Igor E Shparlinski

List of Publications by Year
in descending order

579	5,687	159585	243625
papers	citations	30 h-index	44 g-index

609	609	609	1047
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	The Insecurity of the Digital Signature Algorithm with Partially Known Nonces. Journal of Cryptology, 2002, 15, 151-176.	2.8	156
2	The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces. Designs, Codes, and Cryptography, 2003, 30, 201-217.	1.6	111
3	PARAMETERS OF INTEGRAL CIRCULANT GRAPHS AND PERIODIC QUANTUM DYNAMICS. International Journal of Quantum Information, 2007, 05, 417-430.	1.1	69
4	On the statistical properties of Diffie-Hellman distributions. Israel Journal of Mathematics, 2000, 120, 23-46.	0.8	61
5	Finite Fields: Theory and Computation. , 1999, , .		60
6	On Polynomial Approximation of the Discrete Logarithm and the Diffieâ€"Hellman Mapping. Journal of Cryptology, 2000, 13, 339-360.	2.8	56
7	Pseudorandomness and Dynamics of Fermat Quotients. SIAM Journal on Discrete Mathematics, 2011, 25, 50-71.	0.8	53
8	On the Distribution and Lattice Structure of Nonlinear Congruential Pseudorandom Numbers. Finite Fields and Their Applications, 1999, 5, 246-253.	1.0	50
9	Graphs with integral spectrum. Linear Algebra and Its Applications, 2009, 430, 547-552.	0.9	50
10	Period of the power generator and small values of Carmichael's function. Mathematics of Computation, 2000, 70, 1591-1606.	2.1	48
11	On the distribution of inversive congruential pseudorandom numbers in parts of the period. Mathematics of Computation, 2000, 70, 1569-1575.	2.1	46
12	On the Hidden Shifted Power Problem. SIAM Journal on Computing, 2012, 41, 1524-1557.	1.0	46
13	Recent Advances in the Theory of Nonlinear Pseudorandom Number Generators. , 2002, , 86-102.		45
14	Certain Exponential Sums and Random Walks on Elliptic Curves. Canadian Journal of Mathematics, 2005, 57, 338-350.	0.6	43
15	Predicting nonlinear pseudorandom number generators. Mathematics of Computation, 2004, 74, 1471-1495.	2.1	41
16	On the energy of some circulant graphs. Linear Algebra and Its Applications, 2006, 414, 378-382.	0.9	41
17	Modular hyperbolas. Japanese Journal of Mathematics, 2012, 7, 235-294.	2.1	40
18	On the cycle structure of repeated exponentiation modulo a prime. Journal of Number Theory, 2004, 107, 345-356.	0.4	39

#	Article	IF	Citations
19	On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states. Journal of Mathematical Physics, 2005, 46, 082104.	1.1	39
20	Distribution of Modular Sums and the Security of the Server Aided Exponentiation. , 2001, , 331-342.		39
21	On finding primitive roots in finite fields. Theoretical Computer Science, 1996, 157, 273-275.	0.9	38
22	On the distribution of the power generator. Mathematics of Computation, 2000, 70, 1575-1590.	2.1	37
23	On the linear and nonlinear complexity profile of nonlinear pseudorandom number generators. IEEE Transactions on Information Theory, 2003, 49, 60-64.	2.4	37
24	On the Linear Complexity and Multidimensional Distribution of Congruential Generators over Elliptic Curves. Designs, Codes, and Cryptography, 2005, 35, 111-117.	1.6	36
25	On the divisibility of Fermat quotients. Michigan Mathematical Journal, 2010, 59, .	0.4	36
26	Character sums with exponential functions. Mathematika, 2000, 47, 75-85.	0.5	35
27	On the Unpredictability of Bits of the Elliptic Curve Diffie-Hellman Scheme. Lecture Notes in Computer Science, 2001, , 201-212.	1.3	35
28	Counting curves and their projections. Computational Complexity, 1996, 6, 64-99.	0.3	33
29	Indifferentiable deterministic hashing to elliptic and hyperelliptic curves. Mathematics of Computation, 2012, 82, 491-512.	2.1	33
30	On the Naor-Reingold Pseudo-Random Function from Elliptic Curves. Applicable Algebra in Engineering, Communications and Computing, 2000, 11, 27-34.	0.5	31
31	Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height. Israel Journal of Mathematics, 2009, 173, 253-277.	0.8	31
32	On Routing in Circulant Graphs. Lecture Notes in Computer Science, 1999, , 360-369.	1.3	31
33	Dynamical Systems Generated by Rational Functions. Lecture Notes in Computer Science, 2003, , 6-17.	1.3	28
34	Distribution of some sequences of points on elliptic curves. Journal of Mathematical Cryptology, 2007, 1, 1-11.	0.7	28
35	On the average energy of circulant graphs. Linear Algebra and Its Applications, 2008, 428, 1956-1963.	0.9	28
36	On a ternary quadratic form over primes. Acta Arithmetica, 2011, 150, 285-314.	0.4	28

#	Article	IF	Citations
37	On the Distribution of Pseudorandom Numbers and Vectors Generated by Inversive Methods. Applicable Algebra in Engineering, Communications and Computing, 2000, 10, 189-202.	0.5	27
38	On the concentration of points of polynomial maps and applications. Mathematische Zeitschrift, 2012, 272, 825-837.	0.9	27
39	On the Security of Diffie-Hellman Bits. , 2001, , 257-268.		27
40	On Certain Exponential Sums and the Distribution of Diffie-Hellman Triples. Journal of the London Mathematical Society, 1999, 59, 799-812.	1.0	26
41	On the Multidimensional Distribution of Inversive Congruential Pseudorandom Numbers in Parts of the Period. Monatshefte Fur Mathematik, 2000, 129, 31-36.	0.9	26
42	On the Linear Complexity of the Power Generator. Designs, Codes, and Cryptography, 2001, 23, 5-10.	1.6	25
43	ON THE SOLVABILITY OF BILINEAR EQUATIONS IN FINITE FIELDS. Glasgow Mathematical Journal, 2008, 50, 523-529.	0.3	25
44	On the value set of Fermat quotients. Proceedings of the American Mathematical Society, 2012, 140, 1199-1206.	0.8	25
45	On congruences with products of variables from short intervals and applications. Proceedings of the Steklov Institute of Mathematics, 2013, 280, 61-90.	0.3	25
46	Some doubly exponential sums over Z_m. Acta Arithmetica, 2002, 105, 349-370.	0.4	25
47	On the linear complexity profile of the power generator. IEEE Transactions on Information Theory, 2000, 46, 2159-2162.	2.4	24
48	Character sums over integers with restricted g-ary digits. Illinois Journal of Mathematics, 2002, 46, 819.	0.1	24
49	Number Theoretic Methods in Cryptography. , 1999, , .		24
50	Exponential sums and the distribution of inversive congruential pseudorandom numbers with prime-power modulus. Acta Arithmetica, 2000, 92, 89-98.	0.4	24
51	Prime numbers with Beatty sequences. Colloquium Mathematicum, 2009, 115, 147-157.	0.3	24
52	On the Linear Complexity of the Naorâ€“Reingold Pseudo-random Function from Elliptic Curves. Designs, Codes, and Cryptography, 2001, 24, 279-289.	1.6	23
53	Exponential sums over Mersenne numbers. Compositio Mathematica, 2004, 140, 15-30.	0.8	23
54	MULTIPLICATIVE ORDER OF GAUSS PERIODS. International Journal of Number Theory, 2010, 06, 877-882.	0.5	23

#	Article	IF	Citations
55	Cancellations amongst Kloosterman sums. Acta Arithmetica, 2016, 176, 201-210.	0.4	23
56	On the Distribution of Nonlinear Recursive Congruential Pseudorandom Numbers of Higher Orders. Lecture Notes in Computer Science, 1999, , 87-93.	1.3	22
57	CHARACTER SUMS WITH FERMAT QUOTIENTS. Quarterly Journal of Mathematics, 2011, 62, 1031-1043.	0.8	22
58	BOUNDS OF MULTIPLICATIVE CHARACTER SUMS WITH FERMAT QUOTIENTS OF PRIMES. Bulletin of the Australian Mathematical Society, 2011, 83, 456-462.	0.5	22
59	Fermat quotients: exponential sums, value set and primitive roots. Bulletin of the London Mathematical Society, 2011, 43, 1228-1238.	0.8	22
60	Orders of Gauss Periods in Finite Fields. Applicable Algebra in Engineering, Communications and Computing, 1998, 9, 15-24.	0.5	21
61	Character sums and congruences with $n!$. Transactions of the American Mathematical Society, 2004, 356, 5089-5102.	0.9	21
62	Classical and quantum function reconstruction via character evaluation. Journal of Complexity, 2004, 20, 404-422.	1.3	21
63	On the distribution of rational functions along a curve over <mml:math altimg="si1.gif" overflow="scroll" xmlns:xocs="http://www.elsevier.com/xml/xocs/dtd" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://www.elsevier.com/xml/ja/dtd" xmlns:ja="http://www.elsevier.com/xml/ja/dtd" xmlns:mml="http://www.w3.org/1998/Math/MathML" xmlns:tb="http://www.elsevier.com/xml/common/table/dtd" xmlns:sb="http://www.elsevier.com/xml/co	0.4	21
64	On the Distribution of the RSA Generator. , 1999, , 205-212.		21
65	Security of the most significant bits of the Shamir message passing scheme. Mathematics of Computation, 2001, 71, 333-343.	2.1	20
66	On Decimations of ell-Sequences. SIAM Journal on Discrete Mathematics, 2004, 18, 130-140.	0.8	20
67	Additive Decompositions of Subgroups of Finite Fields. SIAM Journal on Discrete Mathematics, 2013, 27, 1870-1879.	0.8	20
68	Piatetski-Shapiro sequences. Acta Arithmetica, 2013, 157, 37-68.	0.4	20
69	Noisy Chinese remaindering in the Lee norm. Journal of Complexity, 2004, 20, 423-437.	1.3	19
70	On the lower bound of the linear complexity over F/sub p/ of Sidelnikov sequences. IEEE Transactions on Information Theory, 2006, 52, 3299-3304.	2.4	19
71	On Group Structures Realized by Elliptic Curves over Arbitrary Finite Fields. Experimental Mathematics, 2012, 21, 11-25.	0.7	19
72	On sums of Kloosterman and Gauss sums. Transactions of the American Mathematical Society, 2019, 371, 8679-8697.	0.9	19

#	Article	IF	Citations
73	Predicting the Inversive Generator. Lecture Notes in Computer Science, 2003, , 264-275.	1.3	19
74	On the maximal difference between an element and its inverse in residue rings. Proceedings of the American Mathematical Society, 2005, 133, 3463-3468.	0.8	19
75	On the Distribution of Diffie–Hellman Triples with Sparse Exponents. SIAM Journal on Discrete Mathematics, 2001, 14, 162-169.	0.8	18
76	On the degree growth in some polynomial dynamical systems and nonlinear pseudorandom number generators. Mathematics of Computation, 2010, 79, 501-501.	2.1	18
77	Prescribing the binary digits of squarefree numbers and quadratic residues. Transactions of the American Mathematical Society, 2017, 369, 8369-8388.	0.9	18
78	On a sum involving the Euler function. Journal of Number Theory, 2019, 202, 278-297.	0.4	18
79	Short character sums with Beatty sequences. Mathematical Research Letters, 2006, 13, 539-547.	0.5	18
80	Double Character Sums over Elliptic Curves and Finite Fields. Pure and Applied Mathematics Quarterly, 2006, 2, 179-197.	0.4	18
81	On some approximation problems concerning sparse polynomials over finite fields. Theoretical Computer Science, 1996, 157, 259-266.	0.9	17
82	Sparse polynomial approximation in finite fields. , 2001, , .		17
83	Non-residues and primitive roots in Beatty sequences. Bulletin of the Australian Mathematical Society, 2006, 73, 433-443.	0.5	17
84	Reconstructing noisy polynomial evaluation in residue rings. Journal of Algorithms, 2006, 61, 47-59.	0.9	17
85	Elliptic Curves with Low Embedding Degree. Journal of Cryptology, 2006, 19, 553-562.	2.8	17
86	ON THE NUMBER OF SIGN CHANGES OF HECKE EIGENVALUES OF NEWFORMS. Journal of the Australian Mathematical Society, 2008, 85, 87-94.	0.4	17
87	On numbers n dividing the nth term of a linear recurrence. Proceedings of the Edinburgh Mathematical Society, 2012, 55, 271-289.	0.3	17
88	Points on curves in small boxes and applications. Michigan Mathematical Journal, 2014, 63, .	0.4	17
89	Products of Small Integers in Residue Classes and Additive Properties of Fermat Quotients. International Mathematics Research Notices, 2016, 2016, 1424-1446.	1.0	17
90	Divisor problem in arithmetic progressions modulo a prime power. Advances in Mathematics, 2018, 325, 459-481.	1.1	17

#	Article	IF	Citations
91	On the Insecurity of a Server-Aided RSA Protocol. Lecture Notes in Computer Science, 2001, , 21-35.	1.3	17
92	Distribution of modular inverses and multiples of small integers and the Sato-Tate conjecture on average. Michigan Mathematical Journal, 2008, 56, .	0.4	17
93	Polynomial representations of the Diffie-Hellman mapping. Bulletin of the Australian Mathematical Society, 2001, 63, 467-473.	0.5	16
94	On the maximal difference between an element and its inverse modulo n. Periodica Mathematica Hungarica, 2003, 47, 111-117.	0.9	16
95	On the distribution of points on multidimensional modular hyperbolas. Proceedings of the Japan Academy Series A: Mathematical Sciences, 2007, 83, .	0.4	16
96	Arithmetic properties of numbers with restricted digits. Acta Arithmetica, 2004, 112, 313-332.	0.4	16
97	On Exponential Sums with Sparse Polynomials and Rational Functions. Journal of Number Theory, 1996, 60, 233-244.	0.4	15
98	On the spectral ÃđÃ¡m property for circulant graphs. Discrete Mathematics, 2002, 254, 309-329.	0.7	15
99	On values taken by the largest prime factor of shifted primes. Journal of the Australian Mathematical Society, 2007, 82, 133-147.	0.4	15
100	Density of non-residues in Burgess-type intervals and applications. Bulletin of the London Mathematical Society, 2008, 40, 88-96.	0.8	15
101	Corrigenda to: Product Sets of Rationals, Multiplicative Translates of Subgroups in Residue Rings and Fixed Points of the Discrete Logarithm. International Mathematics Research Notices, 2009, 2009, 3146-3147.	1.0	15
102	On the length of critical orbits of stable quadratic polynomials. Proceedings of the American Mathematical Society, 2010, 138, 2653-2653.	0.8	15
103	Functional graphs of polynomials over finite fields. Journal of Combinatorial Theory Series B, 2016, 116, 87-122.	1.0	15
104	MOV attack in various subgroups on elliptic curves. Illinois Journal of Mathematics, 2004, 48, .	0.1	15
105	On some dynamical systems in finite fields and residue rings. Discrete and Continuous Dynamical Systems, 2007, 17, 901-917.	0.9	15
106	Linear Complexity of the Discrete Logarithm. Designs, Codes, and Cryptography, 2003, 28, 135-146.	1.6	14
107	Title is missing!. International Mathematics Research Notices, 2005, 2005, 1.	1.0	14
108	Title is missing!. International Mathematics Research Notices, 2005, 2005, 1391.	1.0	14

#	Article	IF	Citations
109	On a generalisation of a Lehmer problem. Mathematische Zeitschrift, 2009, 263, 619-631.	0.9	14
110	Pseudorandom numbers and hash functions from iterations of multivariate polynomials. Cryptography and Communications, 2010, 2, 49-67.	1.4	14
111	ON THE CONSECUTIVE POWERS OF A PRIMITIVE ROOT: GAPS AND EXPONENTIAL SUMS. Mathematika, 2012, 58, 11-20.	0.5	14
112	The Insecurity of Nyberg-Rueppel and Other DSA-Like Signature Schemes with Partially Known Nonces. Lecture Notes in Computer Science, 2001, , 97-109.	1.3	14
113	Hidden Number Problem with the Trace and Bit Security of XTR and LUC. Lecture Notes in Computer Science, 2002, , 433-448.	1.3	14
114	On the Uniformity of Distribution of Congruential Generators over Elliptic Curves. , 2002, , 257-264.		14
115	Character sums and deterministic polynomial root finding in finite fields. Mathematics of Computation, 2015, 84, 2969-2977.	2.1	14
116	On the concentration of points on modular hyperbolas and exponential curves. Acta Arithmetica, 2010, 142, 59-66.	0.4	14
117	Collisions in Fast Generation of Ideal Classes and Points on Hyperelliptic and Elliptic Curves. Applicable Algebra in Engineering, Communications and Computing, 2005, 15, 329-337.	0.5	13
118	Constructions of Approximately Mutually Unbiased Bases. Lecture Notes in Computer Science, 2006, , 793-799.	1.3	13
119	On the set of distances between two sets over finite fields. International Journal of Mathematics and Mathematical Sciences, 2006, 2006, 1-5.	0.7	13
120	Distribution of matrices with restricted entries over finite fields. Indagationes Mathematicae, 2007, 18, 327-337.	0.4	13
121	On hashing into elliptic curves. Journal of Mathematical Cryptology, 2009, 3, .	0.7	13
122	On the modular inversion hidden number problem. Journal of Symbolic Computation, 2012, 47, 358-367.	0.8	13
123	On the number of solutions of exponential congruences. Acta Arithmetica, 2011, 148, 93-103.	0.4	13
124	Products in Residue Classes. Mathematical Research Letters, 2008, 15, 1133-1147.	0.5	13
125	Counting curves and their projections. , 1993, , .		12
126	The average sensitivity of square-freeness. Computational Complexity, 2000, 9, 39-51.	0.3	12

#	Article	IF	Citations
127	On the Uniformity of Distribution of the Naorâ€“Reingold Pseudo-Random Function. Finite Fields and Their Applications, 2001, 7, 318-326.	1.0	12
128	Hidden number problem with hidden multipliers, timed-release crypto, and noisy exponentiation. Mathematics of Computation, 2003, 72, 1473-1486.	2.1	12
129	On RSA Moduli with Prescribed Bit Patterns. Designs, Codes, and Cryptography, 2006, 39, 113-122.	1.6	12
130	On RSA moduli with almost half of the bits prescribed. Discrete Applied Mathematics, 2008, 156, 3150-3154.	0.9	12
131	On the number of distinct elliptic curves in some families. Designs, Codes, and Cryptography, 2010, 54, 83-99.	1.6	12
132	On pseudorandom numbers from multivariate polynomial systems. Finite Fields and Their Applications, 2010, 16, 320-328.	1.0	12
133	Multiplicative congruences with variables from short intervals. Journal D'Analyse Mathematique, 2014, 124, 117-147.	0.8	12
134	Classical and Quantum Algorithms for Exponential Congruences. Lecture Notes in Computer Science, 2008, , 1-10.	1.3	12
135	Isomorphism classes of elliptic curves over a finite field in some thin families. Mathematical Research Letters, 2012, 19, 335-343.	0.5	12
136	On the number of zeros of exponential polynomials and related questions. Bulletin of the Australian Mathematical Society, 1992, 46, 401-412.	0.5	11
137	Finding irreducible and primitive polynomials. Applicable Algebra in Engineering, Communications and Computing, 1993, 4, 263-268.	0.5	11
138	A Lower Bound for Primality. Journal of Computer and System Sciences, 2001, 62, 356-366.	1.2	11
139	Circuit and Decision Tree Complexity of Some Number Theoretic Problems. Information and Computation, 2001, 168, 113-124.	0.7	11
140	On a question of ErdÃ¶s and Graham. Archiv Der Mathematik, 2002, 78, 445-448.	0.5	11
141	ON THE DISTRIBUTION OF POWER RESIDUES AND PRIMITIVE ELEMENTS IN SOME NONLINEAR RECURRING SEQUENCES. Bulletin of the London Mathematical Society, 2003, 35, 522-528.	0.8	11
142	Catalan and ApÃ©ry numbers in residue classes. Journal of Combinatorial Theory - Series A, 2006, 113, 851-865.	0.8	11
143	Bilinear character sums over elliptic curves. Finite Fields and Their Applications, 2008, 14, 132-141.	1.0	11
144	Approximate polynomial <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si1.gif" display="inline" overflow="scroll"><mml:mstyle mathvariant="normal"><mml:mi>gcd</mml:mi></mml:mstyle></mml:math>: Small degree and small height perturbations. Journal of Symbolic Computation, 2010, 45, 879-886.	0.8	11

#	Article	IF	Citations
145	ON STABLE QUADRATIC POLYNOMIALS. Glasgow Mathematical Journal, 2012, 54, 359-369.	0.3	11
146	Interpolation and Approximation of Polynomials in Finite Fields over a Short Interval from Noisy Values. Experimental Mathematics, 2014, 23, 241-260.	0.7	11
147	Reductions modulo primes of systems of polynomial equations and algebraic dynamical systems. Transactions of the American Mathematical Society, 2019, 371, 1169-1198.	0.9	11
148	Non-linear Complexity of the Naorâ€“Reingold Pseudo-random Function. Lecture Notes in Computer Science, 2000, , 53-59.	1.3	11
149	On the Generalised Hidden Number Problem and Bit Security of XTR. Lecture Notes in Computer Science, 2001, , 268-277.	1.3	11
150	Computational Diffie-Hellman Problem. , 2011, , 240-244.		11
151	Double exponential sums over thin sets. Proceedings of the American Mathematical Society, 2000, 129, 1617-1621.	0.8	11
152	Arithmetic functions on Beatty sequences. Acta Arithmetica, 2009, 136, 81-89.	0.4	11
153	Primitive Points on a Modular Hyperbola. Bulletin of the Polish Academy of Sciences Mathematics, 2006, 54, 193-200.	0.3	11
154	On the construction of solutions of systems of linear ordinary differential equations in the neighbourhood of a regular singularity. Journal of Computational and Applied Mathematics, 1992, 39, 151-163.	2.0	10
155	Bounds of Gauss sums in finite fields. Proceedings of the American Mathematical Society, 2004, 132, 2817-2824.	0.8	10
156	A hidden number problem in small subgroups. Mathematics of Computation, 2005, 74, 2073-2081.	2.1	10
157	Prime divisors of palindromes. Periodica Mathematica Hungarica, 2005, 51, 1-10.	0.9	10
158	Distributional properties of the largest prime factor. Michigan Mathematical Journal, 2005, 53, 665.	0.4	10
159	Exponential sums and congruences with factorials. Journal Fur Die Reine Und Angewandte Mathematik, 2005, 2005, 29-44.	0.9	10
160	Exponential sums with Dickson polynomials. Finite Fields and Their Applications, 2006, 12, 16-25.	1.0	10
161	Prime divisors in Beatty sequences. Journal of Number Theory, 2007, 123, 413-425.	0.4	10
162	Bounds of incomplete multiple Kloosterman sums. Journal of Number Theory, 2007, 126, 68-73.	0.4	10

#	Article	IF	Citations
163	Pseudoprime reductions of elliptic curves. Mathematical Proceedings of the Cambridge Philosophical Society, 2009, 146, 513.	0.4	10
164	Sets with integral distances in finite fields. Transactions of the American Mathematical Society, 2010, 362, 2189-2204.	0.9	10
165	EXPANSION OF ORBITS OF SOME DYNAMICAL SYSTEMS OVER FINITE FIELDS. Bulletin of the Australian Mathematical Society, 2010, 82, 232-239.	0.5	10
166	Product Sets of Rationals, Multiplicative Translates of Subgroups in Residue Rings, and Fixed Points of the Discrete Logarithm. International Mathematics Research Notices, 2010, , .	1.0	10
167	On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average. LMS Journal of Computation and Mathematics, 2015, 18, 308-322.	0.9	10
168	On the smallest pseudopower. Acta Arithmetica, 2009, 140, 43-55.	0.4	10
169	On the distribution of the number of points on algebraic curves in extensions of finite fields. Mathematical Research Letters, 2010, 17, 689-699.	0.5	10
170	Noisy interpolation of sparse polynomials in finite fields. Applicable Algebra in Engineering, Communications and Computing, 2005, 16, 307-317.	0.5	9
171	Values of the Euler Function in Various Sequences. Monatshefte Fur Mathematik, 2005, 146, 1-19.	0.9	9
172	Arithmetic properties of the Ramanujan function. Proceedings of the Indian Academy of Sciences - Section A, 2006, 116, 1-8.	0.2	9
173	Discriminants of Complex Multiplication Fields of Elliptic Curves over Finite Fields. Canadian Mathematical Bulletin, 2007, 50, 409-417.	0.5	9
174	Visible points on multidimensional modular hyperbolas. Journal of Number Theory, 2008, 128, 2695-2703.	0.4	9
175	ON THE LARGEST PRIME FACTOR OF THE MERSENNE NUMBERS. Bulletin of the Australian Mathematical Society, 2009, 79, 455-463.	0.5	9
176	Some additive combinatorics problems in matrix rings. Revista Matematica Complutense, 2010, 23, 501-513.	1.2	9
177	Concentration of points on curves in finite fields. Monatshefte Fur Mathematik, 2013, 171, 315-327.	0.9	9
178	CANCELLATIONS BETWEEN KLOOSTERMAN SUMS MODULO A PRIME POWER WITH PRIME ARGUMENTS. Mathematika, 2019, 65, 475-487.	0.5	9
179	Bilinear forms in Weyl sums for modular square roots and applications. Advances in Mathematics, 2020, 375, 107369.	1.1	9
180	Sums of algebraic trace functions twisted by arithmetic functions. Pacific Journal of Mathematics, 2020, 304, 505-522.	0.5	9

#	Article	IF	Citations
181	Smooth Orders and Cryptographic Applications. Lecture Notes in Computer Science, 2002, , 338-348.	1.3	9
182	Circuit Complexity of Testing Square-Free Numbers. Lecture Notes in Computer Science, 1999, , 47-56.	1.3	9
183	Secure Bilinear Diffie-Hellman Bits. Lecture Notes in Computer Science, 2004, , 370-378.	1.3	9
184	On the number of isogeny classes of pairing-friendly elliptic curves and statistics of MNT curves. Mathematics of Computation, 2011, 81, 1093-1110.	2.1	9
185	Average multiplicative orders of elements modulo n. Acta Arithmetica, 2003, 109, 387-411.	0.4	9
186	Squares in Piatetski-Shapiro sequences. Acta Arithmetica, 2017, 181, 239-252.	0.4	9
187	Visible Points on Curves over Finite Fields. Bulletin of the Polish Academy of Sciences Mathematics, 2007, 55, 193-199.	0.3	9
188	On linear recurrence sequences with polynomial coefficients. Glasgow Mathematical Journal, 1996, 38, 147-155.	0.3	8
189	On The Correlation Of Binary M-sequences. Designs, Codes, and Cryptography, 1999, 16, 249-256.	1.6	8
190	Linear complexity of the Naorâ€“Reingold pseudo-random function. Information Processing Letters, 2000, 76, 95-99.	0.6	8
191	On the Multiplicative Orders of Î³ and Î³+Î³â˜1 over finite fields. Finite Fields and Their Applications, 2001, 7, 327-331.	1.0	8
192	Prime divisors of sparse integers. Periodica Mathematica Hungarica, 2003, 46, 215-222.	0.9	8
193	New Results on the Hardness of Diffie-HellmanÂBits. Lecture Notes in Computer Science, 2004, , 159-172.	1.3	8
194	On the value set of the Ramanujan function. Archiv Der Mathematik, 2005, 85, 508-513.	0.5	8
195	On Sternâ€™s Attack Against Secret Truncated Linear Congruential Generators. Lecture Notes in Computer Science, 2005, , 52-60.	1.3	8
196	Distribution of Nonlinear Congruential Pseudorandom Numbers Modulo Almost Squarefree Integers. Monatshefte Fur Mathematik, 2006, 148, 297-307.	0.9	8
197	On the number of distances between the coordinates of points on modular hyperbolas. Journal of Number Theory, 2008, 128, 1224-1230.	0.4	8
198	Uniform Distribution of Fractional Parts Related to Pseudoprimes. Canadian Journal of Mathematics, 2009, 61, 481-502.	0.6	8

#	Article	IF	Citations
199	On the Values of Kloosterman Sums. IEEE Transactions on Information Theory, 2009, 55, 2599-2601.	2.4	8
200	On the number of Eisenstein polynomials of bounded height. Applicable Algebra in Engineering, Communications and Computing, 2013, 24, 149-156.	0.5	8
201	New Bounds of Weyl Sums. International Mathematics Research Notices, 2019, , .	1.0	8
202	On large values of Weyl sums. Advances in Mathematics, 2020, 370, 107216.	1.1	8
203	GauÃŸ Periods in Finite Fields. , 2001, , 162-177.		8
204	Distribution of Farey fractions in residue classes and Langâ€“Trotter conjectures on average. Proceedings of the American Mathematical Society, 2008, 136, 1977-1986.	0.8	8
205	On the generalized joint linear complexity profile of a class of nonlinear pseudorandom multisequences. Advances in Mathematics of Communications, 2010, 4, 369-379.	0.7	8
206	Average order in cyclic groups. Journal De Theorie Des Nombres De Bordeaux, 2004, 16, 107-123.	0.1	8
207	Elements of large order on varieties over prime finite fields. Journal De Theorie Des Nombres De Bordeaux, 2014, 26, 579-593.	0.1	8
208	On the Distribution of the Diffieâ€“Hellman Pairs. Finite Fields and Their Applications, 2002, 8, 131-141.	1.0	7
209	On the Average Distribution of Inversive Pseudorandom Numbers. Finite Fields and Their Applications, 2002, 8, 491-503.	1.0	7
210	Security of most significant bits of gx2. Information Processing Letters, 2002, 83, 109-113.	0.6	7
211	On the linear complexity of bounded integer sequences over different moduli. Information Processing Letters, 2005, 96, 175-177.	0.6	7
212	Irrationality of Power Series for Various Number Theoretic Functions. Manuscripta Mathematica, 2005, 117, 183-197.	0.6	7
213	On the singularity of generalised Vandermonde matrices over finite fields. Finite Fields and Their Applications, 2005, 11, 193-199.	1.0	7
214	On quadratic fields generated by polynomials. Archiv Der Mathematik, 2008, 91, 399-408.	0.5	7
215	On the Convex Closure of the Graph of Modular Inversions. Experimental Mathematics, 2008, 17, 91-104.	0.7	7
216	Multiplicative character sums and products of sparse integers in residue classes. Periodica Mathematica Hungarica, 2012, 64, 247-255.	0.9	7

#	Article	IF	Citations
217	On the power generator and its multivariate analogue. Journal of Complexity, 2012, 28, 238-249.	1.3	7
218	ON GAPS BETWEEN PRIMITIVE ROOTS IN THE HAMMING METRIC. Quarterly Journal of Mathematics, 2013, 64, 1043-1055.	0.8	7
219	Distribution of values of polynomial Fermat quotients. Finite Fields and Their Applications, 2013, 19, 93-104.	1.0	7
220	On the Lang-Trotter and Sato-Tate conjectures on average for polynomial families of elliptic curves. Michigan Mathematical Journal, 2013, 62, .	0.4	7
221	On vanishing Fermat quotients and a bound of the Ihara sum. Kodai Mathematical Journal, 2013, 36, .	0.3	7
222	On irreducible divisors of iterated polynomials. Revista Matematica Iberoamericana, 2014, 30, 1123-1134.	0.9	7
223	Covering Sets for Limited-Magnitude Errors. IEEE Transactions on Information Theory, 2014, 60, 5315-5321.	2.4	7
224	Subgroups generated by rational functions in finite fields. Monatshefte Fur Mathematik, 2015, 176, 241-253.	0.9	7
225	On the additive energy of the distance set in finite fields. Finite Fields and Their Applications, 2016, 42, 187-199.	1.0	7
226	Bilinear forms with exponential sums with binomials. Journal of Number Theory, 2018, 188, 172-185.	0.4	7
227	Multiplicative Energy of Shifted Subgroups and Bounds On Exponential Sums with Trinomials in Finite Fields. Canadian Journal of Mathematics, 2018, 70, 1319-1338.	0.6	7
228	On the Average Sensitivity of Testing Square-Free Numbers. Lecture Notes in Computer Science, 1999, , 291-299.	1.3	7
229	Periodic Sequences with Maximal Linear Complexity and Almost Maximal k-Error Linear Complexity. Lecture Notes in Computer Science, 2003, , 183-189.	1.3	7
230	Values of linear recurring sequences of vectors over finite fields. Acta Arithmetica, 1993, 65, 221-226.	0.4	7
231	Coincidences in the values of the Euler and Carmichael functions. Acta Arithmetica, 2006, 122, 207-234.	0.4	7
232	Distribution of consecutive modular roots of an integer. Acta Arithmetica, 2008, 134, 83-91.	0.4	7
233	Pseudoprime Cullen and Woodall numbers. Colloquium Mathematicum, 2007, 107, 35-43.	0.3	7
234	On the fixed points of the map $x mapsto x^x$ modulo a prime. Mathematical Research Letters, 2015, 22, 141-168.	0.5	7

#	Article	IF	Citations
235	Square-free values of the Carmichael function. Journal of Number Theory, 2003, 103, 122-131.	0.4	6
236	Finding Points on Curves over Finite Fields. SIAM Journal on Computing, 2003, 32, 1436-1448.	1.0	6
237	PRIME DIVISORS OF SHIFTED FACTORIALS. Bulletin of the London Mathematical Society, 2005, 37, 809-817.	0.8	6
238	Values of arithmetical functions equal to a sum of two squares. Quarterly Journal of Mathematics, 2005, 56, 123-139.	0.8	6
239	Incomplete exponential sums and Diffieâ€“Hellman triples. Mathematical Proceedings of the Cambridge Philosophical Society, 2006, 140, 193.	0.4	6
240	Congruences and Rational Exponential Sums with the Euler Function. Rocky Mountain Journal of Mathematics, 2006, 36, 1415.	0.4	6
241	Least totient in a residue class. Bulletin of the London Mathematical Society, 2008, 40, 532-532.	0.8	6
242	MULTIPLICATIVE CHARACTER SUMS WITH TWICE-DIFFERENTIABLE FUNCTIONS. Quarterly Journal of Mathematics, 2009, 60, 401-411.	0.8	6
243	Short cycles in repeated exponentiation modulo a prime. Designs, Codes, and Cryptography, 2010, 56, 35-42.	1.6	6
244	Character sums over shifted primes. Mathematical Notes, 2010, 88, 585-598.	0.4	6
245	Bilinear character sums and sum-product problems on elliptic curves. Proceedings of the Edinburgh Mathematical Society, 2010, 53, 1-12.	0.3	6
246	Distribution of Elements of Cosets of Small Subgroups and Applications. International Mathematics Research Notices, 2011, , .	1.0	6
247	Sum-Products Estimates with Several Sets and Applications. Integers, 2012, 12, .	0.3	6
248	Algebraic entropy, automorphisms and sparsity of algebraic dynamical systems and pseudorandom number generators. Mathematics of Computation, 2014, 83, 1535-1550.	2.1	6
249	Cyclotomic coefficients: gaps and jumps. Journal of Number Theory, 2016, 163, 211-237.	0.4	6
250	Almost primes of the form <mml:math xmlns:mml="http://www.w3.org/1998/Math/MathML" altimg="si8.gif" display="inline" overflow="scroll"><mml:mrow><mml:mo>âŒŠ</mml:mo><mml:msup><mml:mrow><mml:mi>p</mml:mi></mml:mrow><mml:mrow><mml:mi> Indagationes Mathematicae, 2016, 27, 423-436.	0.4	6
251	Bilinear sums of Kloosterman sums, multiplicative congruences and average values of the divisor function over families of arithmetic progressions. Research in Number Theory, 2020, 6, 1.	0.4	6
252	On the ÃdÃ¡m Conjecture on Circulant Graphs. Lecture Notes in Computer Science, 1998, , 251-260.	1.3	6

#	Article	IF	Citations
253	A Refinement of the Burgess Bound for Character Sums. Michigan Mathematical Journal, 2020, 69, .	0.4	6
254	Exponential Sums with Farey Fractions. Bulletin of the Polish Academy of Sciences Mathematics, 2009, 57, 101-107.	0.3	6
255	Computing components and projections of curves over finite fields. SIAM Journal on Computing, 1998, 28, 822-840.	1.0	5
256	Distribution of inverses in polynomial rings. Indagationes Mathematicae, 2001, 12, 303-315.	0.4	5
257	On Some Properties of the Shrinking Generator. Designs, Codes, and Cryptography, 2001, 23, 147-156.	1.6	5
258	Security of polynomial transformations of the Diffieâ€“Hellman key. Finite Fields and Their Applications, 2004, 10, 123-131.	1.0	5
259	PRIME DIVISORS OF SEQUENCES ASSOCIATED TO ELLIPTIC CURVES. Glasgow Mathematical Journal, 2005, 47, 115-122.	0.3	5
260	On some generalisations of the ErdÅ‘s distance problem over finite fields. Bulletin of the Australian Mathematical Society, 2006, 73, 285-292.	0.5	5
261	Character sums and nonlinear recurrence sequences. Discrete Mathematics, 2006, 306, 1126-1131.	0.7	5
262	On the nonlinearity of linear recurrence sequences. Applied Mathematics Letters, 2006, 19, 340-344.	2.7	5
263	Character sums with exponential functions over smooth numbers. Indagationes Mathematicae, 2006, 17, 157-168.	0.4	5
264	Pseudoprime values of the Fibonacci sequence, polynomials and the Euler function. Indagationes Mathematicae, 2006, 17, 611-625.	0.4	5
265	Least totient in a residue class. Bulletin of the London Mathematical Society, 2007, 39, 425-432.	0.8	5
266	Exponential sums with Catalan numbers and middle binomial coefficients. Indagationes Mathematicae, 2007, 18, 23-37.	0.4	5
267	Bounds on the Fourier coefficients of the weighted sum function. Information Processing Letters, 2007, 103, 83-87.	0.6	5
268	On the elliptic curve analogue of the sum-product problem. Finite Fields and Their Applications, 2008, 14, 721-726.	1.0	5
269	ON CURVES OVER FINITE FIELDS WITH JACOBIANS OF SMALL EXPONENT. International Journal of Number Theory, 2008, 04, 819-826.	0.5	5
270	ON SOME WEIGHTED AVERAGE VALUES OF L-FUNCTIONS. Bulletin of the Australian Mathematical Society, 2009, 79, 183-186.	0.5	5

#	Article	IF	Citations
271	TATE-SHAFAREVICH GROUPS AND FROBENIUS FIELDS OF REDUCTIONS OF ELLIPTIC CURVES. Quarterly Journal of Mathematics, 2010, 61, 255-263.	0.8	5
272	ON POINT SETS IN VECTOR SPACES OVER FINITE FIELDS THAT DETERMINE ONLY ACUTE ANGLE TRIANGLES. Bulletin of the Australian Mathematical Society, 2010, 81, 114-120.	0.5	5
273	On the average distribution of pseudorandom numbers generated by nonlinear permutations. Mathematics of Computation, 2011, 80, 1053-1053.	2.1	5
274	On the Waring problem with Dickson polynomials in finite fields. Proceedings of the American Mathematical Society, 2011, 139, 3815-3820.	0.8	5
275	EXPONENTIAL SUMS WITH CONSECUTIVE MODULAR ROOTS OF AN INTEGER. Quarterly Journal of Mathematics, 2011, 62, 207-213.	0.8	5
276	EXPONENTIAL AND CHARACTER SUMS WITH MERSENNE NUMBERS. Journal of the Australian Mathematical Society, 2012, 92, 1-13.	0.4	5
277	On gaps between quadratic non-residues in the Euclidean and Hamming metrics. Indagationes Mathematicae, 2013, 24, 930-938.	0.4	5
278	Double Character Sums over Subgroups andÂIntervals. Bulletin of the Australian Mathematical Society, 2014, 90, 376-390.	0.5	5
279	On the Distribution of Atkin and Elkies Primes. Foundations of Computational Mathematics, 2014, 14, 285-297.	2.5	5
280	POLYNOMIAL VALUES IN SUBFIELDS AND AFFINE SUBSPACES OF FINITE FIELDS. Quarterly Journal of Mathematics, 2015, 66, 693-706.	0.8	5
281	Quadratic non-residues in short intervals. Proceedings of the American Mathematical Society, 2015, 143, 4261-4269.	0.8	5
282	UPPER AND LOWER BOUNDS FOR HIGHER MOMENTS OF THETA FUNCTIONS. Quarterly Journal of Mathematics, 2016, 67, 53-73.	0.8	5
283	Orbits of polynomial dynamical systems modulo primes. Proceedings of the American Mathematical Society, 2018, 146, 2015-2025.	0.8	5
284	On short products of primes in arithmetic progressions. Proceedings of the American Mathematical Society, 2018, 147, 977-986.	0.8	5
285	Elliptic curves in isogeny classes. Journal of Number Theory, 2018, 191, 194-212.	0.4	5
286	On multiplicatively dependent vectors of algebraic numbers. Transactions of the American Mathematical Society, 2018, 370, 6221-6244.	0.9	5
287	On Multiplicative Dependence of Values of Rational Functions and a Generalization of the Northcott Theorem. Michigan Mathematical Journal, 2019, 68, .	0.4	5
288	On Functional Graphs of Quadratic Polynomials. Experimental Mathematics, 2019, 28, 292-300.	0.7	5

#	Article	IF	Citations
289	Hausdorff dimension of the large values of Weyl sums. Journal of Number Theory, 2020, 214, 27-37.	0.4	5
290	Orbits of Algebraic Dynamical Systems in Subgroups and Subfields. , 2017, , 347-368.		5
291	A Nonuniform Algorithm for the Hidden Number Problem in Subgroups. Lecture Notes in Computer Science, 2004, , 416-424.	1.3	5
292	Exponential Sums and Lattice Reduction: Applications to Cryptography. , 2002, , 286-298.		5
293	On the restricted divisor function in arithmetic progressions. Revista Matematica Iberoamericana, 2012, 28, 231-238.	0.9	5
294	Rank Statistics for a Family of Elliptic Curves over a Function Field. Pure and Applied Mathematics Quarterly, 2010, 6, 21-40.	0.4	5
295	An Identification Scheme Based on Sparse Polynomials. Lecture Notes in Computer Science, 2000, , 68-74.	1.3	5
296	Metric theory of Weyl sums. Mathematische Annalen, 2023, 385, 309-355.	1.4	5
297	Computing Jacobi Symbols modulo Sparse Integers and Polynomials and Some Applications. Journal of Algorithms, 2000, 36, 241-252.	0.9	4
298	On the uniformity of distribution of the RSA pairs. Mathematics of Computation, 2000, 70, 801-809.	2.1	4
299	On the Number of Sparse RSA Exponents. Journal of Number Theory, 2002, 95, 340-350.	0.4	4
300	Finding the group structure of elliptic curves over finite fields. Bulletin of the Australian Mathematical Society, 2005, 72, 251-263.	0.5	4
301	Complexity of inverting the Euler function. Mathematics of Computation, 2006, 75, 983-997.	2.1	4
302	Arithmetic functions with linear recurrence sequences. Journal of Number Theory, 2007, 125, 459-472.	0.4	4
303	Exponential sums and prime divisors of sparse integers. Periodica Mathematica Hungarica, 2008, 57, 93-99.	0.9	4
304	On the values of the divisor function. Monatshefte Fur Mathematik, 2008, 154, 59-69.	0.9	4
305	Geometric properties of points on modular hyperbolas. Proceedings of the American Mathematical Society, 2010, 138, 4177-4185.	0.8	4
306	On the g-Ary Expansions of ApÃ©ry, Motzkin, SchrÃ¶der and Other Combinatorial Numbers. Annals of Combinatorics, 2010, 14, 507-524.	0.6	4

#	Article	IF	Citations
307	Sums with convolutions of Dirichlet characters. Manuscripta Mathematica, 2010, 133, 105-114.	0.6	4
308	On squares in polynomial products. Monatshefte Fur Mathematik, 2010, 159, 215-223.	0.9	4
309	On the Distribution of Pseudopowers. Canadian Journal of Mathematics, 2010, 62, 582-594.	0.6	4
310	On the asymptotic effectiveness of Weil descent attacks. Journal of Mathematical Cryptology, 2010, 4, .	0.7	4
311	On the g-ary expansions of middle binomial coefficients and Catalan numbers. Rocky Mountain Journal of Mathematics, 2011, 41, .	0.4	4
312	MULTIPLICATIVE CHARACTER SUMS OF A CLASS OF NONLINEAR RECURRENCE VECTOR SEQUENCES. International Journal of Number Theory, 2011, 07, 1557-1571.	0.5	4
313	On Group Structures Realized by Elliptic Curves over a Fixed Finite Field. Experimental Mathematics, 2012, 21, 1-10.	0.7	4
314	On the distribution of solutions to polynomial congruences. Archiv Der Mathematik, 2012, 99, 345-351.	0.5	4
315	On products of primes and almost primes in arithmetic progressions. Periodica Mathematica Hungarica, 2013, 67, 55-61.	0.9	4
316	Generating safe primes. Journal of Mathematical Cryptology, 2013, 7, .	0.7	4
317	On shifted Eisenstein polynomials. Periodica Mathematica Hungarica, 2014, 69, 170-181.	0.9	4
318	Products with variables from low-dimensional affine spaces and shifted power identity testing in finite fields. Journal of Symbolic Computation, 2014, 64, 35-41.	0.8	4
319	On the Multidimensional Distribution of the Naorâ€“Reingold Pseudo-Random Function. Mathematics of Computation, 2014, 83, 2429-2434.	2.1	4
320	Congruences with intervals and subgroups modulo a prime. Michigan Mathematical Journal, 2015, 64, .	0.4	4
321	Cayley Graphs Generated by Small Degree Polynomials over Finite Fields. SIAM Journal on Discrete Mathematics, 2015, 29, 376-381.	0.8	4
322	Polynomial values in small subgroups of finite fields. Revista Matematica Iberoamericana, 2016, 32, 1127-1136.	0.9	4
323	Bounds of double multiplicative character sums and gaps between residues of exponential functions. Journal of Number Theory, 2016, 167, 304-316.	0.4	4
324	Counting Co-Cyclic Lattices. SIAM Journal on Discrete Mathematics, 2016, 30, 1358-1370.	0.8	4

#	Article	IF	Citations
325	Double exponential sums with exponential functions. International Journal of Number Theory, 2017, 13, 2531-2543.	0.5	4
326	On abelian multiplicatively dependent points on a curve in a torus. Quarterly Journal of Mathematics, 2018, 69, 391-401.	0.8	4
327	MULTIPLICATIVE ORDERS IN ORBITS OF POLYNOMIALS OVER FINITE FIELDS. Glasgow Mathematical Journal, 2018, 60, 487-493.	0.3	4
328	The Satoâ€“Tate distribution in thin parametric families of elliptic curves. Mathematische Zeitschrift, 2018, 290, 831-855.	0.9	4
329	Bounds of Trilinear and Quadrilinear Exponential Sums. Journal D'Analyse Mathematique, 2019, 138, 613-641.	0.8	4
330	Bounds on short character sums and L-functions with characters to a powerful modulus. Journal D'Analyse Mathematique, 2019, 139, 239-263.	0.8	4
331	On the typical size and cancellations among the coefficients of some modular forms. Mathematical Proceedings of the Cambridge Philosophical Society, 2019, 166, 173-189.	0.4	4
332	Congruences with intervals and arbitrary sets. Archiv Der Mathematik, 2020, 114, 527-539.	0.5	4
333	SMOOTH SQUAREFREE AND SQUAREFULL INTEGERS IN ARITHMETIC PROGRESSIONS. Mathematika, 2020, 66, 56-70.	0.5	4
334	Level curves of rational functions and unimodular points on rational curves. Proceedings of the American Mathematical Society, 2020, 148, 1829-1833.	0.8	4
335	On the Structure of Graphs of Markoff Triples. Quarterly Journal of Mathematics, 2020, 71, 637-648.	0.8	4
336	Multiplicative Dependence Among Iterated Values of Rational Functions Modulo Finitely Generated Groups. International Mathematics Research Notices, 2021, 2021, 9045-9082.	1.0	4
337	Bilinear Forms With Modular Square Roots and Twisted Second Moments of Half Integral Weight Dirichlet Series. International Mathematics Research Notices, 2022, 2022, 17431-17474.	1.0	4
338	The Hidden Number Problem in Extension Fields and Its Applications. Lecture Notes in Computer Science, 2002, , 105-117.	1.3	4
339	Bisecting and Gossiping in Circulant Graphs. Lecture Notes in Computer Science, 2004, , 589-598.	1.3	4
340	On bivariate polynomial factorization over finite fields. Mathematics of Computation, 1993, 60, 787-787.	2.1	4
341	On the distribution of arguments of Gauss sums. Kodai Mathematical Journal, 2009, 32, .	0.3	4
342	Langâ€“Trotter and Satoâ€“Tate distributions in single and double parametric families of elliptic curves. Acta Arithmetica, 2015, 170, 299-325.	0.4	4

#	Article	IF	Citations
343	On a New Exponential Sum. Canadian Mathematical Bulletin, 2001, 44, 87-92.	0.5	4
344	Arithmetic properties of $Ï†(n)/Î»(n)$ and the structure of the multiplicative group modulo n. Commentarii Mathematici Helvetici, 2006, 81, 1-22.	0.7	4
345	Small exponent point groups on elliptic curves. Journal De Theorie Des Nombres De Bordeaux, 2006, 18, 471-476.	0.1	4
346	Cryptographic Applications of Sparse Polynomials over Finite Rings. Lecture Notes in Computer Science, 2001, , 206-220.	1.3	4
347	On the Computational Hardness of Testing Square-Freeness of Sparse Polynomials. Lecture Notes in Computer Science, 1999, , 492-497.	1.3	4
348	On the Linear Complexity of the Naor-Reingold Pseudo-Random Function. Lecture Notes in Computer Science, 1999, , 301-308.	1.3	3
349	Counting the values taken by algebraic exponential polynomials. Proceedings of the American Mathematical Society, 1999, 127, 665-675.	0.8	3
350	Average normalisations of elliptic curves. Bulletin of the Australian Mathematical Society, 2002, 66, 353-358.	0.5	3
351	Corrigendum to ``Period of the power generator and small values of Carmichael's function''. Mathematics of Computation, 2002, 71, 1803-1807.	2.1	3
352	On the hardness of approximating the permanent of structured matrices. Computational Complexity, 2002, 11, 158-170.	0.3	3
353	On the uniformity of distribution of the decryption exponent in fixed encryption exponent RSA. Information Processing Letters, 2004, 92, 143-147.	0.6	3
354	Distribution of exponential functions with squarefull exponent in residue rings. Indagationes Mathematicae, 2004, 15, 283-289.	0.4	3
355	Powerful numbers in short intervals. Bulletin of the Australian Mathematical Society, 2005, 71, 11-16.	0.5	3
356	Waring problem with factorials. Bulletin of the Australian Mathematical Society, 2005, 71, 259-264.	0.5	3
357	Uniform distribution of the fractional part of the average prime divisor. Forum Mathematicum, 2005, 17, .	0.7	3
358	GCD of Random Linear Combinations. Algorithmica, 2006, 46, 137-148.	1.3	3
359	On the bit security of the Diffie-Hellman key. Applicable Algebra in Engineering, Communications and Computing, 2006, 16, 397-404.	0.5	3
360	Statistical distribution and collisions of VSH. Journal of Mathematical Cryptology, 2007, 1, .	0.7	3

#	Article	IF	Citations
361	Geometric progressions in sumsets over finite fields. Monatshefte Fur Mathematik, 2007, 152, 177-185.	0.9	3
362	On quadratic fields generated by the Shanks sequence. Proceedings of the Edinburgh Mathematical Society, 2009, 52, 719-729.	0.3	3
363	On the embedding degree of reductions of an elliptic curve. Information Processing Letters, 2009, 109, 652-654.	0.6	3
364	On quadratic fields generated by discriminants of irreducible trinomials. Proceedings of the American Mathematical Society, 2010, 138, 125-132.	0.8	3
365	On the Distribution of Irreducible Trinomials. Canadian Mathematical Bulletin, 2011, 54, 748-756.	0.5	3
366	SUMâ€“PRODUCT ESTIMATES AND MULTIPLICATIVE ORDERS OF Î³ AND Î³+Î³âˆ’1 IN FINITE FIELDS. Bulletin of the Australian Mathematical Society, 2012, 85, 505-508.	0.5	3
367	Pseudorandom Bits From Points on Elliptic Curves. IEEE Transactions on Information Theory, 2012, 58, 1242-1247.	2.4	3
368	ON DIGIT PATTERNS IN EXPANSIONS OF RATIONAL NUMBERS WITH PRIME DENOMINATOR. Quarterly Journal of Mathematics, 2013, 64, 1231-1238.	0.8	3
369	Additive Combinatorics over Finite Fields: New Results and Applications. , 2013, , 233-272.		3
370	On the fractional parts of a ⁿ /n. Bulletin of the London Mathematical Society, 2013, 45, 249-256.	0.8	3
371	On the Counting Function of Elliptic Carmichael Numbers. Canadian Mathematical Bulletin, 2014, 57, 105-112.	0.5	3
372	ON THE DISTRIBUTION OF POINTS ON THE GENERALIZED MARKOFFâ€“HURWITZ AND DWORK HYPERSURFACES. International Journal of Number Theory, 2014, 10, 151-160.	0.5	3
373	Exponential sums over points of elliptic curves. Journal of Number Theory, 2014, 140, 299-313.	0.4	3
374	Distribution of polynomial discriminants modulo a prime. Archiv Der Mathematik, 2015, 105, 251-259.	0.5	3
375	Fractional parts of Dedekind sums. International Journal of Number Theory, 2016, 12, 1137-1147.	0.5	3
376	ON SOME MULTIPLE CHARACTER SUMS. Mathematika, 2017, 63, 553-560.	0.5	3
377	Power series approximations to Fekete polynomials. Journal of Approximation Theory, 2017, 222, 132-142.	0.8	3
378	Polynomial Interpolation and Identity Testing from High Powers Over Finite Fields. Algorithmica, 2018, 80, 560-575.	1.3	3

#	Article	IF	Citations
379	Linear equations with rational fractions of bounded height and stochastic matrices. Quarterly Journal of Mathematics, 2018, 69, 487-499.	0.8	3
380	Double sums of Kloosterman sums in finite fields. Finite Fields and Their Applications, 2019, 60, 101575.	1.0	3
381	Orders of points in families of elliptic curves. Proceedings of the American Mathematical Society, 2020, 148, 2371-2377.	0.8	3
382	New estimates for exponential sums over multiplicative subgroups and intervals in prime fields. Journal of Number Theory, 2020, 215, 261-274.	0.4	3
383	On smooth squareâ€free numbers in arithmetic progressions. Journal of the London Mathematical Society, 2020, 101, 1041-1067.	1.0	3
384	An Extremely Small and Efficient Identification Scheme. Lecture Notes in Computer Science, 2000, , 378-384.	1.3	3
385	Communication Complexity and Fourier Coefficients of the Diffieâ€“Hellman Key. Lecture Notes in Computer Science, 2000, , 259-268.	1.3	3
386	On the distribution of the power generator modulo a prime power. DIMACS Series in Discrete Mathematics and Theoretical Computer Science, 2004, , 71-79.	0.0	3
387	Restricted Mean Value Theorems and the Metric Theory of Restricted Weyl Sums. Quarterly Journal of Mathematics, 2021, 72, 885-919.	0.8	3
388	EXPONENTIAL SUMS IN CODING THEORY, CRYPTOLOGY AND ALGORITHMS. Lecture Notes Series, Institute for Mathematical Sciences, 2002, , 323-383.	0.2	3
389	Pseudorandom Points on Elliptic Curves over Finite Fields. , 2008, , .		3
390	On the distribution of solutions to linear equations. Glasnik Matematicki, 2009, 44, 7-10.	0.3	3
391	On finite fields for pairing based cryptography. Advances in Mathematics of Communications, 2007, 1, 281-286.	0.7	3
392	Twisted exponential sums over points of elliptic curves. Acta Arithmetica, 2011, 148, 77-92.	0.4	3
393	DISTRIBUTION OF POINTS ON MODULAR HYPERBOLAS. , 2007, , .		3
394	On Pseudosquares and Pseudopowers. , 2009, , .		3
395	Kloosterman sums with twice-differentiable functions. Functiones Et Approximatio, Commentarii Mathematici, 2020, 63, .	0.3	3
396	Zero testing of p-adic and modular polynomials. Theoretical Computer Science, 2000, 233, 309-317.	0.9	2

#	Article	IF	Citations
397	The CREW PRAM Complexity of Modular Inversion. SIAM Journal on Computing, 2000, 29, 1839-1857.	1.0	2
398	On the Uniformity of Distribution of the Elliptic Curve ElGamal Signature. Finite Fields and Their Applications, 2002, 8, 589-596.	1.0	2
399	Complexity of some arithmetic problems for binary polynomials. Computational Complexity, 2003, 12, 23-47.	0.3	2
400	On the multidimensional distribution of the subset sum generator of pseudorandom numbers. Mathematics of Computation, 2003, 73, 1005-1012.	2.1	2
401	Smooth values of shifted primes in arithmetic progressions. Michigan Mathematical Journal, 2004, 52, 603.	0.4	2
402	Distribution of exponential functions with k-full exponent modulo a prime. Indagationes Mathematicae, 2004, 15, 497-503.	0.4	2
403	SOME DIVISIBILITY PROPERTIES OF THE EULER FUNCTION. Glasgow Mathematical Journal, 2005, 47, 517.	0.3	2
404	On the nonlinearity of the sequence of signs of Kloosterman sums. Bulletin of the Australian Mathematical Society, 2005, 71, 405-409.	0.5	2
405	Distribution of harmonic sums and Bernoulli polynomials modulo a prime. Mathematische Zeitschrift, 2006, 253, 855-865.	0.9	2
406	ON THE SUMS OF COMPLEMENTARY DIVISORS. International Journal of Number Theory, 2007, 03, 635-648.	0.5	2
407	Character sums over shifted smooth numbers. Proceedings of the American Mathematical Society, 2007, 135, 2699-2706.	0.8	2
408	On the distribution of Kloosterman sums. Proceedings of the American Mathematical Society, 2007, 136, 419-425.	0.8	2
409	ON THE SQUARE-FREE PARTS OF âŒŠen!âŒ‹. Glasgow Mathematical Journal, 2007, 49, 391-403.	0.3	2
410	Character sums with subsequence sums. Periodica Mathematica Hungarica, 2007, 55, 215-221.	0.9	2
411	Estimates for Wieferich numbers. Ramanujan Journal, 2007, 14, 361-378.	0.7	2
412	On the size of the Jacobians of curves over finite fields. Bulletin of the Brazilian Mathematical Society, 2008, 39, 587-595.	0.8	2
413	On the exponential sumâ€"product problem. Indagationes Mathematicae, 2008, 19, 325-331.	0.4	2
414	Arithmetic properties of ApÃ©ry numbers. Journal of the London Mathematical Society, 2008, 78, 545-562.	1.0	2

#	Article	IF	Citations
415	CONGRUENCES AND EXPONENTIAL SUMS WITH THE SUM OF ALIQUOT DIVISORS FUNCTION. International Journal of Number Theory, 2008, 04, 903-909.	0.5	2
416	INFINITE HILBERT CLASS FIELD TOWERS OVER CYCLOTOMIC FIELDS. Glasgow Mathematical Journal, 2008, 50, 27-32.	0.3	2
417	Multiplicative character sums with the Euler function. Studia Scientiarum Mathematicarum Hungarica, 2009, 46, 223-229.	0.1	2
418	On the density of some special primes. Journal of Mathematical Cryptology, 2009, 3, .	0.7	2
419	On character sums with distances on the upper half plane over a finite field. Finite Fields and Their Applications, 2009, 15, 738-747.	1.0	2
420	OPEN PROBLEMS ON EXPONENTIAL AND CHARACTER SUMS. , 2009, , .		2
421	Partitions into two Lehmer numbers. Monatshefte Fur Mathematik, 2010, 160, 429-441.	0.9	2
422	On small solutions to quadratic congruences. Journal of Number Theory, 2011, 131, 1105-1111.	0.4	2
423	Counting dihedral and quaternionic extensions. Transactions of the American Mathematical Society, 2011, 363, 3233-3253.	0.9	2
424	EXPONENTIAL SUMS OVER POINTS OF ELLIPTIC CURVES WITH RECIPROCALS OF PRIMES. Mathematika, 2012, 58, 21-33.	0.5	2
425	On the distribution of values and zeros of polynomial systems over arbitrary sets. Journal of Number Theory, 2013, 133, 2863-2873.	0.4	2
426	Periodic structure of the exponential pseudorandom number generator. , 2014, , 190-203.		2
427	Random Walks, Bisections and Gossiping in Circulant Graphs. Algorithmica, 2014, 70, 301-325.	1.3	2
428	Distribution of elliptic twin primes in isogeny and isomorphism classes. Journal of Number Theory, 2014, 137, 1-15.	0.4	2
429	Squarefree parts of discriminants of trinomials. Archiv Der Mathematik, 2014, 102, 545-554.	0.5	2
430	Distribution of exponential functions modulo a prime power. Journal of Number Theory, 2014, 143, 224-231.	0.4	2
431	Explicit Form of Casselsâ€™ p-adic Embedding Theorem for Number Fields. Canadian Journal of Mathematics, 2015, 67, 1046-1064.	0.6	2
432	Counting additive decompositions of quadratic residues in finite fields. Functiones Et Approximatio, Commentarii Mathematici, 2015, 52, .	0.3	2

#	Article	IF	Citations
433	Counting irreducible binomials over finite fields. Finite Fields and Their Applications, 2016, 38, 1-12.	1.0	2
434	Linear congruences with ratios. Proceedings of the American Mathematical Society, 2016, 144, 2837-2846.	0.8	2
435	Averaging Operators Over Homogeneous Varieties Over Finite Fields. Journal of Geometric Analysis, 2016, 26, 1415-1441.	1.0	2
436	On small gaps between the elements of multiplicative subgroups of finite fields. Designs, Codes, and Cryptography, 2016, 80, 63-71.	1.6	2
437	The Satoâ€“Tate distribution in families of elliptic curves with a rational parameter of bounded height. Indagationes Mathematicae, 2017, 28, 306-320.	0.4	2
438	On the error term of a lattice counting problem. Journal of Number Theory, 2018, 182, 19-36.	0.4	2
439	Double Character Sums with Intervals and Arbitrary Sets. Proceedings of the Steklov Institute of Mathematics, 2018, 303, 239-258.	0.3	2
440	Analogues of the Balogâ€“Wooley Decomposition for Subsets of Finite Fields and Character Sums with Convolutions. Annals of Combinatorics, 2019, 23, 183-205.	0.6	2
441	Disjointness of the MÃ¶bius Transformation and MÃ¶bius Function. Research in Mathematical Sciences, 2019, 6, 1.	1.0	2
442	On the Number of Products Which Form Perfect Powers and Discriminants of Multiquadratic Extensions. International Mathematics Research Notices, 2021, 2021, 17140-17169.	1.0	2
443	Distribution of short subsequences of inversive congruential pseudorandom numbers modulo 2^t. Mathematics of Computation, 2019, 89, 911-922.	2.1	2
444	Value Sets of Sparse Polynomials. Canadian Mathematical Bulletin, 2020, 63, 187-196.	0.5	2
445	ON THE ARITHMETIC STRUCTURE OF RATIONAL NUMBERS IN THE CANTOR SET. Bulletin of the Australian Mathematical Society, 2021, 103, 22-27.	0.5	2
446	Exponential Sums with Sparse Polynomials over Finite Fields. SIAM Journal on Discrete Mathematics, 2021, 35, 976-987.	0.8	2
447	A SPARSITY RESULT FOR THE DYNAMICAL MORDELLâ€“LANG CONJECTURE IN POSITIVE CHARACTERISTIC. Bulletin of the Australian Mathematical Society, 2021, 104, 381-390.	0.5	2
448	Average distribution of k â€free numbers in arithmetic progressions. Mathematische Nachrichten, 2020, 293, 1505-1514.	0.8	2
449	Elliptic Twin Prime Conjecture. Lecture Notes in Computer Science, 2009, , 77-81.	1.3	2
450	Bounds of Trilinear and Trinomial Exponential Sums. SIAM Journal on Discrete Mathematics, 2020, 34, 2124-2136.	0.8	2

#	Article	IF	Citations
451	KLOOSTERMAN PATHS OF PRIME POWERS MODULI, II. Bulletin De La Societe Mathematique De France, 2020, 148, 173-188.	0.2	2
452	On the distribution of the Euler function of shifted smooth numbers. Colloquium Mathematicum, 2010, 120, 139-148.	0.3	2
453	Short Kloosterman Sums for Polynomials over Finite Fields. Canadian Journal of Mathematics, 2003, 55, 225-246.	0.6	2
454	Divisor Sums of Generalised Exponential Polynomials. Canadian Mathematical Bulletin, 1996, 39, 35-46.	0.5	2
455	On the largest prime factor of n!+ 2^n-1. Journal De Theorie Des Nombres De Bordeaux, 2005, 17, 859-870.	0.1	2
456	Selective Forgery of RSA Signatures with Fixed-Pattern Padding. Lecture Notes in Computer Science, 2002, , 228-236.	1.3	2
457	GCD of Random Linear Forms. Lecture Notes in Computer Science, 2004, , 464-469.	1.3	2
458	Additive energy and a large sieve inequality for sparse sequences. Mathematika, 2022, 68, 362-399.	0.5	2
459	Energy bounds, bilinear forms and their applications in function fields. Finite Fields and Their Applications, 2022, 82, 102048.	1.0	2
460	Distances from differences of roots of polynomials to the nearest integers. Information Processing Letters, 1992, 43, 143-146.	0.6	1
461	On Parameters of Some Graphs from Finite Fields. European Journal of Combinatorics, 1993, 14, 589-591.	0.8	1
462	On the Number of Sparse RSA Exponents. Journal of Number Theory, 2002, 95, 340-350.	0.4	1
463	On the Uniformity of Distribution of the ElGamal Signature. Applicable Algebra in Engineering, Communications and Computing, 2002, 13, 9-16.	0.5	1
464	Exponential Function Analogue of Kloosterman Sums. Rocky Mountain Journal of Mathematics, 2004, 34, 1497.	0.4	1
465	Polynomial Gauss sums. Proceedings of the American Mathematical Society, 2005, 133, 2225-2231.	0.8	1
466	TRUNCATIONS OF L-FUNCTIONS IN RESIDUE CLASSES. Glasgow Mathematical Journal, 2006, 48, 347.	0.3	1
467	Some divisibilities amongst the terms of linear recurrences. Abhandlungen Aus Dem Mathematischen Seminar Der Universitat Hamburg, 2006, 76, 143.	0.2	1
468	On the distribution of angles of the SaliÃ© sums. Bulletin of the Australian Mathematical Society, 2007, 75, 221-227.	0.5	1

#	Article	IF	Citations
469	Quantum period reconstruction of approximate sequences. Information Processing Letters, 2007, 103, 211-215.	0.6	1
470	APPROXIMATION BY SEVERAL RATIONALS. Bulletin of the Australian Mathematical Society, 2008, 77, 325-329.	0.5	1
471	ARITHMETIC AND GEOMETRIC PROGRESSIONS IN PRODUCT SETS OVER FINITE FIELDS. Bulletin of the Australian Mathematical Society, 2008, 78, 357-364.	0.5	1
472	Subset sum pseudorandom numbers: fast generation and distribution. Journal of Mathematical Cryptology, 2009, 3, .	0.7	1
473	Bilinear sums with exponential functions. Proceedings of the American Mathematical Society, 2009, 137, 2217-2224.	0.8	1
474	Some counting questions for matrices with restricted entries. Linear Algebra and Its Applications, 2010, 432, 155-160.	0.9	1
475	Some Divisibility Properties of Binomial Coefficients and the Converse of Wolstenholme's Theorem. Integers, 2010, 10, .	0.3	1
476	On the Satoâ€“Tate conjecture on average for some families of elliptic curves. Forum Mathematicum, 2011, , ---.	0.7	1
477	On the convex hull of solutions to polynomial congruences. Journal of Number Theory, 2012, 132, 254-257.	0.4	1
478	Predicting masked linear pseudorandom number generators over finite fields. Designs, Codes, and Cryptography, 2013, 67, 395-402.	1.6	1
479	Statistics of Different Reduction Types of Fermat Curves. Experimental Mathematics, 2013, 22, 243-249.	0.7	1
480	Elliptic Curves over Finite Fields: Number Theoretic and Cryptographic Aspects. Fields Institute Communications, 2013, , 65-90.	1.3	1
481	Evasive properties of sparse graphs and some linear equations in primes. Theoretical Computer Science, 2014, 547, 117-121.	0.9	1
482	MULTIPLE EXPONENTIAL AND CHARACTER SUMS WITH MONOMIALS. Mathematika, 2014, 60, 363-373.	0.5	1
483	On the singularity of the Demjanenko matrix of quotients of Fermat curves. Proceedings of the American Mathematical Society, 2015, 144, 55-63.	0.8	1
484	Groups generated by iterations of polynomials over finite fields. Proceedings of the Edinburgh Mathematical Society, 2016, 59, 235-245.	0.3	1
485	Multiples of squares in short intervals. Functiones Et Approximatio, Commentarii Mathematici, 2016, 54, .	0.3	1
486	Ratios of Small Integers in Multiplicative Subgroups of Residue Rings. Experimental Mathematics, 2016, 25, 273-280.	0.7	1

#	Article	IF	Citations
487	An explicit polynomial analogue of Romanoff's theorem. Finite Fields and Their Applications, 2017, 44, 22-33.	1.0	1
488	Constructing Dominating Sets in Circulant Graphs. Annals of Combinatorics, 2018, 22, 201-211.	0.6	1
489	On the exponential large sieve inequality for sparse sequences modulo primes. Journal of Mathematical Analysis and Applications, 2018, 459, 53-81.	1.0	1
490	On Constructing Primitive Roots in Finite Fields With Advice. IEEE Transactions on Information Theory, 2018, 64, 7132-7136.	2.4	1
491	Arithmetic Properties of Integers in Chains and Reflections of g-ary Expansions. Experimental Mathematics, 2018, 27, 184-192.	0.7	1
492	DENOMINATORS OF BERNOULLI POLYNOMIALS. Mathematika, 2018, 64, 519-541.	0.5	1
493	Trilinear forms with double Kloosterman sums. International Journal of Number Theory, 2018, 14, 2195-2203.	0.5	1
494	Sums with the MÃ¶bius function twisted by characters with powerful moduli. Transactions of the American Mathematical Society, 2019, 373, 249-272.	0.9	1
495	LOWER BOUNDS FOR PERIODS OF DUCCI SEQUENCES. Bulletin of the Australian Mathematical Society, 2020, 102, 31-38.	0.5	1
496	MÃ¶bius Randomness Law for Frobenius Traces of Ordinary Curves. Canadian Mathematical Bulletin, 2021, 64, 192-203.	0.5	1
497	On the dynamical system generated by the MÃ¶bius transformation at prime times. Research in Mathematical Sciences, 2021, 8, 1.	1.0	1
498	On the Skolem problem and some related questions for parametric families of linear recurrence sequences. Canadian Journal of Mathematics, 2022, 74, 773-792.	0.6	1
499	Order of torsion for reduction of linearly independent points for a family of Drinfeld modules. Journal of Number Theory, 2022, 233, 112-125.	0.4	1
500	Pseudorandom Graphs from Elliptic Curves. , 2008, , 284-292.		1
501	Close values of shifted modular inversions and the decisional modular inversion hidden number problem. Advances in Mathematics of Communications, 2015, 9, 169-176.	0.7	1
502	On the Euler Function on Differences Between the Coordinates of Points on Modular Hyperbolas. Bulletin of the Polish Academy of Sciences Mathematics, 2008, 56, 1-7.	0.3	1
503	On two functions arising in the study of the Euler and Carmichael quotients. Colloquium Mathematicum, 2017, 149, 179-192.	0.3	1
504	Smooth shifted monomial products. Publicationes Mathematicae, 0, , 423-432.	0.2	1

#	Article	IF	Citations
505	On Polynomial Representations of Boolean Functions Related to Some Number Theoretic Problems. Lecture Notes in Computer Science, 2001, , 305-316.	1.3	1
506	Number Theory and Related Fields. Springer Proceedings in Mathematics and Statistics, 2013, , .	0.2	1
507	On the Average Number of Square-Free Values of Polynomials. Canadian Mathematical Bulletin, 2013, 56, 844-849.	0.5	1
508	On some applications of finitely generated semi-groups. Lecture Notes in Computer Science, 1994, , 265-279.	1.3	1
509	On Distances in Lattices from Algebraic Number Fields. Moscow Mathematical Journal, 2017, 17, 239-268.	0.4	1
510	Sparsity of curves and additive and multiplicative expansion of rational maps over finite fields. Acta Arithmetica, 2019, 188, 401-411.	0.4	1
511	Binomial exponential sums. Annali Della Scuola Normale Superiore Di Pisa Classe Di Scienze, 2020, , 931-941.	0.2	1
512	Unlikely intersections over finite fields: Polynomial orbits in small subgroups. Discrete and Continuous Dynamical Systems, 2020, 40, 1065-1073.	0.9	1
513	Hybrid Bounds on Two-Parametric Families of Weyl Sums Along Smooth Curves. Michigan Mathematical Journal, 2021, -1, .	0.4	1
514	On sparsity of representations of polynomials as linear combinations of exponential functions. Journal of the London Mathematical Society, 2022, 105, 2076-2103.	1.0	1
515	On the Glasner property for matrices with polynomial entries. Journal of Number Theory, 2023, 242, 522-531.	0.4	1
516	On Some Uniformity of Distribution Properties of ESIGN. Electronic Notes in Discrete Mathematics, 2001, 6, 132-139.	0.4	0
517	On the Uniformity of Distribution of the Elliptic Curve ElGamal Signature. Finite Fields and Their Applications, 2002, 8, 589-596.	1.0	0
518	An authentication scheme based on roots of sparse polynomials. , 0, , .		0
519	Finite Fields: Theory and Applications. Oberwolfach Reports, 2005, 1, 2913-2970.	0.0	0
520	On reducing a system of equations to a single equation. , 2004, , .		0
521	Number Theoretic Designs for Directed Regular Graphs of Small Diameter. SIAM Journal on Discrete Mathematics, 2004, 17, 377-383.	0.8	0
522	Prime divisors of some shifted products. International Journal of Mathematics and Mathematical Sciences, 2005, 2005, 3057-3073.	0.7	0

#	Article	IF	Citations
523	Multiplicative character sums with the sum of g-ary Digits Function. Ramanujan Journal, 2006, 11, 215-219.	0.7	0
524	Testing set proportionality and the ÃđÃ¡m isomorphism of circulant graphs. Journal of Discrete Algorithms, 2006, 4, 324-335.	0.7	0
525	Prime Divisors Of Some Recurrence Sequence. Periodica Mathematica Hungarica, 2007, 54, 215-227.	0.9	0
526	Distribution of Roots of Polynomial Congruences. International Journal of Mathematics and Mathematical Sciences, 2007, 2007, 1-5.	0.7	0
527	Communication complexity of some number theoretic functions. Applied Mathematics Letters, 2007, 20, 872-875.	2.7	0
528	Chinese Remaindering with Multiplicative Noise. Theory of Computing Systems, 2007, 40, 33-41.	1.1	0
529	Average distribution of prime ideals in families of number fields. Bulletin of the Brazilian Mathematical Society, 2008, 39, 417-425.	0.8	0
530	On pseudopoints of algebraic curves. Archiv Der Mathematik, 2010, 95, 529-537.	0.5	0
531	On the size of the Gelfond exponent. Journal of Number Theory, 2010, 130, 1056-1060.	0.4	0
532	On the Distribution of Orbits of $mathrm{PGL_2(q)}$ in ${mathbbF}_{q^n}$ and the Klapper Conjecture. SIAM Journal on Discrete Mathematics, 2010, 23, 2093-2099.	0.8	0
533	Pseudoprime Reductions of Elliptic Curves â€“ CORRIGENDUM. Mathematical Proceedings of the Cambridge Philosophical Society, 2012, 152, 571-571.	0.4	0
534	Correcting noisy exponentiation black-boxes modulo a prime. Information Processing Letters, 2013, 113, 414-417.	0.6	0
535	â€˜SUM-PRODUCT ESTIMATES AND MULTIPLICATIVE ORDERS OF AND IN FINITE FIELDSâ€™. Bulletin of the Australian Mathematical Society, 2013, 87, 527-528.	0.5	0
536	Enumeration of certain varieties over a finite field. Proceedings of the American Mathematical Society, 2014, 142, 2615-2623.	0.8	0
537	ON SOLUTIONS TO SOME POLYNOMIAL CONGRUENCES IN SMALL BOXES. Bulletin of the Australian Mathematical Society, 2014, 89, 300-307.	0.5	0
538	On the product of small Elkies primes. Proceedings of the American Mathematical Society, 2014, 143, 1441-1448.	0.8	0
539	VSH and multiplicative modular relations between small primes with polynomial exponents. Applicable Algebra in Engineering, Communications and Computing, 2014, 25, 181-188.	0.5	0
540	On Gauss sums and the evaluation of Stechkinâ€™s constant. Mathematics of Computation, 2015, 85, 2569-2581.	2.1	0

#	Article	IF	Citations
541	On the greatest common divisor of shifted sets. Journal of Number Theory, 2015, 154, 63-73.	0.4	0
542	Small discriminants of complex multiplication fields of elliptic curves over finite fields. Czechoslovak Mathematical Journal, 2015, 65, 381-388.	0.3	0
543	Circulant graphs and GCD and LCM of subsets. Information Processing Letters, 2015, 115, 134-138.	0.6	0
544	SYSTEMS OF CONGRUENCES WITH PRODUCTS OF VARIABLES FROM SHORT INTERVALS. Bulletin of the Australian Mathematical Society, 2016, 93, 364-371.	0.5	0
545	ON BILINEAR EXPONENTIAL AND CHARACTER SUMS WITH RECIPROCALS OF POLYNOMIALS. Mathematika, 2016, 62, 842-859.	0.5	0
546	On Coincidences Among Quadratic Fields Generated by the Shanks Sequence. Quarterly Journal of Mathematics, 0, , .	0.8	0
547	On the density of integer points on generalised Markoffâ€“Hurwitz and Dwork hypersurfaces. Mathematische Zeitschrift, 2016, 282, 935-954.	0.9	0
548	Finding elliptic curves with a subgroup of prescribed size. International Journal of Number Theory, 2017, 13, 133-152.	0.5	0
549	On the convex hull of the points on multivariate modular hyperbolas. Journal of Number Theory, 2017, 171, 71-78.	0.4	0
550	Sums of inverses in thin sets of finite fields. Proceedings of the American Mathematical Society, 2017, 146, 1377-1388.	0.8	0
551	Effective results on linear dependence for elliptic curves. Pacific Journal of Mathematics, 2018, 295, 123-144.	0.5	0
552	Identity testing and interpolation from high powers of polynomials of large degree over finite fields. Journal of Complexity, 2018, 49, 74-84.	1.3	0
553	Character sums with smooth numbers. Archiv Der Mathematik, 2018, 110, 467-476.	0.5	0
554	On the GyÅ‘ry-SÃ¡rkÃ¶zy-Stewart conjecture in function fields. , 2018, 68, 1067-1077.		0
555	Bounds on average values of double incomplete Kloosterman sums. Journal of Number Theory, 2019, 203, 1-11.	0.4	0
556	ON FINDING SOLUTIONS TO EXPONENTIAL CONGRUENCES. Bulletin of the Australian Mathematical Society, 2019, 99, 388-391.	0.5	0
557	Codes correcting restricted errors. Designs, Codes, and Cryptography, 2019, 87, 855-863.	1.6	0
558	The Sato-Tate distribution in thin families of elliptic curves over high degree extensions of finite fields. International Journal of Number Theory, 2019, 15, 469-477.	0.5	0

#	Article	IF	Citations
559	On the complexity of exact counting of dynamically irreducible polynomials. Journal of Symbolic Computation, 2020, 99, 231-241.	0.8	0
560	Dynamical irreducibility of polynomials modulo primes. Mathematische Zeitschrift, 2021, 298, 1187.	0.9	0
561	Bounds of some double exponential sums. Journal of Number Theory, 2021, 219, 228-236.	0.4	0
562	Noisy polynomial interpolation modulo prime powers. Journal of Complexity, 2021, 64, 101542.	1.3	0
563	Small values of Weyl sums. Journal of Mathematical Analysis and Applications, 2021, 495, 124743.	1.0	0
564	On elements of large order on elliptic curves and multiplicative dependent images of rational functions over finite fields. Illinois Journal of Mathematics, 2021, 65, .	0.1	0
565	Counting solvable S-unit equations. Proceedings of the American Mathematical Society, 0, , 1.	0.8	0
566	Bounds of trilinear sums with Kloosterman fractions. Archiv Der Mathematik, 2021, 117, 261-266.	0.5	0
567	On a conjecture of Soundararajan. Bulletin of the London Mathematical Society, 2022, 54, 301-317.	0.8	0
568	On the Security o Lenstraâ€™ s Variant o DSA without Long Inversions. Lecture Notes in Computer Science, 2001, , 64-72.	1.3	0
569	Chinese Remaindering for Algebraic Numbers in a Hidden Field. Lecture Notes in Computer Science, 2002, , 349-356.	1.3	0
570	On Rough and Smooth Neighbors. Revista Matematica Complutense, 2007, 20, .	1.2	0
571	Collision in the DSA Function. , 2008, , .		0
572	An Average Bound for Character Sums with Some Counter-Dependent Recurrence Sequences. Rocky Mountain Journal of Mathematics, 2009, 39, .	0.4	0
573	Random Walks and Bisections in Random Circulant Graphs. Lecture Notes in Computer Science, 2012, , 542-555.	1.3	0
574	Character Sums with Division Polynomials. Canadian Mathematical Bulletin, 2012, 55, 850-857.	0.5	0
575	On some exponential sums with exponential and rational functions. Rocky Mountain Journal of Mathematics, 2013, 43, .	0.4	0
576	Geometric progressions in vector sumsets over finite fields. Finite Fields and Their Applications, 2020, 68, 101747.	1.0	0

#	Article	IF	Citations
577	Corrections to â€œValue sets of sparse polynomialsâ€• Canadian Mathematical Bulletin, 2022, 65, 1071-1073.	0.5	0
578	Large Weyl sums and Hausdorff dimension. Journal of Mathematical Analysis and Applications, 2022, 510, 126030.	1.0	0
579	Multiplicative Properties of Hilbert Cubes. SIAM Journal on Discrete Mathematics, 2022, 36, 1064-1070.	0.8	0