Aimed at Math. Comp.

DISTINGUISHING PRIME NUMBERS FROM COMPOSITE NUMBERS: THE STATE OF THE ART IN 2004

DANIEL J. BERNSTEIN

Abstract. This paper compares 21 methods to distinguish prime numbers from composite numbers. It answers the following questions for each method: Does the method certify primality? Conjecturally certify primality? Certify compositeness? Are certificates conjectured to exist for all inputs? Proven to exist for all inputs? Found deterministically for all inputs? Is a certificate verified in essentially linear time? Essentially quadratic time? Et cetera. Is a certificate found immediately? In essentially linear time? Essentially quadratic time? Et cetera. In brief, how does the method work? When and where was the method published?

1. Introduction

This paper summarizes fourteen methods to prove that an integer is prime, three additional methods to prove that an integer is prime if certain conjectures are true, and four methods to prove that an integer is composite. The summary is presented in a compressed chart and in a comprehensive table.

The table has five columns for each method:

- "Method": a brief summary of a theorem encapsulating the method. For example, one method is "if n is not a b-prp, i.e., does not divide $b^n - b$, then n is composite." The target integer is always n. An auxiliary input, such as b in this example, is called a **certificate**.
- "Effect of certificate": what the method tells you about the target integer n. Either "proves primality" or "conjecturally certifies primality" or "proves compositeness."
- "Certificate exists for": which integers can be handled by the method. Either "every prime" or "conjecturally every prime" or "every composite" or "nearly every composite."
- "Time to verify certificate": how quickly one can check whether an auxiliary input is, in fact, a certificate for n. For example, $(\lg n)^{1+o(1)}$ or $(\lg n)^{2+o(1)}$ or $(\lg n)^{O(\lg\lg\lg n)}$. **Time** in this paper is measured on conventional von Neumann computers, such as 2-tape Turing machines; space is ignored.
- "Time to find certificate," at the same level of detail. Some certificate-finding methods use randomness, as indicated by "random" in this column.

Date: 2004.02.12. Permanent ID of this document: `d72f09ae5b05f41a53e2237c53f5f276`.

2000 *Mathematics Subject Classification.* Primary 11Y16.

The author was supported by the National Science Foundation under grant DMS–0140542, and by the Alfred P. Sloan Foundation. He used the libraries at the Mathematical Sciences Research Institute, the University of California at Berkeley, and the American Institute of Mathematics.

The table includes various credits. For example, the original elliptic-curve primality-proving method was published in 1986 by Goldwasser and Kilian in [38]; its proofs of primality rely on a 1936 theorem of Hasse in [44]; it finds certificates using a 1985 algorithm of Schoof in [83]. These credits are listed under "Method," "Effect of certificate," and "Time to find certificate" respectively.

The chart includes the following information for each method:

- Proven upper bounds for exponents in times to (provably deterministically) verify certificates. These upper bounds are listed down the side of the chart.
- Proven upper bounds for exponents in times to (provably deterministically, or provably randomly, or conjecturally) find certificates. These upper bounds are listed across the top of the chart.
- How reliably the method finds certificates: "d" if certificates are provably deterministically found for every n (every prime n for primality-proving methods, or every composite n for compositeness-proving methods); "r" if certificates are provably found for every n but the algorithm uses randomness; or "?" if certificates are merely conjectured to be found for every n. Certificates not believed to exist for every n are not included in the chart.
- What the method does: "p" for certificates that prove primality or "c" for certificates that prove compositeness. (Empty certificates that prove either primality or compositeness, depending on the input, are listed as "dpc" in column $0 + o(1)$.) Certificates that are merely conjectured to imply primality are not included in the chart.
- The year that the method was first published.

For example, the entry "?p 1990" in row $3 + o(1)$ and column $4 + o(1)$ refers to a primality-proving method with the following features: certificates are conjectured to be found for every prime n in time $(\lg n)^{4+o(1)}$; certificates are deterministically verified in time $(\lg n)^{3+o(1)}$; verification of a certificate proves that n is prime. This method is Shallit's variant, published by Lenstra and Lenstra in [53], of the elliptic-curve primality-proving method.

Thanks to Eric Bach for suggesting a 2-dimensional chart. A 3-dimensional chart (with the third dimension labelled ?p, rp, dp, dpc, dc, rc, ?c) would be even better, but would be difficult to compress comprehensibly onto a printed page.

Lower-level subroutines. Implementors should be aware of the state of the art in algorithms to carry out various lower-level operations:

- Integer multiplication, division, and gcd can be done in essentially linear time, as shown by Toom in [87], Cook in [32], and Knuth in [48] respectively. Similar comments apply to various other arithmetic operations; see my survey [16]. Additional constant-factor speedups in arithmetic are an active research area.
- One can quickly find all divisors of n congruent to r modulo m, when m is larger than roughly $n^{1/4}$. This was proven by Coppersmith, Howgrave-Graham, and Nagaraj in 1998, after earlier results by Lenstra, Konyagin, and Pomerance; see [54], [49], [45, Section 5.5], and my survey [18].

Beware that slower subroutines for arithmetic, and larger bounds on m, appear throughout the primality/compositeness literature—usually because the authors were writing before the better results were known, but sometimes because the authors inexplicably refused to take advantage of the best known results.

2. The chart

	$0 + o(1)$	$1 + o(1)$	$2 + o(1)$	$3 + o(1)$	$4 + o(1)$	$5 + o(1)$	$O(1)$	very big
$1 + o(1)$								dc
$2 + o(1)$			rc 1966					dp 1987
$3 + o(1)$					?p 1990	?p 1988	rp 1992 ?p 1986	dp 1914
$4 + o(1)$			rp 2003				dc unp	
$5 + o(1)$								
$6 + o(1)$	dpc unp ?pc 2002							
$O(1)$	dpc 2002							
$O(\lg\lg\lg n)$	dpc 1979							

Here are the methods listed—see the table for more information:

- $1 + o(1)$, very big, dc: proving compositeness with factorization.
- $2+o(1)$, $2+o(1)$, rc 1966: Artjuhov [9], proving compositeness with Fermat.
- $2+o(1)$, very big, dp 1987: Pomerance [77], proving primality with elliptic-curve factors.
- $3+o(1)$, $4+o(1)$, ?p 1990: Shallit [53], proving primality with elliptic-curve factors.
- $3+o(1)$, $5+o(1)$, ?p 1988: Atkin [66], proving primality with elliptic-curve factors.
- $3+o(1)$, $O(1)$, rp 1992: Adleman Huang [4], proving primality with genus-2-hyperelliptic-curve factors.
- $3 + o(1)$, $O(1)$, ?p 1986: Goldwasser Kilian [38], proving primality with elliptic-curve factors.
- $3 + o(1)$, very big, dp 1914: Pocklington [75], proving primality with unit-group factors.
- $4 + o(1)$, $2 + o(1)$, rp 2003: Bernstein [17], proving primality with combinatorics.
- $4 + o(1)$, $6 + o(1)$ (shown as $O(1)$), dc unp: Lenstra Pomerance, to appear, proving compositeness by not proving primality with combinatorics.
- $6+o(1)$, $0+o(1)$, dpc unp: Lenstra Pomerance, to appear, proving primality with combinatorics.
- $6 + o(1)$, $0 + o(1)$, ?pc 2002: Agrawal Kayal Saxena [6], proving primality with combinatorics.
- $O(1)$, $0+o(1)$, dpc 2002: Agrawal Kayal Saxena [6], proving primality with combinatorics.
- $O(\lg\lg\lg n)$, $0 + o(1)$, dpc 1979: Adleman Pomerance Rumely [5], proving primality with unit-group factors.

3. The table

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
proving compositeness with factorization: if b divides n and $1 < b < n$ then n is composite	proves compositeness	every composite n	$(\lg n)^{1+o(1)}$	very slow; but $(\lg n)^{O(1)}$ for most n
proving compositeness with Fermat: if n is not a b-prp, i.e., does not divide $b^n - b$, then n is composite	proves compositeness	nearly every composite n; however, there are infinitely many composites n that are all-b-prp (1994 Alford Granville Pomerance [7])	$(\lg n)^{2+o(1)}$	random $(\lg n)^{2+o(1)}$
if n is not a b-sprp, i.e., does not divide any of the most obvious factors of $b^n - b$, then n is composite (1966 Artjuhov [9])	proves compositeness	every composite n	$(\lg n)^{2+o(1)}$	random $(\lg n)^{2+o(1)}$ (1976 Rabin [81], independently 1980 Monier [64], independently 1982 Atkin Larson [11]; inferior variant: 1976 Lehmer [52], independently 1977 Solovay Strassen [86]; other variants: 1998 Grantham [41], 2001 Grantham [42], 2000 Müller [70], 2001 Müller [71], 2003 Damgard Frandsen [33])

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
conjecturally testing primality: if n is a b-sprp for every prime number b between 1 and $\lceil \lg n \rceil^2$, then n seems to be prime (basic idea: 1975 Miller [62])	conjecturally certifies primality; conjecture follows from GRH (1985 Bach [13]; $35 \lceil \lg n \rceil^2$ announced but not proven 1979 Oesterlé; $O(\lceil \lg n \rceil^2)$, without explicit O constant: 1952 Ankeny [8], 1971 Montgomery [65], 1978 Vélu [90])	every prime n	$(\lg n)^{4+o(1)}$	instant
if n is a b-sprp for the first $2 \lceil \lg n \rceil$ prime numbers b, then n seems to be prime (folklore; simpler variant giving prime power: 1995 Lukes Patterson Williams [58])	conjecturally certifies primality	every prime n	$(\lg n)^{3+o(1)}$	instant
if n is a 2-sprp and passes a similar quadratic test, then n seems to be prime (1980 Baillie Wagstaff [14], 1980 Pomerance Selfridge Wagstaff [78]; variant also including a cubic test: 1998 Atkin [10])	conjecturally certifies primality; conjecture is implausible for very large n (1984 Pomerance [76]), but no counterexamples are known	every prime n	$(\lg n)^{2+o(1)}$	instant

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
proving primality with unit-group factors: if $b^{n-1} = 1$ in $\mathbf{Z}/n$, and $b^{(n-1)/q} - 1$ is nonzero in $\mathbf{Z}/n$ for every prime divisor q of $n - 1$, then n is prime (1876 Lucas [56], [57], except that the switch from "divisor $q > 1$" to "prime divisor q" is from 1927 Lehmer [50] by analogy to 1914 Pocklington [75])	proves primality	every prime n	at most $(\lg n)^{3+o(1)}$; usually $(\lg n)^{2+o(1)}$	very slow; but conjectured to be $(\lg n)^{O(1)}$ for infinitely many n
if $b^{n-1} = 1$ in $\mathbf{Z}/n$, F is a divisor of $n - 1$, and $b^{(n-1)/q} - 1$ is a unit in $\mathbf{Z}/n$ for every prime divisor q of F, then every divisor of n is in $\{1, F + 1, \dots\}$, so if $(F + 1)^2 > n$ then n is prime (1914 Pocklington [75]); similar test for F down to roughly $n^{1/4}$	proves primality	every prime n	at most $(\lg n)^{3+o(1)}$; usually $(\lg n)^{2+o(1)}$	very slow; but fast for more n's than above; $(\lg n)^{O(1)}$ for infinitely many n (1989 Pintz Steiger Szemeredi [74]; variant: 1992 Fellows Koblitz [34]; another variant: 1997 Konyagin Pomerance [49])
Pocklington-type test with quadratic extensions of $\mathbf{Z}/n$ (1876 Lucas [56], 1930 Lehmer [51], 1975 Morrison [69], 1975 Selfridge Wunderlich [85], 1975 Brillhart Lehmer Selfridge [24])	proves primality	every prime n	at most $(\lg n)^{3+o(1)}$; usually $(\lg n)^{2+o(1)}$	very slow; but fast for more n's than above

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
Pocklington-type test with higher-degree extensions of $\mathbf{Z}/n$ (degrees 4 and 6: 1976 Williams Judd [93]; general degrees: 1983 Adleman Pomerance Rumely [5])	proves primality	every prime n	$(\lg n)^{O(\lg\lg\lg n)}$, using distribution of divisors of $n^d - 1$ (1983 Odlyzko Pomerance [5]; weaker bound: 1955 Prachar [79]; best known bound: 2000 Pelikan Pintz Szemeredi [73]); many speedups available (1978 Williams Holte [92], 1984 Cohen Lenstra [31], 1985 Cohen Lenstra [29], 1990 Bosma van der Hulst [22], 1998 Mihăilescu [60])	instant
proving primality with elliptic-curve factors: similar test using elliptic curves (1986 Goldwasser Kilian [38])	proves primality, using bounds on elliptic-curve sizes (1936 Hasse [44])	nearly every prime n; conjecturally, every prime n	$(\lg n)^{3+o(1)}$	$(\lg n)^{O(1)}$, using polynomial-time elliptic-curve point counting (1985 Schoof [83]); many speedups available (1995 Atkin Elkies [84]; 1995 Lercier Morain [55])
similar test with elliptic curves having order divisible by a large power of 2 (1987 Pomerance [77])	proves primality, using bounds on elliptic-curve sizes (1936 Hasse [44])	every prime n	$(\lg n)^{2+o(1)}$	very slow

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
similar test with Jacobians of genus-2 hyperelliptic curves (1992 Adleman Huang [4])	proves primality, using bounds on Jacobian sizes (1948 Weil [91])	every prime n	at most $(\lg n)^{3+o(1)}$	random $(\lg n)^{O(1)}$, using distribution of primes in interval of width $x^{3/4}$ around x (1979 Iwaniec Jutila [46]), and distribution of Jacobian sizes (1992 Adleman Huang [4])
similar test with small-discriminant complex-multiplication elliptic curves (1988 Atkin [66]; special cases: 1985 Bosma [20], 1986 Chudnovsky Chudnovsky [28])	proves primality, using bounds on elliptic-curve sizes (1936 Hasse [44])	conjecturally, every prime n	at most $(\lg n)^{3+o(1)}$	at most $(\lg n)^{5+o(1)}$
similar test with small-discriminant complex-multiplication elliptic curves, merging square-root computations for many discriminants (1990 Shallit [53])	proves primality, using bounds on elliptic-curve sizes (1936 Hasse [44])	conjecturally, every prime n	at most $(\lg n)^{3+o(1)}$	at most $(\lg n)^{4+o(1)}$; many speedups available (1988 Morain [66], 1989 Kaltofen Valente Yui [47], 1990 Morain [67], 1993 Atkin Morain [12], 1998 Morain [68], 2003 Franke Kleinjung Morain Wirth [36])

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
proving primality with combinatorics: if we can write down many elements of a particular subgroup of a prime cyclotomic extension of $\mathbf{Z}/n$ then n is a power of a prime (2002.08 Agrawal Kayal Saxena [6])	proves primality	every prime n	$(\lg n)^{O(1)}$, using analytic fact that, for some $c > 1/2$, many primes r have prime divisor of $r-1$ above r^c (1969 Goldfeld [37]); at most $(\lg n)^{12+o(1)}$, using analytic fact that many primes r have prime divisor of $r-1$ above $r^{2/3}$ (1985 Fouvry [35]); conjecturally $(\lg n)^{6+o(1)}$	instant
variant using arbitrary cyclotomic extensions (2003.01 Lenstra [15, Theorem 2.3])	proves primality	every prime n	at most $(\lg n)^{12+o(1)}$, using crude bound on distribution of primes (1850 Chebyshev); at most $(\lg n)^{8+o(1)}$, using analytic facts as above; conjecturally $(\lg n)^{6+o(1)}$	instant
variant using cyclotomic extensions with better bound on group structure (2002.12 Macaj [59], independently 2003 Agrawal)	proves primality	every prime n	at most $(\lg n)^{10.5+o(1)}$, using crude bound on distribution of primes (1850 Chebyshev); at most $(\lg n)^{7.5+o(1)}$, using analytic facts as above; conjecturally $(\lg n)^{6+o(1)}$	instant
variant using random Kummer extensions (2003.01 Bernstein [17]; independently 2003.03 Mihăilescu Avanzi [61]; idea and 2-power-degree case: 2002.12 Berrizbeitia [19]; prime-degree case: 2003.01 Cheng [27])	proves primality	every prime n	$(\lg n)^{4+o(1)}$, using distribution of divisors of n^d-1 (overkill: 1983 Odlyzko Pomerance [5])	random $(\lg n)^{2+o(1)}$

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
variant using Gaussian periods (Lenstra Pomerance, not yet published)	proves primality	every prime n	$(\lg n)^{6+o(1)}$, using various analytic facts	instant
if n fails any of the Fermat-type tests in these methods then n is composite	proves compositeness	every composite n	at most $(\lg n)^{4+o(1)}$, using analytic facts as above	at most $(\lg n)^{6+o(1)}$, using analytic facts as above

References

[1] —, *Actes du congrès international des mathématiciens, tome 3*, Gauthier-Villars Éditeur, Paris, 1971. MR 54:5.

[2] —, *Proceedings of the 18th annual ACM symposium on theory of computing*, Association for Computing Machinery, New York, 1986. ISBN 0–89791–193–8.

[3] —, *International symposium on symbolic and algebraic computation, ISSAC '89, Portland, Oregon, USA, July 17–19, 1989*, Association for Computing Machinery, New York, 1989.

[4] Leonard M. Adleman, Ming-Deh A. Huang, *Primality testing and abelian varieties over finite fields*, Lecture Notes in Mathematics, 1512, Springer-Verlag, Berlin, 1992. ISBN 3–540–55308–8. MR 93g:11128.

[5] Leonard M. Adleman, Carl Pomerance, Robert S. Rumely, *On distinguishing prime numbers from composite numbers*, Annals of Mathematics **117** (1983), 173–206. ISSN 0003–486X. MR 84e:10008.

[6] Manindra Agrawal, Neeraj Kayal, Nitin Saxena, *PRIMES is in P* (2002). Available from `http://www.cse.iitk.ac.in/news/primality.html`.

[7] W. R. Alford, Andrew Granville, Carl Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics **139** (1994), 703–722. ISSN 0003–486X. MR 95k:11114.

[8] N. C. Ankeny, *The least quadratic non residue*, Annals of Mathematics **55** (1952), 65–72. ISSN 0003–486X. MR 13,538c.

[9] M. M. Artjuhov, *Certain criteria for primality of numbers connected with the little Fermat theorem*, Acta Arithmetica **12** (1966), 355–364. ISSN 0065–1036. MR 35:4153.

[10] A. O. L. Atkin, *Intelligent primality test offer*, in [25] (1998), 1–11. MR 98k:11183.

[11] A. O. L. Atkin, Richard G. Larson, *On a primality test of Solovay and Strassen*, SIAM Journal on Computing **11** (1982), 789–791. ISSN 0097–5397. MR 84d:10013.

[12] A. O. L. Atkin, Francois Morain, *Elliptic curves and primality proving*, Mathematics of Computation **61** (1993), 29–68. ISSN 0025–5718. MR 93m:11136. Available from `http://www.lix.polytechnique.fr/~morain/Articles/articles.english.html`.

[13] Eric Bach, *Analytic methods in the analysis and design of number-theoretic algorithms*, Ph.D. thesis, MIT Press, 1985.

[14] Robert Baillie, Samuel S. Wagstaff, Jr., *Lucas pseudoprimes*, Mathematics of Computation **35** (1980), 1391–1417. ISSN 0025–5718. MR 81j:10005.

[15] Daniel J. Bernstein, *Proving primality after Agrawal-Kayal-Saxena*. Available from `http://cr.yp.to/papers.html`.

[16] Daniel J. Bernstein, *Fast multiplication and its applications*. Available from `http://cr.yp.to/papers.html`.

[17] Daniel J. Bernstein, *Proving primality in essentially quartic random time*. Available from `http://cr.yp.to/papers.html`.

[18] Daniel J. Bernstein, *Reducing lattice bases to find small-height values of univariate polynomials*. Available from `http://cr.yp.to/papers.html`.

[19] Pedro Berrizbeitia, *Sharpening PRIMES is in P for a large family of numbers* (2002). Available from `http://arxiv.org/abs/math.NT/0211334`.

[20] Wieb Bosma, *Primality testing using elliptic curves*, Technical Report 85–12 (1985).

[21] Wieb Bosma (editor), *Algorithmic number theory: ANTS-IV*, Lecture Notes in Computer Science, 1838, Springer-Verlag, Berlin, 2000. ISBN 3–540–67695–3. MR 2002d:11002.

[22] Wieb Bosma, Marc-Paul van der Hulst, *Primality proving with cyclotomy*, Ph.D. thesis, Universiteit van Amsterdam, 1990.

[23] Colin Boyd (editor), *Advances in cryptology—ASIACRYPT 2001: proceedings of the 7th international conference on the theory and application of cryptology and information security held on the Gold Coast, December 9–13, 2001*, Lecture Notes in Computer Science, 2248, Springer-Verlag, Berlin, 2001. ISBN 3–540–42987–5. MR 2003d:94001.

[24] John Brillhart, Derrick H. Lehmer, John L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$., Mathematics of computation **29** (1975), 620–647. ISSN 0025–5718. MR 52:5546.

[25] Duncan A. Buell, Jeremy T. Teitelbaum (editors), *Computational perspectives on number theory*, American Mathematical Society, Providence, 1998. MR 98g:11001.

[26] Joe P. Buhler (editor), *Algorithmic number theory: ANTS-III*, Lecture Notes in Computer Science, 1423, Springer-Verlag, Berlin, 1998. ISBN 3–540–64657–4. MR 2000g:11002.

[27] Qi Cheng, *Primality proving via one round in ECPP and one iteration in AKS* (2003). Available from `http://www.cs.ou.edu/~qcheng/`.

[28] David V. Chudnovsky, Gregory V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Advances in Applied Mathematics **7** (1986), 385–434. MR 88h:11094.

[29] Henri Cohen, Arjen K. Lenstra, *Implementation of a new primality test*, CWI Reports CS R8505, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1985; see also newer version [30]. MR 87a:11133.

[30] Henri Cohen, Arjen K. Lenstra, *Implementation of a new primality test*, Mathematics of Computation **48** (1987), 103–121; see also older version [29]. ISSN 0025–5718. MR 88c:11080.

[31] Henri Cohen, Hendrik W. Lenstra, Jr., *Primality testing and Jacobi sums*, Mathematics of Computation **42** (1984), 297–330. ISSN 0025–5718. MR 86g:11078.

[32] Stephen A. Cook, *On the minimum computation time of functions*, Ph.D. thesis, Department of Mathematics, Harvard University, 1966. Available from `http://cr.yp.to/bib/entries.html#1966/cook`.

[33] Ivan B. Damgård, Gudmund Skovbjerg Frandsen, *An extended quadratic Frobenius primality test with average and worst case error estimates* (2003). Available from `http://www.brics.dk/RS/03/9/index.html`.

[34] Michael R. Fellows, Neal Koblitz, *Self-witnessing polynomial-time complexity and prime factorization*, Designs, Codes and Cryptography **2** (1992), 231–235. ISSN 0925–1022. MR 93e:68032. Available from `http://cr.yp.to/bib/entries.html#1992/fellows`.

[35] Étienne Fouvry, *Théorème de Brun-Titchmarsh: application au théorème de Fermat*, Inventiones Mathematicae **79** (1985), 383–407. ISSN 0020–9910. MR 86g:11052.

[36] Jens Franke, T. Kleinjung, François Morain, T. Wirth, *Proving the primality of very large numbers with fastECPP*. Available from `ftp://lix.polytechnique.fr/pub/submissions/morain/Preprints/large.ps.gz`.

[37] Morris Goldfeld, *On the number of primes* p *for which* $p + a$ *has a large prime factor*, Mathematika **16** (1969), 23–27. ISSN 0025–5793. MR 39:5493.

[38] Shafi Goldwasser, Joe Kilian, *Almost all primes can be quickly certified*, in [2] (1986), 316–329; see also newer version [39].

[39] Shafi Goldwasser, Joe Kilian, *Primality testing using elliptic curves*, Journal of the ACM **46** (1999), 450–472; see also older version [38]. ISSN 0004–5411. MR 2002e:11182.

[40] Ronald L. Graham, Jaroslav Nešetřil (editors), *The mathematics of Paul Erdős. I*, Algorithms and Combinatorics, 13, Springer-Verlag, Berlin, 1997. ISBN 3–540–61032–4. MR 97f:00032.

[41] Jon Grantham, *A probable prime test with high confidence*, Journal of Number Theory **72** (1998), 32–47. ISSN 0022–314X. Available from `http://www.pseudoprime.com/jgpapers.html`.

[42] Jon Grantham, *Frobenius pseudoprimes*, Mathematics of Computation **70** (2001), 873–891. ISSN 0025–5718. Available from `http://www.pseudoprime.com/pseudo.html`.

[43] Louis C. Guillou, Jean-Jacques Quisquater (editors), *Advances in cryptology—EUROCRYPT '95 (Saint-Malo, 1995)*, Lecture Notes in Computer Science, 921, Springer-Verlag, Berlin, 1995. ISBN 3–540–59409–4. MR 96f:94001.

[44] Helmut Hasse, *Zur Theorie der abstrakten elliptischen Funktionenkörper I, II, III*, Journal für die Reine und Angewandte Mathematik (1936), 55–62, 69–88, 193–208. ISSN 0075–4102.

[45] Nicholas Howgrave-Graham, *Computational mathematics inspired by RSA*, Ph.D. thesis, 1998. Available from `http://dimacs.rutgers.edu/~dieter/Seminar/Papers/nick-thesis.ps`.

[46] Henryk Iwaniec, Matti Jutila, *Primes in short intervals*, Arkiv för Matematik **17** (1979), 167–176. MR 80j:10047.

[47] Erich Kaltofen, Thomas Valente, Noriko Yui, *An improved Las Vegas primality test*, in [3] (1989), 26–33. Available from `http://portal.acm.org/citation.cfm?doid=74540.74545`.

[48] Donald E. Knuth, *The analysis of algorithms*, in [1] (1971), 269–274. MR 54:11839. Available from `http://cr.yp.to/bib/entries.html#1971/knuth-gcd`.

[49] Sergei Konyagin, Carl Pomerance, *On primes recognizable in deterministic polynomial time*, in [40] (1997), 176–198. MR 98a:11184. Available from `http://cr.yp.to/bib/entries.html#1997/konyagin`.

[50] Derrick H. Lehmer, *Tests for primality by the converse of Fermat's theorem*, Bulletin of the American Mathematical Society **33** (1927), 327–340. ISSN 0273–0979.

[51] Derrick H. Lehmer, *An extended theory of Lucas' functions*, Annals of Mathematics **31** (1930), 419–448. ISSN 0003–486X.

[52] Derrick H. Lehmer, *Strong Carmichael numbers*, Journal of the Australian Mathematical Society Series A **21** (1976), 508–510. MR 54:5093.

[53] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., *Algorithms in number theory*, in [89] (1990), 673–715.

[54] Hendrik W. Lenstra, Jr., *Divisors in residue classes*, Mathematics of Computation **42** (1984), 331–340. ISSN 0025–5718. MR 85b:11118. Available from `http://www.jstor.org/sici?sici=0025-5718(198401)42:165<331:DIRC>2.0.CO;2-6`.

[55] Reynald Lercier, François Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, in [43] (1995), 79–94. MR 96h:11060.

[56] Edouard Lucas, *Sur la recherche des grands nombres premiers*, Association Française pour l'Avacement des Sciences. Comptes Rendus **5** (1876), 61–68.

[57] Edouard Lucas, *Considérations nouvelles sur la théorie des nombres premiers et sur la division géométrique de la circonférence en parties égales*, Association Française pour l'Avacement des Sciences. Comptes Rendus **6** (1877), 159–167.

[58] Richard F. Lukes, C. D. Patterson, Hugh C. Williams, *Numerical sieving devices: their history and some applications*, Nieuw Archief voor Wiskunde Series 4 **13** (1995), 113–139. ISSN 0028–9825. MR 96m:11082. Available from `http://cr.yp.to/bib/entries.html#1995/lukes`.

[59] Martin Macaj, *Some remarks and questions about the AKS algorithm and related conjecture* (2002). Available from `http://thales.doa.fmph.uniba.sk/macaj/aksremarks.pdf`.

[60] Preda Mihăilescu, *Cyclotomy primality proving—recent developments*, in [26] (1998), 95–110. MR 2000j:11195.

[61] Preda Mihailescu, Roberto M. Avanzi, *Efficient "quasi"-deterministic primality test improving AKS*. Available from `http://www-math.uni-paderborn.de/~preda/`.

[62] Gary L. Miller, *Riemann's hypothesis and tests for primality*, in [82] (1975), 234–239; see also newer version [63]. Available from `http://cr.yp.to/bib/entries.html#1975/miller`.

[63] Gary L. Miller, *Riemann's hypothesis and tests for primality*, Journal of Computer and System Sciences **13** (1976), 300–317; see also older version [62]. ISSN 0022–0000.

[64] Louis Monier, *Evaluation and comparison of two efficient probabilistic primality testing algorithms*, Theoretical Computer Science **12** (1980), 97–108. ISSN 0304–3975. MR 82a:68078.

[65] Hugh L. Montgomery, *Topics in multiplicative number theory*, Lecture Notes in Mathematics, 227, Springer-Verlag, Berlin, 1971. MR 49:2616.

[66] François Morain, *Implementation of the Atkin-Goldwasser-Kilian primality testing algorithm*, Research Report 911 (1988). Available from `http://www.lix.polytechnique.fr/~morain/Articles/articles.english.html`.

[67] François Morain, *Atkin's test: news from the front*, in [80] (1990), 626–635.

[68] François Morain, *Primality proving using elliptic curves: an update*, in [26] (1998), 111–127. MR 2000i:11190. Available from `http://www.lix.polytechnique.fr/~morain/Articles/articles.english.html`.

[69] Michael A. Morrison, John Brillhart, *A method of factoring and the factorization of F_7*, Mathematics of Computation **29** (1975), 183–205. ISSN 0025–5718. MR 51:8017.

[70] Siguna Müller, *On probable prime testing and the computation of square roots mod n*, in [21] (2000), 423–437; see also newer version [72]. MR 2002h:11140.

[71] Siguna Müller, *A probable prime test with very high confidence for $n \equiv 1 \bmod 4$*, in [23] (2001), 87–106. MR 2003j:11148.

[72] Siguna Müller, *A probable prime test with very high confidence for $n \equiv 3 \bmod 4$*, Journal of Cryptology **16** (2003), 117–139; see also older version [70]. ISSN 0933–2790. MR 1982973.

[73] Jozsef Pelikán, János Pintz, Endre Szemerédi, *On the running time of the Adleman-Pomerance-Rumely primality test*, Publicationes Mathematicae Debrecen **56** (2000), 523–534. MR 2001g:11147.

[74] János Pintz, William L. Steiger, Endre Szemerédi, *Infinite sets of primes with fast primality tests and quick generation of large primes*, Mathematics of Computation **53** (1989), 399–406. ISSN 0025–5718. MR 90b:11141.

[75] Henry C. Pocklington, *The determination of the prime or composite nature of large numbers by Fermat's theorem*, Proceedings of the Cambridge Philosophical Society **18** (1914), 29–30. ISSN 0305–0041.

[76] Carl Pomerance, *Are there counter-examples to the Baillie – PSW primality test?* (1984). Available from `http://www.pseudoprime.com/pseudo.html`.

[77] Carl Pomerance, *Very short primality proofs*, Mathematics of Computation **48** (1987), 315–322. ISSN 0025–5718. MR 88b:11088.

[78] Carl Pomerance, John L. Selfridge, Samuel S. Wagstaff, Jr., *The pseudoprimes to $25 \cdot 10^9$*, Mathematics of Computation **35** (1980), 1003–1026. ISSN 0025–5718. MR 82g:10030.

[79] Karl Prachar, *Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p-1$ haben*, Monatshefte für Mathematik **59** (1955), 91–97. ISSN 0026–9255. MR 16:904h.

[80] Jean-Jacques Quisquater, J. Vandewalle (editors), *Advances in cryptology—EUROCRYPT '89: workshop on the theory and application of cryptographic techniques, Houthalen, Belgium, April 10–13, 1989, proceedings*, Lecture Notes in Computer Science, 434, Springer-Verlag, Berlin, 1990. ISBN 3–540–53433–4. MR 91h:94003.

[81] Michael O. Rabin, *Probabilistic algorithms*, in [88] (1976), 21–39. MR 57:4603.

[82] William C. Rounds (chairman), *Proceedings of seventh annual ACM symposium on theory of computing: Albuquerque, New Mexico, May 5–7, 1975*, Association for Computing Machinery, New York, 1975.

[83] René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Mathematics of Computation **44** (1985), 483–494. ISSN 0025–5718. MR 86e:11122.

[84] René Schoof, *Counting points on elliptic curves over finite fields*, Journal de Théorie des Nombres de Bordeaux **7** (1995), 219–254. ISSN 1246–7405. Available from `http://almira.math.u-bordeaux.fr/jtnb/1995-1/schoof.ps`.

[85] John L. Selfridge, Marvin C. Wunderlich, *An efficient algorithm for testing large numbers for primality*, Congressus Numerantium **12** (1975), 109–120. ISSN 0384–9864. MR 51:5461.

[86] Robert M. Solovay, Volker Strassen, *A fast Monte-Carlo test for primality*, SIAM Journal on Computing **6** (1977), 84–85. ISSN 0097–5397. MR 55:2732.

[87] Andrei L. Toom, *The complexity of a scheme of functional elements realizing the multiplication of integers*, Soviet Mathematics Doklady **3** (1963), 714–716. ISSN 0197–6788.

[88] Joseph F. Traub (editor), *Algorithms and complexity: new directions and recent results*, Academic Press, New York, 1976. MR 54:14417.

[89] Jan van Leeuwen (editor), *Handbook of theoretical computer science, volume A*, Elsevier, Amsterdam, 1990. ISBN 0–444–88071–2. MR 92d:68001.

[90] Jacques Vélu, *Tests for primality under the Riemann hypothesis*, SIGACT **10** (1978), 58–59.

[91] André Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann et Cie., Paris, 1948. MR 10:262c.

[92] Hugh C. Williams, R. Holte, *Some observations on primality testing*, Mathematics of Computation **32** (1978), 905–917. ISSN 0025–5718.

[93] Hugh C. Williams, J. S. Judd, *Some algorithms for prime testing using generalized Lehmer functions*, Mathematics of Computation **30** (1976), 867–886. ISSN 0025–5718. MR 54:2574.

Department of Mathematics, Statistics, and Computer Science (M/C 249), The University of Illinois at Chicago, Chicago, IL 60607–7045

E-mail address: `djb@cr.yp.to`