José María Grau; Antonio M. Oller-Marcén; Manuel Rodríguez; Daniel Sadornil
Fermat test with Gaussian base and Gaussian pseudoprimes

Czechoslovak Mathematical Journal, Vol. 65 (2015), No. 4, 969–982

Persistent URL: http://dml.cz/dmlcz/144786

Czechoslovak Mathematical Journal, 65 (140) (2015), 969–982

FERMAT TEST WITH GAUSSIAN BASE AND GAUSSIAN PSEUDOPRIMES

José María Grau, Gijón, Antonio M. Oller-Marcén, Zaragoza,
Manuel Rodríguez, Lugo, Daniel Sadornil, Santander

(Received September 22, 2014)

Abstract. The structure of the group $(\mathbb{Z}/n\mathbb{Z})^\star$ and Fermat's little theorem are the basis for some of the best-known primality testing algorithms. Many related concepts arise: Euler's totient function and Carmichael's lambda function, Fermat pseudoprimes, Carmichael and cyclic numbers, Lehmer's totient problem, Giuga's conjecture, etc. In this paper, we present and study analogues to some of the previous concepts arising when we consider the underlying group $\mathcal{G}_n := \{a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]/n\mathbb{Z}[\mathrm{i}]\colon\ a^2 + b^2 \equiv 1 \pmod{n}\}$. In particular, we characterize Gaussian Carmichael numbers via a Korselt's criterion and present their relation with Gaussian cyclic numbers. Finally, we present the relation between Gaussian Carmichael number and 1-Williams numbers for numbers $n \equiv 3 \pmod 4$. There are also no known composite numbers less than 10^{18} in this family that are both pseudoprime to base $1 + 2\mathrm{i}$ and 2-pseudoprime.

Keywords: Gaussian integer; Fermat test; pseudoprime

MSC 2010: 11A25, 11A51, 11D45

1. Introduction

Most of the classical primality tests are based on Fermat's little theorem: let p be a prime number and let a be an integer such that $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$. This theorem offers a possible way to detect non-primes: if for a certain a coprime to n, $a^{n-1} \not\equiv 1 \pmod n$, then n is not prime. The problem is that the converse is false and there exists composite numbers n such that $a^{n-1} \equiv 1 \pmod n$ for some a coprime to n. In this situation n is called pseudoprime with respect to base a (or

D. Sadornil is partially supported by the Spanish Government under projects MTM2010–21580–C02–02 and MTM2010–16051.

a-pseudoprime). A composite integer n which is a pseudoprime to any base a such that $\gcd(a, n) = 1$ is called a Carmichael number (or absolute pseudoprime).

Fermat theorem can be deduced from the fact that the non-zero elements of $\mathbb{Z}/n\mathbb{Z}$ form a subgroup of order $n - 1$ when n is prime. Associated with the subgroup $(\mathbb{Z}/n\mathbb{Z})^\star$ we can define the well-know Euler's totient function and Carmichael's lambda function which are defined in the following way:

$$\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\star|, \quad \lambda(n) := \exp(\mathbb{Z}/n\mathbb{Z})^\star.$$

It seems reasonable (and natural) to extend these ideas to other general groups G_n. This extension leads to composite/primality tests according to the following steps:

1°) Compute $f(n) = |G_n|$ under the assumption that n is prime.
2°) Given n, if we can find $g \in G_n$ such that $|g| \nmid f(n)$, then n is not prime.

This idea is present in tests based in lucasian sequences [21] and elliptic curves [16]. Recent works have developed these concepts in other contexts. Pinch [13] considers primality tests based on quadratic rings and discuses the absolute pseudoprimes for them. Shettler [15] studies analogues to Lehmer's Problem Totient and Carmichael numbers in a PID. Steele [18] generalizes Carmichael numbers to number rings introducing Carmichael ideals in number rings and proving an analogue to Korselt's criterion for them.

Following these approaches, in this paper we consider the groups

$$\mathcal{G}_n := \{a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]/n\mathbb{Z}[\mathrm{i}] \colon\ a^2 + b^2 \equiv 1 \pmod{n}\}.$$

Note that $\mathcal{G}_n$ is the unit circle modulo n over the Gaussian integers and is a very special case of the so-called *Pell Conics* [12].

For these groups, we define the corresponding Euler and Carmichael functions and study some of their properties. We also present the concepts of Gaussian pseudoprime and Gaussian Carmichael numbers presenting an explicit Korselt's criterion. Cyclic numbers, Lehmer's Totient Problem [3] and Giuga's conjecture [8] are also considered in this gaussian setting.

It is known that Carmichael numbers have at least three prime factors. We show that Gaussian Carmichael numbers with only two prime factors exist and determine their form. Moreover, although there are Gaussian pseudoprimes with respect to any base, if we combine our ideas with a classical Fermat test, we show that no number of the form $4k+3$ smaller than 10^{18} passes both the tests (for some particular bases). This strength is possible due to a relationship with 1-Williams numbers [21] that we make explicit.

2. Preliminaries

In this section we determine the order and structure of the group $\mathcal{G}_n$. We also show some elementary properties and relations between the gaussian counterparts of Euler and Carmichael functions. Some of the results of this section, in particular Proposition 2.1, can be found in [5].

For any positive integer n we will denote by $\mathcal{I}_n$ the ring of Gaussian integers modulo n; i.e.,

$$\mathcal{I}_n := \{a + b\mathrm{i}\colon\ a, b \in \mathbb{Z}/n\mathbb{Z}\} = \mathbb{Z}[\mathrm{i}]/n\mathbb{Z}[\mathrm{i}].$$

Further, we will consider the group $\mathcal{G}_n$ defined by

$$\mathcal{G}_n := \{a + b\mathrm{i} \in \mathcal{I}_n\colon\ a^2 + b^2 \equiv 1 \pmod{n}\}.$$

Once we have defined the group we can define the following arithmetic functions:

$$\Phi(n) := |\mathcal{G}_n|, \quad \lambda(n) := \exp(\mathcal{G}_n).$$

Note that Φ and λ are the analogues to Euler's totient funtion and Carmichael's lambda functions, respectively.

It is quite clear that if $n = p_1^{r_1} \dots p_s^{r_s}$, then

$$\mathcal{G}_n \cong \mathcal{G}_{p_1^{r_1}} \times \ldots \times \mathcal{G}_{p_s^{r_s}}.$$

As a consequence, if $\gcd(m, n) = 1$, then $\Phi(mn) = \Phi(m)\Phi(n)$ and $\lambda(mn) = \operatorname{lcm}(\lambda(m), \lambda(n))$. Hence, in order to study the group $\mathcal{G}_n$ we can restrict ourselves to the case when n is a prime power.

Proposition 2.1. *Let p be a prime and let $k > 0$ be an integer. Then*

$$\mathcal{G}_{p^k} \cong \begin{cases} C_2 & \text{if } p = 2 \text{ and } k = 1; \\ C_{2^{k-2}} \times C_2 \times C_4 & \text{if } p = 2 \text{ and } k \geqslant 2; \\ C_{p^{k-1}} \times C_{p-1} & \text{if } p \equiv 1 \pmod{4}; \\ C_{p^{k-1}} \times C_{p+1} & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

P r o o f. We will focus only on the case $p \equiv 3 \pmod{4}$. In this case, it is well-known that $\mathcal{G}_p \cong GF(p^2)^\star$. Since $\mathcal{G}_p$ is a subgroup of $GF(p^2)^\star$, it must be cyclic. Moreover, counting quadratic residues it can be seen that $|\mathcal{G}_p| = p + 1$ and, consequently, $\mathcal{G}_p \cong C_{p+1}$.

We can now apply the Fundamental Lemma in [9], page 587, to obtain that $|\mathcal{G}_{p^k}| = p^{k-1}(p + 1)$. This means that, if $\Phi\colon\ \mathcal{G}_{p^k} \to \mathcal{G}_p$ is the $(\mathrm{mod}\ p)$ group homomorphism, then $|\operatorname{Ker}\Phi| = p^{k-1}$. Finally, observe that $\operatorname{Ker}\Phi$ is an abelian p-group with exactly $p - 1$ elements of order p, namely $\{1 + Bp^{k-1}\mathrm{i} \in \mathcal{G}_{p^k}\colon\ 1 \leqslant B \leqslant p - 1\}$. Consequently it must be cyclic and the proof is complete in this case. □

As a straightforward consequence we compute $\Phi(p^k)$ and $\lambda(p^k)$.

Corollary 2.2. *Let p be a prime and $k > 0$ an integer. Then*

$$\Phi(p^k) = \begin{cases} 2 & \text{if } p = 2 \text{ and } k = 1; \\ 2^{k+1} & \text{if } p = 2 \text{ and } k > 1; \\ p^{k-1}(p-1) & \text{if } p \equiv 1 \pmod 4; \\ p^{k-1}(p+1) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

$$\lambda(p^k) = \begin{cases} 2 & \text{if } p = 2 \text{ and } k = 1; \\ 4 & \text{if } p = 2 \text{ and } k = 2, 3, 4; \\ 2^{k-2} & \text{if } p = 2 \text{ and } k \geqslant 5; \\ p^{k-1}(p-1) & \text{if } p \equiv 1 \pmod 4; \\ p^{k-1}(p+1) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

For an odd prime number p, let us define $\beta(p) = (-1/p)$ and put $\beta(2) = 0$. With this notation the following result is straightforward.

Proposition 2.3.

$$\Phi(n) = \begin{cases} 2n \displaystyle\prod_{p|n} \Big(1 - \frac{\beta(p)}{p}\Big) & \text{if 4 divides } n; \\ n \displaystyle\prod_{p|n} \Big(1 - \frac{\beta(p)}{p}\Big) & \text{otherwise.} \end{cases}$$

Recall that $\Phi(mn) = \Phi(m)\Phi(n)$ provided $\gcd(m, n) = 1$. The following result describes the general situation.

Proposition 2.4. *Let $m, n \in \mathbb{N}$. Then*

$$\Phi(nm) = \Phi(n)\Phi(m)\frac{\gcd(m, n)}{\Phi(\gcd(m, n))}.$$

P r o o f. It is enough to consider the prime power decomposition of m and n. □

In particular, if we put $m = n$ we obtain the following.

Corollary 2.5. *Let $n, s \in \mathbb{N}$. Then*

$$\Phi(n^s) = \begin{cases} n^{s-1}\Phi(n) & \text{if } n \not\equiv 2 \pmod 4; \\ 2n^{s-1}\Phi(n) & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

Recall that for the classical Euler and Carmichael functions, $\varphi(n) = \lambda(n)$ if and only if $n = 2$, $n = 4$ or $n = p^r, 2p^r$ for some odd prime p and $r > 0$. Note that in all these cases the group $(\mathbb{Z}/n\mathbb{Z})^\star$ is cyclic. For our above defined functions Φ and λ we have the following:

Proposition 2.6. *$\Phi(n) = \lambda(n)$ if and only if $n = 2$ or $n = p^r$ for some odd prime p and $r > 0$.*

P r o o f. Just apply Corollary 2.1 and recall that if $\gcd(m, n) = 1$, then $\Phi(mn) = \Phi(m)\Phi(n)$ while $\lambda(mn) = \operatorname{lcm}(\lambda(m), \lambda(n))$. □

We end this section showing that the asymptotic behavior of $\Phi(n)$ is not exactly the same as that of its classical counterpart.

Proposition 2.7.

$$\liminf \frac{\varphi(n)}{n} = \liminf \frac{\Phi(n)}{n} = 0,$$
$$1 = \limsup \frac{\varphi(n)}{n} \neq \limsup \frac{\Phi(n)}{n} = \infty.$$

P r o o f. For the asymptotic growth of Euler φ function and its limits see [10]. Now consider sequences $\{S_n\}$ and $\{L_n\}$ given by:

$$S_n := \prod_{\substack{p \leqslant n \\ p \equiv 3 \pmod 4}} p, \quad L_n := \prod_{\substack{p \leqslant n \\ p \equiv 1 \pmod 4}} p.$$

We have that $\Phi(p) = p + 1$ for every odd prime $p \equiv 3 \pmod 4$, hence

$$\lim_{n\to\infty} \frac{\Phi(S_n)}{S_n} = \lim_{n\to\infty} \prod_{\substack{p \leqslant n \\ p \equiv 3 \pmod 4}} \frac{p+1}{p} = \infty,$$

since $\prod (p+1)/p \geqslant 1 + \sum 1/p$ and this series is divergent by the strong form of Dirichlet's theorem. On the other hand,

$$\lim_{n\to\infty} \frac{\Phi(L_n)}{L_n} = \lim_{n\to\infty} \prod_{\substack{p \leqslant n \\ p \equiv 1 \pmod 4}} \Big(1 - \frac{1}{p}\Big).$$

Moreover,

$$0 \leqslant \prod_{\substack{p \leqslant n \\ p \equiv 1 \pmod 4}} \Big(1 - \frac{1}{p}\Big) \leqslant \prod_{\substack{p \leqslant n \\ p \equiv 1 \pmod 4}} \mathrm{e}^{-1/p} = \mathrm{e}^{-\sum 1/p},$$

where the sum in the exponent is taken over the primes $p \equiv 1 \pmod 4$, $p \leqslant n$. Again, by the strong form of Dirichlet's theorem, this function tends to 0 and the result holds. □

3. Gaussian Fermat pseudoprimes

We start this section by introducing the arithmetic function $\mathcal{F}$, which will play the same role as $n-1$ plays in the classical setting:

$$\mathcal{F}(n) = \begin{cases} n-1 & \text{if } n \equiv 1 \pmod 4; \\ n+1 & \text{if } n \equiv 3 \pmod 4; \\ n & \text{otherwise.} \end{cases}$$

Note that, if n is prime, $\mathcal{F}(n) = |\mathcal{G}_n|$.

We present the analogue to Fermat's little theorem in this gaussian setting.

Proposition 3.1. *Let p be a prime number and let z be a Gaussian integer such that p is coprime with $z\overline{z}$. Then*

a) $(z/\overline{z})^{\mathcal{F}(p)} \equiv 1 \pmod p$,
b) $\operatorname{Im}(z^{\mathcal{F}(p)}) \equiv 0 \pmod p$.

Proof. Note that if $z \in \mathbb{Z}[\mathrm{i}]$ is such that $\gcd(n, z\overline{z}) = 1$, then $z/\overline{z} \in \mathcal{G}_n$. Hence, it is enough to apply Corollary 2.1. □

Remark 3.2. The two conditions in Proposition 3.1 are equivalent.

We can view the above result as a compositeness test for integers: if for some integer n we find a Gaussian integer z such that either condition a) or b) does not hold, then n is a composite number. Nevertheless, like in the classical setting, the converse is not always true. This fact motivates the following definition:

Definition 3.3. A composite integer n is called a Gaussian Fermat pseudoprime (GFP) with respect to the base $z \in \mathbb{Z}[\mathrm{i}]$ if $\gcd(n, z\overline{z}) = 1$ and condition a) (or equivalently b)) from Proposition 3.1 holds for n.

In the classical setting the choice of different basis leads, in general, to different sets of associated Fermat pseudoprimes. In our case it is easy to describe a family of different bases leading to the same set of associated Gaussian Fermat pseudoprimes.

Proposition 3.4. *Let z, w be two gaussian integers such that $|z| = |w|$. Then an integer n is a Gaussian Fermat pseudoprime with respect to z if and only if n is a Gaussian Fermat pseudoprimes with respect to w.*

P r o o f. Assume that n is a GFP with respect to z. Then $\gcd(n, z\overline{z}) = 1$ and $(z/\overline{z})^{\mathcal{F}(n)} \equiv 1 \pmod{n}$. Now, since $|w| = |z|$ we have that $\gcd(n, w\overline{w}) = \gcd(n, z\overline{z}) = 1$. Moreover, since $(z/\overline{z})^{\mathcal{F}(n)} \equiv 1 \pmod{n}$ and $z/\overline{z} \in \mathcal{G}_n$, it follows that $\lambda(n) \mid \mathcal{F}(n)$. Hence, $(w/\overline{w})^{\mathcal{F}(n)} \equiv 1 \pmod{n}$ because $w/\overline{w} \in \mathcal{G}_n$. The converse is clear since the roles of z and w are symmetric. The proof is complete. □

4. Gaussian Carmichael and cyclic numbers

An integer n that is a Fermat pseudoprime for all bases coprime to n is called a Carmichael number [4]. In the gaussian case there also exists composite numbers which are GFP with respect to all bases.

Definition 4.1. A composite number $n \in \mathbb{N}$ is a Gaussian Carmichael number (G-Carmichael) if it is a GFP to the base z for every Gaussian integer z such that n is coprime to $z\overline{z}$.

An alternative and equivalent definition of Carmichael numbers is given by Korselt's criterion [20] which states that a positive composite integer n is a Carmichael number if and only if n is square-free, and for every prime divisor p of n, $p - 1$ divides $n - 1$. It follows from this characterization that all Carmichael numbers are odd. A similar characterization of G-Carmichael numbers can be given, showing that there are also even G-Carmichael numbers.

Proposition 4.2. *For every composite integer n the following statements are equivalent.*

a) *n is a G-Carmichael number.*
b) *$\lambda(n)$ divides $\mathcal{F}(n)$.*
c) *For every prime divisor p of n, $\mathcal{F}(p)$ divides $\mathcal{F}(n)$ and one of the following conditions holds:*
   α) *n is odd and square-free,*
   β) *n is a multiple of 4 and $n/4 = 2, 3, 5$ or not a prime number.*

P r o o f. Since $\lambda(n)$ is the exponent of the group $\mathcal{G}_n$, a) and b) are clearly equivalent.

From Corollary 2.1 and the fact that $\lambda(mn) = \operatorname{lcm}(\lambda(m), \lambda(n))$ if $\gcd(m, n) = 1$, it is easy to see that c) implies b) when n is a number that satisfies α) or β).

Finally, assume now that $\lambda(n)$ divides $\mathcal{F}(n)$ and let $n = 2^a p_1^{r_1} \dots p_s^{r_s}$. We have that $\lambda(n) = \operatorname{lcm}(\lambda(2^a), \lambda(p_1^{r_1}), \dots, \lambda(p_s^{r_s}))$, so $\lambda(2^a)$ and $\lambda(p_i^{r_i})$ divide $\mathcal{F}(n)$. From Corollary 2.1 it is clear that for every prime p, $\lambda(p) = \mathcal{F}(p)$ divides $\lambda(p^k)$ with $k \geqslant 1$ and $\mathcal{F}(p)$ also divides $\mathcal{F}(n)$ as claimed.

If n is odd ($a = 0$) and $r_i \geqslant 2$ for some $i \in \{1, \dots, s\}$ we get that p_i divides $\lambda(n)$ and, consequently, also $\mathcal{F}(n)$. Thus, p_i divides $n-1$ or $n+1$ which is a contradiction and n must be square-free in this case.

We now turn to the even case. If $a = 1$ and n is divisible by another prime p such that $p \equiv 1 \pmod 4$, then $p - 1$ divides $\mathcal{F}(n) = n$. Hence n is a multiple of 4, a contradiction. The same follows if there exists a prime $p \equiv 3 \pmod 4$ dividing n so we conclude that if $n \neq 2$ is even, it must be a multiple of 4.

Now, let $n = 4p$ with p a prime. If $p = 2$, then $n = 8$ and we are done. If $p \equiv 1 \pmod 4$, it follows that $p - 1$ divides n; i.e., $p - 1$ divides 4 so $p = 5$ and $n = 20$. Finally, if $p \equiv 3 \pmod 4$, it follows that $p + 1$ divides 4 so $p = 3$ and $n = 12$. Hence we see that if 4 divides n and $n \neq 8, 12, 20$, then $n/4$ is not prime and the proof in complete. □

In 1994 it was shown by Alford, Granville and Pomerance [1] that there exist infinitely many Carmichael numbers. It is easy to see that every power of 2 is a G-Carmichael number, hence there are also infinitely many of them. However, if we restrict to odd G-Carmichael numbers, the problem seems to have at least the same difficulty as the classical case.

Carmichael numbers have at least three prime factors. We know that 12 and 20 are the only even G-Carmichael numbers with only two prime factors. The following result describes the family of odd G-Carmichael numbers with exactly two prime factors.

Proposition 4.3. *Let $p < q$ be odd primes. Then $n = pq$ is a Gaussian Carmichael number if and only if p and q are twin primes such that 8 divides $p + q$.*

P r o o f. Assume that $n = pq$ with $p < q$ odd primes is a G-Carmichael number.

If $p, q \equiv 1 \pmod 4$, then $\mathcal{F}(n) = n-1 = pq-1$. From Proposition 4.1, $p-1$ divides $pq-1 = (p-1)(q+1)+q-p$. Hence $p-1$ divides $q-p$ and also $q-1 = (q-p)+(p-1)$. In the same way $q-1$ divides $p-1$. So $p-1 = q-1$, which is impossible. If $p, q \equiv 3 \pmod 4$ we reach a similar contradiction using the same ideas. If $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ we obtain that $p = q + 2$, which is impossible because $p < q$.

Thus $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$ and we have, by similar reasoning, that $q = p + 2$. Moreover, $p + q = 2p + 2 \equiv 0 \pmod 8$.

The converse is trivially true and the proof is complete. □

Recall that a positive integer n which is coprime to $\varphi(n)$ is called a cyclic number (sequence A003277 in [17]). This terminology comes from the group theory since a number n is cyclic if and only if any group of order n is cyclic [19]. From Korselt's criterion it follows that any divisor of a Carmichael number is cyclic. In the gaussian setting we define Gaussian cyclic numbers in the following way.

Definition 4.4. An integer n is called G-cyclic if $\gcd(\Phi(n), n) = 1$.

The relationship between G-Carmichael and G-cyclic numbers is the same as in the previous setting, the proof being also quite similar.

Proposition 4.5. *Any divisor of an odd G-Carmichael number is G-cyclic.*

P r o o f. Let n be an odd G-Carmichael number. Since n is square-free, $n = p_1 p_2 \dots p_r$ and from Proposition 2.2, $\Phi(n) = \prod(p_i - \beta(p_i))$. A divisor d of n is a product of some of these primes, that is, $d = \prod_{h \in J} p_h$, $J \subseteq \{1, 2, \dots, r\}$. If $\gcd(\Phi(d), d) \neq 1$, then there exist two indices $i \neq k$ in J such that p_i divides $p_k - \beta(p_k)$. As n is a Carmichael number, we also have that $p_k - \beta(p_k)$ divides $n - \beta(n)$. Hence, p_i divides $n - \beta(n)$, which is absurd since n is divisible by p_i and $\beta(p_i) = \pm 1$. □

Around 1980, G. Michon conjectured that all odd cyclic numbers have Carmichael multiples. This can be reasonably extended to G-cyclic numbers and we can ask if all odd G-cyclic numbers have G-Carmichael multiples.

Cyclic numbers can also be characterized in terms of congruences. A number n is cyclic if and only if it satisfies $\varphi(n)^{\varphi(n)} \equiv 1 \pmod{n}$ or $\lambda(n)^{\lambda(n)} \equiv 1 \pmod{n}$. In our situation only one implication remains valid, namely

Proposition 4.6. *If $\Phi(n)^{\Phi(n)} \equiv 1 \pmod{n}$ or $\lambda(n)^{\lambda(n)} \equiv 1 \pmod{n}$, then n is a G-cyclic number.*

P r o o f. Let n be a positive integer such that $\Phi(n)^{\Phi(n)} \equiv 1 \pmod{n}$. Then for any prime divisor p of n it holds that $\Phi(n)^{\Phi(n)} \equiv 1 \pmod{p}$. Now, if n is not a G-cyclic number, there exists a prime p with $p \mid \gcd(\Phi(n), n)$. Thus, p divides $\Phi(n)$ and $\Phi(n)^{\Phi(n)} \equiv 0 \pmod{p}$, a contradiction.

On the other hand, let $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$ be a positive integer. If n is not a G-cyclic number then there exists a prime p which $p \mid \gcd(\Phi(n), n)$. Since $p \mid \Phi(n) = \Phi(p_1^{e_1})\Phi(p_2^{e_2}) \dots \Phi(p_r^{e_r})$, there exists $1 \leqslant j \leqslant r$ with $p \mid \Phi(p_j^{e_j})$. If $p_j = 2$ then $p = 2$ and $\lambda(n)$ is even. Otherwise, $\Phi(p_j^{e_j}) = \lambda(p_j^{e_j})$ and p divides $\lambda(n)$. So $\lambda(n)^{\lambda(n)} \equiv 0 \pmod{p}$ and n does not satisfy the hypothesis. □

The converse of the previous proposition is not true. In fact there are G-cyclic numbers n that do not satisfy any of the above conditions. The first of them are:

$$77,\ 119,\ 133,\ 187,\ 217,\ 253,\ 287,\ 301,\ 319,\ 323,\ 341,\ 391,\ \dots$$

5. G-Lehmer's totient problem and G-Giuga's conjecture

Lehmer's totient problem, named after Lehmer, asks whether there is any composite number n such that $\varphi(n)$ divides $n-1$. This is true for every prime number, and Lehmer conjectured in 1932 (see [11]) that the answer to his question was negative. He showed that if any such n exists, it must be odd, square-free, and divisible by at least seven primes. These numbers, called Lehmer numbers, are clearly Carmichael numbers and, up to date, none has been found. It is known that these numbers have at least 15 prime factors and are greater than 10^{30}. Moreover, if a Lehmer number is divisible by 3, the number of prime factors increases to 40,000,000 with more than 360,000,000 digits (see [3]). We now define our analogous concept.

Definition 5.1. A composite number n is a G-Lehmer number if $\Phi(n) \mid \mathcal{F}(n)$.

It is clear that every G-Lehmer number is a G-Carmichael number. Besides, it is easy to note that G-Lehmer numbers exist.

Proposition 5.2. *Let $p < q$ be odd primes. Then $n = pq$ is a G-Lehmer number if and only if p and q are twin primes such that 8 divides $p + q$.*

P r o o f. As n must be a G-Carmichael number, $n = (4k-1)(4k+1)$ where both factors $4k \pm 1$ are primes. Hence $\Phi(n) = \mathcal{F}(n) = (4k)^2$, so n is a G-Lehmer number. □

Note that, from Proposition 4.2 this result means that every odd G-Carmichael number with exactly 2 prime factors is a G-Lehmer number. Nevertheless, there are G-Lehmer numbers with more than 2 prime factors (A182221 in [17]):

$$255,\ 385,\ 34561,\ 65535,\ 147455,\ 195841,\ \ldots$$

This suggests an interesting question:

Question 5.3. *Are there infinitely many G-Lehmer numbers?*

Furthermore, all known G-Lehmer numbers satisfy $\mathcal{F}(n) = \Phi(n)$. Hence, it is reasonable to propose the G-Lehmer's totient problem:

Question 5.4. *Is there any number n such that $\Phi(n)$ is a proper divisor of $\mathcal{F}(n)$?*

In 1932, Giuga [8] proposed another conjecture about prime numbers. He postulated that a number p is prime if and only if $\sum i^{p-1} \equiv -1 \pmod{p}$, where the sum is taken over all integers $1 \leqslant i \leqslant p-1$. Giuga showed that there are no exceptions to his conjecture up to 10^{1000}. This was later improved to 10^{13800}, see [2]. A similar

approach to Giugas's conjecture, replacing $n-1$ by $\mathcal{F}(n)$, leads us to consider the following set, which contains all prime numbers

$$\mathfrak{G} := \left\{ n \in \mathbb{N} \colon \sum_{z \in \mathcal{G}_n} z^{\mathcal{F}(n)} \equiv \mathcal{F}(n) \pmod{n} \right\}.$$

However, this set also contains lots of composite numbers. For example, every power of 2 is in $\mathfrak{G}$. For odd integers we have the next result.

Proposition 5.5. *Let n be an odd integer. If $\Phi(n) = \mathcal{F}(n)$, then $n \in \mathfrak{G}$.*

P r o o f. Since $|\mathcal{G}_n| = \Phi(n)$, for all $z \in \mathcal{G}_n$, we have $z^{\Phi(n)} \equiv 1 \pmod{n}$. If $\Phi(n) = \mathcal{F}(n)$ then

$$\sum_{z \in \mathcal{G}_n} z^{\Phi(n)} \equiv |\mathcal{G}_n| \equiv \Phi(n) \equiv \mathcal{F}(n) \pmod{n},$$

and n is in $\mathfrak{G}$. □

Thus, prime numbers and every known G-Lehmer numbers are in $\mathfrak{G}$. Furthermore, no other odd composite integer is known to be in $\mathfrak{G}$. So, we formulate the following conjecture regarding the numbers in $\mathfrak{G}$.

Conjecture 5.6. *For every odd n, $n \in \mathfrak{G}$ if and only if $\Phi(n) = \mathcal{F}(n)$.*

6. Gaussian Fermat test for numbers of the form $4k+3$.

The use of Gaussian integers to perform the equivalent of Fermat's little theorem to test primality is not just a mere theoretical speculation. Lucas pseudoprimes [21] for some particular sequences can be also seen as Gaussian pseudoprimes. However, Gaussian integers, and the corresponding definition of peudoprimes using powers, are more similar to the classical one than the concept of Lucas sequences.

As we have said before, we can take advantage of Proposition 3.1 to test primality (more precisely, compositeness) of a number. This is what we call the Gaussian Fermat Test with respect to the base z. Computational evidence reveals that this test, based on the structure of $\mathcal{G}_N$, is very powerful when it is combined with the classical one; i.e., there are very few common pseudoprimes. Furthermore, this combination is stronger if we restrict ourselves to numbers of the form $4k+3$. From the William Galway list [7], we have checked that no Fermat pseudoprime number to base 2 less than 10^{18} and of the form $4k+3$ is a Gaussian pseudoprime to base $z = 1 + 2\mathrm{i}$.

Baillie-PSW primality test [14], used in many computer algebra systems and software packages, is also a combination of two primality tests. This test has no known pseudoprimes. Although this is not the case for our test (since it has pseudoprimes of the form $4k+1$), it must be noted that our test is much simpler as it consists of the combination of two basic Fermat tests.

In general, combination of two Fermat tests with respect to two different prime bases (less than 30) presents more than 10 (and a mean of 34) pseudoprimes lower than $4 \cdot 10^7$ of the form $4k+3$. Even if we combine two bases to test if a number n is a prime using the Gaussian Fermat Test, there are more pseudoprimes. However, there is no composite number of the form $4k+3$ less than $4 \cdot 10^7$ which is both a Gaussian pseudoprime with respect to $1+2\mathrm{i}$ and a Fermat pseudoprime with respect to a prime base less than 30. The lowest base to be used to find a Fermat pseudoprime with respect to this base which is also a Gaussian Fermat pseudoprime to the base $1+2\mathrm{i}$ is 10. Also with other Gaussian bases the combination with a Fermat test is very strong as is shown in the following table, which presents the number of composite integers less than $4 \cdot 10^7$ which are simultaneously Gaussian Fermat pseudoprimes with respect to a base z (horizontal) and Fermat pseudoprimes with respect to a base a (vertical).

base	2	3	4	5	6	7	8	9	10	11
$1+2\mathrm{i}$	0	0	0	0	0	0	0	0	1	0
$1+4\mathrm{i}$	0	0	1	0	0	0	0	0	0	1
$1+6\mathrm{i}$	0	1	2	0	2	0	0	1	0	1
$1+10\mathrm{i}$	0	1	1	0	0	0	2	1	2	1
$2+5\mathrm{i}$	0	0	1	0	1	0	0	0	0	1
$2+7\mathrm{i}$	0	0	1	0	1	0	2	1	0	1
$3+8\mathrm{i}$	0	1	2	1	0	0	1	1	0	1
$3+10\mathrm{i}$	0	1	2	0	1	0	2	1	1	1
$4+5\mathrm{i}$	0	0	1	0	0	0	1	0	0	1
$4+9\mathrm{i}$	0	0	1	0	0	0	1	0	0	1

One of the reasons explaining this phenomenon is that Carmichael numbers, which always appear when combining two classical Fermat tests, are avoided when we combine a Fermat test and a Gaussian Fermat test, because Carmichael numbers are not necessarily G-Carmichael numbers and conversely. In fact, there are no Carmichael numbers of the form $4k+3$ smaller than 10^{18} which are also G-Carmichael numbers.

Recall that an integer n is called an r-Williams number [6], [21] if

$$p \mid n \;\Rightarrow\; p+r \mid n+r \text{ and } p-r \mid n-r.$$

The next result relates our previous discussion with 1-Williams numbers.

Proposition 6.1. *An odd number $n \equiv 3 \pmod 4$ is simultaneously a Carmichael number and a G-Carmichael number if and only if n is a 1-Williams number and $p \equiv 3 \pmod 4$ for every p dividing n.*

P r o o f. Let $n \equiv 3 \pmod 4$, then $\mathcal{F}(n) = n + 1$. If n is both a Carmichael and a G-Carmichael number we have that, for every p dividing n

$$\begin{aligned} &p - 1 \mid n - 1, \\ &p - 1 \mid n + 1 \quad \text{if } p \equiv 1 \pmod 4, \\ &p + 1 \mid n + 1 \quad \text{if } p \equiv 3 \pmod 4. \end{aligned}$$

Now, if there exists a prime factor $p \equiv 1 \pmod 4$ it follows that $n-1 = (p-1)k \equiv 0 \pmod 4$, a contradiction. Hence, every prime factor is congruent with 3 modulo 4 and n is a 1-Williams number.

On the other hand, if n is a 1-Williams number, then for each prime factor p of n we have $p - 1 \mid n - 1$ and $p + 1 \mid n + 1$, so n is a Carmichael number. If n were a G-Carmichael number it would be also necessary that every factor $p \equiv 1 \pmod 4$ satisfy $p - 1 \mid n + 1$. But, by hypothesis, n does not have this kind of factors and the result follows. □

Thus, the search for a number of the form $n \equiv 3 \pmod 4$ which is both a G-Carmichael number and a Carmichael number is harder than to find a 1-Williams number and, up to date, no 1-Williams number is known

References

[1] *W. R. Alford, A. Granville, C. Pomerance*: There are infinitely many Carmichael numbers. Ann. Math. (2) *139* (1994), 703–722.

[2] *D. Borwein, C. Maitland, M. Skerritt*: Computation of an improved lower bound to Giuga's primality conjecture. Integers (electronic only) *13* (2013), Paper A67, 14 pages.

[3] *P. Burcsi, S. Czirbusz, G. Farkas*: Computational investigation of Lehmer's totient problem. Ann. Univ. Sci. Budap. Rolando Eötvös, Sect. Comput. *35* (2011), 43–49.

[4] *R. D. Carmichael*: Note on a new number theory function. Amer. Math. Soc. Bull. (2) *16* (1910), 232–238.

[5] *J. T. Cross*: The Euler φ-function in the Gaussian integers. Am. Math. Mon. *90* (1983), 518–528.

[6] *O. Echi*: Williams numbers. C. R. Math. Acad. Sci., Soc. R. Can. *29* (2007), 41–47.

[7] *W. Galway*: Tables of pseudoprimes and related data. `http://www.cecm.sfu.ca/Pseudoprimes/`.

[8] *G. Giuga*: Su una presumibile proprietà caratteristica dei numeri primi. Ist. Lombardo Sci. Lett., Rend., Cl. Sci. Mat. Natur. (3) *14* (1951), 511–528. (In Italian.)

[9] *J. R. Goldman*: Numbers of solutions of congruences: Poincaré series for strongly non-degenerate forms. Proc. Am. Math. Soc. *87* (1983), 586–590.

[10] *G. H. Hardy, E. M. Wright*: An Introduction to the Theory of Numbers. Oxford University Press, Oxford, 2008.
[11] *D. H. Lehmer*: On Euler's totient function. Bull. Am. Math. Soc. *38* (1932), 745–751.
[12] *F. Lemmermeyer*: Conics—a poor man's elliptic curves. Preprint at `http://www.fen.bilkent.edu.tr/~franz/publ/conics.pdf`. arXiv:math/0311306v1[math.NT].
[13] *R. G. E. Pinch*: Absolute quadratic pseudoprimes. Proc. of Conf. on Algorithmic Number Theory. TUCS General Publications 46 (A.-M. Ernvall-Hytönen at al., eds.). 2007, pp. 113–128. `http://tucs.fi/publications/view/?id=pErJuKaLe07a&table=proceeding`.
[14] *C. Pomerance, J. L. Selfridge, S. S. Wagstaff,* Jr.: The pseudoprimes to $25 \cdot 10^9$. Math. Comput. *35* (1980), 1003–1026.
[15] *J. Schettler*: Lehmer's totient problem and Carmichael numbers in a PID. `http://math.ucsb.edu/~jcs/Schettler.pdf`.
[16] *J. H. Silverman*: Elliptic Carmichael numbers and elliptic Korselt criteria. Acta Arith. *155* (2012), 233–246.
[17] *N. J. A. Sloane*: The On-Line Encyclopedia of Integer Sequences. `http://www.oeis.org`.
[18] *G. A. Steele*: Carmichael numbers in number rings. J. Number Theory *128* (2008), 910–917.
[19] *T. Szele*: Über die endlichen Ordnungszahlen zu denen nur eine Gruppe gehört. Comment. Math. Helv. *20* (1947), 265–267. (In German.)
[20] *G. Tarry, I. Franel, A. R. Korselt, G. Vacca*: Problème chinois. L'intermédiaire des mathématiciens *6* (1899), 142–144. `www.oeis.org/wiki/File:Problème_chinois.pdf`. (In French.)
[21] *H. C. Williams*: On numbers analogous to the Carmichael numbers. Can. Math. Bull. *20* (1977), 133–143.

Authors' addresses: José María Grau, Departamento de Matemáticas, Universidad de Oviedo, Avenida Calco Sotelo s/n, 33007, Gijón, Spain, e-mail: `grau@uniovi.es`; Antonio M. Oller-Marcén, Centro Universitario de la Defensa de Zaragoza, Ctra. de Huesca s/n, 50090, Zaragoza, Spain, e-mail: `oller@unizar.es`; Manuel Rodríguez, Avenida Ramón Ferreriro 19, 27002, Lugo, Spain, e-mail: `rodlopmanuel@gmail.com`; Daniel Sadornil, Departamento de Matemáticas, Estadística y Computación, Universidad de Cantabria, Avenida de los Castros s/n, 39005, Santander, Spain, e-mail: `daniel.sadornil@unican.es`.