This holds for $p = 7$ and $g = 3$. The remaining two cases $-g^2 \pm g + 1 = 0$ are equivalent because $-g^2 + g + 1 = 0$ if and only if $-g^{-2} - g^{-1} + 1 = 0$. In other words, we only need to consider the equality $g^2 = g + 1$ over $\mathbb{F}_p$. Such a primitive root g is called a *Fibonacci primitive root* modulo p, as the *golden ratio* φ_{gr} satisfying $\varphi_{gr}^2 = \varphi_{gr} + 1$. The primes p such that $\mathbb{F}_p$ has a Fibonacci primitive root is the sequence A003147: $5, 11, 19, 31, 41, 59, 61, 71, 79, 109, \ldots$ on OEIS [Slo]. Consequently, we have $N(p, (p-1)/2) > 0$ if and only if $\mathbb{F}_p$ has a Fibonacci primitive root. On the other hand, the order $|H|$ of the subgroup $H = \langle -1, 2\rangle$ is an even integer. It follows that $\ell_0 = \frac{p-1}{|H|}$ must divide $\frac{p-1}{2}$. By Proposition 5.3, we see that Equation (2) is solvable over $\mathbb{F}_p$ if $\mathbb{F}_p$ has a Fibonacci primitive root. In this case, there exists a solution $(x, y) \in \mathbb{F}_p^2$ such that $xy \neq 0$ and thus Conjecture C holds.

Proposition 5.4. *If $\mathbb{F}_p$ has a Fibonacci primitive root, then* Conjecture C *holds for this p.*

On a related issue, for the valid cases in Conjecture C established above we would like to know how many prime numbers p are there such that the subgroup H generated by -1 and 2 has the given index ℓ_0 in $\mathbb{F}_p^\times$. This question can be viewed as a generalization of the Artin's primitive root conjecture. It is shown in [Mur91, Theorem 1] that there are infinitely many primes p such that the index $[\mathbb{F}_p^\times : H] = \ell_0$ under the *Generalized Riemann Hypothesis* (GRH). Assuming GRH, we conclude from Corollary B that there are infinitely many prime numbers p with ℓ_0 satisfying conditions in Theorem 5.2 and therefore, the size of optimal CACs of prime lengths is equal to $M(p, \ell_0)$ for *infinitely many* primes p.

Acknowledgment

We would like to thank Professor Yuan-Hsun Lo for bringing [FLS14] to our attention. The first named author is partially supported by MOST grant 110-2115-M-003-007-MY2. The second named author is partially supported by MOST grant 111-2115-M-003-005. The third named author is supported by MOST grant 110-2811-M-003-530.

References

[AA53] D.R. Anderson and T.M. Apostol. The evaluation of Ramanujan's sum and generalizations. *Duke Math. J.*, 20(2):211–216, 1953. doi:10.1215/S0012-7094-53-02021-3.

[Bur11] D.M. Burton. *Elementary Number Theory*. McGraw-Hill, New York, 2011.

[FLM10] H.-L. Fu, Y.-H. Lin, and M. Mishima. Optimal conflict-avoiding codes of even length and weight 3. *IEEE Trans. Inform. Theory*, 56(11):5747–5756, 2010. doi:10.1109/TIT.2010.2069270.

[FLS14] H.-L. Fu, Y.-H. Lo, and S.W. Shum. Optimal conflict-avoiding codes of odd length and weight three. *Des. Codes Cyptogr.*, 72(2):289–309, 2014. doi:10.1007/s10623-012-9764-5.

[GV93] L. Györfi and I. Vajda. Constructions of protocol sequences for multiple access collision channel without feedback. *IEEE Trans. Inform. Theory*, 39(5):1762–1765, 1993. doi:10.1109/18.259673.

[Har77] R. Hartshore. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics*. Springer, New York, 1977. doi:10.1007/978-1-4757-3849-0.