

A GENERALIZED LUCAS SEQUENCE AND PERMUTATION BINOMIALS

AMIR AKBARY AND QIANG WANG

(Communicated by Jonathan M. Borwein)

ABSTRACT. Let p be an odd prime and $q = p^m$. Let l be an odd positive integer. Let $p \equiv -1 \pmod{l}$ or $p \equiv 1 \pmod{l}$ and $l \mid m$. By employing the integer sequence $a_n = \sum_{t=1}^{\frac{l-1}{2}} \left(2 \cos \frac{\pi(2t-1)}{l} \right)^n$, which can be considered as a generalized Lucas sequence, we construct all the permutation binomials $P(x) = x^r + x^u$ of the finite field \mathbb{F}_q .

1. INTRODUCTION

For an integer $n \geq 0$ and an odd positive integer l , let

$$a_n = \sum_{t=1}^{\frac{l-1}{2}} \left(2 \cos \frac{\pi(2t-1)}{l} \right)^n = \sum_{t=1}^{\frac{l-1}{2}} \left((-1)^{t+1} 2 \cos \frac{\pi t}{l} \right)^n.$$

One can show that $\{a_n\}_{n=0}^{\infty}$ is an integer sequence. For $l = 5$, $a_n = L_n$ is the Lucas sequence. For $l = 7$, a_n satisfies the recurrence relation $a_n = a_{n-1} + 2a_{n-2} - a_{n-3}$ with initial values $a_0 = 3$, $a_1 = 1$, $a_2 = 5$. This is the sequence A094648 in Sloane's Encyclopedia [8]. In this paper we investigate the relation of the sequence a_n with permutation properties of a binomial over a finite field.

Let \mathbb{F}_q be a finite field of $q = p^m$ elements with characteristic p . A polynomial $P(x) \in \mathbb{F}_q[x]$ is called a *permutation polynomial* of \mathbb{F}_q if $P(x)$ induces a bijective map from \mathbb{F}_q to itself. Permutation polynomials for a finite prime field \mathbb{F}_p were first investigated by Hermite [4]. The first systematic study of permutation polynomials over a general finite field is due to Dickson [1]. One of the most useful characterizations of permutation polynomials is the following ([5], Theorem 7.4).

Hermite's Criterion. $P(x)$ is a permutation polynomial of \mathbb{F}_q if and only if

- (i) $P(x)$ has exactly one root in \mathbb{F}_q .
- (ii) For each integer t with $1 \leq t \leq q-2$ and $t \not\equiv 0 \pmod{p}$, the reduction of $[P(x)]^t \pmod{(x^q - x)}$ has degree less than or equal to $q-2$.

Using this criterion Dickson classified the permutation polynomials of degree ≤ 6 over a finite field \mathbb{F}_q ; moreover, he showed that for degree $d = 4$ or 6 there

Received by the editors July 27, 2004.

2000 *Mathematics Subject Classification.* Primary 11T06.

The research of both authors was partially supported by NSERC.

are no permutation polynomials over \mathbb{F}_q for large $q = p^m$ provided $p \neq 2$. In 1966 Carlitz conjectured that for a given even integer d there are no permutation polynomials of degree d over \mathbb{F}_q for sufficiently large q . Later Hayes [3] established this conjecture when $p \nmid d$. In 1993, Fried, Guralnick, and Saxl [2] proved that the Carlitz conjecture is true in general. Results of this type in the theory of permutation polynomials indicate that the search for permutation polynomials is an interesting and challenging problem.

In this paper we consider the binomial $P(x) = x^r + x^u$ with $r < u$. Let $l = \frac{q-1}{(u-r, q-1)}$ and $s = \frac{q-1}{l}$. Then we can rewrite $P(x)$ as $P(x) = x^r(1 + x^{es})$ where $(e, l) = 1$. One can show that if $P(x) = x^r(1 + x^{es})$ is a permutation polynomial, then $(r, s) = 1$, and l is odd (these are consequences of Theorem 1.2 of [9]). From now on, we assume that l, r, e and s satisfy the following conditions:

$$(*) \quad (r, s) = 1, (e, l) = 1, \text{ and } l \text{ is odd.}$$

The sequence $\{a_n\}$ is called s -periodic over \mathbb{F}_p if $a_n \equiv a_{n+ks} \pmod{p}$ for integers k and n . We first prove the following.

Theorem 1.1. *Under the conditions (*) on l, r, e and s , the binomial $P(x) = x^r(1 + x^{es})$ is a permutation binomial of \mathbb{F}_q if $(2r + es, l) = 1$, $2^s \equiv 1 \pmod{p}$ and $\{a_n\}$ is s -periodic over \mathbb{F}_p .*

The connection between the s -periodicity of the sequence $\{a_n\}$ and the permutation binomial $P(x)$ arises from the fact that if $P(x)$ is a permutation binomial, then by Hermite's criterion certain lacunary sums of binomial coefficients will be zero. These lacunary sums have expressions in terms of the sequence a_n (see Lemma 2.2 and Corollary 2.3).

As an application of Theorem 1.1, in our next theorem we characterize permutation binomials $P(x) = x^r + x^u$ over certain finite fields. More precisely, we prove the following.

Theorem 1.2. *Let p be an odd prime and $q = p^m$. Let l be an odd positive integer. Let $p \equiv -1 \pmod{l}$ or $p \equiv 1 \pmod{l}$ and $l \mid m$. Under the conditions (*) on r, e and s , the binomial $P(x) = x^r(1 + x^{es})$ is a permutation binomial of \mathbb{F}_q if and only if $(2r + es, l) = 1$.*

Corollary 1.3. *Under the conditions of Theorem 1.2 on q and l , there are exactly $\frac{\phi(l)\phi(q-1)}{2}$ permutation binomials $P(x) = x^r(1 + x^{es})$ of \mathbb{F}_q . Here, ϕ is the Euler totient function.*

The structure of the paper is as follows. We start, in Section 2, by finding an explicit expression for lacunary sums of binomial coefficients. The proofs of Theorems 1.1 and 1.2 are given in Sections 3 and 5 respectively. Section 4 describes a lemma needed in the proof of Theorem 1.2. Finally at the end of the paper, as an application of our theorems, we provide several examples of permutation binomials $P(x) = x^r(1 + x^{es})$ of \mathbb{F}_q .

Note. Note that there is no permutation binomial $P(x) = x^r + x^u$ of a finite field of characteristic 2. This is true since in this case $P(0) = P(1) = 0$.

2. LACUNARY SUMS OF BINOMIAL COEFFICIENTS

In this section we evaluate the sum of the binomial coefficients $\binom{2n}{k}$ as k varies on an arithmetic progression with a common ratio l .

Let $f(z) = \sum_{k=0}^{\infty} c_k z^k$ be the generating function of the sequence $\{c_k\}_{k=0}^{\infty}$. Let $\zeta = e^{\frac{2\pi i}{l}}$. Then we have

$$(1) \quad \sum_{\substack{k=0 \\ k \equiv a \pmod{l}}}^{\infty} c_k z^k = \frac{1}{l} \sum_{t=0}^{l-1} \zeta^{at} \sum_{k=0}^{\infty} c_k \zeta^{-kt} z^k = \frac{1}{l} \sum_{t=0}^{l-1} \zeta^{at} f(\zeta^{-t} z).$$

Now let

$$c_k = \begin{cases} \binom{2n}{k}, & 0 \leq k \leq 2n; \\ 0, & \text{otherwise.} \end{cases}$$

Then $\{c_k\}$ is the sequence of the binomial coefficients with $f(z) = (1+z)^{2n}$.

Definition 2.1. $S(2n, l, a) := \sum_{\substack{k=0 \\ k \equiv a \pmod{l}}}^{2n} \binom{2n}{k}.$

Lemma 2.2. *Let l be an odd positive integer. We have*

$$S(2n, l, a) = \frac{2^{2n}}{l} + \frac{2}{l} \left[\sum_{t=1}^{\frac{l-1}{2}} \left(2 \cos \frac{\pi t}{l} \right)^{2n} \cos \frac{\pi t}{l} (2n - 2a) \right].$$

Proof. From (1) we have

$$\begin{aligned} S(2n, l, a) - \frac{2^{2n}}{l} &= \frac{1}{l} \sum_{t=1}^{l-1} \zeta^{at} (1 + \zeta^{-t})^{2n} = \frac{1}{l} \sum_{t=1}^{l-1} \zeta^{at-nt} (\zeta^{\frac{t}{2}} + \zeta^{-\frac{t}{2}})^{2n} \\ &= \frac{2}{l} \sum_{t=1}^{\frac{l-1}{2}} \left(2 \cos \frac{\pi t}{l} \right)^{2n} \cos \frac{\pi t}{l} (2n - 2a). \quad \square \end{aligned}$$

Next we find another expression for $S(2n, l, a)$. To do this, we need to review some basic facts regarding Chebyshev polynomials (see [7] for details).

We recall that the n -th order Chebyshev polynomial of the first kind is defined by

$$T_n(x) = t_0^{(n)} + t_1^{(n)}x + \dots + t_n^{(n)}x^n = \cos n\theta,$$

where n is a non-negative integer, $x = \cos \theta$, and $0 \leq \theta \leq \pi$. We have $T_n(-x) = (-1)^n T_n(x)$, $t_i^{(n)} \in \mathbb{Z}$ and $2^{n-i-1} \mid t_{n-i}^{(n)}$. Similarly, the n -th order Chebyshev polynomial of the second kind is defined by

$$U_n(x) = \frac{\sin(n+1)\theta}{\sin \theta}$$

where n is a non-negative integer, $x = \cos \theta$, and $0 \leq \theta \leq \pi$. One can show that $U_n(x)$ has exactly n zeros and the k -th zero is

$$z_k = \cos \frac{\pi k}{n+1}.$$

Now let l be an odd integer. Let

$$U_{l-1}^{\text{odd}}(x) = 2^{\frac{l-1}{2}} \prod_{\text{odd } k} (x - z_k) = 2^{\frac{l-1}{2}} \prod_{\text{odd } k} \left(x - \cos \frac{\pi k}{l}\right).$$

We define $U_{l-1}^{\text{even}}(x)$ respectively. We can show that $U_{l-1}^{\text{odd}}(x)$ and $U_{l-1}^{\text{even}}(x)$ both have integer coefficients ([6], Theorem 2). So we have the following factorization over \mathbb{Z} :

$$U_{l-1}(x) = U_{l-1}^{\text{odd}}(x) \times U_{l-1}^{\text{even}}(x).$$

Recall that for an integer $n \geq 0$,

$$a_n = \sum_{t=1}^{\frac{l-1}{2}} \left(2 \cos \frac{\pi(2t-1)}{l}\right)^n = \sum_{t=1}^{\frac{l-1}{2}} \left((-1)^{t+1} 2 \cos \frac{\pi t}{l}\right)^n.$$

From the above discussion it is clear that $\{a_n\}_{n=1}^{\infty}$ is a recursive integer sequence and the monic polynomial $U_{l-1}^{\text{odd}}(\frac{x}{2})$ is the characteristic polynomial of the recursion.

By employing the sequence $\{a_n\}$ and the coefficients $t_i^{(n)}$ of the n -th order Chebyshev polynomial of the first kind in Lemma 2.2, we have the following explicit representation for $S(2n, l, a)$.

Corollary 2.3. *Let $1 \leq j \leq \frac{l-1}{2}$ and $2n - 2a \equiv j, l - j \pmod{l}$. Then*

$$l S(2n, l, a) = 2^{2n} + (-1)^j \left(\frac{t_j^{(j)}}{2^{j-1}} a_{2n+j} + \frac{t_{j-1}^{(j)}}{2^{j-2}} a_{2n+(j-1)} + \cdots + 2t_0^{(j)} a_{2n} \right).$$

This explicit expression for $S(2n, l, a)$ plays a fundamental role in the proof of our first theorem.

3. PROOF OF THEOREM 1.1

Proof. Since l and p are odd, $P(x)$ has only one root in \mathbb{F}_q . So by Hermite's criterion, it suffices to show that for each integer t with $0 < t < q - 1$ and $t \not\equiv 0 \pmod{p}$ the reduction of $[P(x)]^t \pmod{x^q - x}$ has degree less than $q - 1$. We have

$$[P(x)]^t = x^{rt} (1 + x^{es})^t = \sum_{i=0}^t \binom{t}{i} x^{rt+ies}.$$

Note that since $(r, s) = 1$, then $rt + ies$ can be a multiple of $q - 1$ only if $s \mid t$. Let $t = cs$ for some c ($1 \leq c \leq l - 1$). Since $(e, l) = 1$, we have $e^{\phi(l)} \equiv 1 \pmod{l}$ and hence we have

$$(2) \quad [P(x)]^{cs} \pmod{x^q - x} = S(cs, l, -ce^{\phi(l)-1}r)x^{q-1} + \cdots,$$

for $c = 1, \dots, l - 1$. Therefore we need to show that $S(cs, l, -cre^{\phi(l)-1}) \equiv 0 \pmod{p}$ for all $c = 1, \dots, l - 1$. First we note that $(2r + es, l) = 1$ implies $cs + 2cre^{\phi(l)-1} \not\equiv$

0 (mod l). Let $cs + 2cre^{\phi(l)-1} \equiv j$ or $l - j$ (mod l) where $1 \leq j \leq \frac{l-1}{2}$. For these cases by applying $2^s \equiv 1$ (mod p), s -periodicity of $\{a_n\}$, Corollary 2.3, and the definition of the sequence a_n , we get

$$\begin{aligned} l S(cs, l, -cre^{\phi(l)-1}) &= 2^{cs} + (-1)^j \left(\frac{t_j^{(j)}}{2^{j-1}} a_{cs+j} + \frac{t_{j-1}^{(j)}}{2^{j-2}} a_{cs+(j-1)} + \cdots + 2t_0^{(j)} a_{cs} \right) \\ &\equiv 1 + (-1)^j \left(\frac{t_j^{(j)}}{2^{j-1}} a_j + \frac{t_{j-1}^{(j)}}{2^{j-2}} a_{j-1} + \cdots + 2t_0^{(j)} a_0 \right) \pmod{p} \\ &= 1 + (-1)^j 2 \left(\sum_{t=1}^{\frac{l-1}{2}} T_j \left((-1)^{t+1} \cos \frac{\pi t}{l} \right) \right) \\ &= 1 + (-1)^j \sum_{t=1}^{l-1} T_j \left((-1)^{t+1} \cos \frac{\pi t}{l} \right) \\ &= \begin{cases} 1 - \sum_{t=1}^{l-1} (-1)^{t+1} \cos \frac{\pi t j}{l} = 0 & \text{if } j \text{ is odd;} \\ 1 + \sum_{t=1}^{l-1} \cos \frac{\pi t j}{l} = 0 & \text{if } j \text{ is even.} \end{cases} \end{aligned}$$

So $l S(cs, l, -cre^{\phi(l)-1}) \equiv 0$ (mod p). Since $l \mid (q - 1)$, we have $(p, l) = 1$ and thus $S(cs, l, -cre^{\phi(l)-1}) \equiv 0$ (mod p). This shows that $[P(x)]^{cs}$ (mod $x^q - x$) has degree less than $q - 1$. The proof is complete. \square

4. LEMMA

We need the following lemma in the proof of Theorem 1.2.

Lemma 4.1. *Let l be odd. Let p be an odd prime, let $q = p^m$, let $s = \frac{q-1}{l}$ and let α be any nonzero element of \mathbb{F}_p . Then*

- (i) *if $p \equiv -1$ (mod l), we have $\alpha^s = 1$ in \mathbb{F}_p ;*
- (ii) *if $p \equiv 1$ (mod l) and $l \mid m$, we have $\alpha^s = 1$ in \mathbb{F}_p .*

Proof. (i) Let $d = (p - 1, l)$. Since $d = 1$ and $\alpha^{\frac{p-1}{d}} = \alpha^{p-1} = 1$ in \mathbb{F}_p , so α is the l -th power of an element β of \mathbb{F}_p ([5], Exercise 2.14), i.e. $\alpha = \beta^l$. Thus $\alpha^s = (\beta^l)^s = \beta^{q-1} = 1$ in \mathbb{F}_p .

(ii) If α is an l -th power in \mathbb{F}_p , then $\alpha^{\frac{p-1}{l}} = 1$ in \mathbb{F}_p and therefore $\alpha^s = 1$ in \mathbb{F}_p . If α is not an l -th power in \mathbb{F}_p , then the equation $x^l = \alpha$ has no solution in \mathbb{F}_p . Since $l \mid m$, this equation has a solution in \mathbb{F}_q ([5], Exercise 2.16). So there is a $\beta \in \mathbb{F}_q$ such that $\alpha = \beta^l$. We have

$$\alpha^{\frac{q-1}{l}} = \beta^{q-1} = 1$$

in \mathbb{F}_q . \square

We are now ready to prove the main result of this paper.

5. PROOF OF THEOREM 1.2

First of all we show that if $P(x) = x^r(1 + x^{es})$ is a permutation binomial, then $(2r + es, l) = 1$. Suppose that $(2r + es, l) = d$ with $d > 1$. Let $k = \frac{l}{d}$. Then $k < l$ and $2kr + eks \equiv 0 \pmod{l}$. So by Lemma 2.2, we have

$$S(cks, l, -ce^{\phi(l)-1}kr) = \frac{2^{cks} + 2a_{cks}}{l}, \text{ in } \mathbb{F}_p$$

for $c = 1, \dots, l-1$. Next we consider $U_{l-1}^{\text{odd}}(\frac{x}{2})$, the characteristic polynomial of a_n . Under given conditions for p , by Theorem 7 of [6] we know that $U_{l-1}^{\text{odd}}(\frac{x}{2})$ splits in $\mathbb{F}_p[x]$. Let γ_j ($1 \leq j \leq \frac{l-1}{2}$) be roots of $U_{l-1}^{\text{odd}}(\frac{x}{2})$ in \mathbb{F}_p . Then Lemma 4.1 implies that $\gamma_j^{ks} = 0$ or 1 for $j = 1, \dots, \frac{l-1}{2}$. Since l is odd, $\gamma_j^{ks} \neq 0$, so $\gamma_j^{ks} = 1$ for $j = 1, \dots, \frac{l-1}{2}$.

$$(3) \quad a_{ks} = \frac{l-1}{2}.$$

On the other hand, since $P(x)$ is a permutation binomial $S(ks, l, -e^{\phi(l)-1}kr) = \frac{2^{ks} + 2a_{ks}}{l} = 0$ in \mathbb{F}_p , which implies that $a_{ks} = -\frac{1}{2}$. This together with (3) yield $l = 0$ in \mathbb{F}_p . This is a contradiction since $l \mid p^m - 1$. So $(2r + es, l) = 1$.

Conversely, we assume that $(2r + es, l) = 1$. By Lemma 4.1, we have $2^s \equiv 1 \pmod{p}$. Let the γ_j 's be as above. Since the γ_j 's are in \mathbb{F}_p , by Lemma 4.1, we have $\gamma_j^s \equiv 1 \pmod{p}$ for $j = 1, \dots, \frac{l-1}{2}$. From this together with Theorem 8.13 of [5] it follows that $\{a_n\}$ is s -periodic. Now Theorem 1.1 implies that the given condition is also sufficient. \square

Proof of Corollary 1.3. For fixed e with $0 < e \leq l-1$ and $(e, l) = 1$, we count the number of r 's between 0 and $q-1$ such that $(r, s) = 1$ and $(2r + es, l) = 1$. This number is equal to the number of odd r 's between 0 and $q-1$ such that $(r + e\frac{s}{2}, \frac{q-1}{2}) = 1$; we denote this number by $N(e)$. We claim that $N(e) = \phi(q-1)$. To prove this assertion we consider two cases:

Case 1: $\frac{q-1}{2}$ is odd. In this case $\{r + e\frac{s}{2} \mid r \text{ odd}, 0 < r < q-1\}$ forms a complete set of residues mod $\frac{q-1}{2}$ and therefore

$$N(e) = \phi\left(\frac{q-1}{2}\right) = \phi(q-1).$$

Case 2: $\frac{q-1}{2}$ is even. In this case $\{r + e\frac{s}{2} \mid 0 < r \leq \frac{q-1}{2}\}$ forms a complete set of residues mod $\frac{q-1}{2}$ and therefore

$$N(e) = 2\phi\left(\frac{q-1}{2}\right) = \phi(q-1).$$

Note that in this case for even r we have $(r + e\frac{s}{2}, \frac{q-1}{2}) \neq 1$.

Now since $0 < e \leq l-1$ and $(e, l) = 1$, the total number of such permutation polynomials is $\phi(l)\phi(q-1)$. However the permutation polynomial corresponding to $e = e_1$ and $r = r_1$ is the same as the permutation polynomial corresponding to $e = l - e_1$ and $r = r_1 + e_1s$. So the total number of such permutation polynomials is $\frac{\phi(l)\phi(q-1)}{2}$. \square

6. EXAMPLES

In the following tables, as an application of Theorem 1.2, we give some examples of permutation binomials of \mathbb{F}_q . Here N is the corresponding number of permutation binomials of \mathbb{F}_q .

TABLE 1. $q = p^2$ and $p \equiv -1 \pmod{l}$

l	3	5	7	9	11	13	17	...
p	5	19	13	17	43	103	67	...
q	25	361	169	289	1849	10609	4489	...
N	8	192	144	288	2400	18432	10240	...
$P(x)$	$x^9 + x$ $x^{11} + x^3$ $x^{19} + x^3$ $x^{21} + x^5$ $x^{15} + x^7$ $x^{17} + x^9$ $x^{21} + x^{13}$ $x^{23} + x^{15}$...	$x^{73} + x$ $x^{145} + x$ $x^{77} + x^5$ $x^{293} + x^5$ $x^{79} + x^7$ $x^{83} + x^{11}$ $x^{85} + x^{13}$ $x^{89} + x^{17}$...	$x^{25} + x$ $x^{49} + x^5$ $x^{29} + x^5$ $x^{151} + x^7$ $x^{31} + x^7$ $x^{35} + x^{11}$ $x^{37} + x^{13}$ $x^{41} + x^{17}$...	$x^{33} + x$ $x^{129} + x$ $x^{35} + x^3$ $x^{67} + x^3$ $x^{131} + x^3$ $x^{69} + x^5$ $x^{39} + x^7$ $x^{41} + x^9$...	$x^{169} + x$ $x^{337} + x$ $x^{173} + x^5$ $x^{509} + x^5$ $x^{179} + x^{11}$ $x^{181} + x^{13}$ $x^{185} + x^{17}$ $x^{187} + x^{19}$...	$x^{817} + x$ $x^{1633} + x$ $x^{173} + x^5$ $x^{823} + x^7$ $x^{827} + x^{11}$ $x^{829} + x^{13}$ $x^{2461} + x^{13}$ $x^{835} + x^{19}$...	$x^{265} + x$ $x^{529} + x$ $x^{269} + x^5$ $x^{3437} + x^5$ $x^{271} + x^7$ $x^{277} + x^{13}$ $x^{281} + x^{17}$ $x^{283} + x^{19}$

TABLE 2. $q = p^4$ and $p \equiv -1 \pmod{l}$

l	3	5	7	9	11	13	...
p	5	19	13	17	43	103	...
q	625	130321	28561	83521	3418801	112550881	...
N	192	69120	18432	64512	3456000	156303360	...
$P(x)$	$x^{417} + x$ $x^{211} + x^3$ $x^{419} + x^3$ $x^{213} + x^5$ $x^{423} + x^7$ $x^{217} + x^9$ $x^{425} + x^9$ $x^{219} + x^{11}$...	$x^{26065} + x$ $x^{78193} + x$ $x^{104257} + x$ $x^{26069} + x^5$ $x^{52133} + x^5$ $x^{78197} + x^5$ $x^{104261} + x^5$ $x^{20671} + x^7$...	$x^{4081} + x$ $x^{12241} + x$ $x^{4087} + x^7$ $x^{8167} + x^7$ $x^{8171} + x^{11}$ $x^{12251} + x^{11}$ $x^{4093} + x^{13}$ $x^{8173} + x^{13}$...	$x^{18561} + x$ $x^{46401} + x$ $x^{9283} + x^3$ $x^{18563} + x^3$ $x^{18567} + x^7$ $x^{46407} + x^7$ $x^{9289} + x^9$ $x^{18569} + x^9$...	$x^{310801} + x$ $x^{621601} + x$ $x^{310811} + x^{11}$ $x^{621611} + x^{11}$ $x^{310813} + x^{13}$ $x^{310817} + x^{17}$ $x^{621617} + x^{17}$ $x^{932417} + x^{17}$...	$x^{8657761} + x$ $x^{17315521} + x$ $x^{8657767} + x^7$ $x^{17315527} + x^7$ $x^{8657771} + x^{11}$ $x^{17315531} + x^{11}$ $x^{8657773} + x^{13}$ $x^{34631059} + x^{19}$

TABLE 3. $q = p^l$ and $p \equiv 1 \pmod{l}$

l	3	5	7	9	11	...
p	7	11	29	19	23	...
q	343	161051	17249876309	322687697779	952809757913927	...
N	108	128800	22178412144	319524059232	2165476722531100	...
$P(x)$	$x^{115} + x$ $x^{229} + x$ $x^{119} + x^5$ $x^{233} + x^5$ $x^{121} + x^7$ $x^{235} + x^7$ $x^{125} + x^{11}$ $x^{239} + x^{11}$...	$x^{32211} + x$ $x^{64421} + x$ $x^{32213} + x^3$ $x^{64423} + x^3$ $x^{32217} + x^7$ $x^{64427} + x^7$ $x^{32219} + x^9$ $x^{64429} + x^9$...	$x^{2464268045} + x$ $x^{4928536089} + x$ $x^{2464268047} + x^3$ $x^{4928536091} + x^3$ $x^{2464268049} + x^5$ $x^{4928536093} + x^5$ $x^{2464268053} + x^9$ $x^{4928536097} + x^9$...	$x^{35854188643} + x$ $x^{71708377285} + x$ $x^{35854188647} + x^5$ $x^{71708377289} + x^5$ $x^{35854188649} + x^7$ $x^{71708377291} + x^7$ $x^{35854188653} + x^{11}$ $x^{71708377295} + x^{11}$...	$x^{86619068901267} + x$ $x^{173238137802533} + x$ $x^{86619068901269} + x^3$ $x^{173238137802535} + x^3$ $x^{86619068901271} + x^5$ $x^{173238137802537} + x^5$ $x^{86619068901273} + x^7$ $x^{173238137802539} + x^7$

ACKNOWLEDGMENT

The authors would like to thank the referee for helpful comments and suggestions.

REFERENCES

- [1] L. E. Dickson, The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, *Ann. of Math.* **11** (1897), 65–120, 161–183. MR1502221
- [2] M. D. Fried, R. Guralnick, J. Saxl, Schur covers and Carlitz’s conjecture, *Israel J. Math.* **82** (1993), no. 1-3, 157-225. MR1239049 (94j:12007)
- [3] D. R. Hayes, A geometric approach to permutation polynomials over a finite field, *Duke Math. J.*, **34** (1967), 293–305. MR0209266 (35:168)
- [4] C. Hermite, Sur les fonctions de sept lettres, *C. R. Acad. Sci. Paris* **57** (1863), 750-757; *Oeuvres*, vol. 2, pp. 280-288, Gauthier-Villars, Paris, 1908.
- [5] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997. MR1429394 (97i:11115)
- [6] M. O. Rayes, V. Trevisan and P. Wang, Factorization of Chebyshev polynomials, <http://icm.mcs.kent.edu/reports/index1998.html>.
- [7] T. J. Rivlin, *The Chebyshev Polynomials*, Wiley-Interscience, New York, 1974. MR0450850 (56:9142)
- [8] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, Published electronically at <http://www.research.att.com/~njas/sequences/>.
- [9] D. Wan, R. Lidl, Permutation polynomials of the form $x^r f(x^{(q-1)/d})$ and their group structure, *Monatsh. Math.* **112** (1991), 149–163. MR1126814 (92g:11119)

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE, 4401 UNIVERSITY DRIVE WEST, LETHBRIDGE, ALBERTA, CANADA T1K 3M4
E-mail address: akbary@cs.uleth.ca

SCHOOL OF MATHEMATICS AND STATISTICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, CANADA K1S 5B6
E-mail address: wang@math.carleton.ca