



WIKIPEDIA
The Free Encyclopedia

[Main page](#)
[Contents](#)
[Featured content](#)
[Current events](#)
[Random article](#)
[Donate to Wikipedia](#)
[Wikipedia store](#)

Interaction

[Help](#)
[About Wikipedia](#)
[Community portal](#)
[Recent changes](#)
[Contact page](#)


Tools

[What links here](#)
[Related changes](#)
[Upload file](#)
[Special pages](#)
[Permanent link](#)
[Page information](#)
[Wikidata item](#)
[Cite this page](#)

Print/export

[Create a book](#)
[Download as PDF](#)
[Printable version](#)


Languages

 [Add links](#)

[Create account](#) [Log in](#)

Article [Talk](#)

[Read](#) [Edit](#) [View history](#)



Baillie–PSW primality test

From Wikipedia, the free encyclopedia
(Redirected from [Baillie-PSW primality test](#))

The **Baillie–PSW primality test** is a [probabilistic primality testing](#) algorithm that determines if a number is [composite](#) or a [probable prime](#). It is named after Robert Baillie, [Carl Pomerance](#), [John Selfridge](#), and [Samuel Wagstaff](#).

The Baillie-PSW test is a combination of a [strong Fermat probable prime](#) test to base 2 and a strong [Lucas probable prime](#) test. The Fermat and Lucas test each has its own list of pseudoprimes, that is, *composite* numbers that pass the primality test. For example, the first ten strong pseudoprimes to base 2 are

2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, and 52633 (sequence [A001262](#) in [OEIS](#)).

The first ten strong Lucas pseudoprimes (with Lucas parameters $P = 1$, $Q = -1$) are

5459, 5777, 10877, 16109, 18971, 22499, 24569, 25199, 40309, and 58519 (sequence [A217255](#) in [OEIS](#)).

The power of the Baillie-PSW test comes from the fact that these lists of strong Fermat pseudoprimes and strong Lucas pseudoprimes have *no known* overlap. There is even evidence that the numbers in these lists tend to be *different kinds* of numbers. For example, pseudoprimes base 2 tend to fall into the residue class 1 (mod m) for many small m , whereas Lucas pseudoprimes tend to fall into the residue class -1 (mod m).^{[1]:§6[2]:Table 2 & §5} As a result, a number that passes both a strong Fermat and a strong Lucas test is very likely to be prime.

No composite number below 2^{64} (approximately $1.845 \cdot 10^{19}$) passes the Baillie-PSW test.^[3] Consequently, this can be considered a deterministic primality test on numbers below that bound. There are also no *known* composite numbers above that bound that pass the test.

In 1980 the authors Pomerance, Selfridge, and Wagstaff offered \$30 for the discovery of a counterexample, that is, a composite number that passed this test. [Richard Guy](#) incorrectly stated that the value of this prize had been raised to \$620, but he was confusing the [Lucas sequence](#) with the [Fibonacci sequence](#), and his remarks really apply only to a [Conjecture of Selfridge's](#).^[4] As of June 2014 the prize remains unclaimed. However, a heuristic argument by Pomerance suggests that there are infinitely many counterexamples.^[5] Moreover, Chen and Greene ^[6] ^[7] have constructed a set S of 1248 primes such that, among the nearly 2^{1248} products of distinct primes in S , there *may* be about 740 counterexamples. However, they are talking about a weaker Baillie-PSW test that substitutes a Fibonacci test for the Lucas one.

Contents [\[hide\]](#)

- [1 The test](#)
- [2 The danger of relying only on Fermat tests](#)
- [3 Applications of combined Fermat and Lucas primality tests](#)
- [4 References](#)
- [5 Further reading](#)

The test [\[edit\]](#)

Let n be the odd positive integer that we wish to test for primality.

- Optionally, perform [trial division](#) to check if n is divisible by a small [prime number](#) less than some convenient limit.
- Perform a base 2 [strong probable prime](#) test. If n is not a strong probable prime base 2, then n is composite; quit.
- Find the first D in the sequence 5, -7, 9, -11, 13, -15, ... for which the [Jacobi symbol](#) (D/n) is -1 . Set $P = 1$ and $Q = (1 - D) / 4$.
- Perform a strong [Lucas probable prime](#) test on n using parameters D , P , and Q . If n is not a strong Lucas probable prime, then n is composite. Otherwise, n is almost certainly prime.

Remarks.

- The first step is for efficiency only. The Baillie-PSW test works without this step, but if n has small prime factors, then the quickest way to show that n is composite is to find a factor by trial division.

2. The second step is a single application of the [Miller-Rabin primality test](#). There is nothing special about using base 2; other bases might work just as well. However, much work has been done (see above) to verify that the combination of the base 2 strong probable prime test and a strong Lucas test does a good job of distinguishing primes from composites.
3. Baillie and Wagstaff proved in Theorem 9 on page 1413 of [\[2\]](#) that the average number of D s that must be tried is about 3.147755149.
4. If n is a perfect square, then step 3 will never yield a D with $(D/n) = -1$; this is not a problem because perfect squares are easy to detect using [Newton's method](#) for square roots. If step 3 fails to produce a D quickly, one should check whether n is a perfect square.
5. Given n , there are other methods for choosing D , P , and Q .[\[2\]:1401, 1409](#) What is important is that the Jacobi symbol (D/n) be -1 . Bressoud and Wagon explain why we want the Jacobi symbol to be -1 , as well as why one gets more powerful primality tests if $Q \neq \pm 1$.[\[8\]:266–269](#)
6. If $Q \neq \pm 1$, there are additional tests that can be performed at almost no extra computational cost. After one has computed the powers of Q and the terms in the Lucas sequences that are used in the strong Lucas probable prime test, these additional primality conditions provide further opportunities to show that n is composite; see Section 6 of [\[2\]](#)
7. There are weaker versions of the Baillie-PSW test, and this one is sometimes referred to as the *Strong* Baillie-PSW test.
8. If the Lucas test is replaced by a Fibonacci test, then it shouldn't be called a Baillie-PSW test, but rather a Selfridge test or a PSW test. See [Selfridge's Conjecture on Primality Testing](#).
9. Pomerance, Selfridge and Wagstaff offered \$30 in 1980 for a composite number passing a weaker version of the Baillie-PSW test. Such a number passing the (strong) Baillie-PSW test would qualify.[\[1\]](#)

The danger of relying only on Fermat tests [\[edit\]](#)

There is significant overlap among the lists of pseudoprimes to different bases.

Choose a base a . If n is a pseudoprime to base a , then n is likely to be one of those few numbers that is a pseudoprime to many bases.[\[9\]](#)

For example, $n = 341$ is a pseudoprime to base 2. It follows from Theorem 1 on page 1392 of [\[2\]](#) that there are 100 values of $a \pmod{341}$ for which 341 is a pseudoprime base a . (The first ten such a are 1, 2, 4, 8, 15, 16, 23, 27, 29, and 30). The proportion of such a compared to n is usually much smaller.

Therefore, if n is a pseudoprime to base a , then n is more likely than average to be a pseudoprime to some other base.[\[1\]:1020](#) For example, there are 21853 pseudoprimes to base 2 up to $25 \cdot 10^9$. This is only about two out of every million odd integers in this range. However:[\[1\]:1021](#)

- 4709 of these 21853 numbers (over 21 percent) are also pseudoprimes to base 3; (and to all 3-smooth base)
- 2522 of these 4709 numbers (over 53 percent) are pseudoprimes to bases 2, 3, and 5; (and to all 5-smooth base)
- 1770 of these 2522 numbers (over 70 percent) are pseudoprimes to bases 2, 3, 5, and 7. (and to all 7-smooth base)

29341 is the smallest pseudoprime to bases 2 to 10. (and to all 7-smooth base) This suggests that probable prime tests to different bases are not independent of each other, so that performing Fermat probable prime tests to more and more bases will give diminishing returns. On the other hand, the calculations up to 2^{64} , mentioned above, suggest that Fermat and Lucas probable prime tests *are* independent,[\[2\]:1400](#) so that a *combination* of these types of tests would make a powerful primality test, especially if the *strong* forms of the tests are used.

There is also overlap among *strong* pseudoprimes to different bases. For example, 1373653 is the smallest strong pseudoprime to bases 2 to 4 (and to all 3-smooth base), and 3215031751 is the smallest strong pseudoprime to bases 2 to 10 (and to all 7-smooth base). Arnault [\[10\]](#) gives a 397-digit composite number N that is a *strong* pseudoprime to *all* bases less than 307. (and to all 293-smooth base) Because this N is a [Carmichael number](#), N is also a (not necessarily strong) pseudoprime to all bases less than p , where p is the 131-digit smallest prime factor of N . A quick calculation shows that N is *not* a Lucas probable prime when D , P , and Q are chosen by the method described above, so this number would be correctly determined by the Baillie-PSW test to be composite.

Applications of combined Fermat and Lucas primality tests [\[edit\]](#)

The following computer algebra systems and software packages use some version of the Baillie-PSW primality

test.

Maple's `isprime` function,^[11] Mathematica's `PrimeQ` function,^[12] PARI/GP's `isprime` and `ispseudoprime` functions,^[13] and Sage's `is_pseudoprime` function^[14] all use a combination of a Miller-Rabin (Fermat strong probable prime) test and a Lucas test. Maxima's `primep` function uses such a test for numbers greater than 341550071728321.^[15]

The FLINT library has functions `n_is_probabprime` and `n_is_probabprime_BPSW` that use a combined test, as well as other functions that perform Fermat and Lucas tests separately.^[16]

The `BigInteger` class in standard versions of Java and in open-source implementations like OpenJDK, has a method called `isProbablePrime`. This method does one or more Miller-Rabin tests with random bases. If n , the number being tested, has 100 bits or more, this method also does a *non-strong* Lucas test that checks whether U_{n+1} is 0 (mod n).^[17]^[18] The use of random bases in the Miller-Rabin tests has an advantage and a drawback compared to doing a single base 2 test as specified in the Baillie–PSW test. The advantage is that, with random bases, one can get a bound on the probability that n is composite. The drawback is that, unlike the Baillie–PSW test, one cannot say with certainty that if n is less than some fixed bound such as 2^{64} , then n is prime.

In Perl, the `Math::Primality`^[19] and `Math::Prime::Util`^{[20][21]} modules have functions to perform the strong Baillie-PSW test as well as separate functions for strong pseudoprime and strong Lucas tests. In Python, the `NZMATH`^[22] library has the strong pseudoprime and Lucas tests, but does not have a combined function.

GNU Multiple Precision Arithmetic Library's `mpz_probab_prime_p` function uses a Miller-Rabin test, but does not appear to use a Lucas test.^[23] Magma's `IsProbablePrime` and `IsProbablyPrime` functions use 20 Miller-Rabin tests for numbers $> 34 \cdot 10^{13}$, but do not combine them with a Lucas probable prime test.^[24]

References ^[edit]

- ^a ^b ^c ^d Carl Pomerance; John L. Selfridge; Samuel S. Wagstaff, Jr. (July 1980). "The pseudoprimes to $25 \cdot 10^9$ ". *Mathematics of Computation* **35** (151): 1003–1026. doi:10.1090/S0025-5718-1980-0572872-7.
- ^a ^b ^c ^d ^e ^f Robert Baillie; Samuel Wagstaff (October 1980). "Lucas Pseudoprimes". *Mathematics of Computation* **35** (152): 1391–1417. doi:10.1090/S0025-5718-1980-0583518-6. MR 583518.
- ^a "The Baillie-PSW Primality Test". Thomas R. Nicely. Retrieved 2013-03-17.
- ^a Guy, R. (1994). "Pseudoprimes. Euler Pseudoprimes. Strong Pseudoprimes." §A12 in *Unsolved Problems in Number Theory*. 2nd ed., p. 28, New York: Springer-Verlag. ISBN 0-387-20860-7.
- ^a Pomerance, C. (1984), *Are There Counterexamples to the Baillie-PSW Primality Test?* (PDF)
- ^a Baillie-PSW John R. Greene's website.
- ^a Zhuo Chen; John Greene (August 2003). "Some Comments on Baillie-PSW Pseudoprimes" (PDF). *The Fibonacci Quarterly* **41** (4): 334–344.
- ^a David Bressoud; Stan Wagon (2000). *A Course in Computational Number Theory*. New York: Key College Publishing in cooperation with Springer. ISBN 978-1-930190-10-8.
- ^a Samuel S. Wagstaff, Jr. (1982). "Pseudoprimes and a generalization of Artin's conjecture". *Acta Arithmetica* **41** (2): 141–150.
- ^a F. Amault (August 1995). "Constructing Carmichael Numbers Which Are Strong Pseudoprimes to Several Bases" . *Journal of Symbolic Computation* **20** (2): 151–161. doi:10.1006/jsco.1995.1042.
- ^a `isprime` - Maple Help documentation at maplesoft.com.
- ^a *Some Notes on Internal Implementation-Wolfram Mathematica 9 Documentation* documentation at wolfram.com.
- ^a *User's Guide to PARI/GP (version 2.5.1)* documentation for PARI/GP.
- ^a *Sage Reference Manual Release 5.7* documentation for Sage.
- ^a *Maxima Manual Ver. 5.28.0* documentation for Maxima.
- ^a FLINT: Fast Library for Number Theory documentation for FLINT 2.3.0.
- ^a `BigInteger.java` DocJar: Search Open Source Java API.
- ^a `BigInteger.java` documentation for OpenJDK.
- ^a `Math::Primality` Perl module with BPSW test
- ^a `Math::Prime::Util` Perl module with primality tests including BPSW
- ^a `Math::Prime::Util::GMP` Perl module with primality tests including BPSW, using C+GMP
- ^a `NZMATH` number theory calculation system in Python
- ^a *Prime Testing Algorithm - GNU MP 5.1.1* documentation for GMP.
- ^a *Magma Computational Algebra System - Primes and Primality Testing* documentation for Magma.

Further reading ^[edit]

- Nicely, Thomas R., *The Baillie-PSW primality test*.
- Weisstein, Eric W., "Baillie-PSW Primality Test" ; *MathWorld*.

v · t · e	Number-theoretic algorithms [hide]
Primality tests	AKS test · APR test · Baillie–PSW · ECPP test · Elliptic curve · Pocklington · Fermat · Lucas · <i>LUCAS–LEHMER</i> · <i>LUCAS–LEHMER–RIESEL</i> · <i>PROTH'S THEOREM</i> · <i>PÉPIN'S</i> · Quadratic Frobenius test · Solovay–Strassen · Miller–Rabin
Prime-generating	Sieve of Atkin · Sieve of Eratosthenes · Sieve of Sundaram · Wheel factorization
Integer factorization	Continued fraction (CFRAC) · Dixon's · Lenstra elliptic curve (ECM) · Euler's · Pollard's rho · $p - 1$ · $p + 1$ · Quadratic sieve (QS) · General number field sieve (GNFS) · <i>Special number field sieve (SNFS)</i> · Rational sieve · Fermat's · Shanks' square forms · Trial division · Shor's
Multiplication	Ancient Egyptian · Long · Karatsuba · Toom–Cook · Schönhage–Strassen · Fürer's
Discrete logarithm	Baby-step giant-step · Pollard rho · Pollard kangaroo · Pohlig–Hellman · Index calculus · Function field sieve
Greatest common divisor	Binary · Euclidean · Extended Euclidean · Lehmer's
Modular square root	Cipolla · Pocklington's · Tonelli–Shanks
Other algorithms	Chakravala · Cornacchia · Integer relation · Integer square root · Modular exponentiation · Schoof's
<i>Italics</i> indicate that algorithm is for numbers of special forms · Smallcaps indicate a deterministic algorithm	

Categories: Primality tests

This page was last modified on 1 September 2015, at 07:34.

Text is available under the Creative Commons Attribution-ShareAlike License; additional terms may apply. By using this site, you agree to the Terms of Use and Privacy Policy. Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a non-profit organization.

Privacy policy About Wikipedia Disclaimers Contact Wikipedia Developers Mobile view

