MATHEMATICA, 60 (83), N° 1, 2018, pp. 48–53

A BRIEF REMARK ON BALANCING-WIEFERICH PRIMES

UTKAL KESHARI DUTTA, BIJAN KUMAR PATEL, and PRASANTA KUMAR RAY

Abstract. A prime p is said to be a balancing-Wieferich prime if it satisfies the congruence $B_{p-(\frac{8}{p})} \equiv 0 \pmod{p^2}$, equivalently $\pi(p) = \pi(p^2)$. Here B_n denotes the n-th balancing number and $\pi(m)$ is the period of balancing numbers modulo any positive integer m. In this note, we establish some conditions related to the balancing-Wieferich primes.

MSC 2010. 11B25, 11B39, 11B41.

Key words. Balancing numbers, Wieferich primes, balancing-Wieferich primes, periodicity.

1. INTRODUCTION

It is well known that, if p is a prime and a is any integer such that $p \nmid a$, then p divides $a^{p-1} - 1$ and the quotient $\frac{a^{p-1}-1}{p}$ is the Fermat quotient with base a. It is also known that a prime p is a Wieferich prime, if it satisfies $2^{p-1} \equiv 1 \pmod{p^2}$. The primes 1093 and 3511 are the only two known Wieferich primes to date. Sun and Sun [16] proved that, if $p \nmid xyz$ and $x^p + y^p = z^p$, then p^2 divides $F_{p-(\frac{5}{p})}$, where $\{F_n\}$ is the well-known Fibonacci sequence and $(\frac{m}{n})$ denotes the Legendre symbol of m and n. In [4], Elsenhans and Jahnel showed that p^2 divides $F_{p-(\frac{5}{p})}$ if and only if the period of the Fibonacci sequence modulo prime p equals the period of the Fibonacci sequence modulo the square of that prime. The primes satisfying $F_{p-(\frac{5}{p})} \equiv 0 \pmod{p^2}$ are called Fibonacci-Wieferich primes or Sun-Sun primes [2]. According to Mcintosh and Roettger [10], there are no Fibonacci-Wieferich primes less than $p < 2 \times 10^{14}$. Later the bound was improved to 9.7×10^{14} in [3].

The modular representation of Fibonacci sequence modulo any positive integer was studied by Wall [17] in the year 1960. Many important and interesting properties concerning the periodicity of the Fibonacci numbers were established by Marques in [6, 7, 8, 9]. Recently, Panda and Rout [12] considered the periods of the balancing numbers modulo any positive integer that involved some divisibility properties regarding these numbers. They defined

---

The authors wish to thank the referees for useful comments and suggestions. P.K. Ray is the corresponding author.

DOI: 10.24193/mathcluj.2018.1.05

the period of the balancing sequence modulo m, $\pi(m)$, as the least positive integer t satisfying $(B_t, B_{t+1}) \equiv (0,1) \pmod{m}$. In [12], they also conjectured that 13, 31 and 1546463 are the only three primes satisfying $\pi(p) = \pi(p^2)$, which is analogous to the congruence

$$B_{p-(\frac{8}{p})} \equiv 0 \pmod{p^2}.$$

Rout [15] later called those primes as balancing Wieferich primes. Analogously, the primes satisfying $B_{p-(\frac{8}{p})} \not\equiv 0 \pmod{p^2}$ are called balancing non-Wieferich primes. In [15], he also proved that there are infinitely many balancing non-Wieferich primes under the assumption of the *abc* conjecture.

It is now worthy to define the balancing numbers. A balancing number n and its balancer r are the solutions of the Diophantine equation $1+2+\cdots+(n-1) = (n+1)+(n+2)+\cdots+(n+r)$ (see [1]). A balancing sequence $\{B_n\}$ satisfies the recurrence relation $B_{n+1} = 6B_n - B_{n-1}, n \geq 1$, starting with $B_0 = 0$ and $B_1 = 1$, whose Binet formula is given by $B_n = \frac{\lambda_1^n - \lambda_2^n}{4\sqrt{2}}$, where $\lambda_1 = 3+2\sqrt{2}$ and $\lambda_2 = (\lambda_1)^{-1}$ are the roots of the balancing characteristic polynomial $g(x) = x^2 - 6x + 1$ (see [1, 11]). Balancing numbers can be also generated through matrices, which are studied extensively in [14]. A balancing matrix denoted by Q_B is a second order matrix whose entries are the first three balancing numbers 0, 1 and 6, that is

$$Q_B = \begin{pmatrix} 0 & 1 \\ -1 & 6 \end{pmatrix}$$

and its n-th power is

$$Q_B^n = \begin{pmatrix} -B_{n-1} & B_n \\ -B_n & B_{n+1} \end{pmatrix}$$

for any positive integer n (see [14]). In [13], Patel and Ray redefined the period of the balancing numbers, by using the matrix concept. They defined $\pi(p)$ as the smallest positive integer k satisfying $Q_B^k \equiv I \pmod{p}$, where I is the identity matrix of the same order as Q_B. It follows that $\pi(p^2)$ is the smallest positive integer s for which $Q_B^s \equiv I \pmod{p^2}$.

In order to prove the results of the present work, we consider a matrix T_p defined by $T_p = \frac{1}{p}(Q_B^{\pi(p)} - I) = [b_{ij}]$ for any prime p. Consequently,

$$T_p = \begin{pmatrix} -b_{11} & b_{21} \\ -b_{21} & 6b_{21} - b_{11} \end{pmatrix}.$$

The proofs of our results closely follow the work of Klaška [5].

2. PRELIMINARIES

In this section, we need some results which are useful to prove our main theorems.

The following lemma directly follows from the definition of T_p.

LEMMA 2.1. *For any prime p, $\pi(p) \neq \pi(p^2)$ if and only if $T_p \not\equiv 0 \pmod p$.*

LEMMA 2.2. *For $p \neq 2$, $T_p \equiv 0 \pmod p$ if and only if* $\mathrm{detT_p} \equiv 0 \pmod{\mathrm{p}}$.

Proof. The necessary part is trivial. In order to prove the sufficient part, we choose $p \neq 2$ and assume that $\mathrm{detT_p} \equiv 0 \pmod{\mathrm{p}}$. In view of

$$T_p = \begin{pmatrix} -b_{11} & b_{21} \\ -b_{21} & 6b_{21} - b_{11} \end{pmatrix} = \frac{1}{p}(Q_B^{\pi(p)} - I),$$

we have

$$\mathrm{det}Q_B^{\pi(p)} = 1 + 2p(3b_{21} - b_{11}) + p^2\mathrm{detT_p}, \tag{1}$$

where

$$\mathrm{detT_p} = \mathrm{b}_{11}^2 - 6\mathrm{b}_{11}\mathrm{b}_{21} + \mathrm{b}_{21}^2.$$

As $\mathrm{detQ_B} = 1$ and p divides $\mathrm{detT_p}$, (1) reduces to $3b_{21} - b_{11} \equiv 0 \pmod p$ and $\mathrm{detT_p} \equiv -\frac{8}{9}\mathrm{b}_{11}^2 \pmod{\mathrm{p}}$. It follows that $b_{11} \equiv 0 \pmod p$ and hence $3b_{21} \equiv 0 \pmod p$. This completes the proof. □

Let Q_p be the field of p-adic numbers. Consider L_p as the splitting field over Q_p of the balancing characteristic polynomial $g(x) = x^2 - 6x + 1$. Let λ_1 and λ_2, belonging to the ring of integers $\mathcal{O}_p$, be the zeros of $g(x)$ in L_p. Since the discriminant of $g(x)$ is 32, for prime $p \neq 2$, L_p/Q_p does not ramify and the maximal ideal of $\mathcal{O}_p$ is generated by p. For $\xi \in \mathcal{O}_p$, $\mathrm{ord_{p^s}}(\xi)$ is the least positive rational integer l for which $\xi^l \equiv 1 \pmod{p^s}$. Since $\xi^l \equiv 1 \pmod p$, we have $\xi^{pl} \equiv 1 \pmod{p^2}$, which implies either $\mathrm{ord_{p^2}}(\xi) = \mathrm{ord_p}(\xi)$ or $\mathrm{ord_{p^2}}(\xi) = \mathrm{p} \cdot \mathrm{ord_p}(\xi)$. Moreover, if $\xi \neq \pm 1$ and t is the largest positive integer for which $\mathrm{ord_{p^t}}(\xi) = \mathrm{ord_p}(\xi)$, then we have $\mathrm{ord_{p^s}}(\xi) = \mathrm{p^{s-t}}\mathrm{ord_p}(\xi)$ for $s \geq t$.

LEMMA 2.3. *For any prime $p \neq 2$,* $\mathrm{ord_{p^s}}(\lambda_1) = \mathrm{ord_{p^s}}(\lambda_2)$.

Proof. Since $\lambda_1\lambda_2 = 1$, it follows that $\lambda_1 = \pm 1$ if and only if $\lambda_2 = \pm 1$. Now, if $\lambda_2^v = 1$, then $\lambda_1^v = 1$, which gives $\mathrm{ord_{p^s}}(\lambda_1) = \mathrm{ord_{p^s}}(\lambda_2)$. On the other hand, if $\lambda_2^v = -1$, then $\lambda_2^{2v} = 1$. It follows that $\lambda_1^{2v} = 1$ and hence $\mathrm{ord_{p^s}}(\lambda_1) = \mathrm{ord_{p^s}}(\lambda_2)$ and the result follows. □

From the above result, we conclude that, for $p \neq 2$,

$$\mathrm{ord_{p^2}}(\lambda_2) \equiv 0 \pmod{\mathrm{p}} \text{ if and only if } \mathrm{ord_{p^2}}(\lambda_1) \equiv 0 \pmod{\mathrm{p}}. \tag{2}$$

In order to prove the following result, we choose $q = |\mathcal{O}_p/(p)|$ for $p \neq 2$, from which it follows that $q = p^t$, where $t = [L_p : Q_p] \in \{1, 2\}$.

LEMMA 2.4. $\mathrm{ord_{p^2}}(\lambda_1) \not\equiv 0 \pmod{\mathrm{p}}$ *if and only if* $\lambda_1^{q-1} \equiv 1 \pmod{p^2}$.

Proof. Let $r = \mathrm{ord_{p^2}}(\lambda_1)$ and $p \nmid r$. As $[\mathcal{O}_p/(p)]$ has $q(q-1)$ elements, $r \mid q(q-1)$. Since $q = p^t$, it follows that $r \mid (q-1)$ and therefore $\lambda_1^{q-1} \equiv 1 \pmod{p^2}$.

Conversely, assume that $\lambda_1^{q-1} \equiv 1 \pmod{p^2}$. It follows that $r \mid (q-1)$. Since $p \nmid (q-1)$, we conclude that $p \nmid \mathrm{ord_{p^2}}(\lambda_1)$. This ends the proof. □

3. MAIN RESULTS

THEOREM 3.1. *Let s be any positive integer and p be any odd prime. Then* $\pi(p^s) = \operatorname{lcm}\big(\mathrm{ord}_{\mathrm{p^s}}(\lambda_1),\ \mathrm{ord}_{\mathrm{p^s}}(\lambda_2)\big)$.

Proof. For any positive integer n and $C, D \in L_p$, let $B_n = C\lambda_1^n + D\lambda_2^n$, where the coefficients C and D are determined uniquely. The above system of equations can be rewritten in the matrix form as follows:

$$\begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \begin{pmatrix} C \\ D \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Since $\lambda_1 \not\equiv \lambda_2 \pmod{p}$, $C = -(\lambda_2 - \lambda_1)^{-1}$ and $D = (\lambda_2 - \lambda_1)^{-1}$. Letting $k = \pi(p^s)$, we can write

$$(C\lambda_1^k + D\lambda_2^k,\ C\lambda_1^{k+1} + D\lambda_2^{k+1}) \equiv (C + D,\ C\lambda_1 + D\lambda_2) \pmod{p^s}.$$

This can be rewritten as

$$\begin{pmatrix} 1 & 1 \\ \lambda_1 & \lambda_2 \end{pmatrix} \begin{pmatrix} C(\lambda_1^k - 1) \\ D(\lambda_2^k - 1) \end{pmatrix} \equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \pmod{p^s}.$$

It follows that $C(\lambda_1^k - 1) \equiv 0 \pmod{p^s}$ and $D(\lambda_2^k - 1) \equiv 0 \pmod{p^s}$. Further simplification reduces the above congruences to $(\lambda_1^k, \lambda_2^k) \equiv (1, 1) \pmod{p^s}$. Therefore, $\mathrm{ord}_{\mathrm{p^s}}(\lambda_1)$ and $\mathrm{ord}_{\mathrm{p^s}}(\lambda_2)$ both divide k and thus we have that $\operatorname{lcm}(\mathrm{ord}_{\mathrm{p^s}}(\lambda_1), \mathrm{ord}_{\mathrm{p^s}}(\lambda_2))$ divides k.

On the other hand, as $(C, D) \not\equiv (0, 0) \pmod{p}$, the period of the sequences $(C\lambda_1^n)_{n=0}^{\infty}$ and $(D\lambda_2^n)_{n=0}^{\infty}$ modulo p^s are $\mathrm{ord}_{\mathrm{p^s}}(\lambda_1)$ and $\mathrm{ord}_{\mathrm{p^s}}(\lambda_2)$, respectively. Thus the period of the sequence $(B_n)_{n=0}^{\infty} = (C\lambda_1^n + D\lambda_2^n)_{n=0}^{\infty}$ modulo p^s, which is $\pi(p^s)$, divides $\operatorname{lcm}\big(\mathrm{ord}_{\mathrm{p^s}}(\lambda_1),\ \mathrm{ord}_{\mathrm{p^s}}(\lambda_2)\big)$ and the result follows. $\square$

THEOREM 3.2. *For any prime $p \neq 2$, $\pi(p) \neq \pi(p^2)$ if and only if* $\mathrm{ord}_{\mathrm{p^2}}(\lambda_1) \equiv 0 \pmod{\mathrm{p}}$ *and* $\mathrm{ord}_{\mathrm{p^2}}(\lambda_2) \equiv 0 \pmod{\mathrm{p}}$.

Proof. Let $\mathrm{ord}_{\mathrm{p^2}}(\lambda_1) \equiv 0 \pmod{\mathrm{p}}$ and $\mathrm{ord}_{\mathrm{p^2}}(\lambda_2) \equiv 0 \pmod{\mathrm{p}}$. Then

$$\operatorname{lcm}\big(\mathrm{ord}_{\mathrm{p^2}}(\lambda_1),\ \mathrm{ord}_{\mathrm{p^2}}(\lambda_2)\big) \equiv 0 \pmod{\mathrm{p}}.$$

Combining this with Theorem 3.1 for $s = 2$, we have

$$\pi(p^2) = \operatorname{lcm}\big(\mathrm{ord}_{\mathrm{p^2}}(\lambda_1) \text{ and } \mathrm{ord}_{\mathrm{p^2}}(\lambda_2)\big) \equiv 0 \pmod{\mathrm{p}}.$$

Since p is the maximal ideal of $\mathcal{O}_p$ and $\pi(p) = \operatorname{lcm}\big(\mathrm{ord}_{\mathrm{p}}(\lambda_1),\ \mathrm{ord}_{\mathrm{p}}(\lambda_2)\big)$, $\pi(p) \not\equiv 0 \pmod{p}$. The above discussion implies $\pi(p) \neq \pi(p^2)$. Conversely, let $\pi(p) \neq \pi(p^2)$. So $\pi(p^2) = p\pi(p)$. From Theorem 3.1, we have

$$\operatorname{lcm}\big(\mathrm{ord}_{\mathrm{p^2}}(\lambda_1),\ \mathrm{ord}_{\mathrm{p^2}}(\lambda_2)\big) \equiv 0 \pmod{\mathrm{p}},$$

which implies $\mathrm{ord}_{\mathrm{p^2}}(\lambda_1) \equiv 0 \pmod{\mathrm{p}}$ or $\mathrm{ord}_{\mathrm{p^2}}(\lambda_2) \equiv 0 \pmod{\mathrm{p}}$. This, together with (2), gives $\mathrm{ord}_{\mathrm{p^2}}(\lambda_1) \equiv 0 \pmod{\mathrm{p}}$ and $\mathrm{ord}_{\mathrm{p^2}}(\lambda_2) \equiv 0 \pmod{\mathrm{p}}$, which ends the proof. $\square$

From equation (2) and Theorem 3.2, we have $\mathrm{ord}_{\mathrm{p^2}}(\lambda_1) \not\equiv 0 \pmod{\mathrm{p}}$ and $\mathrm{ord}_{\mathrm{p^2}}(\lambda_2) \not\equiv 0 \pmod{\mathrm{p}}$ if and only if p is a balancing-Wieferich prime.

THEOREM 3.3. *Let $p \neq 2, w \in \mathcal{O}_p$ for which $g(w) \equiv 0 \pmod{p}$. Then p is a balancing-Wieferich prime if and only if $w^{2q} - 6w^q + 1 \equiv 0 \pmod{p^2}$, or equivalently, $g(w) + (w^q - w)g'(w) \equiv 0 \pmod{p^2}$.*

Proof. For $w \in \mathcal{O}_p$, consider $w^2 - 6w + 1 \equiv 0 \pmod{p}$. It follows that either $w \equiv \lambda_1 \pmod{p}$ or $w \equiv \lambda_2 \pmod{p}$. We first assume $w \equiv \lambda_1 \pmod{p}$. This implies that $w^q \equiv \lambda_1^q \pmod{p^2}$. Now, for $\pi(p) = \pi(p^2)$, $w^q \equiv \lambda_1^q \equiv \lambda_1 \pmod{p^2}$. Consequently, $w^{2q} - 6w^q + 1 \equiv w^2 - 6w + 1 \equiv 0 \pmod{p^2}$.

Conversely, assume that $w^{2q} - 6w^q + 1 \equiv 0 \pmod{p^2}$. Let $w^q = \lambda_1 + pv$. Therefore, $w^{2q} - 6w^q + 1 = (\lambda_1 + pv)^2 - 6(\lambda_1 + pv) + 1 \equiv 2pv(\lambda_1 - 3) \equiv 0 \pmod{p^2}$. For $p \neq 2$, $\lambda_1 - 3 \not\equiv 0 \pmod{p}$, we have $v \equiv 0 \pmod{p}$. Thus $w^q = \lambda_1 + pv \equiv \lambda_1 \pmod{p^2}$ and hence $\lambda_1^{q-1} \equiv w^{q(q-1)} \equiv 1 \pmod{p^2}$. Using Lemma 2.4, $\mathrm{ord}_{\mathrm{p}^2}(\lambda_1) \not\equiv 0 \pmod{\mathrm{p}^2}$. Theorem 3.2, together with (2) , gives $\pi(p) = \pi(p^2)$. Moreover, for $w = \lambda_1 + pr$, $g(w) + (w^q - w)g'(w) \equiv (\lambda_1^q - \lambda_1)(2\lambda_1 + 2pr - 6) \equiv 0 \pmod{p^2}$. Assuming $\pi(p) = \pi(p^2)$, we have $\lambda_1^q \equiv \lambda_1 \pmod{p^2}$, consequently $(\lambda_1^q - \lambda_1)(2\lambda_1 + 2pr - 6) \equiv 0 \pmod{p^2}$. On the other hand, for $p \neq 2$, $2\lambda_1 + 2pr - 6 \equiv 2w - 6 \equiv 2\lambda_1 - 6 \equiv g'(\lambda_1) \not\equiv 0 \pmod{p}$. Therefore, $\lambda_1^q - \lambda_1 \equiv 0 \pmod{p^2}$. Using Lemma 2.4 and $\lambda_1^q \equiv \lambda_1 \pmod{p^2}$, we conclude that $\pi(p) = \pi(p^2)$. This ends the proof. $\square$

REFERENCES

[1] A. Behera and G. K. Panda, *On the square roots of triangular numbers*, Fibonacci Quart., **37** (1999), 98–105.

[2] R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp., **66** (1997), 443–449.

[3] F. Dorais and D. Klyve, *A Wiefeich prime search up to* 6.7×10^{15}, J. Integer Seq., **14**, Article 11.9.2 (2011), 1–14.

[4] A.S. Elsenhans and J. Jahnel, *The Fibonacci sequence modulo* p^2*-An investigation by computer for* $p < 10^{14}$, The On-Line Encyclopedia of Integer Sequences, 1–26.

[5] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. J., **58** (2008), 1241–1246.

[6] D. Marques, *On the order of appearance of integers at most one away from Fibonacci numbers*, Fibonacci Quart., **50** (2012), 36–43.

[7] D. Marques, *The order of appearance of powers Fibonacci and Lucas numbers*, Fibonacci Quart., **50** (2012), 239–245.

[8] D. Marques, *The order of appearance of product of consecutive Lucas numbers*, Fibonacci Quart., **51** (2013), 38–43.

[9] D. Marques, *The order of appearance of product of five consecutive Lucas numbers*, Tatra Mt. Math. Publ., **59** (2014), 65–77.

[10] R.J. Mcintosh and E.L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp., **76** (2007), 2087–2094.

[11] G.K. Panda, *Some fascinating properties of balancing numbers*, Congr. Numer., **194** (2009), 185–189.

[12] G.K. Panda and S.S. Rout, *Periodicity of balancing numbers*, Acta Math. Hungar., **143** (2014), 274–286.

[13] B.K. Patel and P.K. Ray, *The period, rank and order of the sequence of balancing numbers modulo m*, Math. Rep. (Bucur.), **18** (2016), 395–401.

[14] P.K. Ray, *Certain matrices associated with balancing and Lucas-balancing numbers*, Matematika, **28** (2012), 15–22.
[15] S.S. Rout, *Balancing non-Wieferich primes in arithmetic progression and abc conjecture*, Proc. Japan Acad. Ser. A Math. Sci., **92** (2016), 112–116.
[16] Z.H. Sun and Z.W. Sun, *Fibonacci numbers and Fermat's last theorem*, Acta Arith., **60** (1992), 371–388.
[17] D.D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly, **67** (1960), 525–532.

Received November 2, 2017
Accepted January 23, 2018

Sambalpur University
Department of Mathematics
Sambalpur, India
E-mail: utkaldutta@gmail.com

International Institute of Information Technology
Bhubaneswar, India
E-mail: iiit.bijan@gmail.com

Sambalpur University
Department of Mathematics
Sambalpur, India
E-mail: prasantamath@suniv.ac.in