Research Article

Necklaces, Self-Reciprocal Polynomials, and q -Cycles

Umarin Pintoaptang,^{1,2} Vichian Laohakosol,³ and Suton Tadee⁴

¹ Department of Mathematics, Faculty of Science, Naresuan University, Phitsanulok 65000, Thailand

² Centre of Excellence in Mathematics, CHE, Si Ayutthaya Road, Bangkok 10400, Thailand

³ Department of Mathematics, Faculty of Science, Kasetsart University, Bangkok 10900, Thailand

⁴ Department of Mathematics and Statistics, Faculty of Science and Technology, Thepsatri Rajabhat University, Lopburi 15000, Thailand

Correspondence should be addressed to Vichian Laohakosol; fscivil@ku.ac.th

Received 16 June 2014; Revised 16 October 2014; Accepted 16 October 2014; Published 9 November 2014

Academic Editor: Toufik Mansour

Copyright © 2014 Umarin Pintoaptang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Let $n \geq 2$ be a positive integer and q a prime power. Consider necklaces consisting of n beads, each of which has one of the given q colors. A primitive C_n -orbit is an equivalence class of n necklaces closed under rotation. A C_n -orbit is self-complementary when it is closed under an assigned color matching. In the work of Miller (1978), it is shown that there is a 1-1 correspondence between the set of primitive, self-complementary C_n -orbits and that of self-reciprocal irreducible monic (srim) polynomials of degree n . Let N be a positive integer relatively prime to q . A q -cycle mod N is a finite sequence of nonnegative integers closed under multiplication by q . In the work of Wan (2003), it is shown that q -cycles mod N are closely related to monic irreducible divisors of $x^N - 1 \in \mathbb{F}_q[x]$. Here, we show that: (1) q -cycles can be used to obtain information about srin polynomials; (2) there are correspondences among certain q -cycles and C_n -orbits; (3) there are alternative proofs of Miller's results in the work of Miller (1978) based on the use of q -cycles.

1. Introduction

1.1. Necklaces. Let $n \in \mathbb{N}$, $n \geq 2$, and let q be a prime power. Consider the set

$$\eta(n, q) = \{(c_0, c_1, \dots, c_{n-1}); c_i \in \{0, 1, \dots, q-1\}\} \quad (1)$$

of all necklaces (or seating arrangements) consisting of n beads, each of which is colored with one of q colors denoted by $0, 1, \dots, q-1$. Clearly, $|\eta(n, q)| = q^n$. Partition the colors into $[q/2]$ pairs with one extra color if q is odd. Two colors in the same pair are called *complementary*, and if q is odd the extra color is called *self-complementary*. The complement of color c is so arranged as the color $q-1-c$. Let

$$C_n = \{e := r^0, r, r^2, \dots, r^{n-1}\} \quad (2)$$

be the cyclic group of order n ; the group C_n acts on $\eta(n, q)$ via r^k ($k \in \{0, 1, \dots, n-1\}$) rotating each bead k -times. Let $H = \{e, h\}$ be the group which acts on $\eta(n, q)$ via e , the identity, preserving each color and h replacing each color

by its complement. Each equivalence class of elements in $\eta(n, q)$ under the action of C_n is called a C_n -orbit. For a C_n -orbit $\mathcal{O}$, the element $h(\mathcal{O})$ is an equivalence class derived from $\mathcal{O}$ through the action $h \in H$. A C_n -orbit $\mathcal{O}$ is called a *self-complementary* if it is invariant under H ; that is, $\mathcal{O} = h(\mathcal{O})$. The remaining C_n -orbits fall into pairs $\{\mathcal{O}, h(\mathcal{O})\}$ called *complementary pairs*. A necklace in $\eta(n, q)$ is called *primitive* if its C_n -orbit has cardinality n .

1.2. Self-Reciprocal, Irreducible, Monic Polynomials. Let $\mathbb{F}_q$ denote the finite field of q elements. The reciprocal polynomial f^* of

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{F}_q[x], \quad a_n \neq 0 \quad (3)$$

is defined by

$$f^*(x) = x^n f\left(\frac{1}{x}\right) = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n. \quad (4)$$

A polynomial $f \in \mathbb{F}_q[x]$ is called *self-reciprocal* if $f(x) = f^*(x)$.

The following characterization is well known.

Proposition 1 (see [1, page 275]). *Let $f \in \mathbb{F}_q[x]$ be irreducible and monic of degree ≥ 2 . Then f is self-reciprocal if and only if its set of roots (each of which is evidently nonzero) is closed under inversion (and so its degree must be even).*

We are interested here in *self-reciprocal, irreducible, monic* (srim) polynomials in $\mathbb{F}_q[x]$. Since there is only one first degree srim-polynomial, namely, $x + 1$, from now on we treat only srim-polynomials of even degree ≥ 2 .

Let α be a generator (primitive element) of the group $\mathbb{F}_{q^n}^*$ and let $f(x) \in \mathbb{F}_q[x]$ be an irreducible monic polynomial of degree n . It is well known [2, Theorem 2.14] that all distinct roots of $f(x)$ are of the form

$$\alpha^k, \alpha^{qk}, \alpha^{q^2k}, \dots, \alpha^{q^{n-1}k} \quad (5)$$

for some integer $0 \leq k \leq q^n - 1$. Let

$$k = \sum_{i=0}^{n-1} e_i q^i := (e_0, e_1, \dots, e_{n-1}), \quad (6)$$

$$0 \leq e_i \leq q - 1 \quad (i = 0, 1, \dots, n - 1)$$

be its base q expansion. For an irreducible, monic $f(x) \in \mathbb{F}_q[x]$ of degree n , we associate a C_n -orbit containing the necklace $k := (e_0, e_1, \dots, e_{n-1})$.

1.3. q -Cycles. Let N be a fixed positive integer relatively prime to q . Let $a_0, a_1, \dots, a_{\ell-1}$ be ℓ distinct numbers chosen from $\mathbb{Z}_N := \{0, 1, \dots, N - 1\}$. If

$$\begin{aligned} a_i q &\equiv a_{i+1} \pmod{N} \quad (i = 0, 1, \dots, \ell - 2) \\ (a_0 q^\ell) &\equiv a_{\ell-1} q \equiv a_0 \pmod{N}, \end{aligned} \quad (7)$$

then we say that $(a_0, a_1, \dots, a_{\ell-1})$ forms a q -cycle mod N with leading element a_0 , and call ℓ the *length* of this q -cycle. The notion of q -cycles was introduced by Wan in his book [3, page 203]. Since $q^{o_N(q)} \equiv 1 \pmod{N}$, where $o_N(q)$ is the order of q in $\mathbb{Z}_N^* := \mathbb{Z}_N \setminus \{0\}$ (the multiplicative group of nonzero integers modulo N), it clearly follows that each q -cycle always has a unique length ℓ which is the least positive integer ℓ for which $a \equiv a q^\ell \pmod{N}$. The concept of q -cycles is important because of the following connections with irreducible polynomials in $\mathbb{F}_q[x]$ [3, Theorem 9.11].

Let α be a primitive N th root of unity (if the order of q in $\mathbb{Z}_N^*$ is m , then there exists a primitive N th root of unity in $\mathbb{F}_{q^m}$). If $(a_0, a_1, \dots, a_{\ell-1})$ is a q -cycle, then

$$h(x) = (x - \alpha^{a_0})(x - \alpha^{a_1}) \cdots (x - \alpha^{a_{\ell-1}}) \quad (8)$$

is a monic irreducible factor of $x^N - 1$ in $\mathbb{F}_q[x]$.

Conversely, if $h(x)$ is a monic irreducible factor of $x^N - 1$ in $\mathbb{F}_q[x]$, then all the roots of $h(x)$ are powers of α whose exponents form a q -cycle.

We henceforth refer to these two facts as the cycle-polynomial correspondence.

2. Connection between q -Cycles and Irreducible Polynomials

We start with a basic result.

Lemma 2. *Let $N = N_1 > N_2 > \dots > N_d = 1$ be all the (positive integer) divisors of N .*

- (i) *If $b \in \mathbb{Z}_N$ is such that $\gcd(b, N) = N_r$ for some $r \in \{1, \dots, d\}$, then each q -cycle mod N with leading element b has length $o_{N/N_r}(q)$.*
- (ii) *The polynomial $f \in \mathbb{F}_q[x]$ constructed via (8) from a q -cycle with leading element b , $\gcd(b, N) = N_r$ ($r \in \{1, \dots, d\}$), is a monic irreducible polynomial with $f(0) \neq 0$, and $\deg(f) = o_{N/N_r}(q)$.*
- (iii) *Each irreducible polynomial $f \in \mathbb{F}_q[x]$ with $f(0) \neq 0$, and $\deg(f) = o_{N_r}(q)$ is an irreducible factor of $x^N - 1$ arising, through (8), from a q -cycle with leading element b , $\gcd(b, N) = N/N_r$.*

Proof. (i) Note from the definition of q -cycle that a q -cycle mod N , with leading element b and $\gcd(b, N) = N_r$, has length ℓ if and only if N/N_r divides $q^\ell - 1$ but does not divide $q - 1, q^2 - 1, \dots, q^{\ell-1} - 1$ (if $\ell = 1$, only the first divisibility needs to be considered). This defining condition of ℓ is indeed the meaning of $o_{N/N_r}(q)$.

(ii)-(iii) From part (i), each q -cycle mod N with leading element b , $\gcd(b, N) = N_r$, has length $o_{N/N_r}(q)$. Through the cycle-polynomial correspondence, such a q -cycle gives rise to a monic irreducible $f \in \mathbb{F}_q[x]$, $f(0) \neq 0$, of degree $o_{N/N_r}(q)$ and conversely. $\square$

By Lemma 2(i), a q -cycle mod $q^m + 1$ with leading element $b = 1$ has length $o_{q^m+1}(q)$. Since $q^{2m} \equiv 1 \pmod{q^m + 1}$, we have $o_{q^m+1}(q) \mid 2m$. From the observation that $o_{q^m+1}(q) > m$, we immediately obtain $o_{q^m+1}(q) = 2m$, and hence, a q -cycle mod $q^m + 1$ with leading element $b = 1$ has length $2m$.

The case $N = q^m + 1$ is of particular interest for it shows that q -cycles are closely related to srim-polynomials.

Theorem 3. *Let $m \in \mathbb{N}$. Then each q -cycle mod $q^m + 1$ of length $2m$ gives rise through the cycle-polynomial correspondence to a srim-polynomial in $\mathbb{F}_q[x]$ of degree $2m$ and conversely.*

Proof. Let $(a = a_0, \dots, a_{2m-1})$ be a q -cycle mod $q^m + 1$ of length $2m$. By Lemma 2, this q -cycle gives rise, through (8), to a monic irreducible polynomial in $\mathbb{F}_q[x]$ of degree $2m$ and conversely. There remains only to check that such polynomial is self-reciprocal, that is, to check that, for α being a primitive $(q^m + 1)$ th root of unity, the set $\{\alpha^a, \alpha^{qa}, \dots, \alpha^{aq^{2m-1}}\}$ is closed under inversion. Let $\gcd(a, q^m + 1) = g$. Putting $a = gb$, where $b \in \mathbb{N}$, is such that $\gcd(b, q^m + 1) = 1$. Since α^b is also a primitive $(q^m + 1)$ th root of unity, it suffices to treat only the case $a = g$. The assertion that the set $\{\alpha^a, \alpha^{qa}, \dots, \alpha^{aq^{2m-1}}\}$ is closed under inversion is immediate from $\alpha^{q^m} = \alpha^{-1}$ and the observation that $\alpha^{-gq^j} = \alpha^{gq^{m+j}}$ for $j \in \{0, 1, \dots, m - 1\}$. $\square$

3. Connection between Necklaces and q -Cycles

We start with a characterization of primitive necklaces. In the proof of our next theorem, we make use of a 1-1 correspondence between a necklace $(d_0, d_1, \dots, d_{n-1})$ and a base q representation of the form $d_0 + d_1q + \dots + d_{n-1}q^{n-1}$.

Theorem 4. *Let $(c_0, c_1, \dots, c_{n-1})$ be a primitive necklace in a C_n -orbit. Then this C_n -orbit is self-complementary if and only if there exists $s \in \{0, 1, \dots, n-1\}$ such that*

$$c_{s+j \bmod n} + c_{j \bmod n} = q - 1 \quad \forall j \in \{0, 1, \dots, n-1\}. \quad (9)$$

Proof. The C_n -orbit containing a primitive necklace $(c_0, c_1, \dots, c_{n-1})$ is of the form

$$\begin{aligned} \mathcal{O} = \{ & (c_0, c_1, \dots, c_{n-1}), (c_1, c_2, \dots, c_{n-1}, c_0), \\ & (c_2, c_3, \dots, c_{n-1}, c_0, c_1), \dots, (c_{n-1}, c_0, c_1, \dots, c_{n-2}) \}, \end{aligned} \quad (10)$$

where all the necklaces in $\mathcal{O}$ are distinct. From the 1-1 correspondence mentioned above, the base q representations of the elements in $\mathcal{O}$ are

$$\begin{aligned} L_0 & \sim c_0 + c_1q + \dots + c_{n-1}q^{n-1}, \\ L_1 & \sim c_1 + c_2q + \dots + c_{n-1}q^{n-2} + c_0q^{n-1}, \\ L_2 & \sim c_2 + c_3q + \dots + c_0q^{n-2} + c_1q^{n-1}, \dots, \\ L_{n-1} & \sim c_{n-1} + c_0q + c_1q^2 + \dots + c_{n-2}q^{n-1}. \end{aligned} \quad (11)$$

From the definition, $\mathcal{O}$ is self-complementary if and only if

$$\{L_0, L_1, \dots, L_{n-1}\} = \{h(L_0), h(L_1), \dots, h(L_{n-1})\}, \quad (12)$$

where

$$\begin{aligned} h(L_0) & \sim (q-1-c_0) + (q-1-c_1)q + \dots \\ & \quad + (q-1-c_{n-1})q^{n-1} \\ h(L_1) & \sim (q-1-c_1) + (q-1-c_2)q + \dots \\ & \quad + (q-1-c_{n-1})q^{n-2} + (q-1-c_0)q^{n-1} \\ h(L_2) & \sim (q-1-c_2) + (q-1-c_3)q + \dots \\ & \quad + (q-1-c_0)q^{n-2} + (q-1-c_1)q^{n-1} \\ & \quad \vdots \\ h(L_{n-1}) & \sim (q-1-c_{n-1}) + (q-1-c_0)q + (q-1-c_1)q^2 \\ & \quad + \dots + (q-1-c_{n-2})q^{n-1}. \end{aligned} \quad (13)$$

If $\mathcal{O}$ is self-complementary, then there exists $s \in \{0, 1, \dots, n-1\}$ such that $L_s = h(L_0)$; that is,

$$\begin{aligned} & c_s + c_{s+1}q + \dots + c_{s+(n-s-1)}q^{n-s-1} + c_0q^{n-s} \\ & \quad + c_1q^{n-s+1} + \dots + c_{s-1}q^{n-s+s-1} \\ & = (q-1-c_0) + (q-1-c_1)q + \dots + (q-1-c_{n-1})q^{n-1}, \end{aligned} \quad (14)$$

yielding

$$\begin{aligned} c_s & = q-1-c_0, \\ c_{s+1} & = q-1-c_1, \dots, c_{s+(n-s-1)} = q-1-c_{n-s-1}, \\ c_0 & = q-1-c_{n-s}, \\ c_1 & = q-1-c_{n-(s-1)}, \dots, c_{s-1} = q-1-c_{n-1}, \end{aligned} \quad (15)$$

which is (9). On the other hand, if (9) holds, reversing the above steps and appealing to the action of r^k , we see that $\mathcal{O}$ is self-complementary. $\square$

By the proof of Lemma 2(i), a q -cycle $\bmod q^n - 1$ with leading element $b = 1$ has length n . The case $N = q^n - 1$ shows that q -cycles are related to C_n -orbits containing a primitive necklace.

Let $(a_0, a_1, \dots, a_{n-1})$ be a q -cycle $\bmod q^n - 1$ of length n . Then $a_0, a_1, \dots, a_{n-1}$ are n distinct numbers in $\{0, 1, \dots, q^n - 2\}$ satisfying

$$\begin{aligned} a_i q & \equiv a_{i+1} \pmod{q^n - 1} \quad (i = 0, 1, \dots, n-2) \\ (a_0 q^n) & \equiv a_{n-1} q \equiv a_0 \pmod{q^n - 1}. \end{aligned} \quad (16)$$

Writing with respect to base q representation, we have

$$\begin{aligned} a_0 & := e_0 + e_1q + \dots + e_{n-1}q^{n-1}, \\ 0 & \leq e_i \leq q-1 \quad (i = 0, 1, \dots, n-1), \end{aligned} \quad (17)$$

and associate with a_0 the necklace $(e_0, e_1, \dots, e_{n-1})$. Working $\bmod q^n - 1$, we get

$$a_1 = qa_0 = e_0q + e_1q^2 + \dots + e_{n-2}q^{n-1} + e_{n-1}, \quad (18)$$

showing that the necklace associated with a_1 is $(e_{n-1}, e_0, e_1, \dots, e_{n-2})$. Proceeding in the same manner, we see that the necklace associated with a_j ($j = 0, 1, \dots, n-1$) is

$$(e_{n-j \bmod n}, e_{n-j+1 \bmod n}, \dots, e_{n-j-1 \bmod n}). \quad (19)$$

Since $a_0, a_1, \dots, a_{n-1}$ are distinct, the necklaces associated with each a_i are distinct, and so the necklace $(e_0, e_1, \dots, e_{n-1})$ is primitive. The above steps can evidently be reversed and we have thus proved.

Theorem 5. *For $n \in \mathbb{N}$, there is a 1-1 correspondence between the set of q -cycles $\bmod q^n - 1$ of length n and the set of C_n -orbits containing a primitive necklace.*

We proceed next to consider self-complementary orbits and q -cycles. Let $(b_0, b_1, \dots, b_{2m-1})$ be a q -cycle mod $q^m + 1$ of length $2m$ so that

$$b_i q \equiv b_{i+1} \pmod{q^m + 1} \quad (i = 0, 1, \dots, 2m-2). \quad (20)$$

By Theorem 3, the polynomial

$$h(x) = (x - \beta^{b_0})(x - \beta^{b_1}) \cdots (x - \beta^{b_{2m-1}}) \quad (21)$$

is a srin -polynomial of degree $2m$ over $\mathbb{F}_q$, where β is a primitive $(q^m + 1)$ th root of unity. Let α be a primitive $(q^{2m} - 1)$ th root of unity. Then we may take

$$\beta = \alpha^{q^{m-1}}. \quad (22)$$

Writing $b_0 \in \mathbb{Z}_{q^m+1}$ with respect to base q representation, we get

$$b_0 = f_0 + f_1 q + \cdots + f_{m-1} q^{m-1} \quad \text{or} \quad b_0 = q^m. \quad (23)$$

Now working mod $q^{2m} - 1$, we have either

$$\begin{aligned} (q^m - 1)b_0 &\equiv f_0 q^m + f_1 q^{m+1} + \cdots + f_{m-1} q^{2m-1} - f_0 \\ &\quad - f_1 q - \cdots - f_{m-1} q^{m-1} \pmod{q^{2m} - 1} \\ &\equiv (q - f_0) + (q - 1 - f_1)q + \cdots \\ &\quad + (q - 1 - f_{m-1})q^{m-1} \\ &\quad + (f_0 - 1)q^m + f_1 q^{m+1} + \cdots \\ &\quad + f_{m-1} q^{2m-1} \pmod{q^{2m} - 1}, \end{aligned} \quad (24)$$

provided $f_0 \neq 0$ (if $f_0 = 0$, the above congruences can be adjusted accordingly), or

$$\begin{aligned} (q^m - 1)b_0 &= (q^m - 1)q^m \equiv (q - 1)q^m + (q - 1)q^{m+1} + \cdots \\ &\quad + (q - 1)q^{2m-1} \pmod{q^{2m} - 1}. \end{aligned} \quad (25)$$

Letting

$$\begin{aligned} a_0 &:= e_0 + e_1 q + \cdots + e_{m-1} q^{m-1} + e_m q^m + e_{m+1} q^{m+1} \\ &\quad + \cdots + e_{2m-1} q^{2m-1} \end{aligned} \quad (26)$$

be the right-hand expression in (24) or (25), we see that

$$q - 1 = e_0 + e_m = e_1 + e_{m+1} = \cdots = e_{m-1} + e_{2m-1}; \quad (27)$$

that is, the relation (9) holds with $n = 2m$, $r = m + 1$. Proceeding in the same manner, we see that the digits in $(q^m - 1)b_j := a_j$ also satisfy the relation (9). Theorem 4 shows then that $(a_0, a_1, \dots, a_{2m-1})$ represents a primitive necklace in a self-complementary C_{2m} -orbit.

Conversely, given a self-complementary C_{2m} -orbit containing a primitive necklace $(a_0, a_1, \dots, a_{2m-1})$ whose first element is of the form (26), being self-complementary, we may assume without loss of generality that the digits in the first element are so arranged that the relations in (27) hold. Reversing the arguments, we get a q -cycle mod $q^m + 1$ of length $2m$ of the form $(b_0, b_1, \dots, b_{2m-1})$, where $(q^m - 1)b_j = a_j$ ($j = 0, 1, \dots, 2m-1$). We have thus proved.

Theorem 6. *For $m \in \mathbb{N}$, there is a 1-1 correspondence between the set of q -cycles mod $q^m + 1$ of length $2m$ and the set of self-complementary C_{2m} -orbits containing a primitive necklace.*

An immediate consequence of Theorem 6 is the following result of Miller [4] mentioned in the introduction.

Corollary 7. *For $m \in \mathbb{N}$, there is a 1-1 correspondence between the set of self-complementary C_{2m} -orbits containing a primitive necklace and the set of srin -polynomials of degree $2m$.*

Proof. From the cycle-polynomial correspondence, each q -cycle mod $q^m + 1$ of length $2m$ gives rise, through (21), to a srin -polynomial of degree $2m$ and conversely. The corollary follows at once from Theorem 6. $\square$

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This paper is supported by the Centre of Excellence in Mathematics, the Commission on Higher Education, Thailand, and by Kasetsart University and Faculty of Science through Research Cluster Fund (KU SciRCE, Cluster 4, no. 1).

References

- [1] J. L. Lucas and G. L. Mullen, "Self-reciprocal irreducible polynomials over finite fields," *Designs, Codes and Cryptography*, vol. 33, no. 3, pp. 275–281, 2004.
- [2] R. Lidl and H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge, UK, 1997.
- [3] Z.-X. Wan, *Lectures on Finite Fields and Galois Rings*, World Scientific, Singapore, 2003.
- [4] R. L. Miller, "Necklaces, symmetries and self-reciprocal polynomials," *Discrete Mathematics*, vol. 22, no. 1, pp. 25–33, 1978.