RATIONAL POINTS ON SOME FERMAT CURVES AND SURFACES OVER FINITE FIELDS

JOSÉ FELIPE VOLOCH AND MICHAEL E. ZIEVE

ABSTRACT. We give an explicit description of the $\mathbb{F}_{q^i}$-rational points on the Fermat curve $u^{q-1}+v^{q-1}+w^{q-1}=0$, for $i \in \{1,2,3\}$. As a consequence, we observe that for any such point (u,v,w), the product uvw is a cube in $\mathbb{F}_{q^i}$. We also describe the $\mathbb{F}_{q^2}$-rational points on the Fermat surface $u^{q-1}+v^{q-1}+w^{q-1}+x^{q-1}=0$.

1. INTRODUCTION

Let $q = p^r$ where p is prime and r is a positive integer. We will examine the $\mathbb{F}_{q^i}$-rational points on the Fermat curve $u^{q-1} + v^{q-1} + w^{q-1} = 0$, for $i \in \{1,2,3\}$. Several authors have given estimates for the number of such points, or even formulas for this number in some cases [2, 3, 4, 5]. We will go further and explicitly write down all the points. We find the following unexpected consequence:

Corollary 1.1. *For $i \in \{1,2,3\}$ and $u,v,w \in \mathbb{F}_{q^i}$, if $u^{q-1} + v^{q-1} + w^{q-1} = 0$ then uvw is a cube in $\mathbb{F}_{q^i}$.*

Although the shape of this assertion is suggestive, we do not know any generalizations of this result. Nonetheless, we highlight this result in case it might inspire further developments. In the recent paper [6], this result was shown for even q when $i = 3$, in order to prove a conjecture from [7] about certain functions related to finite projective planes. That proof was quite computational, and the desire for a more conceptual proof led to the present paper.

We now describe the points on these Fermat curves. Write $T(X) := X^{q^2} + X^q + X$.

Theorem 1.2. *The points in $\mathbb{P}^2(\mathbb{F}_{q^3})$ on the curve $u^{q-1}+v^{q-1}+w^{q-1} = 0$ are as follows:*

(1) *points $(cv^{q+1} : v : 1)$ with $c \in \mathbb{F}_q^*$ and v a nonzero root of $T(X)$;*

Date: March 9, 2013.

2010 *Mathematics Subject Classification.* 11G20, 14G15.

The first author was partially supported by the Simons Foundation (grant #234591). The second author was partially supported by NSF grant DMS-1162181.

(2) *points* $(cv^{-q} : v : 1)$ *with* $c \in \mathbb{F}_q^*$ *and* v *a nonzero root of* $T(1/X)$*;*
(3) *points* $(u : v : w)$ *with* $u, v, w \in \mathbb{F}_q$ *and precisely one of* u, v, w *being zero, where* q *is even.*

Theorem 1.3. *The points in* $\mathbb{P}^2(\mathbb{F}_{q^2})$ *on the curve* $u^{q-1}+v^{q-1}+w^{q-1} = 0$ *are as follows:*

(1) *points* $(cv^2 : v : 1)$ *with* $c \in \mathbb{F}_q^*$ *and* v^{q-1} *a primitive cube root of unity, where* $q \equiv 2 \pmod 3$*;*
(2) *points* $(u : v : 1)$ *with* $u, v \in \mathbb{F}_q^*$*, where* $q \equiv 0 \pmod 3$*;*
(3) *points* $(u : v : w)$ *with* $\{u, v, w\} = \{0, 1, d\}$ *where* $d^{q-1} = -1$*.*

The description of the points over $\mathbb{F}_q$ is an easy exercise, and we record the answer just for completeness:

Lemma 1.4. *The points in* $\mathbb{P}^2(\mathbb{F}_q)$ *on the curve* $u^{q-1}+v^{q-1}+w^{q-1} = 0$ *are as follows:*

(1) *points* $(u : v : w)$ *with* $u, v, w \in \mathbb{F}_q^*$*, where* $p = 3$*; and*
(2) *points* $(u : v : w)$ *with* $u, v, w \in \mathbb{F}_q$ *and exactly one of* u, v, w *being zero, where* $p = 2$*.*

These results yield formulas for the numbers of $\mathbb{F}_{q^i}$-rational points on these curves, which agree with the corresponding formulas in [5]. Our proofs are much shorter and more direct than those in [5], but it should be noted that the lengthier proofs in [5] also yielded results about certain twists of these Fermat curves, which we do not consider here.

Our technique also yields a description of the $\mathbb{F}_{q^2}$-rational points on the degree-$(q-1)$ Fermat surface:

Theorem 1.5. *The points in* $\mathbb{P}^3(\mathbb{F}_{q^2})$ *on the surface* $u^{q-1} + v^{q-1} + w^{q-1} + x^{q-1} = 0$ *are as follows:*

(1) *points* $(u_1 : u_2 : u_3 : u_4)$ *with* $u_i \in \mathbb{F}_{q^2}$*, where at least one* u_i *is nonzero and there is a permutation* σ *of* $\{1, 2, 3, 4\}$ *such that* $u_{\sigma(1)}^{q-1} = -u_{\sigma(2)}^{q-1}$ *and* $u_{\sigma(3)}^{q-1} = -u_{\sigma(4)}^{q-1}$*;*
(2) *points* $(u_1 : u_2 : u_3 : u_4)$ *in which exactly one* u_i *is zero and the* $(q-1)$*-th powers of the other* u_i*'s are distinct cube roots of unity, where* $q \equiv 2 \pmod 3$*;*
(3) *points* $(u_1 : u_2 : u_3 : u_4)$ *with* $u_i \in \mathbb{F}_q$ *and exactly one* $u_i = 0$*, where* $q \equiv 0 \pmod 3$*.*

The points in (1) above are the points which are on the lines contained in the surface.

This theorem has the following consequences:

Corollary 1.6. *If $u, v, w, x \in \mathbb{F}_{q^2}$ satisfy $u^{q-1}+v^{q-1}+w^{q-1}+x^{q-1}=0$, then $uvwx$ is a square in $\mathbb{F}_{q^2}$.*

Corollary 1.7. *The number N of points in $\mathbb{P}^3(\mathbb{F}_{q^2})$ on the surface $u^{q-1}+v^{q-1}+w^{q-1}+x^{q-1}=0$ satisfies*

$$N = \begin{cases} 3(q-1)^4+3(q-1)^3+6(q-1) & \text{if } q \equiv 1 \pmod 6 \\ 3(q-1)^4+3(q-1)^3+8(q-1)^2+6(q-1) & \text{if } q \equiv 5 \pmod 6 \\ 3(q-1)^4+3(q-1)^3+4(q-1)^2+6(q-1) & \text{if } q \equiv 0 \pmod 3 \\ (3q+1)(q-1)^3+6(q-1) & \text{if } q \equiv 4 \pmod 6 \\ (3q+1)(q-1)^3+8(q-1)^2+6(q-1) & \text{if } q \equiv 2 \pmod 6. \end{cases}$$

Our proof of Theorem 1.2 involves an unexpected factorization. A similar type of unexpected factorization arose in a paper of Carlitz [1, eqn. (25)] on multiple Kloosterman sums. Carlitz's result was then used in [5], together with a few pages of additional character sum computations, to count the number of $\mathbb{F}_{q^3}$-rational points on the degree-$(q-1)$ Fermat curve. It is tempting to surmise that there should be a natural bijection which shows that our factorization and Carlitz's are in some sense the same factorization in different languages. However, we have not been able to find such a bijection.

We will prove Theorems 1.3 and 1.2 in the next two sections, and prove Corollary 1.1 in Section 5. We conclude in Section 6 with proofs of Theorem 1.5 and its corollaries.

2. Points over $\mathbb{F}_{q^2}$

In this section we prove Theorem 1.3, and then verify that the resulting formula for the number of $\mathbb{F}_{q^2}$-rational points agrees with the previously known value.

Proof of Theorem 1.3. Suppose $u, v \in \mathbb{F}_{q^2}^*$ satisfy $u^{q-1}+v^{q-1}+1=0$. Then

$$\begin{aligned} 1 &= (-u^{q-1})^{q+1} \\ &= (v^{q-1}+1)^{q+1} \\ &= (v^{q-1}+1)^q(v^{q-1}+1) \\ &= (v^{q^2-q}+1)(v^{q-1}+1) \\ &= v^{q^2-1}+v^{q^2-q}+v^{q-1}+1 \\ &= 1+v^{1-q}+v^{q-1}+1, \end{aligned}$$

or equivalently,

$$0 = v^{2q-2}+v^{q-1}+1.$$

Thus, if $p \neq 3$ then v^{q-1} is a primitive cube root of unity, and if $p = 3$ then $v^{q-1} = 1$.

Conversely, if $p \neq 3$ then $\mathbb{F}_{q^2}$ contains two primitive cube roots of unity. In order that these cube roots of unity should be $(q-1)$-th powers, it is necessary and sufficient that $3(q-1) \mid (q^2-1)$, or equivalently, $q \equiv 2 \pmod 3$. If $q \equiv 2 \pmod 3$ then there are precisely $2q-2$ elements $v \in \mathbb{F}_{q^2}^*$ such that v^{q-1} is a primitive cube root of unity, and for any such v the equation $u^{q-1} + v^{q-1} + 1 = 0$ can be rewritten as $u^{q-1} = v^{2q-2}$, or equivalently, $u = cv^2$ with $c \in \mathbb{F}_q^*$. Likewise, if $p = 3$ and $v \in \mathbb{F}_q^*$ then the equation $u^{q-1} + v^{q-1} + 1 = 0$ becomes $u^{q-1} = 1$, so $u \in \mathbb{F}_q^*$. Finally, it is straightforward to solve $u^{q-1} + v^{q-1} + w^{q-1} = 0$ when $xyz = 0$. This completes the proof. □

The following consequence of Theorem 1.3 is immediate.

Corollary 2.1. *The number N of points in $\mathbb{P}^2(\mathbb{F}_{q^2})$ on the curve $u^{q-1} + v^{q-1} + w^{q-1} = 0$ is*

$$N = \begin{cases} 3(q-1) & \text{if } q \equiv 1 \pmod 3 \\ 3(q-1) + (q-1)^2 & \text{if } q \equiv 0 \pmod 3 \\ 3(q-1) + 2(q-1)^2 & \text{if } q \equiv 2 \pmod 3. \end{cases}$$

3. Points over $\mathbb{F}_{q^3}$

In this section we prove Theorem 1.2, and then verify that the resulting formula for the number of $\mathbb{F}_{q^3}$-rational points agrees with the previously known value.

Proof of Theorem 1.2. Suppose $u \in \mathbb{F}_{q^3}^*$ and $v \in \mathbb{F}_{q^3}$ satisfy $u^{q-1} + v^{q-1} + 1 = 0$. Then

$$-1 = (-u^{q-1})^{q^2+q+1} = (v^{q-1} + 1)^{q^2+q+1}.$$

If $v = 0$ then we get $-1 = 1$, so q is even and $u^{q-1} = 1$. Henceforth assume $v \neq 0$. Write $V := v^{q-1}$, so that

$$\begin{aligned} -1 &= (V+1)^{q^2}(V+1)^q(V+1) \\ &= (V^{q^2}+1)(V^q+1)(V+1) \\ &= V^{q^2+q+1} + V^{q^2+q} + V^{q^2+1} + V^{q^2} + V^{q+1} + V^q + V + 1. \end{aligned}$$

Upon substituting $V^{q^2} = 1/V^{q+1}$, we obtain

$$-1 = 1 + V^{-1} + V^{-q} + V^{-q-1} + V^{q+1} + V^q + V + 1.$$

Adding 1 to both sides yields

$$0 = (V^{q+1} + V + 1)(V^{-q-1} + V^{-1} + 1).$$

Since $V = v^{q-1}$, this says

$$0 = (v^{q^2-1} + v^{q-1} + 1) \cdot ((1/v)^{q^2-1} + (1/v)^{q-1} + 1),$$

or equivalently,

$$0 = T(v) \cdot T(1/v).$$

Conversely, if $T(v) = 0$ and $v \neq 0$ then $v \in \mathbb{F}_{q^3}$, since

$$0 = 0^q - 0 = T(v)^q - T(v) = v^{q^3} - v.$$

In this case, $v^{q-1} + 1 = -v^{q^2-1}$, so for $u \in \mathbb{F}_{q^3}^*$ the condition $u^{q-1} + v^{q-1} + 1 = 0$ says that $u^{q-1} = v^{q^2-1}$, or equivalently, $u = cv^{q+1}$ for some $c \in \mathbb{F}_q^*$. Likewise, if $v \neq 0$ and $T(1/v) = 0$ then $v \in \mathbb{F}_{q^3}$ and the condition $u^{q-1} + v^{q-1} + 1 = 0$ becomes $(u/v)^{q-1} + 1 + (1/v)^{q-1} = 0$, or equivalently $(u/v)^{q-1} = (1/v)^{q^2-1}$. This last equation says that $u/v = c/v^{q+1}$ for some $c \in \mathbb{F}_q^*$, so that $u = c/v^q$. Finally, if q is even and $u \in \mathbb{F}_q^*$ then plainly $u^{q-1} + 1 = 0$. This completes the proof. □

Corollary 3.1. *The number N of points in $\mathbb{P}^2(\mathbb{F}_{q^3})$ on the curve $u^{q-1} + v^{q-1} + w^{q-1} = 0$ is*

$$N = \begin{cases} (2q+2)(q-1)^2 & \text{if } q \equiv 5 \pmod 6 \\ (2q+1)(q-1)^2 & \text{if } q \equiv 0 \pmod 3 \\ 2q(q-1)^2 & \text{if } q \equiv 1 \pmod 6 \\ (2q+2)(q-1)^2 + 3(q-1) & \text{if } q \equiv 2 \pmod 6 \\ 2q(q-1)^2 + 3(q-1) & \text{if } q \equiv 4 \pmod 6. \end{cases}$$

Proof. If q is odd then all points have nonzero coordinates; if q is even then there are precisely $3(q-1)$ points with a zero coordinate. Henceforth we consider points with nonzero coordinates. Since the derivative $T'(X)$ is a nonzero constant, we know that $T(X)$ is squarefree, and hence has $q^2 - 1$ distinct nonzero roots. If none of these are roots of $T(1/X)$ then the number of $\mathbb{F}_{q^3}$-rational points on our curve which have nonzero coordinates will equal $2(q^2-1)(q-1)$, or in other words $(2q+2)(q-1)^2$. Next, if $T(v) = T(1/v) = 0$ then

$$v^{q^2} + v^q + v = 0 = v^{q^2+1}T(1/v) = v + v^{q^2-q+1} + v^{q^2},$$

so $v^q = v^{q^2-q+1}$ and thus $v^{q^2-2q+1} = 1$. Since $v \in \mathbb{F}_{q^3}$, it follows that $v^{\gcd(q^2-2q+1, q^3-1)} = 1$. We compute $q^3 - 1 = (q^2-2q+1)(q+2) + 3q - 3$, so $\gcd(q^2-2q+1, q^3-1)$ equals $3q-3$ if $q \equiv 1 \pmod 3$, and equals $q-1$ otherwise. Conversely, if $v \in \mathbb{F}_q^*$ then $T(v) = 3v$ is nonzero unless $q \equiv 0 \pmod 3$, in which case $T(v) = T(1/v) = 0$ and

$$\{(cv^{q+1} : v : 1) \colon c \in \mathbb{F}_q^*\} = \{(cv^{-q} : v : 1) \colon c \in \mathbb{F}_q^*\}.$$

Finally, if $q \equiv 1 \pmod 3$ and $\omega := v^{q-1}$ has order 3, then $T(v) = v(\omega^{q+1} + \omega + 1) = 0$, and likewise $T(1/v) = 0$. In this case, v^3 is in $\mathbb{F}_q^*$, so also $v^{2q+1} \in \mathbb{F}_q^*$, which implies that again

$$\{(cv^{q+1} : v : 1) \colon c \in \mathbb{F}_q^*\} = \{(cv^{-q} : v : 1) \colon c \in \mathbb{F}_q^*\}.$$

The result now follows from Theorem 1.2. □

4. The product of the coordinates

We now prove Corollary 1.1. The conclusion clearly holds if $uvw = 0$, so assume that $uvw \neq 0$. Without loss, we may divide each of u, v, w by w, in order to assume that $w = 1$. The conclusion is immediate if every element of $\mathbb{F}_{q^i}$ is a cube, which occurs when either $p = 3$ or both $i = 3$ and $q \equiv 2 \pmod 3$. Henceforth assume that neither of these situations holds. This rules out all solutions if $i = 1$. If $i = 2$ then $q \equiv 2 \pmod 3$ and $u = cv^2$ with $c \in \mathbb{F}_q^*$, so $uv = cv^3$ is a cube since c is a $(q+1)$-th power. If $i = 3$ then $q \equiv 1 \pmod 3$ and, for some $c \in \mathbb{F}_q^*$, either $u = cv^{q+1}$ or $u = cv^{-q}$. Thus uvw equals either cv^{q+2} or cv^{1-q}. Since $q \equiv 1 \pmod 3$, both v^{q+2} and v^{1-q} are cubes in $\mathbb{F}_{q^3}$. Finally, since c is in $\mathbb{F}_q^*$, it is a (q^2+q+1)-th power in $\mathbb{F}_{q^3}$, and hence is a cube. The result follows.

Remark. Since the statement of Corollary 1.1 is quite clean, it is natural to wonder whether there is a generalization to higher-degree extensions of $\mathbb{F}_q$. However, the most immediate generalization is not true. For instance, there are elements $u, v, w \in \mathbb{F}_{16}$ for which $u + v + w = 0$ but uvw generates the group $\mathbb{F}_{16}^*$. This shows that the immediate generalization of Corollary 1.1 does not hold for $i = 4$ and $q = 2$.

5. The Fermat surface

In this section we prove Theorem 1.5 and its corollaries.

Proof of Theorem 1.5. Let $u, v, w, x \in \mathbb{F}_{q^2}$ satisfy $u^{q-1} + v^{q-1} + w^{q-1} + x^{q-1} = 0$. The desired conclusion follows from Theorem 1.3 if $uvwx = 0$, so assume that $u, v, w, x \in \mathbb{F}_{q^2}^*$. Then

$$\begin{aligned}
1 &= (-x^{q-1})^{q+1} \\
&= (u^{q-1} + v^{q-1} + w^{q-1})^{q+1} \\
&= (u^{q-1} + v^{q-1} + w^{q-1})^q \cdot (u^{q-1} + v^{q-1} + w^{q-1}) \\
&= (u^{q^2-q} + v^{q^2-q} + w^{q^2-q}) \cdot (u^{q-1} + v^{q-1} + w^{q-1}) \\
&= (u^{1-q} + v^{1-q} + w^{1-q}) \cdot (u^{q-1} + v^{q-1} + w^{q-1}) \\
&= 3 + (u/v)^{q-1} + (v/u)^{q-1} + (u/w)^{q-1} + (w/u)^{q-1} + (v/w)^{q-1} + (w/v)^{q-1}.
\end{aligned}$$

After subtracting 1 from both sides, and then multiplying both sides by $(uvw)^{q-1}$, we obtain

$$0 = (u^{q-1} + v^{q-1})(u^{q-1} + w^{q-1})(v^{q-1} + w^{q-1}).$$

Hence two of u^{q-1}, v^{q-1}, and w^{q-1} are negatives of one another. The result follows. □

Corollary 1.6 follows from Theorem 1.5 because, if $u, v, w, x \in \mathbb{F}_{q^2}^*$ satisfy $u^{q-1} = -v^{q-1}$ and $w^{q-1} = -x^{q-1}$, then $(uvwx)^{q-1} = (vx)^{2q-2}$ is a square. Finally, the deduction of Corollary 1.7 from Theorem 1.5 is straightforward.

References

[1] L. Carlitz, *A note on multiple exponential sums*, Pacific J. Math. **15** (1965), 757–765.

[2] H. Davenport and H. Hasse, *Die Nullstellen der Kongruenz Zetafunktion in gewissen zyklischen Fallen*, J. Reine Angew. Math. **172** (1935), 151–182.

[3] A. García and J. F. Voloch, *Fermat curves over finite fields*, J. Number Theory **30** (1988), 345–356.

[4] X.-D. Hou and C. Sze, *On certain diagonal equations over finite fields*, Finite Fields Appl. **15** (2009), 633–643.

[5] M. Moisio, *On the number of rational points on some families of Fermat curves over finite fields*, Finite Fields Appl. **13** (2007), 546–562.

[6] Z. Scherr and M. E. Zieve, *Planar monomials in characteristic* 2, arXiv:1302.1244v1, 6 Feb 2013.

[7] K.-U. Schmidt and Y. Zhou, *Planar functions over fields of characteristic two*, arXiv:1301.6999v1, 29 Jan 2013.

Department of Mathematics, University of Texas, Austin, TX 78712 USA

E-mail address: voloch@math.utexas.edu

URL: http://www.ma.utexas.edu/users/voloch/

Department of Mathematics, University of Michigan, 530 Church Street, Ann Arbor, MI 48109-1043 USA

E-mail address: zieve@umich.edu

URL: http://www.math.lsa.umich.edu/∼zieve/