Bull. Aust. Math. Soc. (First published online 2026), page 1 of 7*
doi:10.1017/S0004972726101853
*Provisional—final page numbers to be inserted when paper edition is published

AN EXACT ROOT COUNT IN A PROBLEM ON OPTIMAL TERNARY CYCLIC CODES

FRANCISCO-JAVIER SOTO

(Received 20 May 2026 UTC; accepted 17 July 2026 UTC)

Abstract

Let $q = 3^m$ with m odd and let $s \geq 1$. We determine exactly the number of roots in $\mathbb{F}_q$ of $x^{3^s+1} - x^2 + 1 = 0$. This equation appears in the study of open problems of Ding and Helleseth ['Optimal ternary cyclic codes from monomials', *IEEE Trans. Inform. Theory* **59**(9) (2013), 5898–5904]. A Cayley transform sends the equation to the norm-one subgroup of $\mathbb{F}_{q^2}^{\times}$, where the question becomes a calculation in a cyclic group. We prove that $\#\{x \in \mathbb{F}_q : x^{3^s+1} - x^2 + 1 = 0\} = \gcd(3^m + 1, 3^s + 2(-1)^s) - 1$. Consequently, the corresponding no-root condition is equivalent to $\gcd(3^m + 1, 3^s + 2(-1)^s) = 1$. As an application, we settle in the negative a conjectural no-root statement from the cyclic-code literature, by giving infinitely many pairs (m, s) satisfying the proposed hypotheses for which the equation has roots.

2020 *Mathematics subject classification*: primary 11T06; secondary 94B15.

Keywords and phrases: finite fields, ternary cyclic codes, Cayley transform, norm-one subgroup, root count.

1. Introduction

Let $q = 3^m$ with $m \geq 1$ odd and let $s \geq 1$. We study the equation

$$x^{3^s+1} - x^2 + 1 = 0 \tag{1.1}$$

over $\mathbb{F}_q$.

The motivation comes from the theory of optimal ternary cyclic codes. Ding and Helleseth [1] formulated several open problems concerning ternary cyclic codes with minimum distance four. In this line of work, one often has to check that certain explicit equations over finite fields have no solutions. This idea has been used in, for example, [2, 4–7].

The author acknowledges support from the 'PREDOCT2022-006' program at Universidad Rey Juan Carlos. In addition, he was partially supported by the grant PID2023-151238OA-I00, financed by MICIU/AEI/10.13039/501100011033 and by EU, ERDF.

© The Author(s), 2026. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (https://creativecommons.org/licenses/by/4.0/), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

https://doi.org/10.1017/S0004972726101853 Published online by Cambridge University Press

In particular, Zhao *et al.* [7] reduce one part of their analysis to the solvability of (1.1) (see [7, Proposition 9 and Theorem 5]). In their conclusion, they formulate the following conjectural no-root statement:

$$\text{if } m \text{ is odd, } \gcd(m,3)=1 \text{ and } \gcd(m,s)=1, \text{ then (1.1) has no solution in } \mathbb{F}_{3^m}.$$

Thus, (1.1) is a concrete finite-field question arising from the cyclic-code problem.

The purpose of this note is to determine the root count exactly. We prove that the number of roots of (1.1) in $\mathbb{F}_{3^m}$ is

$$\gcd(3^m+1,\ 3^s+2(-1)^s)-1.$$

This gives a simple greatest-common-divisor test for the no-root condition. In particular, the hypotheses $\gcd(m,3)=1$ and $\gcd(m,s)=1$ do not decide the question. We also give an infinite family of pairs (m,s) satisfying these two hypotheses for which (1.1) has many roots. In this sense, the conjectural statement quoted above is settled in the negative.

The proof uses a Cayley transform. Since m is odd, -1 is not a square in $\mathbb{F}_q$. Choosing $\beta \in \mathbb{F}_{q^2}$ with $\beta^2=-1$, the map

$$x \longmapsto \frac{x-\beta}{x+\beta}$$

identifies $\mathbb{F}_q$ with the norm-one subgroup of $\mathbb{F}_{q^2}^{\times}$ after removing one point. Under this change of variable, (1.1) becomes a power equation in a cyclic group.

The main result is as follows.

THEOREM 1.1. *Let $q=3^m$ with $m\geq 1$ odd and let $s\geq 1$. Denote by $N_{m,s}$ the number of roots of (1.1) in $\mathbb{F}_q$. Then,*

$$N_{m,s}=\gcd(q+1,\ 3^s+2(-1)^s)-1.$$

Equivalently,

$$N_{m,s}=\begin{cases}\gcd(q+1,3^s-2)-1 & \text{if } s \text{ is odd},\\ \gcd(q+1,3^s+2)-1 & \text{if } s \text{ is even}.\end{cases}$$

In particular, (1.1) has a root in $\mathbb{F}_q$ if and only if $\gcd(q+1,\ 3^s+2(-1)^s)>1$.

2. The Cayley transform

Throughout this section, let $q=3^m$ with $m\geq 1$ odd. Since $q\equiv 3 \pmod 4$, the polynomial T^2+1 is irreducible over $\mathbb{F}_q$. Choose $\beta\in\mathbb{F}_{q^2}$ such that

$$\beta^2=-1.$$

Then, $\beta\notin\mathbb{F}_q$ and the Frobenius automorphism satisfies

$$\beta^q=-\beta.$$

https://doi.org/10.1017/S0004972726101853 Published online by Cambridge University Press

Let

$$\mu_{q+1} = \{u \in \mathbb{F}_{q^2}^{\times} : u^{q+1} = 1\}$$

be the norm-one subgroup of $\mathbb{F}_{q^2}^{\times}$. This group is cyclic of order $q+1$ [3, Ch. 2].

PROPOSITION 2.1. *The map*

$$\phi\colon \mathbb{F}_q \to \mu_{q+1} \setminus \{1\}, \quad \phi(x) = \frac{x-\beta}{x+\beta},$$

is a bijection. Its inverse is

$$\phi^{-1}(u) = \beta\,\frac{1+u}{1-u}.$$

PROOF. Let $x \in \mathbb{F}_q$. Since $\beta \notin \mathbb{F}_q$, the denominator $x+\beta$ is nonzero. Moreover,

$$\phi(x)^q = \left(\frac{x-\beta}{x+\beta}\right)^q = \frac{x+\beta}{x-\beta} = \phi(x)^{-1}.$$

Hence, $\phi(x)^{q+1} = 1$, so $\phi(x) \in \mu_{q+1}$. In addition, $\phi(x) = 1$ would imply $\beta = 0$, which is impossible. Therefore,

$$\phi(x) \in \mu_{q+1} \setminus \{1\}.$$

Conversely, let $u \in \mu_{q+1} \setminus \{1\}$. Since $u^q = u^{-1}$ and $\beta^q = -\beta$,

$$\left(\beta\,\frac{1+u}{1-u}\right)^q = -\beta\,\frac{1+u^{-1}}{1-u^{-1}} = \beta\,\frac{1+u}{1-u}.$$

Thus, $\phi^{-1}(u) \in \mathbb{F}_q$. A direct computation gives

$$\phi(\phi^{-1}(u)) = u \quad \text{and} \quad \phi^{-1}(\phi(x)) = x.$$

This proves the proposition. □

3. The root count

The next proposition is the key step.

PROPOSITION 3.1. *Let $q = 3^m$ with $m \geq 1$ odd, let $s \geq 1$ and let $x \in \mathbb{F}_q^{\times}$. Put*

$$u = \phi(x) = \frac{x-\beta}{x+\beta}.$$

Then, (1.1) is equivalent to

$$u^{3^s+2(-1)^s} = 1.$$

Equivalently,

$$\begin{cases} u^{3^s} = u^2 & \text{if } s \text{ is odd,} \\ u^{3^s} = u^{-2} & \text{if } s \text{ is even.} \end{cases}$$

https://doi.org/10.1017/S0004972726101853 Published online by Cambridge University Press

PROOF. Since $x \neq 0$, (1.1) is equivalent to

$$x^{3^s} = x - x^{-1}. \tag{3.1}$$

By Proposition 2.1,

$$x = \beta \frac{1+u}{1-u}.$$

Since $\phi(0) = -1$, the condition $x \neq 0$ implies $u \neq -1$. We also have $u \neq 1$. Hence, $1 - u^2 \neq 0$.

Now,

$$x^{-1} = -\beta \frac{1-u}{1+u}$$

and, therefore,

$$x - x^{-1} = \beta\left(\frac{1+u}{1-u} + \frac{1-u}{1+u}\right) = \beta \frac{(1+u)^2 + (1-u)^2}{1-u^2}.$$

In characteristic 3, we have $2 = -1$ and so

$$(1+u)^2 + (1-u)^2 = 2(1+u^2) = -(1+u^2).$$

Thus,

$$x - x^{-1} = -\beta \frac{1+u^2}{1-u^2}. \tag{3.2}$$

Since $\beta^3 = -\beta$, iteration gives

$$\beta^{3^s} = (-1)^s \beta.$$

Hence,

$$x^{3^s} = \beta^{3^s} \frac{1+u^{3^s}}{1-u^{3^s}} = (-1)^s \beta \frac{1+u^{3^s}}{1-u^{3^s}}. \tag{3.3}$$

The denominator in (3.3) is nonzero. Indeed, if $u^{3^s} = 1$, then the order of u divides both 3^s and $q+1$. Since $\gcd(3^s, q+1) = 1$, this forces $u = 1$, contrary to $u \in \mu_{q+1} \setminus \{1\}$.

Substituting (3.2) and (3.3) into (3.1) yields

$$(-1)^s \beta \frac{1+u^{3^s}}{1-u^{3^s}} = -\beta \frac{1+u^2}{1-u^2}.$$

All denominators in the preceding identity are nonzero, so the following cross-multiplications are reversible.

If s is odd, the previous equation becomes

$$\frac{1+u^{3^s}}{1-u^{3^s}} = \frac{1+u^2}{1-u^2},$$

and cross-multiplication yields $u^{3^s} = u^2$.

https://doi.org/10.1017/S0004972726101853 Published online by Cambridge University Press

If s is even, it becomes

$$\frac{1+u^{3^s}}{1-u^{3^s}} = -\frac{1+u^2}{1-u^2}.$$

Cross-multiplication gives

$$(1+u^{3^s})(1-u^2) = -(1+u^2)(1-u^{3^s}).$$

Equivalently, in characteristic 3,

$$u^{3^s+2} = 1,$$

or $u^{3^s} = u^{-2}$. This gives the asserted equivalence. □

PROOF OF THEOREM 1.1. Since the constant term in (1.1) is 1, every root of (1.1) lies in $\mathbb{F}_q^\times$. By Propositions 3.1 and 2.1, the roots of (1.1) in $\mathbb{F}_q$ are in bijection with the elements

$$u \in \mu_{q+1} \setminus \{1, -1\}$$

such that

$$u^{3^s+2(-1)^s} = 1.$$

Put

$$M = 3^s + 2(-1)^s.$$

Since μ_{q+1} is cyclic of order $q+1$, the equation $u^M = 1$ has exactly

$$\gcd(q+1, M)$$

solutions in μ_{q+1}.

The integer M is odd. Hence, $u = -1$ does not satisfy $u^M = 1$. Thus, among the solutions in μ_{q+1}, the only element excluded by passing to $\mu_{q+1} \setminus \{1, -1\}$ is $u = 1$. It follows that

$$N_{m,s} = \gcd(q+1, M) - 1 = \gcd(q+1, 3^s + 2(-1)^s) - 1.$$

This proves the theorem. □

4. Application to the conjectural no-root condition

We now give the consequence in the form in which (1.1) is used in the cyclic-code setting. Whenever the nonexistence of roots of (1.1) over $\mathbb{F}_{3^m}$ is required, the obstruction is completely determined by the following greatest common divisor.

COROLLARY 4.1. *Let $m \geq 1$ be odd and let $s \geq 1$. Then, (1.1) has no root in $\mathbb{F}_{3^m}$ if and only if*

$$\gcd(3^m + 1, 3^s + 2(-1)^s) = 1.$$

https://doi.org/10.1017/S0004972726101853 Published online by Cambridge University Press

If this greatest common divisor is greater than 1*, then* (1.1) *has exactly*

$$\gcd(3^m + 1, 3^s + 2(-1)^s) - 1$$

roots in $\mathbb{F}_{3^m}$.

PROOF. This follows at once from Theorem 1.1 with $q = 3^m$. □

REMARK 4.2. The precise cyclic code depends on the exponent family under consideration. However, whenever the analysis reduces to the no-root condition for (1.1), Corollary 4.1 gives the exact answer. The Cayley transform therefore changes the finite-field solvability question appearing in the coding-theoretic argument into an elementary calculation in a cyclic group.

The following consequence strengthens the single counterexample obtained by taking $(m, s) = (83, 11)$.

COROLLARY 4.3. *Let* $s = 11$ *and put* $m = 83 + 166t$ *with* $t \geq 0$. *If*

$$t \not\equiv 1 \pmod 3 \quad \textit{and} \quad t \not\equiv 5 \pmod{11},$$

then m *is odd and*

$$\gcd(m, 3) = \gcd(m, 11) = 1.$$

Equation (1.1) *has at least* 498 *roots in* $\mathbb{F}_{3^m}$. *Consequently, the conjectural no-root statement from the conclusion of* [7] *fails for infinitely many pairs* (m, s) *satisfying its hypotheses.*

PROOF. A direct computation gives

$$3^{11} \equiv 2 \pmod{499} \quad \text{and} \quad 3^{83} \equiv -1 \pmod{499}.$$

Squaring the second congruence gives

$$3^{166} \equiv 1 \pmod{499}.$$

Hence, for every m of the form $m = 83 + 166t$,

$$3^m = 3^{83}(3^{166})^t \equiv -1 \pmod{499}.$$

Therefore,

$$499 \mid 3^{11} - 2 \quad \text{and} \quad 499 \mid 3^m + 1.$$

Since $s = 11$ is odd, Theorem 1.1 gives

$$N_{m,11} = \gcd(3^m + 1, 3^{11} - 2) - 1 \geq 499 - 1 = 498.$$

It remains to check the hypotheses in the conjectural statement. Since 83 is odd and 166 is even, every integer $m = 83 + 166t$ is odd. In addition,

$$m = 83 + 166t \equiv 2 + t \pmod 3,$$

https://doi.org/10.1017/S0004972726101853 Published online by Cambridge University Press

so $\gcd(m, 3) = 1$ precisely when $t \not\equiv 1 \pmod 3$. Similarly,

$$m = 83 + 166t \equiv 6 + t \pmod{11},$$

so $\gcd(m, 11) = 1$ precisely when $t \not\equiv 5 \pmod{11}$. For example, all integers $t = 33r$ with $r \geq 0$ satisfy both restrictions. This gives infinitely many admissible pairs and the assertion follows. □

COROLLARY 4.4. *Let $m \geq 1$ be odd. Then, the equation*

$$x^4 - x^2 + 1 = 0$$

has no root in $\mathbb{F}_{3^m}$.

PROOF. Take $s = 1$ in Theorem 1.1. Then,

$$N_{m,1} = \gcd(3^m + 1, 3 - 2) - 1 = \gcd(3^m + 1, 1) - 1 = 0.$$

This gives the claim. □

REMARK 4.5. Theorem 1.1 shows that the root count depends only on

$$\gcd(3^m + 1, 3^s + 2(-1)^s).$$

Thus, the condition $\gcd(m, s) = 1$ alone does not control the root count. Together with Corollary 4.3, this gives a negative answer to the conjectural no-root statement in [7].

References

[1] C. Ding and T. Helleseth, 'Optimal ternary cyclic codes from monomials', *IEEE Trans. Inform. Theory* **59**(9) (2013), 5898–5904.
[2] D. Han and H. Yan, 'On an open problem about a class of optimal ternary cyclic codes', *Finite Fields Appl.* **59** (2019), 335–343.
[3] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd edn, Encyclopedia of Mathematics and its Applications, 20 (Cambridge University Press, Cambridge, 1997).
[4] L. Wang and G. Wu, 'Several classes of optimal ternary cyclic codes with minimal distance four', *Finite Fields Appl.* **40** (2016), 126–137.
[5] Z. Zha and L. Hu, 'New classes of optimal ternary cyclic codes with minimum distance four', *Finite Fields Appl.* **64** (2020), Article no. 101671.
[6] Z. Zha, L. Hu, Y. Liu and X. Cao, 'Further results on optimal ternary cyclic codes', *Finite Fields Appl.* **75** (2021), Article no. 101898.
[7] H. Zhao, R. Luo and T. Sun, 'Two families of optimal ternary cyclic codes with minimal distance four', *Finite Fields Appl.* **79** (2022), Article no. 101995.

FRANCISCO-JAVIER SOTO, Escuela Técnica Superior de Ingeniería Informática,
Universidad Rey Juan Carlos (URJC), 28933 Móstoles, Spain
Current address:
Departamento de Matemáticas, Estadística y Computación,
Universidad de Cantabria, 39005 Santander, Spain
e-mail: fjavier.soto@unican.es

https://doi.org/10.1017/S0004972726101853 Published online by Cambridge University Press