Journal of
Mathematical
Inequalities
Volume 17, Number 4 (2023), 1323–1333
doi:10.7153/jmi-2023-17-86

REPRESENTATIONS OF ELEMENT AS SUM OF PRIMITIVE ROOT AND LEHMER NUMBER IN $\mathbb{Z}_p$

BO ZHANG, JIANKANG WANG, YONGLI SU AND ZHEFENG XU*

Abstract. Let p be an odd prime and $\mathbb{Z}_p$ the residue class ring modulo p. In this paper, we study representations of any element of $\mathbb{Z}_p$ as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_p$, and give an explicit inequality better than asymptotic formula for the number of representations. From this inequality, we obtained that each element of $\mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root for $p > 2.5 \times 10^{14}$. Moreover, using the algorithm we provided, we examined all the cases when $p < 10^6$ by computer. We also analyzed the time complexity of the algorithm and illustrated that it is extremely difficult to verify all the cases up to the bound 2.5×10^{14}, and conjectured that any given element $n \in \mathbb{Z}_p$ can be represented as the sum of a Lehmer number and a primitive root in $\mathbb{Z}_p$ for all primes p except 2, 3, 5, 7, 11, 19, 31.

Mathematics subject classification (2020): 11A07, 11N69, 11L05.

Keywords and phrases: Residue class ring, Lehmer number, primitive root, representation, numerical computation.

REFERENCES

[1] J. CILLERUELO, ANA ZUMALACÁRREGUI, *An additive problem in finite fields with powers of elements of large multiplicative order*, Rev. Mat. Comput., **27** (2014) 501–508.

[2] S. D. COHEN, G. L. MULLEN, *Primitive elements in Costas arrays*, Appl. Algebra Eng. Comm. Comput, **2** (1991) 45–53.

[3] S. D. COHEN, W. P. ZHANG, *Sums of two exact powers*, Finite Fields Appl., **8** (2002) 471–477.

[4] S. D. COHEN, T. TRUDGAIN, *Lehmer numbers and primitive roots modulo a prime*, J. Number Theory, **203** (2019) 68–79.

[5] C. V. GARCIA, *A note on an additive problem with powers of a primitive root*, Bol. Soc. Mat. Mexicana, **11** (2005) 1–4.

[6] M. Z. GARAEV, KA-LAM KUEH, *Distribution of special sequences modulo a large prime*, Int. J. Math. Math. Sci., **50** (2003) 3189–3194.

[7] R. K. GUY, *Unsolved Problems in Number Theory*, 3rd. edn, Springer-Verlag, New York, 2004.

[8] S. W. GOLOMB, *Algebraic constructions for costas arrays*, J. Comb. Theory, **37** (1984) 13–21.

[9] S. R. LOUBOUTIN, J. RIVAT, A. SARKOZY, *On a Problem of D. H. Lehmer*, Proc. Amer. Math. Soc., **135** (2007) 969–975.

[10] Y. M. LU, Y. YI, *Partitions involving D. H. Lehmer numbers*, Monatsh. Math., **159** (2010) 45–58.

[11] I. E. SHPARLINSKI, *On a generalisation of a Lehmer problem*, Math. Z., **263** (2009) 619–631.

[12] I. E. SHPARLINSKI, A. WINTERHOF, *Partitions into two Lehmer numbers*, Monatsh. Math., **160** (2010) 429–441.

[13] M. VÂJÂITU, A. ZAHARESCU, *Differences between powers of a primitive root*, Int. J. Math. Math. Sci. **29** (2002), 325–331.

[14] J. P. WANG, *On Golomb's conjectures*, Sci. Sinica Ser. A **31** (1988) 152–161.

[15] Z. F. XU, W. P. ZHANG, *On a problem of D. H. Lehmer over short intervals*, J. Math. Anal. Appl., **320** (2006) 756–770.

[16] W. P. ZHANG, *A problem of D. H. Lehmer and its generalization (II)*, Compositio Math., **91** (1994) 47–56.

Paper JMI-17-86