MATHEMATICA, 64 (87), N° 1, 2022, pp. 34–38

ON A CONJECTURE OF AYAD AND KIHEL

ZOULIKHA BELBARGAT

Abstract. In this paper,we will prove some cases of the conjecture by Ayad and Kihel about Catalan pseudoprimes and generalize a result by the author.

MSC 2010. 11A07.
Key words. Catalan number, pseudoprime.

1. INTRODUCTION

The Catalan numbers are the set of integers given recursively by

$$C_0 = 1 \quad \text{and} \quad C_n = \sum_{i=0}^{n-1} C_i C_{n-1-i} \text{ for } n \geq 1.$$

The nth Catalan number is given explicitly as

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

The only prime Catalan numbers are $C_2 = 2$ and $C_3 = 5$, but we can suitably define some Catalan numbers as Catalan pseudoprimes. The definition for these Catalan pseudoprimes follows similarly to that of the Fermat pseudoprimes, which we briefly recall here. Fermat's little theorem states that if p is a prime number and a is an integer relatively prime to p, then $a^{p-1} \equiv 1 \pmod{p}$. While the converse is not true in general, there exist infinitely many n, the Carmichael numbers or Fermat pseudoprimes, for which $a^{n-1} \equiv 1 \pmod{n}$. A theorem of Lucas [5] states that if p is a prime number, then $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$ for every $0 \leq k < p$. Setting $k = \frac{p-1}{2}$ yields

$$(-1)^{\frac{p-1}{2}} C_{\frac{p-1}{2}} \equiv 2 \pmod{p}$$

whenever p is an odd prime. Aebi and Cairns [1] provided an alternative proof of this same equivalence, which motivates the definition of the Catalan pseudoprimes (A163209 in the OEIS [6]): a Catalan pseudoprime is an odd integer n such that

$$(-1)^{\frac{n-1}{2}} C_{\frac{n-1}{2}} \equiv 2 \pmod{n}.$$

The authors thank the referee for his helpful comments and suggestions.

DOI: 10.24193/mathcluj.2022.1.05

Aebi and Cairns [1] proceeded to prove the following result:

THEOREM 1.1. *If p and q are odd primes such that $p < q < 2p$, then pq is not a Catalan pseudoprime.*

Ayad and Kihel [2] made the following conjecture:

CONJECTURE 1.2. *If p and q are two odd primes, then pq is not a Catalan pseudoprime.*

Belbargat [3] then proved the following generalization of Theorem 1.1:

THEOREM 1.3. *Let p and q be odd primes such that $p < q < p^2$, and let l be the unique positive integer such that $lp < q < (l+1)p$. If l is odd, then pq is not a Catalan pseudoprime.*

The aim of this paper is to further generalize Theorems 1.1 and 1.3, proving more cases of Conjecture 1.2. In particular, we prove the following theorem:

THEOREM 1.4. *Let p and q be odd primes such that $p < q$. If the p-adic expansion of q is of the form*

$$q = \sum_{i=0}^{n} a_i p^i$$

where a_j is odd for a single $j \in \{1, \ldots, n\}$ and a_i is even for all $i \in \{0, \ldots, n\} \setminus \{j\}$, then pq is not a Catalan pseudoprime.

2. PROOF OF THE MAIN RESULT

The proof of Theorem 1.4 relies on two lemmas. The first lemma is a result due to Cai and Granville [4].

LEMMA 2.1. *If p and q are distinct odd primes, then*

$$\binom{pq-1}{\frac{pq-1}{2}} = \binom{p-1}{\frac{p-1}{2}}\binom{q-1}{\frac{q-1}{2}} \pmod{pq}.$$

The second lemma is the well-known Legendre formula:

LEMMA 2.2. *Let n be a positive integer. Then the p-adic valuation of $n!$ is given by*

$$v_p(n!) = \frac{n - s_p}{p-1},$$

where s_p represents the sum of the digits in the p-adic expansion of n.

With these at our disposal, we proceed to the proof of Theorem 1.4.

Proof. For convenience, we let $I = \{1, \dots, n\}$. Since p does not divide q, we have $a_0 \neq 0$. Then $q - 1 = (a_0 - 1) + \sum_{i \in I} a_i p^i$ so that

$$\begin{aligned} v_p\big((q-1)!\big) &= \frac{q - 1 - \left((a_0 - 1) + \sum_{i \in I} a_i\right)}{p-1} \\ &= \frac{(a_0 - 1) + \sum_{i \in I} a_i p^i - (a_0 - 1) - \sum_{i \in I} a_i}{p-1} \\ &= \frac{1}{p-1} \sum_{i \in I} a_i (p^i - 1). \end{aligned}$$

Writing a_i as $2b_i$ for each $i \in I \setminus \{j\}$ and $a_j = 2k + 1$, we obtain

$$\begin{aligned} \frac{q-1}{2} &= \frac{1}{2} \left((2b_0 - 1) + (2k+1)p^j + \sum_{i \in I \setminus \{j\}} 2b_i p^i \right) \\ &= b_0 + kp^j + \frac{p^j - 1}{2} + \sum_{i \in I \setminus \{j\}} b_i p^i \\ &= b_0 + kp^j + \frac{p-1}{2} \left(1 + p + \cdots + p^{j-1}\right) + \sum_{i \in I \setminus \{j\}} b_i p^i \\ &= kp^j + \sum_{0 \leq i < j} \left(\frac{p-1}{2} + b_i \right) p^i + \sum_{j < i \leq n} b_i p^i. \end{aligned}$$

Since $b_i \leq \frac{p-1}{2}$ for each $i \in I \setminus \{j\}$, we have $\frac{p-1}{2} + b_i < p$. Thus, we have the p-adic expansion of $\frac{q-1}{2}$. It follows that

$$\begin{aligned} v_p\left(\left(\frac{q-1}{2}\right)!\right) &= \frac{\frac{q-1}{2} - \left(k + \sum_{0 \leq i < j} \left(\frac{p-1}{2} + b_i \right) + \sum_{j < i \leq n} b_i \right)}{p-1} \\ &= \frac{1}{2(p-1)} \left(a_0 - 1 + \sum_{i \in I} a_i p^i - 2k - \sum_{0 \leq i < j} (p - 1 + a_i) - \sum_{j < i \leq n} a_i \right) \\ &= \frac{1}{2(p-1)} \left(\sum_{i \in I} a_i p^i - (2k+1) - \sum_{0 \leq i < j} (p-1) - \sum_{i \in I \setminus \{j\}} a_i \right) \\ &= \frac{1}{2(p-1)} \left(\sum_{i \in I} a_i p^i - j(p-1) - \sum_{i \in I} a_i \right) \end{aligned}$$

$$= \frac{1}{2(p-1)} \left(\sum_{i \in I} a_i(p^i - 1) - j(p-1) \right)$$
$$= \frac{1}{2} v_p\big((q-1)!\big) - \frac{j}{2}.$$

Consequently, we obtain

$$v_p\left(\Big(\frac{q-1}{2} \Big)!^2 \right) = v_p\big((q-1)!\big) - j,$$

and conclude that

$$v_p \binom{q-1}{\frac{q-1}{2}} = j > 0.$$

Therefore,

$$\binom{q-1}{\frac{q-1}{2}} \equiv 0 \pmod{p}.$$

Suppose now for contradiction that pq is a Catalan pseudoprime. Then

$$\binom{pq-1}{\frac{pq-1}{2}} \equiv (-1)^{\frac{pq-1}{2}} \pmod{pq},$$

and Lemma 2.1 implies that

$$\binom{pq-1}{\frac{pq-1}{2}} \equiv \binom{p-1}{\frac{p-1}{2}} \binom{q-1}{\frac{q-1}{2}} \pmod{pq}.$$

Since

$$\binom{p-1}{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$$

by Lucas' theorem, we obtain

$$\binom{q-1}{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \pmod{p},$$

which is a contradiction. Thus, pq cannot be a Catalan pseudoprime. □

3. CONCLUDING REMARKS

We conclude by justifying that Theorem 1.4 is indeed a generalization of Theorem 1.3 and, by extension, also of Theorem 1.1. Suppose that p and q are two prime numbers statisfying the conditions of Theorem 1.3. Then we have $p < q < p^2$ and an odd integer l such that $lp < q < (l+1)p$.

Writing q in its p-adic expansion

$$q = \sum_{i=0}^{n} a_i p^i$$

it follows from $0 \leq a_i < p$ for each $i \in \{0, \ldots, n\}$ that $p < q < p^2$ imposes on q the form

$$q = a_1 p + a_0.$$

Since both p and q are assumed odd, exactly one of $\{a_0, a_1\}$ must be odd. We have $lp < q < (l+1)p$, from which we obtain the two inequalities

$$a_1 p < a_1 p + a_0 = q < (l+1)p$$

and

$$lp < q = a_1 p + a_0 < a_1 p + p = (a_1 + 1)p.$$

The first yields $a_1 < l + 1$, while the second yields $a_1 + 1 > l$ or $l - 1 < a_1$. Since a_1 is an integer, we deduce that $a_1 = l$, which itself is assumed odd under the conditions of Theorem 1.3. Thus, a_1 is odd, a_0 is even, and the conditions of Theorem 1.4 are satisfied.

That Theorems 1.3 and 1.4 are not equivalent follows by way of an example. The only known Catalan pseudoprimes are $\{5907, 1194649, 12327121\}$, and the fourth would necessarily either have more than two prime factors or be greater than 10^{10} [1]. In light of this, we choose an appropriate example. Let $p = 1087$ and $q = 16785407$. The 1087-adic expansion of 16785407 is

$$16785407 = 14 \cdot 1087^2 + 223 \cdot 1087^1 + 1040 \cdot 1087^0.$$

This clearly satisfies the conditions of Theorem 1.4, so $pq = 18245737409$ is not a Catalan pseudoprime. It is also clear that showing such is beyond the reach of Theorems 1.3 and 1.1 as 16785407 is not less than 1087^2 or $2 \cdot 1087$ respectively.

REFERENCES

[1] C. Aebi and G. Cairns, *Catalan numbers, primes, and twin primes*, Elem. Math., **63** (2008), 153–164.
[2] M. Ayad and O. Kihel, *Recognizing the primes using permutations*, Int. J. Number Theory, **8** (2012), 2045–2057.
[3] Z. Belbargat, *On the Catalan pseudoprimes*, J. Comb. Number Theory, **6** (2014), 63–66.
[4] T.X. Cai and A. Granville, *On the residues of binomial coefficients and their products modulo prime powers*, Acta Math. Sin. (Engl. Ser.), **18** (2002), 277–288.
[5] E. Lucas, Amer. J. Math., **1** (1897), 229–230.
[6] N.J.A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, https://oeis.org.

Received July 5, 2020
Accepted March 16, 2021

University of Oran1, Ahmed Benbella
Department of Mathematics
Laboratory of mathematics
and its applications(LAMAP)
Oran, Algeria
E-mail: b.zoulikha@live.fr
https://orcid.org/0000-0003-1705-9538