#A111 INTEGERS 21 (2021)

PROOF OF TWO CONJECTURES OF ANDRICA AND BAGDASAR

Jon Grantham
Institute for Defense Analyses/Center for Computing Sciences, Bowie, Maryland
grantham@super.org

Received: 7/20/21, Accepted: 11/10/21, Published: 11/19/21

Abstract

Andrica and Bagdasar conjecture that there are infinitely many Pell-Lucas pseudoprimes and Pell-Pell-Lucas pseudoprimes. We generalize these pseudoprimality definitions and show that they are satisfied by certain Carmichael numbers. As these Carmichael numbers comprise an infinite set, the conjectures are proven.

1. Introduction

In [2], Andrica and Bagdasar define and conjecture the infinitude of two types of pseudoprimes. We prove a relationship to Carmichael numbers which, along with a previous result, proves the conjectures.

This article demonstrates a technique that can be applied to other pseudoprimes with respect to recurrence sequences. In [3], the author related many notions of pseudoprime to the definition of Frobenius pseudoprimes. In [4], the infinitude of these pseudoprimes was established by proving that there are infinitely many Frobenius pseudoprimes. The present paper takes a different approach — it uses a result from the latter paper to prove the conjectures directly.

2. Let's Remember Some Definitions

We recall from Andrica and Bagdasar [2] the following sequences.

Definitions 1. The *Pell sequence* P_n is given by $P_0 = 0$, $P_1 = 1$ and $P_{n+2} = 2P_{n+1} + P_n$. The *Pell-Lucas sequence* Q_n is given by $Q_0 = 2$, $Q_1 = 2$, $Q_{n+2} = 2Q_{n+1} + Q_n$. In fact, the *generalized Pell sequence* $U_n(a,b)$ is given by $U_0 = 0$, $U_1 = 1$, $U_{n+2} = aU_{n+1} - bU_n$. The *generalized Pell-Lucas sequence* $V_n(a,b)$ is given by $V_0 = 2$, $V_1 = a$, $V_{n+2} = aV_{n+1} - bV_n$.

They observe that $P_n = U_n(2,-1)$ and $Q_n = V_n(2,-1)$, and they define notions of pseudoprimality related to these sequences.

Definition 2. A *Pell-Lucas pseudoprime* is a composite n satisfying $Q_n \equiv 2 \bmod n$. A *Pell-Pell-Lucas pseudoprime* is a composite where $Q_n \equiv 2 \bmod n$ and $P_{n-(-1)^{\frac{n^2-1}{8}}} \equiv 0 \bmod n$.

Note that a Pell-Pell-Lucas pseudoprime is also a Pell-Lucas pseudoprime.

Furthermore, the generalized sequences are integers if and only if $b = \pm 1$. We introduce the following generalization.

Definition 3. Let a and b be integers such that $b = \pm 1$ and $a^2 - 4b \neq 0$. A *generalized Pell-Lucas pseudoprime with parameters* (a, b) is a composite n where $V_n(a, b) \equiv a \bmod n$, and a *generalized Pell-Pell-Lucas pseudoprime* is a composite where both $V_n(a, b) \equiv a \bmod n$ and $U_{n-(-1)^{\frac{n^2-1}{8}}}(a, b) \equiv 0 \bmod n$ hold.

Note that a generalized Pell-Pell-Lucas pseudoprime with parameters (a, b) is also a generalized Pell-Lucas pseudoprime with parameters (a, b), so it suffices to prove the conjecture for generalized Pell-Pell-Lucas pseudoprimes.

Finally, we recall what a Carmichael number is.

Definition 4. A Carmichael number is a composite integer n such that for every $x \in \mathbb{Z}$, $x^n \equiv x \bmod n$.

3. Proof of the Conjectures

Theorem 1. *Let ζ_8 be a primitive 8th root of unity. Let a and b be as in Definitions 3. A Carmichael number n such that for all $p|n$, p splits completely in $\mathbb{Q}[\sqrt{a^2-4b}, \zeta_8]$, is also a generalized Pell-Pell-Lucas pseudoprime with parameters (a, b).*

Proof. For compactness, we write $U_n = U_n s(a, b)$ and $V_n = V_n(a, b)$ below.

We recall a couple of Binet-like formulas from [2]. Let $f(x) = x^2 - ax + b$; it has discriminant $a^2 - 4b$. If r_1 and r_2 are the roots of $f(x)$ in a ring R, $V_n = r_1^n + r_2^n$ and $U_n = \frac{r_1^n - r_2^n}{r_1 - r_2}$ when evaluated in R.

Because p splits completely in $\mathbb{Q}[\sqrt{a^2-4b}, \zeta_8]$, it splits completely in the subfield $\mathbb{Q}[\sqrt{a^2-4b}]$. This statement is equivalent to the fact that $x^2 - ax + b$ splits into two linear factors modulo each $p|n$. (See, for example, [5], Proposition I.8.3). Recalling that Carmichael numbers are squarefree, we have that $f(x)$ splits modulo n into two linear factors, $x - r_1$ and $x - r_2$. Because the discriminant is nonzero, these are distinct roots.

Because n is a Carmichael number, $r_1^n \equiv r_1$ and $r_2^n \equiv r_2 \bmod n$, and we have $V_n \equiv r_1 + r_2 \equiv a \bmod n$. Therefore, n is a generalized Pell-Lucas pseudoprime.

To verify that it is a generalized Pell-Pell-Lucas pseudoprime, we must show that $U_{n-(-1)^{\frac{n^2-1}{8}}} \equiv 0 \bmod n$.

Because each $p|n$ splits completely in $\mathbb{Q}[\zeta_8]$, it is 1 modulo 8. Because n is a product of numbers that are 1 mod 8, it is 1 mod 8 itself, and therefore $n - (-1)^{\frac{n^2-1}{8}} \equiv n - 1$. So we must show that $U_{n-1} \equiv 0 \bmod n$.

We have $U_{n-1} = \frac{r_1^{n-1} - r_2^{n-1}}{r_1 - r_2}$. Because n is a Carmichael number, $r_1^{n-1} \equiv r_2^{n-1} \equiv 1$ and $U_{n-1} \equiv 0 \bmod n$. □

Corollary 1. *There are infinitely many generalized Pell-Pell-Lucas pseudoprimes.*

Proof. We refer to Theorem 4.1 of [4], which proves that there are infinitely many Frobenius pseudoprimes by constructing Carmichael numbers all of whose primes split completely in any number field K. Here we take $K = \mathbb{Q}[\sqrt{a^2 - 4b}, \zeta_8]$. □

4. Conclusion

The proof could also be accomplished by taking primes congruent to 1 modulo $8(a^2 - 4b)$, and then modifying the original proof that there are infinitely many Carmichael numbers [1] so that all prime factors of the Carmichael numbers are in this congruence. By using the proof of [4], though, we need not modify the details of any proofs. Further, that paper discusses a third-order recurrence sequence — Perrin's sequence, and likewise the technique in this article could be applied to other pseudoprimes with respect to higher-order recurrence sequences.

Acknowledgements. The author thanks his colleagues, Katie Ahrens and Hester Graves, for being close readers of a draft version of this article. Their helpful comments much improved the final version.

References

[1] W. R. Alford, Andrew Granville, and Carl Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math. (2)*, **139** (1994), 703–722.

[2] Dorin Andrica and Ovidiu Bagdasar, On some new arithmetic properties of the generalized Lucas sequences, *Mediterr. J. Math.*, **18** (2021), Paper No. 47.

[3] Jon Grantham, Frobenius pseudoprimes, *Math. Comp.*, **70** (2001), 873–891.

[4] Jon Grantham, There are infinitely many Perrin pseudoprimes, *J. Number Theory*, **130** (2010), 1117–1128.

[5] Jürgen Neukirch, *Algebraic Number Theory*, Springer-Verlag, Berlin, 1999.