ACTA ARITHMETICA
XCVIII.2 (2001)

A construction of curves over finite fields

by

ARNALDO GARCIA and LUCIANE QUOOS (Rio de Janeiro)

1. Introduction. The theory of equations over finite fields is a basic topic in classical number theory. In this theory the congruences of the form

$$y^2 \equiv f(x) \quad \text{(modulo a prime number)},$$

where $f(x)$ is a polynomial or a quotient of polynomials with integer coefficients, were one of the first objects of study. Assuming an analogue of Riemann's hypothesis for the zeta function that he had introduced, E. Artin conjectured an upper bound for the number N of solutions of such congruences.

A celebrated theorem of A. Weil proving, in particular, the conjecture of E. Artin says: Let $\mathcal{X}$ be a nonsingular, projective, geometrically irreducible algebraic curve of genus g defined over a finite field $\mathbb{F}_q$. Then the number $N := \#\mathcal{X}(\mathbb{F}_q)$ of $\mathbb{F}_q$-rational points of $\mathcal{X}$ satisfies

$$|N - (q+1)| \le 2g\sqrt{q}.$$

The particular case of elliptic curves (i.e., $g = 1$) was first proved by H. Hasse.

Particularly interesting is the case of *maximal curves*, i.e., curves $\mathcal{X}$ over $\mathbb{F}_q$, with q a square, attaining the Hasse–Weil upper bound:

$$N = q + 1 + 2g\sqrt{q}.$$

According to Ihara [I], the genus g of a maximal curve over $\mathbb{F}_q$ satisfies

$$g \le \sqrt{q}(\sqrt{q} - 1)/2.$$

In this same paper [I], the following upper bound is also shown for $N := \#\mathcal{X}(\mathbb{F}_q)$:

$$N \le q + 1 + (\sqrt{(8q+1)g^2 + 4(q^2 - q)g} - g)/2.$$

2000 *Mathematics Subject Classification*: 11G20, 14G15, 14Hxx.

Both authors were partially supported by CNPq (Brazil) and the first author was also partially supported by PRONEX # 41.96.0883.00.

The interest in curves over finite fields with many rational points (i.e., with the number N close to known upper bounds) was renewed after Goppa's construction of linear codes with good parameters from such curves (see [Go]). Other applications are: estimates of exponential sums over finite fields, finite geometries and sequences with low discrepancy (see [Mo], [Hi] and [Li-Ni]).

The aim of this paper is to introduce an effective method for the construction of curves over finite fields with many rational points. The method is motivated by a recent paper of van der Geer and van der Vlugt [G-V]. In our method we assign a curve $\mathcal{X}$ over $\mathbb{F}_{q^n}$ to each polynomial $g(x) \in \mathbb{F}_{q^n}[x]$ with $\deg(g(x)) \geq q^n$ and this curve $\mathcal{X}$ quite frequently has many rational points over $\mathbb{F}_{q^n}$. This is done by introducing a reduced polynomial $R(g(x))$ and then considering the curve $\mathcal{X}$ given by the Kummer extension of the type

$$(1.1) \qquad y^m = \frac{g(x)}{R(g(x))}, \quad m \text{ a divisor of } q^n - 1.$$

We illustrate the method with several examples and some of the constructed curves $\mathcal{X}$ are really good (i.e., the number of rational points of $\mathcal{X}$ over the finite field in question is strictly greater than the previously known largest number for a curve of the same genus). In the last section we apply the method of [G-V] to certain polynomials from [G-S] and we get some other examples of curves with many rational points.

We refer to Section III.7 of [S] for the theory of Kummer extensions of function fields over finite fields (see also [H]).

2. The construction.

For a polynomial $g(x) \in \mathbb{F}_l[x]$ of degree greater than or equal to l, we define the *associated reduced polynomial* $R(g(x))$ as the polynomial of degree $\leq l-1$ obtained from $g(x)$ by operating on its monomials as follows:

- $R(x^j) = x^j$ for all $j \leq l-1$.
- $R(x^{l+j}) = R(x^{1+j})$ for all $j \geq 0$.

For example,

$$R(x^{2l-1}) = R(x^{l+l-1}) = R(x^{1+l-1}) = R(x^l) = R(x) = x,$$
$$R(x^{2l-2}) = R(x^{l+l-2}) = R(x^{1+l-2}) = R(x^{l-1}) = x^{l-1}.$$

More generally, one can easily show that $R(x^m) = x^n$ if $m \equiv n \pmod{(l-1)}$ and $1 \leq n \leq l-1$. Note that by the definition of R, for every $\alpha \in \mathbb{F}_l$ we have

$$g(x)(\alpha) = 0 \quad \text{if and only if} \quad R(g(x))(\alpha) = 0.$$

Remark 1. The main property of the right hand side of (1.1) is the following:

$$\frac{g(x)}{R(g(x))}(\alpha) = 1 \quad \text{for all } \alpha \in \mathbb{F}_l \text{ with } g(x)(\alpha) \neq 0.$$

Hence the curves $\mathcal{X}$ over $\mathbb{F}_l$ given by

$$y^m = \frac{g(x)}{R(g(x))} \quad \text{with } m \text{ a divisor of } l-1, \tag{2.1}$$

are such that the number N of rational points over $\mathbb{F}_l$ satisfies

$$N \geq m \cdot \#\{\alpha \in \mathbb{F}_l \mid g(x)(\alpha) \neq 0\}.$$

The exact value for N is obtained after analyzing the rationality of the points with first coordinate $x = \infty$ or $x = \alpha$, with $\alpha \in \mathbb{F}_l$ satisfying $g(x)(\alpha) = 0$. We will always take

$$g(x) = f(x)^r \quad \text{for some polynomial } f(x) \text{ and some } r \geq 2.$$

This is done with the objective that the curve $\mathcal{X}$ given by (2.1) has "low genus".

Hence the curves $\mathcal{X}$ we will be considering here (over the finite field $\mathbb{F}_l$ with l elements) are of the type

$$y^m = \frac{f(x)^r}{R(f(x)^r)} \quad \text{with } r \geq 2 \text{ and } m \text{ a divisor of } l-1. \tag{2.2}$$

It will always be the case, in the examples considered here, that in the function field extension $\mathbb{F}_l(x,y)|\mathbb{F}_l(x)$, given by (2.2), there is a fully ramified place and hence it follows that equation (2.2) is indeed absolutely irreducible (see Corollary III.7.4 of [S]).

In the next theorem we write $l = q^n$ and we denote by $\overline{\mathbb{F}}_q$ the algebraic closure of $\mathbb{F}_q$.

Theorem 2.1. *Let $f(x) \in \mathbb{F}_{q^n}[x]$ be a separable polynomial and let q^j be a power of the characteristic such that $q^j \cdot \deg(f) \geq q^n$. Suppose that the reduced polynomial $R(f(x)^{q^j})$ is also separable and that the curve $\mathcal{X}$ given by*

$$y^m = \frac{f(x)^{q^j}}{R(f(x)^{q^j})}, \quad m \text{ a divisor of } q^n - 1,$$

is absolutely irreducible. Then the genus g and the number N of rational points of the curve $\mathcal{X}$ over $\mathbb{F}_{q^n}$ satisfy

$$2g = (\delta + \delta' - 2c - 2)(m-1) + c(m-d) + (m-d') \quad \text{and} \quad N \geq (q^n - c_1)m,$$

where $\delta = \deg(f(x))$, $\delta' = \deg(R(f(x)^{q^j}))$, $d = \gcd(m, q^j - 1)$, $d' =$

$\gcd(m, q^j \cdot \delta - \delta')$ *and moreover* $c_1 \le c$ *are given by*

$$c_1 = \#\{\alpha \in \mathbb{F}_{q^n} \mid f(x)(\alpha) = 0\},$$
$$c = \#\{\alpha \in \overline{\mathbb{F}}_q \mid f(x)(\alpha) = R(f(x)^{q^j})(\alpha) = 0\}.$$

Proof. The assertion on g follows from the Riemann–Hurwitz formula applied to the extension $\mathbb{F}_{q^n}(x, y)|\mathbb{F}_{q^n}(x)$ of degree m. The assertion on N follows directly from Remark 1. ■

We end up this section with the only situation that we are going to consider here in which the exponent r in (2.2) is not a power of the characteristic p. We consider the curve $\mathcal{X}$ given by (2.2) with r being a divisor of $l - 1$ and with

$$f(x) = x(x^{(l-1)/r} - 1). \tag{2.3}$$

Assumption. We assume below that p is an odd prime, that $r^2 \le l - 1$ and that $x = 0$ is the unique multiple root of the polynomial $R(f(x)^r)$.

Because of the Assumption above, the multiplicity of $x = 0$ in $R(f(x)^r)$ is r if r is even, and $r + (l-1)/r$ if r is odd. Then the number S of nonrational roots (i.e., not belonging to $\mathbb{F}_l$) of the polynomial $R(f(x)^r)$ satisfies

$$S = \begin{cases} \dfrac{l-1}{r}(r-2) & \text{if } r \text{ is even,} \\ \dfrac{l-1}{r}(r-3) & \text{if } r \text{ is odd.} \end{cases}$$

In fact, note that the hypothesis $r^2 \le l - 1$ means that

$$R(f(x)^r) = f(x)^r - x^{l-1+r} + x^r.$$

In particular, $\deg(R(f(x)^r)) = l - 1 - \left(\frac{l-1}{r} - r\right)$.

Then the genus g of the curve $\mathcal{X}$ (given by (2.2), with $f(x)$ chosen as in (2.3) and satisfying the Assumption above) satisfies

$$2g = (m-1)(S-2) + \frac{l-1}{r}(m-d) + \delta_1(m-d'),$$

where $d = \gcd(m, r-1)$, $d' = \gcd(m, (l-1)/r)$, $\delta_1 = 1$ if r is even and $\delta_1 = 2$ if r is odd.

The number N of rational points over $\mathbb{F}_l$ on $\mathcal{X}$ is

$$N = \left(l - 1 - \frac{l-1}{r}\right)m + N_1 + N_0 + N_\infty,$$

where N_1 is the number of rational points with the first coordinate satisfying $x^{(l-1)/r} = 1$, N_0 is the number of rational points with $x = 0$ and N_∞ is the number of rational points with $x = \infty$.

A careful analysis gives the following possible values for N_1, N_0 and N_∞:

$$N_1 = \begin{cases} d(l-1)/r & \text{if } -r \text{ is a } d\text{-power,} \\ 0 & \text{otherwise,} \end{cases}$$

$$N_0 = \begin{cases} m & \text{if } r \text{ is even and } 2 \text{ is an } m\text{-power,} \\ d' & \text{if } r \text{ is odd and } -r \text{ is a } d'\text{-power,} \\ 0 & \text{otherwise,} \end{cases}$$

$$N_\infty = \begin{cases} d' & \text{if } -r \text{ is a } d'\text{-power,} \\ 0 & \text{otherwise.} \end{cases}$$

We omit the details.

Remark. Because of the Assumption above, the roots of $(x^{(l-1)/r} - 1)$ are zeros of multiplicity $r - 1$ for the rational function $f(x)^r/R(f(x)^r)$. Particularly interesting here seems to be the case when

$$d_1 = \gcd(r-1, l-1) > 1.$$

In this case, taking a divisor $m \geq 2$ of d_1, one sees that $d = m$; i.e., one does not have ramification in the extension $\mathbb{F}_l(x,y)|\mathbb{F}_l(x)$ over the points with $x^{(l-1)/r} = 1$.

3. Examples of curves with many rational points. In this section we are going to construct curves over $\mathbb{F}_{q^n}$ with many rational points by applying the method of the preceding section, with r being a power of q (say $r = q^j$) and with the polynomial $f(x)$ carefully chosen, so that both $f(x)$ and $R(f(x)^{q^j})$ have "low degrees". From the genus formula in Theorem 2.1, we see that one wants the sum $\delta + \delta'$ of their degrees to be small. All examples here will satisfy the hypotheses of Theorem 2.1.

Remark. When we say that a curve over $\mathbb{F}_{q^n}$ of genus g gives a *new record* (resp., *meets the record*), we mean that its number of rational points over the finite field is strictly greater than (resp., is equal to) the largest number previously known for curves of genus g. When we say that a curve over $\mathbb{F}_{q^n}$ of genus g *completes some table*, we mean that there was no entry on that table for the number N of rational points over the finite field and that we got a curve of genus g whose N satisfies:

• If $g < q^n$, then $N \geq \min\{N_1/\sqrt{2}, N_2/\sqrt{2}\}$, where $N_1 = q^n + 1 + g[2\sqrt{q^n}]$ is Serre's bound and $N_2 = q^n + 1 + [(\sqrt{(8q^n+1)g^2 + 4(q^{2n} - q^n)g} - g)/2]$ is Ihara's bound.

• If $g \geq q^n$, then $N/g \geq \sqrt{q^n} - 1$, where $\sqrt{q^n} - 1$ is the Drinfeld–Vladut bound.

The tables that we are going to use here are:

1. For $p = 2$ or $p = 3$, the table from Geer–Vlugt [Ge-Vl].
2. For $p = 5$, the table from Shabat [Sh].

3.1. *Curves over* $\mathbb{F}_{q^2}$

Example 1. Consider the curve

$$y^m = \frac{(x^{q+1}+x+1)^q}{x^{q+1}+x^q+1} \quad \text{with } m \text{ a divisor of } q^2-1.$$

The common roots of the numerator and denominator belong to $\mathbb{F}_q$ and satisfy $x^2+x+1=0$. We then have three cases to consider. We write $d := \gcd(m, q-1)$.

Case 1. If $q \equiv 1 \pmod 3$, then $c = c_1 = 2$. Hence

$$g = (q-2)(m-1) + (m-d)$$

and

$$N = \begin{cases} (q^2-1)m & \text{if } (q-1)/d \not\equiv 0 \pmod 3, \\ (q^2-1)m + 2d & \text{if } (q-1)/d \equiv 0 \pmod 3. \end{cases}$$

Case 2. If $q \equiv 0 \pmod 3$, then $c = c_1 = 1$. Hence

$$g = (q-1)(m-1) + (m-d)/2 \quad \text{and} \quad N = q^2m + d.$$

Case 3. If $q \equiv 2 \pmod 3$, then $c = c_1 = 0$. Hence

$$g = q(m-1) \quad \text{and} \quad N = (q^2+1)m.$$

From this example we have the following tables (concerning the first table below, the former record was a curve with 64 rational points):

New record

Finite field	m	g	N
$\mathbb{F}_9$	8	17	74

Complete the table

Finite field	m	g	N
$\mathbb{F}_{25}$	6	25	156
$\mathbb{F}_{25}$	8	35	208

Meet the record

Finite field	m	g	N
$\mathbb{F}_4$	3	4	15
$\mathbb{F}_{16}$	3	4	45
$\mathbb{F}_{16}$	15	40	225
$\mathbb{F}_9$	2	2	20

Example 2. Suppose that $p \neq 2$ and consider

$$y^m = \frac{(x^{q+1}+x-1)^q}{x^{q+1}+x^q-1} \quad \text{with } m \text{ a divisor of } q^2-1.$$

The common roots of the numerator and denominator are exactly the elements α in $\mathbb{F}_q$ satisfying $\alpha^2+\alpha-1=0$. Hence, if $p \neq 5$ and q is a square or if $p \equiv \pm 1 \pmod 5$, we get $c = c_1 = 2$. Hence

$$g = (q-2)(m-1) + (m-d) \quad \text{with } d = \gcd(m, q-1).$$

Denoting by $O(\alpha)$ the order of the element α in $\mathbb{F}_q^*$ with $\alpha^2+\alpha-1=0$, we see that the number N of rational points over $\mathbb{F}_{q^2}$ is

$$N = \begin{cases} (q^2-1)m + 2d & \text{if } O(\alpha) \text{ divides } 4(q-1)/d, \\ (q^2-1)m & \text{otherwise.} \end{cases}$$

For example, if $p = 3$ and q is a square, then $O(\alpha) = 8$ and we get $2d$ extra rational points if $(q-1)/d$ is even. Hence for $q = 9$ and $m = 2$ we get a curve over $\mathbb{F}_{81}$ with $g = 7$ and $N = 164$, which is a new record. The former record was a curve with 160 rational points.

New record

Finite field	m	g	N
$\mathbb{F}_{81}$	2	7	164

Example 3. Let $p \neq 2$, $q \geq 5$ and choose $\alpha \in \mathbb{F}_q^* \setminus \{\pm 1\}$. We consider the curve

$$y^m = \frac{(x^{q+1} + x^q - x - \alpha^2)^q}{x^{q+1} + x - x^q - \alpha^2} \quad \text{with } m \text{ a divisor of } q^2 - 1.$$

The only common roots of the numerator and denominator are $x = \pm\alpha$, hence $c = c_1 = 2$. The genus is then

$$g = (q-2)(m-1) + (m-d) \quad \text{with } d = \gcd(m, q-1).$$

It is possible to choose α in $\mathbb{F}_q$ such that $\left(\frac{\alpha-1}{\alpha+1}\right)^{2(q-1)/d} = 1$, and for this choice of α we get

$$N = (q^2-1)m + 2d.$$

The condition on α above is just to make sure that the $2d$ points above $x = \pm\alpha$ are indeed rational points over $\mathbb{F}_{q^2}$.

This example produces the next table:

Complete the tables

Finite field	m	g	N
$\mathbb{F}_{81}$	8	49	656
$\mathbb{F}_{25}$	2	3	52
$\mathbb{F}_{25}$	4	9	104
$\mathbb{F}_{25}$	6	19	148
$\mathbb{F}_{25}$	8	25	200

Remark. There exists a curve of genus 3 over $\mathbb{F}_{25}$ with 56 rational points (see Theorem 5.1 of [G-S-X]).

Example 4. Suppose that $p \geq 2$ and consider

$$y^m = \frac{(x^q + x + \alpha)^q}{x^q + x + \alpha^q} \quad \text{with } \alpha \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q \text{ and } m \mid (q^2 - 1).$$

We have $c = c_1 = 0$ and $\delta = \delta' = q$, hence

$$g = (q-1)(m-1) + (m-d)/2 \quad \text{with } d = \gcd(m, q-1).$$

The number N of rational points over $\mathbb{F}_{q^2}$ is

$$N = q^2 m + d.$$

So we get the following tables (concerning the first table below, the former record was a curve with 101 rational points):

New record

Finite field	m	g	N
$\mathbb{F}_{25}$	4	12	104

Complete the tables

Finite field	m	g	N
$\mathbb{F}_{16}$	15	48	243
$\mathbb{F}_{25}$	8	30	204
$\mathbb{F}_{25}$	12	48	304

Meets the record

Finite field	m	g	N
$\mathbb{F}_9$	2	2	20

Remark. For $q = 9$ and for $m = 16, 20, 40$ or 80, Example 4 produces curves such that $N/g \geq \sqrt{q^2} = q = 9$.

Remark. In characteristic $p \geq 3$ the curves given by

$$y^m = \frac{(x^q - x + 1)^q}{x - x^q + 1} \quad \text{or} \quad y^m = \frac{(x^{q+1} + x^q - x)^q}{x^{q+1} + x - x^q},$$

with $m \mid (q^2 - 1)$, provide curves over $\mathbb{F}_{q^2}$ with the same genus and the same number of rational points as the curve in Example 4.

Example 5. Let m be a divisor of $q^2 - 1$, let $a \in \mathbb{F}_{q^2}^*$ and consider the curve

$$y^m = \frac{(x^q - ax)^q}{x - a^q x^q}.$$

There are two cases to consider.

Case 1. $a^{q+1} = 1$ and $\gcd(m, q-1) = 1$. In this case we have $c = c_1 = q$ and hence

$$g = (m-1)(q-1)/2 \quad \text{and} \quad N = (q^2 - q)m + (q+1).$$

Case 2. $a^{q+1} \neq 1$. In this case $c = c_1 = 1$ and hence

$$g = (q-2)(m-1) + (m-d) \qquad \text{with } d = \gcd(m, q-1).$$

The number N of rational points over $\mathbb{F}_{q^2}$ is

$$N = \begin{cases} (q^2-1)m & \text{if } d = q-1, \\ (q^2-1)m + 2d & \text{if } d < q-1 \text{ and } a^{(q^2-1)/d} = 1. \end{cases}$$

For $q = 9$ and $m = 2$ we get a curve of genus $g = 7$ with $N = 164$ rational points over $\mathbb{F}_{81}$, which is a new record (already obtained here in Example 2).

From this example we have the following tables:

Complete the tables

(all examples being from Case 2)

Finite field	m	g	N
$\mathbb{F}_{64}$	7	36	441
$\mathbb{F}_{25}$	2	3	52
$\mathbb{F}_{25}$	6	19	148
$\mathbb{F}_{25}$	8	25	192
$\mathbb{F}_{25}$	12	41	288

Meet the record

Finite field	m	g	N	Case
$\mathbb{F}_4$	3	1	9	1
$\mathbb{F}_{16}$	5	6	65	1
$\mathbb{F}_{16}$	3	4	45	2
$\mathbb{F}_{64}$	3	7	177	1
$\mathbb{F}_{64}$	9	28	513	1
$\mathbb{F}_9$	2	1	16	2
$\mathbb{F}_9$	4	5	32	2
$\mathbb{F}_9$	8	13	64	2
$\mathbb{F}_{81}$	5	16	370	1
$\mathbb{F}_{25}$	3	4	66	1

3.2. *Curves over* $\mathbb{F}_{q^3}$

Example 6. We consider the curve over $\mathbb{F}_{q^3}$ given by

$$y^m = \frac{(x^{q+1}+x+1)^{q^2}}{x^{q^2+1}+x^{q^2}+1} \quad \text{with } m \text{ a divisor of } q^3-1.$$

In this case $c = c_1 = q+1$, $\delta = q+1$ and $\delta' = q^2+1$. Hence

$$g = \frac{(q-2)(q+1)(m-1)+(q+1)(m-d)}{2} \quad \text{with } d = \gcd(m, q-1).$$

The number N of rational points over $\mathbb{F}_{q^3}$ is

$$N = \begin{cases} (q^3-q)m + (q+1)d & \text{if } p = 2, \\ (q^3-q)m + (q+1)d & \text{if } p \geq 3 \text{ and } (q-1)/d \text{ is even}, \\ (q^3-q)m & \text{if } p \geq 3 \text{ and } (q-1)/d \text{ is odd}. \end{cases}$$

Hence we get the tables below:

Complete the tables

Finite field	m	g	N
$\mathbb{F}_{64}$	7	45	425
$\mathbb{F}_{125}$	2	9	252

Meet the record

Finite field	m	g	N
$\mathbb{F}_8$	7	9	45
$\mathbb{F}_{27}$	2	2	48

Example 7. For $p \geq 3$ we consider the curve over $\mathbb{F}_{q^3}$ given by

$$y^m = \frac{-(x^q-x+1)^{q^2}}{x^{q^2}-x-1} \quad \text{with } m \text{ a divisor of } q^3-1.$$

For $p = 3$ we have $c = c_1 = q$ and for $p \geq 5$ we have $c = c_1 = 0$. Hence (with $d := \gcd(m, q-1)$)

$$2g = \begin{cases} (q-2)(q+1)(m-1)+(q+1)(m-d) & \text{if } p = 3, \\ (q+2)(q-1)(m-1)+(m-d) & \text{if } p \geq 5. \end{cases}$$

The number N of rational points over $\mathbb{F}_{q^3}$ equals

$$N = \begin{cases} (q^3-q)m+(q+1)d & \text{if } p=3 \text{ and } (q-1)/d \text{ is even,} \\ (q^3-q)m & \text{if } p=3 \text{ and } (q-1)/d \text{ is odd,} \\ q^3m+d & \text{if } p\geq 5 \text{ and } (q-1)/d \text{ is even,} \\ q^3m & \text{if } p\geq 5 \text{ and } (q-1)/d \text{ is odd.} \end{cases}$$

Remark. Note that Example 7 in characteristic $p=3$ has the same invariants g and N as in Example 6. In particular, for $q=3$ and $m=2$, we get again a curve over $\mathbb{F}_{27}$ with $g=2$ and $N=48$ rational points; i.e., a curve meeting the record.

Example 8. In characteristic $p\geq 3$ we consider the curve

$$y^m = \frac{(x^q+x)^{q^2}}{x^{q^2}+x} \quad \text{with } m \text{ a divisor of } q^3-1.$$

Then $x=0$ is the only common root for the numerator and denominator, and we have $c=c_1=1$, $\delta=q$ and $\delta'=q^2$. Hence for the genus g and the number N of rational points of $\mathbb{F}_{q^3}$ we get

$$\begin{aligned} g &= \frac{(q^2+q-4)(m-1)}{2}+(m-d), \\ N &= (q^3-1)m+2d \quad \text{with } d=\gcd(m,q-1). \end{aligned}$$

Remark. If one considers the curve in Example 8 in characteristic $p=2$, then one has $c=c_1=q$. This curve (for $p=2$) has the same invariants g and N as the curve in Example 6.

3.3. *Curves over* $\mathbb{F}_{q^n}$

Example 9. For an odd integer $n\geq 3$, we consider the curve over $\mathbb{F}_{q^n}$ given by

$$y^m = \frac{(x^{q^{(n+1)/2}}-x)^{q^{(n-1)/2}}}{x-x^{q^{(n-1)/2}}} \quad \text{with } m \text{ a divisor of } q^n-1.$$

The only common roots for the denominator and numerator are exactly the elements in $\mathbb{F}_q$. The genus equals

$$g = [(q^{(n+1)/2}+q^{(n-1)/2}-2q-2)(m-1)+(q+1)(m-d)]/2$$

with $d=\gcd(m,q-1)$. The number of rational points over $\mathbb{F}_{q^n}$ is

$$N = \begin{cases} (q^n-q)m+(q+1)d & \text{if } p=2, \\ (q^n-q)m+(q+1)d & \text{if } p\geq 3 \text{ and } (q-1)/d \text{ is even,} \\ (q^n-q)m & \text{if } p\geq 3 \text{ and } (q-1)/d \text{ is odd.} \end{cases}$$

This example produces the next tables:

Completes the table

Finite field	q	m	g	N
$\mathbb{F}_{125}$	5	2	9	252

Meet the record

Finite field	q	m	g	N
$\mathbb{F}_{8}$	2	7	9	45
$\mathbb{F}_{27}$	3	2	2	48

EXAMPLE 10. For an even integer $n \geq 4$, we consider the curve over $\mathbb{F}_{q^n}$ given by

$$y^m = \frac{(x^{q^{(n-2)/2}} - x)^{q^{(n+2)/2}}}{x - x^{q^{(n+2)/2}}} \qquad \text{with } m \text{ a divisor of } q^n - 1.$$

The common roots of the denominator and numerator are exactly all the elements in $\mathbb{F}_q$ if $n \equiv 0 \pmod 4$, or all the elements in $\mathbb{F}_{q^2}$ if $n \equiv 2 \pmod 4$. Hence

$$2g = \begin{cases} (q^{(n+2)/2} + q^{(n-2)/2} - 2q - 2)(m-1) + (q+1)(m-d) \\ \hfill \text{if } n \equiv 0 \pmod 4, \\ (q^{(n+2)/2} + q^{(n-2)/2} - 2q^2 - 2)(m-1) + (q^2+1)(m-d') \\ \hfill \text{if } n \equiv 2 \pmod 4, \end{cases}$$

where $d = \gcd(m, q-1)$ and $d' = \gcd(m, q^2-1)$. The number N of rational points over $\mathbb{F}_{q^n}$ satisfies

$$N = \begin{cases} (q^n - q)m + (q+1)d & \text{if } n \equiv 0 \pmod 4, \\ (q^n - q^2)m + (q^2+1)d' & \text{if } n \equiv 2 \pmod 4. \end{cases}$$

So we get the following table:

Meets the record

Finite field	q	m	g	N
$\mathbb{F}_{16}$	2	15	49	213

EXAMPLE 11. Suppose that n is an even integer and that m is a divisor of $q^n - 1$ such that $\gcd(m, q^{n/2} - 1) = 1$. Consider the curve over $\mathbb{F}_{q^n}$ given by the equation

$$y^m = (x^{q^{n/2}} - x)^{q^{n/2} - 1}.$$

This curve has

$$g = (q^{n/2} - 1)(m-1)/2 \quad \text{and} \quad N = (q^n - q^{n/2})m + (q^{n/2} + 1).$$

This produces the following table:

Meet the record

Finite field	q	m	g	N
$\mathbb{F}_{4}$	2	3	1	9
$\mathbb{F}_{16}$	2	5	6	65
$\mathbb{F}_{64}$	2	3	7	177
$\mathbb{F}_{64}$	2	9	28	513
$\mathbb{F}_{81}$	3	5	16	370
$\mathbb{F}_{25}$	5	3	4	66

Remark. The curve in Example 11 is a generalization of the curve in Case 1 of Example 5.

4. Other examples of curves with many points. In this last section we will get other interesting curves by similar constructions, specially the one in [G-V] which inspired this work.

Example 12. Let $n = 2l$, with $l \geq 2$. The curve over $\mathbb{F}_{q^{2l}}$ given by

$$y^{q^l+1} = \frac{w \cdot (\sum_{i=0}^{l-1} x^{q^{l-1}-q^i})}{x^{q^{l-1}}} \quad \text{with } w^{q^l-1} = -1,$$

has genus $g = q^l(q^{l-1}-1)/2$ and $N = q^{3l-1}+1$ rational points over $\mathbb{F}_{q^{2l}}$; i.e., it is a maximal curve.

In fact, consider the polynomial

$$f(x) := \sum_{i=0}^{2l-1} x^{q^0+q+q^2+\ldots+\widehat{q^i}+\ldots+q^{2l-1}},$$

where the symbol $\widehat{q^i}$ means that we omit q^i from the sum $q^0+q+\ldots+q^{2l-1}$. This polynomial has all its roots in $\mathbb{F}_{q^{2l}}$ (see [G-S]). We split the polynomial $f(x)$ as $f(x) = f_1(x) + f_2(x)$ with

$$f_1(x) = \sum_{i=l}^{2l-1} x^{1+q+\ldots+\widehat{q^i}+\ldots+q^{2l-1}} \quad \text{and} \quad f_2(x) = \sum_{i=0}^{l-1} x^{q^0+q+\ldots+\widehat{q^i}+\ldots+q^{2l-1}},$$

and we then apply the method of [G-V]. This method gives us the following equation:

$$y^{q^{2l}-1} = -\frac{f_1(x)}{f_2(x)} = -\frac{x^{1+q+\ldots+q^{2l-2}}(\sum_{i=0}^{l-1} x^{q^{l-1}-q^i})^{q^l}}{x^{1+q+\ldots+\widehat{q^{l-1}}+\ldots+q^{2l-1}}(\sum_{i=0}^{l-1} x^{q^{l-1}-q^i})}.$$

Hence

$$(y^{q^l+1})^{q^l-1} = -\left(\frac{\sum_{i=0}^{l-1} x^{q^{l-1}-q^i}}{x^{q^{l-1}}}\right)^{q^l-1}.$$

Taking the (q^l-1)th root of this equation we get the curve of this example. The genus of this curve comes from a straightforward calculation and the number N of rational points comes from the fact that $f(x)$ has $x = 0$ as its only multiple root; its multiplicity is $1+q+q^2+\ldots+q^{2l-2}$ and hence the polynomial $f(x)$ has $q^{2l-1}-1$ simple roots in $\mathbb{F}_{q^n}$. From these considerations we get

$$N = ((q^{2l-1}-1)-(q^{l-1}-1))(q^l+1)+(q^{l-1}+1) = q^{3l-1}+1.$$

Remark. Let m be a divisor of q^l+1. Then the curve over $\mathbb{F}_{q^{2l}}$ given by

$$y^m = w \cdot \frac{(\sum_{i=0}^{l-1} x^{q^{l-1}-q^i})}{x^{q^{l-1}}} \quad \text{with } w^{q^l-1} = -1$$

has genus $g = (q^{l-1}-1)(m-1)/2$ and $N = q^l(q^{l-1}-1)(m-1)+q^{2l}+1$ rational points over $\mathbb{F}_{q^{2l}}$.

This curve is covered by the curve of Example 12, hence it is also maximal (see [L]).

Remark. Notice that the curve of Example 12 is covered by the Hermitian curve (see [G-S-X]). In fact, let $z = 1/x$ in Example 12, so we get the equation

$$y^{q^l+1} = w(z + z^q + \ldots + z^{q^{l-1}}).$$

Now, let $z = v/w - (v/w)^q$ to obtain the Hermitian curve given by $v^{q^l} + v = y^{q^l+1}$. This shows that the Hermitian curve is a degree q Galois covering of the curve of Example 12.

Example 13. Let $n = 2l+1$ with $l \geq 1$. The curve over $\mathbb{F}_{q^{2l+1}}$ given by

$$y^{q^{2l+1}-1} = -\frac{(\sum_{i=0}^{l-1} x^{q^{l-1}-q^i})^{q^{l+1}}}{x^{q^{2l}-q^l}(\sum_{i=0}^{l} x^{q^l-q^i})}$$

has

$$g = \frac{q^{3l+1}+q^{3l}-2q^{2l+1}-2q^l-2q^{l-1}-2q+8}{2},$$

$$N = \begin{cases} (q^{2l}-1)(q^{2l+1}-1)+2(q-1) & \text{if } q \text{ is even,} \\ (q^{2l}-1)(q^{2l+1}-1) & \text{if } q \text{ is odd.} \end{cases}$$

This example is a direct application of the method in [G-V] for

$$f(x) = \sum_{i=0}^{2l} x^{q^0+q+\ldots+\widehat{q^i}+\ldots+q^{2l}}$$

split as $f(x) = f_1(x) + f_2(x)$ with

$$f_1(x) = \sum_{i=l+1}^{2l} x^{q^0+q+\ldots+\widehat{q^i}+\ldots+q^{2l}} \quad \text{and} \quad f_2(x) = \sum_{i=0}^{l} x^{q^0+q+\ldots+\widehat{q^i}+\ldots+q^{2l}}.$$

We omit the details here.

Example 14. Let l be a divisor of n and write $n = lk$. We consider the curve over $\mathbb{F}_{q^n}$ given by

$$y^m = (x^{q^{l(k-1)}} + x^{q^{l(k-2)}} + \ldots + x^{q^l} + x)^{q^l-1},$$

where m is a divisor of $q^n - 1$ satisfying $\gcd(m, q^l - 1) = 1$. Note that the polynomial in x on the right hand side of the equation above is inspired by the trace of the extension $\mathbb{F}_{q^n}|\mathbb{F}_{q^l}$. We then have

$$g = (q^{l(k-1)} - 1)(m-1)/2 \quad \text{and} \quad N = (q^n - q^{l(k-1)})m + q^{l(k-1)} + 1.$$

Hence we get the table below:

Meet the record

Finite field	m	l	g	N
$\mathbb{F}_4$	3	1	1	9
$\mathbb{F}_{16}$	5	2	6	65
$\mathbb{F}_{64}$	3	3	7	177
$\mathbb{F}_{64}$	9	3	28	513
$\mathbb{F}_{81}$	5	2	16	370
$\mathbb{F}_{25}$	3	1	4	66

REMARK. For large values of the integer m, the best performance in Example 14 for the quotient N/g is obtained by taking l as the greatest proper divisor of n; for example, if n is even one should take (for large values of m) $l = n/2$. In this case the curve obtained here has the same invariants g and N as the curve in Example 11.

References

[G] A. Garcia, *The curves $y^n = f(x)$ over finite fields*, Arch. Math. (Basel) 54 (1990), 36–44.

[G-S] A. Garcia and H. Stichtenoth, *A class of polynomials over finite fields*, Finite Fields Appl. 5 (1999), 424–435.

[G-S-X] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of the Hermitian function field*, Compositio Math. 120 (2000), 137–170.

[G-V] G. van der Geer and M. van der Vlugt, *Kummer covers with many points*, Math. AG/9909037.

[Ge-Vl] —, —, *Tables of curves with many points*, available at http://www.wins.uva.nl/~geer.

[Go] V. D. Goppa, *Codes on algebraic curves*, Soviet Math. Dokl. 24 (1981), 170–172.

[H] H. Hasse, *Theorie der relativ zyklischen algebraischen Funktionenkörper*, J. Reine Angew. Math. 172 (1934), 37–54.

[Hi] J. W. P. Hirschfeld, *Projective Geometries over Finite Fields*, Oxford Univ. Press, Oxford, 1979.

[I] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1981), 721–724.

[L] G. Lachaud, *Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C. R. Acad. Sci. Paris 305 (1987), 729–732.

[Li-Ni] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia Math. Appl. 20, Addison-Wesley, Reading, MA, 1983.

[Mo] C. Moreno, *Algebraic Curves over Finite Fields*, Cambridge Univ. Press, Cambridge, 1991.

[Sh] V. Shabat, *Tables of curves with many points*, available at http://www.turing.wins.uva.nl/~shabat/tables.html.

[S] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

IMPA
Instituto de Matemática Pura e Aplicada
22.460-320, Rio de Janeiro, RJ
Brazil
E-mail: garcia@impa.br

Instituto de Matemática
Univ. Federal do Rio de Janeiro
21.945-970, Rio de Janeiro, RJ
Brazil
E-mail: luciane@impa.br

Received on 4.5.2000 (3817)