

RABIN-MILLER PRIMALITY TEST: COMPOSITE NUMBERS WHICH PASS IT

F. ARNAULT

ABSTRACT. The Rabin-Miller primality test is a probabilistic test which can be found in several algebraic computing systems (such as Pari, Maple, Scratch-Pad) because it is very easy to implement and, with a reasonable amount of computing, indicates whether a number is composite or “probably prime” with a very low probability of error. In this paper, we compute composite numbers which are strong pseudoprimes to several chosen bases. Because these bases are those used by the ScratchPad implementation of the test, we obtain, by a method which differs from a recent one by Jaeschke, composite numbers which are found to be “probably prime” by this test.

1. PRELIMINARIES

First, we recall the following definitions:

1.1. **Definitions.** Let $b \in \mathbb{N}^*$. A number $n \in \mathbb{N}^*$ is a pseudoprime to base b if

$$b^{n-1} \equiv 1 \text{ modulo } n.$$

It is a strong pseudoprime to base b if it is odd and if one of the following conditions is satisfied, with $n - 1 = 2^k q$ and q odd:

$$b^q \equiv 1 \text{ modulo } n$$

or

there exists an integer i such that $0 \leq i < k$ and $b^{2^i q} \equiv -1 \text{ modulo } n$.

The Rabin-Miller test consists in, given an odd number n , checking if n is a strong pseudoprime to several bases which are either chosen randomly or taken in a predetermined set, depending on the implementation. If n is not a strong pseudoprime to some of the chosen bases, n is proved to be composite. Conversely, Rabin has shown in [12] that if n is a strong pseudoprime to k bases, it is “probably prime” with an error probability of less than $1/4^k$. This test is implemented in the Computing Algebra System ScratchPad, in which the bases used are the first ten prime numbers 2, 3, 5, 7, 11, 13, 17, 19, 23, 29. In this paper, we compute a composite number which is a strong pseudoprime to these bases. So, this number passes the ScratchPad test. In order to show that

Received by the editor February 7, 1992 and, in revised form, October 15, 1992.

1991 *Mathematics Subject Classification.* Primary 11A15, 11A51, 11Y11.

Key words and phrases. Primality testing, strong pseudoprimes, biquadratic reciprocity.

© 1995 American Mathematical Society
0025-5718/95 \$1.00 + \$.25 per page

our method can be used with some other sets of prime bases, we successfully apply it to the set of all prime bases below 200.

2. BIQUADRATIC RECIPROCITY

It is an easy task, using quadratic reciprocity, to distinguish the primes p such that a fixed prime b is a square, or a nonsquare, modulo p . In a similar way, we will need sufficient conditions on a prime p congruent to 1 modulo 4 for another given prime number b to be a square but not a fourth power, modulo p . For this purpose, we will use the biquadratic reciprocity law, the statement of which can be found in [7] and which we recall here. Instead of its quadratic analogue, it involves the set $\mathbb{Z}[i]$ of Gaussian integers.

We say that a Gaussian integer is primary if it is congruent to 1 or to $3 + 2i$ modulo 4 and, for $z, \rho \in \mathbb{Z}[i]$ with ρ prime, we denote by $\left(\frac{z}{\rho}\right)_4$ the biquadratic power residue symbol of z modulo ρ . Note that this symbol is equal to 1 (resp. -1) if and only if z is a fourth power (resp. a square but not a fourth power) modulo ρ .

2.1. Theorem [7, Chapter 9, Theorem 2]. *Let $\pi, \rho \in \mathbb{Z}[i]$ be two primary and distinct primes; then the following relation holds:*

$$\left(\frac{\pi}{\rho}\right)_4 = (-1)^{\frac{N(\pi)-1}{4} \frac{N(\rho)-1}{4}} \left(\frac{\rho}{\pi}\right)_4.$$

We will also use the following “complementary law” as found in [4] (or see [7, Chapter 5, exercise 27]):

2.2. Proposition [4, Theorem 4.23]. *Let $\pi = r + is$ be a primary prime in $\mathbb{Z}[i]$; then*

$$\left(\frac{2}{\pi}\right)_4 = i^{rs/2}.$$

In order to find the sufficient conditions we referred to above, recall that a prime $p \equiv 1$ modulo 4 is the product $p = \pi\bar{\pi} = r^2 + s^2$ of two primes in $\mathbb{Z}[i]$, where $\pi = r + is$, and it is easily seen that π can be chosen primary, so that $\bar{\pi}$ is also primary. We also know that either the prime b is the product $\omega\bar{\omega}$ of two primary prime Gaussian integers, or $-b$ is a primary prime in $\mathbb{Z}[i]$, according as b is congruent to 1 or to 3 modulo 4. Since there is a canonical isomorphism between $\mathbb{Z}/(p)$ and $\mathbb{Z}[i]/(\pi)$, the number b is a square but not a fourth power modulo p if and only if it is such modulo π . We shall therefore need to find primary primes π such that $\left(\frac{b}{\pi}\right)_4 = -1$. We now give details of the use of biquadratic reciprocity.

• First consider the case where $b \equiv 3$ modulo 4. Since π and $-b$ are primary primes in $\mathbb{Z}[i]$, the biquadratic reciprocity law shows that

$$\begin{aligned} \left(\frac{-b}{\pi}\right)_4 &= (-1)^{\frac{b^2-1}{4} \frac{p-1}{4}} \left(\frac{\pi}{b}\right)_4 \\ &= \left(\frac{\pi}{b}\right)_4 \quad \text{since } b^2 \equiv 1 \text{ modulo } 8. \end{aligned}$$

So,

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{-1}{\pi}\right)_4 \left(\frac{-b}{\pi}\right)_4 = (-1)^{(p-1)/4} \left(\frac{\pi}{b}\right)_4.$$

Now b is a square, but not a fourth power modulo $p = N(\pi)$, if and only if the above quantity is equal to -1 . So if we find a primary Gaussian integer z which is a solution of

$$(A_3) \quad (-1)^{(N(z)-1)/4} \left(\frac{z}{b}\right)_4 = -1,$$

then any prime π congruent to z modulo $4b$ will also be a solution of (A_3) , and thus b will be a square but not a fourth power modulo $p = N(\pi)$.

• Next, the case where $b \equiv 1$ modulo 4 is studied (recall that we can write $b = \omega\bar{\omega}$, with ω primary). The biquadratic reciprocity law states that

$$\left(\frac{\omega}{\pi}\right)_4 = (-1)^{\frac{b-1}{4}\frac{p-1}{4}} \left(\frac{\pi}{\omega}\right)_4 \quad \text{and} \quad \left(\frac{\bar{\omega}}{\pi}\right)_4 = (-1)^{\frac{b-1}{4}\frac{p-1}{4}} \left(\frac{\pi}{\bar{\omega}}\right)_4.$$

The product of these equalities leads to

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{\pi}{\omega}\right)_4 \left(\frac{\pi}{\bar{\omega}}\right)_4.$$

As the symbols $\left(\frac{\pi}{\omega}\right)_4$ and $\left(\frac{\pi}{\bar{\omega}}\right)_4$ are the inverse of each other, the above equation becomes

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{\pi\bar{\pi}^{-1}}{\omega}\right)_4,$$

where $\bar{\pi}^{-1}$ denotes the inverse of $\bar{\pi}$ modulo b . Since b is a square but not a fourth power if and only if the symbol $\left(\frac{b}{\pi}\right)_4$ equals -1 , it remains to find primary solutions z of the equation

$$(A_1) \quad \left(\frac{z\bar{z}^{-1}}{\omega}\right)_4 = -1.$$

Then, any prime π congruent to such a z modulo $4b$ will be also a solution of (A_1) , and thus b will be a square but not a fourth power modulo $p = N(\pi)$.

3. COMPOSITE STRONG PSEUDOPRIMES TO SEVERAL BASES

Our first aim was to find composite numbers which are strong pseudoprimes to the ten bases used by ScratchPad. We are now able to do this. We choose to focus our attention on numbers n which are products of two primes p_1 and p_2 . Moreover, we will assume that these primes are related to each other by the following equalities:

$$p_1 = 2q + 1, \quad p_2 = 4q + 1 \quad \text{with } q \in \mathbb{Z}.$$

As a consequence, we have $n - 1 = (4q + 3)(p_1 - 1)$ and so, by Fermat's little theorem, $b^{n-1} \equiv 1$ modulo p_1 , provided that b is an integer prime to p_1 . Hence, n is a pseudoprime to base b if and only if $b^{n-1} \equiv 1$ modulo p_2 .

But we can also write $n - 1 = p_1(p_2 - 1) + (p_2 - 1)/2$, and so we have

$$b^{n-1} \equiv \left(\frac{b}{p_2}\right) \text{ modulo } p_2.$$

Thus, we can state the following lemma:

3.1. Lemma. *With the above notations, the number n is a pseudoprime to base b if and only if b is a square modulo p_2 .*

From now on, we assume that the conditions of this lemma are satisfied. We are now looking for further sufficient conditions for n to be a strong pseudo-prime to base b . Thus, an investigation of the value of $b^{\frac{n-1}{2}}$ modulo n allows us to state the following:

3.2. Lemma. *Let n , p_1 , p_2 be as in Lemma 3.1 and let $\pi \in \mathbb{Z}[i]$ be such that $p_2 = N(\pi)$. Then n is a strong pseudoprime to base b provided that the following conditions are satisfied:*

$$\left(\frac{b}{p_1}\right) = -1 \quad \text{and} \quad \left(\frac{b}{\pi}\right)_4 = -1;$$

i.e., b is a nonsquare modulo p_1 and a square but not a fourth power modulo p_2 .

Proof. We first note that, as $(n-1)/2 = (4q+3)(p_1-1)/2$, we have

$$b^{\frac{n-1}{2}} \equiv \left(\frac{b}{p_1}\right) \equiv b^{\frac{p_1-1}{2}} \pmod{p_1}.$$

So, the first equality of the statement gives $b^{\frac{n-1}{2}} \equiv -1 \pmod{p_1}$. We also have $(n-1)/2 = p_1(p_2-1)/2 + (p_2-1)/4$. This shows that (we recall that the conditions of 3.1 are assumed to be satisfied)

$$b^{\frac{n-1}{2}} \equiv b^{\frac{p_2-1}{4}} \pmod{p_2}.$$

Hence, the second equality of the statement gives $b^{\frac{n-1}{2}} \equiv -1 \pmod{\pi}$. As π and $\bar{\pi}$ are relatively prime, this is equivalent to $b^{\frac{n-1}{2}} \equiv -1 \pmod{p_2}$. Thus, both equalities give

$$b^{\frac{n-1}{2}} \equiv -1 \pmod{n},$$

which is a sufficient condition for n to be a strong pseudoprime to base b . \square

We will use quadratic and biquadratic reciprocity to find sufficient conditions (in terms of congruences over π in $\mathbb{Z}[i]$) for b to satisfy the conditions of Lemma 3.2.

First, the case $b = 2$ needs special treatment. By 2.2, the second equality of 3.2 is equivalent to $i^{\frac{p_2}{2}} = -1$ if we assume that $\pi = r + is$ is primary. This is equivalent to

$$\pi \equiv 1 + 4i \text{ or } 5 + 4i \pmod{8}.$$

Notice that $\pi \equiv 1 + 4i \pmod{8}$ implies $p_2 \equiv 1 \pmod{16}$, while $\pi \equiv 5 + 4i \pmod{8}$ implies $p_2 \equiv 9 \pmod{16}$. However, in order to also satisfy the first equality of 3.2, we must have $p_1 \equiv 3$ or $5 \pmod{8}$. Because of the connection between p_1 and p_2 , only the condition $\pi \equiv 5 + 4i \pmod{8}$ remains valid. We state this as a lemma:

3.3. Lemma. *Let n , p_1 , p_2 be as in Lemma 3.1 and assume that π is a primary prime in $\mathbb{Z}[i]$ such that $p_2 = N(\pi)$. The number n is a strong pseudo-prime to base 2 provided that π is congruent to $5 + 4i \pmod{8}$.*

We noticed in §2 that the second equality of 3.2 can be handled by finding solutions of (A_3) and (A_1) . In a similar way, the first equality of 3.2 is

TABLE 1

for $b = 2$:	$\pi \equiv 5 + 4i$		modulo 8
for $b = 3$:	$\pi \equiv$	$7 + 6i$	modulo 12
for $b = 7$:	$\pi \equiv 1 + 8i$	or $7 + 6i$	modulo 28
for $b = 11$:	$\pi \equiv 5 + 12i$	or $3 + 22i$	modulo 44
for $b = 13$:	$\pi \equiv 5 + 24i$	or $7 + 18i$	modulo 52
for $b = 17$:	$\pi \equiv 1 + 12i$	or $3 + 2i$	modulo 68
for $b = 19$:	$\pi \equiv 1 + 28i$	or $3 + 6i$	modulo 76
for $b = 23$:	$\pi \equiv 1 + 32i$	or $3 + 30i$	modulo 92
for $b = 29$:	$\pi \equiv 1 + 56i$	or $3 + 10i$	modulo 116

equivalent to

$$(-1)^{\frac{p_1-1}{2} \frac{b-1}{2}} \left(\frac{p_1}{b}\right) = -1.$$

Because of $p_1 = (N(\pi) + 1)/2$, this becomes

$$(-1)^{\frac{N(\pi)-1}{4} \frac{b-1}{2}} \left(\frac{(N(\pi) + 1)/2}{b}\right) = -1.$$

So, for any prime π congruent modulo $4b$ to a given solution z of

$$(B) \quad (-1)^{\frac{N(z)-1}{4} \frac{b-1}{2}} \left(\frac{(N(z) + 1)/2}{b}\right) = -1,$$

we will have $N(\pi) \equiv N(z)$ modulo $8b$ and $(N(\pi) + 1)/2 \equiv (N(z) + 1)/2$ modulo $4b$. Hence, π will be also a solution of (B), and thus the first equality of 3.2 will be satisfied.

Therefore, a common solution z of (A₃) and (B) (resp. of (A₁) and (B)), will be such that any prime π congruent to z modulo $4b$ will make true both conditions of 3.2. For example, consider the case $b = 7$. To find Gaussian integers τ which satisfy $(\frac{\tau}{7})_4 = -1$ is an easy task and we can take $\tau = 1 + i$. Because $z_1 = 1 + 8i$ is congruent to 1 modulo 4 and to $1 + i$ modulo 7, it is a solution of (A₃). Moreover, z_1 is also a solution of (B). Hence, with the notations of Lemma 3.2, the number n is a strong pseudoprime to base 7 provided that π is congruent to $1 + 8i$ modulo 28. The same reasoning holds for $z_2 = 7 + 6i$, which satisfies both equation (A₃) and (B).

Now, we explain the relevance of the part of the coset modulo 4 of the chosen z . Lemma 3.3 points out that if we want n to be a pseudoprime in both bases b and 2 ($b \neq 2$), we must choose solutions z for (A₃) and (B) (resp. for (A₁) and (B)) such that $z \equiv 1$ modulo 4 (as z_1 in the above example). If we choose $z \equiv 3 + 2i$ modulo 4 (as z_2), the conditions of Lemma 3.3 can no longer be satisfied. Moreover, we have in this case $p_2 \equiv 5$ modulo 8, so that 2 is a nonsquare modulo p_2 and by 3.1, the number n cannot in any way be a pseudoprime to base 2.

In Table 1 we give, for several values of b , sufficient conditions for n to be a strong pseudoprime to base b , which can be found following the above example.

This table shows, whenever possible, two solutions for equations (A₃) and (B) (resp. (A₁) and (B)). The solutions in the left-hand column are congruent

TABLE 2

$\pi \equiv 1 \pmod{12}$
$\pi \equiv 1 \pmod{20}$

to 1 modulo 4 and so are compatible with the conditions of Lemma 3.3, while the solutions in the right-hand column are congruent to $3 + 2i$ modulo 4 and so lead to numbers n which are not pseudoprimes to base 2.

Unfortunately, the bases 3 and 5 cannot be handled so easily. Indeed, if $b = 5$, then p_2 must be congruent to 1 or to 9 modulo 10 for 5 to be a square modulo p_2 . This makes p_1 congruent to 1, 5, 6, or 0 modulo 10. As p_1 is a prime, only the relation $p_1 \equiv 1 \pmod{10}$ is possible (except if $p_1 = 5$, which is not of interest). So 5 is therefore a square modulo p_1 which is contrary to what we want.

The case $b = 3$ is somewhat less recalcitrant. One can verify that a solution of (A_3) must belong to one of the four cosets $9 + 4i$, $9 + 8i$, $7 + 6i$, $11 + 6i$ modulo 12. If π belongs to one of the first two, we have $p_1 \equiv 1 \pmod{12}$, and so equation (B) is not satisfied. If π belongs to one of the last two, we have $p_1 \equiv 7 \pmod{12}$, and so equation (B) is satisfied but this no longer preserves compatibility with the conditions of Lemma 3.3. This explains why the left-hand column in row $b = 3$ of Table 1 has been left blank.

Hence, this method does not allow us to find strong pseudoprimes neither to base 5 nor to both bases 2 and 3.

However, a more heuristic method can handle these exceptions: the relations of Table 2 ensure that 3 and 5 are fourth powers modulo p_2 and squares modulo p_1 , so that

$$3^{\frac{n-1}{2}} \equiv 1 \pmod{n} \quad \text{and} \quad 5^{\frac{n-1}{2}} \equiv 1 \pmod{n},$$

which in particular makes n a pseudoprime to bases 3 and 5.

The eight conditions in the left-hand column of Table 1 and the two of Table 2 are mutually compatible and, applying the Chinese remainder theorem, we see that they are all satisfied provided that $\pi = r + is$ is such that

$$r \equiv r_0 = 11310652501 \quad \text{and} \quad s \equiv s_0 = 8996896140 \pmod{m = 25878772920}.$$

For example, we can take $r = r_0 + 8m$ and $s = s_0 + m$. In this case p_1 and p_2 are prime numbers, so

$$p_1 p_2 = 1195068768795265792518361315725116351898245581$$

is a strong pseudoprime to the bases 2, 7, 11, 13, 17, 19, 23, 29 and a pseudoprime to the bases 3 and 5. Moreover, luckily, this number is also a strong pseudoprime to bases 3 and 5 (even to base 31). It passes the ScratchPad test.¹

As we pointed out, this method applies to other sets of bases. We used it to find the following number n (337 digits):

¹However, after this work was completed, ScratchPad was further developed and renamed *Axiom* [9]. Its primality test has improved and is no longer a plain Rabin-Miller test. Now, it would be more difficult to find composite numbers which pass the *Axiom* test.

80383745745363949125707961434194210813883768828755814583748891752229
 74273765333652186502336163960045457915042023603208766569966760987284
 0439654082329287387918508691668573282677617710293896977394701670823
 0428687109997439976544144845341155872450633409279022275296229414984
 2306881685404326457534018329786111298960644845216191652872597534901,

which has the following factor p_2 :

400958216639499605418306452084546853005188166041132508774
 50620473800321707011962427162231915972197335821631650853
 58166969145233813917169287527980445796800452592031836601,

but which is a strong pseudoprime to all forty-six prime bases up to 200. We hope that for all prime values of b greater than 5, the conditions of Lemma 3.2 are attainable, and we have checked the validity of this assumption up to $2 \cdot 10^5$. The only limitation towards finding strong pseudoprimes to more bases in this way seems to be the difficulty of doing computations involving such large numbers.

ACKNOWLEDGMENT

The author would like to thank Claude Quitté for his constant help in this work and the referee for his valuable suggestions.

BIBLIOGRAPHY

1. C. Batut, *Aspects algorithmiques du système de calcul arithmétique en multiprécision PARI*, Thesis, Bordeaux I University, France, 1989.
2. B. W. Char, K. O. Geddes, G. H. Gonnet, B. L. Leong, M. B. Monagan, and S. M. Watt, *Maple library reference manual*, Springer-Verlag, New York, 1991.
3. H. Cohen, *Cryptographie, factorisation et primalité: l'utilisation des courbes elliptiques*, J. Annuelle Soc. Math. France, 1987.
4. D. A. Cox, *Primes of the form $x^2 + ny^2$* , Interscience, New York, 1989.
5. J. D. Dixon, *Factorization and primality tests*, Amer. Math. Monthly **91** (1974), 333–352.
6. IBM Computer Algebra Group, *The Scratchpad computer algebra system interactive environment users guide* (R. Sutor, ed.), 1989.
7. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, New York, 1982.
8. G. Jaeschke, *On strong pseudoprimes to several bases*, Math. Comp. **61** (1993), 915–926.
9. R. Jenks and R. Sutor, *Axiom, the scientific computation system*, Springer-Verlag, New York, 1992.
10. D. E. Knuth, *The art of computer programming. Vol. 2: Semi-numerical algorithms*, Addison-Wesley, Reading, MA, 1973.
11. C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to $25 \cdot 10^9$* , Math. Comp. **35** (1980), 1003–1026.
12. M. O. Rabin, *Probabilistic algorithms for testing primality*, J. Number Theory **12** (1980), 128–138.
13. H. Riesel, *Prime numbers and computer methods for factorizations*, Birkhäuser, Boston, MA, 1985.

DÉPARTEMENT DE MATHÉMATIQUES, UNIVERSITÉ DE POITIERS, 40, AV DU RECTEUR PINEAU,
 86022 POITIERS CEDEX, FRANCE
 E-mail address: arnault@knuth.univ-poitiers.fr