Grau, José María; **Oller-Marcén, Antonio M.**; **Rodríguez, Manuel**; **Sadornil, Daniel**
Fermat test with Gaussian base and Gaussian pseudoprimes. (English) Zbl 1363.11012
Czech. Math. J. 65, No. 4, 969-982 (2015).

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

MSC:

11A51 Factorization; primality

Cited in **1** Document

Keywords:

Gaussian integer; Fermat test; pseudoprime

Software:

OEIS

Full Text: DOI Link

References:

[1] W. R. Alford, A. Granville, C. Pomerance: There are infinitely many Carmichael numbers. Ann. Math. (2) 139 (1994), 703–722. · Zbl 0816.11005 · doi:10.2307/2118576

[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. · Zbl 1284.11002

[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. · Zbl 1240.11005

[4] R. D. Carmichael: Note on a new number theory function. Amer. Math. Soc. Bull. (2)16 (1910), 232–238. · Zbl 41.0226.04 · doi:10.1090/S0002-9904-1910-01892-9

[5] J. T. Cross: The Euler' -function in the Gaussian integers. Am. Math. Mon. 90 (1983), 518–528. · Zbl 0525.12001 · doi:10.2307/2322785

[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.) · Zbl 0045.01801

[9] J. R. Goldman: Numbers of solutions of congruences: Poincaré series for strongly nondegenerate forms. Proc. Am. Math. Soc. 87 (1983), 586–590. · Zbl 0511.12014

[10] G. H. Hardy, E. M. Wright: An Introduction to the Theory of Numbers. Oxford University Press, Oxford, 2008. · Zbl 1159.11001

[11] D. H. Lehmer: On Euler's totient function. Bull. Am. Math. Soc. 38 (1932), 745–751. · Zbl 58.0158.01 · doi:10.1090/S0002-9904-1932-05521-5

[12] F. Lemmermeyer: Conics-a poor man's elliptic curves. Preprint at http://www.fen.bilkent.edu.tr/\(\sim\)franz/publ/conics.pdf.arXiv:math/03113 /\(\sim\)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 {\(\cdot\)} 109. Math. Comput. 35 (1980), 1003–1026.

[15] J. Schettler: Lehmer's totient problem and Carmichael numbers in a PID. http://math.ucsb.edu/\(\sim\)jcs/Schettler.pdf .

[16] J. H. Silverman: Elliptic Carmichael numbers and elliptic Korselt criteria. Acta Arith. 155 (2012), 233–246. · Zbl 1304.11047

· doi:10.4064/aa155-3-1

[17] N. J. A. Sloane: The On-Line Encyclopedia of Integer Sequences. http://www.oeis.org . · Zbl 1274.11001

[18] G. A. Steele: Carmichael numbers in number rings. J. Number Theory 128 (2008), 910–917. · Zbl 1176.11049 · doi:10.1016/j.jnt.2007.08.009

[19] T. Szele: Über die endlichen Ordnungszahlen zu denen nur eine Gruppe gehört. Comment. Math. Helv. 20 (1947), 265–267. (In German.) · Zbl 0034.30502 · doi:10.1007/BF02568132

[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 /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. · Zbl 0368.10011 · doi:10.4153/CMB-1977-025-9