NUMBER OF POINTS OF
CERTAIN ARITIN–SCHREIER CURVES

JĘDRZEJ GARNEK

Abstract. We prove a conjecture of Johansen, Helleseth and Kholosha concerning equality of exponential sums related to the cross-correlation of \(m\)-sequences. In the proof we show that certain Artin–Schreier curves have the same number of points over finite fields. This has a consequence regarding the \(L\)-polynomials of these curves.

1. Introduction

For any positive integers \(k\) and \(m\) consider the following exponential sum:

\[
G^{(k)}_m := \sum_{x \in \mathbb{F}_2^m} (-1)^{\text{tr}_{\mathbb{F}_2^m/\mathbb{F}_2}(x^{2^k+1}+x^{-1})}.
\]

The following conjecture was stated in [1].

Conjecture 1.1. \(G^{(k)}_m = G^{\text{GCD}(k,m)}_m\).

As shown in the article [1], Conjecture 1.1 is equivalent to the following statement.

Conjecture 1.2. For any positive integer \(k\) consider the smooth projective curve \(E_k\) over \(\mathbb{F}_2\) with the function field given by the equation:

\[
y^2 + y = x^{2k+1} + x^{-1}.
\]

Then:

\[
\#E_k(\mathbb{F}_{2^m}) = \#E^{\text{GCD}(k,m)}(\mathbb{F}_{2^m}).
\]

The goal of this paper is to prove Conjecture 1.2. Actually, we prove a more general criterion.

Theorem 1.3. Let \(p\) be an arbitrary prime. For any \(a, b \in \mathbb{Z}\), \((a, b) \neq (0, 0)\) consider the smooth projective curve \(C_{a,b}\) over \(\mathbb{F}_p\) with the function field given by the equation:

\[
y^p - y = x^a + x^b.
\]

If the following conditions hold:

\[
2020 \text{ Mathematics Subject Classification. Primary 11G20, Secondary 11T06.}
\]
(1) \( \text{GCD}(a_1, p^m - 1) = \text{GCD}(a_2, p^m - 1) \),
(2) \( \text{GCD}(b_1, p^m - 1) = \text{GCD}(b_2, p^m - 1) \),
(3) \( a_1, a_2 > 0, b_1 \cdot b_2 > 0 \) and \( p \nmid a_1, a_2, b_1, b_2 \),
then
\[
\#C_{a_1, b_1}(\mathbb{F}_{p^m}) = \#C_{a_2, b_2}(\mathbb{F}_{p^m}).
\]

The main idea behind Theorem 1.3 is to use the equality \( x^{p^m-1} = 1 \) valid for all \( x \in \mathbb{F}_p^\times \).

Using a simple number-theoretic result we derive from Theorem 1.3 the following corollary.

**Corollary 1.4.** Conjecture 1.2 is true.

By [1, Theorem 21] one obtains immediately a corollary regarding the L-polynomials of the studied family.

**Corollary 1.5.** Denote by \( L_{E_k}(t) \in \mathbb{Z}[t] \) the L-polynomial of \( E_k \). Then:
\[
L_{E_k}(t) = q_1(t^{p^1}) \cdots \cdot q_r(t^{p^r}) \cdot L_{E_1}(t),
\]
where \( k = \prod_{i=1}^{r} p^{\alpha_i} \) is the decomposition into prime powers and \( q_1, \ldots, q_r \in \mathbb{Z}[t] \) are certain polynomials.

Our method applies also to the family considered in the articles [3] and [5].

**Corollary 1.6.** Let \( p \) be an arbitrary prime. For any positive integer \( k \) consider the smooth projective curve \( C_k \) over \( \mathbb{F}_p \) with the function field given by the equation:
\[
y^p - y = x^{p^k+1} + x.
\]
Then for any \( k, m \in \mathbb{Z}_+ \):
\[
\#C_k(\mathbb{F}_{p^m}) = \#C_{\text{GCD}(k, m)}(\mathbb{F}_{p^m}).
\]

**Outline of the paper.** We prove Theorem 1.3 in Section 2. Section 3 contains the proofs of Corollaries 1.4 and 1.6.

**Acknowledgements.** The author wishes to thank Wojciech Gajda for many helpful conversations. The author also thanks Bartosz Naskręki for valuable comments regarding the first version of the manuscript.

2. **Proof of Theorem 1.3**

In this section we prove Theorem 1.3. Before the proof we need the following simple lemma. We give its proof for a lack of reference.

**Lemma 2.1.** The congruence
\[
a \cdot z \equiv b \pmod{n}
\]
has a solution \( z \in (\mathbb{Z}/n)^\times \) if and only if \( \text{GCD}(a, n) = \text{GCD}(b, n) \).
Proof. If the congruence (2.1) has a solution \( z \in \mathbb{Z}/n^\times \) then it is clear that \( \gcd(a, n) \mid b \) and \( \gcd(b, n) \mid a \). This easily implies that \( \gcd(a, n) = \gcd(b, n) \).

Assume now that \( \gcd(a, n) = \gcd(b, n) =: D \) and define the integers \( a', b', n' \) by the equations:

\[
a = D \cdot a', \quad b = D \cdot b', \quad n = D \cdot n'.
\]

Note that by assumption \( \gcd(a', n') = \gcd(b', n') = 1 \). Thus the congruence \( a' \cdot z \equiv b' \pmod{n'} \) has a solution \( z_0 \). One easily checks that \( \gcd(z_0, n') = 1 \). Using Chinese Remainder Theorem we may choose \( t \in \mathbb{Z} \) such that for every \( p \mid n \):

\[
t \equiv \begin{cases} 
1 \pmod{p}, & \text{if } p \mid z_0, \\
0 \pmod{p}, & \text{if } p \nmid z_0.
\end{cases}
\]

Then one may take \( z := z_0 + t \cdot n' \). Indeed, \( z \in \mathbb{Z}/n^\times \), since for every prime \( p \mid n \) one of the following cases holds:

- \( 1^\circ \) \( p \mid z_0 \). Then \( p \nmid n' \) and thus \( z \equiv z_0 + n' \not\equiv 0 \pmod{p} \).
- \( 2^\circ \) \( p \nmid z_0 \). Then \( z \equiv z_0 \not\equiv 0 \pmod{p} \).

It is immediate that \( z \) satisfies (2.1). \( \square \)

We prove now Theorem 1.3. Let \( X \) be an Artin–Schreier curve over \( \mathbb{F}_{p^m} \) with the function field given by the equation \( y^p - y = f(x) \). Consider the canonical \( \mathbb{Z}/p \)-cover \( \pi : X \to \mathbb{P}^1 \), \( \pi(x, y) = x \). Then for every \( P \in \mathbb{P}^1(\overline{\mathbb{F}_p}) \):

\[
\#\pi^{-1}(P) = \begin{cases} 
p, & \text{if } P \text{ is not a pole of } f, \\
1, & \text{if } P \text{ is a pole of } f \text{ and } p \nmid v_P(f).
\end{cases}
\]

(see e.g. [6, sec. 2.2]). Moreover, if \( P \) is a pole of \( f \) and \( p \nmid v_P(f) \) then \( \pi^{-1}(P) \subset X(\mathbb{F}_{p^m}) \) by the ’efg theorem’ (cf. [7, Proposition 4.1.6]). Therefore the condition (3) of Theorem 1.3 assures that the curves \( C_{a_1,b_1}, C_{a_2,b_2} \) have the same number of points at infinity and both contain or both do not contain the point \((0,0)\). Hence we may count only points \((x,y)\) with \( x \in \mathbb{F}_{p^m}^\times \).

Note that for any \( x \in \mathbb{F}_{p^m}^\times \) one has \( x^{p^m-1} = 1 \). Therefore, if

\[
a_1 \equiv a_2 \pmod{p^m - 1}
\]

then \( x^{a_1} = x^{a_2} \) and

\[
\#C_{a_1,b}(\mathbb{F}_{p^m}) = \#C_{a_2,b}(\mathbb{F}_{p^m}). \quad (2.2)
\]
Observe that \((x, y) \mapsto (x, y + x^a)\) provides an isomorphism between \(\mathcal{C}_{p,a,b}\) and \(\mathcal{C}_{a,b}\). Thus:

\[(2.3) \quad \#\mathcal{C}_{a,b}(\mathbb{F}_{p^m}) = \#\mathcal{C}_{p,a,b}(\mathbb{F}_{p^m})\]

Assume finally that \(\gcd(a_1, p^m - 1) = \gcd(a_2, p^m - 1)\) and \(a_1 \cdot a_2 > 0\). Then by Lemma 2.1

\[a_1 \equiv a_2 \cdot z \pmod{p^m - 1}\]

for some \(z \in (\mathbb{Z}/(p^m - 1))^\times\). Note that \((\mathbb{Z}/(p^m - 1))^\times = \langle p \rangle\), since for \(0 < s < m\) one has \(p^m - 1 \nmid p^s - 1\). Hence

\[z \equiv p^t \pmod{p^m - 1}\]

for some \(t \in \mathbb{N}\). By (2.2) and (2.3) it follows that:

\[\#\mathcal{C}_{a_1,b}(\mathbb{F}_{p^m}) = \#\mathcal{C}_{a_2,b}(\mathbb{F}_{p^m}).\]

Similarly, if \(\gcd(b_1, n) = \gcd(b_2, n)\) and \(b_1 \cdot b_2 > 0\) then

\[\#\mathcal{C}_{a,b_1}(\mathbb{F}_{p^m}) = \#\mathcal{C}_{a,b_2}(\mathbb{F}_{p^m}).\]

This ends the proof of Theorem 1.3.

### 3. Proof of Corollaries 1.2 and 1.6

In this section we will denote \((a, b) := \gcd(a, b)\) for brevity.

**Lemma 3.1.** Let \(p\) be a prime and \(k, m \in \mathbb{N}\). Then:

\[(p^k + 1, p^m - 1) = \begin{cases} 
\frac{p^{(2k,m)} - 1}{p^{(k,m)} - 1}, & \text{if } v_2(k) < v_2(m), \\
1, & \text{otherwise},
\end{cases}\]

where \(v_2(k)\) denotes the 2-adic valuation of \(k\).

**Proof.** Let \(\Phi_n\) denote the \(n\)-th cyclotomic polynomial. Recall that if \(d_1/d_2\) is not a power of a prime then the resultant of \(\Phi_{d_1}(x)\) and \(\Phi_{d_2}(x)\) is 1, see e.g. [2]. Therefore, for some \(A, B \in \mathbb{Z}[x]\):

\[A(x) \cdot \Phi_{d_1}(x) + B(x) \cdot \Phi_{d_2}(x) = 1,
\]

which implies that:

\[(3.1) \quad (\Phi_{d_1}(p), \Phi_{d_2}(p)) = 1.
\]
Therefore:

\[
(p^k + 1, p^m - 1) = \left( \frac{p^{2k} - 1}{p^k - 1}, p^m - 1 \right)
\]

\[
= \left( \prod_{d_1 | 2k} \Phi_{d_1}(p), \prod_{d_2 | m} \Phi_{d_2}(p) \right)
\]

\[
= \prod_{d | (2k, m), d | (k, m)} \Phi_d(p) \cdot \left( \prod_{d_1 | 2k} \Phi_{d_1}(p), \prod_{d_2 | m, d_2 | k} \Phi_{d_2}(p) \right)
\]

\[
= \frac{p^{(2k, m)} - 1}{p^{(k, m)} - 1} \cdot \left( \prod_{d_1 | 2k} \Phi_{d_1}(p), \prod_{d_2 | m, d_2 | k} \Phi_{d_2}(p) \right)
\]

\[
= \frac{p^{(2k, m)} - 1}{p^{(k, m)} - 1}.
\]

(the last equality is a consequence of (3.1)). The proof follows. \(\square\)

Let \(k, m \in \mathbb{N}, d := (k, m)\). Using Lemma 3.1 we can easily check that for curves \(E_k\) and \(E_d\) and the assumption of Theorem 1.3 is satisfied. Indeed, observe that \(v_2(d) = \min\{v_2(k), v_2(m)\}\) and therefore

\[v_2(d) < v_2(k)\] if and only if \(v_2(k) < v_2(m)\).

Hence:

\[
(p^k + 1, p^m - 1) = \begin{cases} 
  p^d + 1, & \text{if } v_2(k) < v_2(m) \\
  1, & \text{otherwise}
\end{cases}
\]

\[
= \begin{cases} 
  p^d + 1, & \text{if } v_2(d) < v_2(m) \\
  1, & \text{otherwise}
\end{cases}
\]

\[
= (p^d + 1, p^m - 1).
\]

This proves Corollaries 1.4 and 1.6.

References

[1] O. Ahmadi, G. McGuire, and A. Rojas-León. Decomposing Jacobians of curves over finite fields in the absence of algebraic structure. J. Number Theory, 156:414–431, 2015.

[2] T. M. Apostol. Resultants of cyclotomic polynomials. Proc. Amer. Math. Soc., 24:457–462, 1970.

[3] I. Blanco-Chacón, R. Chapman, S. Fordham, and G. McGuire. Divisibility of L-polynomials for a family of curves. In Contemporary developments in finite fields and applications, pages 1–10. World Sci. Publ., Hackensack, NJ, 2016.
[4] A. Johansen, T. Helleseth, and A. Kholosha. Further results on $m$-sequences with five-valued cross correlation. *IEEE Trans. Inform. Theory*, 55(12):5792–5802, 2009.

[5] G. McGuire and E. S. Yılmaz. Divisibility of L-polynomials for a family of Artin-Schreier curves. *J. Pure Appl. Algebra*, 223(8):3341–3358, 2019.

[6] R. Pries and H. J. Zhu. The $p$-rank stratification of Artin-Schreier curves. *Ann. Inst. Fourier (Grenoble)*, 62(2):707–726, 2012.

[7] T. Szamuely. *Galois groups and fundamental groups*, volume 117 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 2009.

**Address**

Adam Mickiewicz University, Faculty of Mathematics and Computer Science, ul. Uniwersytetu Poznańskiego 4, 61-614 Poznań, Poland

*Email address: jgarnek@amu.edu.pl*