RESEARCH ARTICLE

Ducci sequences and cyclotomic fields

Florian Breuer,
Department of Mathematical Sciences, Stellenbosch University, Stellenbosch 7600, South Africa.
Tel: +27 21 8083288, Fax: +27 21 8083828, Email: fbreuer@sun.ac.za
(Received 00 Month 200x; in final form 00 Month 200x)

Let $G$ be an abelian group and $n \in \mathbb{N}$. A Ducci sequence over $G$ is a sequence of $n$-tuples $u, D(u), D^2(u), \ldots \in G^n$, where $D(u_1, u_2, \ldots, u_n) := (u_1 + u_2 + u_3, \ldots, u_n + u_1)$. When $G$ is finite, this sequence is eventually periodic. In this paper, we study Ducci sequences over $G = \mathbb{Z}/p\mathbb{Z}$, where $p \nmid n$, using properties of cyclotomic polynomials. We first characterize the vanishing sequences (i.e. those for which the cyclic part consists only of 0), as well as the tuples in the cyclic part of a sequence. We then derive an expression for the period of a given Ducci sequence in terms of orders of roots of unity plus one modulo powers of a prime above $p$ in a cyclotomic number field. Lastly, the dependence of the period on $t$ leads us to a connection with Wieferich primes.

Keywords: Ducci sequences, cyclotomic fields, cyclotomic polynomials, finite abelian groups, finite fields, multiplicative orders, Wieferich primes.

AMS Subject Classification: 11B83, 11T22

1. Introduction

A Ducci sequence is a sequence of integer $n$-tuples $u, D(u), D^2(u), \ldots \in \mathbb{Z}^n$ generated by

$$D(u_1, \ldots, u_n) := (|u_1 - u_2|, |u_2 - u_3|, \ldots, |u_n - u_1|).$$

For example, when $n = 4$, the Ducci sequence starting with $u = (2, -1, 5, 7)$ is

$$(2, -1, 5, 7), (3, 6, 2, 5), (3, 4, 3, 2), (1, 1, 1, 1), (0, 0, 0, 0), (0, 0, 0, 0), \ldots$$

Indeed, if $n$ is a power of 2, then every Ducci sequence stabilizes at $(0, 0, \ldots, 0)$. This result was first observed by E. Ducci about a century ago, and has been rediscovered many times since. The study of Ducci sequences has recently enjoyed a resurgence of interest, see for example [1, 3–7, 9–11, 16, 18], and the references therein.

Every Ducci sequence eventually forms a cycle, and the periods of these cycles are a popular object of study, see for example [4, 7, 9, 12]. The tuples in such a cycle are constant multiples of binary tuples, i.e. of tuples with entries in $\{0, 1\}$, see e.g. [8]. For binary tuples, then, the absolute difference is merely addition modulo 2, and the operator $D$ becomes linear:

$$D : (\mathbb{Z}/2\mathbb{Z})^n \rightarrow (\mathbb{Z}/2\mathbb{Z})^n; \quad D(u_1, \ldots, u_n) = (u_1 + u_2, u_2 + u_3, \ldots, u_n + u_1).$$

At this point the study of the linear operator $D$ becomes predominantly alge-
braic (see for example [2, 4, 9, 18, 24]), and the following generalisation of Ducci sequences to abelian groups is natural (see [2]):

**Definition 1.1.** Let \( G \) be an abelian group, and \( n \in \mathbb{N} \). A Ducci sequence over \( G \) is a sequence \( u, D(u), D^2(u), \ldots \in G^n \) where

\[
D(u_1, \ldots, u_n) := (u_1 + u_2, u_2 + u_3, \ldots, u_n + u_1).
\]

One may also consider non-abelian groups, of course, but then \( D \) is no longer a group homomorphism and much of the structure is lost. For other generalizations, see for example [3], [10] and [23].

If \( G \) is finite, then every such sequence eventually becomes cyclic, and we denote by \( \text{Per}(u) \) the eventual period of \( u, Du, D^2u, \ldots \). If \( \text{Per}(u) = 1 \), then the cyclic part is just \( 0, 0, 0, \ldots \), in which case we say that \( u \) vanishes. It is shown in [23] that every Ducci sequence in \((\mathbb{Z}/m\mathbb{Z})^n\) vanishes if and only if \( m \) and \( n \) both are powers of 2.

The present paper is a sequel to both [2] and [4], in that we will study Ducci sequences over \( G = \mathbb{Z}/p^t\mathbb{Z} \) using properties of cyclotomic polynomials. The link between Ducci sequences and polynomials is not new, see also [9, 14, 16, 24].

We will assume throughout this paper that \( p \) is a prime not dividing \( n \) (the separable case), and hope to treat the inseparable case in the future. It follows from the structure of finite abelian groups that our results extend easily to any finite abelian group of order prime to \( n \).

We will study extensions of such classic questions as determining which tuples vanish, which tuples are in the cyclic part of a Ducci sequence, how to compute the periods of given sequences, and bounding maximal periods.

The rest of this paper is structured as follows. In §2 we rephrase Ducci sequences in terms of polynomials, and classify the vanishing behavior of Ducci sequences in §3 (Theorem 3.2). In §§4 and 5 we prove our second main result (Theorem 5.2), an expression for the period of a given Ducci sequence in terms of orders of roots of unity plus one. In §§6 and 7 we simplify the computation of such orders (Theorems 6.2 and 7.3). In §8 we study some properties of the maximal period (Theorems 8.1 and 8.2), which extends results of [12]. Lastly, in §9 we explore a simple heuristic argument for the dependence of the maximal period on the exponent \( t \), which also relates to Wieferich primes.

An excellent reference for some technical results from algebraic number theory which we shall use (e.g. Hensel’s Lemma and cyclotomic fields) is the book [20].

### 2. Cyclotomic polynomials

Cyclotomic polynomials are the irreducible factors of \( x^n - 1 \) over \( \mathbb{Z} \), which typically factorize further over \( \mathbb{Z}/p\mathbb{Z} \). Since the characteristic polynomial of the linear operator \( D \) on \((\mathbb{Z}/p\mathbb{Z})^n \) is \((x - 1)^n - 1\), it is hardly surprising that this factorization plays an important role in our approach. But first, we need a definition.

**Definition 2.1.** For any finite ring \( R \) and \( a \in R \), we denote by \( \text{Ord}_R(a) \) the eventual period of the sequence \( 1, a, a^2, \ldots \). (We allow the trivial case \( R = \{0\} \), in which case \( \text{Ord}_R(a) := 1 \).)

If \( a \) is invertible then \( \text{Ord}_R(a) \) is the multiplicative order of \( a \) in \( R^* \).

Consider the polynomial ring

\[
R(t) := \frac{\mathbb{Z}/p^t\mathbb{Z}[x]}{\langle x^n - 1 \rangle}.
\]
We have an isomorphism of abelian groups

\[(\mathbb{Z}/p^i\mathbb{Z})^n \xrightarrow{\sim} R(t)\]

\[u = (u_1, \ldots, u_n) \mapsto f_u(x) = u_1x^{n-1} + u_2x^{n-2} + \cdots + u_n.\]  

Note that \((\mathbb{Z}/p^i\mathbb{Z})^n\) is a \(\mathbb{Z}/p^i\mathbb{Z}[D]\)-module and \(R(t)\) is a \(\mathbb{Z}/p^i\mathbb{Z}[x + 1]\)-module, and (1) is an isomorphism of modules, where the action of \(D\) on \((\mathbb{Z}/p^i\mathbb{Z})^n\) corresponds to multiplication by \((x + 1)\) in \(R(t)\). This idea appears in [24].

Now the Ducci sequence \(u, D(u), D^2(u), \ldots \in (\mathbb{Z}/p^i\mathbb{Z})^n\) corresponds to the sequence

\[f_u(x), (x + 1)f_u(x), (x + 1)^2f_u(x), \ldots\]

in \(R(t)\).

Over the finite field \(\mathbb{F}_p\) we have the following factorization.

\[x^n - 1 = \prod_{d|n} \Phi_d(x) = \prod_{d|n} \prod_{i=1}^{r_d} \phi_{d,i}(x).\]  

Here \(\Phi_d(x)\) is the \(d\)th cyclotomic polynomial, which has degree \(\varphi(d)\) (Euler’s \(\varphi\) function), \(r_d = \varphi(d)/\text{Ord}_{\mathbb{Z}/d\mathbb{Z}}(p) = [(\mathbb{Z}/d\mathbb{Z})^* : \langle p \rangle]\), and each \(\phi_{d,i}(x) \in \mathbb{F}_p[x]\) is irreducible of degree \(\text{Ord}_{\mathbb{Z}/d\mathbb{Z}}(p)\).

As \(p \nmid n\), \(x^n - 1\) is separable and we can lift the factorization (3) to the \(p\)-adic integers \(\mathbb{Z}_p := \lim \downarrow \mathbb{Z}/p^i\mathbb{Z}\), by Hensel’s Lemma. In other words, the factorization (3) also holds in \(\mathbb{Z}_p[x]\), and thus in \(\mathbb{Z}/p^i\mathbb{Z}[x]\) for all \(t \in \mathbb{N}\).

From now on we assume that the polynomials \(\phi_{d,i}(x)\) have coefficients in \(\mathbb{Z}\) and satisfy (3) modulo \(p^i\).

**Example 2.2** Let \(n = 7\) and \(p^i = 8\). Then

\[x^7 - 1 = \Phi_1(x)\Phi_7(x) = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)\]

\[\equiv (x - 1)(x^3 - 2x^2 - 3x + 1)(x^3 + 3x^2 + 2x - 1) \mod 8\]

\[= \phi_{1,1}(x)\phi_{7,1}(x)\phi_{7,2}(x).\]

\(\Box\)

The Chinese Remainder Theorem gives

\[R(t) = \frac{\mathbb{Z}/p^i\mathbb{Z}[x]}{\langle x^n - 1 \rangle} \cong \prod_{d|n} \prod_{i=1}^{r_d} \frac{\mathbb{Z}/p^i\mathbb{Z}[x]}{\langle \phi_{d,i}(x) \rangle} = \prod_{d|n} \prod_{i=1}^{r_d} R_{d,i}(t).\]  

(4)

Since \(\phi_{d,i}(x)\) is irreducible in \(\mathbb{Z}/p^i\mathbb{Z}[x]\), the complete set of ideals of \(R_{d,i}(t)\) is

\[0 = \langle p^i \rangle \subset \langle p^{i-1} \rangle \subset \cdots \subset \langle p \rangle \subset \langle p^0 \rangle = R_{d,i}(t)\].

**3. Vanishing sequences**

Our first result is a classification of vanishing tuples and of tuples in a cycle (i.e. in the cyclic part of a Ducci sequence).
Example 3.1 When $n = 3$ and $p^4 = 8$, then all the vanishing tuples in $(\mathbb{Z}/8\mathbb{Z})^n$ are scalars, and they transition to each other in the following way:

\[
\begin{align*}
(1,1,1) & \rightarrow (5,5,5) \\
(3,3,3) & \rightarrow (2,2,2) \\
(7,7,7) & \rightarrow (6,6,6) \rightarrow (4,4,4) \rightarrow (0,0,0)
\end{align*}
\]

On the other hand, when $n = 4$ and $p^4 = 5$, then the vanishing tuples turn out to be the alternating scalars, which all vanish directly:

\[
(1,4,1,4) \rightarrow (2,3,2,3) \rightarrow (3,2,3,2) \rightarrow (4,1,4,1) \rightarrow (0,0,0,0)
\]

In both cases, the tuples in a cycle make up the orthogonal complement of the set of vanishing tuples. \hfill \square

In general, we have

**Theorem 3.2.** Let $u = (u_1, \ldots, u_n) \in (\mathbb{Z}/p^4\mathbb{Z})^n$, where $p \nmid n$.

1. If $p = 2$ (and $n$ is odd), then $u$ vanishes if and only if $u = (a,a,\ldots,a)$ is a scalar. The tuple $u$ is in a cycle if and only if $\sum_{i=1}^n u_i = 0$ in $G$. The tuple $D^t(u)$ is always in a cycle, but $D^t(0,0,\ldots,0,1)$ is not in a cycle.

2. If $p \neq 2$ and $n$ is even, then $u$ vanishes if and only if $u = (a,-a,a,-a,\ldots)$ is an alternating scalar. The tuple $u$ is in a cycle if and only if $\sum_{i=1}^n (-1)^i u_i = 0$. The tuple $D(u)$ is always in a cycle, but $(0,0,\ldots,0,1)$ is not in a cycle.

3. If $p \neq 2$ and $n$ is odd, then the only vanishing tuple is $(0,0,\ldots,0)$, and every tuple is in a cycle.

**Proof.** First, notice that every element of $R_{d,i}(t)$ is either invertible or nilpotent. The tuple $u$ vanishes if and only if the sequence (2) vanishes in $R_{d,i}(t)$ for all $d,i$. This happens precisely when $f_u(x) = 0$ in those $R_{d,i}(t)$ in which $x + 1$ is invertible. Similarly, $u$ is in a cycle precisely when $f_u(x) = 0$ in those $R_{d,i}(t)$ in which $x + 1$ is nilpotent.

If $p = 2$ (and $n$ is odd), then $x + 1$ is nilpotent in $R_{1,1}(t) = \mathbb{Z}/2\mathbb{Z}[x]/(x-1)$, and invertible in every other $R_{d,i}(t)$. Hence $u$ vanishes if and only if $f_u(x)$ is a multiple of $(x^n - 1)/(x-1) = x^{n-1} + x^{n-2} + \cdots + 1$, and $u$ is in a cycle if and only if $f_u(x)$ is a multiple of $x - 1$, i.e. $f_u(1) = 0$. Note that $f_{D(u)}(1) = 2 f_u(1)$, and (1) follows.

If $p \neq 2$ and $n$ is even, then $x + 1$ is nilpotent (indeed, zero) in $R_{2,1}(t) = \mathbb{Z}/p^4\mathbb{Z}[x]/(x+1)$, and invertible in every other $R_{d,i}(t)$. Hence $u$ vanishes if and only if $f_u(x)$ is a multiple of $(x^n - 1)/(x + 1) = x^{n-1} - x^{n-2} + \cdots - 1$, and $u$ is in a cycle if and only if $f_u(x)$ is a multiple of $x + 1$, i.e. $f_u(-1) = 0$. Since $f_{D(u)}(-1) = 0$, (2) follows.

If $p \neq 2$ and $n$ is odd, then $x + 1$ is invertible in every $R_{d,i}(t)$, and (3) follows. \hfill \square
$D(u) \mid u \in G^n$. This is the state diagram for $G^n$, viewed as a finite automaton with transitions $u \to D(u)$ (see [22]).

The connected component of 0 in $X_n(G)$ consists of the cycle $0 \to 0$, together with a tree of vanishing tuples rooted in 0. We call this the vanishing tree. The other components of $X_n(G)$ consist of non-trivial cycles, with a tree isomorphic to the vanishing tree rooted in each vertex of the cycle.

To describe the structure of $X_n(\mathbb{Z}/p^t\mathbb{Z})$, one must determine the periods of the various cycles, which is the object of the rest of this paper, and determine the vanishing tree. Using Theorem 3.2, we obtain

- If $p = 2$ (and $n$ odd), the vanishing tree consists of all the scalar tuples, arranged in a complete binary tree of height $t$.
- If $p \neq 2$ and $n$ is even, then the vanishing tree consists of all the alternating scalars, each transitioning directly to 0.
- If $p \neq 2$ and $n$ is odd, then the vanishing tree contains the single vertex 0.

4. Periods and orders

We let $\text{Per}_f(x)$ denote the period of the Ducci sequence generated by the tuple corresponding to $f(x) \in \mathbb{Z}/p^t\mathbb{Z}[x]$. It is the period of the sequence (2) in $R(t)$. Similarly, we denote by $\text{Per}_{d,i}(x)$ the period of the sequence (2) in $R_{d,i}(t)$. From (4) we have

$$\text{Per}_f(x) = \text{lcm}_{d \leq t} \text{lcm}_{1 \leq i \leq r_d} \text{Per}_{d,i}(x).$$

**Example 4.1** Let $n = 10$ and $p^t = 27$. The cyclotomic polynomials remain irreducible mod 3 and we have

$$x^{10} - 1 = \phi_{1,1}(x)\phi_{2,1}(x)\phi_{5,1}(x)\phi_{10,1}(x) = (x - 1)(x + 1)(x^4 + x^3 + x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1).$$

Consider the tuple $u = (0, 0, 6, 0, 3, 0, 9, 6, 9, 21) \in \mathbb{Z}/27\mathbb{Z}^{10}$. It corresponds to the polynomial

$$f_u(x) = 6x^7 + 3x^5 + 9x^3 + 6x^2 + 9x + 21 \in R(3) = \mathbb{Z}/27\mathbb{Z}[x]/(x^{10} - 1),$$

and to $(0, 0, 9x^3 + 12x^2 + 9x + 24, 9x^3 + 9x + 18)$ in

$$\mathbb{Z}/27\mathbb{Z}[x]/(x - 1) \oplus \mathbb{Z}/27\mathbb{Z}[x]/(x + 1) \oplus \mathbb{Z}/27\mathbb{Z}[x]/(x^4 + x^3 + x^2 + x + 1) \oplus \mathbb{Z}/27\mathbb{Z}[x]/(x^4 - x^3 + x^2 - x + 1).$$

Now

$$\text{Per}(u) = \text{Per}_f(x) = \text{lcm}\{\text{Per}_{1,1}(f_u(x)), \text{Per}_{2,1}(f_u(x)), \text{Per}_{5,1}(f_u(x)), \text{Per}_{10,1}(f_u(x))\} = \text{lcm}\{1, 1, \text{Ord}_{R_{5,1}}(x + 1), \text{Ord}_{R_{10,1}}(x + 1)\},$$

which follows from the next result. \qed
Proposition 4.2. Let \( r = \nu_p(f(x)) \) be the largest integer \( r \leq t \) such that \( f(x) \mod \phi_{d,i}(x) \) lies in the ideal \((p^r)\) of \( R_{d,i}(t) \). Then

\[
\text{Per}_{d,i}(f(x)) = \text{Ord}_{R_{d,i}(t-r)}(x + 1).
\]

Proof. If \( f(x) = 0 \) in \( R_{d,i}(t) \), then \( \text{Per}_{d,i}(f(x)) = 1 \). Suppose \( f(x) \neq 0 \) in \( R_{d,i}(t) \). Then we may write \( f(x) = p^r u(x) \), where \( u(x) \in R_{d,i}(t) \) is invertible. Recall that \((x + 1)^t f(x)\) is in a cycle, by Theorem 3.2. Then

\[
(x + 1)^{k+t} f(x) = (x + 1)^t f(x) \quad \text{in} \quad R_{d,i}(t)
\]

\[
\iff (x + 1)^{k+t} p^r = (x + 1)^t p^r \quad \text{in} \quad R_{d,i}(t)
\]

\[
\iff (x + 1)^{k+t} = (x + 1)^t \quad \text{in} \quad R_{d,i}(t - r).
\]

\[\square\]

5. Roots of unity

We denote by \( \mu_d(K) \) and \( \mu_d'(K) \) the group of \( d \)-th roots of unity and the set of primitive \( d \)-th roots of unity, respectively, in the field \( K \).

Let \( \zeta_d \in \mu_d'(C) \) and \( K_d = \mathcal{O}(\zeta_d) \) the \( d \)-th cyclotomic number field with ring of integers \( \mathcal{O}_d = \mathbb{Z}[[\zeta_d]] \cong \mathbb{Z}[x]/(\Phi_d(x)) \). As \( p \nmid n \), the prime \( p \) does not ramify in \( K_d/\mathbb{Q} \), and we have the explicit prime decomposition

\[
p\mathcal{O}_d = p_1 \cdots p_r, \quad \text{where} \quad p_i = \langle p, \phi_{d,i}(\zeta_d) \rangle \subset \mathcal{O}_d.
\]

Lemma 5.1. \( R_{d,i}(t) = \mathbb{Z}/p^t\mathbb{Z}[x]/(\phi_{d,i}(x)) \cong \mathcal{O}_d/p_i^t.\)

Proof.

\[
\mathcal{O}_d/p_i^t \cong \frac{\mathbb{Z}[\zeta_d]}{(p, \phi_{d,i}(\zeta_d))} \cong \frac{\mathbb{Z}[x]}{(p^t - 1, \phi_{d,i}(x))} \cong \frac{\mathbb{Z}/p^t\mathbb{Z}[x]}{(\phi_{d,i}(x))}.
\]

The last isomorphism is obtained as follows. The inclusion of \( \mathbb{Z}/p^t\mathbb{Z}[x] \)-ideals

\[
\langle p^t - 1, \phi_{d,i}(x) \rangle \subset \langle \phi_{d,i}(x) \rangle
\]

induces a surjective homomorphism from (6) to (7). But both rings have the same cardinality, so the map is an isomorphism. \[\square\]

Now let \( \zeta_n \in \mu_n'(C) \) and fix a prime \( \mathfrak{P} \) of \( \mathcal{O}_n = \mathbb{Z}[\zeta_n] \) lying above \( p \), and let \( \nu_{\mathfrak{P}} : K_n \to \mathbb{Z} \cup \{\infty\} \) denote the valuation corresponding to \( \mathfrak{P} \). For \( a \in \mathcal{O}_n \) and \( r \in \mathbb{Z} \),
we denote \( \text{Ord}_r(a) := \text{Ord}_{\mathbb{Z}/p^r\mathbb{Z}}(a) \) if \( r > 0 \) and \( \text{Ord}_r(a) := 1 \) for \(-\infty \leq r \leq 0\).

Our second main result is

**Theorem 5.2.** Suppose that \( p \nmid n \), and let \( u = (u_1, u_2, \ldots, u_n) \in \mathbb{Z}^n \) represent a tuple in \( \mathbb{Z}/p^r\mathbb{Z} \). Let \( f_u(x) = u_1x^{n^{-1}} + u_2x^{n^{-2}} + \cdots + u_n \in \mathbb{Z}[x] \). Then the period of the Ducci sequence starting with \( u \) is given by

\[
\text{Per}(u) = \text{lcm}\{\text{Ord}_{t-v_p(f_u(\zeta))}(\zeta + 1) \mid \zeta \in \mu_n(\mathbb{C})\}.
\]

**Proof.** First note that \( \mu_n(\mathbb{C}) = \cup_{d|n} \mu'_d(\mathbb{C}) \). Now let \( \zeta \in \mu'_d(\mathbb{C}) \), so \( \zeta \in \mathcal{O}_d \), and let \( p = \mathfrak{P} \cap \mathcal{O}_d \). Then \( v_p(f_u(\zeta)) = v_p(f_u(\zeta)) \), as \( f_u(\zeta) \in \mathcal{O}_d \) and \( \mathfrak{P}|p \) is unramified. Hence we write

\[
\text{lcm}_{\zeta \in \mu_n(\mathbb{C})} \text{Ord}_{t-v_p(f_u(\zeta))}(\zeta + 1)
\]

\[
= \text{lcm}_{d|n} \text{lcm}_{\zeta \in \mu'_d(\mathbb{C})} \text{Ord}_{t-v_p(f_u(\zeta))}(\zeta + 1)
\]

\[
= \text{lcm}_{d|n} \text{lcm}_{\zeta \in \mu'_d(\mathbb{C})} \text{Ord}_{\mathcal{O}_d/p^t-v_p(f_u(\zeta))}(\zeta + 1).
\]

Next, we notice that \( \text{Gal}(K_d/\mathbb{Q}) \cong (\mathbb{Z}/d\mathbb{Z})^* \) acts transitively on \( \mu'_d(\mathbb{C}) \) and on the primes \( p_1, \ldots, p_{r_d} \) of \( K_d \) above \( p \). Now, after applying the elements of \( \text{Gal}(K_d/\mathbb{Q}) \), we may fix one primitive \( d \)th root of unity \( \zeta_d \) and let the primes \( p_1, \ldots, p_{r_d} \) above \( p \) vary in the above lcm, rather than fixing one prime \( p \) and letting the roots of unity vary. This gives us

\[
\text{lcm}_{d|n} \text{lcm}_{\zeta \in \mu'_d(\mathbb{C})} \text{Ord}_{\mathcal{O}_d/p^t-v_p(f_u(\zeta))}(\zeta + 1)
\]

\[
= \text{lcm}_{d|n} \text{lcm}_{1 \leq i \leq r_d} \text{Ord}_{\mathcal{O}_d/p^t-v_p(f_u(\zeta_i))}(\zeta_i + 1)
\]

\[
= \text{lcm}_{d|n} \text{lcm}_{1 \leq i \leq r_d} \text{Ord}_{R_{d,i}(t-1)}(x + 1) \quad \text{(by Lemma 5.1)}
\]

\[
= \text{lcm}_{d|n} \text{lcm}_{1 \leq i \leq r_d} \text{Per}_{d,i}f_u(x) \quad \text{(by Proposition 4.2)}
\]

\[
= \text{Per}_uf_u(x) \quad \text{(by (5))}.
\]

Here we have used the isomorphism of Lemma 5.1, which maps \( \zeta_d \) to \( x \), and where \( v_p(f_u(\zeta_d)) \) corresponds to the exponent \( r \) of Proposition 4.2. \( \square \)

**Example 5.3** We continue with Example 4.1, where \( n = 10, p^t = 27 \) and \( u = (0, 0, 6, 0, 3, 0, 9, 6, 9, 21) \in (\mathbb{Z}/27\mathbb{Z})^{10} \). Then

\[
\text{Per}(u) = \text{lcm}\{\text{Ord}_{R_{1,i}(2)}(x + 1), \ \text{Ord}_{R_{11,i}(1)}(x + 1)\}
\]

\[
= \text{lcm}\{\text{Ord}_2(\zeta_5 + 1), \ \text{Ord}_1(\zeta_{10} + 1)\}
\]

\[
= \text{lcm}\{3 \cdot \text{Ord}_1(\zeta_5 + 1), \ \text{Ord}_1(\zeta_{10} + 1)\}
\]

\[
= \text{lcm}\{3 \cdot 40, 80\} = 240.
\]

The reason \( \text{Ord}_2(\zeta_5 + 1) = 3 \cdot \text{Ord}_1(\zeta_5 + 1) \) will become clear in \S 7. \( \square \)

In the case \( t = 1 \), i.e. over \( \mathbb{F}_p \), we have a particularly elegant expression for the period, apparently first realized (but not published) by D. Richman in the case \( p = 2 \), see [17].

**Corollary 5.4.** Assume \( p \nmid n \). Let \( u = (u_1, u_2, \ldots, u_n) \in \mathbb{F}_p^n \) and \( f_u(x) = u_1x^{n^{-1}} + u_2x^{n^{-2}} + \cdots + u_n \in \mathbb{F}_p[x] \). Then

\[
\text{Per}(u) = \text{lcm}\{\text{Ord}_p(\zeta + 1) \mid \zeta \in \mu_n(\mathbb{F}_p), f_u(\zeta) \neq 0\}.
\]
Here $\overline{\mathbb{F}}_p$ denotes an algebraic closure of $\mathbb{F}_p$, but we may replace it with the splitting field of $x^n - 1$ over $\mathbb{F}_p$.

Proof. Just set $t = 1$ in Theorem 5.2. Alternatively, one may prove this directly using the fact that $R_{d,i}(t)$ is a finite field when $t = 1$. □

See [4, Corollary 4.5] for a version of this result without the condition $p \nmid n$, but assuming $p = 2$. The proof there can easily be extended to arbitrary primes $p$. Similar results abound in the literature, see for example [9], [14] and [22].

Remark 1. The results of this section are phrased in terms of roots of unity for aesthetic reasons. Actual computations are more easily performed with polynomials, see Examples 7.5 and 7.6 below.

6. The case $d = 3$

It turns out that the qualitative behavior of $\text{Ord}_t(\zeta + 1)$ depends on whether or not $\zeta$ is a primitive cube root of unity. We study this case first.

We have $x^3 - 1 = (x - 1)(x^2 + x + 1) = \Phi_1(x)\Phi_3(x)$ in $\mathbb{Z}[x]$. Furthermore, $K_3 = \mathbb{Q}(\zeta_3)$ and $\mathcal{O}_3 = \mathbb{Z}[\zeta_3]$, where $\zeta_3 = \frac{1}{2}(\sqrt{-3} - 1) = \exp(2i\pi/3)$ and $\bar{\zeta}_3 = \frac{1}{2}(-\sqrt{-3} - 1) = \exp(4i\pi/3)$. Now, for a given prime $p \neq 3$, we have

$$r_3 = \varphi(3)/\text{Ord}_{\mathbb{Z}/3}(p) = \begin{cases} 1 & \text{if } p \equiv 2 \mod 3 \\ 2 & \text{if } p \equiv 1 \mod 3, \end{cases}$$

so we see that $p$ splits in $K_3/\mathbb{Q}$ if $p \equiv 1 \mod 3$ and remains prime if $p \equiv 2 \mod 3$. If $p$ splits, then $x^2 + x + 1 \equiv (x - \alpha)(x - \beta) = \phi_{3,1}(x)\phi_{3,2}(x) \mod p$, with $\alpha + \beta \equiv -1$ and $\alpha\beta \equiv 1 \mod p$. It follows that in this case the primes above $p$ are

$$p_1 = (p, \zeta_3 - \alpha),$$

$$p_2 = (p, \zeta_3 - \beta).$$

Lemma 6.1.

$$\text{Ord}_t(\zeta_3 + 1) = \text{Ord}_t(\bar{\zeta}_3 + 1) = \begin{cases} 3 & \text{if } p^t = 2 \\ 6 & \text{otherwise.} \end{cases}$$

Proof. First notice that $(x + 1)^6 \equiv 1 \mod (x^2 + x + 1)$ over $\mathbb{Z}$, so we see that $\text{Ord}_t(\zeta_3 + 1)/6$. On the other hand, $(x + 1)^2 \equiv x \not\equiv 1 \mod \phi_{3,1}(x)$, as $\alpha \not\equiv 1 \not\equiv \beta \mod p$. Hence $\text{Ord}_t(\zeta_3 + 1) \neq 2$. Lastly, $(x + 1)^3 \equiv -1 \equiv 1 \mod \phi_{3,1}(x)$ if and only if $p^t = 2$. This completes the proof. □

Combining our results thus far, we obtain:

Theorem 6.2. Suppose $p \neq 3$ and let $u = (u_1, u_2, u_3) \in \mathbb{Z}^3$ represent a tuple in $(\mathbb{Z}/p^t\mathbb{Z})^3$. Let $f_u(x) = u_1x^2 + u_2x + u_3 \in \mathbb{Z}[x]$. Fix a prime $p$ of $\mathcal{O}_3$ above $p$. Then

(1) If $p = 2$ or $f_u(1) \in p^t$, then

$$\text{Per}(u) = \begin{cases} 1 & \text{if } u \text{ vanishes} \\ 3 & \text{if } p^t = 2 \text{ and } u \text{ does not vanish} \\ 6 & \text{otherwise.} \end{cases}$$
Lemma 7.1

Let \( \zeta = \zeta_d \in \mu'_d(\mathbb{C}) \), with associated polynomial \( \phi_{d,i}(x) \in \mathbb{Z}[x] \). How does \( \text{Ord}_t(\zeta + 1) \) relate to \( \text{Ord}_1(\zeta + 1) \)?

Let \( \phi(x) \in \hat{\mathbb{Z}}_p[x] \) be the factor of \( x^n - 1 \) which is congruent to \( \phi_{d,i}(x) \mod p^t \).

Then \( R_{d,i}(t) \equiv \frac{\hat{\mathbb{Z}}_p[x]}{(p^t, \phi(x))} \), and \( \text{Ord}_t(\zeta + 1) = \text{Ord}_1(\zeta + 1) = \text{Ord}_1(\zeta + 1) \).

Lemma 7.1. We have \( \text{Ord}_t(\zeta + 1) = p^{k(t)}\text{Ord}_1(\zeta + 1) \), with \( 0 \leq k(t) \leq t - 1 \). Moreover, if \( d \neq 3 \), then \( k(t) \to \infty \) as \( t \to \infty \).

Proof. Consider the exact sequence

\[
1 \to \frac{1 + \langle p, \phi(x) \rangle}{1 + \langle p^t, \phi(x) \rangle} \to \left( \frac{\hat{\mathbb{Z}}_p[x]}{(p^t, \phi(x))} \right)^* \to \left( \frac{\hat{\mathbb{Z}}_p[x]}{(\phi(x))} \right)^* \to 1.
\]

The group on the left is a \( p \)-group with exponent \( p^{t-1} \), which implies the first assertion. Now suppose that \( k(t) \) is bounded for all \( t \). Then we must have \( (x+1)^m = 1 \) in \( \frac{\hat{\mathbb{Z}}_p[x]}{(\phi(x))} \), in which case \( \zeta_d + 1 = \zeta_m \) is an \( m \)th root of unity in \( \bar{\mathbb{Q}}_p \), an algebraic closure of the field \( \mathbb{Q}_p \) of \( p \)-adic numbers, hence also in \( \bar{\mathbb{Q}} \subset \mathbb{C} \). This is only possible if \( d = 3 \) and \( m = 6 \). Indeed, \( \zeta_m \) must lie on the intersection of the two unit circles centered at 0 and 1 in the complex plane. \( \square \)

We will need the following technical lemma.

Lemma 7.2. Let \( p \) be a prime, \( Q(x) \in \hat{\mathbb{Z}}_p[x] \) and \( t \in \mathbb{N} \). If \( p = 2 \) we assume further that \( t \geq 2 \). Let \( g(x) \in \hat{\mathbb{Z}}_p[x] \) such that

\[
g(x) \equiv 1 \mod (Q(x), p^t) \]
\[
g(x) \not\equiv 1 \mod (Q(x), p^{t+1}).
\]

Then

\[
g(x)^p \equiv 1 \mod (Q(x), p^{t+1})
\]
\[
g(x)^p \not\equiv 1 \mod (Q(x), p^{t+2}).
\]

Proof. Suppose \( g(x) \) is reduced modulo \( Q(x) \), and write \( g(x) = 1 + \sum a_i x^{m_i} \), with exponents \( 0 \leq m_i < \deg(Q) \), and all \( a_i \equiv 0 \mod p^t \), but at least one \( a_i \not\equiv 0 \mod p^{t+1} \).

Then

\[
g(x)^p = 1 + p \sum a_i x^{m_i} + \text{(terms involving } a_i a_j).\]
If \( p > 2 \), then each of the terms involving \( a_i a_j \) either picks up a factor \( p \) from a binomial coefficient, or it involves \( a_i a_j a_k \). These terms are then divisible by \( p^{2t+1} \) or \( p^{3t} \), respectively. If \( p = 2 \), these terms are at least divisible by \( p^t \), from the \( a_i a_j \)-factor. In all cases, these terms are divisible by \( p^{t+2} \) (here we need \( t \geq 2 \) when \( p = 2 \)).

Thus we see that

\[
g(x)^p \equiv 1 + p \sum a_i x^{m_i} \mod p^{t+2},
\]

which is congruent to 1 mod \( p^{t+1} \) but not mod \( p^{t+2} \). Note also that the degree is still the same (after reducing mod \( p^{t+2} \)), so \( g(x)^p \) is still reduced modulo \( Q(x) \). □

For polynomials \( f(x), \phi(x) \in \hat{\mathbb{Z}}_p[x] \) we denote by \( v_p(f(x) \mod \phi(x)) \) the largest integer \( r \) for which \( f(x) \equiv 0 \mod (p^r, \phi(x)) \).

**Theorem 7.3.** Suppose that \( d \neq 3 \). Let \( \zeta \in \mu'_d(\mathbb{C}) \) be a primitive \( d \)th root of unity, with associated polynomial \( \phi(x) \in \hat{\mathbb{Z}}_p[x] \), as above. Then for any multiple \( n \) of \( d \), we have

\[
v_p((x + 1)^{\text{Ord}_1(\zeta + 1)} - 1 \mod \phi(x)) = v_p((x + 1)^{p^{r(n)} - 1} - 1 \mod \phi(x)) = t_0 \quad (8)
\]

and

\[
v_p((x + 1)^{2\text{Ord}_1(\zeta + 1)} - 1 \mod \phi(x)) = v_p((x + 1)^{2(p^{r(n)} - 1)} - 1 \mod \phi(x)) = t_1. \quad (9)
\]

Moreover,

(1) If \( p > 2 \), or \( p = 2 \) and \( t_0 > 1 \), then

\[
\text{Ord}_t(\zeta + 1) = p^\max\{0, t-t_0\} \text{Ord}_1(\zeta + 1).
\]

(2) If \( p = 2 \) and \( t_0 = 1 \), then

\[
\text{Ord}_t(\zeta + 1) = 2^{\max\{1, t-t_1+1\}} \text{Ord}_1(\zeta + 1) \quad \text{for } t \geq 2.
\]

**Proof.** We first show that (8) and (9) hold. Since \( d \neq 3 \), it follows from Lemma 7.1 that \((x + 1)^{\text{Ord}_1(\zeta + 1)} \neq 1 \) in \( \hat{\mathbb{Z}}_p[x] / \phi(x) \). Now, since deg \( \phi(x) = \text{Ord}_{\mathbb{Z}/d\mathbb{Z}}(p) \mod \phi(d) \), we have \( \text{Ord}_1(\zeta + 1) \mod p^{r(d)} \neq 1 \mod p^{r(n)} - 1 \), and we write \( p^{r(n)} - 1 = M \cdot \text{Ord}_1(\zeta + 1) \). Then we have, for \( a = x + 1 \),

\[
a^{p^{r(n)} - 1} - 1 = a^{\text{Ord}_1(\zeta + 1)} - 1 = \left(a^{\text{Ord}_1(\zeta + 1)} - 1\right)\left(a^{(M-1)\text{Ord}_1(\zeta + 1)} + a^{(M-2)\text{Ord}_1(\zeta + 1)} + \cdots + 1\right) \quad \text{(\star)}
\]

As \((x + 1)^{\text{Ord}_1(\zeta + 1)} \equiv 1 \mod (p, \phi(x))\), we see that \((\star) \equiv M \neq 0 \mod (p, \phi(x))\), and so (8) must hold. Similarly, we show (9) by applying the above argument to \( a = (x + 1)^2 \).

To show (1), it is clear that \( \text{Ord}_t(\zeta + 1) = \text{Ord}_1(\zeta + 1) \) when \( t \leq t_0 \). If \( t > t_0 \), we can apply Lemma 7.2 to obtain \( \text{Ord}_t(\zeta + 1) = p\text{Ord}_{t-1}(\zeta + 1) \) (note that \( t_0 \geq 2 \) if \( p = 2 \)), from which the result follows.

To show (2), first note that \( t_0 = 1 \) and Lemma 7.1 imply that \( \text{Ord}_2(\zeta + 1) = 2\text{Ord}_1(\zeta + 1) \). Next, it is clear that \( \text{Ord}_t(\zeta + 1) = \text{Ord}_2(\zeta + 1) \) if \( 2 \leq t \leq t_1 \). On the other hand, applying Lemma 7.2 to \( g(x) = (x + 1)^{2\text{Ord}_1(\zeta + 1)} \) gives \( \text{Ord}_t(\zeta + 1) = 2\text{Ord}_{t-1}(\zeta + 1) \) for \( t > t_1 + 1 \), and the result follows. □
COROLLARY 7.4. Suppose \( p \neq 2 \) and let \( t_2 = v_p(2^{p-1} - 1) \). Then

\[
\text{Ord}_{\mathbb{Z}/p\mathbb{Z}}(2) = p^{\max(0,t-t_2)} \text{Ord}_{\mathbb{F}_p}(2).
\]

Proof. Just let \( d = 1 \), \( \zeta_1 = 1 \). \( \square \)

Example 7.5 Let \( p = 11 \) and \( n = d = 6 \). Then

\[
x^6 - 1 = (x - 1)(x + 1)(x^2 + x + 1)(x^2 - x + 1) \quad \text{in } \mathbb{Z}[x]
\]

and also in \( \hat{Z}_{11}[x] \).

We let \( \zeta_6 \) be a primitive 6th root of unity, with minimal polynomial \( \phi(x) = x^2 - x + 1 \in \mathbb{Z}[x] \). Then \( \text{Ord}_1(\zeta_6 + 1) = 60 \) and we can compute

\[
g(x) := (x + 1)^{60} \equiv 11^2 + 1 \mod (\phi(x), 11^3),
\]

So \( t_0 = 2 \) and \( \text{Ord}_1(\zeta_6 + 1) = 11^{t-2}60 \) for \( t \geq 2 \). \( \square \)

Remark 1. The condition that \( t \geq 2 \) if \( p = 2 \) in Lemma 7.2 is necessary. Indeed, let \( p = 2 \) and \( n = d = 7 \), and set \( Q(x) = x^3 + x^2 + 1 \in \hat{Z}_2[x] \). Then \( \text{Ord}_1(\zeta + 1) = 7 \), and

\[
g(x) := (x + 1)^7 \equiv 1 \mod (Q(x), 2^3).
\]

However, \( g(x)^2 \equiv 1 \mod (Q(x), 2^3) \), so the conclusion of Lemma 7.2 does not hold for \( t = 1 \). Note that \( Q(x) = x^3 + x^2 + 1 \) is a factor of \( x^7 - 1 \) over \( \mathbb{F}_2 \), but not over \( \hat{Z}_2 \).

The author could not find a similar example for which \( Q(x) \) is a factor of \( x^d - 1 \) over \( \hat{Z}_2 \), i.e. for which we will see \( t_1 > 2 \) in Theorem 7.3. In general it is very rare to find examples for which \( \text{Ord}_1(\zeta + 1) \neq p^{t-1} \text{Ord}_1(\zeta + 1) \) for some \( p \).

Remark 2. To compute the periods of arbitrary Ducci sequences in \( (\mathbb{Z}/p^t\mathbb{Z})^n \) (still assuming \( p \nmid n \)), it suffices to precompute \( \text{Ord}_1(\zeta + 1) \) and \( t_0 \) (and \( t_1 \) if \( p = 2 \)) for each \( \zeta \in \mu_n(\mathbb{C}) \) (actually, one \( \zeta \) in each conjugacy class mod \( p \) is enough). Then the period of any given tuple in \( (\mathbb{Z}/p^t\mathbb{Z})^n \) can be obtained from Theorems 5.2, 6.2 and 7.3. We demonstrate this next.

Example 7.6 We continue with Example 7.5, so let \( p = 11 \), \( n = 6 \). Up to conjugacy, we must precompute data for four roots of unity:

\[
\zeta_1 = 1 \quad \rightarrow \quad \text{Ord}_1(\zeta_1 + 1) = 10, \ t_0 = 1
\]

\[
\zeta_2 = -1 \quad \rightarrow \quad \text{Ord}_1(\zeta_2 + 1) = 1, \text{ for all } t \geq 1
\]

\[
\zeta_3 = \exp(2\pi i / 3) \quad \rightarrow \quad \text{Ord}_1(\zeta_3 + 1) = 6, \text{ for all } t \geq 1
\]

\[
\zeta_6 = \exp(2\pi i / 6) \quad \rightarrow \quad \text{Ord}_1(\zeta_6 + 1) = 60, \ t_0 = 2.
\]

Now let \( u = (96, 154, 1250, 704, 162, 650) \in (\mathbb{Z}/11^3\mathbb{Z})^6 \). This corresponds to the polynomial

\[
p_u(x) = 96x^5 + 154x^4 + 1250x^3 + 704x^2 + 162x + 650 \in R(3) = \frac{\mathbb{Z}/11^3\mathbb{Z}[x]}{(x^6 - 1)}.
\]
Next, denote by $\mathfrak{p}$ a prime of $\mathbb{Z}[\zeta_6]$ above 11. We find:

\[
\begin{align*}
p_u(x) &\equiv 354 \pmod{x - 1}, \text{ so } \nu_{\mathfrak{p}}(f_u(\zeta_1)) = v_{11}(354) = 0, \\
p_u(x) &\equiv 0 \pmod{x + 1}, \text{ so } \nu_{\mathfrak{p}}(f_u(\zeta_2)) = v_{11}(0) = \infty \text{ (and } u \text{ is in a cycle)}, \\
p_u(x) &\equiv 847x + 1100 \pmod{x^2 + x + 1}, \text{ so } \nu_{\mathfrak{p}}(f_u(\zeta_3)) = v_{11}(847x + 1100) = 1, \\
p_u(x) &\equiv 616x + 123 \pmod{x^2 - x + 1}, \text{ so } \nu_{\mathfrak{p}}(f_u(\zeta_5)) = v_{11}(616x + 123) = 0.
\end{align*}
\]

It follows that

\[
\begin{align*}
\text{Per}(u) &= \text{lcm}\{\text{Ord}_3(\zeta_1 + 1), \text{Ord}_{-\infty}(\zeta_2 + 1), \text{Ord}_2(\zeta_4 + 1), \text{Ord}_3(\zeta_6 + 1)\} \\
&= \text{lcm}\{11^2\text{Ord}_1(\zeta_1 + 1), 1, 6, 11\text{Ord}_1(\zeta_6 + 1)\} \\
&= \text{lcm}\{11^2 \cdot 10, 1, 6, 11 \cdot 60\} = 11^2 \cdot 60.
\end{align*}
\]

\[
\square
\]

8. Maximal Periods

Define $P_{\rho'}(n) := \text{Per}(0, 0, 0, \ldots, 0, 1) = \text{Ord}_{R(t)}(x + 1)$ to be the maximal period of Ducci sequences in $(\mathbb{Z}/p^t\mathbb{Z})^n$. It is clear that $\text{Per}(u)|P_{\rho'}(n)$ for every $u \in (\mathbb{Z}/p^t\mathbb{Z})^n$.

If there exists an integer $k \geq 1$ such that $p^k \equiv -1 \pmod{n}$, then we say that $n$ is "with a $-1$" (in the terminology of [12]). In this case $\text{Ord}_{\mathbb{Z}/n\mathbb{Z}}(p)$ is even, and the minimal such $k$ is $\text{Ord}_{\mathbb{Z}/n\mathbb{Z}}(p)/2$.

It is shown in [19, Theorem 2] that if $n$ is coprime to $2p$, then $n$ is with a $-1$ if and only if there exists $e \geq 1$ such that for every prime divisor $q$ of $n$, we have $2^e|\text{Ord}_{\mathbb{Z}/q\mathbb{Z}}(p)$ and $2^{e+1} \nmid \text{Ord}_{\mathbb{Z}/q\mathbb{Z}}(p)$. Asymptotics for the number of integers with a $-1$ are also derived in [19].

**Theorem 8.1.** Suppose $p \nmid n$ and let $m = \text{Ord}_{\mathbb{Z}/n\mathbb{Z}}(p)$.

1. $P_{\rho'}(n)|p^{t-1}(p^m - 1)$.
2. If $n$ is with a $-1$, then $P_{\rho'}(n)|p^{t-1}n(p^{m/2} - 1)$.
3. If $n \geq 3$, then $n|P_{\rho'}(n)$.
4. If $p \geq 3$ then $\text{Ord}_{\mathbb{Z}/p^t\mathbb{Z}}(2) = P_{\rho'}(2)|P_{\rho'}(n)$.

**Proof.**

By Theorems 6.2 and 7.3 it suffices to prove (1) and (2) in the case $t = 1$. If $p^m \equiv 1 \pmod{n}$, then

\[
(x + 1)^{p^m} = (x^m + 1) = (x + 1) \text{ in } R(1),
\]

and (1) follows.

If $p^k \equiv -1 \pmod{n}$, then

\[
(x + 1)^{np^k} = (x^{p^k} + 1)^n = (x^{-1} + 1)^n = (1 + x)^n \text{ in } R(1),
\]

where in the last equality we have multiplied by $x^n = 1$. (2) follows.

To prove (3), consider the transformation

\[
\sigma_k : R(t) \to R(t), \quad \sigma_k(f(x)) := x^k f(x^{-1}), \quad \text{for } k \in \mathbb{Z}/n\mathbb{Z}.
\]
If $\sigma_k$ fixes $f(x) \in R(t)$, then we say that $f(x)$ is symmetric about $k$.

We first show that $(x + 1)^{l}$ is symmetric about $k$ if and only if $k \equiv l \mod n$. Indeed, $\sigma_k((x + 1)^l) = x^k(x^{-1} + 1)^l = x^{k-l}(1 + x)^l$, which equals $(x + 1)^l$ when $k \equiv l \mod n$. Conversely, if $n \geq 3$ then $x + 1$ is invertible in $R_{n,1}(t)$. Now, if $x^k-l(1 + x)^l = (x + 1)^l$ in $R(t)$, then $x^{k-l} = 1$ in $R_{n,1}(t)$, and $k \equiv l \mod n$ because $x$ has order $n$ in $R_{n,1}(t)$.

It now follows that, if $(x + 1)^{l+t} = (x + 1)^l$, then this is symmetric about $t$ and about $t + l$, so $l \equiv 0 \mod n$.

(4) Follows from the contribution of $\zeta_1 = 1$ in Theorem 5.2. $\square$

Some values of $P_p(n)$ for $p \mid n$ are listed in Table 1.

We can also express $P_{p'}(n)$ in terms of $P_p(n)$:

**Theorem 8.2.** Let $t_2 = v_p((2^{p-1} - 1)$ and set

$$Q_n(x) := \begin{cases} x^n - 1 & \text{if } p \neq 2 \\
\frac{x^n - 1}{x^t - 1} & \text{if } p = 2 \\
\frac{x^n - 1}{x^t - 1} & \text{if } p \neq 2 \text{ and } n \text{ is even} \\
x^t - 1 & \text{if } p \neq 2 \text{ and } n \text{ is odd.} \end{cases}$$

(10)

Then

(1) $P_{p'}(1) = 1$.

(2) If $p \neq 2$ then

$$P_{p'}(1) = P_{p'}(2) = \text{Ord}_{Z/p'Z}(2) = p^{\text{max}(0, t-t_2)}\text{Ord}_{Z/pZ}(2).$$

(3)

$$P_{p'}(3) = \begin{cases} 3 & p = 2, t = 1 \\
6 & p = 2, t \geq 2 \\
\text{lcm}\{6, p^{\text{max}(0, t-t_2)}\text{Ord}_{Z/pZ}(2)\} & p \neq 2, \end{cases}$$

(4) If $p \neq 2$ and $n > 3$ then

$$P_{p'}(n) = p^{\text{max}(0, t-t_n)}P_p(n),$$

where

$$t_n = v_p((x + 1)^{p^{(n-1)}} - 1 \mod Q_n(x)).$$

Table 1. Some values of $P_p(n)$ for $p \mid n$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$P_2(n)$</th>
<th>$P_3(n)$</th>
<th>$P_5(n)$</th>
<th>$P_7(n)$</th>
<th>$P_{11}(n)$</th>
<th>$P_{13}(n)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>7</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
<td>11</td>
</tr>
<tr>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
<td>13</td>
</tr>
<tr>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
<td>17</td>
</tr>
<tr>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>23</td>
<td>23</td>
<td>23</td>
<td>23</td>
<td>23</td>
<td>23</td>
<td>23</td>
</tr>
</tbody>
</table>
If $p = 2$ and $n > 3$ is odd, let

$$t'_n = v_2((x + 1)^{2^{v(n)} - 1} - 1 \mod Q_n(x)) \geq t_n + 1.$$ 

If $t_n = 1$, then

$$P_{2^t}(n) = 2^{\max\{1, t - t'_n + 1\}}P_2(n) \text{ if } t \geq 2.$$ 

If $t_n > 1$, then

$$P_{2^t}(n) = 2^{\max\{0, t - t_n\}}P_2(n).$$

Proof. (1) is trivial, whereas (2) and (3) follow from Theorem 6.2 and Corollary 7.4.

Next, notice that $P_{p^t}(n) = \text{lcm}\{\text{Ord}_t(\zeta + 1) \mid \zeta \in \mu_n(\mathbb{C}), \ Q_n(\zeta) = 0\}$, and since

$$v_p((x + 1)^{p^t(n)} - 1 \mod Q_n(x)) = \min_{\phi(x) \in \mathbb{Z}_p[x]} \min_{\phi(x)\in\mathbb{Z}_p[x]} v_p((x + 1)^{p^t(n)} - 1 \mod \phi(x)),$$

we see that (4) follows from Theorem 7.3. Similarly, (5) follows after Replacing $x + 1$ in the above by $(x + 1)^2$. \qed

The advantage of Theorem 8.2 is that $t_n$ and $t'_n$ can be computed without the need to factorize $x^n - 1$ over $\mathbb{Z}_p$.

Corollary 8.3. If $p \nmid 2n$ and $p^2 \nmid 2^{p-1} - 1$, then $P_{p^t}(n) = p^{l-1}P_p(n)$.

Proof. This follows since $\text{Ord}_{\mathbb{Z}/p^t\mathbb{Z}}(2) \mid P_{p^t}(n)$. \qed

9. Heuristics of exceptional cases

If $p^2|2^{p-1} - 1$, then $p$ is called a Wieferich prime. The only two Wieferich primes less than $1.25 \times 10^{15}$ are 1093 and 3511, see [15]. In these cases, we have

$$P_{p^t}(3) = p^{\max\{0, t-2\}}(p-1)$$

for $p = 1093$ and $p = 3511$.

Silverman has shown [21], that the Masser-Oesterlé abc-Conjecture implies that there are infinitely many non-Wieferich primes.

Definition 9.1. The pair $(p, n)$ is called exceptional if $P_{p^t}(n) \neq p^{l-1}P_p(n)$.

We see from Theorem 8.2 that $(p, n)$ is exceptional if

$$\begin{align*}
(x + 1)^{2^{v(n)} - 1} &\equiv 1 \mod (8, Q_n(x)) \quad \text{when } p = 2 \\
(x + 1)^{p^{v(n)} - 1} &\equiv 1 \mod (p^2, Q_n(x)) \quad \text{when } p \neq 2,
\end{align*}$$

where $Q_n(x)$ is defined in (10). Moreover, if $(p, n)$ is exceptional and $p \neq 2$, then $p$ is a Wieferich prime, by Corollary 8.3. Conversely, if $n \leq 3$ and $p$ is a Wieferich prime, then $(p, n)$ is exceptional. The pair $(2, 3)$ is also exceptional.

Although Wieferich primes certainly seem to be rare, the following standard heuristic argument suggests that there should nevertheless be infinitely many of them. If we assume that the residue class of $(2^{p-1} - 1)/p$ is uniformly distributed
in \( \mathbb{Z}/p\mathbb{Z} \), then we see that every prime \( p \) has “probability” \( p^{-1} \) to be a Wieferich prime. This suggests that the number of Wieferich primes less than some \( N \) should be asymptotic to

\[
\sum_{p < N \text{ prime}} \frac{1}{p} \sim \log \log N,
\]

according to [13, Theorem 427]. A similar argument suggests that the expected number of primes \( p \) such that \( p^3 \mid 2^{p-1} - 1 \) is \( \sum_p p^{-2} \), which is finite. Since no primes less than \( 1.25 \times 10^{15} \) have this property, we expect that none exist.

We apply a similar heuristic to exceptional pairs. If we assume that the residue class of \( \left( (x + 1)p^{n(x)} - 1 \right) / p \) (respectively \( \left( (x + 1)^2p^{n(x)} - 1 \right) / 4 \) if \( p = 2 \)) is uniformly distributed in \( \hat{\mathbb{Z}}_p[x] / (p, Q(x)) \) (respectively \( \hat{\mathbb{Z}}_2[x] / (4, Q(x)) \)), then the “probability” that \((p, n)\) is exceptional is given by \( p^{-\deg(Q(x))} \) or \( p^{-1-n} \).

A computer search for \( p \in \{2, 1093, 3511\} \) and \( n \leq 500 \) has revealed the following exceptional pairs: \((2, 3), (1093, 1), (1093, 2), (1093, 3), (1093, 4), (3511, 1), (3511, 2), (3511, 3), (3511, 4)\).

The expected number of exceptional pairs with \( n > 4 \) outside the range of our computer search is less than

\[
\sum_{n=500}^{\infty} \left( \frac{1}{2^n} + \frac{1}{1093^n} + \frac{1}{3511^n} \right) + \sum_{n=4}^{\infty} \sum_{p > 1.25 \times 10^{15}} \frac{1}{p^n} < 5 \times 10^{-46}.
\]

**Question 9.2** If \( p \) is a Wieferich prime, is \((p, 4)\) exceptional? Are there any exceptional pairs \((p, n)\) with \( n > 4 \)?

**Acknowledgement**

The author would like to thank Stephan Wagner for fruitful discussions, and the anonymous referees for suggesting improvements to the manuscript.

**References**


REFERENCES