View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

Finite Fields and Their Applications 13 (2007) 773–777

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

On a bound of Garcia and Voloch for the number of points of a Fermat curve over a prime field

Sandro Mattarei

Dipartimento di Matematica, Università degli Studi di Trento, via Sommarive 14, I-38050 Povo (Trento), Italy

Received 10 August 2005; revised 17 March 2006

Available online 3 May 2006

Communicated by Gary L. Mullen

Abstract

In 1988 Garcia and Voloch proved the upper bound $4n^{4/3}(p-1)^{2/3}$ for the number of solutions over a prime finite field $\mathbb{F}_p$ of the Fermat equation $x^n + y^n = a$, where $a \in \mathbb{F}_p^*$ and $n \geqslant 2$ is a divisor of $p-1$ such that $(n-\frac{1}{2})^4 \geqslant p-1$. This is better than Weil's bound $p+1+(n-1)(n-2)\sqrt{p}$ in the stated range. By refining Garcia and Voloch's proof we show that the constant 4 in their bound can be replaced by $3 \cdot 2^{-2/3}$.
© 2006 Elsevier Inc. All rights reserved.

Keywords: Fermat curve; Finite field

Let $\mathbb{F}_q$ be the finite field of q elements and let p be its characteristic. Consider the *Fermat curve* $ax^n + by^n = z^n$, expressed in homogeneous coordinates, where $n > 1$ is an integer prime to p, and $a, b \in \mathbb{F}_q^*$. A classical estimate on the number $N_n(a,b,q)$ of its projective $\mathbb{F}_q$-rational points is $|N_n(a,b,q) - q - 1| \leqslant (n-1)(n-2)\sqrt{q}$. This is originally due to Hasse and Davenport [1] but is a special case of *Weil's bound* for curves over finite fields. In the special case of Fermat curves Weil's bound is easy to prove by means of Gauss and Jacobi sums, as well as its generalisation to *diagonal equations* in several variables, see [5,7] or [10]. An alternative proof uses character theory of finite groups, see [2, Section 26] for the basic idea and [8] for a refinement.

Weil's upper bound for $N_n(a,b,q)$ is not optimal when n (and with it the genus of the curve) is relatively large with respect to q. Better upper bounds in this situation were found by Garcia

E-mail address: mattarei@science.unitn.it.
URL: http://www-math.science.unitn.it/~mattarei/.

1071-5797/$ – see front matter © 2006 Elsevier Inc. All rights reserved.
doi:10.1016/j.ffa.2006.03.005

and Voloch, using methods from algebraic geometry. According to [3, Corollary 1], rewritten here after elementary calculations, if s is an integer such that $1 \leqslant s \leqslant n-3$ and $sn \leqslant p$, then

$$N_n(a,b,q) \leqslant \frac{1}{4}\left(s^2 - s - 2 + 16\frac{1}{s+3}\right)n^2 + 2\frac{n(q-1-d)}{s+3} + d, \tag{1}$$

where d is the number of $\mathbb{F}_q$-rational points of the curve with $xyz = 0$. Garcia and Voloch pointed out that their bounds (1) hold in more general circumstances where the assumption $sn \leqslant p$ may not be satisfied, and described those circumstances in detail for the cases $s = 1, 2$. However, the special case stated above, and with $q = p$, was sufficient to them for an application to Waring's problem in $\mathbb{F}_p$. By estimating the minimum of their bounds, for $1 \leqslant s \leqslant n-3$ and $sn \leqslant p$, they obtained the following intermediate result in [3, Section 3]: The number of solutions $(x, y) \in \mathbb{F}_p \times \mathbb{F}_p$ of $x^n + y^n = a$, for p a prime, $a \in \mathbb{F}_p^*$ and $n \geqslant 2$ a divisor of $p-1$ such that $(n - \frac{1}{2})^4 \geqslant p - 1$, is at most $4n^{4/3}(p-1)^{2/3}$. A version of this bound (but for the equation $x^n - y^n = a$) with an unspecified constant in place of 4 was later proved by Heath-Brown and Konyagin using Stepanov's method; this is the case $T = 1$ of [4, Lemma 5], but see also [6, Chapter 3] for a generalization. We comment further on this bound in Remark 3. Mit'kin has recently shown in [9] through elementary means that Garcia and Voloch's bound holds (for the equation $x^n - y^n = a$) with the constant 4 replaced by 2, for $n > 2^{3/4}(p-1)^{1/4}$. However, it is also apparent from Garcia and Voloch's proof that the coefficient 4 in their bound can be lowered by refining their argument. In this note we bring the coefficient in that bound down to its optimal value subject to being a consequence of the collection of Garcia and Voloch's bounds (1), as follows.

Corollary. *Let p be a prime and $a, b \in \mathbb{F}_p^*$. Let $n \geqslant 4$ be a divisor of $p-1$ such that $n^4 \geqslant 4(p-1)$. Then $N_n(a,b,p) < 3 \cdot 2^{-2/3} n^{4/3}(p-1)^{2/3}$.*

Since $3 \cdot 2^{-2/3}$ is slightly less than 1.88989, the corollary is a little stronger than the result in [9]. We will deduce this result from the following more precise bound.

Theorem. *Let p be a prime and $a, b \in \mathbb{F}_p^*$. Let $n \geqslant 4$ be a divisor of $p-1$ such that $n^4 - 2n^3 - 3n^2 - 8n \geqslant 4(p-1)$. Then*

$$N_n(a,b,p) < n^2\left(3(k/2)^{2/3} - \frac{7}{2}(k/2)^{1/3} + \frac{25}{12}\right),$$

where $k = (p-1)/n$.

Proof. Because of the assumption $s \leqslant n-3$, each bounding function in (1) does not decrease by replacing d with its minimum value 0. We comment on the effect of this simplification in Remark 2. In terms of k and dropping the dependency on d as described, the collection of bounds (1) reads

$$N_n(a,b,p)/n^2 \leqslant \min\{U_s(k):\ 1 \leqslant s \leqslant n-3,\ s \leqslant k\}, \tag{2}$$

where

$$U_s(k) = \frac{s^2 - s - 2}{4} + 2\frac{k+2}{s+3}.$$

Thus, the upper bound for $N_n(a, b, p)/n^2$ given by inequality (2) is a piece-wise linear function of k. Computation shows that $U_{s+1}(k) = U_s(k)$ when $k = k_s$, where $k_s + 2 = s(s+3)(s+4)/4$. Because $k_k \geqslant k$ we have $U_s(k) \geqslant U_k(k)$ for $s \geqslant k$, and hence the condition $s \leqslant k$ is actually immaterial in evaluating the minimum at the right-hand side of inequality (2). It also follows that the right-hand side of inequality (2) is independent of n for $k \leqslant k_{n-3} = \frac{1}{4}(n-3)n(n+1) - 2$, which is equivalent to our assumption $n^4 - 2n^3 - 3n^2 - 8n \geqslant 4(p-1)$. Therefore, under this assumption bound (2) can be written as $N_n(a, b, p)/n^2 \leqslant V(k)$, where $V(k) = \min\{U_s(k)\colon s \geqslant 1\}$.

It remains to find a convenient function $W(k)$ which bounds the piece-wise linear function $V(k)$ from above. Since $V(k_s) = U_s(k_s) = (3s^2 + 7s - 2)/4$, any concave function $W(k)$ such that $W(k_s) \geqslant (3s^2 + 7s - 2)/4$ for all integers $s \geqslant 1$ will do. Consider the function $W_c(k) = 3(k/2)^{2/3} - \frac{7}{2}(k/2)^{1/3} + c$, where c is a constant. We have

$$W_c\big((s + 7/3)^3/4\big) = \big(3s^2 + 7s + 4c\big)/4,$$

and $W_c'(k) = (k/2)^{-1/3} - \frac{7}{12}(k/2)^{-4/3} \leqslant (k/2)^{-1/3}$. In particular, $W_c'(k_s) \leqslant 2/s$ because $k_s \geqslant s^3/4$. Since $W_c(k)$ is a concave function we have

$$\begin{aligned} W_c(k_s) &\geqslant W_c\big((s + 7/3)^3/4\big) - \big((s + 7/3)^3/4 - k_s\big)W_c'(k_s) \\ &\geqslant \frac{3s^2 + 7s + 4c}{4} - \left(\frac{13}{12}s + \frac{559}{108}\right)\frac{2}{s} = V(k_s) + c - \frac{5}{3} - \frac{559}{54s}. \end{aligned}$$

Thus, if $c > 5/3$ then $W_c(k_s) \geqslant V(k_s)$ for all integers $s \geqslant 1$ except a finite number. A calculation now shows that the smallest value of c such that $W_c(k_s) \geqslant V(k_s)$ for all $s \geqslant 1$ is $c = 6 - 3(13/2)^{2/3} + (7/2)(13/2)^{1/3}$. (Equality then occurs for $s = 2$.) Since the value of this expression is (close to and) slightly less than $25/12$, the conclusion follows. □

Remark 1. The argument in the proof of the theorem can be extended to show that $W_{71/48}(k) \leqslant V(k) < W_{25/12}(k)$ for all $k \geqslant 1$. The lower function equals the first three terms of the asymptotic expansion, for $k \to \infty$, of the envelope of the family of linear functions $U_s(k)$, where $s \geqslant 1$ is viewed as a real parameter instead of integral. It follows that the bound for $N_n(a, b, p)$ given in the theorem exceeds by less than $29n^2/48$ the minimum of the collection of bounds (1).

Remark 2. We briefly explain the effect of having disregarded d in the proof of the theorem. Let G be the set of nth powers in $\mathbb{F}_p^*$, that is, the subgroup of $\mathbb{F}_p^*$ of order $k = (p-1)/n$. If (x, y) is a solution of $ax^n + by^n = 1$ with $xy = 0$ then any pair obtained from that by multiplying x and y by elements of G is also a solution. Consequently, $N_n(a, b, p) - d$ is a multiple of n^2, and we can write (1) in the form

$$\big(N_n(a, b, p) - d\big)/n^2 \leqslant \left[U_s(k) - \frac{2}{s+3}(d/n)\right],$$

where $U_s(k)$ as in the proof of the theorem and with the square brackets denoting the integral part. The ratio d/n can only assume the values $0, 1, 2, 3$, because it equals how many of a, b and $-a/b$ belong to G (counting repetitions). The proof of the theorem (and, specifically, the formula for k_s) shows that the strongest of bounds (1) for a given value of k occurs, roughly, for s close to $2(k/2)^{1/3}$. Accordingly, one can improve the bound given in the theorem by making it

dependent on d, but this would affect at most the term $\frac{7}{2}(k/2)^{1/3}$, and not the leading term of the bound.

Proof of corollary. We only need to explain how the weakened conclusion allows us to relax our hypothesis $n^4 - 2n^3 - 3n^2 - 8n \geqslant 4(p-1)$ to the weaker assumption $n^4 \geqslant 4(p-1)$, which is equivalent to $n^3 \geqslant 4k$. When the stronger assumption is not satisfied, that is, when $k > k_{n-3} = \frac{1}{4}(n^3 - 2n^2 - 3n - 8)$, bound (2) reads $N_n(a, b, p)/n^2 \leqslant U_{n-3}(k)$. Thus, it suffices to show that $U_{n-3}(k) < 3(k/2)^{2/3}$ for $k_{n-3} < k \leqslant n^3/4$. Viewing n as fixed, and hence p as a function of k, the left-hand side of the desired inequality is a linear function of k, while the right-hand side is a concave function. Since we know from the theorem that the inequality is satisfied for $k = k_{n-3}$, it remains only to check that this is the case also for $k = n^3/4$. Indeed, we have

$$U_{n-3}\bigl(n^3/4\bigr)^3 = \left(\frac{3n^2 - 7n + 10}{4} + \frac{4}{n}\right)^3 < \left(\frac{3n^2}{4}\right)^3 = 3\left(\frac{(n^3/4)}{2}\right)^2$$

for all $n \geqslant 4$. □

Remark 3. The results from [4,9] quoted in the introductory comments both give upper bounds for the number of solutions $(x, y) \in \mathbb{F}_p^* \times \mathbb{F}_p^*$ of $x^n - y^n = a$, for p a prime, $a \in \mathbb{F}_p^*$ and n a divisor of $p - 1$. In particular, the special case $T = 1$ of [4, Lemma 5] implies that there is a constant c such that the number of solutions is at most $cn^{4/3}(p-1)^{2/3}$ if $n^4 \geqslant p - 1$. An acceptable value for c which follows from their proof is $4/(\sqrt{3} - 1)$. Our attempts to improve on this constant by refining their estimates could not attain values lower than $2^{5/3}$, which is larger than 3.

Mit'kin's result in [9] is that the number of solutions is at most $2n^{4/3}(p-1)^{2/3}$ if $n^4 > 8(p-1)$. Although his method is very different from that of [3], Mit'kin also establishes a family of bounds for the number of solutions divided by n^2, which are linear in $k = (p-1)/n$ (like those of Garcia and Voloch summarized in Eq. (2)), and then concludes by selecting the best of those for a given value of k. However, Mit'kin's family of bounds depends on three parameters rather than one, and it seems not possible to individually match them with those of Garcia and Voloch. The constant 2 in Mit'kin's final bound appears to be the best which can be attained by his method; in fact, the stated purpose of Lemma 1 in [9] is to prove the bound with the constant 2 rather than just $2 + \varepsilon$ for some $\varepsilon > 0$.

Acknowledgment

The author is grateful to Ministero dell'Istruzione, dell'Università e della Ricerca, Italy, for financial support of the project "Graded Lie algebras and pro-p-groups of finite width."

References

[1] Davenport, Hasse, Die Nullstellen der Kongruenz Zetafunktion in gewissen zyklischen Fällen, J. Reine Angew. Math. 172 (1935) 151–182.
[2] Walter Feit, Characters of Finite Groups, Benjamin, New York, 1967. MR MR0219636 (36 #2715).
[3] A. García, J.F. Voloch, Fermat curves over finite fields, J. Number Theory 30 (3) (1988) 345–356. MR MR966097 (90a:14027).
[4] D.R. Heath-Brown, S. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, Q. J. Math. 51 (2) (2000) 221–235. MR MR1765792 (2001h:11106).
[5] Kenneth Ireland, Michael Rosen, A Classical Introduction to Modern Number Theory, second ed., Grad. Texts in Math., vol. 84, Springer-Verlag, New York, 1990. MR MR1070716 (92e:11001).

[6] Sergei V. Konyagin, Igor E. Shparlinski, Character Sums with Exponential Functions and Their Applications, Cambridge Tracts in Math., vol. 136, Cambridge Univ. Press, Cambridge, 1999. MR MR1725241 (2000h:11089).
[7] Rudolf Lidl, Harald Niederreiter, Finite Fields, Encyclopedia Math. Appl., vol. 20, Addison–Wesley, Reading, MA, 1983. With a foreword by P.M. Cohn. MR MR746963 (86c:11106).
[8] S. Mattarei, Fermat curves over finite fields and characters of nonabelian groups, submitted for publication.
[9] D.A. Mit'kin, On the number of rational points of a Fermat curve over a finite prime field, Chebyshevskiĭ Sb. 4 (3(7)) (2003) 83–91 (in Russian) (dedicated to the 75th birthday of Aleksandr Vasil'evich Malyshev). MR MR2051595 (2005d:11091).
[10] Charles Small, Arithmetic of Finite Fields, Monogr. Textbooks Pure Appl. Math., vol. 148, Dekker, New York, 1991. MR MR1186215 (93i:11144).