Int. J. Communications, Network and System Sciences, **2012, 5, 513-519**
http://dx.doi.org/10.4236/ijcns.2012.59062 Published Online September 2012 (http://www.SciRP.org/journal/ijcns)

Primality Testing Using Complex Integers and Pythagorean Triplets

Boris S. Verkhovsky
Computer Science Department, New Jersey Institute of Technology, Newark, USA
Email: verb@njit.edu

Received July 23, 2012; revised August 16, 2012; accepted August 31, 2012

"*Mathematicians have tried in vain to this day to discover some order in the sequence of prime numbers, and we have reason to believe that it is a mystery, into which the human mind will never penetrate.*"

Leonard Euler

ABSTRACT

Prime integers and their generalizations play important roles in protocols for secure transmission of information via open channels of telecommunication networks. Generation of multidigit large primes in the design stage of a cryptographic system is a formidable task. Fermat primality checking is one of the simplest of all tests. Unfortunately, there are composite integers (called Carmichael numbers) that are not detectable by the Fermat test. In this paper we consider modular arithmetic based on complex integers; and provide several tests that verify the primality of real integers. Although the new tests detect most Carmichael numbers, there are a small percentage of them that escape these tests.

Keywords: Cryptosystem Design; Primality Testing; Fermat Test; Pythagorean Triplet; Strong Carmichael Number; Quaternions

1. Introduction

Large prime numbers are at the core of every modern cryptographic protocol. These protocols rely on multidigit large primes to ensure that the cryptanalysis of an encrypted message is too complicated to break in any relevant time. Therefore, the efficiency of primality tests is important [1].

Primality testing has a long history. Paul Erdös, rephrasing Einstein's famous statement, expressed his view as "*God may not play dice with the Universe, but something strange is going on with the prime numbers*", [2]. I believe that maybe the following proposition explains the views of L. Euler and P. Erdös:

Conjecture: If there exists an algorithm that describes an order in the sequence of primes smaller than *n*, it has complexity $\Omega\left[f(n) \right]$, where *f*(*n*) is a monotone non-decreasing function of *n*, [3].

There are many ways to test an integer for primality. The Sieve of Eratosthenes, although able to detect all primes, has a time complexity in the order of *n*, [4]. Fermat's Little Theorem (FLT) can be used to test for primality. Although the Fermat test is very simple, there exists an infinite set of composite integers, {called Carmichael numbers or CMNs, for short}, that are not detectable by the Fermat test, [5].

2. Basic Properties of Primes

***Euclid Lemma*:** If *p* is a prime number and *p* divides a product *ab* of integers, then *p* divides *a* or *p* divides *b*. This is used in some proofs of the uniqueness of prime factorizations.

Fermat Little Theorem (FLT): If *p* is a prime that does not divide an integer *a*, then $a^{p-1}-1$ is divisible by *p*,

$$\text{otherwise } \left(a^p - a\right) \bmod p = 1. \tag{2.1}$$

***Wilson Theorem*:** provides a necessary and sufficient condition for primality testing: an integer $p \geq 2$ is a prime if and only if

$$(p-1)!+1 \text{ is divisible by } p. \tag{2.2}$$

However, since the Wilson Theorem has complexity O(*p*), it is not computationally efficient.

***Prime Number Theorem*:** The number of primes smaller than *x* is asymptotic to $\mathrm{O}(x/\ln x)$ [6]. (2.3)

***Dirichlet Theorem*:** In every arithmetic progression $a, a+q, a+2q, .., a+kq, ..$ where the positive integers *a* and $q \geq 1$ are relatively prime, there are infinitely many

primes. This property can be applied to generate large primes (greater than 10^{100}), which are important components in public-key cryptography.

***Existence of Generator*:** For every prime p there exists an integer $1 < g < p$, called a *generator*, such that every integer $1 \le b \le p-1$ can be expressed as

$$b = g^d, \bmod p. \tag{2.4}$$

Here d is called a *discrete logarithm* of b modulo p. This property plays an important role in the ElGamal cryptographic algorithm [7] and in elliptic-curve cryptography, [8].

3. Generalizations

The concept of prime numbers is so important that it has been generalized in different ways in various branches of mathematics. For example, we can define complex primes. Notice that 5 is not a complex prime, because it is the product of two complex integers $(1+2i)$ and $(1-2i)$. Another observation:

$$5 = (2+i)(2-i) = (1+2i)(1-2i);$$

which means that complex factorization is not unique. However, integer 3 is a complex prime. In general, every real prime n that satisfies $n \bmod 4 = 3$ (called *Blum prime*) is also a complex prime. Yet, every real prime n that satisfies $n \bmod 4 = 1$ is the complex composite, [9]. A public key cryptographic algorithm based on complex moduli is described in [10].

4. Arithmetic Operations on Complex Integers

Modular arithmetic with modulus n, unlike the "school-grade" arithmetic, operates on a finite set of integers in the interval $[0, n-1]$.

4.1. Multiplications of Complex Numbers

Let $L = a + bi$; and $R = c + di$; consider

$$LR = (a+bi)(c+di) = m + wi;$$

where $m = ac - bd$ and $w = ad + bc$. Hence, the computation of m and w requires *four* multiplications of real numbers, where integers in a cryptographic scheme might be of size 10^{100} or larger. However, [11] describes an algorithm that computes LR using only *three* multiplications. Indeed, let $P = (a+b)(c+d)$; $Q = ab$ and $S = bd$; then $m = Q - S$ and $w = P - Q - S$.

Consider now the squaring of a complex integer:

$$(a+bi)^2 = a^2 - b^2 + 2abi = m + wi;$$

and $r = a + b$, $p = a - b$, and $q = ab$.

Then $m = pr$; and $w = 2q$, where the latter can be performed by left shift, if integers are in binary form. Therefore, squaring is done using *two* multiplications and *two* additions.

If each integer A and B has s decimal digits, then algebraic addition $A \pm B$ requires $O(s)$ digital operations and multiplication AB has complexity $O(s^2)$.

4.2. Modular Multiplicative Inverse of Complex Integer

***Definition*4.1:** Let b and d be complex integers, where $bd \bmod n = 1$; then b and d are called mutually multiplicative inverse modulo n.

Let $b = c + fi$ and $d = g + hi$; (4.1)

compute $s = c^2 + f^2$ and $t = s^{-1}$. (4.2)

If gcd(s,n) = 1, then the inverse of s can be computed using either the extended Euclid algorithm, [12] or the algorithms in [2,13,14].

Finally, $g = ct$ and $h = (n - f)t$. (4.3)

4.3. Complex Primes

It is known that for every prime p congruent to 1 modulo 4 (non-Blum prime) there exists two real integers u and w such that

$$p = u^2 + w^2. \tag{4.4}$$

Thus, every such prime can be presented as two products of two factors each:

$$p = (u+wi)(u-wi) = (w+ui)(w-ui). \tag{4.5}$$

Therefore, there are no complex primes among non-Blum integers.

However, every Blum prime is also a complex prime, since it cannot be presented as a product of two complex integers except as $p = (\pm pi)(\pm i)$, [6].

In the following consideration we are using the notation:

$$(a,b) := a + bi. \tag{4.6}$$

5. Fundamental Identity

Proposition 5.1: If p is a real prime, then for every complex integer (a,b),

where $\gcd(a^2 + b^2, p) = 1$; (5.1)

the following identity holds

$$(a,b)^{p^2-1} \bmod p = (1,0) = 1. \tag{5.2}$$

Proof: First of all, if $(a,b) \neq (0,0)$; then

$$(a,b)(u,v) \equiv (a,b)(x,y) (\bmod\ p); \tag{5.3}$$

implies that $(u,v) \equiv (x,y) (\bmod\ p)$. (5.4)

Indeed, there exists a complex integer

$$(a,b)^{-1} \equiv (a, p-b)(a^2 + b^2)^{-1} (\bmod\ p) \tag{5.5}$$

such that $(a,b)^{-1}(a,b) \bmod p = (1,0)$.

By multiplying both parts of (5.3) with $(a,b)^{-1}$ we prove (5.4).

Let's consider a product A of all complex numbers (j,k) with components

$$0 \le j,k \le p-1 \quad \text{and} \quad j+k > 0, \tag{5.6}$$

i.e., at least one of the components is strictly *positive*:

$$A := \prod_{\substack{0 \le j,k \le p-1 \\ (j,k) \ne 0}} (j,k) \bmod p. \tag{5.7}$$

Consider now

$$B := \prod_{\substack{0 \le j,k \le p-1 \\ (j,k) \ne 0}} (j,k)(a,b)^{p^2-1} \bmod p; \tag{5.8}$$

$$\text{then} \quad B := (a,b)^{p^2-1} \left[\prod_{\substack{0 \le j,k \le p-1 \\ (j,k) \ne 0}} (j,k) \bmod p \right]. \tag{5.9}$$

$$= \prod_{\substack{0 \le j,k \le p-1 \\ (j,k) \ne 0}} \left[(a,b)(j,k) \right] \bmod p$$

Since every (j,k) satisfying (5.6) is an element of a cyclic group, then all (a,b) (j,k) are a permutation of the elements of the same group.

Hence,

$$A := \prod_{\substack{0 \le j,k \le p-1 \\ (j,k) \ne 0}} (j,k) \bmod p = B. \tag{5.10}$$

Therefore, (5.7), (5.8) and (5.10) imply that

$$(a,b)^{p^2-1} \bmod p = 1. \quad \text{Q.E.D.} \tag{5.11}$$

*Remark*5.1: If p is not a prime, then there exists (a,b), for which neither (5.1) holds, nor (5.3) implies (5.4). If $p=qr$, then

$$(a,b)^{(q^2-1)(r^2-1)} \bmod p = (1,0). \tag{5.12}$$

Proposition 5.2: For every real prime p there exists a complex integer G, called a complex generator, such that every complex integer (a,b), where (5.1) holds, can be expressed as

$$G^d \equiv (a,b) (\bmod p); \tag{5.13}$$

here d is called a discrete logarithm of (a,b) modulo p.

6. Major Results

Proposition 6.1: Let (a,b) be a complex integer, satisfying (5.1), and p be a Blum prime {$p$mod4=3}; then Proposition5.1 implies the following identity for every a, b and p:

$$(a,b)^{(p+1)/2} \bmod p = (d,e); \tag{6.1}$$

where either $d = 0$ or $e = 0$, but $d + e \ne 0$.

Furthermore, if $\sqrt{(a^2+b^2)} \bmod p$ exists, then

$$d + e = \pm\sqrt{(a^2+b^2)} \bmod p; \tag{6.2}$$

otherwise

$$d + e = \pm\sqrt{-(a^2+b^2)} \bmod p. \tag{6.3}$$

*Remark*6.1: $\sqrt{a^2+b^2}$ is the absolute value of (a,b). The alternative in (6.3) is based on the following observation: if p is a Blum prime, and $1 \le q \le p-1$; then from the Euler criterion of quadratic residuosity either q or $p-q$, but not both, is a quadratic residue modulo p [6].

The identity (6.1) in the following text is called the *BV*-3 *primality test*. Thousands of computer experiments have demonstrated that this test detects the overwhelming majority of CMNs {see Section 7 for details}.

***Definition* 6.1:** A triplet $\{a, b, c\}$ of positive integers where a and b are co-prime and satisfy

$$a^2 + b^2 = c^2; \tag{6.4}$$

is called a Pythagorean triplet.

Proposition 6.2: For every Pythagorean triplet $\{a,b,c\}$, and every Blum prime p the following identity holds

$$(a,b)^{(p+1)/2} \equiv c (\bmod p). \tag{6.5}$$

Example 6.1: Let p = 2011; a = 5 and b = 12; then $(5,12)^{1006} \equiv 13 \bmod 2011$; where $\{5^2 + 12^2 = 13^2\}$. More examples are provided in **Table 2**.

7. Carmichael Numbers

Carmichael numbers {CMNs} are *composite* integers that nevertheless satisfy Fermat's Little Theorem [15]. Carmichael found that 561 is the smallest integer that escapes the primality test of Fermat's Little Theorem [5]. Indeed, for every $0 < a < 561$, co-prime with 561, holds:

$$(a^{561} - a) \bmod 561 = 0$$

Table 1. Classification of integers and Fermat Test (FT).

n	***n*mod4=1**	***n*mod4=3**
Primes	Pass the Fermat test	Pass the Fermat and BV-3 tests
Ordinary composites	Detectable by FT	Detectable by FT
Carmichael numbers	Non-detectable by FT; Highly likely detectable by the BV-1 test	Non-detectable by FT; Highly likely detectable by the BV-3 test

Table 2. BV-3 test with primes and Pythagorean triplets (3,4); (5,12) (8,15) and (21,20) as testing seeds.

Primes	(3,4)	(5,12)	(8,15)	(21,20)	Primes	(3,4)	(5,12)	(8,15)	(21,20)
499	(5,0)	(13,0)	(–17,0)	(29,0)	**827**	(5,0)	(13,0)	(-17,0)	(29,0)
503	(5,0)	(13,0)	(17,0)	(29,0)	**863**	(5,0)	(13,0)	(17,0)	(29,0)
563	(5,0)	(13,0)	(–17,0)	(29,0)	**1031**	(5,0)	(13,0)	(17,0)	(29,0)
647	(5,0)	(13,0)	(17,0)	(29,0)	**1051**	(5,0)	(13,0)	(–17,0)	(29,0)
727	(5,0)	(13,0)	(17,0)	(29,0)	**1063**	(5,0)	(13,0)	(17,0)	(29,0)
739	(5,0)	(13,0)	(–17,0)	(29,0)	**1999**	(5,0)	(13,0)	(17,0)	(29,0)
823	(5,0)	(13,0)	(17,0)	(29,0)	**2011**	(5,0)	(13,0)	(–17,0)	(29,0)

According to Richard Pinch, there are 585,355 CMNs smaller than 10^{17}. Moreover, there are 8241 CMNs smaller than 10^{12}; 19,279 smaller than 10^{13}; 44,706 smaller than 10^{14}; 105,212 smaller than 10^{15}; and 246,683 smaller than 10^{16}.

For the experiments provided in this paper, CMNs numbers smaller than 10^{16} [16] are used. An algorithm that generates large CMNs is provided in [17].

Proposition 7.1: Since every CMN is a product of at least three primes, *i.e.*, $\mathrm{CMN} = p_1 p_2 p_3$, therefore at least one of these factors is smaller than the cubic root of the this CMN:

$$p_k \le \sqrt[3]{\mathrm{CMN}}\,. \tag{7.1}$$

Therefore, (2.3) and (7.1) imply that the complexity to find the smallest factor f of a CMN is of order

$$f = \mathrm{O}\left(\sqrt[3]{n} / \ln \sqrt[3]{n}\right) \tag{7.2}$$

The smaller factors of each CMN are shown in the left-most column of **Table 5**.

Example 7.1: If n = 612816751 {see **Table 3**} is a CMN, then in order to find its smallest factor it is sufficient to check whether n is divisible by at most one of the first 140 primes. It is easy to verify that f = 251.

Computer experiments indicate that for numerous CMNs the smallest factor of a CMN does not exceed $\sqrt[4]{\mathrm{CMN}}$ {see **Tables 5** and **Table A.1** in the Appendix}.

8. Primality Tests

***BV*-3 *test*:** If n is a Blum prime, a and b are distinct positive integers $0 < a < n$, $0 < b < n$, and $a + b \ne n$, then for every complex (a, b) holds that

$$(a,b)^{(n+1)/2} \bmod n = (c,d)\,; \tag{8.1}$$

where either c or d, but not both, are equal *zero*.

***BV*-1 *test*:** If n is a non-Blum prime, a and b are distinct positive integers $0 < a < n$, $0 < b < n$, and $a + b \ne n$, then for every complex (a,b) holds that

$$(a,b)^{(n-1)/2} \bmod n = (c,d)\,; \tag{8.2}$$

where either c or d, but not both, are equal *zero*.

Example 8.1: Let n=561 and (2,3); then

$$(2,3)^{280} \bmod 561 = (16,459)\,.$$

Therefore, 561 is not a prime, because (8.2) does not hold.

For more numeric examples see **Table 5**.

9. Primality Testing with Quaternions

For integers congruent to 1 modulo 4 we introduce a primality test based on quaternions

$$(a,b,c,d) := a + bi + cj + dk; \tag{9.1}$$

where

$$\begin{aligned} &i^2 = j^2 = k^2 = -1; \\ &ij = k;\ jk = i;\ ki = j; \\ &ji = -k; kj = -i; ik = -j. \end{aligned} \tag{9.2}$$

Conjecture 10.1: If n is a prime, then for every seed (a,b,c,d) holds

$$(a,b,c,d)^{n+1} \bmod n = (h,0,0,0)\,, \tag{9.3}$$

where

$$a^2 + b^2 + c^2 + d^2 = h\,. \tag{9.4}$$

10. Computer Experiments

The goal of the experiments is to verify the correctness of the primality tests.

The inputs for the experiments included all 246,683 Carmichael numbers smaller than 10^{16}. For other inputs we only considered complex primes to verify the tests, see Proposition 5.1. **Table 1** provides the classification of integers.

In parallel we tested various types of inputs using the Fermat test: in the two right-most columns of **Tables 3**-**5** are computed $2^{p-1} \bmod p$ and $5^{p-1} \bmod p$.

Table 2 displays results of Pythagorean triplets, {see Proposition 6.2}. Each seed represents (a,b) and the result is c of the Pythagorean triplet

$$a^2 + b^2 = c^2\,. \tag{10.1}$$

Table 3. BV-3 test with CMNs and testing seeds (3,2); 2; 5.

CMN *n*	(3,2)	2	5
612816751	(166608777,8114326)	1	1
7689096933451	(711030612716,887774073594)	1	1
42057129199051	(30876218159239,23205152153739)	1	1
160754105325451	(157881729352807,112064545099932)	1	1
236807688261991	(30786938340319,53087149566046)	1	1
3256635189018331	(493659725299301,3009342191292109)	1	1
7655741140594051	(5285004092343118,512008698445306)	1	1
9849406894481251	(1060236062683878,5602999134151296)	1	1

Table 4. BV-1 test with CMNs and seeds (4,7); 2; 5.

CMN *n*	(4,7)	2	5
1742169256201	(1722693465525,772900186399)	1	1
33812972024833	(27880593218382,28911607645602)	1	1
74243421107857	(56003783964933,54351804989873)	1	1
6876256816044001	(5628728581599734,1975253037870091)	1	1
9996906808980001	(6555953650183133,1380686298748699)	1	1
9997112118840001	(298421257278807,9251058975642986)	1	1
9999568870200001	(7972930190493543,5790396227732740)	1	1
9999731048186881	(4457231781813884,5226353781905389)	1	1
9999924433632001	(746295025284997,8421553345672929)	1	1

Table 5. BV-1 test with CMNs and testing seeds (2,1); (3,2); (3,4); (3,5); (8,3); 2; 5.

CM *n*	(2,1)	(3,2)	(3,4)	(3,5)	(8,3)	2	5
3|561	(544,327)	(16,102)	(511,102)	(280,393)	(34,429)	1	1
5|1105	(833,429)	(696,425)	(443,884)	(586,325)	(391,650)	1	1
7|1729	(1275,1638)	(995,763)	(729,1365)	(729,364)	(1275,1638)	1	1
5|2465	(1973,1479)	**(1,0)**	(1973,1479)	(2321,1885)	**(1,0)**	1	1
7|2821	(2028,317)	(2203,1902)	(833,2197)	(26,2501)	(26,1230)	1	1
1|5411	**(1,0)**	**(0,2989)**	**(1,0)**	**(5440,0)**	**(0,2989)**	**1**	**1**
7|**6601**	(2254,4346)	(6027,3312)	**(2092,0)**	**(0,2715)**	(2828,2829)	1	1

Remark 10.1: $3^2+4^2=5^2$; $5^2+12^2=13^2$; $8^2+15^2=17^2$; and $21^2+20^2=29^2$; are the Pythagorean triplets.

More generally, for every pair $\{g,h\}$ of positive integer parameters and

$$a := g^2-h^2; b := 2gh; c := g^2+h^2; \qquad (10.2)$$

holds (10.1). For instance, if $\{g,h\} = \{5,2\}$, then $a = 21$; $b = 20$; and $c = 29$.

Thousands of computer experiments show that the BV-3 test detects every CMN; several examples are provided below in **Table 3**.

Indeed, in the Fermat tests $2^{n-1} \bmod n = 1$; and $5^{n-1} \bmod n = 1$; however, $(3,2)^{(n+1)/2} \bmod n$ does not satisfy (8.1).

The BV-1 test detects CMNs congruent to 1 modulo 4; several examples are provided below in **Table 4**.

However, the BV-1 test is not reliable in all cases. Indeed, **Table 5** shows the instance (CMN = 2465) where

the BV-1 test fails. Numerous computer experiments detected CMNs in 95% of cases with the BV-1 test; more details on the experiments are provided in [18].

Remark 10.2: **Table 3** shows the cases where every CMN is detected by the BV-3 test using one seed (3,2) only.

Remark 10.3: **Table 4** shows the cases where every CMN is detected by BV-1 with one complex seed (4,7) only.

*Remark*10.4: n = 2465 in **Table 5** is a *strong* CMN since it escapes the BV-1 test with seeds (3,2) and (8,3); n = 6601 is another strong CMN since it escapes this test with seeds (3,4) and (3,5). Yet, n = 5441 is a prime; these cases are shown in bold in **Table 5**.

11. Acknowledgements

Several graduate and undergraduate students of New Jersey Institute of Technology have participated in thousands of computer experiments. I express my special appreciations to A. Mutovic, D. Rodik, K. Sauraj and S. Naredla. I also deeply appreciate insightful comments of C. Pomerance and R. Rubino.

REFERENCES

[1] L. M. Adleman, C. Pomerance and R. S. Rumley, "On Distinguishing Prime Numbers from Composite Numbers", *The Annals of Mathematics*, Vol. 117, No. 1, 1983, pp. 173-206. doi:10.2307/2006975

[2] C. Pomerance, "Paul Erdös, Number Theorist Extraordinaire", *The Notices of the American Mathematical Society*, Vol. 45, 1998, pp. 19-23.

[3] B. Verkhovsky, "Multiplicative Inverse Algorithm and Its Space Complexity", *Annals of European Academy of Sciences*, Vol. 2, 2004, pp. 110-124.

[4] M. Agrawal, N. Kayal and N. Saxena, "PRIMES Is in P", *The Annals of Mathematics*, Vol. 160, No. 2, 2002, pp. 781-793.

[5] W. R. Alford, A. Granville and C. Pomerance, "There Are Infinitely Many Carmichael Numbers", *The Annals of Mathematics*, Vol. 140, No. 3, 1994, pp. 703-722.

[6] C. F. Gauss, "Disquisitiones Arithmeticae", Yale University Press, New Haven, 1986.

[7] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Log-Arithmetic", *IEEE Transactions on Information Theory*, Vol. 31, No. 4, 1985, pp. 469-472. doi:10.2307/2006975

[8] N. Koblitz, A. Menezes and S. Vanstone, "The State of Elliptic Curve Cryptography", *Designs, Codes and Cryptography*, Vol. 19, No. 2-3, 2000, pp. 173-193. doi:10.1023/A:1008354106356

[9] E. Gethner, S. Wagon and B. Wick, "A Stroll through the Gaussian Primes", *American Mathematics Monthly*, Vol. 105, No. 4, 1998, pp. 327-337. doi:10.2307/2589708

[10] B. Verkhovsky, "Double-Moduli Gaussian Encryption/Decryption with Primary Residues and Secret Controls", *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 7, 2011, pp. 475-481. doi:10.4236/ijcns.2011.47058

[11] A. Karatsuba and Yu. Ofman, "Multiplication of Multi-Digit Numbers on Automata", *Soviet Physics Doklady*, Vol. 7, 1963, pp. 595-596.

[12] D. Knuth, "The Art of Computer Programming, Vol. 1: Fundamental Algorithms", 2nd Edition, Addison-Wesley, Boston, 1973.

[13] B. Verkhovsky, "Hardness of Cryptanalysis of Public Keys Crypto-Systems with Known Timing of Modular Exponentiation", *Advances in Computer Cybernetics*, Vol. 6, 1998, pp. 80-84.

[14] B. Verkhovsky, "Space Complexity of Algorithm for Modular Multiplicative Inverse", *International Journal of Communications, Network and System Sciences*, Vol. 4, No. 6, 2011, pp. 357-363. doi:10.4236/ijcns.2011.46041

[15] R. D. Carmichael, "Note on a New Number Theory Function", *Bulletin of American Mathematical Society*, Vol. 16, No. 5, 1910, pp. 232-238. doi:10.1090/S0002-9904-1910-01892-9

[16] R. G. E. Pinch, "The Carmichael Numbers up to 10^{15}", *Mathematics of Computation*, Vol. 61, 1993, pp. 381-391.

[17] H. Dubner, "A New Method for Producing Large Carmichael Numbers", *Mathematics of Computation*, Vol. 53, 1989, pp. 411-414. doi:10.1090/S0025-5718-1989-0969484-8

[18] B. Verkhovsky and A. Mutovic, "Primality Testing Algorithm Using Pythagorean Integers", *Proceedings of International Computer Science and Information Systems Conference*, Athens, June 2005.

Appendix

Table A1. Smallest factors *f*(*m*) of CMN *m* {see Table 3}.

m	*f*(*m*)	*exp*(*m*)	*m*	*f*(*m*)	*exp*(*m*)
9164559313	7	0.0848	9584174881	17	0.1232
9166911601	71	0.1858	9593125081	331	0.2524
9167487781	499	0.2708	9595140409	103	0.2016
9172425601	157	0.2204	9624742921	1171	0.3073
9237473281	223	0.2356	9653421961	53	0.1726
9261585313	337	0.2536	9701285761	433	0.2639
9294465601	31	0.1496	9793709857	29	0.1463
9371873281	241	0.2388	9891283585	5	0.0699
9410913721	11	0.1044	9907185601	37	0.1568
9423125713	89	0.1954	9973625581	163	0.2212
9434224801	23	0.1365	9983803921	7	0.0845
9558334369	67	0.1829	9999109081	13	0.1113

Legend:

$c(m) :=$ largest prime smaller than or equal to $\lfloor \sqrt[3]{m} \rfloor$;

$$\exp(m) := \log_m f(m) = \ln f(m) / \ln m; \quad \text{(A.1)}$$

*Example*A1: if *m*=612816751; then *f*(*m*)=251; ln251= 5.525; ln612816751=20.234. Therefore, exp(*m*)=0.2731.

Table A2. Frequency distribution of exp(*m*) for CMNs *m* on interval $\left[10^9, 10^{10}\right]$.

[.03,.06]	(.06,.09]	(.09,.12]	(.12,.15]	(.15,.18]	(.18,.21]	(.21,.24]	(.24,.27]	(.27,.3]	(.3,1/3]
12	230	252	139	64	38	45	63	34	2

*Remark*A1: Among Carmichael numbers *m* on the interval $\left[10^9, 10^{10}\right]$ there are no *f*(*m*) with the corresponding exp(*m*)<0.03.

Average value of exp(*m*) is equal 0.137, therefore,

$$f(m) = \Theta\left(m^{0.137}\right). \quad \text{(A.2)}$$

