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

DANIEL J. BERNSTEIN

		$1+o(1)$	$2+o(1)$	$3+o(1)$	$4+o(1)$	$5+o(1)$	$6+o(1)$	$O(1)$	$O(\lg\lg\lg n)$	big
	big	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$
	$O(1)$		1966	1966	1966	1966	1966	1966	1966	$-\infty$
	$2+o(1)$		1966	1966	1966	1966	1966	1966	1966	$-\infty$
rc	$o(1)$						2004	2002	1983	$-\infty$

		$1+o(1)$	$2+o(1)$	$3+o(1)$	$4+o(1)$	$5+o(1)$	$6+o(1)$	$O(1)$	$O(\lg\lg\lg n)$	big
	big	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$	$-\infty$
	$O(1)$				2004	2004	2004	2002	1983	$-\infty$
dc	$o(1)$						2004	2002	1983	$-\infty$

		$1+o(1)$	$2+o(1)$	$3+o(1)$	$4+o(1)$	$5+o(1)$	$6+o(1)$	$O(1)$	$O(\lg\lg\lg n)$	big
dpc							2004	2002	1983	$-\infty$

		$1+o(1)$	$2+o(1)$	$3+o(1)$	$4+o(1)$	$5+o(1)$	$6+o(1)$	$O(1)$	$O(\lg\lg\lg n)$	big
dp	$o(1)$						2004	2002	1983	$-\infty$
	big		1987	1914	1914	1914	1914	1914	1914	$-\infty$

		$1+o(1)$	$2+o(1)$	$3+o(1)$	$4+o(1)$	$5+o(1)$	$6+o(1)$	$O(1)$	$O(\lg\lg\lg n)$	big
rp	$o(1)$						2004	2002	1983	$-\infty$
	$2+o(1)$				2003	2003	2003	2002	1983	$-\infty$
	$O(1)$			1992	1992	1992	1992	1992	1983	$-\infty$
	big		1987	1914	1914	1914	1914	1914	1914	$-\infty$

		$1+o(1)$	$2+o(1)$	$3+o(1)$	$4+o(1)$	$5+o(1)$	$6+o(1)$	$O(1)$	$O(\lg\lg\lg n)$	big
?p	$o(1)$						2002	2002	1983	$-\infty$
	$2+o(1)$				2003	2003	2002	2002	1983	$-\infty$
	$4+o(1)$			1990	1990	1990	1990	1990	1983	$-\infty$
	$5+o(1)$			1988	1988	1988	1988	1988	1983	$-\infty$
	$O(1)$			1986	1986	1986	1986	1986	1983	$-\infty$
	big		1987	1914	1914	1914	1914	1914	1914	$-\infty$

Date: 2004.12.23. Permanent ID of this document: `d72f09ae5b05f41a53e2237c53f5f276`.

2000 *Mathematics Subject Classification.* Primary 11Y11.

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.

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 table in Section 2 of this paper has one row for each method, with five columns:

- "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**. This column includes various credits, such as "1986 [39] Goldwasser Kilian" for a method published in 1986 in [39] by Goldwasser and Kilian. When a method is published by one person with credit to another, the second person is named; for example, Lenstra and Lenstra in [56, Section 5.10] published a primality-proving method with credit to Shallit, so the table says "1990 [56, Section 5.10] Shallit."
- "Effect of certificate": what the method tells you about the target integer n. Either "proves primality" or "conjecturally certifies primality" or "proves compositeness." This column sometimes includes separate proof credits; for example, the table says "1936 [46] Hasse" for the Goldwasser-Kilian primality-proving method, because the primality proofs rely on a theorem published by Hasse in 1936.
- "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 a certificate for n. For example, $(\lg n)^{1+o(1)}$ or $(\lg n)^{2+o(1)}$ or $(\lg n)^{O(\lg \lg \lg n)}$. This column sometimes includes separate credits for proofs of, or improvements in, the speed of certificate verification; for example, the table says "1969 [38] Goldfeld" for the Agrawal-Kayal-Saxena primality-proving method, because the upper bound for certificate-verification time relies on a theorem published by Goldfeld in 1969.
- "Time to find certificate," at the same level of detail. The word "random" indicates a certificate-finding algorithm that uses randomness. This column sometimes includes separate credits; for example, the table says "1985 [86] Schoof" for the Goldwasser-Kilian primality-proving method, because the method finds certificates using an algorithm published by Schoof in 1985.

Complexity measures. When I say "time" in this paper, I mean "time on a 2-tape Turing machine, using fast subroutines for arithmetic."

A 2-tape Turing machine is a typical example of a conventional von Neumann computer. Extra tapes, random access to memory, etc. often save time, but not enough to matter at the level of detail of run times in this paper. I have followed the (questionable) tradition of measuring time and ignoring space.

Fast subroutines for arithmetic are surveyed in my paper [17]. In particular, integer multiplication, division, and gcd can be done in essentially linear time, as shown by Toom in [90], Cook in [33, pages 81–86], and Knuth in [51] respectively.

Beware that the primality/compositeness literature often uses quadratic-time subroutines for arithmetic—usually because the authors were writing before the essentially-linear-time algorithms were known, but sometimes because the authors inexplicably refused to take advantage of the essentially-linear-time algorithms. In every case I have retroactively substituted essentially-linear-time algorithms.

Information presented in the chart. A compressed chart appears on the first page of this paper, summarizing the results achieved by various methods. Thanks to Eric Bach for suggesting that I include a chart.

The chart is, conceptually, three-dimensional. The first dimension indicates what the certificates do—for example, prove primality—and how reliably the certificates are found; the second dimension indicates how quickly certificates are found; the third dimension indicates how quickly certificates are verified. Specifically:

- In the outer labels (rc, dc, dpc, dp, rp, ?p), "p" means that certificates prove primality; "c" means that certificates prove compositeness; "?" means that certificates are conjectured to be found for every n (every prime n for primality-proving methods, or every composite n for compositeness-proving methods); "r" means that certificates are provably found for every n; "d" means that certificates are provably deterministically found for every n. Certificates not believed to exist for every n are not included in the chart; certificates that are merely conjectured to imply primality are not included in the chart.
- The row labels ($o(1)$, $2+o(1)$, $4+o(1)$, $5+o(1)$, $O(1)$, big) are proven upper bounds for exponents in times to (provably deterministically, or provably randomly, or conjecturally) find certificates.
- The column labels ($1+o(1)$, $2+o(1)$, $\ldots$, $6+o(1)$, $O(1)$, $O(\lg\lg\lg n)$, big) are proven upper bounds for exponents in times to (provably deterministically) verify certificates.

Each chart entry is the publication year for a method achieving that combination of speed and results. For example, the entry 1992 at position $(\mathrm{rp}, O(1), 3+o(1))$ refers to a method published in 1992 that proves primality of every prime n, provably finds certificates (perhaps using randomness) in time $(\lg n)^{O(1)}$, and provably verifies certificates (deterministically) in time $(\lg n)^{3+o(1)}$: namely, the Adleman-Huang method in [4] of proving primality with genus-2-hyperelliptic-curve factors.

Often one cares only about the total time to find and verify certificates. Chart entries are separated by horizontal or vertical lines if their total times are different at this level of detail. For example, 1990 at position $(?\mathrm{p}, 4+o(1), 4+o(1))$ indicates that a method published in 1990 is conjectured to find and verify a certificate of primality in total time $(\lg n)^{4+o(1)}$; 2003 at position $(?\mathrm{p}, 2+o(1), 4+o(1))$ has the same total time $(\lg n)^{4+o(1)}$; there is no line separating these entries in the chart.

Here are the methods shown in the chart:

- $(\mathrm{dc}, \mathrm{big}, 1+o(1))$ $-\infty$, proving compositeness with factorization. Can also be used to prove primality: $(\mathrm{dpc}, o(1), \mathrm{big})$. "PRIMES is in coNP" refers to $(\mathrm{dc}, \mathrm{big}, O(1))$.
- $(\mathrm{dp}, \mathrm{big}, 3+o(1))$ 1914 [78] Pocklington, proving primality with unit-group factors. "PRIMES is in NP" refers to $(\mathrm{dp}, \mathrm{big}, O(1))$.
- $(\mathrm{rc}, 2+o(1), 2+o(1))$ 1966 [9] Artjuhov, proving compositeness with Fermat. "PRIMES is in coRP" refers to $(\mathrm{rc}, O(1), O(1))$.
- $(\mathrm{dpc}, o(1), O(\lg\lg\lg n))$ 1983 [5] Adleman Pomerance Rumely (announced in 1979), proving primality with unit-group factors.
- $(?\mathrm{p}, O(1), 3+o(1))$ 1986 [39] Goldwasser Kilian, proving primality with elliptic-curve factors.
- $(\mathrm{dp}, \mathrm{big}, 2+o(1))$ 1987 [80] Pomerance, proving primality with elliptic-curve factors.
- $(?\mathrm{p}, 5+o(1), 3+o(1))$ 1988 [69] Atkin, proving primality with elliptic-curve factors.
- $(?\mathrm{p}, 4+o(1), 3+o(1))$ 1990 [56, Section 5.10] Shallit, proving primality with elliptic-curve factors.
- $(\mathrm{rp}, O(1), 3+o(1))$ 1992 [4] Adleman Huang, proving primality with genus-2-hyperelliptic-curve factors. "PRIMES is in RP" refers to $(\mathrm{rp}, O(1), O(1))$.
- $(\mathrm{dpc}, o(1), O(1))$—"PRIMES is in P"—2002 [6] Agrawal Kayal Saxena, proving primality with combinatorics. Also $(?\mathrm{p}, o(1), 6+o(1))$.
- $(\mathrm{rp}, 2+o(1), 4+o(1))$ 2003 [18] Bernstein, proving primality with combinatorics.
- $(\mathrm{dpc}, o(1), 6+o(1))$ 2004 [44, Section 7] Lenstra Pomerance (announced in 2003.03), proving primality with combinatorics. Can also be used to prove compositeness: $(\mathrm{dc}, 6+o(1), 4+o(1))$.

The chart poses several challenges. For example, can we find an $(\mathrm{rp}, \mathrm{big}, 1+o(1))$ algorithm—an algorithm that verifies a certificate of primality in essentially linear time? Similarly, can we find an $(\mathrm{rc}, O(1), 1+o(1))$ algorithm—an algorithm that finds certificates of compositeness in polynomial time and verifies them in essentially linear time? Can we find a $(?\mathrm{p}, 3+o(1), 3+o(1))$ algorithm—an algorithm that proves primality in, conjecturally, essentially cubic time?

Different perspectives. This paper discusses time at a particular level of detail—not always enough detail to figure out which method is fastest. Is proving primality with combinatorics faster than proving primality with elliptic-curve factors? To answer this question, one needs to carry out a more detailed run-time analysis; what this paper says is that the first method (provably) takes essentially quartic time, and that the second method (conjecturally) takes essentially quartic time.

This paper's viewpoint is ruthlessly asymptotic, considering only what happens for *extremely large* values of n. For example, any constant is viewed as being better than $\lg\lg\lg n$. But $\lg\lg\lg n$ is actually rather small for *reasonable* values of n. Is proving primality with unit-group factors faster, for reasonable values of n, than proving primality with elliptic-curve factors? The exponent bounds $O(\lg\lg\lg n)$

and $4 + o(1)$ are of no use in answering this question; one needs a much more detailed run-time analysis.

Small values of n also raise interest in "non-uniform" algorithms: algorithms that perform precomputations for a range of inputs n, with the precomputation time measured separately. For example, a positive integer n below 2^{48} is prime if and only if it is a 2-sprp, 3-sprp, 5-sprp, 7-sprp, 11-sprp, 13-sprp, and 17-sprp; Jaeschke in [49] proved this by a large computation. The test of [61, Theorem 2] is somewhat less efficient but uses less precomputation; this test, in combination with a large "pseudosquare" computation by Williams and Wooding using my algorithm in [15, Section 4], now allows primes up to 2^{100} to be quickly proven prime.

This paper focuses primarily on upper bounds for time. Some algorithms, for some inputs, take much less time than the upper bounds indicate. For example, for *many* primes n, Pocklington's 1914 method finds a certificate of primality for n in polynomial time and verifies the certificate in essentially quadratic time. This set of primes n has been considerably expanded, thanks to an application of lattice-basis reduction by Lenstra, Konyagin, Pomerance, Coppersmith, Howgrave-Graham, and Nagaraj; see my exposition [19, Section 5], or the original papers [57], [52], and [47, Section 5.5]. This information is absent from the chart in this paper, and is covered only briefly in the table.

2. 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 [7] Alford Granville Pomerance)	$(\lg n)^{2+o(1)}$	random $(\lg n)^{2+o(1)}$

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
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 [9] Artjuhov)	proves compositeness	every composite n	$(\lg n)^{2+o(1)}$	random $(\lg n)^{2+o(1)}$ (1976 [84] Rabin, independently 1980 [67] Monier, independently 1982 [11] Atkin Larson; inferior variant: 1976 [55] Lehmer, independently 1977 [89] Solovay Strassen; other variants: 1998 [42] Grantham, 2001 [43] Grantham, 2000 [73] Müller, 2001 [74] Müller, 2003 [34] Damgard Frandsen)
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 [65] Miller)	conjecturally certifies primality; conjecture follows from GRH (1985 [13] Bach; $35 \lceil \lg n \rceil^2$ announced but not proven 1979 Oesterlé; $O(\lceil \lg n \rceil^2)$, without explicit O constant: 1952 [8] Ankeny, 1971 [68] Montgomery, 1978 [94] Vélu)	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: 1995 [61, Theorem 2] Lukes Patterson Williams)	conjecturally certifies primality	every prime n	$(\lg n)^{3+o(1)}$	instant

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
if n is a 2-sprp and passes a similar quadratic test, then n seems to be prime (1980 [14] Baillie Wagstaff, 1980 [81] Pomerance Selfridge Wagstaff; variant also including a cubic test: 1998 [10] Atkin)	conjecturally certifies primality; conjecture is implausible for very large n (1984 [79] Pomerance), but no counterexamples are known	every prime n	$(\lg n)^{2+o(1)}$	instant
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 [59] [60] Lucas, except that the switch from "divisor $q > 1$" to "prime divisor q" is from 1927 [53] Lehmer by analogy to 1914 [78] Pocklington)	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 [78] Pocklington); 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 [77] Pintz Steiger Szemeredi; variant: 1992 [35] Fellows Koblitz; another variant: 1997 [52] Konyagin Pomerance)

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
Pocklington-type test with quadratic extensions of $\mathbf{Z}/n$ (1876 [59] Lucas, 1930 [54] Lehmer, 1975 [72] Morrison, 1975 [88] Selfridge Wunderlich, 1975 [25] Brillhart Lehmer Selfridge)	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
Pocklington-type test with higher-degree extensions of $\mathbf{Z}/n$ (degrees 4 and 6: 1976 [97] Williams Judd; general degrees: 1983 [5] Adleman Pomerance Rumely)	proves primality	every prime n	$(\lg n)^{O(\lg\lg\lg n)}$, using distribution of divisors of $n^d - 1$ (1983 [5] Odlyzko Pomerance; weaker bound: 1955 [82] Prachar; best known bound: 2000 [76] Pelikan Pintz Szemeredi); many speedups available (1978 [96] Williams Holte, 1984 [32] Cohen Lenstra, 1985 [30] Cohen Lenstra, 1990 [23] Bosma van der Hulst, 1998 [63] Mihăilescu)	instant
proving primality with elliptic-curve factors: similar test using elliptic curves (1986 [39] Goldwasser Kilian)	proves primality, using bounds on elliptic-curve sizes (1936 [46] Hasse)	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 [86] Schoof); many speedups available (1995 [87] Atkin Elkies; 1995 [58] Lercier Morain)

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
similar test with elliptic curves having order divisible by a large power of 2 (1987 [80] Pomerance)	proves primality, using bounds on elliptic-curve sizes (1936 [46] Hasse)	every prime n	$(\lg n)^{2+o(1)}$	very slow
similar test with Jacobians of genus-2 hyperelliptic curves (1992 [4] Adleman Huang)	proves primality, using bounds on Jacobian sizes (1948 [95] Weil)	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 [48] Iwaniec Jutila), and distribution of Jacobian sizes (1992 [4] Adleman Huang)
similar test with small-discriminant complex-multiplication elliptic curves (1988 [69] Atkin; special cases: 1985 [21] Bosma, 1986 [29] Chudnovsky Chudnovsky)	proves primality, using bounds on elliptic-curve sizes (1936 [46] Hasse)	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 [56, Section 5.10] Shallit)	proves primality, using bounds on elliptic-curve sizes (1936 [46] Hasse)	conjecturally, every prime n	at most $(\lg n)^{3+o(1)}$	at most $(\lg n)^{4+o(1)}$; many speedups available (1988 [69] Morain, 1989 [50] Kaltofen Valente Yui, 1990 [70] Morain, 1993 [12] Atkin Morain, 1998 [71] Morain, 2003 [37] Franke Kleinjung Morain Wirth)

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 [6] Agrawal Kayal Saxena)	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 [38] Goldfeld); 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 [36] Fouvry); conjecturally $(\lg n)^{6+o(1)}$	instant
variant using arbitrary cyclotomic extensions (2003.01 [16, Theorem 2.3] Lenstra)	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 [62] Macaj, 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

Method	Effect of certificate	Certificate exists for	Time to verify certificate	Time to find certificate
variant using random Kummer extensions (2003.01 [18] Bernstein; independently 2003.03 [64] Mihăilescu Avanzi; idea and 2-power-degree case: 2002.12 [20] Berrizbeitia; prime-degree case: 2003.01 [28] Cheng)	proves primality	every prime n	$(\lg n)^{4+o(1)}$, using distribution of divisors of $n^d - 1$ (overkill: 1983 [5] Odlyzko Pomerance)	random $(\lg n)^{2+o(1)}$
variant using Gaussian periods (2004 [44, Section 7] Lenstra Pomerance)	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). URL: `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 [26] (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. URL: `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, *Doubly focused enumeration of locally square polynomial values*, in [92] (2004), 69–76. URL: `http://cr.yp.to/papers.html#focus`. ID `b4795a4f12863c26de5b7afe9296ffd8`.

[16] Daniel J. Bernstein, *Proving primality after Agrawal-Kayal-Saxena*. URL: `http://cr.yp.to/papers.html#aks`.

[17] Daniel J. Bernstein, *Fast multiplication and its applications*, to appear in Buhler-Stevenhagen *Algorithmic number theory* book. URL: `http://cr.yp.to/papers.html#multapps`. ID `8758803e61822d485d54251b27b1a20d`.

[18] Daniel J. Bernstein, *Proving primality in essentially quartic random time*, submitted. URL: `http://cr.yp.to/papers.html#quartic`. ID `43f1d5199196c0593c1e8442af682180`.

[19] Daniel J. Bernstein, *Reducing lattice bases to find small-height values of univariate polynomials*, to appear in Buhler-Stevenhagen *Algorithmic number theory* book. URL: `http://cr.yp.to/papers.html#smallheight`. ID `82f82c041b7e2bdce94a5e1f94511773`.

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

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

[22] 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.

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

[24] 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.

[25] 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.

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

[27] 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.

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

[29] 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.

[30] 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 [31]. MR 87a:11133.

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

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

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

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

[35] 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. URL: `http://cr.yp.to/bib/entries.html#1992/fellows`.

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

[37] Jens Franke, T. Kleinjung, François Morain, T. Wirth, *Proving the primality of very large numbers with fastECPP*. URL: `http://www.lix.polytechnique.fr/Labo/Francois.Morain/Articles/large.ps.gz`.

[38] 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.

[39] Shafi Goldwasser, Joe Kilian, *Almost all primes can be quickly certified*, in [2] (1986), 316–329; see also newer version [40].

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

[41] 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.

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

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

[44] Andrew Granville, *It is easy to determine whether a given integer is prime*, Bulletin of the American Mathematical Society **42** (2005), 3–38; online in 2004. ISSN 0273–0979.

[45] 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.

[46] 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.

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

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

[49] Gerhard Jaeschke, *On strong pseudoprimes to several bases*, Mathematics of Computation **61** (1993), 915–926. ISSN 0025–5718. MR 94d:11004.

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

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

[52] Sergei Konyagin, Carl Pomerance, *On primes recognizable in deterministic polynomial time*, in [41] (1997), 176–198. MR 98a:11184. URL: `http://cr.yp.to/bib/entries.html#1997/konyagin`.

[53] 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.

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

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

[56] Arjen K. Lenstra, Hendrik W. Lenstra, Jr., *Algorithms in number theory*, in [93] (1990), 673–715. URL: `http://cr.yp.to/bib/entries.html#1990/lenstra-survey`.

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

[58] Reynald Lercier, François Morain, *Counting the number of points on elliptic curves over finite fields: strategies and performances*, in [45] (1995), 79–94. MR 96h:11060.

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

[60] 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.

[61] 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. URL: `http://cr.yp.to/bib/entries.html#1995/lukes`.

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

[63] Preda Mihăilescu, *Cyclotomy primality proving—recent developments*, in [27] (1998), 95–110. MR 2000j:11195.

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

[65] Gary L. Miller, *Riemann's hypothesis and tests for primality*, in [85] (1975), 234–239; see also newer version [66]. URL: `http://cr.yp.to/bib/entries.html#1975/miller`.

[66] Gary L. Miller, *Riemann's hypothesis and tests for primality*, Journal of Computer and System Sciences **13** (1976), 300–317; see also older version [65]. ISSN 0022–0000.

[67] 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.

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

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

[70] François Morain, *Atkin's test: news from the front*, in [83] (1990), 626–635.

[71] François Morain, *Primality proving using elliptic curves: an update*, in [27] (1998), 111–127. MR 2000i:11190. URL: `http://www.lix.polytechnique.fr/~morain/Articles/articles.english.html`.

[72] 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.

[73] Siguna Müller, *On probable prime testing and the computation of square roots mod* n, in [22] (2000), 423–437; see also newer version [75]. MR 2002h:11140.

[74] Siguna Müller, *A probable prime test with very high confidence for* $n \equiv 1 \bmod 4$, in [24] (2001), 87–106. MR 2003j:11148.

[75] 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 [73]. ISSN 0933–2790. MR 1982973.

[76] 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.

[77] 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.

[78] 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.

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

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

[81] 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.

[82] 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.

[83] 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.

[84] Michael O. Rabin, *Probabilistic algorithms*, in [91] (1976), 21–39. MR 57:4603.

[85] 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.

[86] René J. 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.

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

[88] 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.

[89] 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.

[90] 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.

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

[92] Alf van der Poorten, Andreas Stein (editors), *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, American Mathematical Society, Providence, 2004. ISBN 0–8218–3353–7. MR 2005b:11003.

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

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

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

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

[97] 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`