A generalization of very odd sequences

Cheng Yeaw Ku
Department of Mathematics
National University of Singapore
Singapore 117543.
matkcy@nus.edu.sg

Kok Bin Wong
Institute of Mathematical Sciences
University of Malaya
50603 Kuala Lumpur, Malaysia
kbwong@um.edu.my

Submitted: Mar 2, 2015; Accepted: Apr 6, 2015; Published: Apr 21, 2015
Mathematics Subject Classifications: 11B50, 11B83

Abstract

Let $\mathbb{N}$ be the set of positive integers and $n \in \mathbb{N}$. Let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ be a sequence of length n, with $a_i \in \{0, 1\}$. For $0 \leqslant k \leqslant n-1$, let

$$A_k(\mathbf{a}) = \sum_{\substack{0 \leqslant i \leqslant j \leqslant n-1 \\ j-i=k}} a_i a_j.$$

The sequence $\mathbf{a}$ is called a very odd sequence if $A_k(\mathbf{a})$ is odd for all $0 \leqslant k \leqslant n-1$. In this paper, we study a generalization of very odd sequences and give a characterisation of these sequences.

Keywords: very odd sequence, Pelikán's conjecture

1 Introduction

Let $\mathbb{N}$ be the set of positive integers and $n \in \mathbb{N}$. Let $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ be a sequence of length n, with $a_i \in \{0, 1\}$. For $0 \leqslant k \leqslant n-1$, let

$$A_k(\mathbf{a}) = \sum_{\substack{0 \leqslant i \leqslant j \leqslant n-1 \\ j-i=k}} a_i a_j.$$

The sequence $\mathbf{a}$ is called a *very odd sequence* if $A_k(\mathbf{a})$ is odd for all $0 \leqslant k \leqslant n-1$.

Pelikán [6] conjectured that very odd sequences of length $n \geqslant 5$ do not exist. Later, Alles [1] and MacWilliams and Odlyzko [4] proved that Pelikán conjecture is false (see also [5]). In fact, Inglis and Wiseman [2] and MacWilliams and Odlyzko [4] proved the following theorem which gives a necessary and sufficient condition for the existence of a very odd sequences of length n.

Theorem 1. *A very odd sequence of length $n > 1$ exists if and only if the order of 2 is odd in the multiplicative group of integers modulo $2n-1$.*

Let p be a prime and $\mathbf{z} = (z_0, z_1, z_2, \dots)$ be an infinite sequence. A sequence $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ of length n with $a_i \in \mathbb{N} \cup \{0\}$ is called a $(\mathbf{z}, p)$-*sequence* if

$$A_k(\mathbf{a}) \equiv z_k \mod p, \quad \forall \;\; 0 \leqslant k \leqslant n-1.$$

For each $k \in \mathbb{N} \cup \{0\}$, let $\overline{k} = (k, k, k, \dots)$ be the infinite sequence with all entries equal to k. Then, Theorem 1 can be rewritten as follows:

Theorem 2. *A $(\overline{1}, 2)$-sequence of length $n > 1$ exists if and only if the order of 2 is odd in the multiplicative group of integers modulo $2n-1$.*

In this paper, we give necessary and sufficient conditions for the existence of a $(\overline{k}, p)$-sequence of length $n > 1$ (Theorem 12). We will also consider the existence of a $(\mathbf{y}_k, p)$-sequence of length $n > 1$ (Theorem 14) where $\mathbf{y}_k = (y_0, y_1, y_2, \dots)$ and $y_i = (-1)^i k$.

2 Main Results

Let p be a prime and $\mathbb{Z}_p$ be the field with p elements. We shall denote the set of all polynomials over the field $\mathbb{Z}_p$ by $\mathbb{Z}_p[x]$. For any sequence $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ of length n with $a_i \in \mathbb{N} \cup \{0\}$, we set

$$f_{\mathbf{a}}(x) = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}.$$

Then $f_{\mathbf{a}}(x) \in \mathbb{Z}_p[x]$.

For a polynomial $g(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \in \mathbb{Z}_p[x]$, we set

$$g^*(x) = c_{n-1} + c_{n-2} x + \cdots + c_0 x^{n-1}.$$

Note that $g^*(x) = x^{n-1} g\left(\frac{1}{x}\right)$ and $(g^*(x))^* = g(x)$. Furthermore, $f^*_{\mathbf{a}}(x) = f_{\mathbf{a}^*}(x)$ where $\mathbf{a}^* = (a_{n-1}, \dots, a_1, a_0)$ is the reverse of $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$.

The following two lemmas are obvious.

Lemma 3. *Let $f(x), g(x), h(x)$ be polynomials of degree at least 1 in $\mathbb{Z}_p[x]$. If $f(x) = g(x)h(x)$, then $f^*(x) = g^*(x)h^*(x)$.*

Lemma 4. *If $f(x)$ is a monic irreducible polynomial in $\mathbb{Z}_p[x]$, then $\frac{1}{f(0)} f^*(x)$ is also a monic irreducible polynomial in $\mathbb{Z}_p[x]$.*

Lemma 5. *A sequence $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ is a $(\mathbf{z}, p)$-sequence if and only if*

$$f_{\mathbf{a}}(x) f^*_{\mathbf{a}}(x) = \sum_{i=0}^{n-1} z_{n-1-i} x^i + x^{n-1} \sum_{i=1}^{n-1} z_i x^i,$$

in $\mathbb{Z}_p[x]$.

Proof. Note that

$$\begin{aligned} f_{\mathbf{a}}(x)f_{\mathbf{a}}^*(x) &= \left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{j=0}^{n-1} a_j x^{n-1-j}\right) \\ &= \sum_{l=0}^{2n-2}\left(\sum_{\substack{0\leqslant i,j\leqslant n-1\\ j-i=n-1-l}} a_i a_j\right) x^l \\ &= \sum_{l=0}^{2n-2} A_{|n-1-l|}(\mathbf{a})x^l \\ &= \sum_{i=0}^{n-1} A_{n-1-i}(\mathbf{a})x^i + x^{n-1}\sum_{i=1}^{n-1} A_i(\mathbf{a})x^i. \end{aligned}$$

The lemma follows by noting that $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ is a $(\mathbf{z}, p)$-sequence if and only if $A_i(\mathbf{a}) \equiv z_i \mod p$ for all i. □

The following corollary follows immediately from Lemma 5.

Corollary 6. *If $k \equiv 0 \mod p$, then there is exactly one $(\overline{k}, p)$-sequence of length $n > 1$, which is $(\overbrace{0, 0, \ldots, 0}^{n})$.*

We shall require the following lemmas.

Lemma 7. ([3, Theorem 2.14 on p. 128]) *Let $f(x)$ and $g(x) \neq 0$ be polynomials in $F[x]$, where F is a field. Then there exist polynomials $q(x)$ and $r(x) \in F[x]$ with the degree of $r(x)$ less than the degree of $g(x)$ such that $f(x) = q(x)g(x) + r(x)$.*

Lemma 8. ([3, Theorem 4.26 on p. 288]) *Let F be a finite field with $q = p^m$ elements and E be a field extension of F with $[E : F] = n$. Then the Galois group $G(E/F)$ is a cyclic group with generator η, where $\eta : a \to a^q$.*

Note that the Galois group $G(E/F)$ is the group of all automorphisms of E that fix F, i.e., $\theta \in G(E/F)$ if and only if $\theta(a) = a$ for all $a \in F$ and $\theta \in \mathrm{Aut}(E)$ the group of all automorphisms of E.

Lemma 9. ([3, Section 4.4 on p. 229]) *Let $f(x) \in \mathbb{Z}_p[x]$ and $f'(x)$ be the formal derivative of $f(x)$. If β is a multiple root of $f(x)$, then $f'(\beta) = 0$.*

We denote the greatest common divisor of c, d by $\gcd(c, d)$.

Lemma 10. *Let $\gcd(p, 2n-1) = 1 = \gcd(p-1, 2n-1)$ and β be a root of $\sum_{i=0}^{2n-2} x^i$. If $h(x) \in \mathbb{Z}_p[x]$ is a monic irreducible polynomial with $h(\beta) = 0$ and the order of p modulo $2n-1$ is odd, then the degree of $h(x)$ is odd and $h(0) = -1$. Furthermore, $-h^*(x) \neq h(x)$.*

Proof. Let E be a field extension of $\mathbb{Z}_p$ containing β. Let the order of β in E be t, i.e., t is the least positive integer such that $\beta^t = 1$. Note that $(x-1)\sum_{i=0}^{2n-2} x^i = x^{2n-1} - 1$. So, β is a root of $x^{2n-1} - 1$, i.e., $\beta^{2n-1} = 1$. This implies that t divides $2n-1$ and $\gcd(p,t) = 1 = \gcd(p-1,t)$. Let the order of p modulo t be e. Then $\beta^{p^e} = \beta$ and $\beta^{p^i} \neq \beta$ for $1 \leqslant i \leqslant e-1$. Furthermore, e is odd as the order of p modulo $2n-1$ is odd.

By Lemma 8, the Galois group $G(E/\mathbb{Z}_p)$ is a cyclic group with generator η. Note that $\eta((x-\beta)(x-\beta^p)\dots(x-\beta^{p^{e-1}})) = (x-\beta)(x-\beta^p)\dots(x-\beta^{p^{e-1}})$. So, $(x-\beta)(x-\beta^p)\dots(x-\beta^{p^{e-1}}) \in \mathbb{Z}_p[x]$ and $h(x) = (x-\beta)(x-\beta^p)\dots(x-\beta^{p^{e-1}})$. Thus, the degree of $h(x)$ is e which is odd.

Now, $(p-1)(1+p+\dots+p^{e-1}) = p^e - 1 \equiv 0 \mod t$. Since $\gcd(p-1,t) = 1$, we have $1+p+\dots+p^{e-1} \equiv 0 \mod t$. Therefore $h(0) = (-1)^e \beta^{1+p+\dots+p^{e-1}} = (-1)^e = -1$.

By Lemma 4, $-h^*(x)$ is a monic irreducible polynomial and $-h^*(\beta^{-1}) = 0$. Suppose $-h^*(x) = h(x)$. Then $\beta^{p^{i_0}} = \beta^{-1}$ for some $0 \leqslant i_0 \leqslant e-1$. This implies that $p^{i_0} \equiv -1 \mod t$ and $p^{2i_0} \equiv 1 \mod t$. So, e divides $2i_0$, and e divides i_0 for e is odd. This means that $p^{i_0} \equiv 1 \mod t$ and $2 \equiv 0 \mod t$. Therefore, $t = 1$ or 2. If $t = 1$, then $\beta = 1$ and $0 = \sum_{i=0}^{2n-2} \beta^i = 2n-1$ (in $\mathbb{Z}_p$), contradicting the fact that $\gcd(p, 2n-1) = 1$. If $t = 2$, then 2 divides $2n-1$, which is another contradiction. Hence, $-h^*(x) \neq h(x)$. $\square$

Lemma 11. *Let F be a field. Then $x^{m_1} - 1 = (x^{m_2} - 1)w(x)$ for some polynomial $w(x) \in F[x]$ if and only if m_2 divides m_1.*

Proof. Let $m_1 = qm_2 + r$ where r, q are integers with $0 \leqslant r < m_2$. Note that

$$x^{m_1} - 1 = x^{qm_2+r} - 1 = (x^{m_2} - 1)(x^{(q-1)m_2+r} + x^{(q-2)m_2+r} + \dots + x^{m_2+r} + x^r) + x^r - 1.$$

It then follows from Lemma 7 that $x^{m_1} - 1 = (x^{m_2} - 1)w(x)$ for some polynomial $w(x) \in F[x]$ if and only if $r = 0$. $\square$

For each $d \in \mathbb{N}$, let $\mathbb{Z}_d$ be the ring of integers modulo d and U_d be the multiplicative group of units in $\mathbb{Z}_d$.

Theorem 12. *Let p be a prime, $k \in \mathbb{Z}_p \setminus \{0\}$ and $\gcd(p, 2n-1) = 1 = \gcd(p-1, 2n-1)$. A $(\overline{k}, p)$-sequence of length $n > 1$ exists if and only if*

(a) *the order of p is odd in U_{2n-1},*

(b) *$(-1)^{n-1}k$ is a quadratic residue modulo p.*

Furthermore, if such a sequence exists, then there are exactly 2^l of them if $p = 2$ and 2^{l+1} if p is odd, where $2l$ is the number of irreducible factors of $\sum_{i=0}^{2n-2} x^i$.

Proof. ($\Rightarrow$) Let $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ be a $(\overline{k}, p)$-sequence of length $n > 1$. By Lemma 5,

$$f_{\mathbf{a}}(x) f_{\mathbf{a}}^*(x) = k \sum_{i=0}^{2n-2} x^i.$$

Note that $h(x) = (x-1)\sum_{i=0}^{2n-2} x^i = x^{2n-1} - 1$ and $h'(x) = (2n-1)x^{n-2} \neq 0$ in $\mathbb{Z}_p[x]$ for $\gcd(p, 2n-1) = 1$. It follows from Lemma 9 that $h(x)$ has no multiple roots. Thus, $\sum_{i=0}^{2n-2} x^i$ has no multiple roots.

Note that $a_{n-1}a_0 = k \not\equiv 0 \mod p$ for $a_{n-1}a_0$ is the coefficient of x^{2n-2} in $f_{\mathbf{a}}(x)f_{\mathbf{a}}^*(x)$. So, $a_{n-1} \not\equiv 0 \mod p$. Let $f_{\mathbf{a}}(x) = a_{n-1}q_1(x)q_2(x)\dots q_m(x)$ where each $q_i(x)$ is a monic irreducible polynomial.

Suppose p is of even order in U_{2n-1}. Let $2l$ be the order of p modulo $2n-1$. Then $(p^l-1)(p^l+1) = p^{2l}-1 \equiv 0 \mod (2n-1)$. Let $\beta_1, \beta_2, \dots, \beta_{2n-2}$ be all the distinct roots of $\sum_{i=0}^{2n-2} x^i$. Then each β_i is also a root of $x^{2n-1}-1$. Suppose $\beta_i^{p^l-1} = 1$ for all $1 \leqslant i \leqslant 2n-2$. Then each β_i is a root of $x^{p^l-1} - 1$. This implies that $x^{p^l-1} - 1 = (x^{2n-1} - 1)w(x)$ for some $w(x) \in \mathbb{Z}_p[x]$. By Lemma 11, $p^l \equiv 1 \mod (2n-1)$, a contradiction. So, $\beta_{i_0}^{p^l-1} \neq 1$ for some $1 \leqslant i_0 \leqslant 2n-2$. Let $\beta_{i_0}^{p^l-1}$ be a root of $q_{j_0}(x)$. Let E be a field extension of $\mathbb{Z}_p$ containing $\beta_{i_0}^{p^l-1}$. By Lemma 8, the Galois group $G(E/\mathbb{Z}_p)$ is a cyclic group with generator η. Note that $\eta^l(\beta_{i_0}^{p^l-1}) = \beta_{i_0}^{(p^l-1)p^l} = \beta_{i_0}^{(p^{2l}-1)+1-p^l} = \beta_{i_0}^{-(p^l-1)}$ where the last equality follows from $\beta_{i_0}^{2n-1} = 1$ and $p^{2l} - 1 \equiv 0 \mod 2n-1$. So, $\beta_{i_0}^{-(p^l-1)}$ is a root of $q_{j_0}(x)$. On the other hand, $\beta_{i_0}^{-(p^l-1)}$ is also a root of the monic irreducible polynomial $\frac{q_{j_0}^*(x)}{q_{j_0}(0)}$ (Lemma 4). This means $q_{j_0}(x) = \frac{q_{j_0}^*(x)}{q_{j_0}(0)}$. By Lemma 3, $\frac{q_{j_0}^*(x)}{q_{j_0}(0)}$ is an irreducible factor of $f_{\mathbf{a}}^*(x)$. Therefore, $\beta_{i_0}^{-(p^l-1)}$ a root of $\sum_{i=0}^{2n-2} x^i$ of multiplicity at least 2, a contradiction. Hence, the order of p is odd in U_{2n-1}. This proves part (a) of the theorem.

By part (a) of the theorem and Lemma 10, the degree of $q_i(x)$ is odd and $q_i(0) = -1$ for $1 \leqslant i \leqslant m$. Then by Lemma 3,

$$\begin{aligned} f_{\mathbf{a}}^*(x) &= a_{n-1}q_1(0)q_2(0)\dots q_m(0)\left(\frac{q_1^*(x)}{q_1(0)}\right)\left(\frac{q_2^*(x)}{q_2(0)}\right)\dots\left(\frac{q_m^*(x)}{q_m(0)}\right) \\ &= a_{n-1}(-1)^m\left(-q_1^*(x)\right)\left(-q_2^*(x)\right)\dots\left(-q_m^*(x)\right), \end{aligned}$$

where each $-q_i^*(x)$ is a monic irreducible polynomial (Lemma 4). Therefore $(-1)^m k \equiv a_{n-1}^2 \mod p$. Let e_i be the degree of $q_i(x)$. The degree of $f_{\mathbf{a}}(x)f_{\mathbf{a}}^*(x)$ is $2\sum_{i=1}^m e_i$. So, $2\sum_{i=1}^m e_i = 2n-2$, i.e., $\sum_{i=1}^m e_i = n-1$. Since each e_i is odd, we have $m \equiv \sum_{i=1}^m e_i \equiv n-1 \mod 2$. Hence, $(-1)^m = (-1)^{n-1}$ and part (b) of the theorem follows.

($\Leftarrow$) Suppose (a) and (b) hold. Note that $\left(\sum_{i=0}^{2n-2} x^i\right)^* = \sum_{i=0}^{2n-2} x^i$. So, if β is a root of $\sum_{i=0}^{2n-2} x^i$, then β^{-1} is also a root of $\sum_{i=0}^{2n-2} x^i$. This means that if $h(x)$ is a monic irreducible polynomial appearing in the factorization of $\sum_{i=0}^{2n-2} x^i$, then by Lemma 4 and 10, $-h^*(x)$ is also a monic irreducible polynomial appearing in the factorization of $\sum_{i=0}^{2n-2} x^i$. Furthermore, the degree of $h(x)$ and $-h^*(x)$ are odd and $-h^*(x) \neq h(x)$. So, we may write

$$\sum_{i=0}^{2n-2} x^i = h_1(x)h_2(x)\dots h_l(x)(-h_1^*(x))(-h_2^*(x))\dots(-h_l^*(x)).$$

If f_i is the degree of h_i, then $l \equiv \sum_{i=1}^{l} f_i \equiv n-1 \mod 2$. Therefore $(-1)^l = (-1)^{n-1}$. Since $(-1)^{n-1}k$ is a quadratic residue modulo p, there exists an $a_{n-1} \in \mathbb{Z}_p \setminus \{0\}$ with $a_{n-1}^2 \equiv (-1)^{n-1}k$. Now, there exists a unique $\mathbf{b} = (b_0, b_1, \dots, b_{n-2}, 1)$ with $f_{\mathbf{b}}(x) = h_1(x)h_2(x)\dots h_l(x)$. Let $\mathbf{a} = a_{n-1}\mathbf{b} = (a_{n-1}b_0, a_{n-1}b_1, \dots, a_{n-1}b_{n-2}, a_{n-1})$. Then $f_{\mathbf{a}}(x) = a_{n-1}h_1(x)h_2(x)\dots h_l(x)$ and by Lemma 3, $f_{\mathbf{a}}^*(x) = a_{n-1}h_1^*(x)h_2^*(x)\dots h_l^*(x)$. Therefore,

$$\begin{aligned}
f_{\mathbf{a}}(x)f_{\mathbf{a}}^*(x) &= a_{n-1}^2 h_1(x)h_2(x)\dots h_l(x)h_1^*(x)h_2^*(x)\dots h_l^*(x)\\
&= a_{n-1}^2(-1)^l h_1(x)h_2(x)\dots h_l(x)(-h_1^*(x))(-h_2^*(x))\dots(-h_l^*(x))\\
&= k\sum_{i=0}^{2n-2} x^i.
\end{aligned}$$

Hence, $\mathbf{a}$ is a $(\overline{k}, p)$-sequence (Lemma 5).

Finally, note that a_{n-1} and $-a_{n-1}$ are roots of $x^2-(-1)^{n-1}k$. We may choose $q_i = h_i(x)$ or $-h_i^*(x)$ for $1 \leqslant i \leqslant l$ and set $g_{\mathbf{c}}(x) = \pm a_{n-1}q_1(x)q_2(x)\dots q_l(x)$. Then $\mathbf{c}$ is also a $(\overline{k}, p)$-sequence. So, if such a sequence exists, there are exactly 2^l of them if $p=2$ and 2^{l+1} if p is odd. This completes the proof of the theorem. □

Note that when $p=2$, Theorem 12 is the same as Theorem 2. So, Theorem 12 can be considered as a generalization of Theorem 2.

Recall that $\mathbf{y}_k = (y_0, y_1, y_2, \dots)$ with $y_i = (-1)^i k$. If $k \equiv 0 \mod p$, then $\mathbf{y}_k = \overline{0}$. This case has been considered in Corollary 6. So, we may assume $k \in \mathbb{Z}_p \setminus \{0\}$. If $p=2$, then $\mathbf{y}_k = \overline{1}$. This case has been considered in Theorem 2 and 12. So, we may assume that p is an odd prime.

Lemma 13.

(a) *Suppose n is odd. Then $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ is a $(\overline{k}, p)$-sequence if and only if $\mathbf{b} = (a_0, -a_1, \dots, (-1)^{n-1}a_{n-1})$ is a $(\mathbf{y}_k, p)$-sequence.*

(b) *Suppose n is even. Then $\mathbf{a} = (a_0, a_1, \dots, a_{n-1})$ is a $(\overline{-k}, p)$-sequence if and only if $\mathbf{b} = (a_0, -a_1, \dots, (-1)^{n-1}a_{n-1})$ is a $(\mathbf{y}_k, p)$-sequence.*

Proof. By Lemma 5, $\mathbf{b}$ is a $(\mathbf{y}_k, p)$-sequence if and only if

$$\begin{aligned}
f_{\mathbf{b}}(x)f_{\mathbf{b}}^*(x) &= \sum_{i=0}^{n-1}(-1)^{n-1-i}kx^i + x^{n-1}\sum_{i=1}^{n-1}(-1)^i kx^i\\
&= (-1)^{n-1}k\sum_{i=0}^{2n-2}(-1)^i x^i.
\end{aligned}$$

Suppose n is odd. Then $f_{\mathbf{b}}(x)f_{\mathbf{b}}^*(x) = k\sum_{i=0}^{2n-2}(-1)^i x^i$. By Lemma 5, $\mathbf{a}$ is a $(\overline{k}, p)$-sequence if and only if

$$f_{\mathbf{a}}(x)f_{\mathbf{a}}^*(x) = k\sum_{i=0}^{2n-2} x^i.$$

Hence, part (a) of the lemma follows by noting that $f_{\mathbf{b}}(x) = f_{\mathbf{a}}(-x)$ and $f_{\mathbf{a}}(x) = f_{\mathbf{b}}(-x)$.

Suppose n is even. Then $f_{\mathbf{b}}(x)f^*_{\mathbf{b}}(x) = -k\sum_{i=0}^{2n-2}(-1)^i x^i$. By Lemma 5, $\mathbf{a}$ is a $(\overline{-k}, p)$-sequence if and only if

$$f_{\mathbf{a}}(x)f^*_{\mathbf{a}}(x) = -k\sum_{i=0}^{2n-2} x^i.$$

Hence, part (b) of the lemma follows by noting that $f_{\mathbf{b}}(x) = f_{\mathbf{a}}(-x)$ and $f_{\mathbf{a}}(x) = f_{\mathbf{b}}(-x)$. □

Theorem 14. *Let p be an odd prime, $k \in \mathbb{Z}_p \setminus \{0\}$ and $\gcd(p, 2n-1) = 1 = \gcd(p-1, 2n-1)$. A $(\mathbf{y}_k, p)$-sequence of length $n > 1$ exists if and only if*

(a) *the order of p is odd in U_{2n-1},*

(b) *k is a quadratic residue modulo p.*

Furthermore, if such a sequence exists, then there are exactly 2^{l+1} of them, where $2l$ is the number of irreducible factors of $\sum_{i=0}^{2n-2} x^i$.

Proof. Suppose n is odd. By part (a) of Lemma 13, there is a $(\mathbf{y}_k, p)$-sequence of length $n > 1$ if and only if there is a $(\overline{k}, p)$-sequence of length $n > 1$. Hence, Theorem 14 follows from Theorem 12 by noting that $(-1)^{n-1}k = k$.

Suppose n is even. By part (a) of Lemma 13, there is a $(\mathbf{y}_k, p)$-sequence of length $n > 1$ if and only if there is a $(\overline{-k}, p)$-sequence of length $n > 1$. Hence, Theorem 14 follows from Theorem 12 by noting that $(-1)^{n-1}(-k) = k$. □

Corollary 15. *Let p be a prime, $k \in \mathbb{Z}_p \setminus \{0\}$ and $\gcd(p, 2n-1) = 1 = \gcd(p-1, 2n-1)$. If there is a $(\overline{k}, p)$-sequence or a $(\mathbf{y}_k, p)$-sequence of length $n > 1$, then p is a quadratic residue modulo $2n-1$.*

Proof. By Theorem 12 or 14, the order of p is odd in U_{2n-1}. Let $2e+1$ be the order of p. Then $(p^{e+1})^2 \equiv p^{2e+2} \equiv p \mod (2n-1)$. Thus, p is a quadratic residue modulo $2n-1$. □

Part (a) of the following Corollary was proved by Inglis and Wiseman [2, Proposition 1]. It was asked by Alles [1, Problem (1)].

Corollary 16. *Let p be a prime, $k \in \mathbb{Z}_p \setminus \{0\}$ and $\gcd(p, 2n-1) = 1 = \gcd(p-1, 2n-1)$. Suppose there is a $(\overline{k}, p)$-sequence or a $(\mathbf{y}_k, p)$-sequence of length $n > 1$. Then*

(a) $n \equiv 0$ *or* $1 \mod 4$, *if* $p = 2$;

(b) $n \equiv 0$ *or* $1 \mod 6$, *if* $p = 3$;

(c) $n \equiv 0$ *or* $1 \mod 5$, *if* $p = 5$;

(d) $n \equiv 0, 1, 10, 13, 15, 16, 19, 24, 27, 28, 30, 33 \mod 42$, *if* $p = 7$.

Proof. (a) By Corollary 15, 2 is a quadratic residue modulo $2n-1$. Let q be a prime appearing in the factorization of $2n-1$. Then q is odd and 2 is a quadratic residue modulo q. Therefore $q \equiv 1$ or $7 \mod 8$. This implies that $2n-1 \equiv 1$ or $7 \mod 8$. Thus, $n \equiv 1$ or $0 \mod 4$.

(b) Since $\gcd(3, 2n-1) = 1$, we require $2n-1 \equiv 1$ or $2 \mod 3$, that is $n \equiv 1$ or $0 \mod 3$. By Corollary 15, 3 is a quadratic residue modulo $2n-1$. If q is a prime appearing in the factorization of $2n-1$, then q is odd and 3 is a quadratic residue modulo q. By the Quadratic Reciprocity Law, $q \equiv \pm 1 \mod 12$. This implies that $2n-1 \equiv 1$ or $11 \mod 12$. Thus, $n \equiv 1$ or $0 \mod 6$.

(c) Since $\gcd(5, 2n-1) = 1$, we require $2n-1 \equiv 1, 2, 3,$ or $4 \mod 5$, that is $n \equiv 1, 4, 2,$ or $0 \mod 5$. As in part (b), if q is a prime appearing in the factorization of $2n-1$, then 5 is a quadratic residue modulo q. By the Quadratic Reciprocity Law, $q \equiv \pm 1 \mod 5$. This implies that $2n-1 \equiv 1$ or $4 \mod 5$. Thus, $n \equiv 1$ or $0 \mod 5$.

(d) Since $\gcd(7, 2n-1) = 1$ and $\gcd(6, 2n-1) = 1$, $n \not\equiv 4 \mod 7$ and $n \not\equiv 2 \mod 3$. As before, if q is a prime appearing in the factorization of $2n-1$, then 7 is a quadratic residue modulo q. By the Quadratic Reciprocity Law, $q \equiv \pm 1, \pm 3,$ or $\pm 9 \mod 28$. This implies that $2n-1 \equiv \pm 1, \pm 3,$ or $\pm 9 \mod 28$. Thus, $n \equiv 0, 1, 2, 5, 10,$ or $13 \mod 14$. Since $n \not\equiv 2 \mod 3$ and $\gcd(3, 14) = 1$, we must have $n \equiv 0, 28, 1, 15, 16, 30, 19, 33, 10, 24, 13$ or $27 \mod 42$. □

Acknowledgments

We would like to thank the anonymous referee for the comments that helped us make several improvements to this paper. This project was supported by the Frontier Science Research Cluster, University of Malaya (RG367-15AFR).

References

[1] P. Alles, On a conjecture of J. Pelikán, *J. Combin. Theory Ser. A* **60** (1992), 312–313.

[2] N.F.J. Inglis and J.D.A. Wiseman, Very odd sequences, *J. Combin. Theory Ser. A* **71** (1995), 89–96.

[3] N. Jacobson, *Basic Algebra I*, second edition, W.H. Freeman and Company, U.S.A., 1985.

[4] F.J. MacWilliams and A.M. Odlyzko, Pelikan's conjecture and cyclotomic cosets, *J. Combin. Theory Ser. A* **22** (1977), 110–114.

[5] P. Moree and P. Solé, Around Pelikán's conjecture on very odd sequences, *Manuscripta Math.* **117**, (2005), 219–238.

[6] J. Pelikán, Contribution to "Problems", *Colloq. Math. Soc. János Bolyai* **10** p. 1549, North-Holland, Amsterdam, 1975.