number theory with applications*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 1–68. MR **89a:**11130

240. H. Chung and J.-S. No, *Linear span of extended sequences and cascaded GMW sequences*, IEEE Trans. Inform. Theory **45** (1999), no. 6, 2060–2065. MR **2000h:**94024

241. J. Cigler and G. Helmberg, *Neuere Entwicklungen der Theorie der Gleichverteilung*, Jber. Deutsch. Math. Verein. **64** (1961), no. Abt. 1, 1–50 (1961). MR 23 #A2409

242. D. A. Clark and M. Kuwata, *Generalized Artin's conjecture for primitive roots and cyclicity mod* $\mathfrak{p}$ *of elliptic curves over function fields*, Canad. Math. Bull. **38** (1995), no. 2, 167–173. MR **96f:**11150

243. W. E. Clark and L. W. Lewis, *Prime cyclic arithmetic codes and the distribution of power residues*, J. Number Theory **32** (1989), no. 2, 220–225. MR **90f:**94049

244. F. Clarke, *The discrete Fourier transform of a recurrent sequence*, Appl. Algebra Engrg. Comm. Comput. **8** (1997), no. 6, 485–489. MR **98g:**65133

245. A. Clementi and R. Impagliazzo, *The reachability problem for finite cellular automata*, Inform. Process. Lett. **53** (1995), no. 1, 27–31. MR **95k:**68165

246. C. I. Cobeli, S. M. Gonek, and A. Zaharescu, *On the distribution of small powers of a primitive root*, J. Number Theory **88** (2001), no. 1, 49–58. MR **2002c:**11119

247. C. I. Cobeli and A. Zaharescu, *On the distribution of primitive roots mod p*, Acta Arith. **83** (1998), no. 2, 143–153. MR **99a:**11110

248. A. Cobham, *Uniform tag sequences*, Math. Systems Theory **6** (1972), 164–192. MR 56 #15230

249. G. L. Cohen and H. J. J. te Riele, *Iterating the sum-of-divisors function*, Experiment. Math. **5** (1996), no. 2, 91–100, Erratum: **6** (1997), 177. MR **97m:**11007

250. S. D. Cohen and D. Hachenberger, *Actions of linearized polynomials on the algebraic closure of a finite field*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), Amer. Math. Soc., Providence, RI, 1999, pp. 17–32. MR **2000d:**11153

251. ———, *The dynamics of linearized polynomials*, Proc. Edinburgh Math. Soc. (2) **43** (2000), no. 1, 113–128. MR **2001a:**11195

252. S. D. Cohen, H. Niederreiter, I. E. Shparlinski, and M. Zieve, *Incomplete character sums and a special class of permutations*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 53–63. MR **2002e:**11111

253. P. Collas and D. Klein, *An ergodic adding machine on the Cantor set*, Enseign. Math. (2) **40** (1994), no. 3-4, 249–266. MR **96a:**58115

254. A. Compagner and A. Hoogland, *Maximum-length sequences, cellular automata, and random numbers*, J. Comput. Phys. **71** (1987), no. 2, 391–428. MR **89a:**65009

255. A. Conflitti and I. E. Shparlinski, *On the multidimensional distribution of the subset sum generator of pseudorandom numbers*, Math. Comp. (to appear).

256. J. H. Conway and N. J. A. Sloane, *Sphere packings, lattices and groups*, third ed., Springer-Verlag, New York, 1999. MR **2000b:**11077

257. D. Coppersmith and J. Davenport, *Polynomials whose powers are sparse*, Acta Arith. **58** (1991), no. 1, 79–87. MR **92h:**12001

258. D. Coppersmith, H. Krawczyk, and Y. Mansour, *The shrinking generator*, Advances in cryptology—CRYPTO '93 (Santa Barbara, CA, 1993), Springer, Berlin, 1994, pp. 22–39. MR **95c:**94010

259. R. Cordovil, R. Dilão, and A. Noronha da Costa, *Periodic orbits for additive cellular automata*, Discrete Comput. Geom. **1** (1986), no. 3, 277–288. MR **87k:**68114

260. I. P. Cornfeld, S. V. Fomin, and Ya. G. Sinaĭ, *Ergodic theory*, Springer-Verlag, New York, 1982. MR **87f:**28019

261. C. Corrales-Rodrigáñez and R. Schoof, *The support problem and its elliptic analogue*, J. Number Theory **64** (1997), no. 2, 276–290. MR **98c:**11049

262. P. Corvaja and U. Zannier, *Diophantine equations with power sums and universal Hilbert sets*, Indag. Math. (N.S.) **9** (1998), no. 3, 317–332. MR **2000j:**11045

263. ———, *Finiteness of integral values for the ratio of two linear recurrences*, Invent. Math. **149** (2002), no. 2, 431–451. MR 1 918 678

264. ———, *Some new applications of the subspace theorem*, Compositio Math. **131** (2002), 319–340. MR **2003e:**11076

265. ———, *On the greatest prime factor of* $(ab + 1)(ac + 1)$, Proc. Amer. Math. Soc. **131** (2003), no. 6, 1705–1709 (electronic). MR 1 955 256

266. R. Couture and P. L'Ecuyer, *On the lattice structure of certain linear congruential sequences related to AWC/SWB generators*, Math. Comp. **62** (1994), no. 206, 799–808. MR **94g:**65007

267. R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, Springer-Verlag, New York, 2001. MR **2002a:**11007

268. R. Crocker, *On the sum of a prime and of two powers of two*, Pacific J. Math. **36** (1971), 103–107. MR 43 #3200

269. J. Cullen, *Question 15897*, Educational Times (December, 1905), 534.

270. A. J. C. Cunningham and H.J. Woodall, *Factorisation of* $Q = 2^q \pm q$ *and* $q \cdot 2^q \pm 1$, Math. Mag. **47** (1917), 1–38.

271. T. W. Cusick, *Properties of the* x^2 *mod N pseudorandom number generator*, IEEE Trans. Inform. Theory **41** (1995), no. 4, 1155–1159. MR **96k:**65006

272. T. W. Cusick, C. Ding, and Ari Renvall, *Stream ciphers and number theory*, North-Holland Publishing Co., Amsterdam, 1998. MR **99h:**94045

273. T. W. Cusick and H. Dobbertin, *Some new three-valued crosscorrelation functions for binary m-sequences*, IEEE Trans. Inform. Theory **42** (1996), no. 4, 1238–1240. MR **98c:**94013

274. T. W. Cusick and G. Gong, *A conjecture on binary sequences with the "trinomial property"*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 426–427. MR **2001k:**94039

275. Z. D. Dai, *Binary sequences derived from ML-sequences over rings. I. Periods and minimal polynomials*, J. Cryptology **5** (1992), no. 3, 193–207. MR **93g:**68030

276. Z. D. Dai, T. Beth, and D. Gollmann, *Lower bounds for the linear complexity of sequences over residue rings*, Advances in cryptology—EUROCRYPT '90 (Aarhus, 1990), Springer, Berlin, 1991, pp. 189–195.

277. Z. D. Dai, X. N. Feng, M. L. Liu, and Z. X. Wan, *Nonlinear feedforward sequences of m-sequences. III*, Systems Sci. Math. Sci. **7** (1994), no. 4, 367–370. MR **95m:**94004

278. K. Dajani and C. Kraaikamp, *A Gauss-Kusmin theorem for optimal continued fractions*, Trans. Amer. Math. Soc. **351** (1999), no. 5, 2055–2079. MR **99h:**11089

279. ———, *"The mother of all continued fractions"*, Colloq. Math. **84/85** (2000), no. , part 1, 109–123, Dedicated to the memory of Anzelm Iwanik. MR **2001h:**11100

280. ———, *Ergodic theory of numbers*, Carus Mathematical Monographs, vol. 29, Mathematical Association of America, Washington, DC, 2002. MR **2003f:**37014

281. H. Davenport, *Linear forms associated with an algebriac number-field*, Quart. J. Math., Oxford Ser. (2) **3** (1952), 32–41. MR 13,918c

282. ———, *Bases for finite fields*, J. London Math. Soc. **43** (1968), 21–39, Addendum: **44** (1969), 378. MR 37 #2729

283. A. M. Décaillot, *L'arithméticien Édouard Lucas (1842–1891): théorie et instrumentation*, Rev. Histoire Math. **4** (1998), no. 2, 191–236. MR **2000i:**01024

284. F. M. Dekking, *Iteration of maps by an automaton*, Discrete Math. **126** (1994), no. 1-3, 81–86. MR **95d:**11031

285. F. M. Dekking, M. Mendès France, and A. J. van der Poorten, *Folds! 1–3*, Math. Intell. **4** (1982), 130–138, 173–181, 190–195.

286. P. Deligne, *La conjecture de Weil. I*, Inst. Hautes Études Sci. Publ. Math. **43** (1974), 273–307. MR 49 #5013

287. J. Denef, *The rationality of the Poincaré series associated to the p-adic points on a variety*, Invent. Math. **77** (1984), no. 1, 1–23. MR **86c:**11043

288. J. Denef and L. Lipshitz, *Algebraic power series and diagonals*, J. Number Theory **26** (1987), no. 1, 46–67. MR **88f:**16002

289. J. Denef, L. Lipshitz, T. Pheidas, and J. Van Geel (eds.), *Hilbert's tenth problem: relations with arithmetic and algebraic geometry*, Contemporary Mathematics, vol. 270, American Mathematical Society, Providence, RI, 2000, Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999. MR **2001g:**00018

290. C. Deninger, *Deligne periods of mixed motives, K-theory and the entropy of certain $\mathbb{Z}^n$-actions*, J. Amer. Math. Soc. **10** (1997), no. 2, 259–281. MR **97k:**11101

291. L. Denis, *Géométrie et suites récurrentes*, Bull. Soc. Math. France **122** (1994), no. 1, 13–27. MR **95b:**11065

292. ———, *Points périodiques des automorphismes affines*, J. Reine Angew. Math. **467** (1995), 157–167. MR **96m:**14018

293. R. Devaney, *The fractal geometry of the Mandelbrot set*, `math.bu.edu/DYSYS/FRACGEOM/`.

294. A. Diab, *Sur les zéros communs des polynômes exponentiels*, C. R. Acad. Sci. Paris Sér. A-B **281** (1975), no. 18, Ai, A757–A758. MR 52 #11012

295. ———, *Une remarque sur les polynômes exponentiels*, C. R. Acad. Sci. Paris Sér. A-B **280** (1975), Ai, A759–A761. MR 51 #3408

296. C. Ding, *Linear complexity of generalized cyclotomic binary sequences of order* 2, Finite Fields Appl. **3** (1997), no. 2, 159–174. MR **99a:**11017

297. ———, *Autocorrelation values of generalized cyclotomic sequences of order two*, IEEE Trans. Inform. Theory **44** (1998), no. 4, 1699–1702. MR **99h:**94042

298. ———, *Linear complexity of some generalized cyclotomic sequences*, Internat. J. Algebra Comput. **8** (1998), no. 4, 431–442. MR **99k:**11026

299. ———, *Pattern distributions of Legendre sequences*, IEEE Trans. Inform. Theory **44** (1998), no. 4, 1693–1698. MR **2000a:**94011

300. C. Ding and T. Helleseth, *On cyclotomic generator of order r*, Inform. Process. Lett. **66** (1998), no. 1, 21–25. MR **99c:**94029

301. C. Ding, T. Helleseth, and H. Martinsen, *New families of binary sequences with optimal three-level autocorrelation*, IEEE Trans. Inform. Theory **47** (2001), no. 1, 428–433. MR **2003b:**94033

302. C. Ding, T. Helleseth, and W. Shan, *On the linear complexity of Legendre sequences*, IEEE Trans. Inform. Theory **44** (1998), no. 3, 1276–1278. MR **99d:**94017

303. H. Dobbertin, T. Helleseth, P. V.F Kumar, and H. Martinsen, *Ternary m-sequences with three-valued cross-correlation function: new decimations of Welch and Niho type*, IEEE Trans. Inform. Theory **47** (2001), no. 4, 1473–1481. MR **2002f:**94028

304. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), no. 4, 391–401. MR **80i:**10040

305. E. Dobrowolski and K. S. Williams, *An upper bound for the sum $\sum_{n=a+1}^{a+H} f(n)$ for a certain class of functions f*, Proc. Amer. Math. Soc. **114** (1992), no. 1, 29–35. MR **92c:**11086

306. A. Dress and F. Luca, *A characterization of certain binary recurrence sequences*, Algebraic combinatorics and applications (Gößweinstein, 1999), Springer, Berlin, 2001, pp. 89–101. MR **2002e:**11011

307. ———, *Real numbers that have good Diophantine approximations of the form r_{n+1}/r_n*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **28** (2001), 13–19. MR **2002j:**11071

308. ———, *Unbounded integer sequences $(A_n)_{n\geq 0}$ with $A_{n+1}A_{n-1} - A_n^2$ bounded are of Fibonacci type*, Algebraic combinatorics and applications (Gößweinstein, 1999), Springer, Berlin, 2001, pp. 102–109. MR **2002e:**11012

309. M. Drmota, *The distribution of patterns in digital expansions*, Algebraic number theory and Diophantine analysis (Graz, 1998), de Gruyter, Berlin, 2000, pp. 103–121. MR **2001f:**11124

310. M. Drmota and J. Gajdosik, *The distribution of the sum-of-digits function*, J. Théor. Nombres Bordeaux **10** (1998), no. 1, 17–32. MR **2002e:**11095

311. M. Drmota and G. Larcher, *The sum-of-digits-function and uniform distribution modulo 1*, J. Number Theory **89** (2001), no. 1, 65–96. MR **2002e:**11094

312. H. Dubner and W. Keller, *New Fibonacci and Lucas primes*, Math. Comp. **68** (1999), no. 225, 417–427, S1–S12. MR **99c:**11008

313. A. Dujella and R. F. Tichy, *Diophantine equations for second-order recursive sequences of polynomials*, Q. J. Math. **52** (2001), no. 2, 161–169. MR **2002d:**11030

314. J.-M. Dumont, P. J. Grabner, and A. Thomas, *Distribution of the digits in the expansions of rational integers in algebraic bases*, Acta Sci. Math. (Szeged) **65** (1999), no. 3-4, 469–492. MR **2001f:**11132

315. J.-M. Dumont and A. Thomas, *Modifications de nombres normaux par des transducteurs*, Acta Arith. **68** (1994), no. 2, 153–170. MR **96c:**11086

316. B. Durand, *A random NP-complete problem for inversion of 2D cellular automata*, Theoret. Comput. Sci. **148** (1995), no. 1, 19–32. MR **96g:**68086

317. D. Duverney, *Sur l'irrationalité de $\sum_{n=1}^{+\infty} r^n/(q^n - r)$*, C. R. Acad. Sci. Paris Sér. I Math. **320** (1995), no. 1, 1–4. MR **95m:**11075

318. D. Duverney, T. Kanoko, and T. Tanaka, *Transcendence of certain reciprocal sums of linear recurrences*, Monatsh. Math. **137** (2002), no. 2, 115–128. MR 1 937 623

319. R. Dvornicich and U. Zannier, *On sums of roots of unity*, Monatsh. Math. **129** (2000), no. 2, 97–108. MR **2001f:**11183

320. B. M. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648. MR 25 #3914

321. B. M. Dwork and A. J. van der Poorten, *The Eisenstein constant*, Duke Math. J. **65** (1992), no. 1, 23–43. MR **93c:**12010

322. S. Egami, *The distribution of residue classes modulo $\mathfrak{a}$ in an algebraic number field*, Tsukuba J. Math. **4** (1980), no. 1, 9–13. MR **82d:**10070

323. ———, *Average version of Artin's conjecture in an algebraic number field*, Tokyo J. Math. **4** (1981), no. 1, 203–212. MR **83b:**12015

324. J. Eichenauer-Herrmann, *Improved lower bounds for the discrepancy of inversive congruential pseudorandom numbers*, Math. Comp. **62** (1994), no. 206, 783–786. MR **94g:**11058

325. ———, *On generalized inversive congruential pseudorandom numbers*, Math. Comp. **63** (1994), no. 207, 293–299. MR **94k:**11088

326. J. Eichenauer-Herrmann and F. Emmerich, *Compound inversive congruential pseudorandom numbers: an average-case analysis*, Math. Comp. **65** (1996), no. 213, 215–225. MR **96i:**65005

327. J. Eichenauer-Herrmann, F. Emmerich, and G. Larcher, *Average discrepancy, hyperplanes, and compound pseudorandom numbers*, Finite Fields Appl. **3** (1997), no. 3, 203–218. MR **98j:**11059

328. J. Eichenauer-Herrmann, E. Herrmann, and S. Wegenkittl, *A survey of quadratic and inversive congruential pseudorandom numbers*, Monte Carlo and quasi-Monte Carlo methods 1996 (Salzburg), Springer, New York, 1998, pp. 66–97. MR **99d:**11085

329. J. Eichenauer-Herrmann and G. Larcher, *Average behaviour of compound nonlinear congruential pseudorandom numbers*, Finite Fields Appl. **2** (1996), no. 1, 111–123. MR **97b:**11103

330. J. Eichenauer-Herrmann and H. Niederreiter, *An improved upper bound for the discrepancy of quadratic congruential pseudorandom numbers*, Acta Arith. **69** (1995), no. 2, 193–198. MR **95k:**11099

331. J. Eichenauer-Herrmann and A. Topuzoğlu, *On the period length of congruential pseudorandom number sequences generated by inversions*, J. Comput. Appl. Math. **31** (1990), no. 1, 87–96. MR **92e:**65008

332. M. Einsiedler, G. R. Everest, and T. Ward, *Primes in sequences associated to polynomials (after Lehmer)*, LMS J. Comput. Math. **3** (2000), 125–139. MR **2002a:**11017

333. ———, *Morphic heights and periodic points*, New York Number Theory Seminar (2001), `arXiv:math.NT/0204179`.

334. ———, *Primes in elliptic divisibility sequences*, LMS J. Comput. Math. **4** (2001), 1–15. MR **2002e:**11181

335. M. Einsiedler and T. Ward, *Asymptotic geometry of non-mixing shapes*, Ergodic Theory Dynam. Systems **23** (2003), 75–85.

336. E. El Mahassni, P. Q. Nguyen, and I. E. Shparlinski, *The insecurity of Nyberg-Rueppel and other DSA-like signature schemes with partially known nonces*, Cryptography and lattices (Providence, RI, 2001), Lecture Notes in Comput. Sci., vol. 2146, Springer, Berlin, 2001, pp. 97–109. MR **2003e:**94066

337. E. El Mahassni and I. E. Shparlinski, *On the uniformity of distribution of congruential generators over elliptic curves*, Sequences and their applications (Bergen, 2001), Springer, Berlin, 2002, pp. 257–264. MR **2003e:**94055

338. S. Eliahou, *The $3x + 1$ problem: new lower bounds on nontrivial cycle lengths*, Discrete Math. **118** (1993), no. 1-3, 45–56. MR **94h:**11017

339. N. Elkies, *Non-torsion points of low height on elliptic curves*, `www.math.harvard.edu/~elkies/low_height.html`.

340. ———, *On finite sequences satisfying linear recursions*, New York J. Math. **8** (2002), 85–97. MR **2003e:**15029

341. N. Elkies, G. Kuperberg, M. Larsen, and J. Propp, *Alternating-sign matrices and domino tilings. I*, J. Algebraic Combin. **1** (1992), no. 2, 111–132. MR **94f:**52035

342. ———, *Alternating-sign matrices and domino tilings. II*, J. Algebraic Combin. **1** (1992), no. 3, 219–234. MR **94f:**52036

343. P. D. T. A. Elliott and L. Murata, *On the average of the least primitive root modulo p*, J. London Math. Soc. (2) **56** (1997), no. 3, 435–454. MR **98m:**11094

344. F. Emmerich, *Pseudorandom vector generation by the compound inversive method*, Math. Comp. **65** (1996), no. 214, 749–760. MR **96m:**11064

345. ———, *Equidistribution properties of compound inversive pseudorandom vectors*, Finite Fields Appl. **4** (1998), no. 1, 16–28. MR **99b:**11087

346. J. W. England, *The zeta function of toral endomorphisms*, Proc. Amer. Math. Soc. **34** (1972), 321–322. MR 45 #3431

347. J. W. England and R. L. Smith, *The zeta function of automorphisms of solenoid groups*, J. Math. Anal. Appl. **39** (1972), 112–121. MR 46 #6400

348. D. Erdmann and S. Murphy, *An approximate distribution for the maximum order complexity*, Des. Codes Cryptogr. **10** (1997), no. 3, 325–339. MR **97k:**94027

349. P. Erdős, *On the sum* $\sum_{d|2^n-1} d^{-1}$, Israel J. Math. **9** (1971), 43–48. MR 42 #4508

350. P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic number theory (Allerton Park, IL, 1989), Birkhäuser Boston, Boston, MA, 1990, pp. 165–204. MR **92a:**11113

351. P. Erdős, P. Kiss, and C. Pomerance, *On prime divisors of Mersenne numbers*, Acta Arith. **57** (1991), no. 3, 267–281. MR **92d:**11104

352. P. Erdős, P. Kiss, and A. Sárközy, *A lower bound for the counting function of Lucas pseudoprimes*, Math. Comp. **51** (1988), no. 183, 315–323. MR **89e:**11011

353. P. Erdős and K. Mahler, *Some arithmetical properties of the convergents of a continued fraction*, J. London Math. Soc. **14** (1939), 12–18.

354. P. Erdős and M. Ram Murty, *On the order of* $a \pmod p$, Number theory (Ottawa, ON, 1996), Amer. Math. Soc., Providence, RI, 1999, pp. 87–97. MR **2000c:**11152

355. P. Erdős and A. M. Odlyzko, *On the density of odd integers of the form* $(p-1)2^{-n}$ *and related questions*, J. Number Theory **11** (1979), no. 2, 257–263. MR **80i:**10077

356. P. Erdős and T. N. Shorey, *On the greatest prime factor of* $2^p - 1$ *for a prime p and other expressions*, Acta Arith. **30** (1976), no. 3, 257–265. MR 54 #7402

357. P. Erdős, C. L. Stewart, and R. Tijdeman, *Some Diophantine equations with many solutions*, Compositio Math. **66** (1988), no. 1, 37–56. MR **89j:**11027

358. A. Eremenko and L. A. Rubel, *On the zero sets of certain entire functions*, Proc. Amer. Math. Soc. **124** (1996), no. 8, 2401–2404. MR **96j:**30045

359. G. R. Everest, *A "Hardy-Littlewood" approach to the S-unit equation*, Compositio Math. **70** (1989), no. 2, 101–118. MR **90g:**11124

360. ———, *p-primary parts of unit traces and the p-adic regulator*, Acta Arith. **62** (1992), no. 1, 11–23. MR **93i:**11134

361. ———, *An asymptotic formula implied by the Leopoldt conjecture*, Quart. J. Math. Oxford Ser. (2) **45** (1994), no. 177, 19–28. MR **95b:**11103

362. ———, *The mean value of a sum of S-units*, J. London Math. Soc. (2) **51** (1995), no. 3, 417–428. MR **96h:**11022

363. ———, *Mean values of algebraic linear forms*, Proc. London Math. Soc. (3) **70** (1995), no. 3, 529–555. MR **96b:**11096

364. ———, *On the p-adic integral of an exponential polynomial*, Bull. London Math. Soc. **27** (1995), no. 4, 334–340. MR **96c:**11137

365. G. R. Everest and J. H. Loxton, *Counting algebraic units with bounded height*, J. Number Theory **44** (1993), no. 2, 222–227. MR **94g:**11105

366. G. R. Everest and A. J. van der Poorten, *Factorisation in the ring of exponential polynomials*, Proc. Amer. Math. Soc. **125** (1997), no. 5, 1293–1298. MR **97h:**16038

367. G. R. Everest, A. J. van der Poorten, Y. Puri, and T. Ward, *Integer sequences and periodic points*, J. Integer Seq. **5** (2002), no. 2, Article 02.2.3, 10 pp. MR 1 938 222

368. G. R. Everest, P. Rogers, and T. Ward, *A higher rank Mersenne problem*, ANTS V Springer Lecture Notes in Computer Science **2369** (2002), 95–107.

369. G. R. Everest and I. E. Shparlinski, *Divisor sums of generalised exponential polynomials*, Canad. Math. Bull. **39** (1996), no. 1, 35–46. MR **97g:**11021

370. ———, *Counting the values taken by algebraic exponential polynomials*, Proc. Amer. Math. Soc. **127** (1999), no. 3, 665–675. MR **99f:**11042

371. ———, *Zsigmondy's theorem for elliptic curves*, Preprint, 2002.

372. G. R. Everest and N. Stephens, *Primes generated by elliptic curves*, Preprint, 2002.

373. G. R. Everest and T. Ward, *Heights of polynomials and entropy in algebraic dynamics*, Springer-Verlag London Ltd., London, 1999. MR **2000e:**11087

374. ———, *The canonical height of an algebraic point on an elliptic curve*, New York J. Math. **6** (2000), 331–342. MR **2001j:**11056

375. J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **75** (1984), no. 3, 561–584. MR **85f:**11048

376. ———, *On sums of S-units and linear recurrences*, Compositio Math. **53** (1984), no. 2, 225–244. MR **86c:**11045

377. ———, *The number of solutions of linear equations in roots of unity*, Acta Arith. **89** (1999), no. 1, 45–51. MR **2000e:**11033

378. J.-H. Evertse, K. Győry, C. L. Stewart, and R. Tijdeman, *S-unit equations and their applications*, New advances in transcendence theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, pp. 110–174. MR **89j:**11028

379. J.-H. Evertse, P. Moree, C. L. Stewart, and R. Tijdeman, *Multivariate Diophantine equations with many solutions*, Acta Arith. **107** (2003), no. 1, 103–125.

380. J.-H. Evertse and H. P. Schlickewei, *The absolute subspace theorem and linear equations with unknowns from a multiplicative group*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 121–142. MR **2000d:**11094

381. ———, *A quantitative version of the absolute subspace theorem*, J. Reine Angew. Math. **548** (2002), 21–127. MR 1 915 209

382. J.-H. Evertse, H. P. Schlickewei, and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2) **155** (2002), no. 3, 807–836. MR 1 923 966

383. F. Fabris, *Periods distribution in the linear feedback generalized registers*, J. Inform. Optim. Sci. **16** (1995), no. 1, 61–82. MR **96c:**94003

384. J. Fabrykowski, *On quadratic residues and nonresidues in difference sets modulo m*, Proc. Amer. Math. Soc. **122** (1994), no. 2, 325–331. MR **95a:**11003

385. G. Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), no. 3, 549–576. MR **93d:**11066

386. G. Faltings and G. Wüstholz, *Diophantine approximations on projective spaces*, Invent. Math. **116** (1994), no. 1-3, 109–138. MR **95g:**11068

387. W. Feit, *On large Zsigmondy primes*, Proc. Amer. Math. Soc. **102** (1988), no. 1, 29–36. MR **89b:**11009

388. R. G. Ferretti, *An estimate for the multiplicity of binary recurrences*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 11, 1143–1148. MR **99f:**11086

389. M. Filaseta and S. Konyagin, *On a limit point associated with the abc-conjecture*, Colloq. Math. **76** (1998), no. 2, 265–268. MR **99b:**11029

390. P. Fitzpatrick and S. M. Jennings, *Comparison of two algorithms for decoding alternant codes*, Appl. Algebra Engrg. Comm. Comput. **9** (1998), no. 3, 211–220. MR **99h:**94069

391. P. Fitzpatrick and G. H. Norton, *The Berlekamp-Massey algorithm and linear recurring sequences over a factorial domain*, Appl. Algebra Engrg. Comm. Comput. **6** (1995), no. 4-5, 309–323. MR **96j:**94015

392. M. Flahive and H. Niederreiter, *On inversive congruential generators for pseudorandom numbers*, Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991), Dekker, New York, 1993, pp. 75–80. MR **94a:**11117

393. P. Flajolet, P. J. Grabner, P. Kirschenhofer, H. Prodinger, and R. F. Tichy, *Mellin transforms and asymptotics: digital sums*, Theoret. Comput. Sci. **123** (1994), no. 2, 291–314. MR **94m:**11090

394. A. Flammenkamp and F. Luca, *Binomial coefficients and Lucas sequences*, J. Number Theory **93** (2002), no. 2, 246–284. MR **2003d:**11047

395. L. Flatto, *Z-numbers and β-transformations*, Symbolic dynamics and its applications (New Haven, CT, 1991), Amer. Math. Soc., Providence, RI, 1992, pp. 181–201. MR **94c:**11065

396. L. Flatto, J. C. Lagarias, and A. D. Pollington, *On the range of fractional parts $\{\xi(p/q)^n\}$*, Acta Arith. **70** (1995), no. 2, 125–147. MR **96a:**11073

397. L. Flatto, J. C. Lagarias, and B. Poonen, *The zeta function of the beta transformation*, Ergodic Theory Dynam. Systems **14** (1994), no. 2, 237–266. MR **95c:**58141

398. M. Fletcher and G. C. Smith, *Chaos, elliptic curves and all that*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 245–256. MR **95a:**11055

399. E. V. Flynn, B. Poonen, and E. F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-*2 *curve*, Duke Math. J. **90** (1997), no. 3, 435–463. MR **98j:**11048

400. N. P. Fogg, *Substitutions in dynamics, arithmetics and combinatorics*, Lecture Notes in Mathematics, vol. 1794, Springer, Berlin, 2002.

401. W. Forman and H. N. Shapiro, *An arithmetic property of certain rational powers*, Comm. Pure Appl. Math. **20** (1967), 561–573. MR 35 #2852

402. A. S. Fraenkel, *Iterated floor function, algebraic numbers, discrete chaos, Beatty subsequences, semigroups*, Trans. Amer. Math. Soc. **341** (1994), no. 2, 639–664. MR **94d:**11011

403. Z. Franco and C. Pomerance, *On a conjecture of Crandall concerning the $qx + 1$ problem*, Math. Comp. **64** (1995), no. 211, 1333–1336. MR **95j:**11019

404. J. N. Franklin, *Deterministic simulation of random processes*, Math. Comp. **17** (1963), 28–59. MR 26 #7125

405. ______, *Equidistribution of matrix-power residues modulo one*, Math. Comp. **18** (1964), 560–568. MR 30 #3077

406. J. B. Friedlander, J. Hansen, and I. E. Shparlinski, *Character sums with exponential functions*, Mathematika **47** (2000), no. 1-2, 75–85 (2002). MR 1 924 489

407. ______, *On the distribution of the power generator modulo a prime power*, Preprint, 2001.

408. J. B. Friedlander, S. Konyagin, and I. E. Shparlinski, *Some doubly exponential sums over $\mathbb{Z}_m$*, Acta Arith. **105** (2002), no. 4, 349–370. MR 1 932 568

409. J. B. Friedlander, M. Larsen, D. Lieman, and I. E. Shparlinski, *On the correlation of binary M-sequences*, Des. Codes Cryptogr. **16** (1999), no. 3, 249–256. MR **2000g:**94024

410. J. B. Friedlander, D. Lieman, and I. E. Shparlinski, *On the distribution of the RSA generator*, Sequences and their applications (Singapore, 1998), Springer, London, 1999, pp. 205–212. MR **2002f:**11108

411. J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Period of the power generator and small values of Carmichael's function*, Math. Comp. **70** (2001), no. 236, 1591–1605. MR **2002g:**11112

412. J. B. Friedlander and I. E. Shparlinski, *Double exponential sums over thin sets*, Proc. Amer. Math. Soc. **129** (2001), no. 6, 1617–1621. MR **2001m:**11137

413. ______, *On the distribution of Diffie–Hellman triples with sparse exponents*, SIAM J. Discrete Math. **14** (2001), no. 2, 162–169. MR **2003a:**94036

414. ______, *On the distribution of the power generator*, Math. Comp. **70** (2001), no. 236, 1575–1589. MR **2002f:**11107

415. A. M. Frieze, J. Håstad, R. Kannan, J. C. Lagarias, and A. Shamir, *Reconstructing truncated integer variables satisfying linear congruences*, SIAM J. Comput. **17** (1988), no. 2, 262–280. MR **89d:**11115

416. C. Frougny, *Representations of numbers and finite automata*, Math. Systems Theory **25** (1992), no. 1, 37–60. MR **93b:**68054

417. ______, *On multiplicatively dependent linear numeration systems, and periodic points*, Theor. Inform. Appl. **36** (2002), no. 3, 293–314. MR 1 958 245

418. C. Fuchs, *An upper bound for the G.C.D. of two linear recurring sequences*, Math. Slovaca (to appear).

419. C. Fuchs and R. F. Tichy, *Perfect powers in linear recurring sequences*, Acta Arith. **107** (2003), 9–25. MR 1 956 982

420. A. Fúster-Sabater and P. Caballero-Gil, *On the linear complexity of nonlinearly filtered PN-sequences*, Advances in cryptology—ASIACRYPT '94 (Wollongong, 1994), Springer, Berlin, 1995, pp. 80–90.

421. D. Gale, *Somos sequence update*, Mathematical Intelligencer **13** (1991), no. 4, 49–50.

422. ______, *The strange and surprising saga of the Somos sequences*, Mathematical Intelligencer **13** (1991), no. 1, 40–42.

423. S. Gao, J. von zur Gathen, and D. Panario, *Gauss periods: orders and cryptographical applications*, Math. Comp. **67** (1998), no. 221, 343–352. MR **98c:**11134

424. A. García and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory **30** (1988), no. 3, 345–356. MR **90a:**14027

425. M. V. P. Garcia and F. A. Tal, *A note on the generalized* $3n+1$ *problem*, Acta Arith. **90** (1999), no. 3, 245–250. MR **2000i:**11019

426. J. von zur Gathen, A. Knopfmacher, F. Luca, L. G. Lucht, and I. E. Shparlinski, *Average order in cyclic groups*, J. Théor. Nombres Bordeaux (to appear).

427. J. von zur Gathen and F. Pappalardi, *Density estimates related to Gauss periods*, Proc. Workshop on Cryptography and Computational Number Theory (CCNT'99), Singapore (K.-Y. Lam, I. E. Shparlinski, H. Wang, and C. Xing, eds.), Birkhäuser, 2001, pp. 33–41.

428. J. von zur Gathen and I. E. Shparlinski, *Orders of Gauss periods in finite fields*, Appl. Algebra Engrg. Comm. Comput. **9** (1998), no. 1, 15–24. MR **99j:**11142

429. ______, *Constructing elements of large order in finite fields*, Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999), Springer, Berlin, 1999, pp. 404–409. MR **2002g:**12001

430. ______, *Gauß periods in finite fields*, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 162–177. MR **2002h:**11132

431. G. Ge, *Recognizing units in number fields*, Math. Comp. **63** (1994), no. 207, 377–387. MR **94i:**11107

432. A. O. Gelfond, *Sur les divisere premiers de valeurs de la fonction exponentielle*, Proc. Phys. Math. Inst. Acad. Sci. USSR **5** (1934).

433. A. Ghosh, *The distribution of* αp^2 *modulo* 1, Proc. London Math. Soc. (3) **42** (1981), no. 2, 252–269. MR **82j:**10067

434. K. Girstmair, *On the cosets of the* $2q$*-power group in the unit group modulo* p, Abh. Math. Sem. Univ. Hamburg **62** (1992), 217–232. MR **94a:**11165

435. ______, *The digits of* $1/p$ *in connection with class number factors*, Acta Arith. **67** (1994), no. 4, 381–386. MR **96g:**11134

436. ______, *Class number factors and distribution of residues*, Abh. Math. Sem. Univ. Hamburg **67** (1997), 65–104. MR **99e:**11141

437. J. P. Glass, J. H. Loxton, and A. J. van der Poorten, *Identifying a rational function*, C. R. Math. Rep. Acad. Sci. Canada **3** (1981), no. 5, 279–284. MR **82m:**10018

438. D. Gluck and B. D. Taylor, *A new statistic for the* $3x+1$ *problem*, Proc. Amer. Math. Soc. **130** (2002), no. 5, 1293–1301. MR **2002k:**11031

439. J. Dj. Golić, *On the linear complexity of functions of periodic* GF(q) *sequences*, IEEE Trans. Inform. Theory **35** (1989), no. 1, 69–75. MR **90e:**94022

440. S. W. Golomb and G. Gong, *Periodic binary sequences with the "trinomial property"*, IEEE Trans. Inform. Theory **45** (1999), no. 4, 1276–1279. MR **2000g:**94026

441. S. W. Golomb, G. Gong, and Z. D. Dai, *Cyclic inequivalence of cascaded GMW-sequences*, Discrete Math. **219** (2000), no. 1-3, 279–285. MR **2001i:**94046

442. G. Gong, *Theory and applications of* q*-ary interleaved sequences*, IEEE Trans. Inform. Theory **41** (1995), no. 2, 400–411. MR **96b:**94008

443. ______, *On* q*-ary cascaded GMW sequences*, IEEE Trans. Inform. Theory **42** (1996), 263–267.

444. ______, *New designs for signal sets with low cross-correlation, balance property and large linear span:* GF(p) *case*, Faculty of Math., Univ. Waterloo, Research Report CORR 2000-32 (2000).

445. G. Gong, T. A. Berson, and D. R. Stinson, *Elliptic curve pseudorandom sequence generators*, Selected areas in cryptography (Kingston, ON, 1999), Springer, Berlin, 2000, pp. 34–48. MR **2001j:**94032

446. G. Gong, Z. D. Dai, and S. W. Golomb, *Enumeration and criteria for cyclically shift-distinct GMW sequences*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 474–484. MR **2001h:**94019

447. G. Gong and S. W. Golomb, *Binary sequences with two-level autocorrelation*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 692–693. MR **99j:**94032

448. G. Gong and C. C. Y. Lam, *Linear recursive sequences over elliptic curves*, Sequences and their applications (Bergen, 2001), Springer, Berlin, 2002, pp. 182–196.

449. M. I. González Vasco, M. Näslund, and I. E. Shparlinski, *The hidden number problem in extension fields and its applications*, Lect. Notes in Comp. Sci. **2286** (2002).

450. M. I. González Vasco and I. E. Shparlinski, *On the security of Diffie–Hellman bits*, Proc. Workshop on Cryptography and Computational Number Theory (CCNT'99), Singapore (K.-Y. Lam, I. E. Shparlinski, H. Wang, and C. Xing, eds.), Birkhäuser, 2001, pp. 257–268.

451. ———, *Security of the most significant bits of the Shamir message passing scheme*, Math. Comp. **71** (2002), no. 237, 333–342. MR **2002j:**11153

452. D. M. Gordon, *On the number of elliptic pseudoprimes*, Math. Comp. **52** (1989), no. 185, 231–245. MR **89f:**11169

453. ———, *Pseudoprimes on elliptic curves*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 290–305. MR **91g:**11158

454. ———, *Equidistant arithmetic codes and character sums*, J. Number Theory **46** (1994), no. 3, 323–333. MR **95d:**11165

455. D. M. Gordon and C. Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), no. 196, 825–838. MR **92h:**11081

456. M. Goresky and A. Klapper, *Arithmetic crosscorrelations of feedback with carry shift register sequences*, IEEE Trans. Inform. Theory **43** (1997), no. 4, 1342–1345. MR **98j:**94010

457. M. Goresky, A. Klapper, M. Ram Murty, and I. E. Shparlinski, *On decimations of ℓ-sequences*, Preprint, 2002.

458. M. Goresky, A. Klapper, and L. Washington, *Fourier transforms and the 2-adic span of periodic binary sequences*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 687–691. MR **2001k:**94041

459. R. Göttfert and H. Niederreiter, *On the minimal polynomial of the product of linear recurring sequences*, Finite Fields Appl. **1** (1995), no. 2, 204–218. MR **96h:**11007

460. X. Gourdon and B. Salvy, *Effective asymptotics of linear recurrences with rational coefficients*, Proceedings of the 5th Conference on Formal Power Series and Algebraic Combinatorics (Florence, 1993), vol. 153, 1996, pp. 145–163. MR **97c:**11013

461. E. Gourin, *On irreducible polynomials in several variables which become reducible when the variables are replaced by powers of themselves*, Trans. Amer. Math. Soc. **32** (1930), no. 3, 485–501.

462. W. T. Gowers, *Fourier analysis and Szemerédi's theorem*, Proceedings of the International Congress of Mathematicians, Vol. I (Berlin, 1998), vol. Extra Vol. I, 1998, pp. 617–629. MR **2000i:**11026

463. ———, *A new proof of Szemerédi's theorem for arithmetic progressions of length four*, Geom. Funct. Anal. **8** (1998), no. 3, 529–551, Erratum: **11** (2001), 869. MR **2000d:**11019

464. ———, *A new proof of Szemerédi's theorem*, Geom. Funct. Anal. **11** (2001), no. 3, 465–588. MR **2002k:**11014

465. P. J. Grabner, P. Kirschenhofer, H. Prodinger, and R. F. Tichy, *On the moments of the sum-of-digits function*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 263–271. MR **95d:**11123

466. P. J. Grabner, P. Kiss, and R. F. Tichy, *Diophantine approximation in terms of linear recurrent sequences*, Number theory (Halifax, NS, 1994), Amer. Math. Soc., Providence, RI, 1995, pp. 187–195. MR **97h:**11085

467. P. J. Grabner and P. Liardet, *Harmonic properties of the sum-of-digits function for complex bases*, Acta Arith. **91** (1999), no. 4, 329–349. MR **2001f:**11126

468. P. J. Grabner, P. Liardet, and R. F. Tichy, *Odometers and systems of numeration*, Acta Arith. **70** (1995), no. 2, 103–123. MR **96b:**11108

469. P. J. Grabner and J. M. Thuswaldner, *On the sum of digits function for number systems with negative bases*, Ramanujan J. **4** (2000), no. 2, 201–220. MR **2001m:**11015

470. P. J. Grabner, R. F. Tichy, and R. Winkler, *On the stability of the quotients of successive terms of linear recurring sequences*, Number-theoretic and algebraic methods in computer science (Moscow, 1993), World Sci. Publishing, River Edge, NJ, 1995, pp. 185–192. MR **97b:**11099

471. M. Grady and M. Newman, *Residue periodicity in subgroup counting functions*, The Rademacher legacy to mathematics (University Park, PA, 1992), Amer. Math. Soc., Providence, RI, 1994, pp. 265–273. MR **96b:**20028

472. S. W. Graham and C. J. Ringrose, *Lower bounds for least quadratic nonresidues*, Analytic number theory (Allerton Park, IL, 1989), Birkhäuser Boston, Boston, MA, 1990, pp. 269–309. MR **92d:**11108

473. D. Grant, *Sequences of fields with many solutions to the unit equation*, Rocky Mountain J. Math. **26** (1996), no. 3, 1017–1029. MR **98f:**11121

474. J. Grantham, *A probable prime test with high confidence*, J. Number Theory **72** (1998), no. 1, 32–47. MR **2000e:**11160

475. ______, *Frobenius pseudoprimes*, Math. Comp. **70** (2001), no. 234, 873–891. MR **2001g:**11191

476. A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*, Organic mathematics (Burnaby, BC, 1995), Amer. Math. Soc., Providence, RI, 1997, pp. 253–276. MR **99h:**11016

477. A. Granville and Z.-W. Sun, *Values of Bernoulli polynomials*, Pacific J. Math. **172** (1996), no. 1, 117–137. MR **98b:**11018

478. F. Griffin, H. Niederreiter, and I. E. Shparlinski, *On the distribution of nonlinear recursive congruential pseudorandom numbers of higher orders*, Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999), Springer, Berlin, 1999, pp. 87–93. MR **2002j:**94038

479. F. Griffin and I. E. Shparlinski, *On the linear complexity of the Naor-Reingold pseudorandom function*, Lect. Notes in Comp. Sci. **1726** (1999), 301–308.

480. ______, *On the linear complexity profile of the power generator*, IEEE Trans. Inform. Theory **46** (2000), no. 6, 2159–2162. MR **2001k:**94053

481. G. Grisel, *Sur la longueur de la fraction continue de α^n*, Acta Arith. **74** (1996), no. 2, 161–176. MR **96m:**11004

482. ______, *Length of the powers of a rational fraction*, J. Number Theory **62** (1997), no. 2, 322–337. MR **98a:**11088

483. ______, *Length of continued fractions in principal quadratic fields*, Acta Arith. **85** (1998), no. 1, 35–49. MR **99g:**11015

484. M. Gromov, *Groups of polynomial growth and expanding maps*, Inst. Hautes Études Sci. Publ. Math. **53** (1981), 53–73. MR **83b:**53041

485. G. Grossman and F. Luca, *Sum of factorials in binary recurrence sequences*, J. Number Theory **93** (2002), 87–107. MR **2002m:**11011

486. D. Guillaume and F. Morain, *Building pseudoprimes with a large number of prime factors*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 4, 263–277. MR **98d:**11011

487. R. Gupta and M. Ram Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130. MR **86d:**11003

488. ______, *Primitive points on elliptic curves*, Compositio Math. **58** (1986), no. 1, 13–44. MR **87h:**11050

489. ______, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math. **101** (1990), no. 1, 225–235. MR **91e:**11065

490. S. Gupta and D. Zagier, *On the coefficients of the minimal polynomials of Gaussian periods*, Math. Comp. **60** (1993), no. 201, 385–398. MR **93d:**11086

491. S. Gurak, *Pseudoprimes for higher-order linear recurrence sequences*, Math. Comp. **55** (1990), no. 192, 783–813. MR **91a:**11067

492. ______, *On higher-order pseudoprimes of Lehmer type*, Number theory (Halifax, NS, 1994), Amer. Math. Soc., Providence, RI, 1995, pp. 215–227. MR **96f:**11167

493. ______, *On the minimal polynomials for certain Gauss periods over finite fields*, Finite fields and applications (Glasgow, 1995), Cambridge Univ. Press, Cambridge, 1996, pp. 85–96. MR **97m:**11150

494. ______, *On the middle factor of the period polynomial for finite fields*, Number theory (Ottawa, ON, 1996), Amer. Math. Soc., Providence, RI, 1999, pp. 121–131. MR **2000b:**11134

495. R. Guralnick, T. Penttila, C. E. Praeger, and J. Saxl, *Linear groups with orders having certain large prime divisors*, Proc. London Math. Soc. (3) **78** (1999), no. 1, 167–214. MR **99m:**20113

496. J. Gutierrez and D. Gomes-Perez, *Iterations of multivariate polynomials and discrepancy of pseudorandom numbers*, Lect. Notes in Comp. Sci. **2227** (2001), 192–199.

497. J. Gutierrez, H. Niederreiter, and I. E. Shparlinski, *On the multidimensional distribution of inversive congruential pseudorandom numbers in parts of the period*, Monatsh. Math. **129** (2000), no. 1, 31–36. MR **2001e:**11088

498. J. Gutierrez, I. E. Shparlinski, and A. Winterhof, *On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators*, IEEE Trans. Inform. Theory **49** (2003), 60–64.

499. R. K. Guy, *Unsolved problems in number theory*, second ed., Springer-Verlag, New York, 1994. MR **96e:**11002

500. K. Győry, *On some arithmetical properties of Lucas and Lehmer numbers*, Acta Arith. **40** (1981/82), no. 4, 369–373. MR **83k:**10018

501. ———, *On arithmetic graphs associated with integral domains*, A tribute to Paul Erdős, Cambridge Univ. Press, Cambridge, 1990, pp. 207–222. MR **92h:**11023

502. ———, *On arithmetic graphs associated with integral domains. II*, Sets, graphs and numbers (Budapest, 1991), North-Holland, Amsterdam, 1992, pp. 365–374. MR **94e:**11025

503. ———, *Some recent applications of S-unit equations*, Astérisque **209** (1992), 11, 17–38. MR **94e:**11026

504. K. Győry, P. Kiss, and A. Schinzel, *On Lucas and Lehmer sequences and their applications to Diophantine equations*, Colloq. Math. **45** (1981), no. 1, 75–80 (1982). MR **83g:**10009

505. L. Hajdu, *A quantitative version of Dirichlet's S-unit theorem in algebraic number fields*, Publ. Math. Debrecen **42** (1993), no. 3-4, 239–246. MR **94e:**11118

506. L. Halbeisen and N. Hungerbühler, *Optimal bounds for the length of rational Collatz cycles*, Acta Arith. **78** (1997), no. 3, 227–239. MR **98g:**11025

507. M. Hall, *An isomorphism between linear recurring sequences and algebraic rings*, Trans. Amer. Math. Soc. **44** (1938), no. 2, 196–218.

508. S. Hallgren, *Linear congruential generators over elliptic curves*, Preprint CS-94-143, Dept. of Comp. Sci., Carnegie Mellon Univ., 1994.

509. F. Halter-Koch and W. Narkiewicz, *Finiteness properties of polynomial mappings*, Math. Nachr. **159** (1992), 7–18. MR **94j:**14016

510. ———, *Polynomial mappings defined by forms with a common factor*, Sém. Théor. Nombres Bordeaux (2) **4** (1992), no. 2, 187–198. MR **94g:**11020

511. ———, *Polynomial cycles in finitely generated domains*, Monatsh. Math. **119** (1995), no. 4, 275–279. MR **96d:**13035

512. ———, *Scarcity of finite polynomial orbits*, Publ. Math. Debrecen **56** (2000), no. 3-4, 405–414, Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday. MR **2001h:**11028

513. G. Hansel, *Une démonstration simple du théorème de Skolem-Mahler-Lech*, Theoret. Comput. Sci. **43** (1986), no. 1, 91–98. MR **88j:**11091

514. J. C. Hansen and E. Schmutz, *How random is the characteristic polynomial of a random matrix?*, Math. Proc. Cambridge Philos. Soc. **114** (1993), no. 3, 507–515. MR **94j:**05009

515. G. H. Hardy, *Divergent series*, Oxford, at the Clarendon Press, 1949. MR 11,25a

516. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, fifth ed., The Clarendon Press Oxford University Press, New York, 1979. MR **81i:**10002

517. D. Harkin, *On the mathematical work of François-Édouard-Anatole Lucas*, Enseignement Math. (2) **3** (1957), 276–288. MR 20 #3762

518. G. Harman, *Trigonometric sums over primes. I*, Mathematika **28** (1981), no. 2, 249–254 (1982). MR **83j:**10045

519. ———, *One hundred years of normal numbers*, Number Theory for the Millennium, Vol.II, A. K. Peters, Natick, MA, 2002, pp. 149–166.

520. S. Hatjispyros and F. Vivaldi, *A family of rational zeta functions for the quadratic map*, Nonlinearity **8** (1995), no. 3, 321–332. MR **96c:**58141

521. D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38. MR **88a:**11004

522. ———, *Integer sets containing no arithmetic progressions*, J. London Math. Soc. (2) **35** (1987), no. 3, 385–394. MR **88g:**11005

523. ———, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), no. 2, 265–338. MR **93a:**11075

524. D. R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum*, Q. J. Math. **51** (2000), no. 2, 221–235. MR **2001h:**11106

525. T. Helleseth, *Some results about the cross-correlation function between two maximal linear sequences*, Discrete Math. **16** (1976), no. 3, 209–232. MR 55 #2341

526. ———, *Correlation of m-sequences and related topics*, Sequences and their applications (Singapore, 1998), Springer, London, 1999, pp. 49–66. MR **2002f:**94030

527. T. Helleseth and P. V. Kumar, *Sequences with low correlation*, Handbook of coding theory, Vol. I, II, North-Holland, Amsterdam, 1998, pp. 1765–1853.

528. T. Helleseth, P. V. Kumar, and H. Martinsen, *A new family of ternary sequences with ideal two-level autocorrelation function*, Des. Codes Cryptogr. **23** (2001), no. 2, 157–166. MR **2002e**:94090

529. T. Helleseth and H. M. Martinsen, *Binary sequences of period $2^m - 1$ with large linear complexity*, Inform. and Comput. **151** (1999), no. 1-2, 73–91. MR **2000c**:11025

530. D. Hensley, *The distribution mod n of fractions with bounded partial quotients*, Pacific J. Math. **166** (1994), no. 1, 43–54. MR **95i**:11083

531. T. Herlestam, *On functions of linear shift register sequences*, Advances in cryptology—EUROCRYPT '85 (Linz, 1985), Springer, Berlin, 1986, pp. 119–129. MR **87g**:94017

532. S. Hernándes and F. Luca, *On the largest prime factor of $(ab+1)(ac+1)(bc+1)$*, Preprint, 2002.

533. M. Hindry and J. H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), no. 2, 419–450. MR **89k**:11044

534. ______, *On Lehmer's conjecture for elliptic curves*, Séminaire de Théorie des Nombres, Paris 1988–1989, Birkhäuser Boston, Boston, MA, 1990, pp. 103–116. MR **92e**:11062

535. P. A. Hines, *Characterising the linear complexity of span 1 de Bruijn sequences over finite fields*, J. Combin. Theory Ser. A **81** (1998), no. 2, 140–148. MR **99b**:05012

536. ______, *On the minimum linear complexity of de Bruijn sequences over non-prime finite fields*, J. Combin. Theory Ser. A **86** (1999), no. 1, 127–139. MR **2000b**:94014

537. A. Hinkkanen, *Zeta functions of rational functions are rational*, Ann. Acad. Sci. Fenn. Ser. A I Math. **19** (1994), no. 1, 3–10. MR **94h**:58137

538. J. G. Hinz, *A note on Artin's conjecture in algebraic number fields*, J. Number Theory **22** (1986), no. 3, 334–349. MR **87f**:11067

539. A. Hof and O. Knill, *Cellular automata with almost periodic initial conditions*, Nonlinearity **8** (1995), no. 4, 477–491. MR **96g**:58093

540. H. D. L. Hollmann and Q. Xiang, *A proof of the Welch and Niho conjectures on cross-correlations of binary m-sequences*, Finite Fields Appl. **7** (2001), no. 2, 253–286. MR **2002f**:94031

541. A. N. W. Hone, N. Joshi, and A. V. Kitaev., *An entire function defined by a nonlinear recurrence relation*, J. London Math. Soc. (2) **66** (2002), no. 2, 377–387. MR 1 920 409

542. C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR 34 #7445

543. ______, *Applications of sieve methods to the theory of numbers*, Cambridge University Press, Cambridge, 1976. MR 53 #7976

544. A. E. D. Houston, *On the limit of maximal density of sequences with a perfect linear complexity profile*, Des. Codes Cryptogr. **10** (1997), no. 3, 351–359. MR **98a**:94022

545. E. W. Howe, *Higher-order Carmichael numbers*, Math. Comp. **69** (2000), no. 232, 1711–1719. MR **2001a**:11012

546. E. Hrushovski, P. H. Kropholler, A. Lubotzky, and A. Shalev, *Powers in finitely generated groups*, Trans. Amer. Math. Soc. **348** (1996), no. 1, 291–304. MR **96f**:20061

547. H. Hu and Z.-W. Sun, *An extension of Lucas' theorem*, Proc. Amer. Math. Soc. **129** (2001), no. 12, 3471–3478 (electronic). MR **2002i**:11019

548. P.-C. Hu and C.-C. Yang, *A generalized abc-conjecture over function fields*, J. Number Theory **94** (2002), 286–298. MR **2003d**:11055

549. C. Hua and G.-Z. Xiao, *The linear complexity of binary sequences with period $(2^n - 1)^k$*, IEEE Trans. Inform. Theory **37** (1991), 672–673.

550. L. K. Hua, *Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie*, B. G. Teubner Verlagsgesellschaft, Leipzig, 1959. MR 24 #A94

551. K. Huber, *On the period length of generalized inversive pseudorandom number generators*, Appl. Algebra Engrg. Comm. Comput. **5** (1994), no. 5, 255–260. MR **96c**:11090

552. M. Iosifescu and C. Kraaikamp, *On Denjoy's canonical continued fraction expansion*, Osaka J. Math. **40** (2003), no. 1, 235–244. MR 1 955 806

553. S. Jakubec, J. Kostra, and K. Nemoga, *On the existence of an integral normal basis generated by a unit in prime extensions of rational numbers*, Math. Comp. **56** (1991), no. 194, 809–815. MR **91h**:11117

554. D. Jarden, *Any Lucas number L_{5p}, for any prime $p > 5$, has at least two distinct primitive prime divisors*, Fibonacci Quart. **6** (1968), 407.

555. D. Jarden and M. Jarden, *On the existence of an infinitude of composite primitive divisors of second-order recurring sequences*, Fibonacci Quart. **6** (1968), 322–334, 406. MR 39 #1422

556. E. Jen, *Linear cellular automata and recurring sequences in finite fields*, Comm. Math. Phys. **119** (1988), no. 1, 13–28. MR **90h:**68085

557. ———, *Aperiodicity in one-dimensional cellular automata*, Chaos (Woods Hole, MA, 1989), Amer. Inst. Phys., New York, 1990, pp. 121–144. MR **93d:**68052

558. ———, *Exact solvability and quasiperiodicity of one-dimensional cellular automata*, Nonlinearity **4** (1991), no. 2, 251–276. MR **92j:**68084

559. E. Jensen and M. Ram Murty, *Artin's conjecture for polynomials over finite fields*, Number theory, Birkhäuser, Basel, 2000, pp. 167–181. MR **2001h:**11153

560. T. Johansson, *A shift register construction of unconditionally secure authentication codes*, Des. Codes Cryptogr. **4** (1994), no. 1, 69–81. MR **94j:**94014

561. J. P. Jones and P. Kiss, *An asymptotic formula concerning Lehmer numbers*, Publ. Math. Debrecen **42** (1993), no. 3-4, 199–213. MR **94j:**11015

562. ———, *Representation of integers as terms of a linear recurrence with maximal index*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **25** (1998), 21–37 (1999). MR **2000i:**11032

563. J. A. Joseph, *A chaotic extension of the $3x + 1$ function to $\mathbb{Z}_2[i]$*, Fibonacci Quart. **36** (1998), no. 4, 309–316. MR **99f:**11026

564. N. Joshi and A. V. Kitaev, *On Boutroux's tritronquée solutions of the first Painlevé equation*, Stud. Appl. Math. **107** (2001), no. 3, 253–291. MR **2002g:**34202

565. A. Joux and J. Stern, *Lattice reduction: a toolbox for the cryptanalyst*, J. Cryptology **11** (1998), no. 3, 161–185. MR **99c:**94031

566. S.-M. Jung and B. Volkmann, *Remarks on a paper of Wagner*, J. Number Theory **56** (1996), no. 2, 329–335. MR **96k:**11095

567. T. Kagawa and N. Terai, *Squares in Lucas sequences and some Diophantine equations*, Manuscripta Math. **96** (1998), no. 2, 195–202. MR **99i:**11019

568. T. Kaida, S. Uehara, and K. Imamura, *An algorithm for the k-error linear complexity of sequences over* GF(p^m) *with period p^n, p a prime*, Inform. and Comput. **151** (1999), no. 1-2, 134–147. MR **2000f:**94020

569. ———, *A new algorithm for the k-error linear complexity of sequences over* GF(p^m) *with period p^n*, Sequences and their applications (Singapore, 1998), Springer, London, 1999, pp. 284–296. MR **2002i:**11129

570. ———, *On the profile of the k-error linear complexity and zero sum property of sequences over* GF(p^m) *with period p^n*, Sequences and their applications (Bergen, 2001), Springer, Berlin, 2002, pp. 218–227. MR **2003d:**94060

571. T. Kamae, *Number-theoretic problems involving two independent bases*, Number theory and cryptography (Sydney, 1989), Cambridge Univ. Press, Cambridge, 1990, pp. 196–203. MR **91h:**11073

572. O. V. Kamlovskiĭ and A. S. Kuz′min, *Distribution of elements on cycles of linear recurrent sequences over Galois rings*, Uspekhi Mat. Nauk **53** (1998), no. 2(320), 149–150. MR **99e:**11022

573. R. Kannan and R. J. Lipton, *Polynomial-time algorithm for the orbit problem*, J. Assoc. Comput. Mach. **33** (1986), no. 4, 808–821. MR **88b:**68086

574. H. Kano, *General constructions of normal numbers of Korobov type*, Osaka J. Math. **30** (1993), no. 4, 909–919. MR **94j:**11069

575. ———, *A remark on Wagner's ring of normal numbers*, Arch. Math. (Basel) **60** (1993), no. 1, 46–50. MR **94f:**11068

576. H. Kano and I. Shiokawa, *Rings of normal and nonnormal numbers*, Israel J. Math. **84** (1993), no. 3, 403–416. MR **95e:**11086

577. H. J. Karloff and P. Raghavan, *Randomized algorithms and pseudorandom numbers*, J. Assoc. Comput. Mach. **40** (1993), no. 3, 454–476. MR **96h:**68096

578. M. Karpinski, A. J. van der Poorten, and I. E. Shparlinski, *Zero testing of p-adic and modular polynomials*, Theoret. Comput. Sci. **233** (2000), no. 1-2, 309–317. MR **2001m:**12016

579. M. Karpinski and I. E. Shparlinski, *On some approximation problems concerning sparse polynomials over finite fields*, Theoret. Comput. Sci. **157** (1996), no. 2, 259–266. MR **96m:**68084

580. T. Kato, L.-M. Wu, and N. Yanagihara, *The serial test for a nonlinear pseudorandom number generator*, Math. Comp. **65** (1996), no. 214, 761–769. MR **96g:**65007

581. A. Katok and B. Hasselblatt, *Introduction to the modern theory of dynamical systems*, Cambridge University Press, Cambridge, 1995. MR **96c:**58055

582. N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Princeton University Press, Princeton, NJ, 1988. MR **91a:**11028

583. W. Keller, *New Cullen primes*, Math. Comp. **64** (1995), no. 212, 1733–1741, S39–S46, With a biographical sketch of James Cullen by T. G. Holt and a supplement by Keller and Wolfgang Niebuhr. MR **95m:**11015

584. B. W. Kernighan and D. M. Ritchie, *The* **C** *programming language*, Prentice Hall, Englewood Cliffs, NJ, 1988.

585. K. H. Kim, N. S. Ormes, and F. W. Roush, *The spectra of nonnegative integer matrices via formal power series*, J. Amer. Math. Soc. **13** (2000), no. 4, 773–806. MR **2001g:**15013

586. C. Kimberling, *Terms common to two sequences satisfying the same linear recurrence*, Applications of Fibonacci numbers, Vol. 4 (Winston-Salem, NC, 1990), Kluwer Acad. Publ., Dordrecht, 1991, pp. 177–188. MR **93j:**11009

587. P. Kiss, *Zero terms in second-order linear recurrences*, Math. Sem. Notes Kobe Univ. **7** (1979), no. 1, 145–152. MR **80j:**10015

588. ______, *On common terms of linear recurrences*, Acta Math. Acad. Sci. Hungar. **40** (1982), no. 1-2, 119–123. MR **84h:**10014

589. ______, *Differences of the terms of linear recurrences*, Studia Sci. Math. Hungar. **20** (1985), no. 1-4, 285–293. MR **88f:**11008

590. ______, *Primitive divisors of Lucas numbers*, Applications of Fibonacci numbers (San Jose, CA, 1986), Kluwer Acad. Publ., Dordrecht, 1988, pp. 29–38. MR **89j:**11016

591. ______, *On rank of apparition of primes in Lucas sequences*, Publ. Math. Debrecen **36** (1989), no. 1-4, 147–151 (1990). MR **91e:**11019

592. ______, *On prime divisors of the terms of second order linear recurrence sequences*, Applications of Fibonacci numbers, Vol. 3 (Pisa, 1988), Kluwer Acad. Publ., Dordrecht, 1990, pp. 203–207. MR **92g:**11013

593. ______, *On primitive prime power divisors of Lucas numbers*, Number theory, Vol. II (Budapest, 1987), North-Holland, Amsterdam, 1990, pp. 773–786. MR **91g:**11014

594. ______, *Some results concerning the reciprocal sum of prime divisors of a Lucas number*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 417–420. MR **95b:**11091

595. ______, *Pure powers and power classes in recurrence sequences*, Math. Slovaca **44** (1994), no. 5, 525–529. MR **96c:**11017

596. ______, *An approximation problem concerning linear recurrences*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 289–293. MR **99d:**11089

597. ______, *On sums of the reciprocals of prime divisors of terms of a linear recurrence*, Applications of Fibonacci numbers, Vol. 7, Kluwer Acad. Publ., Dordrecht, 1998, pp. 215–220.

598. ______, *On a problem concerning perfect powers in linear recurrences*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **26** (1999), 25–30 (2000). MR **2001a:**11021

599. ______, *Note on a result of I. Nemes and A. Pethő concerning polynomial values in linear recurrences*, Publ. Math. Debrecen **56** (2000), no. 3-4, 451–455, Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday. MR **2001f:**11018

600. ______, *Results concerning products and sums of the terms of linear recurrences*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **27** (2000), 1–7 (2001). MR **2002a:**11011

601. P. Kiss and F. Mátyás, *An asymptotic formula for π*, J. Number Theory **31** (1989), no. 3, 255–259. MR **90e:**11036

602. ______, *Perfect powers from the sums of terms of linear recurrences*, Period. Math. Hungar. **42** (2001), no. 1-2, 163–168. MR **2002k:**11017

603. ______, *Products of the terms of linear recurrences*, Studia Sci. Math. Hungar. **37** (2001), no. 3-4, 355–362. MR **2002i:**11014

604. P. Kiss and B. M. Phong, *Weakly composite Lucas numbers*, Ann. Univ. Sci. Budapest. Eötvös Sect. Math. **31** (1988), 179–182 (1989). MR **90j:**11017

605. ______, *Reciprocal sum of prime divisors of Lucas numbers*, Acta Acad. Paed. Agriensis, Sect. Math. **19** (1989), 47–54.

606. P. Kiss and B. Tropak, *Average order of logarithms of terms in binary recurrences*, Discuss. Math. **10** (1990), 29–39 (1991). MR **93e:**11021

607. P. Kiss and B. Zay, *On sequences of zeros and ones*, Studia Sci. Math. Hungar. **29** (1994), no. 3-4, 437–442. MR **95h:**11021

608. B. Kitchens and K. Schmidt, *Markov subgroups of* $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{Z}^2}$, Symbolic dynamics and its applications (New Haven, CT, 1991), Amer. Math. Soc., Providence, RI, 1992, pp. 265–283. MR **93k:**58136

609. ______, *Mixing sets and relative entropies for higher-dimensional Markov shifts*, Ergodic Theory Dynam. Systems **13** (1993), no. 4, 705–735. MR **95f:**28022

610. A. Klapper, *The vulnerability of geometric sequences based on fields of odd characteristic*, J. Cryptology **7** (1994), no. 1, 33–51. MR **94j:**94015

611. ______, *d-form sequences: families of sequences with low correlation values and large linear spans*, IEEE Trans. Inform. Theory **41** (1995), no. 2, 423–431. MR **96f:**11162

612. ______, *Large families of sequences with near-optimal correlations and large linear span*, IEEE Trans. Inform. Theory **42** (1996), no. 4, 1241–1248. MR **97m:**94017

613. ______, *On the existence of secure feedback registers*, Lect. Notes in Comp. Sci. **1070** (1996), 256–267.

614. ______, *Cross-correlations of quadratic form sequences in odd characteristic*, Des. Codes Cryptogr. **11** (1997), no. 3, 289–305. MR **98j:**94021

615. A. Klapper, A. H. Chan, and M. Goresky, *Cross-correlations of linearly and quadratically related geometric sequences and GMW sequences*, Discrete Appl. Math. **46** (1993), no. 1, 1–20. MR **94g:**94015

616. A. Klapper and M. Goresky, *Partial period autocorrelations of geometric sequences*, IEEE Trans. Inform. Theory **40** (1994), no. 2, 494–502. MR **95h:**94016

617. ______, *Feedback shift registers, 2-adic span, and combiners with memory*, J. Cryptology **10** (1997), no. 2, 111–147. MR **98f:**94012

618. A. Klapper and J. Xu, *Algebraic feedback shift registers*, Theoret. Comput. Sci. **226** (1999), no. 1-2, 61–92, Cryptography. MR **2001m:**94040

619. D. E. Knuth, *The art of computer programming. Vol. 2*, third ed., Addison-Wesley Publishing Co., Reading, Mass., 1998. MR **83i:**68003

620. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag, New York, 1977. MR 57 #5964

621. ______, *A course in number theory and cryptography*, Springer-Verlag, New York, 1987. MR **88i:**94001

622. ______, *Elliptic curve cryptosystems*, Math. Comp. **48** (1987), no. 177, 203–209. MR **88b:**94017

623. D. R. Kohel and I. E. Shparlinski, *On exponential sums and group generators for elliptic curves over finite fields*, Algorithmic number theory (Leiden, 2000), Springer, Berlin, 2000, pp. 395–404. MR **2003c:**11094

624. S. V. Konjagin, *Letter to the editors: "The number of solutions of congruences of the nth degree with one unknown" [Mat. Sb. (N.S.) 109(151)(2), 171–187, 327, 1979; MR 80k:10013a]*, Mat. Sb. (N.S.) **110(152)** (1979), no. 1, 158. MR **80k:**10013b

625. ______, *The number of solutions of congruences of the nth degree with one unknown*, Mat. Sb. (N.S.) **109(151)** (1979), no. 2, 171–187, 327. MR **80k:**10013a

626. M. Kontsevich and D. Zagier, *Periods*, Mathematics unlimited—2001 and beyond, Springer, Berlin, 2001, pp. 771–808. MR **2002i:**11002

627. S. V. Konyagin, *Estimates for Gaussian sums and Waring's problem modulo a prime*, Trudy Mat. Inst. Steklov. **198** (1992), 111–124. MR **96e:**11122

628. S. V. Konyagin and C. Pomerance, *On primes recognizable in deterministic polynomial time*, The mathematics of Paul Erdős, I, Springer, Berlin, 1997, pp. 176–198. MR **98a:**11184

629. S. V. Konyagin and I. E. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge University Press, Cambridge, 1999. MR **2000h:**11089

630. S. V. Konyagin and T. Steger, *Polynomial congruences*, Mat. Zametki **55** (1994), no. 6, 73–79, 158. MR **96e:**11043

631. A. N. Korobov, *Continued fractions of some normal numbers*, Mat. Zametki **47** (1990), no. 2, 28–33, 158. MR **91c:**11044

632. N. M. Korobov, *The distribution of non-residues and of primitive roots in recurrence series*, Doklady Akad. Nauk SSSR (N.S.) **88** (1953), 603–606. MR 14,846j

633. ———, *Unimprovable estimates of trigonometric sums with exponential functions*, Doklady Akad. Nauk SSSR (N.S.) **89** (1953), 597–600. MR 15,15d

634. ———, *Teoretiko-chislovye metody v priblizhennom analize*, Gosudarstv. Izdat. Fiz.-Mat. Lit., Moscow, 1963. MR 28 #716

635. ———, *Distribution of fractional parts of exponential functions*, Vestnik Moskov. Univ. Ser. I Mat. Meh. **21** (1966), no. 4, 42–46. MR 33 #5600

636. ———, *Trigonometric sums with exponential functions, and the distribution of the digits in periodic fractions*, Mat. Zametki **8** (1970), 641–652. MR 43 #6165

637. ———, *The distribution of digits in periodic fractions*, Mat. Sb. (N.S.) **89(131)** (1972), 654–670, 672. MR 54 #12619

638. C. Kraaikamp, *A new class of continued fraction expansions*, Acta Arith. **57** (1991), no. 1, 1–39. MR **92a:**11090

639. C. Kraaikamp and H. Nakada, *On normal numbers for continued fractions*, Ergodic Theory Dynam. Systems **20** (2000), no. 5, 1405–1421. MR **2001i:**11101

640. I. Krasikov and J. C. Lagarias, *Bounds for the $3x+1$ problem using difference inequalities*, `arXiv:math.NT/0205002`, 2002.

641. H. Krawczyk, *How to predict congruential generators*, J. Algorithms **13** (1992), no. 4, 527–545. MR **93g:**65013

642. ———, *LFSR-based hashing and authentication*, Lect. Notes in Comp. Sci. **839** (1994), 129–139.

643. M. Křížek, F. Luca, and L. Somer, *17 lectures on Fermat numbers*, Springer-Verlag, New York, 2001, From number theory to geometry, With a foreword by Alena Šolcová. MR **2002i:**11001

644. K. K. Kubota, *On a conjecture of Morgan Ward. I*, Acta Arith. **33** (1977), no. 1, 11–28.

645. ———, *On a conjecture of Morgan Ward. II*, Acta Arith. **33** (1977), no. 1, 29–48.

646. ———, *On a conjecture of Morgan Ward. III*, Acta Arith. **33** (1977), no. 2, 99–109. MR 56 #235b

647. L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience [John Wiley & Sons], New York, 1974. MR 54 #7415

648. M. R. S. Kulenović and G. Ladas, *Dynamics of second order rational difference equations*, Chapman & Hall/CRC, Boca Raton, FL, 2002, With open problems and conjectures. MR 1 935 074

649. P. V. Kumar and T. Helleseth, *An expansion for the coordinates of the trace function over Galois rings*, Appl. Algebra Engrg. Comm. Comput. **8** (1997), no. 5, 353–361. MR **98e:**11142

650. S. R. Kumar and D. Sivakumar, *Efficient self-testing/self-correction of linear recurrences*, 37th Annual Symposium on Foundations of Computer Science (Burlington, VT, 1996), IEEE Comput. Soc. Press, Los Alamitos, CA, 1996, pp. 602–611.

651. E. Kuo, *Applications of graphical condensation for enumerating matchings and tilings*, Preprint, 2002.

652. V. L. Kurakin, *Representations over the ring $\mathbb{Z}_{p^n}$ of a linear recursive sequence of maximal period over the field $GF(p)$*, Diskret. Mat. **4** (1992), no. 4, 96–116. MR **94e:**11013

653. ———, *Convolution of linear recurrent sequences*, Uspekhi Mat. Nauk **48** (1993), no. 4(292), 235–236. MR **94k:**11018

654. ———, *The structure of Hopf algebras of linear recurrent sequences*, Uspekhi Mat. Nauk **48** (1993), no. 5(293), 177–178. MR **94k:**16066

655. ———, *The first coordinate sequence of a linear recurrence of maximum period over a Galois ring*, Diskret. Mat. **6** (1994), no. 2, 88–100. MR **95h:**11140

656. ———, *Representations over a field of linear recurrents of maximal period over a residue ring*, Uspekhi Mat. Nauk **49** (1994), no. 2(296), 157–158. MR **95g:**11011

657. P. Kurlberg, *On the order of unimodular matrices modulo integers*, `arXiv:math.NT/0202053`, 2001.

658. P. Kurlberg and Z. Rudnick, *On quantum ergodicity for linear maps of the torus*, Comm. Math. Phys. **222** (2001), no. 1, 201–227. MR **2002j:**81082

659. K. Kurosawa, F. Sato, T. Sakata, and W. Kishimoto, *A relationship between linear complexity and k-error linear complexity*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 694–698. MR **2001i:**94055

660. H. C. Kurtz, *The linear cubic p-adic recurrence and its value function*, Illinois J. Math. **8** (1964), 125–131. MR 28 #2993

661. A. S. Kuz′min, *Distribution of elements on cycles of linear recurrence sequences over residue rings*, Uspekhi Mat. Nauk **47** (1992), no. 6(288), 213–214. MR **94c:**11018

662. A. S. Kuz′min and A. A. Nechaev, *Construction of noise-stable codes using linear recurrent sequences over Galois rings*, Uspekhi Mat. Nauk **47** (1992), no. 5(287), 183–184. MR **93m:**51010

663. ———, *Linear recurrence sequences over Galois rings*, Uspekhi Mat. Nauk **48** (1993), no. 1(289), 167–168. MR **95b:**11113

664. J. C. Lagarias, *The* $3x+1$ *problem and its generalizations*, Amer. Math. Monthly **92** (1985), no. 1, 3–23. MR **86i:**11043

665. ———, *The set of primes dividing the Lucas numbers has density* 2/3, Pacific J. Math. **118** (1985), no. 2, 449–461, Erratum: **162** (1994), 393–396. MR **86i:**11007

666. ———, *Pseudorandom number generators in cryptography and number theory*, Cryptology and computational number theory (Boulder, CO, 1989), Amer. Math. Soc., Providence, RI, 1990, pp. 115–143. MR **92f:**11109

667. J. C. Lagarias, H. A. Porta, and K. B. Stolarsky, *Asymmetric tent map expansions. I. Eventually periodic points*, J. London Math. Soc. (2) **47** (1993), no. 3, 542–556. MR **94h:**58139

668. ———, *Asymmetric tent map expansions. II. Purely periodic points*, Illinois J. Math. **38** (1994), no. 4, 574–588. MR **96b:**58093

669. J. C. Lagarias and J. A. Reeds, *Unique extrapolation of polynomial recurrences*, SIAM J. Comput. **17** (1988), no. 2, 342–362. MR **89c:**11025

670. J. C. Lagarias and A. Weiss, *The* $3x+1$ *problem: two stochastic models*, Ann. Appl. Probab. **2** (1992), no. 1, 229–261. MR **92k:**60159

671. D. Laksov, *Linear recurring sequences over finite fields*, Math. Scand. **16** (1965), 181–196. MR 33 #2559

672. E. Lange, *Cellular automata, substitutions and factorization of polynomials over finite fields*, Finite fields and applications (Glasgow, 1995), Cambridge Univ. Press, Cambridge, 1996, pp. 163–179. MR **98e:**11028

673. ———, *Substitutions for linear shift register sequences and the factorization algorithms of Berlekamp and Niederreiter*, Linear Algebra Appl. **249** (1996), 217–228. MR **98a:**94014

674. T. Lange, S. V. Konyagin, and I. E. Shparlinski, *Linear complexity of the discrete logarithm*, Des. Codes Cryptogr. **28** (2003), 135–146.

675. K. Langmann, *Primzahlen in Fibonacci-Progressionen*, Arch. Math. (Basel) **65** (1995), no. 2, 125–129. MR **96d:**11022

676. V. Laohakosol, *Some extensions of the Skolem-Mahler-Lech theorem*, Exposition. Math. **7** (1989), no. 2, 137–187. MR **91b:**11017

677. G. Larcher, *A bound for the discrepancy of digital nets and its application to the analysis of certain pseudo-random number generators*, Acta Arith. **83** (1998), no. 1, 1–15. MR **99j:**11086

678. G. Larcher and H. Niederreiter, *Optimal coefficients modulo prime powers in the three-dimensional case*, Ann. Mat. Pura Appl. (4) **155** (1989), 299–315. MR **91e:**65014

679. G. Larcher, R. Wolf, and J. Eichenauer-Herrmann, *On the average discrepancy of successive tuples of pseudo-random numbers over parts of the period*, Monatsh. Math. **127** (1999), no. 2, 141–154. MR **2000c:**11130

680. R. G. Larson and E. J. Taft, *The algebraic structure of linearly recursive sequences under Hadamard product*, Israel J. Math. **72** (1990), no. 1-2, 118–132. MR **92g:**16056

681. A. Lasjaunias, *A survey of Diophantine approximation in fields of power series*, Monatsh. Math. **130** (2000), no. 3, 211–229. MR **2001k:**11135

682. A. Lasjaunias and J.-J. Ruch, *Algebraic and badly approximable power series over a finite field*, Finite Fields Appl. **8** (2002), no. 1, 91–107. MR **2002i:**11067

683. A. G. B. Lauder, *Polynomials with odd orthogonal multiplicity*, Finite Fields Appl. **4** (1998), no. 4, 453–464. MR **99h:**11020

684. ———, *Continued fractions of Laurent series with partial quotients from a given set*, Acta Arith. **90** (1999), no. 3, 251–271. MR **2000j:**11103

685. M. Laurent, *Minoration de la hauteur de Néron-Tate*, Seminar on number theory, Paris 1981–82 (Paris, 1981/1982), Birkhäuser Boston, Boston, MA, 1983, pp. 137–151. MR **85e:**11048

686. ———, *Équations exponentielles-polynômes et suites récurrentes linéaires. II*, J. Number Theory **31** (1989), no. 1, 24–53. MR **90b:**11023

687. W. M. Lawton, *A problem of Boyd concerning geometric means of polynomials*, J. Number Theory **16** (1983), no. 3, 356–362. MR **84i:**10056

688. R. R. Laxton, *Linear recurrences of order two*, J. Austral. Math. Soc. **7** (1967), 108–114. MR 34 #7489

689. ———, *On groups of linear recurrences. I*, Duke Math. J. **36** (1969), 721–736. MR 41 #3427

690. ———, *On groups of linear recurrences. II. Elements of finite order*, Pacific J. Math. **32** (1970), 173–179. MR 41 #3428

691. ———, *On a problem of M. Ward*, Fibonacci Quart. **12** (1974), 41–44. MR 52 #10577

692. J. W. Layman, *Maximum zero strings of Bell numbers modulo primes*, J. Combin. Theory Ser. A **40** (1985), no. 1, 161–168. MR **87a:**11020

693. M. H. Le, *A note on the Diophantine equation $(x^m-1)/(x-1)=y^n+1$*, Math. Proc. Cambridge Philos. Soc. **116** (1994), no. 3, 385–389. MR **95h:**11030

694. C. Lech, *A note on recurring series*, Ark. Mat. **2** (1953), 417–421. MR 15,104e

695. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.

696. ———, *The mathematical work of Morgan Ward*, Math. Comp. **61** (1993), no. 203, 307–311. MR **93k:**01071

697. S. Lehr, J. Shallit, and J. Tromp, *On the vector space of the automatic reals*, Theoret. Comput. Sci. **163** (1996), no. 1-2, 193–210. MR **97i:**03037

698. F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields*, Exposition. Math. **13** (1995), no. 5, 385–416. MR **96i:**11115

699. H. W. Lenstra, Jr., *Euclidean number fields of large degree*, Invent. Math. **38** (1976/77), no. 3, 237–254. MR 55 #2836

700. ———, *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224. MR 58 #576

701. H. W. Lenstra, Jr. and R. J. Schoof, *Primitive normal bases for finite fields*, Math. Comp. **48** (1987), no. 177, 217–231. MR **88c:**11076

702. H. W. Lenstra, Jr. and J. Shallit, *Continued fractions and linear recurrences*, Math. Comp. **61** (1993), no. 203, 351–354. MR **93k:**11004

703. A. Leutbecher and G. Niklasch, *On cliques of exceptional units and Lenstra's construction of Euclidean fields*, Number theory (Ulm, 1987), Springer, New York, 1989, pp. 150–178. MR **90i:**11123

704. V. I. Levenshteĭn, *Bounds for packings of metric spaces and some of their applications*, Problemy Kibernet. **40** (1983), 43–110. MR **86c:**52014

705. M. B. Levin, *The uniform distribution of the sequence $\{\alpha\lambda^x\}$*, Mat. Sb. (N.S.) **98(140)** (1975), no. 2 (10), 207–222, 333. MR 53 #10732

706. ———, *The distribution of the fractional parts of the exponential function*, Izv. Vysš. Učebn. Zaved. Matematika **11** (1977), no. 186, 50–57. MR 58 #21963

707. ———, *Absolutely normal numbers*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. **1** (1979), 31–37, 87. MR **80d:**10076

708. ———, *On the complete uniform distribution of the fractional parts of the exponential function*, Trudy Sem. Petrovsk. **7** (1981), 245–256. MR **83j:**10059

709. ———, *Uniform distribution of a matrix exponential function*, Investigations in number theory (Russian), Saratov. Gos. Univ., Saratov, 1988, pp. 46–62. MR **91d:**11085

710. ———, *The choice of parameters in generators of pseudorandom numbers*, Dokl. Akad. Nauk SSSR **307** (1989), no. 3, 529–534. MR **91d:**11093

711. ———, *Simultaneously absolutely normal numbers*, Mat. Zametki **48** (1990), no. 6, 61–71. MR **92g:**11077

712. ———, *On the discrepancy of Markov-normal sequences*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 413–428. MR **97k:**11113

713. ———, *Discrepancy estimates of completely uniformly distributed and pseudorandom number sequences*, Internat. Math. Res. Notices **22** (1999), 1231–1251. MR **2001f:**11129

714. ———, *On the discrepancy estimate of normal numbers*, Acta Arith. **88** (1999), no. 2, 99–111. MR **2000j:**11115

715. M. B. Levin and I. E. Shparlinski, *Uniform distribution of fractional parts of recurrent sequences*, Uspekhi Mat. Nauk **34** (1979), no. 3(207), 203–204. MR **80k:**10046

716. M. B. Levin and M. Smorodinsky, *A $\mathbb{Z}^d$ generalization of the Davenport-Erdős construction of normal numbers*, Colloq. Math. **84/85** (2000), no. part 2, 431–441, Dedicated to the memory of Anzelm Iwanik. MR **2002a:**11087

717. D. J. Lewis and J. Turk, *Repetitiveness in binary recurrences*, J. Reine Angew. Math. **356** (1985), 19–48. MR **86e:**11015

718. S. Li, *On the number of elements with maximal order in the multiplicative group modulo n*, Acta Arith. **86** (1998), no. 2, 113–132. MR **99k:**11144

719. ———, *On extending Artin's conjecture to composite moduli*, Mathematika **46** (1999), no. 2, 373–390. MR **2002d:**11118

720. ———, *Artin's conjecture on average for composite moduli*, J. Number Theory **84** (2000), no. 1, 93–118. MR **2001h:**11127

721. S. Li and C. Pomerance, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math. **556** (2003), 205–224.

722. W.-C. W. Li, M. Näslund, and I. E. Shparlinski, *Hidden number problem with the trace and bit security of XTR and LUC*, Advances in cryptology—CRYPT0 '02 (Santa Barbara, 2002) (Berlin), Springer, 2002.

723. A. I. Lichtman, *The soluble subgroups and the Tits alternative in linear groups over rings of fractions of polycylic group rings. I*, J. Pure Appl. Algebra **86** (1993), no. 3, 231–287. MR **94d:**20056

724. ———, *The soluble subgroups and the Tits alternative in linear groups over rings of fractions of polycyclic group rings. II*, J. Group Theory **2** (1999), no. 2, 173–189. MR **2000c:**20077

725. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley Publishing Company Advanced Book Program, Reading, MA, 1983. MR **86c:**11106

726. D. Lieman and I. E. Shparlinski, *On a new exponential sum*, Canad. Math. Bull. **44** (2001), no. 1, 87–92. MR **2001m:**11138

727. D. Lind, *Ergodic automorphisms of the infinite torus are Bernoulli*, Israel J. Math. **17** (1974), 162–168. MR 49 #10856

728. ———, *Dynamical properties of quasihyperbolic toral automorphisms*, Ergodic Theory Dynamical Systems **2** (1982), no. 1, 49–68. MR **84g:**28017

729. ———, *Applications of ergodic theory and sofic systems to cellular automata*, Phys. D **10** (1984), no. 1-2, 36–44. MR **86g:**68128

730. D. Lind and B. Marcus, *An introduction to symbolic dynamics and coding*, Cambridge University Press, Cambridge, 1995. MR **97a:**58050

731. D. Lind, K. Schmidt, and T. Ward, *Mahler measure and entropy for commuting automorphisms of compact groups*, Invent. Math. **101** (1990), no. 3, 593–629. MR **92j:**22013

732. D. Lind and T. Ward, *Automorphisms of solenoids and p-adic entropy*, Ergodic Theory Dynam. Systems **8** (1988), no. 3, 411–419. MR **90a:**28031

733. U. V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem*, Rec. Math. [Mat. Sbornik] N.S. **15(57)** (1944), 139–178. MR 6,260b

734. L. Lipshitz, *The diagonal of a D-finite power series is D-finite*, J. Algebra **113** (1988), no. 2, 373–378. MR **89c:**13027

735. ———, *D-finite power series*, J. Algebra **122** (1989), no. 2, 353–373. MR **90g:**13032

736. L. Lipshitz and A. J. van der Poorten, *Rational functions, diagonals, automata and arithmetic*, Number theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, pp. 339–358. MR **93b:**11095

737. L. Lipshitz and L. A. Rubel, *A gap theorem for power series solutions of algebraic differential equations*, Amer. J. Math. **108** (1986), no. 5, 1193–1213. MR **87m:**12008

738. B. Litow and Ph. Dumas, *Additive cellular automata and algebraic series*, Theoret. Comput. Sci. **119** (1993), no. 2, 345–354. MR **94f:**68141

739. F. Lorenz, *Normal bases of units*, Number theory, Vol. II (Budapest, 1987), North-Holland, Amsterdam, 1990, pp. 851–869. MR **91h:**11119

740. J. H. Loxton, *Automata and transcendence*, New advances in transcendence theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, pp. 215–228. MR **90b:**11068

741. J. H. Loxton and A. J. van der Poorten, *Arithmetic properties of certain functions in several variables. III*, Bull. Austral. Math. Soc. **16** (1977), no. 1, 15–47. MR **81g:**10046

742. ______, *On the growth of recurrence sequences*, Math. Proc. Cambridge Philos. Soc. **81** (1977), no. 3, 369–376. MR 56 #8480

743. ______, *Arithmetic properties of the solutions of a class of functional equations*, J. Reine Angew. Math. **330** (1982), 159–172. MR **83i:**10046

744. ______, *Multiplicative dependence in number fields*, Acta Arith. **42** (1983), no. 3, 291–302. MR **86b:**11052

745. ______, *Arithmetic properties of automata: regular sequences*, J. Reine Angew. Math. **392** (1988), 57–69. MR **90a:**11082

746. A. Lubotzky, *Subgroup growth and congruence subgroups*, Invent. Math. **119** (1995), no. 2, 267–295. MR **95m:**20054

747. A. de Luca and S. Varricchio, *Some combinatorial properties of the Thue-Morse sequence and a problem in semigroups*, Theoret. Comput. Sci. **63** (1989), no. 3, 333–348. MR **90k:**68090

748. F. Luca, *Products of factorials in binary recurrence sequences*, Rocky Mountain J. Math. **29** (1999), no. 4, 1387–1411. MR **2000k:**11086

749. ______, *Distinct digits in base b expansions of linear recurrence sequences*, Quaest. Math. **23** (2000), no. 4, 389–404. MR **2001i:**11014

750. ______, *Divisibility properties of binary recurrent sequences*, Indag. Math. (N.S.) **12** (2001), no. 3, 353–367. MR **2003e:**11011

751. ______, *Multiply perfect numbers in Lucas sequences with odd parameters*, Publ. Math. Debrecen **58** (2001), no. 1-2, 121–155. MR **2002a:**11005

752. ______, *On the greatest common divisor of two Cullen numbers*, Preprint, 2002.

753. ______, *Arithmetic properties of members of a binary recurrence sequence*, Acta Arith. **109** (2003), 81–107.

754. ______, *Palindromes in Lucas sequences*, Monatsh. Math. **138** (2003), 209–223.

755. F. Luca and I. E. Shparlinski, *Arithmetical functions with linear recurrence sequences*, Preprint, 2002.

756. ______, *Average multiplicative orders of elements modulo n*, Acta Arith. (to appear).

757. F. Luca and P. G. Walsh, *Squares in Lehmer sequences and some Diophantine applications*, Acta Arith. **100** (2001), no. 1, 47–62. MR **2002h:**11024

758. ______, *The product of like-indexed terms in binary recurrences*, J. Number Theory **96** (2002), 152–173.

759. L. G. Lucht, *Arithmetical aspects of certain functional equations*, Acta Arith. **82** (1997), no. 3, 257–277. MR **98m:**11005

760. ______, *Arithmetical sequences and systems of functional equations*, Aequationes Math. **53** (1997), no. 1-2, 73–90. MR **98h:**11007

761. ______, *Recurrent and almost-periodic sequences*, Arch. Math. (Basel) **68** (1997), no. 1, 22–26. MR **97k:**11116

762. L. G. Lucht and C. Methfessel, *Recurrent sequences and endomorphisms of Euclidean spaces*, Arch. Math. (Basel) **63** (1994), no. 1, 92–96. MR **95i:**11010

763. ______, *Recurrent sequences and affine functional equations*, J. Number Theory **57** (1996), no. 1, 105–113. MR **96k:**11014

764. L. G. Lucht and M. Peter, *On the characterization of exponential polynomials*, Arch. Math. (Basel) **71** (1998), no. 3, 201–210. MR **99e:**11019

765. W. F. Lunnon, P. A. B. Pleasants, and N. M. Stephens, *Arithmetic properties of Bell numbers to a composite modulus. I*, Acta Arith. **35** (1979), no. 1, 1–16. MR **80k:**05006

766. R. C. Lyness, *Notes 1581, 1847 and 2952*, Math. Gaz. **26, 29, 45** (1942, 1945, 1961), 62, 231, 201.

767. F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I*, North-Holland Publishing Co., Amsterdam, 1977. MR 57 #5408a

768. ______, *The theory of error-correcting codes. II*, North-Holland Publishing Co., Amsterdam, 1977. MR 57 #5408b

769. K. Mahler, *Eine arithmetische Eigenschaft der rekurrierenden Reihen*, Mathematika **3** (1934), 1–4.

770. ______, *Eine arithmetische Eigenschaft der Taylor Koeffizienten rationaler Funktionen*, Proc. Akad. Wet. Amsterdam **38** (1935), 51–60.

771. ———, *On the Taylor coefficients of rational functions*, Proc. Cambridge Philos. Soc. **52** (1956), 39–48, Addendum: **53** (1957), 544. MR 17,597c

772. ———, *A remark on recursive sequences*, J. Math. Sci. **1** (1966), 12–17. MR 35 #2853

773. ———, *An unsolved problem on the powers of* 3/2, J. Austral. Math. Soc. **8** (1968), 313–321. MR 37 #2694

774. ———, *Arithmetical properties of the digits of the multiples of an irrational number*, Bull. Austral. Math. Soc. **8** (1973), 191–203. MR 47 #8448

775. J. L. Malouf, *An integer sequence from a rational recursion*, Discrete Math. **110** (1992), no. 1-3, 257–261. MR **93m:**11011

776. A. Manning, *Axiom A diffeomorphisms have rational zeta functions*, Bull. London Math. Soc. **3** (1971), 215–220. MR 44 #5982

777. M. Margenstern and Y. V. Matiyasevich, *A binomial representation of the* $3x + 1$ *problem*, Acta Arith. **91** (1999), no. 4, 367–378. MR **2001g:**11015

778. G. Marsaglia, *The mathematics of random number generators*, The unreasonable effectiveness of number theory (Orono, ME, 1991), Amer. Math. Soc., Providence, RI, 1992, pp. 73–90. MR **94a:**11119

779. G. Martin, *The least prime primitive root and the shifted sieve*, Acta Arith. **80** (1997), no. 3, 277–288. MR **98c:**11101

780. O. Martin, A. M. Odlyzko, and S. Wolfram, *Algebraic properties of cellular automata*, Comm. Math. Phys. **93** (1984), no. 2, 219–258. MR **86a:**68073

781. R. C. Mason, *The study of Diophantine equations over function fields*, New advances in transcendence theory (Durham, 1986), Cambridge Univ. Press, Cambridge, 1988, pp. 229–247. MR **90e:**11047

782. D. W. Masser, *Counting points of small height on elliptic curves*, Bull. Soc. Math. France **117** (1989), no. 2, 247–265. MR **90k:**11068

783. ———, *Mixing and equations over groups in positive characteristic*, Preprint, 2002.

784. J. L. Massey and S. Serconek, *Linear complexity of periodic sequences: a general theory*, Advances in cryptology—CRYPTO '96 (Santa Barbara, CA), Springer, Berlin, 1996, pp. 358–371. MR **98i:**94015

785. T. Matala-aho and M. Prévost, *Irrationality measures for the series of reciprocals from recurrence sequences*, J. Number Theory **96** (2002), 275–292.

786. Y. V. Matiyasevich, *Hilbert's tenth problem*, MIT Press, Cambridge, MA, 1993. MR **94m:**03002b

787. K. Matsumoto, *C^*-algebras associated with cellular automata*, Math. Scand. **75** (1994), no. 2, 195–216. MR **96a:**46120

788. H. Matsumura, *Commutative ring theory*, second ed., Cambridge University Press, Cambridge, 1989. MR **90i:**13001

789. K. R. Matthews, *Some Borel measures associated with the generalized Collatz mapping*, Colloq. Math. **63** (1992), no. 2, 191–202. MR **93i:**11090

790. ———, *The generalized* $3x + 1$ *problem*, Preprint, 1995.

791. R. Matthews, *Strong pseudoprimes and generalized Carmichael numbers*, Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), Amer. Math. Soc., Providence, RI, 1994, pp. 227–233. MR **95g:**11125

792. C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences. II. The Champernowne, Rudin-Shapiro, and Thue-Morse sequences, a further construction*, J. Number Theory **73** (1998), no. 2, 256–276. MR **99m:**11084

793. J. E. Maxfield, *Normal k-tuples*, Pacific J. Math. **3** (1953), 189–196. MR 14,851b

794. G. L. Mayhew and S. W. Golomb, *Linear spans of modified deBruijn sequences*, IEEE Trans. Inform. Theory **36** (1990), 1166–1167.

795. J. Mazoyer and I. Rapaport, *Additive cellular automata over* $\mathbb{Z}_p$ *and the bottom of* $(\mathrm{CA}, \leq)$, Mathematical foundations of computer science, 1998 (Brno), Springer, Berlin, 1998, pp. 834–843. MR **2000b:**68163

796. K. S. McCurley, *Odds and ends from cryptology and computational number theory*, Cryptology and computational number theory (Boulder, CO, 1989), Amer. Math. Soc., Providence, RI, 1990, pp. 145–166. MR **92j:**11149

797. W. L. McDaniel and P. Ribenboim, *Square-classes in Lucas sequences having odd parameters*, J. Number Theory **73** (1998), no. 1, 14–27. MR **99j:**11017

798. I. McFarlane and S. G. Hoggar, *Combinatorics for faster fractal pictures*, Number-theoretic and algebraic methods in computer science (Moscow, 1993), World Sci. Publishing, River Edge, NJ, 1995, pp. 95–124. MR **97f:**68191

799. M. D. McIlroy, *Number theory in computer graphics*, The unreasonable effectiveness of number theory (Orono, ME, 1991), Amer. Math. Soc., Providence, RI, 1992, pp. 105–121. MR **94a:**11199

800. J. F. McKee, *Families of Pisot numbers with negative trace*, Acta Arith. **93** (2000), no. 4, 373–385. MR **2001b:**11096

801. J. F. McKee, P. Rowlinson, and C. J. Smyth, *Salem numbers and Pisot numbers from stars*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 309–319. MR **2000d:**11127

802. W. Meidl and H. Niederreiter, *Counting functions and expected values for the k-error linear complexity*, Finite Fields Appl. **8** (2002), 142–154.

803. ______, *Linear complexity, k-error linear complexity and the discrete Fourier transform*, J. Complexity **18** (2002), 87–103.

804. W. Meidl and A. Winterhof, *Lower bounds on the linear complexity of the discrete logarithm in finite fields*, IEEE Trans. Inform. Theory **47** (2001), no. 7, 2807–2811. MR **2003b:**94079

805. ______, *On the linear complexity profile of explicit nonlinear pseudorandom numbers*, Inform. Process. Lett. **85** (2003), no. 1, 13–18. MR 1 950 157

806. W. Meier and O. Staffelbach, *The self-shrinking generator*, Advances in cryptology—EUROCRYPT '94 (Perugia), Springer, Berlin, 1995, pp. 205–214.

807. D. Meiri, *Entropy and uniform distribution of orbits in $\mathbb{T}^d$*, Israel J. Math. **105** (1998), 155–183. MR **99f:**58129

808. M. Mendès France, *The depth of a rational number*, Topics in number theory (Proc. Colloq., Debrecen, 1974), North-Holland, Amsterdam, 1976, pp. 183–194. Colloq. Math. Soc. János Bolyai, Vol. 13. MR 55 #12625

809. ______, *The Rudin-Shapiro sequence, Ising chain, and paperfolding*, Analytic number theory (Allerton Park, IL, 1989), Birkhäuser Boston, Boston, MA, 1990, pp. 367–382. MR **92e:**11154

810. ______, *Remarks and problems on finite and periodic continued fractions*, Enseign. Math. (2) **39** (1993), no. 3-4, 249–257. MR **94i:**11045

811. M. Mendès France and A. J. van der Poorten, *Arithmetic and analytic properties of paper folding sequences*, Bull. Austral. Math. Soc. **24** (1981), no. 1, 123–131. MR **83b:**10040

812. ______, *Automata and the arithmetic of formal power series*, Acta Arith. **46** (1986), no. 3, 211–214. MR **88a:**11064

813. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC Press Series on Discrete Mathematics and its Applications, CRC Press, Boca Raton, FL, 1997, With a foreword by Ronald L. Rivest. MR **99g:**94015

814. L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449. MR **96i:**11057

815. C. Methfessel, *Multiplicative and additive recurrent sequences*, Arch. Math. (Basel) **63** (1994), no. 4, 321–328. MR **95e:**11018

816. ______, *Rekurrente Folgen mit lokal gleichmäßig beschränkter Primteileranzahl*, Acta Arith. **70** (1995), no. 1, 1–7. MR **95k:**11012

817. F. Mignosi, *On a generalization of the $3x+1$ problem*, J. Number Theory **55** (1995), no. 1, 28–45. MR **96m:**11016

818. M. Mignotte, *A note on linear recursive sequences*, J. Austral. Math. Soc. **20** (1975), no. 2, 242–244. MR 52 #5581

819. ______, *Une extension du théorème de Skolem-Mahler*, C. R. Acad. Sci. Paris Sér. A-B **288** (1979), no. 4, A233–A235. MR **80b:**10013

820. ______, *Une extension de théorème de Skolem-Mahler*, Noncommutative structures in algebra and geometric combinatorics (Naples, 1978), CNR, Rome, 1981, pp. 97–100. MR **83k:**10020

821. ______, *Determination des répetitions d'une certaine suite recurrente linéaire*, Publ. Math. Debrecen **33** (1986), no. 3-4, 297–306. MR **88h:**11012

822. ______, *Propriétés arithmétiques des suites récurrentes linéaires*, Théorie des nombres, Année 1988/89, Fasc. 1, Univ. Franche-Comté, Besançon, 1989, p. 30. MR **91g:**11012

823. M. Mignotte, T. N. Shorey, and R. Tijdeman, *The distance between terms of an algebraic recurrence sequence*, J. Reine Angew. Math. **349** (1984), 63–76. MR **85f:**11007

824. M. Mignotte and N. Tzanakis, *Arithmetical study of recurrence sequences*, Acta Arith. **57** (1991), no. 4, 357–364. MR **92c:**11013

825. M. Mihaljević, Y. Zheng, and H. Imai, *A fast cryptographic hash function based on linear cellular automata*, Proc. IFIP 14th Intern. Inform. Security Conf., Vienna, 1998, Chapman and Hall, to appear.

826. P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture. draft*, Preprint, 2002.

827. A. V. Mikhalev and A. A. Nechaev, *Linear recurring sequences over modules*, Acta Appl. Math. **42** (1996), no. 2, 161–202. MR **97j:**16031

828. G. L. Miller, *Riemann's hypothesis and tests for primality*, Seventh Annual ACM Symposium on Theory of Computing (Albuquerque, N.M., 1975), Assoc. Comput. Mach., New York, 1975, pp. 234–239. MR 58 #470b

829. D. A. Mit′kin, *Estimates and asymptotic formulas for rational trigonometric sums that are nearly complete*, Mat. Sb. (N.S.) **122(164)** (1983), no. 4, 527–545. MR **85c:**11074

830. I. Miyamoto and M. Ram Murty, *Elliptic pseudoprimes*, Math. Comp. **53** (1989), no. 187, 415–430. MR **89j:**11055

831. H. L. Montgomery, *Distribution of small powers of a primitive root*, Advances in number theory (Kingston, ON, 1991), Oxford Univ. Press, New York, 1993, pp. 137–149. MR **96j:**11112

832. F. Montoya Vitini, J. Muñoz Masqué, and A. Peinado Domínguez, *Maximum cycles of quadratic functions in* GF(2^n), XXX National Congress of the Mexican Mathematical Society (Spanish) (Aguascalientes, 1997), Soc. Mat. Mexicana, México, 1998, pp. 125–130.

833. ______, *Linear complexity of the* x^2 mod p *orbits*, Inform. Process. Lett. **72** (1999), no. 1-2, 3–7.

834. F. Morain, *Pseudoprimes: a survey of recent results*, Eurocode '92 (Udine, 1992), Springer, Vienna, 1993, pp. 207–215. MR **95d:**11172

835. W. Moran and A. D. Pollington, *Metrical results on normality to distinct bases*, J. Number Theory **54** (1995), no. 2, 180–189. MR **96i:**11084

836. ______, *The discrimination theorem for normality to non-integer bases*, Israel J. Math. **100** (1997), 339–347. MR **98h:**11097

837. W. More, *The LD probable prime test*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), Amer. Math. Soc., Providence, RI, 1999, pp. 185–191. MR **99h:**11145

838. P. Moree, *On the prime density of Lucas sequences*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 449–459. MR **98f:**11127

839. ______, *On a conjecture of Rodier on primitive roots*, Abh. Math. Sem. Univ. Hamburg **67** (1997), 165–171. MR **98i:**11081

840. ______, *On the divisors of* $a^k + b^k$, Acta Arith. **80** (1997), no. 3, 197–212. MR **98e:**11105

841. ______, *Counting divisors of Lucas numbers*, Pacific J. Math. **186** (1998), no. 2, 267–284. MR **99m:**11013

842. ______, *Improvement of an estimate of H. Müller involving the order of* 2 (mod u), Arch. Math. (Basel) **71** (1998), no. 3, 197–200. MR **99m:**11111

843. ______, *On some sums connected with primitive roots*, `www.mpim-bonn.mpg.de/html/preprints/preprints.html`, 1998.

844. ______, *On some sums involving primitive roots, 2*, `www.mpim-bonn.mpg.de/html/preprints/preprints.html`, 1998.

845. ______, *On primes in arithmetic progression having a prescribed primitive root*, J. Number Theory **78** (1999), no. 1, 85–98. MR **2001i:**11118

846. ______, *Uniform distribution of primes having a prescribed primitive root*, Acta Arith. **89** (1999), no. 1, 9–21. MR **2000d:**11121

847. ______, *Approximation of singular series and automata*, Manuscripta Math. **101** (2000), no. 3, 385–399, With an appendix by Gerhard Niklasch. MR **2001f:**11204

848. ______, *Asymptotically exact heuristics for (near) primitive roots*, J. Number Theory **83** (2000), no. 1, 155–181. MR **2001m:**11161

849. P. Moree and P. Stevenhagen, *Prime divisors of Lucas sequences*, Acta Arith. **82** (1997), no. 4, 403–410. MR **98i:**11098

850. ______, *A two-variable Artin conjecture*, J. Number Theory **85** (2000), no. 2, 291–304. MR **2001k:**11188

851. ______, *Prime divisors of the Lagarias sequence*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 241–251, 21st Journées Arithmétiques (Rome, 2001). MR **2002c:**11016

852. M. D. Morgan, *The distribution of second order linear recurrence sequences mod* 2^m, Acta Arith. **83** (1998), no. 2, 181–195. MR **99e:**11021

853. M. Morii and M. Kasahara, *Perfect staircase profile of linear complexity for finite sequences*, Inform. Process. Lett. **44** (1992), no. 2, 85–89. MR **93j:**68081

854. K. Morita, *Reversible simulation of one-dimensional irreversible cellular automata*, Theoret. Comput. Sci. **148** (1995), no. 1, 157–163. MR **96h:**68139

855. G. Morris and T. Ward, *Entropy bounds for endomorphisms commuting with K actions*, Israel J. Math. **106** (1998), 1–11. MR **99m:**28042

856. P. Morton, *Connections between binary patterns and paperfolding*, Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 1, 1–12. MR **91i:**11010

857. ______, *Arithmetic properties of periodic points of quadratic maps*, Acta Arith. **62** (1992), no. 4, 343–372. MR **93k:**12004

858. ______, *Characterizing cyclic cubic extensions by automorphism polynomials*, J. Number Theory **49** (1994), no. 2, 183–208. MR **95j:**12006

859. ______, *On certain algebraic curves related to polynomial maps*, Compositio Math. **103** (1996), no. 3, 319–350. MR **97m:**14030

860. ______, *Periods of maps on irreducible polynomials over finite fields*, Finite Fields Appl. **3** (1997), no. 1, 11–24. MR **98d:**11075

861. ______, *Arithmetic properties of periodic points of quadratic maps. II*, Acta Arith. **87** (1998), no. 2, 89–102. MR **2000c:**11103

862. P. Morton and W. J. Mourant, *Paper folding, digit patterns and groups of arithmetic fractals*, Proc. London Math. Soc. (3) **59** (1989), no. 2, 253–293. MR **91c:**11007

863. P. Morton and P. Patel, *The Galois theory of periodic points of polynomial maps*, Proc. London Math. Soc. (3) **68** (1994), no. 2, 225–263. MR **94i:**11090

864. P. Morton and J. H. Silverman, *Rational periodic points of rational functions*, Internat. Math. Res. Notices **2** (1994), 97–110. MR **95b:**11066

865. ______, *Periodic points, multiplicities, and dynamical units*, J. Reine Angew. Math. **461** (1995), 81–122. MR **96b:**11090

866. P. Morton and F. Vivaldi, *Bifurcations and discriminants for polynomial maps*, Nonlinearity **8** (1995), no. 4, 571–584. MR **96k:**11028

867. P. Moss, *Algebraic realizability problems*, Ph.D. thesis, The University of East Anglia, 2004.

868. M. J. Mossinghoff, *Polynomials with small Mahler measure*, Math. Comp. **67** (1998), no. 224, 1697–1705, S11–S14. MR **99a:**11119

869. M. J. Mossinghoff, C. G. Pinner, and J. D. Vaaler, *Perturbing polynomials with all their roots on the unit circle*, Math. Comp. **67** (1998), no. 224, 1707–1726. MR **99b:**26024

870. J. Muñoz Masqué, F. Montoya Vitini, and A. Peinado Domínguez, *Iterated quadratic functions in* $\mathbb{F}_{2^n}$, Int. J. Appl. Math. **5** (2001), no. 1, 65–83. MR **2002i:**94045

871. J. Mueller, *S-unit equations in function fields via the abc-theorem*, Bull. London Math. Soc. **32** (2000), no. 2, 163–170. MR **2001a:**11053

872. G. L. Mullen and I. E. Shparlinski, *Values of linear recurring sequences of vectors over finite fields*, Acta Arith. **65** (1993), no. 3, 221–226. MR **94m:**11144

873. G. L. Mullen and T. P. Vaughan, *Cycles of linear permutations over a finite field*, Linear Algebra Appl. **108** (1988), 63–82. MR **89m:**11118

874. H. Müller, *Über eine Klasse 2-adischer Funktionen im Zusammenhang mit dem "$3x+1$"-Problem*, Abh. Math. Sem. Univ. Hamburg **64** (1994), 293–302. MR **95e:**11032

875. ______, *Eine Bemerkung über die Ordnungen von* $2 \pmod{u}$ *bei ungeradem* u, Arch. Math. (Basel) **69** (1997), no. 3, 217–220. MR **98i:**11072

876. S. Müller, *A note on strong Dickson pseudoprimes*, Appl. Algebra Engrg. Comm. Comput. **9** (1998), no. 3, 247–264. MR **99j:**11008

877. ______, *Carmichael numbers and Lucas tests*, Finite fields: theory, applications, and algorithms (Waterloo, ON, 1997), Amer. Math. Soc., Providence, RI, 1999, pp. 193–202. MR **99m:**11008

878. ______, *On the combined Fermat/Lucas probable prime test*, Cryptography and coding (Cirencester, 1999), Springer, Berlin, 1999, pp. 222–235. MR **2002h:**11141

879. ______, *On the rank of appearance of Lucas sequences*, Applications of Fibonacci numbers, Vol. 8 (Rochester, NY, 1998), Kluwer Acad. Publ., Dordrecht, 1999, pp. 259–275. MR **2000j:**11018

880. ______, *On probable prime testing and the computation of square roots mod n*, Algorithmic number theory (Leiden, 2000), Springer, Berlin, 2000, pp. 423–437. MR **2002h:**11140

881. ______, *On QF-pseudoprimes and second-order recurrence sequences*, Contributions to general algebra, 12 (Vienna, 1999), Heyn, Klagenfurt, 2000, pp. 299–310. MR **2001e:**11016

882. ______, *On the rank of appearance and the number of zeros of the Lucas sequences over* $\mathbb{F}_q$, Finite fields and applications (Augsburg, 1999), Springer, Berlin, 2001, pp. 390–408. MR **2002e:**11177

883. ______, *A probable prime test with very high confidence for $n \equiv 1 \mod 4$*, Lect. Notes in Comp. Sci. **2248** (2001), 87–106.

884. ______, *Some remarks on primality testing based on Lucas functions*, Number Theory for the Millennium, Vol.III, A. K. Peters, Natick, MA, 2002, pp. 1–22.

885. W. B. Müller and A. Oswald, *Generalized Fibonacci pseudoprimes and probable primes*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 459–464. MR **95f:**11105

886. L. Murata, *On the magnitude of the least primitive root*, Astérisque **198-200** (1991), 253–257 (1992). MR **93b:**11127

887. ______, *A problem analogous to Artin's conjecture for primitive roots and its applications*, Arch. Math. (Basel) **57** (1991), no. 6, 555–565. MR **93c:**11071

888. M. Ram Murty, *On Artin's conjecture*, J. Number Theory **16** (1983), no. 2, 147–168. MR **86f:**11087

889. ______, *An analogue of Artin's conjecture for abelian extensions*, J. Number Theory **18** (1984), no. 3, 241–248. MR **85j:**11161

890. ______, *Finitely generated groups (mod p)*, Proc. Amer. Math. Soc. **122** (1994), no. 1, 37–45. MR **94k:**11113

891. ______, *Artin's conjecture and elliptic analogues*, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), Cambridge Univ. Press, Cambridge, 1997, pp. 325–344. MR **2000a:**11098

892. M. Ram Murty, V. Kumar Murty, and T. N. Shorey, *Odd values of the Ramanujan τ-function*, Bull. Soc. Math. France **115** (1987), no. 3, 391–395. MR **89c:**11071

893. M. Ram Murty, M. Rosen, and J. H. Silverman, *Variations on a theme of Romanoff*, Internat. J. Math. **7** (1996), no. 3, 373–391. MR **97d:**11093

894. M. Ram Murty and Wong S., *The abc conjecture and prime divisors of the Lucas and Lehmer sequences*, Number Theory for the Millennium, Vol.III, A. K. Peters, Natick, MA, 2002, pp. 43–54.

895. M. Ram Murty and S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull. **30** (1987), no. 1, 80–85. MR **88e:**11094

896. G. Myerson, *A combinatorial problem in finite fields. I*, Pacific J. Math. **82** (1979), no. 1, 179–187. MR **80i:**05010

897. ______, *A combinatorial problem in finite fields. II*, Quart. J. Math. Oxford Ser. (2) **31** (1980), no. 122, 219–231. MR **81i:**05014

898. ______, *An arithmetic property of certain rational powers*, Preprint, 1997.

899. G. Myerson and A. J. van der Poorten, *Some problems concerning recurrence sequences*, Amer. Math. Monthly **102** (1995), no. 8, 698–705. MR **97a:**11029

900. I. T. Nabney, *Growth functions for groups and recurrence sequences*, Proc. London Math. Soc. (3) **63** (1991), no. 2, 315–343. MR **92f:**20030

901. H. Nakada, *Metrical theory for a class of continued fraction transformations and their natural extensions*, Tokyo J. Math. **4** (1981), no. 2, 399–426. MR **83k:**10095

902. T. Nakahara, *On a periodic solution of some congruences*, Rep. Fac. Sci. Engrg. Saga Univ. Math. **14** (1986), 1–5. MR **87e:**11004

903. K. Nakamula and A. Pethő, *Squares in binary recurrence sequences*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 409–421. MR **99g:**11020

904. S. Nandi, B. K. Kar, and P. Pal Chaudhuri, *Theory and applications of cellular automata in cryptography*, IEEE Trans. Comput. **43** (1994), no. 12, 1346–1357. MR **95k:**94023

905. M. Naor and O. Reingold, *Number-theoretic constructions of efficient pseudo-random functions*, Proc. 38th IEEE Symp. on Foundations of Comp. Sci., IEEE, 1997, pp. 458–467.

906. W. Narkiewicz, *Classical problems in number theory*, Państwowe Wydawnictwo Naukowe (PWN), Warsaw, 1986. MR **90e**:11002

907. ———, *A note on Artin's conjecture in algebraic number fields*, J. Reine Angew. Math. **381** (1987), 110–115. MR **89a**:11007

908. ———, *Units in residue classes*, Arch. Math. (Basel) **51** (1988), no. 3, 238–241. MR **89k**:11097

909. ———, *Elementary and analytic theory of algebraic numbers*, second ed., Springer-Verlag, Berlin, 1990. MR **91h**:11107

910. ———, *Polynomial mappings*, Springer-Verlag, Berlin, 1995. MR **97e**:11037

911. W. Narkiewicz and T. Pezda, *Finite polynomial orbits in finitely generated domains*, Monatsh. Math. **124** (1997), no. 4, 309–316. MR **99b**:11117

912. V. I. Nečaev, *The group of non-singular matrices over a finite field, and recurrent sequences*, Dokl. Akad. Nauk SSSR **152** (1963), 275–277. MR 27 #5748

913. ———, *Linear recurrent congruences with periodic coefficients*, Mat. Zametki **3** (1968), 625–632. MR 38 #3241

914. ———, *Recurrent sequences*, Algebra and number theory, Moskov. Gos. Ped. Inst. Učen. Zap. **375** (1971), 103–123. MR 48 #5983

915. ———, *Trigonometric sums for recurrent sequences of elements of a finite field*, Mat. Zametki **11** (1972), 597–607. MR 48 #3893

916. V. I. Nečaev and L. L. Stepanova, *The distirbution of nonresidues and primitive roots in recurrence sequences over a field of algebraic numbers*, Uspehi Mat. Nauk **20** (1965), no. 3 (123), 197–203. MR 33 #115

917. A. A. Nechaev, *Linear recurrent sequences over commutative rings*, Diskret. Mat. **3** (1991), no. 4, 105–127. MR **93b**:13028

918. ———, *Cycle types of linear maps over finite commutative rings*, Mat. Sb. **184** (1993), no. 3, 21–56. MR **94e**:15028

919. ———, *Linear codes and polylinear recurrences over finite rings and quasi-Frobenius modules*, Dokl. Akad. Nauk **345** (1995), no. 4, 451–454.

920. Yu. V. Nesterenko, *Estimates for the number of zeros of functions of certain classes*, Acta Arith. **53** (1989), no. 1, 29–46. MR **91d**:11078

921. Yu. V. Nesterenko and T. N. Shorey, *On an equation of Goormaghtigh*, Acta Arith. **83** (1998), no. 4, 381–389. MR **98m**:11022

922. S.-H. Ng and E. J. Taft, *Quantum convolution of linearly recursive sequences*, J. Algebra **198** (1997), no. 1, 101–119. MR **98k**:16055

923. P. Q. Nguyen and I. E. Shparlinski, *The insecurity of the digital signature algorithm with partially known nonces*, J. Cryptology **15** (2002), no. 3, 151–176. MR 1 927 452

924. ———, *The insecurity of the elliptic curve Digital Signature Algorithm with partially known nonces*, Design, Codes and Cryptography (to appear).

925. H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), no. 6, 957–1041. MR **80d**:65016

926. ———, *Distribution properties of feedback shift register sequences*, Problems Control Inform. Theory/Problemy Upravlen. Teor. Inform. **15** (1986), no. 1, 19–34. MR **87m**:94029

927. ———, *On a problem of Kodama concerning the Hasse-Witt matrix and the distribution of residues*, Proc. Japan Acad. Ser. A Math. Sci. **63** (1987), no. 9, 367–369. MR **90a**:11007

928. ———, *Rational functions with partial quotients of small degree in their continued fraction expansion*, Monatsh. Math. **103** (1987), no. 4, 269–288. MR **88h**:12002

929. ———, *Sequences with almost perfect linear complexity profile*, Lect. Notes in Comp. Sci. **304** (1988), 37–51.

930. ———, *The serial test for digital k-step pseudorandom numbers*, Math. J. Okayama Univ. **30** (1988), 93–119. MR **90g**:65011

931. ———, *Some new cryptosystems based on feedback shift register sequences*, Math. J. Okayama Univ. **30** (1988), 121–149. MR **90a**:94039

932. ———, *A combinatorial approach to probabilistic results on the linear-complexity profile of random sequences*, J. Cryptology **2** (1990), no. 2, 105–112. MR **91g**:94018

933. ———, *Keystream sequences with a good linear complexity profile for every starting point*, Advances in cryptology—EUROCRYPT '89 (Houthalen, 1989), Springer, Berlin, 1990, pp. 523–532.

934. ______, *The linear complexity profile and the jump complexity of keystream sequences*, Advances in cryptology—EUROCRYPT '90 (Aarhus, 1990), Springer, Berlin, 1991, pp. 174–188.

935. ______, *Recent trends in random number and random vector generation*, Ann. Oper. Res. **31** (1991), no. 1-4, 323–345. MR **92h:**65010

936. ______, *Random number generation and quasi-Monte Carlo methods*, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 1992. MR **93h:**65008

937. ______, *Finite fields and cryptology*, Finite fields, coding theory, and advances in communications and computing (Las Vegas, NV, 1991), Dekker, New York, 1993, pp. 359–373. MR **93m:**11133

938. ______, *New developments in uniform pseudorandom number and vector generation*, Monte Carlo and quasi-Monte Carlo methods in scientific computing (Las Vegas, NV, 1994), Springer, New York, 1995, pp. 87–120. MR **97k:**65019

939. ______, *Pseudorandom vector generation by the multiple-recursive matrix method*, Math. Comp. **64** (1995), no. 209, 279–294. MR **95j:**65006

940. ______, *Some computable complexity measures for binary sequences*, Sequences and their applications (Singapore, 1998), Springer, London, 1999, pp. 67–78. MR **2002j:**94045

941. H. Niederreiter and H. Paschinger, *Counting functions and expected values in the stability theory of stream ciphers*, Sequences and their applications (Singapore, 1998), Springer, London, 1999, pp. 318–329. MR **2002f:**94041

942. H. Niederreiter and I. E. Shparlinski, *On the distribution and lattice structure of nonlinear congruential pseudorandom numbers*, Finite Fields Appl. **5** (1999), no. 3, 246–253. MR **2000i:**11126

943. ______, *Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus*, Acta Arith. **92** (2000), no. 1, 89–98. MR **2001g:**11127

944. ______, *On the distribution of pseudorandom numbers and vectors generated by inversive methods*, Appl. Algebra Engrg. Comm. Comput. **10** (2000), no. 3, 189–202. MR **2001f:**11130

945. ______, *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, Math. Comp. **70** (2001), no. 236, 1569–1574. MR **2002e:**11104

946. ______, *On the average distribution of inversive pseudorandom numbers*, Finite Fields and Their Appl. **8** (2002), 491–503.

947. ______, *Recent advances in the theory of nonlinear pseudorandom number generators*, Proc. Conf. on Monte Carlo and Quasi-Monte Carlo Methods, 2000, Springer, Berlin, 2002, pp. 86–102.

948. ______, *Dynamical systems generated by rational functions*, Lect. Notes in Comp. Sci. **2643** (2003).

949. ______, *On the distribution of power residues and primitive elements in some nonlinear recurring sequences*, Bull. London Math. Soc. (to appear).

950. H. Niederreiter and M. Vielhaber, *Tree complexity and a doubly exponential gap between structured and random sequences*, J. Complexity **12** (1996), no. 3, 187–198. MR **97g:**94025

951. ______, *Linear complexity profiles: Hausdorff dimensions for almost perfect profiles and measures for general profiles*, J. Complexity **13** (1997), no. 3, 353–383. MR **99f:**94012

952. ______, *Simultaneous shifted continued fraction expansions in quadratic time*, Appl. Algebra Engrg. Comm. Comput. **9** (1998), no. 2, 125–138. MR **99k:**11195

953. ______, *An algorithm for shifted continued fraction expansions in parallel linear time*, Theoret. Comput. Sci. **226** (1999), no. 1-2, 93–104. MR **2001m:**94048

954. H. Niederreiter and A. Winterhof, *Incomplete exponential sums over finite fields and their applications to new inversive pseudorandom number generators*, Acta Arith. **93** (2000), no. 4, 387–399. MR **2001d:**11120

955. ______, *On a new class of inversive pseudorandom numbers for parallelized simulation methods*, Period. Math. Hungar. **42** (2001), no. 1-2, 77–87. MR **2002b:**65011

956. ______, *On the distribution of compound inversive congruential pseudorandom numbers*, Monatsh. Math. **132** (2001), no. 1, 35–48. MR **2002g:**11113

957. ______, *On the lattice structure of pseudorandom numbers generated over arbitrary finite fields*, Appl. Algebra Engrg. Comm. Comput. **12** (2001), no. 3, 265–272. MR **2002f:**11102

958. G. Niklasch, *Counting exceptional units*, Collect. Math. **48** (1997), no. 1-2, 195–207. MR **98g:**11124

959. G. Niklasch and R. Quême, *An improvement of Lenstra's criterion for Euclidean number fields: the totally real case*, Acta Arith. **58** (1991), no. 2, 157–168. MR **92f:**11149

960. K. Nishioka, *Mahler functions and transcendence*, Springer-Verlag, Berlin, 1996. MR **98d:**11084

961. ______, *Algebraic independence of reciprocal sums of binary recurrences*, Monatsh. Math. **123** (1997), no. 2, 135–148. MR **98a:**11095

962. ______, *Algebraic independence of reciprocal sums of binary recurrences, II*, Monatsh. Math. **136** (2002), 123–141. MR **2003c:**11083

963. J.-S. No, H. Chung, H.-Y. Song, K. Yang, J.-D. Lee, and T. Helleseth, *New construction for binary sequences of period* $p^m - 1$ *with optimal autocorrelation using* $(z+1)^d + az^d + b$, IEEE Trans. Inform. Theory **47** (2001), no. 4, 1638–1644. MR **2002f:**94078

964. J.-S. No, H. Chung, and M.-S. Yun, *Binary pseudorandom sequences of period* $2^m - 1$ *with ideal autocorrelation generated by the polynomial* $z^d + (z+1)^d$, IEEE Trans. Inform. Theory **44** (1998), no. 3, 1278–1282. MR **99c:**94021

965. J.-S. No, S. W. Golomb, G. Gong, H.-K. Lee, and P. Gaal, *Binary pseudorandom sequences of period* $2^n - 1$ *with ideal autocorrelation*, IEEE Trans. Inform. Theory **44** (1998), no. 2, 814–817.

966. J.-S. No, K. Yang, H. Chung, and H.-Y. Song, *New construction for families of binary sequences with optimal correlation properties*, IEEE Trans. Inform. Theory **43** (1997), no. 5, 1596–1602. MR **98f:**11134

967. D. G. Northcott, *Periodic points on an algebraic variety*, Ann. of Math. (2) **51** (1950), 167–177. MR 11,615c

968. G. H. Norton, *On the minimal realizations of a finite sequence*, J. Symbolic Comput. **20** (1995), no. 1, 93–115. MR **97h:**13027

969. ______, *On minimal realization over a finite chain ring*, Des. Codes Cryptogr. **16** (1999), no. 2, 161–178. MR **2000f:**13048

970. ______, *On shortest linear recurrences*, J. Symbolic Comput. **27** (1999), no. 3, 325–349. MR **2000i:**13033

971. W.-G. Nowak and R. F. Tichy, *An improved estimate on the distribution mod* 1 *of powers of real matrices*, Compositio Math. **49** (1983), no. 2, 283–289. MR **84m:**10044

972. R. W. K. Odoni, *A conjecture of Krishnamurthy on decimal periods and some allied problems*, J. Number Theory **13** (1981), no. 3, 303–319. MR **83a:**10098

973. ______, *The Galois theory of iterates and composites of polynomials*, Proc. London Math. Soc. (3) **51** (1985), no. 3, 385–414. MR **87c:**12005

974. ______, *On the prime divisors of the sequence* $w_{n+1} = 1 + w_1 \cdots w_n$, J. London Math. Soc. (2) **32** (1985), no. 1, 1–11. MR **87b:**11094

975. ______, *On the Galois groups of iterated generic additive polynomials*, Math. Proc. Cambridge Philos. Soc. **121** (1997), no. 1, 1–6. MR **98g:**12004

976. T. Oliveira e Silva, *Maximum excursion and stopping time record-holders for the* $3x+1$ *problem: computational results*, Math. Comp. **68** (1999), no. 225, 371–384. MR **2000g:**11015

977. F. Pappalardi, *On Hooley's theorem with weights*, Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), no. 4, 375–388. MR **98c:**11102

978. ______, *On minimal sets of generators for primitive roots*, Canad. Math. Bull. **38** (1995), no. 4, 465–468. MR **96k:**11120

979. ______, *On the order of finitely generated subgroups of* $\mathbb{Q}^*$ (mod p) *and divisors of* $p-1$, J. Number Theory **57** (1996), no. 2, 207–222. MR **97d:**11141

980. F. Pappalardi and I. E. Shparlinski, *On Artin's conjecture over function fields*, Finite Fields Appl. **1** (1995), no. 4, 399–404. MR **97g:**11132

981. W. Parry, *An analogue of the prime number theorem for closed orbits of shifts of finite type and their suspensions*, Israel J. Math. **45** (1983), no. 1, 41–52. MR **85c:**58089

982. W. Parry and M. Pollicott, *An analogue of the prime number theorem for closed orbits of Axiom A flows*, Ann. of Math. (2) **118** (1983), no. 3, 573–591. MR **85i:**58105

983. ______, *Zeta functions and the periodic orbit structure of hyperbolic dynamics*, Astérisque **187-188** (1990), 268. MR **92f:**58141

984. K. G. Paterson, *Root counting, the DFT and the linear complexity of nonlinear filtering*, Des. Codes Cryptogr. **14** (1998), no. 3, 247–259. MR **2000j:**94008

985. K. G. Paterson and P. J. G. Lothian, *Bounds on partial correlations of sequences*, IEEE Trans. Inform. Theory **44** (1998), no. 3, 1164–1175. MR **99c:**94022

986. A. Peinado Domínguez, F. Montoya Vitini, J. Muñoz Masqué, and A. J. Yuste, *Maximal periods of $x^2 + c$ in $\mathbb{F}_q$*, Lect. Notes in Comp. Sci. **2227** (2001), 219–228.

987. A. Perelli and U. Zannier, *Arithmetic properties of certain recurrence sequences*, J. Austral. Math. Soc. Ser. A **37** (1984), no. 1, 4–16. MR **85i:**11016

988. A. Pethő, *Perfect powers in second order linear recurrences*, J. Number Theory **15** (1982), no. 1, 5–13. MR **84f:**10024

989. ———, *Divisibility properties of linear recursive sequences*, Number theory, Vol. II (Budapest, 1987), North-Holland, Amsterdam, 1990, pp. 899–916. MR **91i:**11019

990. ———, *Diophantine properties of linear recursive sequences. I*, Applications of Fibonacci numbers, Vol. 7 (Graz, 1996), Kluwer Acad. Publ., Dordrecht, 1998, pp. 295–309.

991. A. Pethő and R. F. Tichy, *S-unit equations, linear recurrences and digit expansions*, Publ. Math. Debrecen **42** (1993), no. 1-2, 145–154. MR **94a:**11013

992. A. Pethő and H. G. Zimmer, *Lineare rekurrente Folgen auf elliptischen Kurven*, Sém. Théor. Nombres Bordeaux (2) **2** (1990), no. 1, 217–227. MR **91k:**11044

993. T. Pezda, *Cycles of polynomial mappings in several variables*, Manuscripta Math. **83** (1994), no. 3-4, 279–289. MR **95f:**11094

994. ———, *Polynomial cycles in certain local domains*, Acta Arith. **66** (1994), no. 1, 11–22. MR **95a:**11102

995. ———, *Cycles of polynomials in algebraically closed fields of positive chracteristic. II*, Colloq. Math. **71** (1996), no. 1, 23–30. MR **97g:**11026

996. ———, *Cycles of rational mappings in algebraically closed fields of positive characteristics*, Ann. Math. Sil. **12** (1998), 15–21, Number theory (Cieszyn, 1998). MR **99m:**11024

997. ———, *Cycles of polynomial mappings in several variables over rings of integers in finite extensions of the rationals*, Acta Arith. **108** (2003), no. 1, 127–146.

998. T. Pheidas, *An effort to prove that the existential theory of $\mathbb{Q}$ is undecidable*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 237–252. MR **2001m:**03085

999. B. M. Phong, *On generalized Lehmer sequences*, Acta Math. Hungar. **57** (1991), no. 3-4, 201–211. MR **92m:**11021

1000. T. A. Pierce, *Numerical factors of the arithmetic forms $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$*, Ann. of Math. **18** (1917), 53–64.

1001. R. G. E. Pinch, *Recurrent sequences modulo prime powers*, Cryptography and coding, III (Cirencester, 1991), Oxford Univ. Press, New York, 1993, pp. 297–310. MR **95b:**11019

1002. Á. Pintér, *Exponential Diophantine equations over function fields*, Publ. Math. Debrecen **41** (1992), no. 1-2, 89–98. MR **93i:**11039

1003. P. Piret, *An upper bound on the weight distribution of some systematic codes*, IEEE Trans. Inform. Theory **31** (1985), no. 4, 520–521. MR **86i:**94054

1004. I. M. Pjatetski-Shapiro, *On the distribution of franction parts of exponential functions*, Proc. Moscow State Pedagogical Inst. **108** (1957), 317–322.

1005. V. Pless, P. Solé, and Z. Qian, *Cyclic self-dual $\mathbb{Z}_4$-codes*, Finite Fields Appl. **3** (1997), no. 1, 48–69, With an appendix by P. Moree. MR **97m:**94036

1006. M. Poe, *On distribution of solutions of S-unit equations*, J. Number Theory **62** (1997), no. 2, 221–241. MR **97k:**11043

1007. A. M. Polosuev, *The structure of the solutions of linear recurrent congruences with coefficients that are periodic modulo a prime*, Vestnik Moskov. Univ. Ser. I Mat. Meh. **27** (1972), no. 1, 57–61. MR 46 #7145

1008. G. Pólya, *Arithmetische eigenschaften der Reihenentwicklungen rationaler Funktionen*, J. Reine Angew. Math. **151** (1920), 1–31.

1009. G. Pólya and G. Szegő, *Problems and theorems in analysis. I*, German ed., Springer-Verlag, Berlin, 1978. MR **81e:**00002

1010. C. Pomerance, J. M. Robson, and J. Shallit, *Automaticity. II. Descriptional complexity in the unary case*, Theoret. Comput. Sci. **180** (1997), no. 1-2, 181–201. MR **99a:**11026

1011. A. J. van der Poorten, *Generalizing Turán's main theorems on lower bounds for sums of powers*, Acta Math. Acad. Sci. Hungar. **24** (1973), 93–96. MR 47 #2038

1012. ———, *A note on recurrence sequences*, J. Proc. Roy. Soc. New South Wales **106** (1973), no. 3-4, 115–117 (1974). MR 52 #14740

1013. ———, *Hermite interpolation and p-adic exponential polynomials*, J. Austral. Math. Soc. Ser. A **22** (1976), no. 1, 12–26. MR 56 #5453

1014. ______, *On the distribution of zeros of exponential polynomials*, Math. Slovaca **26** (1976), no. 4, 299–307. MR 55 #3226

1015. ______, *Zeros of p-adic exponential polynomials*, Nederl. Akad. Wetensch. Proc. Ser. A **79** = Indag. Math. **38** (1976), no. 1, 46–49. MR 53 #5543

1016. ______, *Effectively computable bounds for the solutions of certain Diophantine equations*, Acta Arith. **33** (1977), no. 3, 195–207. MR 56 #8491

1017. ______, *Linear forms in logarithms in the p-adic case*, Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), Academic Press, London, 1977, pp. 29–57. MR 58 #16544

1018. ______, *On the number of zeros of functions*, Enseignement Math. (2) **23** (1977), no. 1-2, 19–38. MR 57 #16221

1019. ______, *The growth conditions for recurrence sequences*, Macquarie University Mathematical Reports **41** (1982), 27pp.

1020. ______, *Identification of rational functions: lost and regained*, C. R. Math. Rep. Acad. Sci. Canada **4** (1982), no. 5, 309–314. MR **84c:**10009

1021. ______, *Hadamard operations on rational functions*, Study group on ultrametric analysis, 10th year: 1982/83, No. 1, Inst. Henri Poincaré, Paris, 1984, pp. Exp. No. 4, 11. MR **85k:**11050

1022. ______, *p-adic methods in the study of Taylor coefficients of rational functions*, Bull. Austral. Math. Soc. **29** (1984), no. 1, 109–117. MR **86g:**11073

1023. ______, *Some problems of recurrent interest*, Topics in classical number theory, Vol. I, II (Budapest, 1981), North-Holland, Amsterdam, 1984, pp. 1265–1294. MR **86h:**11015

1024. ______, *Remarks on automata, functional equations and transcendence*, Semin. de Theorie des Nombres de Bordeaux **27** (1988), 1–11.

1025. ______, *Solution de la conjecture de Pisot sur le quotient de Hadamard de deux fractions rationnelles*, C. R. Acad. Sci. Paris Sér. I Math. **306** (1988), no. 3, 97–102. MR **89c:**11153

1026. ______, *Some facts that should be better known, especially about rational functions*, Number theory and applications (Banff, AB, 1988), Kluwer Acad. Publ., Dordrecht, 1989, pp. 497–528. MR **92k:**11011

1027. ______, *Notes on continued fractions and recurrence sequences*, Number theory and cryptography (Sydney, 1989), Cambridge Univ. Press, Cambridge, 1990, pp. 86–97. MR **91e:**11079

1028. ______, *Recurrence sequences, continued fractions, and the Hadamard Quotient Theorem*, Macquarie Math. Report 92–109, Macquarie Univ., 1992.

1029. ______, *Continued fractions of formal power series*, Advances in number theory (Kingston, ON, 1991), Oxford Univ. Press, New York, 1993, pp. 453–466. MR **97a:**11017

1030. ______, *Power series representing algebraic functions*, Séminaire de Théorie des Nombres, Paris, 1990–91, Birkhäuser Boston, Boston, MA, 1993, pp. 241–262. MR **95d:**13030

1031. ______, *Explicit formulas for units in certain quadratic number fields*, Algorithmic number theory (Ithaca, NY, 1994), Springer, Berlin, 1994, pp. 194–208. MR **96b:**11146

1032. ______, *Factorisation in fractional powers*, Acta Arith. **70** (1995), no. 3, 287–293. MR **96c:**12001

1033. ______, *A note on Hadamard roots of rational functions*, Rocky Mountain J. Math. **26** (1996), no. 3, 1183–1197. MR **98b:**11009

1034. ______, *Notes on Fermat's last theorem*, John Wiley & Sons Inc., New York, 1996. MR **98c:**11026

1035. A. J. van der Poorten and R. S. Rumely, *Zeros of p-adic exponential polynomials. II*, J. London Math. Soc. (2) **36** (1987), no. 1, 1–15. MR **88m:**11103

1036. A. J. van der Poorten and H. P. Schlickewei, *A Diophantine problem in harmonic analysis*, Math. Proc. Cambridge Philos. Soc. **108** (1990), no. 3, 417–420. MR **91j:**11052

1037. ______, *Additive relations in fields*, J. Austral. Math. Soc. Ser. A **51** (1991), no. 1, 154–170. MR **93d:**11036

1038. ______, *Zeros of recurrence sequences*, Bull. Austral. Math. Soc. **44** (1991), no. 2, 215–223. MR **93d:**11017

1039. A. J. van der Poorten and J. Shallit, *Folded continued fractions*, J. Number Theory **40** (1992), no. 2, 237–250. MR **93a:**11008

1040. A. J. van der Poorten and I. E. Shparlinski, *On the number of zeros of exponential polynomials and related questions*, Bull. Austral. Math. Soc. **46** (1992), no. 3, 401–412. MR **93i:**11041

1041. ———, *On sequences of polynomials defined by certain recurrence relations*, Acta Sci. Math. (Szeged) **61** (1995), no. 1-4, 77–103. MR **97j:**11007

1042. ———, *On linear recurrence sequences with polynomial coefficients*, Glasgow Math. J. **38** (1996), no. 2, 147–155. MR **97b:**11013

1043. A. J. van der Poorten and R. Tijdeman, *On common zeros of exponential polynomials*, Enseignement Math. (2) **21** (1975), no. 1, 57–67. MR 52 #292

1044. A. G. Postnikov, *A solution of a set of simultaneous difference equations corresponding to the Dirichlet problem by means of a normal sequence of digits*, Dokl. Akad. Nauk SSSR **123** (1958), 407–409. MR 21 #3043

1045. ———, *Arithmetic modeling of random processes*, Trudy Mat. Inst. Steklov. **57** (1960), 84. MR 26 #6146

1046. ———, *Ergodic problems in the theory of congruences and of Diophantine approximations*, American Mathematical Society, Providence, R.I., 1967. MR 35 #5409

1047. L. P. Postnikova and A. Šincel′, *Primitive divisors of the expression $a^n - b^n$ in algebraic number fields*, Mat. Sb. (N.S.) **75 (117)** (1968), 171–177. MR 36 #6378

1048. C. Powell, *Bounds for multiplicative cosets over fields of prime order*, Math. Comp. **66** (1997), no. 218, 807–822. MR **97f:**11005

1049. K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin, 1978. MR **81k:**10060

1050. C. E. Praeger, *Primitive prime divisor elements in finite classical groups*, Groups St. Andrews 1997 in Bath, II, Cambridge Univ. Press, Cambridge, 1999, pp. 605–623. MR **2000h:**20090

1051. V. R. Pratt, *Every prime has a succinct certificate*, SIAM J. Comput. **4** (1975), no. 3, 214–220. MR 52 #12395

1052. J. Propp, *The Somos Sequence Site*, `www.math.wisc.edu/~propp/somos.html`.

1053. Y. Puri, *Arithmetic Properties of Periodic Orbits*, Ph.D. thesis, The University of East Anglia, 2000.

1054. Y. Puri and T. Ward, *Arithmetic and growth of periodic orbits*, J. Integer Seq. **4** (2001), no. 2, Article 01.2.1, 18 pp. MR **2002i:**11026

1055. ———, *A dynamical property unique to the Lucas sequence*, Fibonacci Quart. **39** (2001), no. 5, 398–402. MR **2002j:**37020

1056. L. N. Pushkin, *A metric variant of the Cassels-Schmidt theorem*, Mat. Zametki **46** (1989), no. 1, 60–66, 124. MR **90h:**11067

1057. ———, *Vectors that are Borel normal on a manifold in $\mathbb{R}^n$*, Teor. Veroyatnost. i Primenen. **36** (1991), no. 2, 372–376. MR **92g:**11078

1058. M. van der Put, *Reduction modulo p of differential equations*, Indag. Math. (N.S.) **7** (1996), no. 3, 367–387. MR **99e:**12009

1059. M. O. Rabin, *Computationally hard algebraic problems (extended abstract)*, 37th Annual Symposium on Foundations of Computer Science (Burlington, VT, 1996), IEEE Comput. Soc. Press, Los Alamitos, CA, 1996, pp. 284–289.

1060. C. Radoux, *Nombres de Bell, modulo p premier, et extensions de degré p de $\mathbb{F}_p$*, C. R. Acad. Sci. Paris Sér. A-B **281** (1975), no. 21, Ai, A879–A882. MR 53 #13105

1061. U. Rausch, *Geometrische Reihen in algebraischen Zahlkörpern*, Acta Arith. **47** (1986), no. 4, 313–345. MR **89b:**11074

1062. ———, *A summation formula in algebraic number fields and applications. I*, J. Number Theory **36** (1990), no. 1, 46–79. MR **92b:**11082

1063. L. Rédei, *Lacunary polynomials over finite fields*, North-Holland Publishing Co., Amsterdam, 1973. MR 50 #4548

1064. B. Reznick, *Some binary partition functions*, Analytic number theory (Allerton Park, IL, 1989), Birkhäuser Boston, Boston, MA, 1990, pp. 451–477. MR **91k:**11092

1065. P. Ribenboim, *On the factorization of $X^n - BX - A$*, Enseign. Math. (2) **37** (1991), no. 3-4, 191–200. MR **93d:**11030

1066. ———, *Catalan's conjecture*, Academic Press Inc., Boston, MA, 1994. MR **95a:**11029

1067. ———, *The Fibonacci numbers and the Arctic Ocean*, Proceedings of the 2nd Gauss Symposium. Conference A: Mathematics and Theoretical Physics (Munich, 1993) (Berlin), de Gruyter, 1995, pp. 41–83. MR **96g:**11015

1068. ______, *An algorithm to determine the points with integral coordinates in certain elliptic curves*, J. Number Theory **74** (1999), no. 1, 19–38. MR **99j:**11028

1069. ______, *Binary recurring sequences and powers. I*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 419–430. MR **2000k:**11035

1070. ______, *Binary recurring sequences and powers. II*, Publ. Math. Debrecen **54** (1999), no. 3-4, 349–375. MR **2000k:**11036

1071. ______, *On square factors of terms of binary recurring sequences and the ABC conjecture*, Publ. Math. Debrecen **59** (2001), no. 3-4, 459–469. MR **2002i:**11033

1072. ______, *The terms Cx^h ($h \geq 3$) in Lucas sequences: An algorithm and applications to Diophantine equations*, Acta Arith. **106** (2002), 105–114.

1073. P. Ribenboim and W. L. McDaniel, *The square terms in Lucas sequences*, J. Number Theory **58** (1996), no. 1, 104–123. MR **97c:**11021

1074. ______, *On Lucas sequence terms of the form kx^2*, Number theory (Turku, 1999), de Gruyter, Berlin, 2001, pp. 293–303. MR **2002b:**11028

1075. P. Ribenboim and P. G. Walsh, *The ABC conjecture and the powerful part of terms in binary recurring sequences*, J. Number Theory **74** (1999), no. 1, 134–147. MR **99k:**11047

1076. K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476. MR **91g:**11066

1077. G. J. Rieger, *Mischung und Ergodizität bei Kettenbrüchen nach nächsten Ganzen*, J. Reine Angew. Math. **310** (1979), 171–181. MR **81c:**10066

1078. H. J. J. te Riele, *Iteration of number-theoretic functions*, Nieuw Arch. Wisk. (4) **1** (1983), no. 3, 345–360. MR **85e:**11003

1079. H. Riesel, *Prime numbers and computer methods for factorization*, second ed., Birkhäuser Boston Inc., Boston, MA, 1994. MR **95h:**11142

1080. J. F. Ritt, *A factorisation theory for functions $\sum_{i=1}^{n} a_i e^{\alpha_i z}$*, Trans. Amer. Math. Soc. **29** (1927), 584–596.

1081. ______, *Algebraic combinations of exponentials*, Trans. Amer. Math. Soc. **31** (1929), 654–679.

1082. ______, *On the zeros of exponential polynomials*, Trans. Amer. Math. Soc. **31** (1929), 680–686.

1083. P. Robba, *Zéros de suites récurrentes linéaires*, Groupe d'Etude d'Analyse Ultramétrique, 5e année (1977/78), Secrétariat Math., Paris, 1978, pp. Exp. No. 13, 5. MR **80b:**10015

1084. R. M. Robinson, *Periodicity of Somos sequences*, Proc. Amer. Math. Soc. **116** (1992), no. 3, 613–619. MR **93a:**11012

1085. ______, *Numbers having m small mth roots mod p*, Math. Comp. **61** (1993), no. 203, 393–413. MR **93k:**11002

1086. A. M. Rockett, *The metrical theory of continued fractions to the nearer integer*, Acta Arith. **38** (1980/81), no. 2, 97–103. MR **82d:**10074

1087. P. Rogers, *Topics in elliptic divisibility sequences*, M.Phil. thesis, The University of East Anglia, 2002.

1088. M. Roitman, *On Zsigmondy primes*, Proc. Amer. Math. Soc. **125** (1997), no. 7, 1913–1919. MR **97i:**11005

1089. M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR **2003d:**11171

1090. H. Roskam, *A quadratic analogue of Artin's conjecture on primitive roots*, J. Number Theory **81** (2000), no. 1, 93–109. MR **2000k:**11128

1091. ______, *Prime divisors of linear recurrences and Artin's primitive root conjecture for number fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 1, 303–314, 21st Journées Arithmétiques (Rome, 2001). MR **2002c:**11013

1092. A. Rotkiewicz, *On strong Lehmer pseudoprimes in the case of negative discriminant in arithmetic progressions*, Acta Arith. **68** (1994), no. 2, 145–151. MR **96h:**11008

1093. Z. Rudnick, P. Sarnak, and A. Zaharescu, *The distribution of spacings between the fractional parts of $n^2\alpha$*, Invent. Math. **145** (2001), no. 1, 37–57. MR **2002e:**11093

1094. Z. Rudnick and A. Zaharescu, *The distribution of spacings between small powers of a primitive root*, Israel J. Math. **120** (2000), no. part A, 271–287. MR **2003e:**11099

1095. R. A. Rueppel, *Analysis and design of stream ciphers*, Springer-Verlag, Berlin, 1986. MR **88h:**94002

1096. ______, *Stream ciphers*, Contemporary cryptology, IEEE, New York, 1992, pp. 65–134.

1097. R. A. Rueppel and J. L. Massey, *Knapsack as a nonlinear function*, IEEE Intern. Symp. of Inform. Theory, IEEE, 1985, p. 46.

1098. R. A. Rueppel and O. J. Staffelbach, *Products of linear recurring sequences with maximum complexity*, IEEE Trans. Inform. Theory **33** (1987), 124–131.

1099. R. S. Rumely, *Notes on van der Poorten's proof of the Hadamard quotient theorem. I, II*, Séminaire de Théorie des Nombres, Paris 1986–87, Birkhäuser Boston, Boston, MA, 1988, pp. 349–382, 383–409. MR **90d:**11090

1100. R. S. Rumely and A. J. van der Poorten, *A note on the Hadamard kth root of a rational function*, J. Austral. Math. Soc. Ser. A **43** (1987), no. 3, 314–327. MR **88j:**11009

1101. ______, *Remarks on generalised power sums*, Bull. Austral. Math. Soc. **36** (1987), no. 2, 311–329. MR **88j:**11008

1102. I. Z. Ruzsa, *Erdős and the integers*, J. Number Theory **79** (1999), no. 1, 115–163. MR **2002e:**11002

1103. N. Saradha and T. N. Shorey, *The equation $(x^n - 1)/(x - 1) = y^q$ with x square*, Math. Proc. Cambridge Philos. Soc. **125** (1999), no. 1, 1–19. MR **99h:**11037

1104. D. Sarwate and M. Pursley, *Crosscorrelation properties of pseudorandom and related sequences*, Proc. IEEE **68** (1980), 593–619.

1105. T. Sato, *Decidability for some problems of linear cellular automata over finite commutative rings*, Inform. Process. Lett. **46** (1993), no. 3, 151–155. MR **94h:**68165

1106. ______, *Group structured linear cellular automata over $\mathbb{Z}_m$*, J. Comput. System Sci. **49** (1994), no. 1, 18–23. MR **96b:**68132

1107. ______, *Ergodicity of linear cellular automata over $\mathbb{Z}_m$*, Inform. Process. Lett. **61** (1997), no. 3, 169–172. MR **97m:**68148

1108. ______, *Ergodic characterization of linear cellular automata over $\mathbb{Z}_m$*, Theoret. Comput. Sci. **205** (1998), no. 1-2, 135–144. MR **2000e:**68116

1109. ______, *Surjective linear cellular automata over $\mathbb{Z}_m$*, Inform. Process. Lett. **66** (1998), no. 2, 101–104. MR **99c:**68183

1110. N. P. F. du Sautoy, *Finitely generated groups, p-adic analytic groups and Poincaré series*, Ann. of Math. (2) **137** (1993), no. 3, 639–670. MR **94j:**20029

1111. ______, *Counting congruence subgroups in arithmetic subgroups*, Bull. London Math. Soc. **26** (1994), no. 3, 255–262. MR **95k:**11111

1112. ______, *Mersenne primes, irrationality and counting subgroups*, Bull. London Math. Soc. **29** (1997), no. 3, 285–294. MR **98c:**11091

1113. J. Schiffer, *Discrepancy of normal numbers*, Acta Arith. **47** (1986), no. 2, 175–186. MR **88d:**11072

1114. A. Schinzel, *On two theorems of Gelfond and some of their applications*, Acta Arith **13** (1967/1968), 177–236. MR 36 #5086

1115. ______, *Primitive divisors of the expression $A^n - B^n$ in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33. MR 49 #8961

1116. ______, *Selected topics on polynomials*, University of Michigan Press, Ann Arbor, Mich., 1982. MR **84k:**12010

1117. ______, *Systems of exponential congruences*, Demonstratio Math. **18** (1985), no. 1, 377–394. MR **87c:**11036

1118. ______, *An extension of the theorem on primitive divisors in algebraic number fields*, Math. Comp. **61** (1993), no. 203, 441–444. MR **93k:**11107

1119. ______, *Exponential congruences*, Number theory and its applications (Kyoto, 1997), Kluwer Acad. Publ., Dordrecht, 1999, pp. 303–308. MR **2001e:**11031

1120. ______, *Polynomials with special regard to reducibility*, Cambridge University Press, Cambridge, 2000, With an appendix by Umberto Zannier. MR **2001h:**11135

1121. H. P. Schlickewei, *The number of subspaces occurring in the p-adic subspace theorem in Diophantine approximation*, J. Reine Angew. Math. **406** (1990), 44–108. MR **91e:**11076

1122. ______, *The quantitative subspace theorem for number fields*, Compositio Math. **82** (1992), no. 3, 245–273. MR **93f:**11050

1123. ______, *Multiplicities of algebraic linear recurrences*, Acta Math. **170** (1993), no. 2, 151–180. MR **94i:**11015

1124. ______, *Equations in roots of unity*, Acta Arith. **76** (1996), no. 2, 99–108. MR **97g:**11037

1125. ______, *Multiplicities of recurrence sequences*, Acta Math. **176** (1996), no. 2, 171–243. MR **97g:**11031

1126. ———, *Lower bounds for heights on finitely generated groups*, Monatsh. Math. **123** (1997), no. 2, 171–178. MR **98d:**11077

1127. ———, *The multiplicity of binary recurrences*, Invent. Math. **129** (1997), no. 1, 11–36. MR **98k:**11100

1128. ———, *The subspace theorem and applications*, Proceedings of the International Congress of Mathematicians, Vol. II (Berlin, 1998), vol. Extra Vol. II, 1998, pp. 197–205. MR **99h:**11075

1129. H. P. Schlickewei and W. M. Schmidt, *Equations $au_n^l = bu_m^k$ satisfied by members of recurrence sequences*, Proc. Amer. Math. Soc. **118** (1993), no. 4, 1043–1051. MR **93j:**11010

1130. ———, *Linear equations in members of recurrence sequences*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **20** (1993), no. 2, 219–246. MR **94h:**11004

1131. ———, *On polynomial-exponential equations*, Math. Ann. **296** (1993), no. 2, 339–361. MR **94e:**11032

1132. ———, *The intersection of recurrence sequences*, Acta Arith. **72** (1995), no. 1, 1–44. MR **96g:**11011

1133. ———, *The number of solutions of polynomial-exponential equations*, Compositio Math. **120** (2000), no. 2, 193–225. MR **2001b:**11022

1134. H. P. Schlickewei, W. M. Schmidt, and M. Waldschmidt, *Zeros of linear recurrence sequences*, Manuscripta Math. **98** (1999), no. 2, 225–241. MR **99m:**11034

1135. H. P. Schlickewei, I. E. Shparlinski, and S. A. Stepanov, *On the distribution of normal bases of number fields*, Preprint, 1994.

1136. H. P. Schlickewei and S. A. Stepanov, *Algorithms to construct normal bases of cyclic number fields*, J. Number Theory **44** (1993), no. 1, 30–40. MR **94d:**11081

1137. J. Schmeling, *Symbolic dynamics for β-shifts and self-normal numbers*, Ergodic Theory Dynam. Systems **17** (1997), no. 3, 675–694. MR **98c:**11080

1138. K. Schmidt, *On periodic expansions of Pisot numbers and Salem numbers*, Bull. London Math. Soc. **12** (1980), no. 4, 269–278. MR **82c:**12003

1139. ———, *Mixing automorphisms of compact groups and a theorem by Kurt Mahler*, Pacific J. Math. **137** (1989), no. 2, 371–385. MR **90c:**28031

1140. ———, *Dynamical systems of algebraic origin*, Birkhäuser Verlag, Basel, 1995. MR **97c:**28041

1141. K. Schmidt and T. Ward, *Mixing automorphisms of compact groups and a theorem of Schlickewei*, Invent. Math. **111** (1993), no. 1, 69–76. MR **95c:**22011

1142. W. M. Schmidt, *On normal numbers*, Pacific J. Math. **10** (1960), 661–672. MR 22 #7994

1143. ———, *Simultaneous approximation to algebraic numbers by rationals*, Acta Math. **125** (1970), 189–201. MR 42 #3028

1144. ———, *Linear forms with algebraic coefficients. I*, J. Number Theory **3** (1971), 253–277. MR 46 #7176

1145. ———, *Linearformen mit algebraischen Koeffizienten. II*, Math. Ann. **191** (1971), 1–20. MR 46 #7177

1146. ———, *Diophantine approximation*, Lecture Notes in Mathematics, vol. 785, Springer, Berlin, 1980. MR **81j:**10038

1147. ———, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith. **56** (1990), no. 2, 161–179. MR **91m:**11021

1148. ———, *The zero multiplicity of linear recurrence sequences*, Acta Math. **182** (1999), no. 2, 243–282. MR **2000j:**11043

1149. ———, *Zeros of linear recurrence sequences*, Publ. Math. Debrecen **56** (2000), no. 3-4, 609–630, Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday. MR **2001f:**11051

1150. E. Schmutz, *The order of a typical matrix with entries in a finite field*, Israel J. Math. **91** (1995), no. 1-3, 349–371. MR **97e:**15011

1151. F. Schweiger, *Normalität bezüglich zahlentheoretischer Transformationen*, J. Number Theory **1** (1969), 390–397. MR 40 #2616

1152. ———, *Ergodic theory of fibred systems and metric number theory*, The Clarendon Press Oxford University Press, New York, 1995. MR **97h:**11083

1153. C. Seo, S. Lee, Y. Sung, K. Han, and S. Kim, *A lower bound on the linear span of an FCSR*, IEEE Trans. Inform. Theory **46** (2000), no. 2, 691–693. MR **2000m:**94017

1154. G. Seroussi and N. H. Bshouty, *Vector sets for exhaustive testing of logic circuits*, IEEE Trans. Inform. Theory **34** (1988), no. 3, 513–522. MR **89j:**94049

1155. J. Shallit, *Real numbers with bounded partial quotients: a survey*, Enseign. Math. (2) **38** (1992), no. 1-2, 151–187. MR **93g:**11011

1156. ———, *Numeration systems, linear recurrences, and regular sets*, Inform. and Comput. **113** (1994), no. 2, 331–347. MR **95g:**11007

1157. ———, *Automaticity. IV. Sequences, sets, and diversity*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 347–367, Erratum: **9** (1997), 247. MR **99a:**11027a

1158. ———, *Number theory and formal languages*, Emerging applications of number theory (Minneapolis, MN, 1996), Springer, New York, 1999, pp. 547–570. MR **2000d:**68123

1159. ———, *Automaticity and rationality*, J. Autom. Lang. Comb. **5** (2000), no. 3, 255–268, Descriptional complexity of automata, grammars and related structures (Magdeburg, 1999). MR **2001h:**68083

1160. J. Shallit and Y. Breitbart, *Automaticity. I. Properties of a measure of descriptional complexity*, J. Comput. System Sci. **53** (1996), no. 1, 10–25. MR **97m:**68074

1161. H. N. Shapiro and G. H. Sparer, *Composite values of exponential and related sequences*, Comm. Pure Appl. Math. **25** (1972), 569–615. MR 46 #8958

1162. ———, *Extension of a theorem of Mason*, Comm. Pure Appl. Math. **47** (1994), no. 5, 711–718. MR **95c:**11036

1163. H. S. Shapiro, *The expansion of mean-periodic functions in series of exponentials.*, Comm. Pure Appl. Math. **11** (1958), 1–21. MR 21 #2157

1164. A. Shields, *On quotients of exponential polynomials*, Comm. Pure Appl. Math. **16** (1963), 27–31. MR 26 #6411

1165. I. Shiokawa, *Asymptotic distributions of digits in integers*, Number theory, Vol. I (Budapest, 1987), North-Holland, Amsterdam, 1990, pp. 505–525. MR **91g:**11082

1166. R. Shipsey, *Elliptic divisibility sequences*, Ph.D. thesis, Goldsmith's College (University of London), 2000.

1167. ———, *Elliptic divisibility sequences and elliptic curves*, Preprint, 2001.

1168. T. N. Shorey, *Applications of linear forms in logarithms to binary recursive sequences*, Seminar on number theory, Paris 1981–82 (Paris, 1981/1982), Birkhäuser Boston, Boston, MA, 1983, pp. 287–301. MR **85f:**11009

1169. ———, *Divisors of convergents of a continued fraction*, J. Number Theory **17** (1983), no. 1, 127–133. MR **85d:**11068

1170. ———, *The greatest square free factor of a binary recursive sequence*, Hardy-Ramanujan J. **6** (1983), 23–36. MR **85i:**11019

1171. ———, *Linear forms in members of a binary recursive sequence*, Acta Arith. **43** (1984), no. 4, 317–331. MR **85m:**11038

1172. ———, *Ramanujan and binary recursive sequences*, J. Indian Math. Soc. (N.S.) **52** (1987), 147–157 (1988). MR **90e:**11033

1173. ———, *Some exponential Diophantine equations. II*, Number theory and related topics (Bombay, 1988), Tata Inst. Fund. Res., Bombay, 1989, pp. 217–229. MR **98d:**11038

1174. ———, *The equation $a(x^n-1)/(x-1) = by^q$ with $ab > 1$*, Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, pp. 473–485. MR **2000d:**11045

1175. ———, *Exponential Diophantine equations involving products of consecutive integers and related equations*, Number theory, Birkhäuser, Basel, 2000, pp. 463–495. MR **2001g:**11045

1176. ———, *Some conjectures in the theory of exponential Diophantine equations*, Publ. Math. Debrecen **56** (2000), no. 3-4, 631–641, Dedicated to Professor Kálmán Győry on the occasion of his 60th birthday. MR **2001i:**11038

1177. T. N. Shorey and S. Srinivasan, *Metrical results on square free divisors of convergents of continued fractions*, Bull. London Math. Soc. **19** (1987), no. 2, 135–138. MR **88e:**11069

1178. T. N. Shorey and C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. II*, J. London Math. Soc. (2) **23** (1981), no. 1, 17–23. MR **82m:**10025

1179. ———, *On the Diophantine equation $ax^{2t} + bx^ty + cy^2 = d$ and pure powers in recurrence sequences*, Math. Scand. **52** (1983), no. 1, 24–36. MR **84g:**10038

1180. ———, *Pure powers in recurrence sequences and some related Diophantine equations*, J. Number Theory **27** (1987), no. 3, 324–352. MR **89a:**11024

1181. T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge University Press, Cambridge, 1986. MR **88h:**11002

1182. V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp. **58** (1992), no. 197, 369–380. MR **92e:**11140

1183. I. E. Shparlinski, *Bounds for exponential sums with recurrence sequences and their applications*, Proc. Voronezh State Pedagogical Inst. **197** (1978), 74–85.

1184. ———, *Distribution of nonresidues and primitive roots in recurrent sequences*, Mat. Zametki **24** (1978), no. 5, 603–613, 733. MR **80b:**10066

1185. ———, *Completely uniform distribution*, Zh. Vychisl. Mat. i Mat. Fiz. **19** (1979), no. 5, 1330–1333, 1359. MR **81b:**10033

1186. ———, *Prime divisors of recurrence sequences*, Izv. Vyssh. Uchebn. Zaved. Mat. **4** (1980), 100–103. MR **81j:**10015

1187. ———, *On the distribution of the fractional parts of recurrent sequences*, Zh. Vychisl. Mat. i Mat. Fiz. **21** (1981), no. 6, 1588–1591, 1616. MR **83e:**10074

1188. ———, *On some properties of linear cyclic codes*, Problemy Peredachi Inform. **19** (1983), 106–110.

1189. ———, *A multiplicative pseudo-random number transducer*, Zh. Vychisl. Mat. i Mat. Fiz. **24** (1984), no. 9, 1406–1408. MR **85m:**65006

1190. ———, *The number of prime divisors of recurrence sequences*, Mat. Zametki **38** (1985), no. 1, 29–34, 168. MR **87a:**11017

1191. ———, *Weight spectra of certain codes*, Problemy Peredachi Informatsii **22** (1986), no. 2, 43–48. MR **88f:**94047

1192. ———, *The number of different prime divisors of recurrent sequences*, Mat. Zametki **42** (1987), no. 4, 494–507, 622. MR **89k:**11092

1193. ———, *Residue classes modulo a prime in an algebraic number field*, Mat. Zametki **43** (1988), no. 4, 433–438, 573. MR **89j:**11089

1194. ———, *A sequence of pseudorandom numbers*, Avtomat. i Telemekh. **7** (1988), 185–188. MR **90m:**65019

1195. ———, *Arithmetic properties of solutions of norm form equations*, Uspekhi Mat. Nauk **44** (1989), no. 3(267), 183–184. MR **90j:**11028

1196. ———, *Distribution of values of recurrent sèquences*, Problemy Peredachi Informatsii **25** (1989), no. 2, 46–53. MR **90k:**11017

1197. ———, *Some arithmetic properties of recurrence sequences*, Mat. Zametki **47** (1990), no. 6, 124–131. MR **91m:**11006

1198. ———, *Estimates for Gauss sums*, Mat. Zametki **50** (1991), no. 1, 122–130. MR **92m:**11082

1199. ———, *On polynomial congruences*, Acta Arith. **58** (1991), no. 2, 153–156. MR **92h:**11078

1200. ———, *On the distribution of values of recurring sequences and the Bell numbers in finite fields*, European J. Combin. **12** (1991), no. 1, 81–87. MR **92a:**11021

1201. ———, *On exponential sums with sparse polynomials and rational functions*, J. Number Theory **60** (1996), no. 2, 233–244. MR **97g:**11089

1202. ———, *Finite fields: Theory and computation*, Kluwer Academic Publishers, Dordrecht, 1999. MR **2001g:**11188

1203. ———, *Number theoretic methods in cryptography: Complexity lower bounds*, Birkhäuser Verlag, Basel, 1999. MR **2001a:**94026

1204. ———, *On the Naor-Reingold pseudo-random function from elliptic curves*, Appl. Algebra Engrg. Comm. Comput. **11** (2000), no. 1, 27–34. MR **2001m:**65015

1205. ———, *On some properties of the shrinking generator*, Des. Codes Cryptogr. **23** (2001), no. 2, 147–155. MR **2002d:**94036

1206. ———, *On the generalised hidden number problem and bit security of XTR*, Lect. Notes in Comp. Sci. **2227** (2001), 268–277.

1207. ———, *On the linear complexity of the power generator*, Des. Codes Cryptogr. **23** (2001), no. 1, 5–10. MR **2003a:**11095

1208. ———, *On the uniformity of distribution of the Naor-Reingold pseudo-random function*, Finite Fields Appl. **7** (2001), no. 2, 318–326. MR **2002b:**11104

1209. ———, *Bounds of Gauss sums in finite fields*, Proc. Amer. Math. Soc. (to appear).

1210. I. E. Shparlinski and J. H. Silverman, *On the linear complexity of the Naor-Reingold pseudo-random function from elliptic curves*, Des. Codes Cryptogr. **24** (2001), no. 3, 279–289. MR **2002j:**11087

1211. V. M. Sidel′nikov, *Estimates for the number of appearances of elements on an interval of a recurrent sequence over a finite field*, Diskret. Mat. **3** (1991), no. 2, 87–95. MR **92h:**11108

1212. L. Sigler, *Fibonacci's Liber Abaci*, Springer-Verlag, New York, 2002, A Translation into Modern English of Leonardo Pisano's Book of Calculation.

1213. J. H. Silverman, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48** (1981), no. 3, 633–648. MR **82k:**14043

1214. ———, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986. MR **87g:**11070

1215. ———, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237. MR **89m:**11027

1216. ———, *Integer points, Diophantine approximation, and iteration of rational maps*, Duke Math. J. **71** (1993), no. 3, 793–829. MR **95e:**11070

1217. ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994. MR **96b:**11074

1218. ———, *The field of definition for dynamical systems on* $\mathbb{P}^1$, Compositio Math. **98** (1995), no. 3, 269–304. MR **96j:**11090

1219. ———, *The space of rational maps on* $\mathbb{P}^1$, Duke Math. J. **94** (1998), no. 1, 41–77. MR **2000m:**14010

1220. S. Kh. Sirazhdinov, T. A. Azlarov, and T. M. Zuparov, *Additivnye zadachi s rastushchim chislom slagaemykh*, Izdat. "Fan" Uzbek. SSR, Tashkent, 1975. MR 58 #16554

1221. T. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen*, Comptes rendus du congrés des mathématiciens scandinaves, Stockholm, 1934 (1935), 163–188.

1222. N. J. A. Sloane, *An on-line version of the encyclopedia of integer sequences*, Electron. J. Combin. **1** (1994), Feature 1, approx. 5 pp., `www.research.att.com/~njas/sequences/`. MR **95b:**05001

1223. N. J. A. Sloane and S. Plouffe, *The encyclopedia of integer sequences*, Academic Press Inc., San Diego, CA, 1995. MR **96a:**11001

1224. S. Smale, *Differentiable dynamical systems*, Bull. Amer. Math. Soc. **73** (1967), 747–817. MR 37 #3598

1225. C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175. MR 44 #6641

1226. I. M. Sobol′, *Mnogomernye kvadraturnye formuly i funktsii Khaara*, Izdat. "Nauka", Moscow, 1969. MR 54 #10952

1227. L. Somer, *Linear recurrences having almost all primes as maximal divisors*, Fibonacci numbers and their applications (Patras, 1984), Reidel, Dordrecht, 1986, pp. 257–272. MR **87i:**11027

1228. ———, *Divisibility of terms in Lucas sequences by their subscripts*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 515–525. MR **94m:**11022

1229. ———, *Upper bounds for frequencies of elements in second-order recurrences over a finite field*, Applications of Fibonacci numbers, Vol. 5 (St. Andrews, 1992), Kluwer Acad. Publ., Dordrecht, 1993, pp. 527–546. MR **95c:**11021

1230. ———, *Periodicity properties of kth order linear recurrences whose characteristic polynomial splits completely over a finite field. I*, Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), Amer. Math. Soc., Providence, RI, 1994, pp. 327–339. MR **95k:**11018

1231. ———, *Periodicity properties of kth order linear recurrences whose characteristic polynomial splits completely over a finite field. II*, Finite fields and applications (Glasgow, 1995), Cambridge Univ. Press, Cambridge, 1996, pp. 333–347. MR **97m:**11022

1232. M. Somos, *Problem 1470*, Crux Mathematicorum **15** (1989), 208.

1233. V. G. Sprindzhuk, *Klassicheskie diofantovy uravneniya ot dvukh neizvestnykh*, "Nauka", Moscow, 1982. MR **85d:**11022

1234. V. G. Sprindžuk, *Problema Malera v metricheskoiteorii chisel*, Izdat. "Nauka i Tehnika", Minsk, 1967. MR 39 #6832

1235. ———, *Mahler's problem in metric number theory*, American Mathematical Society, Providence, R.I., 1969. MR 39 #6833

1236. R. P. Stanley, *Differentiably finite power series*, European J. Combin. **1** (1980), no. 2, 175–188. MR **81m:**05012

1237. S. A. Stepanov and I. E. Shparlinski, *On the construction of a primitive normal basis of a finite field*, Mat. Sb. **180** (1989), no. 8, 1067–1072, 1151. MR **90j:**12003

1238. ———, *On the construction of primitive elements and primitive normal bases in a finite field*, Computational number theory (Debrecen, 1989), de Gruyter, Berlin, 1991, pp. 1–14. MR **93a:**11102

1239. ———, *On normal bases of algebraic number fields*, New trends in probability and statistics, Vol. 2 (Palanga, 1991), VSP, Utrecht, 1992, pp. 369–378. MR **94a:**11177

1240. P. J. Stephens, *An average result for Artin's conjecture*, Mathematika **16** (1969), 178–188. MR 58 #16565

1241. ———, *Prime divisors of second-order linear recurrences. I*, J. Number Theory **8** (1976), no. 3, 313–332. MR 54 #5142

1242. ———, *Prime divisors of second order linear recurrences. II*, J. Number Theory **8** (1976), no. 3, 333–345. MR 54 #5143

1243. C. L. Stewart, *On divisors of Fermat, Fibonacci, Lucas, and Lehmer numbers*, Proc. London Math. Soc. (3) **35** (1977), no. 3, 425–447. MR 58 #10694

1244. ———, *Primitive divisors of Lucas and Lehmer numbers*, Transcendence theory: advances and applications (Proc. Conf., Univ. Cambridge, Cambridge, 1976), Academic Press, London, 1977, pp. 79–92. MR 57 #16187

1245. ———, *On divisors of terms of linear recurrence sequences*, J. Reine Angew. Math. **333** (1982), 12–31. MR **83i:**10010

1246. ———, *On some Diophantine equations and related linear recurrence sequences*, Progress in Math., vol. 22, Birkhäuser, Boston, 1982, pp. 317–321.

1247. ———, *On divisors of Fermat, Fibonacci, Lucas and Lehmer numbers. III*, J. London Math. Soc. (2) **28** (1983), no. 2, 211–217. MR **85g:**11021

1248. ———, *On the greatest prime factor of terms of a linear recurrence sequence*, Rocky Mountain J. Math. **15** (1985), no. 2, 599–608. MR **87h:**11017

1249. C. L. Stewart and K. R. Yu, *On the abc conjecture*, Math. Ann. **291** (1991), no. 2, 225–230. MR **92k:**11037

1250. ———, *On the abc conjecture. II*, Duke Math. J. **108** (2001), no. 1, 169–181. MR **2002e:**11046

1251. D. R. Stinson, *Cryptography: Theory and practice*, CRC Press, Boca Raton, FL, 1995. MR **96k:**94015

1252. M. Stoll, *Galois groups over $\mathbb{Q}$ of some iterated polynomials*, Arch. Math. (Basel) **59** (1992), no. 3, 239–244. MR **93h:**12004

1253. ———, *Bounds for the length of recurrence relations for convolutions of P-recursive sequences*, European J. Combin. **18** (1997), no. 6, 707–712. MR **99f:**05007

1254. R. G. Stoneham, *A general arithmetic construction of transcendental non-Liouville normal numbers from rational fractions*, Acta Arith. **16** (1969/1970), 239–253. MR 42 #207b

1255. ———, *On (j, ε)-normality in the rational fractions*, Acta Arith. **16** (1969/1970), 221–237. MR 42 #207a

1256. ———, *On absolute (j, ε)-normality in the rational fractions with applications to normal numbers*, Acta Arith. **22** (1972/73), 277–286. MR 47 #6621

1257. ———, *On the uniform ε-distribution of residues within the periods of rational fractions with applications to normal numbers*, Acta Arith. **22** (1973), 371–389. MR 47 #6640

1258. ———, *On a sequence of (j, ε)-normal approximations to $\pi/4$ and the Brouwer conjecture*, Acta Arith. **42** (1983), no. 3, 265–279. MR **85g:**11062

1259. R. Stong, *The average order of a matrix*, J. Combin. Theory Ser. A **64** (1993), no. 2, 337–343. MR **94j:**11094

1260. S. Strandt, *Quadratic congruential generators with odd composite modulus*, Monte Carlo and quasi-Monte Carlo methods 1996 (Salzburg), Springer, New York, 1998, pp. 415–426. MR **99d:**65024

1261. R. Strassmann, *Uber den wertevorrat von Potenzreihen im gebiet der $\mathfrak{p}$-adischen Zahlen*, J. Reine Angew. Math. **159** (1928), 13–28.

1262. O. Strauch, *On distribution functions of $\xi(3/2)^n$ mod 1*, Acta Arith. **81** (1997), no. 1, 25–35. MR **98c:**11075

1263. M. Strauss, *Normal numbers and sources for BPP*, Theoret. Comput. Sci. **178** (1997), no. 1-2, 155–169. MR **98a:**68077

1264. W. Sun, A. Klapper, and Y. X. Yang, *On correlations of a family of generalized geometric sequences*, IEEE Trans. Inform. Theory **47** (2001), no. 6, 2609–2618. MR **2002m:**94046

1265. Z.-W. Sun, *A congruence for primes*, Proc. Amer. Math. Soc. **123** (1995), no. 5, 1341–1346. MR **95f:**11003

1266. ———, *On the sum* $\sum_{k\equiv r \pmod{m}} \binom{n}{k}$ *and related congruences*, Israel J. Math. **128** (2002), 135–156. MR **2003d:**11026

1267. Z.-W. Sun and M.-H. Le, *Integers not of the form* $c(2^a + 2^b) + p^\alpha$, Acta Arith. **99** (2001), no. 2, 183–190. MR **2002e:**11043

1268. C. S. Swart, *Elliptic divisibility sequences*, Ph.D. thesis, Royal Holloway (University of London), 2003.

1269. E. Szemerédi, *On sets of integers containing no k elements in arithmetic progression*, Acta Arith. **27** (1975), 199–245. MR 51 #5547

1270. ———, *Integer sets containing no arithmetic progressions*, Acta Math. Hungar. **56** (1990), no. 1-2, 155–158. MR **92c:**11100

1271. P. Szüsz and B. Volkmann, *A combinatorial method for constructing normal numbers*, Forum Math. **6** (1994), no. 4, 399–414. MR **95f:**11053

1272. E. J. Taft, *Hadamard invertibility of linearly recursive sequences in several variables*, Discrete Math. **139** (1995), no. 1-3, 393–397. MR **96f:**16048

1273. S. Takahashi, *Cellular automata, fractals and multifractals: space-time patterns and dimension spectra of linear cellular automata*, Chaos in Australia (Sydney, 1990), World Sci. Publishing, River Edge, NJ, 1993, pp. 173–195. MR **96f:**58084

1274. T. Tapsoba, *Automates calculant la complexité de suites automatiques*, J. Théor. Nombres Bordeaux **6** (1994), no. 1, 127–134. MR **95i:**11017

1275. R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572. MR **96d:**11072

1276. S. Tezuka, *The k-dimensional distribution of combined GFSR sequences*, Math. Comp. **62** (1994), no. 206, 809–817. MR **94i:**65014

1277. ———, *Uniform random numbers*, Kluwer, Dordrecht, 1996.

1278. R. F. Tichy, *Stability of a class of nonuniform random number generators*, J. Math. Anal. Appl. **181** (1994), no. 2, 546–561. MR **94m:**65018

1279. ———, *Diophantine properties of digital expansions*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 501–522. MR **99g:**11016

1280. ———, *Three examples of triangular arrays with optimal discrepancy and linear recurrences*, Applications of Fibonacci numbers, Vol. 7, Kluwer Acad. Publ., Dordrecht, 1998, pp. 415–421.

1281. R. Tijdeman, *On the number of zeros of general exponential polynomials*, Nederl. Akad. Wetensch. Proc. Ser. A **74** = Indag. Math. **33** (1971), 1–7. MR 44 #4193

1282. ———, *Note on Mahler's* 3/2*-problem*, Det Kong. Norske Vidensk. Selsk. **16** (1972), 1–4.

1283. ———, *On the maximal distance between integers composed of small primes*, Compositio Math. **28** (1974), 159–162. MR 49 #10646

1284. ———, *Multiplicities of binary recurrences*, Seminar on Number Theory, 1980–1981 (Talence, 1980–1981), Univ. Bordeaux I, Talence, 1981, pp. Exp. No. 29, 11. MR **83f:**10014

1285. ———, *Exponential Diophantine equations 1986–1996*, Number theory (Eger, 1996), de Gruyter, Berlin, 1998, pp. 523–539. MR **99f:**11046

1286. ———, *Some applications of Diophantine approximation*, Number Theory for the Millennium, Vol.III, A. K. Peters, Natick, MA, 2002, pp. 261–284.

1287. J. Tits, *Appendix to: "Groups of polynomial growth and expanding maps" [Inst. Hautes Études Sci. Publ. Math. No. 53 (1981), 53–73] by M. Gromov*, Inst. Hautes Études Sci. Publ. Math. **53** (1981), 74–78. MR **83b:**53042

1288. M. Tompa, *Lecture notes on probabilistic algorithms and pseudorandom generators*, Technical Report 91-07-05, Dept. of Comp. Sci. and Engin., Univ. of Washington, 1991.

1289. Th. Töpfer, *Simultaneous approximation measures for functions satisfying generalized functional equations of Mahler type*, Abh. Math. Sem. Univ. Hamburg **66** (1996), 177–201. MR **97k:**11108

1290. J. Tromp and J. Shallit, *Subword complexity of a generalized Thue-Morse word*, Inform. Process. Lett. **54** (1995), no. 6, 313–316. MR **96d:**68170

1291. P. Turán, *Eine Extremalaufgabe aus der Graphentheorie*, Mat. Fiz. Lapok **48** (1941), 436–452. MR 8,284j

1292. P. Udaya and M. U. Siddiqi, *Optimal and suboptimal quadriphase sequences derived from maximal length sequences over* $\mathbb{Z}_4$, Appl. Algebra Engrg. Comm. Comput. **9** (1998), no. 2, 161–191. MR **2000j:**94021

1293. ———, *Optimal large linear complexity frequency hopping patterns derived from polynomial residue class rings*, IEEE Trans. Inform. Theory **44** (1998), no. 4, 1492–1503. MR **2000e:**94003

1294. E. Ugalde, *An alternative construction of normal numbers*, J. Théor. Nombres Bordeaux **12** (2000), no. 1, 165–177. MR **2002b:**11101

1295. R. Vaidyanathaswamy, *The theory of multiplicative arithmetic functions*, Trans. Amer. Math. Soc. **33** (1931), no. 2, 579–662.

1296. M. Vâjâitu and A. Zaharescu, *A finiteness theorem for a class of exponential congruences*, Proc. Amer. Math. Soc. **127** (1999), no. 8, 2225–2232. MR **99j:**11003

1297. R. C. Vaughan, *On the distribution of* αp *modulo* 1, Mathematika **24** (1977), no. 2, 135–141. MR 57 #12423

1298. G. Venturini, *Iterates of number-theoretic functions with periodic rational coefficients (generalization of the* $3x + 1$ *problem)*, Stud. Appl. Math. **86** (1992), no. 3, 185–218. MR **93b:**11102

1299. ———, *On a generalization of the* $3x + 1$ *problem*, Adv. in Appl. Math. **19** (1997), no. 3, 295–305. MR **98j:**11013

1300. N. K. Vereshchagin, *Zeros of linear recursive sequences*, Dokl. Akad. Nauk SSSR **278** (1984), no. 5, 1036–1039. MR **86c:**68064

1301. ———, *The problem of the appearance of a zero in a linear recursive sequence*, Mat. Zametki **38** (1985), no. 2, 177–189, 347. MR **87b:**11018

1302. ———, *Effective upper bounds for the number of zeros of a linear recurrence sequence*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. **1** (1986), 25–30, 92. MR **87d:**11016

1303. I. M. Vinogradov, *A new estimation of a trigonometric sum involving primes*, Bull. Acad. Sc. URSS Ser. Math. **2** (1938), 1–13.

1304. F. Vivaldi, *Dynamics over irreducible polynomials*, Nonlinearity **5** (1992), no. 4, 941–960. MR **93i:**11152

1305. ———, *Geometry of linear maps over finite fields*, Nonlinearity **5** (1992), no. 1, 133–147. MR **93c:**11111

1306. ———, *Cellular automata and finite fields*, Phys. D **79** (1994), no. 2-4, 115–131. MR **95k:**11159

1307. F. Vivaldi and S. Hatjispyros, *Galois theory of periodic orbits of rational maps*, Nonlinearity **5** (1992), no. 4, 961–978. MR **93i:**11153

1308. J. F. Voloch, *Diagonal equations over function fields*, Bol. Soc. Brasil. Mat. **16** (1985), no. 2, 29–39. MR **87g:**11157

1309. ———, *The equation* $ax + by = 1$ *in characteristic* p, J. Number Theory **73** (1998), no. 2, 195–200. MR **2000b:**11029

1310. ———, *On some subgroups of the multiplicative group of finite rings*, Preprint, 2003.

1311. B. Voorhees, *A note on injectivity of additive cellular automata*, Complex Systems **8** (1994), no. 3, 151–159. MR **96d:**68158

1312. M. Voorhoeve, *On the oscillation of exponential polynomials*, Math. Z. **151** (1976), no. 3, 277–294. MR 55 #3224

1313. ———, *Zeros of exponential polynomials*, Rijksuniversiteit te Leiden, Leiden, 1977, Doctoral dissertation, University of Leiden, Leiden. MR 56 #3263

1314. M. Voorhoeve and A. J. van der Poorten, *Wronskian determinants and the zeros of certain functions*, Nederl. Akad. Wetensch. Proc. Ser. A **78** = Indag. Math. **37** (1975), no. 5, 417–424. MR 53 #3275

1315. M. Voorhoeve, A. J. van der Poorten, and R. Tijdeman, *On the number of zeros of certain functions*, Nederl. Akad. Wetensch. Proc. Ser. A **78** = Indag. Math. **37** (1975), no. 5, 407–416. MR 53 #3274

1316. P. M. Voutier, *Primitive divisors of Lucas and Lehmer sequences*, Math. Comp. **64** (1995), no. 210, 869–888. MR **95f:**11022

1317. ———, *Primitive divisors of Lucas and Lehmer sequences. II*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 251–274. MR **98h:**11037

1318. ———, *Primitive divisors of Lucas and Lehmer sequences. III*, Math. Proc. Cambridge Philos. Soc. **123** (1998), no. 3, 407–419. MR **99b:**11027

1319. M. A. Vsemirnov, *Diophantine representations of linear recurrent sequences. I*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **227** (1995), no. Voprosy Teor. Predstav. Algebr i Grupp. 4, 52–60, 156–157. MR **97b:**11015

1320. ———, *Diophantine representations of linear recurrent sequences. II*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI) **241** (1997), no. Issled. po Konstr. Mat. i Mat. Log. X, 5–29, 150. MR **2000k:**11019

1321. S. S. Wagstaff, Jr., *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arith. **41** (1982), no. 2, 141–150. MR **83m:**10004

1322. ———, *Divisors of Mersenne numbers*, Math. Comp. **40** (1983), no. 161, 385–397. MR **84j:**10052

1323. ———, *Aurifeuillian factorizations and the period of the Bell numbers modulo a prime*, Math. Comp. **65** (1996), no. 213, 383–391. MR **96f:**11033

1324. M. Waldschmidt, *Introduction to recent results in transcendental number theory*, Preprint of the Math. Sci. Inst., Berkeley, MSRI 074-93, 1993.

1325. ———, *Diophantine approximation on linear algebraic groups*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 326, Springer-Verlag, Berlin, 2000, Transcendence properties of the exponential function in several variables. MR **2001c:**11075

1326. J. T.-Y. Wang, *A note on Wronskians and the ABC theorem in function fields of prime characteristic*, Manuscripta Math. **98** (1999), no. 2, 255–264. MR **2000d:**11086

1327. M. Z. Wang, *Linear complexity profiles and jump complexity*, Inform. Process. Lett. **61** (1997), no. 3, 165–168. MR **98a:**94016

1328. M. Ward, *The arithmetical theory of linear recurring series*, Trans. Amer. Math. Soc. **35** (1933), no. 3, 600–628.

1329. ———, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J. **15** (1948), 941–946. MR 10,283e

1330. ———, *Memoir on elliptic divisibility sequences*, Amer. J. Math. **70** (1948), 31–74. MR 9,332j

1331. ———, *Prime divisors of second order recurring sequences*, Duke Math. J. **21** (1954), 607–614. MR 16,221f

1332. ———, *The laws of apparition and repetition of primes in a cubic recurrence*, Trans. Amer. Math. Soc. **79** (1955), 72–90. MR 16,906d

1333. ———, *The linear p-adic recurrence of order two*, Illinois J. Math. **6** (1962), 40–52. MR 25 #2028

1334. T. Ward, *Additive relations in fields: an entropy approach*, J. Number Theory **53** (1995), no. 1, 137–143. MR **97d:**11126

1335. ———, *Three results on mixing shapes*, New York J. Math. **3A** (1997/98), no. Proceedings of the New York Journal of Mathematics Conference, June 9–13, 1997, 1–10. MR **99e:**28031

1336. ———, *Almost all S-integer dynamical systems have many periodic points*, Ergodic Theory Dynam. Systems **18** (1998), no. 2, 471–486. MR **99k:**58152

1337. ———, *Additive cellular automata and volume growth*, Entropy **2** (2000), 142–167.

1338. T. Washio and T. Kodama, *Hasse-Witt matrices of hyperelliptic function fields*, Sci. Bull. Fac. Ed. Nagasaki Univ. **37** (1986), 9–15. MR **87k:**11064

1339. ———, *A note on a supersingular function field*, Sci. Bull. Fac. Ed. Nagasaki Univ. **37** (1986), 17–21. MR **87m:**14034

1340. B. Weiss, *Single orbit dynamics*, American Mathematical Society, Providence, RI, 2000. MR **2000k:**37001

1341. H. Weyl, *Uber die Gleichverteilung von Zahlen mod Eins*, Math. Ann. **77** (1916), 313–352.

1342. M. J. Wiener, *Cryptanalysis of short RSA secret exponents*, IEEE Trans. Inform. Theory **36** (1990), no. 3, 553–558. MR **91f:**94018

1343. K. Wiertelak, *On the density of some sets of primes. I*, Acta Arith. **34** (1977/78), no. 3, 183–196. MR 58 #5554a

1344. ———, *On the density of some sets of primes. II*, Acta Arith. **34** (1977/78), no. 3, 197–210. MR 58 #5554b

1345. ———, *On the density of some sets of primes. III*, Funct. Approx. Comment. Math. **10** (1981), 93–103. MR **84i:**10045

1346. ———, *On the density of some sets of primes. III*, Studies in pure mathematics, Birkhäuser, Basel, 1983, pp. 761–773. MR **87c:**11082

1347. ———, *On the density of some sets of primes. IV*, Acta Arith. **43** (1984), no. 2, 177–190. MR **86e:**11081

1348. ———, *On the density of some sets of integers*, Funct. Approx. Comment. Math. **19** (1990), 71–76. MR **92d:**11099

1349. ———, *On the density of some sets of primes p, for which* $(\operatorname{ord}_p b, n) = d$, Funct. Approx. Comment. Math. **21** (1992), 69–73. MR **95f:**11069

1350. ———, *On the distribution of the smallest natural numbers having order mod p not coprime with a given integer*, Acta Math. Hungar. **80** (1998), no. 4, 271–284. MR **99h:**11112

1351. ———, *On the density of some sets of primes p, for which* $n \mid \operatorname{ord}_p a$, Funct. Approx. Comment. Math. **28** (2000), 237–241, Dedicated to Włodzimierz Staś on the occasion of his 75th birthday. MR **2003a:**11120

1352. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR **96d:**11071

1353. H. C. Williams, *Some generalizations of the* S_n *sequence of Shanks*, Acta Arith. **69** (1995), no. 3, 199–215. MR **96a:**11118

1354. ———, *Édouard Lucas and primality testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. 22, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR **2000b:**11139

1355. H. C. Williams and J. Shallit, *Factoring integers before computers*, Mathematics of Computation 1943–1993: a half-century of computational mathematics (Vancouver, BC, 1993), Amer. Math. Soc., Providence, RI, 1994, pp. 481–531. MR **95m:**11143

1356. S. Williams, *Zeros in nth order linear recurrence sequences*, Master's thesis, Macquarie University (Honours Thesis), 1994.

1357. G. J. Wirsching, *The dynamical system generated by the* $3n + 1$ *function*, Springer-Verlag, Berlin, 1998. MR **99g:**11027

1358. S. Wolfram, *Random sequence generation by cellular automata*, Adv. in Appl. Math. **7** (1986), no. 2, 123–169. MR **87i:**68057

1359. S. Wolfram (ed.), *Theory and applications of cellular automata*, World Scientific Publishing Co., Singapore, 1986. MR **87j:**68007

1360. J. W. Wrench, Jr., *Evaluation of Artin's constant and the twin-prime constant*, Math. Comp. **15** (1961), 396–398. MR 23 #A1619

1361. C. Xing, H. Niederreiter, K. Y. Lam, and C. Ding, *Constructions of sequences with almost perfect linear complexity profile from curves over finite fields*, Finite Fields Appl. **5** (1999), no. 3, 301–313. MR **2000g:**94027

1362. J. Xu and A. Klapper, *Feedback with carry shift registers over* $\mathbb{Z}/(N)$, Sequences and their applications (Singapore, 1998), Springer, London, 1999, pp. 379–392. MR **2002f:**94035

1363. A. A. Yacobson, *Bounds for exponential sums with recurring sequences and their applications*, Proc. Voronezh State Pedagogical Inst. **197** (1978), 86–91.

1364. Y. X. Yang, *New binary sequences with perfect staircase profile of linear complexity*, Inform. Process. Lett. **46** (1993), no. 1, 27–29. MR **94e:**94011

1365. K. Yokoyama, Z. Li, and I. Nemes, *Finding roots of unity among quotients of the roots of an integral polynomial*, Proc. Intern. Symp. on Symb. and Algebraic Comp. (1995), 85–89.

1366. K. R. Yu, *Linear forms in p-adic logarithms*, Acta Arith. **53** (1989), no. 2, 107–186. MR **90k:**11093

1367. ———, *Linear forms in p-adic logarithms. II*, Compositio Math. **74** (1990), no. 1, 15–113, Erratum: **76** (1990), 307. MR **91h:**11065a

1368. ———, *Linear forms in p-adic logarithms. III*, Compositio Math. **91** (1994), no. 3, 241–276. MR **95f:**11050

1369. K. R. Yu and L.-K. Hung, *On binary recurrence sequences*, Indag. Math. (N.S.) **6** (1995), no. 3, 341–354. MR **96i:**11081

1370. L. Yu and M. Le, *On the Diophantine equation* $(x^m - 1)/(x - 1) = y^n$, Acta Arith. **73** (1995), no. 4, 363–366. MR **96m:**11023

1371. A. Zaharescu, *Small values of* $n^2\alpha \pmod 1$, Invent. Math. **121** (1995), no. 2, 379–388. MR **96d:**11079

1372. ———, *Correlation of fractional parts of* $n^2\alpha$, Forum Math. **15** (2003), no. 1, 1–21. MR 1 957 276

1373. U. Zannier, *Some remarks on the S-unit equation in function fields*, Acta Arith. **64** (1993), no. 1, 87–98. MR **94c:**11111

1374. ———, *Vanishing sums of roots of unity*, Rend. Sem. Mat. Univ. Politec. Torino **53** (1995), no. 4, 487–495. MR **98j:**11086

1375. ———, *A proof of Pisot's dth root conjecture*, Ann. of Math. (2) **151** (2000), no. 1, 375–383. MR **2001f:**11191

1376. Y. Zheng, *Existence of nonperiodic solutions of the Lyness equation* $x_{n+1} = (\alpha + x_n)/x_{n-1}$, J. Math. Anal. Appl. **209** (1997), no. 1, 94–102. MR **99k:**39046

1377. C. Z. Zhou, *Some discussion on the* $3x+1$ *problem*, J. South China Normal Univ. Natur. Sci. Ed. **3** (1995), 103–105. MR **97h:**11021

1378. N. Zierler, *Linear recurring sequences*, J. Soc. Indust. Appl. Math. **7** (1959), 31–48. MR 21 #781

1379. N. Zierler and W. H. Mills, *Products of linear recurring sequences*, J. Algebra **27** (1973), 147–157. MR 48 #3930

1380. M. Zieve, *Cycles of polynomial mappings*, Ph.D. thesis, Univ. of California, Berkeley, 1996.

1381. R. Zippel, *Effective polynomial computation*, Kluwer A. P., Dordrecht, 1993.

1382. K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. **3** (1892), 265–284.

Index

Titles in This Series

104 **Graham Everest, Alf van der Poorten, Igor Shparlinski, and Thomas Ward,** Recurrence sequences, 2003

103 **Octav Cornea, Gregory Lupton, John Oprea, and Daniel Tanré,** Lusternik-Schnirelmann category, 2003

102 **Linda Rass and John Radcliffe,** Spatial deterministic epidemics, 2003

101 **Eli Glasner,** Ergodic theory via joinings, 2003

99 **Philip S. Hirschhorn,** Model categories and their localizations, 2003

98 **Victor Guillemin, Viktor Ginzburg, and Yael Karshon,** Moment maps, cobordisms, and Hamiltonian group actions, 2002

97 **V. A. Vassiliev,** Applied Picard-Lefschetz theory, 2002

96 **Martin Markl, Steve Shnider, and Jim Stasheff,** Operads in algebra, topology and physics, 2002

95 **Seiichi Kamada,** Braid and knot theory in dimension four, 2002

94 **Mara D. Neusel and Larry Smith,** Invariant theory of finite groups, 2002

93 **Nikolai K. Nikolski,** Operators, functions, and systems: An easy reading. Volume 2: Model operators and systems, 2002

92 **Nikolai K. Nikolski,** Operators, functions, and systems: An easy reading. Volume 1: Hardy, Hankel, and Toeplitz, 2002

91 **Richard Montgomery,** A tour of subriemannian geometries, their geodesics and applications, 2002

90 **Christian Gérard and Izabella Łaba,** Multiparticle quantum scattering in constant magnetic fields, 2002

89 **Michel Ledoux,** The concentration of measure phenomenon, 2001

88 **Edward Frenkel and David Ben-Zvi,** Vertex algebras and algebraic curves, 2001

87 **Bruno Poizat,** Stable groups, 2001

86 **Stanley N. Burris,** Number theoretic density and logical limit laws, 2001

85 **V. A. Kozlov, V. G. Maz′ya, and J. Rossmann,** Spectral problems associated with corner singularities of solutions to elliptic equations, 2001

84 **László Fuchs and Luigi Salce,** Modules over non-Noetherian domains, 2001

83 **Sigurdur Helgason,** Groups and geometric analysis: Integral geometry, invariant differential operators, and spherical functions, 2000

82 **Goro Shimura,** Arithmeticity in the theory of automorphic forms, 2000

81 **Michael E. Taylor,** Tools for PDE: Pseudodifferential operators, paradifferential operators, and layer potentials, 2000

80 **Lindsay N. Childs,** Taming wild extensions: Hopf algebras and local Galois module theory, 2000

79 **Joseph A. Cima and William T. Ross,** The backward shift on the Hardy space, 2000

78 **Boris A. Kupershmidt,** KP or mKP: Noncommutative mathematics of Lagrangian, Hamiltonian, and integrable systems, 2000

77 **Fumio Hiai and Dénes Petz,** The semicircle law, free random variables and entropy, 2000

76 **Frederick P. Gardiner and Nikola Lakic,** Quasiconformal Teichmüller theory, 2000

75 **Greg Hjorth,** Classification and orbit equivalence relations, 2000

74 **Daniel W. Stroock,** An introduction to the analysis of paths on a Riemannian manifold, 2000

73 **John Locker,** Spectral theory of non-self-adjoint two-point differential operators, 2000

72 **Gerald Teschl,** Jacobi operators and completely integrable nonlinear lattices, 1999

71 **Lajos Pukánszky,** Characters of connected Lie groups, 1999

TITLES IN THIS SERIES

70 **Carmen Chicone and Yuri Latushkin,** Evolution semigroups in dynamical systems and differential equations, 1999

69 **C. T. C. Wall (A. A. Ranicki, Editor),** Surgery on compact manifolds, second edition, 1999

68 **David A. Cox and Sheldon Katz,** Mirror symmetry and algebraic geometry, 1999

67 **A. Borel and N. Wallach,** Continuous cohomology, discrete subgroups, and representations of reductive groups, second edition, 2000

66 **Yu. Ilyashenko and Weigu Li,** Nonlocal bifurcations, 1999

65 **Carl Faith,** Rings and things and a fine array of twentieth century associative algebra, 1999

64 **Rene A. Carmona and Boris Rozovskii, Editors,** Stochastic partial differential equations: Six perspectives, 1999

63 **Mark Hovey,** Model categories, 1999

62 **Vladimir I. Bogachev,** Gaussian measures, 1998

61 **W. Norrie Everitt and Lawrence Markus,** Boundary value problems and symplectic algebra for ordinary differential and quasi-differential operators, 1999

60 **Iain Raeburn and Dana P. Williams,** Morita equivalence and continuous-trace C^*-algebras, 1998

59 **Paul Howard and Jean E. Rubin,** Consequences of the axiom of choice, 1998

58 **Pavel I. Etingof, Igor B. Frenkel, and Alexander A. Kirillov, Jr.,** Lectures on representation theory and Knizhnik-Zamolodchikov equations, 1998

57 **Marc Levine,** Mixed motives, 1998

56 **Leonid I. Korogodski and Yan S. Soibelman,** Algebras of functions on quantum groups: Part I, 1998

55 **J. Scott Carter and Masahico Saito,** Knotted surfaces and their diagrams, 1998

54 **Casper Goffman, Togo Nishiura, and Daniel Waterman,** Homeomorphisms in analysis, 1997

53 **Andreas Kriegl and Peter W. Michor,** The convenient setting of global analysis, 1997

52 **V. A. Kozlov, V. G. Maz′ya, and J. Rossmann,** Elliptic boundary value problems in domains with point singularities, 1997

51 **Jan Malý and William P. Ziemer,** Fine regularity of solutions of elliptic partial differential equations, 1997

50 **Jon Aaronson,** An introduction to infinite ergodic theory, 1997

49 **R. E. Showalter,** Monotone operators in Banach space and nonlinear partial differential equations, 1997

48 **Paul-Jean Cahen and Jean-Luc Chabert,** Integer-valued polynomials, 1997

47 **A. D. Elmendorf, I. Kriz, M. A. Mandell, and J. P. May (with an appendix by M. Cole),** Rings, modules, and algebras in stable homotopy theory, 1997

46 **Stephen Lipscomb,** Symmetric inverse semigroups, 1996

45 **George M. Bergman and Adam O. Hausknecht,** Cogroups and co-rings in categories of associative rings, 1996

44 **J. Amorós, M. Burger, K. Corlette, D. Kotschick, and D. Toledo,** Fundamental groups of compact Kähler manifolds, 1996

For a complete list of titles in this series, visit the
AMS Bookstore at **www.ams.org/bookstore/**.

Recurrence sequences are of great intrinsic interest and have been a central part of number theory for many years. Moreover, these sequences appear almost everywhere in mathematics and computer science. This book surveys the modern theory of linear recurrence sequences and their generalizations. Particular emphasis is placed on the dramatic impact that sophisticated methods from Diophantine analysis and transcendence theory have had on the subject. Related work on bilinear recurrences and an emerging connection between recurrences and graph theory are covered. Applications and links to other areas of mathematics, including combinatorics, dynamical systems and cryptography, and to computer science are described.

ISBN 0-8218-3387-1

9 780821 833872

SURV/104