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.