Submitted to the Bulletin of the Australian Mathematical Society
doi:10.1017/S ...

PERIODS OF DUCCI SEQUENCES AND ODD SOLUTIONS TO A PELLIAN EQUATION

FLORIAN BREUER

Abstract

A Ducci sequence is a sequence of integer n-tuples generated by iterating the map

$$D : (a_1, a_2, \dots, a_n) \mapsto (|a_1 - a_2|, |a_2 - a_3|, \dots, |a_n - a_1|).$$

Such a sequence is eventually periodic and we denote by $P(n)$ the maximal period of such sequences for given n. Upper bounds on $P(n)$ have been known since the 1980's. In this paper, we prove a new upper bound in the case where n is a power of a prime $p \equiv 5 \bmod 8$ for which 2 is a primitive root and the Pellian equation

$$x^2 - py^2 = -4$$

has no solutions in odd integers x and y.

2010 *Mathematics subject classification:* primary 11B83; secondary 11D09, 11R18.
Keywords and phrases: Ducci sequences, Pellian equation, Cyclotomic fields, Real quadratic units.

1. Introduction

Let n be a positive integer and consider the map $D : \mathbb{Z}^n \to \mathbb{Z}^n$ defined by

$$D : (a_1, a_2, \dots, a_n) \mapsto (|a_1 - a_2|, |a_2 - a_3|, \dots, |a_n - a_1|).$$

A sequence of integer n-tuples obtained by iterating this map is known as a Ducci sequence, in honor of E. Ducci, who first studied them in the 1930s and discovered that every such sequence of integer n-tuples eventually stabilizes at $(0, 0, \dots, 0)$ if and only if n is a power of 2, see [8].

Ducci sequences and their generalizations have received much attention in the literature, see for example [4–7, 9, 11, 18] and the references therein, and they have been independently rediscovered in various guises by various authors, for example in [1–3, 12, 16].

Since the entries in a Ducci sequence remain bounded, the sequence eventually becomes periodic, and in this paper, we're interested in the period $P(n)$ of the Ducci sequence starting with $(0, \dots, 0, 1)$.

The function $P(n)$ was studied in detail in [11], where the following results may be found: The period of any Ducci sequence of n-tuples divides $P(n)$, n divides $P(n)$

and $P(2^k n) = 2^k P(n)$, thus it suffices to study $P(n)$ for odd n. Furthermore, one has the following upper bounds on $P(n)$.

THEOREM 1.1. *Suppose n is odd.*

1. *Denote by* $m = \mathrm{ord}_n(2)$ *the multiplicative order of* 2 *modulo n. Then* $P(n)$ *divides* $B_1(n) := 2^m - 1$.
2. *Suppose there exists an integer M for which* $2^M \equiv -1 \bmod n$, *in this case we say that "n is with a* -1*". Let M be the smallest such integer, then* $P(n)$ *divides* $B_2(n) := n(2^M - 1)$.

In [4] we list the first few odd values of n satisfying various sharpness conditions relative to the bounds in Theorem 1.1. In particular, the first examples of n with a -1 for which $P(n) < B_2(n)$ were found to be $n = 37, 101, 197, 269, 349, 373, 389, 541, 557$ and 677. Searching the Online Encyclopedia of Integer Sequences we find that, with the exception of 541, these are the first nine entries of Sequence A130229 [15]: the primes of the form $p \equiv 5 \bmod 8$ for which the Pellian equation

$$x^2 - py^2 = -4 \tag{1.1}$$

has no solution in odd integers x and y.

Our goal is to prove the following result, which explains this discovery.

THEOREM 1.2. *Let* $p \equiv 5 \bmod 8$ *be a prime such that* 2 *is a primitive root modulo p, and for which the equation (1.1) has no solution in odd integers x and y. Then* $P(p)$ *divides* $\frac{1}{3}B_2(p)$.

If furthermore p is not a Wieferich prime, then $P(p^k)$ *divides* $\frac{1}{3}B_2(p^k)$ *for all positive integers k.*

Recall that an integer a is a primitive root modulo n if $\mathrm{ord}_n(a) = \varphi(n)$, i.e. a generates $(\mathbb{Z}/n\mathbb{Z})^*$. Artin's Conjecture states every non-square integer $a \neq -1$ is a primitive root modulo p for infinitely many primes p. When 2 is a primitive root modulo n, then $2^{\mathrm{ord}_n(2)/2} \equiv -1 \bmod n$, so n is with a -1.

A prime p is called a Wieferich prime if $2^{p-1} \equiv 1 \bmod p^2$. Only two Wieferich primes are known, 1093 and 3511, neither of which satisfies the hypothesis of Theorem 1.2. However, a standard heuristic argument suggests that the number of Wieferich primes $p \leq x$ should grow like $\log\log(x)$, see [5, §9].

The condition that 2 be a primitive root modulo p in Theorem 1.2 is essential: the first entry in sequence A130229 which for which 2 is not a primitive root is 997 and in fact we have $P(997) = B_2(997) = 997(2^{166} - 1)$.

The case $n = 541$ does not fit into our scheme, instead $P(541) = \frac{1}{7}B_2(541)$.

2. Periods and cyclotomy

It is known (see e.g. [7]) that the tuples in the periodic part of a Ducci sequence all lie in $\{0, c\}^n$, for some constant c. Therefore, after discarding the common factor c, we may assume that all entries lie in $\{0,1\}^n = \mathbb{F}_2^n$, in which case the Ducci operator D becomes linear:

$$D : \mathbb{F}_2^n \to \mathbb{F}_2^n; \quad (a_1, a_2, \ldots, a_n) \mapsto (a_1 + a_2, a_2 + a_3, \ldots, a_n + a_1).$$

Next, mapping a tuple $u = (a_1, a_2, \ldots, a_n)$ to the element represented by the polynomial $f = a_1x^{n-1} + a_2x^{n-2} + \cdots + a_n$ in the ring $R = \mathbb{F}_2[x]/\langle x^n - 1\rangle$, we find that the Ducci sequence $u, Du, D^2u, \ldots \in \mathbb{F}_2^n$ corresponds to the sequence $f, (x+1)f, (x+1)^2 f, \ldots \in R$, an idea going back to [18].

We thus find that $P(n)$ equals the multiplicative period of $x + 1$ in R. Realizing R as the ring of cyclotomic integers modulo 2, we thus obtain (see [5, Thm. 5.2])

Theorem 2.1. *Suppose n is odd. Denote by $L = \mathbb{Q}(\zeta_n)$ the n^{th} cyclotomic field, where $\zeta_n \in \mathbb{C}$ is a primitive n^{th} root of unity. Denote by $\mathcal{O}_L = \mathbb{Z}[\zeta_n]$ the ring of integers in L. Let $\mathfrak{P} \subset \mathcal{O}_L$ be a prime ideal containing 2. Then $P(n)$ equals the lowest common multiple of the multiplicative orders of $\zeta + 1$ modulo $\mathfrak{P}$, where ζ ranges over all n^{th} roots of unity $\zeta \neq 1$.*

Since $(\mathcal{O}_L/\mathfrak{P})^*$ has order $B_1(n)$, we recover the bound $P(n)|B_1(n)$. Note that $\zeta + 1 = (1 - \zeta^2)/(1 - \zeta)$ is a unit in $\mathcal{O}_L$ by [10, Prop. 3.5.5], so one source of sharper bounds on $P(n)$ is when the units of $\mathcal{O}_L$ generate a proper subgroup of $(\mathcal{O}_L/\mathfrak{P})^*$. Determining the units of $\mathcal{O}_L$ is generally difficult, but under certain circumstances this phenomenon can be detected already at the level of a quadratic subfield $\mathbb{Q}(\sqrt{d}) \subset L = \mathbb{Q}(\zeta_n)$, which is where the Pellian equation (1.1) comes into play.

3. Proof of Theorem 1.2

Suppose that $p \equiv 5 \bmod 8$ and that 2 is a primitive root modulo $n = p^k$. If p is not a Wieferich prime, then this follows if 2 is a primitive root modulo p, by [10, Prop. 2.1.24]. Now 2 remains prime in $\mathbb{Q}(\zeta_n)$, i.e. $\mathfrak{P} = 2\mathcal{O}_L$, by [10, Prop. 3.5.18].

By [10, Prop. 3.4.1 and Prop. 3.5.14], $\mathbb{Q}(\zeta_p)$, and thus also L, contains the real quadratic field $K = \mathbb{Q}(\sqrt{p})$, whose ring of integers is $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{p})/2]$. Let $\mathfrak{p} = \mathfrak{P} \cap K = 2\mathcal{O}_K$.

Since $\mathfrak{p}$ is inert in L/K, we have $\mathrm{Gal}(L/K) \cong \mathrm{Gal}\left((\mathcal{O}_L/\mathfrak{P})/(\mathcal{O}_K/\mathfrak{p})\right)$, and thus the norm $N_{L/K} : L \to K$ induces the commutative diagram

$$\begin{tikzcd} \mathcal{O}_L^* \arrow[r] \arrow[d, "N_{L/K}"] & (\mathcal{O}_L/\mathfrak{P})^* \arrow[d, two heads, "N"] \\ \mathcal{O}_K^* \arrow[r] & (\mathcal{O}_K/\mathfrak{p})^* \end{tikzcd}$$

where the second vertical map is the norm of finite fields, which is surjective by [10, Prop. 2.4.12].

The group of units $\mathcal{O}_K^*$ is generated by -1 and the fundamental unit $\varepsilon = (x + y\sqrt{p})/2$, where (x, y) is the fundamental solution to the equation (1.1), see [10, Prop.

6.3.16] and [17]. Therefore, we see that the units O_K^* generate the trivial subgroup $\{1\} < (O_K/\mathfrak{p})^* \cong \mathbb{F}_4^*$ if and only if (1.1) has no odd solutions. In this case, the image of the bottom horizontal arrow is a subgroup of index 3. It follows that the image of the top arrow lies in a subgroup of index 3 and thus $P(n)|\frac{1}{3}B_1(n)$. Since $p \equiv 1 \bmod 4$, we have $3|B_2(n) = n(2^{p^{k-1}(p-1)/2} - 1)$ and so the following lemma completes the proof of Theorem 1.2.

Lemma 3.1. *Suppose n is with a -1. Let $\ell \nmid n$ be an odd prime with $\ell | B_2(n)$. Then $P(n)|\frac{1}{\ell}B_2(n)$ if and only if $P(n)|\frac{1}{\ell}B_1(n)$.*

Proof. Let $m = \mathrm{ord}_n(2)$, then $B_2(n) = n(2^{m/2} - 1)$. Since $\ell|B_2(n)$ and $\ell \nmid n$, we have $\ell | 2^{m/2} - 1$. Since ℓ is odd, $\ell \nmid 2^{m/2} + 1$. Now denote by $v_\ell(x)$ the ℓ-adic order of x. We have

$$v_\ell(B_1(n)) = v_\ell(2^m-1) = v_\ell((2^{m/2}-1)(2^{m/2}+1)) = v_\ell(2^{m/2}-1) = v_\ell(n(2^{m/2}-1)) = v_\ell(B_2(n)).$$

The result follows. □

4. Remarks

As the example of $p = 997$ shows, our argument requires 2 to remain prime in $\mathbb{Q}(\zeta_n)$. This means that 2 generates $(\mathbb{Z}/n\mathbb{Z})^*$ and so $n = p^k$ for some prime p. We must have $p \equiv 3$ or $5 \bmod 8$, otherwise 2 is a square modulo p. Furthermore, we need $3|B_2(n)$, which requires $p \equiv 1 \bmod 4$. This explains the condition $p \equiv 5 \bmod 8$.

We expect that there are infinitely many primes p for which (1.1) has no odd solutions. Heuristically, we expect the fundamental unit to fall in each of the three non-zero residue classes modulo $\mathfrak{p}$ with equal probability, which suggests that these primes have density $1/3$ in the set of all primes $p \equiv 5 \bmod 8$. Meanwhile, the Generalised Riemann Hypothesis implies that the proportion of primes $p \equiv 5 \bmod 8$ for which 2 is a primitive root is $A/2$, where $A \approx 0.3739558$ is Artin's constant, as follows from the main result of [14]. Assuming that these two conditions on p are independent, we thus expect that the primes satisfying the hypothesis of Theorem 1.2 have density $A/6 \approx 0.0623259689$.

Numerically, we find that for primes up to 10^9, this proportion is 0.0612819, but this proportion creeps up as one considers ever larger upper bounds on p, see Figure 1. This suggests that a Chebychev bias-type phenomenon might be at work.

It is known that there are infinitely many squarefree integers $d \equiv 5 \bmod 8$ for which the equation

$$x^2 - dy^2 = 4$$

has no odd solutions, see [17]. (One can replace -4 by 4 in (1.1), this has the effect of merely squaring the fundamental unit).

Finally, our argument is related to that in [13]. That paper considers the same fields $K \subset L$ as we do, and uses the unit $N_{L/K}(1 + \zeta_n) \in O_K^*$ to produce a relatively small solution to (1.1).

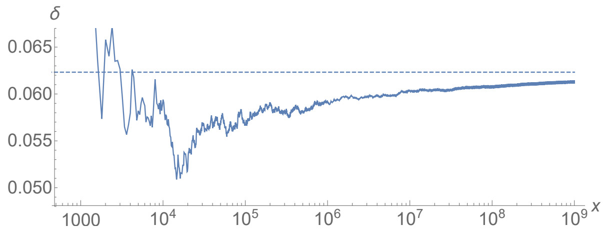

FIGURE 1. Proportion $\delta(x)$ of primes $p \leq x$ for which the hypothesis of Theorem 1.2 holds

Acknowledgement

The author would like to thank the anonymous referee for useful comments and for pointing out the reference [14].

References

[1] V. I. Arnold, Complexity of finite sequences of zeroes and ones and geometry of finite spaces of functions, *Funct. Anal. Other Math.* **1** (2006), 1–15.

[2] A. Behn, C. Kribs-Zaleta, V. Ponomarenko, The convergence of difference boxes, *Amer. Math. Monthly* **112 (5)** (2005) 426–439.

[3] E. R. Berlekamp, The design of slowly shrinking labelled squares, *Math. Comp.* **29** (1975) 25–27.

[4] F. Breuer, E. Lötter, A.B. van der Merwe, Ducci sequences and cyclotomic polynomials, *Finite Fields Appl.* **13** (2007), 293–304.

[5] F. Breuer, Ducci sequences and cyclotomic fields, *J. Difference Equ. Appl.* **16** (2010), no. 7, 847–862.

[6] G. Brockman, R. J. Zerr, Asymptotic behaviour of certain Ducci sequences, *Fibonacci Quart.* **45 (2)** (2007) 155–163.

[7] M. Burmester, R. Forcade and E. Jacobs, Circles of numbers, *Glasgow Math. J.* **19** (1978), 115–119.

[8] C. Ciamberlini and A. Marengoni, Su una interessante curiosità numerica, *Periodiche di Matematiche* **17** (1937), 25–30.

[9] A. Clausing, Ducci Matrices, *Amer. Math. Monthly*, to appear.

[10] H. Cohen, Number Theory, Volume I: Tools and Diophantine Equations, *Graduate Texts in Mathematics* **239**, Springer-Verlag, 2007.

[11] A. Ehrlich, Periods of Ducci's N-number game of differences, *Fibonacci Quart.* **28 (4)** (1990), 302–305.

[12] B. Freedman, The four number game, *Scripta Math.* **14** (1948) 35–47, reprinted in arXiv:1109.0051v1.

[13] P. G. Hartung, On the Pellian equation, *J. Number Theory* **12 (1)** (1980), 110–112.

[14] P. Moree, On primes in arithmetic progression having a prescribed primitive root. II, *Funct. Approx. Comment. Math.* **39** (2008), 133–144.

[15] On-line Encyclopedia of Integer Sequences, entry #A130229. https://oeis.org/A130229.

[16] G. J. Simmons, The structure of the differentiation digraphs of binary sequences, *Ars Combin.* **35** (1993), A, 71–88.

[17] P. Stevenhagen, On a problem of Eisenstein, *Acta Arith.* **74 (3)** (1996), 259–268.

[18] P. Zvengrowski, Iterated absolute differences, *Math. Mag.* **52 (1)** (1979), 36–40.

Florian Breuer, University of Newcastle, Australia
e-mail: florian.breuer@newcastle.edu.au