A Class of Fermat Curves for which Weil-Serre's Bound Can Be Improved

Francis N. Castro[1], Ernesto Gomez[2], and Oscar Moreno[3]

[1] Department of Mathematics, University of Puerto Rico, Rio Piedras
fcastro@goliath.cnnet.clu.edu
[2] Department of Computer Science,
California State University, San Bernardino
egomez@csci.causb.edu
[3] Department of Computer Sciences,
University of Puerto Rico, Rio Piedras
moreno@uprr.pr

Abstract. In this paper we introduce the class of semiprimitive Fermat curves, for which Weil-Serre's bound can be improved using Moreno-Moreno p-adic techniques. The basis of the improvement is a technique for giving the exact divisibility for Fermat curves, by reducing the problem to a simple finite computation.

1 Summary of p-Adic Bounds for Curves

In this paper we are going to present new curves satisfying Theorem 1 below and using it we obtain our improved Weil-Serre's bound.

In the present section we recall how O. Moreno and C. Moreno combine Serre's techniques with the Moreno-Moreno improved Ax-Katz estimate (see [3])to produce a p-adic version of Serre's estimate. For Fermat curves considered here, we can formulate the best possible Moreno-Moreno type p-adic Serre Bound.

Let

$$aX^d + bY^d = cZ^d,\ (abc \neq 0) \tag{1}$$

be a Fermat curve over $\mathbb{F}_{p^f}$ and let $|N|$ be the number of affine points of $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{p^f}$. Note that the Fermat curves are nonsingular curves. Hence we can apply to them the Weil's Theorem.

Now we apply the p-adic estimate of [1] to the curve (1). Note that the genus of a Fermat equation is less than or equal to $(d-1)(d-2)/2$, where d is the degree of the Fermat equation.

Theorem 1. *Let $aX^d + bY^d = cZ^d$ be an equation over $\mathbb{F}_{p^f}$ and let μ be a positive integer satisfying $|N(\mathbb{F}_{p^{fm}})| \equiv 0 \bmod p^{\mu m}\ \forall\ m > 0$. Then the number of solutions $|\tilde{N}|$ of $aX^d + bY^d = cZ^d$ in $\mathbb{P}^2(\mathbb{F}_{p^{mf}})$ satisfies the following bound:*

$$\big|\,|\tilde{N}| - (p^{mf}+1)\big| \leq \frac{1}{2}(d-1)(d-2)p^{\mu m}[2p^{mf/2}p^{-\mu m}].$$

M. Fossorier et al. (Eds.): AAECC 2006, LNCS 3857, pp. 128–135, 2006.

Remark 1. Note that in order to obtain in the above theorem a non-trivial improvement, m and f must both be odd. That is the reason why throughout the paper, and in particular in Tables 1, 2 and 3, f and m are always odd.

Also note that in order to apply Theorem 1 we need curves where the divisibility grows upon extensions or $|N(\mathbb{F}_{p^{fm}})| \equiv 0 \bmod p^{\mu m} \ \forall \ m > 0$.

Remark 2. In general, it is difficult to find curves satisfying the property of divisibility of Theorem 1. This is to find curves $\mathcal{C}$ over $\mathbb{F}_q$ and $\mu > 0$ such that $p^{m\,\mu}$ divides the number of rational points of $\mathcal{C}$ over $\mathbb{F}_{q^m}$ for $m = 1, 2 \ldots$ (Artin-Schreier's curves satisfy this property.).

In the following section we are going to present new families of curves satisfying Remark 2. Hence we obtain an improved p-adic bound for their number of rational points.

2 Divisibility of Fermat Curves

In this section we are going to reduce the estimation of the divisibility of Fermat curves to a computational problem. Let $|N|$ be the number of solutions of the Fermat curve $aX^d + bY^d = cZ^d$ over the finite field $\mathbb{F}_{p^f}$. Note that that if $(p^f - 1, d) = k$, then the number of solutions of $aX^d + bY^d = cZ^d$ is equal to the number of solutions of $aX^k + bY^k = cZ^k$ over $\mathbb{F}_{p^f}$. Hence, we assume that d divides $p^f - 1$.

Let n be a positive integer $n = a_0 + a_1 p + a_2 p^2 + \cdots + a_l p^l$ where $0 \leq a_i < p$ we define the p-weight of n by $\sigma_p(n) = \sum_{i=0}^{l} a_i$.

Following the techniques of [3, Theorem 22], we associate to equation (1) the following system of modular equations:

$$\begin{aligned} dj_1 &\equiv 0 \bmod p^f - 1 \\ dj_2 &\equiv 0 \bmod p^f - 1 \\ dj_3 &\equiv 0 \bmod p^f - 1 \\ j_1 + j_2 + j_3 &\equiv 0 \bmod p^f - 1, \end{aligned} \tag{2}$$

where $1 \leq j_1, j_2, j_3 \leq q - 1$.

This modular system of equations determines the p-divisibility of $|N|$, i.e., if

$$\mu = \min_{\substack{(j_1, j_2, j_3) \\ is\ solution\ of\ (2)}} \left\{ \frac{\sigma_p(j_1) + \sigma_p(j_2) + \sigma_p(j_3)}{p - 1} \right\} - f, \tag{3}$$

then p^μ divides $|N|$. This implies that any solution of the modular equation $dj_i \equiv 0 \bmod p^f - 1$ is of the form $c_i \cdot \frac{p^f - 1}{d}$ where $1 \leq c_i \leq d$. We are going to use the following results of [3]: for any positive integer k

$$\sigma_p((p^f - 1)k) \geq \sigma_p(p^f - 1) = (p - 1)f. \tag{4}$$

Now we state one of the main theorem of [3, Theorem 25],

Theorem 2. *Consider the family of polynomial equations:*

$$\mathcal{G} = \{aX^d + bY^d = cZ^d \,|\, a, b, c \in \mathbb{F}_{p^f}^{\times}\}.$$

Then there exists a polynomial $G \in \mathcal{G}$ such that the number of solutions of G is divisible by p^μ but not divisible by $p^{\mu+1}$, where μ is defined in (3).

Now we consider 3-tuples $(c_1, c_2, c_3) \in \mathbf{N}^3$ satisfying:

$$\frac{c_1}{d} + \frac{c_2}{d} + \frac{c_3}{d} \tag{5}$$

is a positive integer, where $1 \leq c_i \leq d$. The following Lemma gives a simpler way to compute μ of (3).

Lemma 1. *Let $q = p^f$ and d be a divisor of $q - 1$. Let $aX^d + bY^d = cZ^d$ be a polynomial over $\mathbb{F}_q$. Then μ defined in (3) satisfies*

$$\mu = \min_{\substack{(c_1,c_2,c_3) \\ \text{satisfies (5)}}} \frac{\sum_{i=1}^{3} \sigma_p(c_i(q-1)/d)}{p-1} - f. \tag{6}$$

Proof. We know that the solutions of (2) are of the form $(c_1(p^f - 1)/d, c_2(p^f - 1)/d, c_3(p^f - 1)/d)$. We obtain from the last congruence of (2) the following:

$$\frac{c_1(p^f-1)}{d} + \frac{c_2(p^f-1)}{d} + \frac{c_3(p^f-1)}{d} = (\frac{c_1}{d} + \frac{c_2}{d} + \frac{c_3}{d})(p^f - 1) = k(p^f - 1).$$

Therefore $\frac{c_1}{d} + \frac{c_2}{d} + \frac{c_3}{d}$ is positive integer.

The following Lemma is the one that allows us to apply Theorem 1.

Lemma 2. *Let q be power of a prime and d divides $q-1$. Then $\sigma_p(c(q^m-1)/d) = m\,\sigma_p(c(q-1)/d)$, where $1 \leq c \leq d-1$.*

Proof. Note that $c(q^m - 1) = c(q - 1)(q^{m-1} + \cdots + q + 1)$. Hence

$$\begin{aligned}\sigma_p(c(q^m-1)/d) &= \sigma_p(c\tfrac{q-1}{d}(q^{m-1} + \cdots + q + 1)) \\ &= m\,\sigma_p(\tfrac{c(q-1)}{d})\end{aligned}$$

Combining the above two lemmas, we obtain the following proposition.

Proposition 1. *Let $q = p^f$ and d be a divisor of $q-1$. Let $aX^d + bY^d = cZ^d$ be a polynomial over $\mathbb{F}_{q^m}$. Then μ defined in (3) satisfies*

$$\mu = (\min_{\substack{(c_1,c_2,c_3) \\ \text{satisfies (5)}}} \frac{\sum_{i=1}^{3} \sigma_p(c_i(q^m-1)/d)}{p-1} - f) = m(\min_{\substack{(c_1,c_2,c_3) \\ \text{satisfies (5)}}} \frac{\sum_{i=1}^{3} \sigma_p(c_i(q-1)/d)}{p-1} - f).$$

Remark 3. Note that using Proposition 1, we only need to do one computation to estimate the divisibility of (1), the smallest $q-1$ such that d divides $q-1$. Consequently we have reduced the problem of finding the divisibility of Fermat Curves to a finite computation. Proposition 1 gives the exact divisibility in the sense that there are coefficients a', b', c' in $\mathbb{F}_{q^m}$ such that the number of solutions of $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{q^m}$ is divisible by p^μ but not by $p^{\mu+1}$. In some sense this theorem completely solves the problem of divisibility for Fermat curves. Furthermore, the property of Lemma 1 is very important since from it we obtain a best possible Moreno-Moreno's p-adic Serre bound (see Theorem 1).

Our next theorem shows how or system of modular equations (2) can in some cases be reduced to a single equation. This considerably lowers the complexity of our computational problem.

Proposition 2. *Let d be a divisor of p^f-1. Consider the diagonal equation $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{p^{mf}}$. Let*

$$\lambda = \min_{1\le c\le d-1} \sigma_p(c(p^f-1)/d).$$

Then $p^{(\frac{3\lambda}{p-1}-f)m}$ divides the number of solutions of $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{p^{fm}}$.

Proof. Note that if $\sigma_p(c(p^f-1)/d) \ge \lambda$ for $1 \le c \le d$. Then $\sigma_p(j_1) + \sigma_2(j_2) + \sigma(j_3) \ge 3\lambda$.

Remark 4. In many cases we have that $\min_{1\le c\le d-1} \sigma_p(c(p^f-1)/d) = \sigma_p((p^f-1)/d)$.

Example 1. Let $d = 23$ and $\mathbb{F}_{2^f} = \mathbb{F}_{2^{11}}$. In this case we compute

$$\min_{1\le c\le 22} \sigma_2(c(2^{11}-1)/23).$$

We have that $\sigma_2(c(2^{11}-1)/23) = 4$ for $c \in \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$. Hence $\min_{1\le c_i\le 22} \sigma_2(c_1(2^{11}-1)/23) + \sigma_2(c_2(2^{11}-1)/23)) + \sigma_2(c_2(2^{11}-1)/23)) = 12$ since $c_1 = 1, c_2 = 4$ and $c_3 = 18$ gives a solution of (5). Applying Proposition 1 and Theorem 2, we obtain the best divisibility for the families curves $\mathcal{G} = \{aX^{23} + bY^{23} = cZ^{23} \,|\, a, b, c \in \mathbb{F}^\times_{2^{11m}}\}$. Hence there is an equation $a_0X^{23} + b_0Y^{23} = c_0Z^{23} \in \mathcal{G}$ with exact divisibility 2^m.

Example 2. Let $d = 151$ and $\mathbb{F}_{2^f} = \mathbb{F}_{2^{15}}$. In this case we compute

$$\min_{1\le c\le 150} \sigma_2(c(2^{15}-1)/151).$$

We have that $\sigma_2(c(2^{15}-1)/151) = 5$. Hence $\min_{1\le c_i\le 150} \sigma_2(c_1(2^{15}-1)/151) + \sigma_2(c_2(2^{15}-1)/151)) + \sigma_2(c_2(2^{15}-1)/151)) = 15$ since $c_1 = 57, c_2 = 19$ and $c_3 = 4(\sigma_2(c_i(2^{15}-1)/151) = 5$ for $i = 1, 2, 3)$ gives a solution of (5). Applying Proposition 1 and Theorem 2, we obtain the best divisibility for the families curves $\mathcal{G} = \{aX^{151} + bY^{151} = cZ^{151} \,|\, a, b, c \in \mathbb{F}^\times_{2^{15m}}\}$. Hence there is an equation $a_0X^{151} + b_0Y^{151} = c_0Z^{151} \in \mathcal{G}$ where 2 does not divide its number of solutions over $\mathbb{F}_{2^{15m}}$.

Example 3. Let $d = 23^2 = 529$ and $\mathbb{F}_{2^f} = \mathbb{F}_{2^{253}}$ (The first finite field of characteristic 2 satisfying that 529 divides $2^f - 1$ is $\mathbb{F}_{2^{253}}$). In this case we compute

$$\min_{1 \leq c \leq 528} \sigma_2(c(2^{253} - 1)/529).$$

We have that $\sigma_2(c(2^{253} - 1)/151) = 92$. We have that $\sigma_2(c(2^{253} - 1)/529) = 92$ for

$$c \in \{23, 46, 69, 92, 138, 184, 207, 276, 299, 368, 414, 500\}.$$

Hence $\min_{1 \leq c_i \leq 529} \sigma_2(c_1(2^{253} - 1)/529) + \sigma_2(c_2(2^{253} - 1)/529)) + \sigma_2(c_2(2^{253} - 1)/259)) = 276$ since $c_1 = 23, c_2 = 92$ and $c_3 = 414(\sigma_2(c_i(2^{253} - 1)/529) = 5$ for $i = 1, 2, 3)$ gives a solution of (5). Applying Proposition 1 and Theorem 2, we obtain the best divisibility for the families curves $\mathcal{G} = \{aX^{529} + bY^{529} = cZ^{529} \mid a, b, c \in \mathbb{F}^{\times}_{2^{253m}}\}$. Hence there is an equation $a_0X^{529} + b_0Y^{529} = c_0Z^{529} \in \mathcal{G}$ with exact divisibility 2^{23m}.

Example 3 is an example where $\min_{1 \leq c \leq d-1} \sigma_p(c(p^f - 1)/d) \neq \sigma_p((p^f - 1)/d)$. Also note that in Example 3 we computed μ for a large finite field.

3 Tables

In the following tables, we are going to calculate μ for the curves $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{p^f}$,where f is odd, in order to apply Theorem 1.

In Table 1 we compute μ for the first f such that d divides $2^f - 1$. Recall that if we know μ for the first f such that d divides $2^f - 1$, the we know μ for all the extensions of $\mathbb{F}_{2^f}$ (see Proposition 1). Note that we can assume that d is odd since the characteristic of $\mathbb{F}_{2^f}$ is 2.

Table 1. Best Divisibility of $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{2^f}$

d	smallest f such that d divides $2^f - 1$.	μ
23	11	1
47	23	4
71	35	7
529	253	23

Table 2. Best Divisibility of $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{3^f}$

d	smallest f such that d divides $3^f - 1$.	μ
11	5	1
23	11	1
46	11	1
47	23	4
59	29	10

In Table 2 we compute μ for the first f such that d divides $3^f - 1$. Recall that if we know μ for the first f such that d divides $3^f - 1$, then we know μ for all the extensions of $\mathbb{F}_{3^f}$ (see Proposition 1). Note that we can assume that d is not divisible by 3 since the characteristic of $\mathbb{F}_{3^f}$ is 3.

Theorem 3. *Let $aX^d + bY^d = cZ^d$ be a Fermat curve of the tables. Then $aX^d + bY^d = cZ^d$ satisfies Theorem 1, where μ is given by the table.*

4 Semiprimitive Fermat Curves

In this section we obtain a general family of Fermat curves satisfying Theorem 1, generalizing the results of Tables 1,2,3.

Now we are going to consider odd primes l for which p is of order exactly $(l-1)/2$, i.e., the smallest positive integer k for which $p^k \equiv 0 \bmod l$. We call p a semiprimitive root for such l. Note that 2 is a semiprimitive root for $l = 7, 23, 47, 71$. We would obtain a new family of Fermat curves that satisfy Theorem 1.

Let $g(j)$ be the Gauss sum defined by:

$$g(j) = \sum_{x \in \mathbb{F}_q^\times} \chi^{-j}(x)\psi(x),$$

where χ is multiplicative character of order $q-1$ and ψ is an additive character of $\mathbb{F}_q$. In [2], Moreno-Moreno proved that

$$S(l) = \sum_{x \in \mathbb{F}_q} (-1)^{Tr(x^l)} = \frac{l-1}{2}\{g(\frac{q-1}{l}) + g(q-1-\frac{q-1}{l})\}. \tag{7}$$

This implies that 2^λ divides $S(l)$, where $l = \min\{\sigma_2((q-1)/l), \sigma_2((q-1)-((q-1)/l))\}$. They proved the above identity for finite fields of characteristic 2. The proof for arbitrary characteristic follows from their proof using $g(j) = g(p^a j)$.

Table 3. Best Divisibility of $aX^d + bY^d = cZ^d$ over $\mathbb{F}_{p^f}$

d	smallest f such that d divides $p^f - 1$.	μ
11	$\mathbb{F}_{5^5}$	1
38	$\mathbb{F}_{5^9}$	2
20	$\mathbb{F}_{7^7}$	2
31	$\mathbb{F}_{7^{15}}$	3
37	$\mathbb{F}_{7^9}$	3
58	$\mathbb{F}_{7^7}$	1
43	$\mathbb{F}_{11^7}$	2
23	$\mathbb{F}_{13^{11}}$	1
46	$\mathbb{F}_{13^{11}}$	1
53	$\mathbb{F}_{13^{53}}$	5
19	$\mathbb{F}_{17^9}$	3
38	$\mathbb{F}_{19^9}$	2

Lemma 3. *Let $q = p^{(l-1)/2}$ and let p be a prime for which p is a semiprimitive root for l. Given $aX^l + bY^l = cZ^l$ over $\mathbb{F}_{q^m}$, the μ of (3) is such that $\mu > 0$, whenever 3 does not divide $(l-1)(p-1)/2$.*

Proof. Using Proposition 1, we need only estimates μ of (3) for the finite field $\mathbb{F}_q$. Let $f = (l-1)/2$. First we consider the solutions of $aX^l + bY^l = cZ^l$ over $\mathbb{F}_q$. We have the following modular system associated to $aX^l + bY^l = cZ^l$:

$$\begin{aligned} lj_1 &\equiv 0 \bmod q-1 \\ lj_2 &\equiv 0 \bmod q-1 \\ lj_3 &\equiv 0 \bmod q-1 \\ j_1 + j_2 + j_3 &\equiv 0 \bmod q-1 \end{aligned} \tag{8}$$

By the identity (7), we have that $\sigma_2(c(q-1)/l)) = \sigma_2((q-1)/l)$ or $\sigma_2(q - 1 - ((q-1)/l))$. Note that $\sigma_2((q-1)/l) + \sigma_2(q-1-((q-1)/l)) = f(p-1)$. If $\sigma_2(j_{k_1}) \neq \sigma_2(j_{k_2})$, then $\sigma_2(j_{k_1}) + \sigma_2(j_{k_2}) + \sigma_2(j_{k_3}) > (p-1)f$. Hence we can assume that the minimal solution of (8) satisfies $\sigma_2(j_1) = \sigma_2(j_2) = \sigma_2(j_3)$. Applying the function σ_2 to the last modular equation of (8), we obtain $\sigma_2(j_1) + \sigma_2(j_2) + \sigma_2(j_3) \geq f(p-1)$. Therefore

$$\mu = \min \sigma_2(j_1) + \sigma_2(j_2) + \sigma_2(j_3) = 3 \min \sigma_2(j_1) \geq f(p-1).$$

Hence $\mu \geq 1$ whenever 3 does not divide $(l-1)(p-1)/2$. Hence at least p^μ divides $|N(\mathbb{F}_q)|$. Then by Lemma 2, we obtain that $p^{\mu m}$ divides $|N(\mathbb{F}_{q^m})|$.

Now we state a p-adic Serre bound for the Fermat curves of Lemma 3.

Theorem 4. *Let $q = p^{(l-1)/2}$ and let l be an odd prime for which p is a semiprimitive root for l. Let μ be as defined in (3) for the curve $aX^l + bY^l = cZ^l$ over $\mathbb{F}_{q^m}$. Then*

$$||\tilde{N}| - (q^m + 1)| \leq \frac{(p-1)(p-2)}{2} p^{\mu m}[q^{m/2} p^{1-\mu m}],$$

whenever 3 does not divide $(l-1)(p-1)/2$.

Futhermore, we have $\mu \geq 1$ by Lemma 3 .

Proof. Combining Lemma 3 and Theorem 1, we obtain the result.

We apply Theorem 4 to some semiprimitive primes.

Example 4. Note 2 is a semiprimitive root for 23 and $\mu = 1$. Applying Theorem 4, we obtain

$$||\tilde{N}| - (2^{11m} + 1)| \leq 231 \times 2^m [2^{(9m+2)/2}].$$

Example 5. Note 2 is a semiprimitive root for 47 and $\mu = 4$. Applying Theorem 4, we obtain

$$||\tilde{N}| - (2^{23m} + 1)| \leq 1035 \times 2^{4m} [2^{(15m+2)/2}].$$

In particular, for the finite field $\mathbb{F}_{2^{69}}$, Serre improvement to Weil's bound gives $1035 \times [2 \times 2^{69/2}] = 50292728269650$ and our improvement gives $1035 \times 2^{12} \times [2^{47/2}] = 50292727418880$.

Example 6. Note 2 is a semiprimitive root for 71 and $\mu = 7$. Applying Theorem 4, we obtain

$$||\tilde{N}| - (2^{35m} + 1)| \leq 2415 \times 2^{7m}[2^{(21m+2)/2}].$$

Remark 5. Using our computations of Table 1 we have obtained the above best bounds. Notice that each example of μ gives a family of bounds.

5 Conclusion

The main result of this paper is obtaining a general class(the semiprimitive case presented in the last section) of Fermat curves for which Weil-Serre's bound can be improved using Moreno-Moreno p-adic techniques. We also prove that for each particular case, the best bound μ is computed in a simple computation which is presented in the second section.

Acknowledgment

We would like to thank the referee for his careful reading and for his generous suggestions that helped improved the paper considerably.

References

1. O. Moreno and C. J. Moreno, A p-adic Serre Bound, *Finite Fields and Their Applications,* **4:**(1998), pp. 241-244.
2. O. Moreno and C.J. Moreno, The MacWilliams-Sloane Conjecture on the Tightness of the Carlitz-Uchiyama Bound and the Weights of Duals of BCH Codes, *IEEE Trans. Inform. Theory*, **4:**6(1994), pp. 1894-1907.
3. O. Moreno, K. Shum, F. N. Castro and P.V. Kumar, Tight Bounds for Chevalley-Warning-Ax Type Estimates, with Improved Applications, *Proc. of the London Mathematical Society*, **4** (2004) pp. 201-217.