Revista Colombiana de Matemáticas
Volumen 47(2013)2, páginas 131-147

Division Algorithm and Construction of Curves with Many Points

Algoritmo de la división y construcción de curvas con muchos puntos

Álvaro Garzón✉, Horacio Navarro

Universidad del Valle, Cali, Colombia

Abstract. We give a simple and effective method for the construction of algebraic curves over finite fields with many rational points. The curves are given as Kummer covers of the projective line.

Key words and phrases. Algebraic curves, Finite fields, Rational points, Kummer extensions.

2010 Mathematics Subject Classification. 14G05, 14H50.

Resumen. Se presenta un simple y efectivo método para la construcción de curvas algebraicas sobre campos finitos con muchos puntos racionales. Las curvas son dadas como coberturas de Kummer de la línea proyectiva.

Palabras y frases clave. Curvas algebraicas, campos finitos, puntos racionales, extensiones de Kummer.

1. Introduction

Let $\mathfrak{C}$ be a nonsingular, projective, geometrically irreducible curve defined over a finite field $\mathbb{F}_q$ with q elements. Let $\mathfrak{C}(\mathbb{F}_q)$ denote the set of $\mathbb{F}_q$-rational points on $\mathfrak{C}$; i.e; points on $\mathfrak{C}$ having all coordinates in $\mathbb{F}_q$. The Hasse-Weil bound implies

$$\#\mathfrak{C}(\mathbb{F}_q) \leq q + 1 + 2\sqrt{q}g(\mathfrak{C}), \tag{1}$$

where $g(\mathfrak{C})$ stands for the genus of the curve $\mathfrak{C}$. Curves which attains the Weil's upper bound are called *maximal curves*.

The interest on curves over finite fields with many rational points with respect to their genera (i.e; with $\#\mathfrak{C}(\mathbb{F}_q)$ close to known upper bounds; e.g., see the tables in [7].) was greatly renewed after Goppa's construction of linear

codes with good parameters from such curves. This created a much stronger interest in the area and attracted new groups of researchers such as coding theorists and algorithmically inclined mathematicians. An added incentive was provided by the invention of elliptic-curve cryptosystem in 1985. The reader may refer to the book [4] for extensive work on this topic.

The aim hence is to exhibit the construction of Kummer covers of the projective line over finite fields with many rational points. The key idea comes from [6] (see also [3] and [2]) and that is the construction of functions $\mu(x) \in \mathbb{F}_q[x]$ via Euclidean algorithm, such that for many elements $x = \beta \in \mathbb{F}_q$, $\mu(\beta)$ is a r–th power in $\mathbb{F}_q$ with r a divisor of $q-1$.

The paper is organized as follows: in Section 2 we present the method for the construction of good curves $\mathfrak{C}$ and we explain how one computes its genus and its number of rational points; in Section 3 we give some characterization of the remainder polynomial in particular cases obtained after having applied the division algorithm and in Section 4 we give several examples based in our construction.

In tables 1, 2 and 3 we summarize the good pairs $\big(g(\mathfrak{C}), \#\mathfrak{C}(\mathbb{F}_q)\big)$ obtained in the examples of Section 4.

2. The Method

Let $r > 1$ be a divisor of $q-1$ and $f(x)$, $\ell(x)$ two polynomials in $\mathbb{F}_q[x]$ such that $\deg\big(f(x)^r\big) \geq \deg\big(\ell(x)\big)$. We will denote by $\mathcal{R}_\ell\big(f(x)^r\big)$ the remainder of the Euclidean division of $f(x)^r$ by $\ell(x)$, i.e.,

$$f(x)^r = \ell(x)h(x) + \mathcal{R}_\ell\big(f(x)^r\big). \tag{2}$$

We will always assume that $\mathcal{R}_\ell\big(f(x)^r\big) \neq 0$ (i.e, $f(x)$ is not multiple of $\ell(x)$).

The method for the construction is then to consider the nonsingular projective model $\mathfrak{C}$ of the curve given by the affine Kummer equation:

$$y^r = \mu(x) \coloneqq \mathcal{R}_\ell\big(f(x)^r\big). \tag{3}$$

As it was shown in [5, Proposition III.7.3], the genus $g(\mathfrak{C})$ can be easily derived from the multiplicities of the zeros and poles of the function $\mu(x) \in \mathbb{F}_q(x)$.

Now we will explain how one computes the genus. If $\alpha \in \overline{\mathbb{F}}_q$ is a zero of $\mu(x)$ of multiplicity m_α, then we have d_α points on the curve $\mathfrak{C}$ with first coordinate $x = \alpha$, where $d_\alpha = \gcd(r, m_\alpha)$. These d_α points have ramification index $e_\alpha \coloneqq r/d_\alpha$ and they have different exponent equal to $e_\alpha - 1$ by Dedekind's Exponent Theorem. The same holds for the points on the curve $\mathfrak{C}$ above the point at infinite of the projective line i.e., for $\alpha = \infty$ one defines its multiplicity as $m_\infty = -\deg\big(\mathcal{R}_\ell\big(f(x)^r\big)\big)$ and, similarly, $d_\infty = \gcd(r, m_\infty)$ and $e_\infty = r/d_\infty$.

New records			
q	$g(\mathfrak{C})$	$\#\mathfrak{C}(\mathbb{F}_q)$	Former Entry
11^3	4	1580	1422
17^3	7	5220	5204

Table 1

New entries		
q	$g(\mathfrak{C})$	$\#\mathfrak{C}(\mathbb{F}_q)$
5^3	7	220
7^3	46	1512
11^3	5	1438
11^3	16	1810
13^3	5	2356
13^3	13	2592
13^3	15	2688
17^3	8	5202
17^3	21	5768
19^3	8	6588
19^3	16	6972
19^3	19	7560
3^5	4	306
3^5	6	345
3^5	15	519

Table 2

Meets the record		
q	$g(\mathfrak{C})$	$\#\mathfrak{C}(\mathbb{F}_q)$
2^3	3	24
2^3	9	45
3^3	1	38
3^3	24	208
3^5	5	364
5^3	1	148
5^3	3	192

Table 3

It now follows from Hurwitz's genus formula that

$$g(\mathfrak{C}) = 1 + r\left(-1 + \frac{1}{2} \sum_{\alpha \in \overline{\mathbb{F}}_q \cup \infty} \left(1 - \frac{d_\alpha}{r}\right)\right). \tag{4}$$

The sum over $\alpha \in \overline{\mathbb{F}}_q \cup \infty$ in the Formula (4) above is indeed a finite sum over only the zeros and poles of the function $\mu(x) \in \mathbb{F}_q(x)$. In fact, if $\alpha \in \mathbb{F}_q$ is not a zero of $\mu(x)$, then the multiplicity is equal to zero and hence $d_\alpha = r$.

From the genus Formula (4), we see that the genus $g(\mathfrak{C})$ is smaller as the function $\mu(x)$ has fewer distinct zeros. So in general the inseparability of $\mu(x)$ is desirable.

Now we turn to the rational points on $\mathbb{F}_q$ of the curve $\mathfrak{C}$ given by Equation (3).

If $\alpha \in \overline{\mathbb{F}}_q \cup \infty$ is a zero or pole of $\mu(x)$ with multiplicity m_α, then we have $d_\alpha = \gcd(r, m_\alpha)$ points on $\mathfrak{C}$ with first coordinate $x = \alpha$. On the other hand, if $\alpha \in \mathbb{F}_q$, then it may be happen that the d_α points on $\mathfrak{C}$ with $x = \alpha$ are again rational points over $\mathbb{F}_q$. Here is how one decides if this is the case: If α is a zero of $\mu(x)$, we can write

$$y^r = g(x)(x-\alpha)^{m_\alpha} \quad \text{or} \quad \left(\frac{y^{r/d_\alpha}}{(x-\alpha)^{m_\alpha/d_\alpha}}\right)^{d_\alpha} = g(x), \tag{5}$$

where $g(x) \in \mathbb{F}_q[x]$ with $g(\alpha) \neq 0$. Then the d_α points are all rational over $\mathbb{F}_q$ if and only if $g(\alpha)$ is a d_α–th power of an element of $\mathbb{F}_q$.

On the other hand, if $\beta \in \mathbb{F}_q$ satisfies $\ell(\beta)h(\beta) = 0$ and $f(\beta) \neq 0$. Then, the value of the function $\mu(x)$ at β is a r–th power (see formula 2). This guarantees that we have r rational points on the curve $\mathfrak{C}$ with first coordinate $x = \beta$ as above. So in order to have many rational points over $\mathbb{F}_q$ we will always take $\ell(x)$ as a polynomial having all its roots in the finite field $\mathbb{F}_q$.

Now, if we denote by $l_1(x)$, the polynomial $\ell(x)h(x)/\gcd\big(\ell(x)h(x), f(x)\big)$, then the number of $\mathbb{F}_q$–rational points satisfies $\#\mathfrak{C}\big(\mathbb{F}_q\big) \geq r\lambda$ where $\lambda = \deg\big(l_1(x)\big)$.

Observe that here we only counted the rational points coming from the roots of the polynomial $l_1(x)$ in $\mathbb{F}_q$. Other rational points can coming from the rational solutions $\gamma \in \mathbb{F}_q$ of the equation

$$\mathcal{R}_\ell\big(f(x)^r\big)^{(q-1)/r} - 1 = 0 \tag{6}$$

such that $l_1(\gamma) \neq 0$. i.e.; those elements

$$\gamma \in \mathbb{F}_q \text{ such that } f(\gamma)^r - \ell(\gamma)h(\gamma) \text{ is a } r\text{–th power of an element in } \mathbb{F}_q. \tag{7}$$

We some times have carried out a computer search to determine the cardinality κ of the set of such elements

$$\kappa \coloneqq \#\big\{\gamma \in \mathbb{F}_q \text{ such that } l_1(\gamma) \neq 0 \text{ and } \gamma \text{ is a } r\text{-th power in } \mathbb{F}_q.\big\} \tag{8}$$

For each $\gamma \in \mathbb{F}_q$ satisfying (7) we have r rational points on $\mathfrak{C}$ with first coordinate $x = \gamma$. So in practice (when r is a proper divisor of $q-1$), after having a good candidate for a curve $\mathfrak{C}$ with many rational points over $\mathbb{F}_q$ with respect to its genus $g(\mathfrak{C})$ we some times have carried out a computer search to determine the cardinality κ of the set of such elements.

3. Some Characterizations of Remainder Polynomial

The goal of this section is give some characterizations of the polynomial $\mathcal{R}_\ell\big(f(x)\big)$ and then, we will use them to construct curves with many rational points

Theorem 3.1. *Let $m \geq 1$ be a positive integer, $f(x)$ and $\ell(x) \in \mathbb{F}_q[x]$ polynomials such that:*

(i) $f(x)$ and $\ell(x)$ are relatively prime.

(ii) $deg\big(\ell(x)\big) = d$, a divisor of m.

(iii) $\ell(x)$ is irreducible.

Then, $\mathcal{R}_\ell\big(f(x)^{q^m-1}\big) = 1$.

Proof. First suppose that $\deg\big(\ell(x)\big) = m$. Since $\gcd\big(f(x), \ell(x)\big) = 1$ and $\ell(x)$ is an irreducible polynomial, then $f(x) \notin \big\langle \ell(x) \big\rangle$, and therefore the class of $f(x)$, in the residue class field $F \coloneqq \mathbb{F}_q[x]/\big\langle \ell(x) \big\rangle$, is non zero. On the other hand, since the finite field F has cardinality q^m, then we have that

$$f(x)^{q^m-1} + \big\langle \ell(x) \big\rangle = \big(f(x) + \big\langle \ell(x) \big\rangle\big)^{q^m-1} = 1 + \big\langle \ell(x) \big\rangle$$

and therefore,

$$f(x)^{q^m-1} - 1 \in \big\langle \ell(x) \big\rangle;$$

consequently, there exits $h(x) \in \mathbb{F}_q[x]$ such that

$$f(x)^{q^m-1} = \ell(x)h(x) + 1,$$

that is to say, $\mathcal{R}_\ell\big(f(x)^{q^m-1}\big) = 1$.

Now if $\deg\big(\ell(x)\big) = d$ with $d \neq m$, then by similar arguments as above we obtain that $f(x)^{q^d-1} = \ell(x)h(x) + 1$ for some $h(x) \in \mathbb{F}_q[x]$ and since

$$q^m - 1 = q^{dt} - 1 = \big(q^d\big)^t - 1 = \big(q^d - 1\big)\big(q^{d(t-1)} + \cdots + 1\big),$$

then we have:

$$f(x)^{q^m-1} = \Big(f(x)^{q^d-1}\Big)^{\left(q^{d(t-1)}+\cdots+1\right)} = \big(\ell(x)h(x) + 1\big)^{\left(q^{d(t-1)}+\cdots+1\right)} = \ell(x)\widetilde{h}(x) + 1$$

for some $\widetilde{h}(x) \in \mathbb{F}_q[x]$. ☑

Corollary 3.2. *Let $m \geq 1$ be a positive integer and let $f(x)$, $l_i(x) \in \mathbb{F}_q[x]$ with $i = 1, 2$ polynomials such that*

(1) $f(x)$ and $l_i(x)$ are relatively prime,

(2) $deg\big(l_i(x)\big) = d_i$, a divisor of m,

(3) $l_i(x)$ is irreducible.

Then $\mathcal{R}_{l_1 l_2}\big(f(x)^{q^m-1}\big) = 1$.

Proof. Suppose that

$$f(x)^{q^m-1} \neq l_1(x) l_2(x) h(x) + 1$$

for all $h(x) \in \mathbb{F}_q[x]$. By Theorem 3.1, the polynomial

$$\frac{f(x)^{q^m-1} - 1}{l_2(x)} \notin \big\langle l_1(x) \big\rangle$$

and, since $\gcd\big(l_1(x), l_2(x)\big) = 1$, we have that $l_2(x) \notin \big\langle l_1(x)\big\rangle$ and therefore,

$$f(x)^{q^m-1} - 1 = \frac{f(x)^{q^m-1} - 1}{l_2(x)} l_2(x) \notin \big\langle l_1(x)\big\rangle$$

which is a contradiction. ☑

Corollary 3.3. *If $f(x)$ and $\ell(x) \in \mathbb{F}_q[x]$ are coprime and $\ell(x)$ is a proper divisor of the polynomial $x^{q^m} - x$ then*

$$\mathcal{R}_\ell\big(f(x)^{q^m-1}\big) = 1.$$

Proof. It follows from Corollary 3.2 and the fact that the product of all monic irreducible polynomials over $\mathbb{F}_q$, whose degrees divide m, is precisely $x^{q^m} - x$. ☑

In accordance with previous results, if we are interested in obtaining non-constant remainders, the polynomials $f(x)$ and $\ell(x)$ must have at least one common factor. This fact does not guarantee that it is always possible to characterize the remainder polynomial, however with an appropriate choice of such polynomials one has a nice results as it is shown in the next theorem.

Theorem 3.4. *Let $f(x) = x - 1$ and $\ell(x) = x^h - 1$ be polynomials in $\mathbb{F}_q[x]$ with $h = \big(q^m - 1\big)/(q-1)$. Then*

$$\mathcal{R}_\ell\Big((x-1)^{q^m-1}\Big) = -\sum_{i=1}^{h-1} x^i = -\big(x + x^2 + \cdots + x^{h-1}\big)$$

Proof. Let $q(x)$ be the polynomial defined by

$$q(x)=\sum_{i=1}^{q-2} i\Big(x^{(q-1-i)h}+x^{(q-1-i)h-1}+x^{(q-1-i)h-2}+\cdots+ x^{(q-1-i)h-(h-1)}\Big)-1=\sum_{i=1}^{q-2} i\left(\sum_{k=0}^{h-1} x^{(q-1-i)h-k}\right).$$

Then,

$$\begin{aligned}\big(x^h-1\big)q(x)&=\sum_{i=1}^{q-2} i\left(\sum_{k=0}^{h-1} x^{(q-i)h-k}\right)-x^h-\sum_{i=1}^{q-2} i\left(\sum_{k=0}^{h-1} x^{(q-1-i)h-k}\right)+1\\ &=\sum_{k=0}^{h-1} x^{(q-1)h-k}+\sum_{i=2}^{q-2} i\left(\sum_{k=0}^{h-1} x^{(q-i)h-k}\right)-x^h\\ &\quad-\sum_{i=1}^{q-3} i\left(\sum_{k=0}^{h-1} x^{(q-1-i)h-k}\right)-(q-2)\sum_{k=0}^{h-1} x^{h-k}+1\\ &=\sum_{k=0}^{h-1} x^{(q-1)h-k}+\sum_{i=1}^{q-3}(i+1)\left(\sum_{k=0}^{h-1} x^{(q-1-i)h-k}\right)-x^h\\ &\quad-\sum_{i=1}^{q-3} i\left(\sum_{k=0}^{h-1} x^{(q-1-i)h-k}\right)+2\sum_{k=0}^{h-1} x^{h-k}+1\\ &=\sum_{k=0}^{h-1} x^{(q-1)h-k}+\sum_{i=1}^{q-3}\left(\sum_{k=0}^{h-1} x^{(q-1-i)h-k}\right)-x^h+2\sum_{k=0}^{h-1} x^{h-k}+1\\ &=\sum_{i=0}^{q-3}\left(\sum_{k=0}^{h-1} x^{(q-1-i)h-k}\right)+x^h+2\sum_{k=1}^{h-1} x^{h-k}+1\\ &=x^{(q-1)h}+\cdots+x^h+2\big(x^{h-1}+\cdots+x\big)+1.\end{aligned}$$

On the other hand,

$$\begin{aligned}(x-1)^{q^m-1}&=x^{q^m-1}+\cdots+x^h+x^{h-1}+\cdots+x+1\\ &=x^{(q-1)h}+\cdots+x^h+2\big(x^{h-1}+\cdots+x\big)+1-\big(x^{h-1}+\cdots+x\big)\\ &=\big(x^h-1\big)q(x)-\big(x^{h-1}+\cdots+x\big).\end{aligned}$$ ☑

***Remark* 3.5.** Observe that the polynomial $\mathcal{R}_\ell\big((x-1)^{q^m-1}\big)$ has $q^{m-2}+\cdots+q^2+2$ different roots in $\mathbb{F}_{q^{m-1}}$. In fact, first

$$\mathcal{R}_\ell\big((x-1)^{q^m-1}\big)=-(x^{h-1}+\cdots+x)=-x(x-1)^{q-1}\left(\sum_{i=0}^{q+\cdots+q^{m-2}} x^i\right)^q.$$

Second, the polynomial $p(x) = \sum_{i=0}^{q+\cdots+q^{m-2}} x^i = 1 + x + x^2 + \cdots + x^{q+\cdots+q^{m-2}}$ is separable because if $\widetilde{h} = 1 + q + \cdots + q^{m-2}$, then the polynomial $x^{\widetilde{h}} - 1$ is separable and since

$$p(x)(x-1) = x^{\widetilde{h}} - 1,$$

then $p(x)$ is also separable. Finally, it is easy to see that if $\alpha^{\widetilde{h}} - 1 = 0$, then $\alpha \in \mathbb{F}_{q^{m-1}}$.

We end up this section with some characterizations of the remainder polynomial in the particular case when the polynomial $\ell(x)$ belongs to certain class of polynomials over finite fields, that will be used in next section for the construction of some curves with many rational points. First we begin with a definition.

Let m, j be integers with $m \geq 1$ and let $s_j(x_1, x_2, \ldots, x_m)$ be the elementary symmetric function in m variables over $\mathbb{F}_q$. For all $j \in \mathbb{Z}$ and integers $m \geq 1$ we define a polynomial $s_{m,j}(x) \in \mathbb{F}_q[x]$ (see [1]) as follows:

$$\begin{aligned}
s_{m,j}(x) &\coloneqq 0, \quad \text{for} \quad j < 0 \\
s_{m,0}(x) &\coloneqq 1 \\
s_{m,1}(x) &\coloneqq s_1\left(x, x^q, \ldots, x^{q^{m-1}}\right) = x + x^q + \cdots + x^{q^{m-1}} \\
s_{m,2}(x) &\coloneqq s_2\left(x, x^q, \ldots, x^{q^{m-1}}\right) = x^{1+q} + x^{1+q^2} + \cdots + x^{q^{m-2}+q^{m-1}} \\
&\vdots \\
s_{m,m}(x) &\coloneqq s_m\left(x, x^q, \ldots, x^{q^{m-1}}\right) = x^{1+q+\cdots+q^{m-1}} \\
s_{m,j}(x) &\coloneqq 0, \quad \text{for} \quad j > m.
\end{aligned}$$

Observe that the polynomials $s_{m,1}(x) = x + x^q + \cdots + x^{q^{m-1}}$ and $s_{m,m}(x) = x^{1+q+\cdots+q^{m-1}}$ are nothing but the trace and norm polynomials corresponding to the finite extension $\mathbb{F}_{q^m}/\mathbb{F}_q$.

Theorem 3.6. *If $f(x) = x$ and $\ell(x) = s_{m,1}(x)$, then*

$$\mathcal{R}_{s_{m,1}}\left(x^{q^m-1}\right) = -\frac{x^q + \cdots + x^{q^{m-1}}}{x} = -\frac{s_{m-1,1}(x)^q}{x}$$

Proof. The proof is direct:

$$\begin{aligned} x^{q^m-1} = \frac{x^{q^m}}{x} &= \frac{x^q + \cdots + x^{q^{m-1}} + x^{q^m} - \left(x^q + \cdots + x^{q^{m-1}}\right)}{x} \\ &= \frac{\left(x + x^q + \cdots + x^{q^{m-1}}\right)^q - \left(x^q + \cdots + x^{q^{m-1}}\right)}{x} \\ &= \frac{\left(x + x^q + \cdots + x^{q^{m-1}}\right)^q}{x} - \frac{\left(x^q + \cdots + x^{q^{m-1}}\right)}{x} \\ &= s_{m,1}(x)\frac{s_{m,1}(x)^{q-1}}{x} - \frac{s_{m-1,1}(x)^q}{x} \end{aligned}$$ ☑

Theorem 3.7. *Let* $f(x) = x + 1$, $\tau_m(x) \coloneqq \sum_{j=0}^{m-1} s_{m,j}(x)$ *and* $h = \big(q^m - 1\big)/(q-1)$ *then*

$$\mathcal{R}_{\tau_m}\big((x+1)^h\big) = -x(x+1)\tau_{m-1}(x)^q$$

Proof. See [2] Lemma 3.3. ☑

***Remark* 3.8.** With notations as Theorem 3.7, we have:

(i) The polynomial $\tau_m(x)$ is separable, its roots belong to $\mathbb{F}_{q^m}$ and has degree $h-1$.

(ii) The polynomial $\mathcal{R}_{\tau_m}\big((x+1)^h\big)$ has $q^{m-2} + \cdots + q + 2$ different roots in $\mathbb{F}_{q^{m-1}}$.

(iii) $s_{m,m}(x+1) = \tau_m(x) + s_{m,m}(x)$.

Proof. See [2] Lemmas 3.2 and 3.3. ☑

4. Constructions

In this section we will construct curves over finite fields using the characterizations obtained in section above.

Theorem 4.1. *Let* $h = (q^m - 1)/(q-1)$. *The nonsingular complete geometrically irreducible curve* $\mathfrak{C}$ *over* $\mathbb{F}_{q^m}$ *defined by the Kummer equation*

$$y^r = \mathcal{R}_\ell\big((x-1)^{q^m-1}\big) = -\big(x + x^2 + \cdots + x^{h-1}\big)$$

with $r > 1$ *a divisor of* $q^m - 1$, *has genus*

$$g(\mathfrak{C}) = \frac{2 + (r-1)\big(\sum_{i=0}^{m-2} q^i\big) - e_1 - e_\infty}{2}$$

with $e_1 = \gcd(r, q-1)$ *and* $e_\infty = \gcd\big(r, 1+q+\cdots+q^{m-2}\big)$. *The number of rational points satisfies*

$$\#\mathfrak{C}\big(\mathbb{F}_q\big) \geq r(h-1) = r\big(q^{m-1}+\cdots+q\big)$$

Proof. By Remark 3.5, the polynomial $\mathcal{R}_\ell\big((x-1)^{q^m-1}\big)$ has $q^{m-2}+\cdots+q^2+2$ different roots in $\mathbb{F}_{q^{m-1}}$ and one can write $\mathcal{R}_\ell\big((x-1)^{q^m-1}\big)$ as

$$\mathcal{R}_\ell\big((x-1)^{q^m-1}\big) = -x(x-1)^{q-1}\left(\sum_{i=0}^{q+\cdots+q^{m-2}} x^i\right)^q.$$

In this case, we have $q^{m-2}+\cdots+q^2+1$ points totally ramified in $\mathfrak{C}$ with ramification index r, namely $x=0$ and $x=\alpha$ with $\alpha \in \mathbb{F}_{q^{m-1}}$ corresponding to the roots of $\mathcal{R}_\ell\big((x-1)^{q^m-1}\big)$ in $\mathbb{F}_{q^{m-1}} \smallsetminus \{0,1\}$. The point with first coordinate $x=1$ has ramification index $e_1 = \gcd(r, q-1)$, and the point at infinity has ramification index $e_\infty = \gcd(r, 1+q+\cdots+q^{m-2})$. Then, the formula for the genus follows by (4).

The claim about the number of rational points is clear. ☑

Corollary 4.2. *If* $m=2$ *and* $r=q^2-1$, *then the curve* $\mathfrak{C}$ *over* $\mathbb{F}_{q^2}$ *defined by the Kummer equation*

$$y^{q^2-1} = \mathcal{R}_\ell\big((x-1)^{q^2-1}\big) = -x(x-1)^{q-1}$$

is the Hermitian curve.

Proof. Observe that the points with first coordinate $x=0$, $x=1$ and $x=\infty$ have ramification index $e_0 = q^2-1$, $e_1 = q+1$ and $e_\infty = q^2-1$ respectively. Now it is easy to see that $g(\mathfrak{C}) = \big(q^2-q\big)/2$.

For the rational points, by Theorem 4.1, we have $\#\mathfrak{C}(\mathbb{F}_{q^2}) \geq (q^2-1)q$.

The points above $x=0$ and $x=\infty$ are rational and those $(q-1)$ above $x=1$ are also rational. Therefore $\#\mathfrak{C}(\mathbb{F}_{q^2}) = (q^2-1)q+(q-1)+2 = q^3+1$. ☑

As an application of Theorem 4.1 we have:

Example 4.3. In this example we will construct a curve $\mathfrak{C}$ over $\mathbb{F}_{5^3}$ with $g(\mathfrak{C}) = 7$ and 220 rational points. This is a new entry in [7]. The curve $\mathfrak{C}$ is defined by the Kummer equation

$$y^4 = \mu(x) \coloneqq -(x+x^2+\cdots+x^{30}) = -x(1+x)^5(4+x)^4(1+x+x^2)^5(1+4x+x^2)^5.$$

In this case we have that $h = (5^3-1)/4 = 31$ and therefore by Theorem 4.1, the polynomial $\ell(x) = x^{31}-1$ provides $r \times (h-1) = 4 \times 30 = 120$ rational points. Other points could be found if we analyze the solutions of Equation (6).

In this particular case the exact value of κ in (8) is 24, namely, the roots of the polynomial

$$1+x+x^2+3x^3+2x^4+3x^5+3x^6+4x^8+ \\ 4x^9+4x^{10}+x^{11}+x^{12}+4x^{13}+x^{14}+4x^{15}+4x^{16}+ \\ x^{17}+4x^{18}+4x^{19}+2x^{20}+2x^{21}+3x^{22}+3x^{23}+x^{24},$$

and hence we have $4 \times 24 = 96$ additional points.

Finally, we will analyze the ramification points of the function $\mu(x)$. First, observe that $\mu(x)$ has three roots in $\mathbb{F}_5 \subset \mathbb{F}_{5^3}$, namely $x = 0$, $x = 1$ and $x = -1$, the other four roots (those roots of the polynomials $1+x+x^2$ and $1+4x+x^2$) belongs to $\mathbb{F}_{5^2}$.

By (5), the points with first coordinate $x = 0$, $x = -1$ and $x = \infty$ are rational, while the points above $x = 1$ are not rational. Hence we have $d_0 + d_1 + d_\infty = 1 + 1 + 2 = 4$ extra rational points. Summarizing, the curve $\mathfrak{C}$ has $120 + 96 + 4 = 220$ rational points. The genus follows from Theorem 4.1.

We now summarize the results obtained in the particular case when $q = p^3$ (Table 4). In this case r a divisor of $p^3 - 1$, $h = p^2 + p + 1$ and the curves are defined by the Kummer equation:

$$y^r = -\Big(x + x^2 + \cdots + x^{p^2+p}\Big).$$

We omit the details.

q^3	r	$g(\mathfrak{C})$	$\#\mathfrak{C}(\mathbb{F}_{q^3})$	old entry
2^3	7	9	45	45
3^3	2	1	38	38
5^3	4	7	220	
11^3	2	5	1438	
13^3	3	13	2592	
17^3	2	8	5202	
19^3	3	19	7560	

TABLE 4. Examples of curves with many points using Theorem 4.1.

Now we will construct curves over $\mathbb{F}_{q^m}$ using the Theorem 3.6.

Theorem 4.4. *The nonsingular complete geometrically irreducible curve $\mathfrak{C}$ over $\mathbb{F}_{q^m}$ defined by the Kummer equation*

$$y^r = \mathcal{R}_{s_{m,1}}\big(x^{q^m-1}\big) = -\frac{s_{m-1,1}(x)^q}{x}$$

with $r > 1$, a divisor of $q^m - 1$, has genus

$$g(\mathfrak{C}) = \frac{(r-1)\big(q^{m-1}-2\big) - 2(e_0-1)}{2}$$

where $e_0 = \gcd(r, q-1)$, and the number of rational points satisfies

$$\#\mathfrak{C}(\mathbb{F}_q) \geq r\big(q^{m-1}-1\big).$$

Proof. First observe that the polynomial $s_{m-1,1}(x)$ is separable and has its roots in $\mathbb{F}_{q^{m-1}}$. Therefore we have exactly $q^{m-2}-1$ points totally ramified in $\mathfrak{C}$ with ramification index r. The points $x = 0$ and $x = \infty$ have ramification index $e_0 = \gcd(r, q-1)$. Here we write the polynomial $\mathcal{R}_{s_{m,1}}\big(x^{q^m-1}\big)$ as

$$\mathcal{R}_{s_{m,1}}\big(x^{q^m-1}\big) = -\frac{s_{m-1,1}(x)^q}{x} = -x^{q-1}\big(1 + x^{q-1} + \cdots + x^{q^{m-2}-1}\big)^q.$$

Now the genus follows from (4). The affirmation corresponding to the number of rational points is clear. ☑

Example 4.5. In this example we will construct a curve $\mathfrak{C}$ over $\mathbb{F}_{5^3}$ with $g(\mathfrak{C}) = 3$ and 192 rational points. This is the better value known in [7]. The curve $\mathfrak{C}$ is defined by the Kummer equation $\mathbb{F}_{5^3}$

$$y^4 = -\big(x^4 + x^{24}\big) = -x^4\big(2 + x^2\big)^5\big(3 + x^2\big)^5.$$

Since the polynomial $\ell(x) = x^{25} + x^5 + x$ has all its roots in $\mathbb{F}_{5^3}$, then we have $r \times (h-1) = 4 \times 24 = 96$ rational points. The value κ in (8) for this case is $\kappa = 24$, namely, the roots of the polynomial

$$1 + x^{20} + x^{24}$$

hence we have $4 \times 24 = 96$ additional points. Finally, by (5), the points with first coordinate $x = 0$, $x = \infty$ and $x = \alpha \in \overline{\mathbb{F}}_{5^3}$, which are roots of the polynomials $\big(2 + x^2\big)$ and $\big(3 + x^2\big)$, are not rational. The genus follows from Theorem 4.4.

In Table 5 we summarize some results obtained using Theorem 4.4 in the particular case $q = p$ and $m = 3$. The curves $\mathfrak{C}$ are defined by the Kummer equation

$$y^r = -\big(x^{p-1} + x^{p^2-1}\big)$$

Now, we will construct curves over $\mathbb{F}_{q^m}$ using Theorem 3.7.

Theorem 4.6. *Let $m \geq 2$. The nonsingular complete geometrically irreducible curve $\mathfrak{C}$ over $\mathbb{F}_{q^m}$ defined by the Kummer equation*

$$y^r = \mathcal{R}_{\tau_m}((x+1)^h) = -x(x+1)\tau_{m-1}(x)^q$$

q^3	r	$g(\mathfrak{C})$	$\#\mathfrak{C}(\mathbb{F}_{q^3})$	old entry
2^3	7	3	24	24
3^3	26	24	208	208
5^3	2	1	148	148
5^3	4	3	192	192
7^3	18	46	1512	
11^3	2	4	1580	1422
11^3	5	16	1810	
13^3	2	5	2356	
13^3	4	15	2688	
17^3	2	7	5220	5204
17^3	4	21	5768	
19^3	2	8	6588	
19^3	3	16	6972	

TABLE 5. Examples of curves with many points using Theorem 4.4.

with $r|d$, has genus

$$g(\mathfrak{C}) = \frac{(r-1)\big(\sum_{i=1}^{m-2} q^i\big) + r - e_\infty}{2}$$

where $e_\infty = \gcd(r, q-1)$ and the number rational points satisfies

$$\#\mathfrak{C}(\mathbb{F}_q) \geq r(h-1) = r\big(q + q^2 + \cdots + q^{m-1}\big).$$

Proof. By Remark 3.8, the polynomial $\mathcal{R}_{l_m}\big((x+1)^h\big)$ has $q^{m-2} + \cdots + q + 2$ different roots $\alpha \in \mathbb{F}_{q^{m-1}}$, so, each point on $\mathfrak{C}$ with first coordinate $x = \alpha$ has ramification index r. The point at ∞ has ramification index $e_\infty = \gcd(r, q-1)$. Now the genus follows from (4).

To obtain a bound to the number of rational points, observe that since $\tau_m(x) = s_{m,m}(x+1) - s_{m,m}(x)$, then $\tau_m(-1) = (-1)^{m+1} \neq 0$; so, the polynomials $x+1$ and $\tau_m(x)$ are coprimes and hence we conclude that the number rational points satisfies $\#\mathfrak{C}(\mathbb{F}_q) \geq r(h-1)$. ☑

Corollary 4.7. *If $m = 2$ and $r = q+1$, then the curve $\mathfrak{C}$ over $\mathbb{F}_{q^2}$ defined by the Kummer equation*

$$y^{q+1} = \mathcal{R}_{\tau_2}\big((x+1)^h\big) = -x(x+1)$$

is maximal.

Proof. The points $x = 0$, $x = 1$ and the point at ∞ have ramification index $e_0 = q + 1$, $e_1 = q + 1$ and $e_\infty = (q + 1)/\gcd(q + 1, 2)$ respectively. Now it is easy to see that $g(\mathfrak{C}) = \big(q + 1 - \gcd(q + 1, 2)\big)/2$.

For the rational points, observe that since $\tau_2(x) = x^q + x + 1$, then by Theorem 4.6, we have at least $(q + 1)q$ rational points. The points on $\mathfrak{C}$ with first coordinate $x = 0$, $x = 1$ are rational and the $\gcd(q + 1, 2)$ points above ∞ are also rational.

On the other hand, the exact value of κ in (8) is

$$\kappa = \begin{cases} (q + 1)(q - 2), & \text{if } q \text{ is even;} \\ (q + 1)(q - 3), & \text{if } q \text{ is odd.} \end{cases}$$

Therefore

$$\#\mathfrak{C}\big(\mathbb{F}_{q^2}\big) = \begin{cases} 2q^2 + 1, & \text{if } q \text{ is even;} \\ 2q^2 - q + 1, & \text{if } q \text{ is odd.} \end{cases}$$ ☑

As an application of Theorem 4.6 we have:

Example 4.8. In this example we will construct a curve $\mathfrak{C}$ over $\mathbb{F}_{2^3}$ with $g(\mathfrak{C}) = 9$ and $\#\mathfrak{C}\big(\mathbb{F}_{2^3}\big) = 45$. This is the better value known in [7]. We defined the curve $\mathfrak{C}$ over $\mathbb{F}_{2^3}$ by equation

$$y^7 = \mu(x) \coloneqq x(1 + x)\big(1 + x + x^2\big)^2.$$

In this case we have that $h = \big(2^3 - 1\big)/1 = 7$ and therefore by Theorem 4.6, the polynomial

$$\tau_2(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$$

provides $r \times (h - 1) = 7 \times 6 = 42$ rational points. Other points could come from the analysis of the solutions of Equation (6). In this case the exact value of κ in (8) is 0.

Finally, we will analyze the ramification points of the function $\mu(x)$. First, observe that $\mu(x)$ has two roots in $\mathbb{F}_2 \subset \mathbb{F}_{2^3}$, namely $x = 0$ and $x = 1$. The other two roots (those roots of the polynomial $1 + x + x^2$) belongs to $\mathbb{F}_{2^2}$. By (5) the points with first coordinate $x = 0$, $x = 1$ and $x = \infty$ are rational, and we have exactly $d_0 + d_1 + d_\infty = 1 + 1 + 1 = 3$ extra rational points. Summarizing, the curve $\mathfrak{C}$ has $42 + 3 = 45$ rational points. The genus follows from Theorem 4.6.

In Table 6 we summarize some examples using Theorem 4.6. In the particular case $q = p$ and $m = 3$ we have that $h = q + 1$, r is a divisor of $q + 1$ and the Kummer equation

$$y^r = -x(x + 1)\tau_2(x)^q = -x(x + 1)(x^q + x + 1)^q$$

Example	q	r	$g(\mathfrak{C})$	$\#\mathfrak{C}(\mathbb{F}_q)$	old entry
3.1	2^3	7	9	45	45
3.2	13^3	3	13	2592	
3.3	19^3	3	19	7560	

TABLE 6. Examples of curves with many points using Theorem 4.6.

5. Others Examples

In general, given two polynomials $f(x)$, $\ell(x) \in \mathbb{F}_q[x]$, it is very hard to give a characterization of the remainder polynomial $\mathcal{R}_\ell\big(f(x)\big)$. However, although we do not give an explicit formula for the remainder, we are going to give 4 examples of good curves over the finite field $\mathbb{F}_{243}$. These curves are defined as always by Kummer equations of the kind $y^n = \mathcal{R}_\ell\big(f(x)\big)$, with r and n divisors of $q-1$. In this particular case we will take $f(x) = x$ and the polynomial $\ell(x)$ as a product of irreducible polynomials form the list below.

$$
\begin{aligned}
l_1(x) &= 1 + x \\
l_2(x) &= 2 + x \\
l_3(x) &= 1 + x + 2x^2 + x^3 + x^4 + x^5 \\
l_4(x) &= 1 + 2x^2 + 2x^3 + x^4 + x^5 \\
l_5(x) &= 1 + x + 2x^4 + x^5 \\
l_6(x) &= 1 + 2x + 2x^3 + 2x^4 + x^5 \\
l_7(x) &= 2 + 2x^2 + 2x^3 + x^4 + x^5 \\
l_8(x) &= 2 + 2x^2 + 2x^4 + x^5 \\
l_9(x) &= 2 + x + x^2 + x^3 + 2x^4 + x^5 \\
l_{10}(x) &= 2 + 2x + 2x^2 + x^3 + 2x^4 + x^5 \\
l_{11}(x) &= 2 + 2x + 2x^3 + x^4 + x^5
\end{aligned}
$$

Example 5.1. Taking $\ell(x) = l_3(x)l_4(x)l_5(x)l_6(x)$, $r = 22$ and $n = 2$, we obtain

$$\mathcal{R}_\ell\big(x^{22}\big) = 2x^2(1+x)^2(2+x)\big(1+x^2\big)^2\big(2+2x+x^4\big)\big(1+2x+x^5\big).$$

Now it is easy to verify that the curve $\mathfrak{C}$ defined by the equation

$$y^2 = 2x^2(1+x)^2(2+x)\big(1+x^2\big)^2\big(2+2x+x^4\big)\big(1+2x+x^5\big)$$

has $g(\mathfrak{C}) = 4$ and $\#\mathfrak{C}\big(\mathbb{F}_{3^5}\big) = 306$.

Example 5.2. Taking $\ell(x) = l_7(x)l_8(x)l_9(x)l_{10}(x)$, $r = 22$ and $n = 2$, we gets the curve $\mathfrak{C}$ defined by the equation

$$y^2 = x\big(2+2x+x^2\big)^2\big(1+x+x^2+x^3+x^4\big)\big(1+2x+2x^2+x^3+x^4+2x^5+2x^6+2x^7+x^9\big),$$

which has $g(\mathfrak{C}) = 6$ and 345 rational points.

Example 5.3. The curve $\mathfrak{C}$ given by $y^{11} = 2 + x + x^2$ has $g(\mathfrak{C}) = 5$ and $\#\mathfrak{C}\big(\mathbb{F}_{3^5}\big) = 364$.

Here we take $r = n = 11$ and $\ell(x) = l_1(x)^2 l_2(x)$. Then $\mathcal{R}_\ell\big(x^{11}\big) = 2+x+x^2$.

Example 5.4. The curve $\mathfrak{C}$ defined by $y^{11} = (2+x)^3\big(2+x^2+x^3\big)$ has $g(\mathfrak{C}) = 15$ and $\#\mathfrak{C}\big(\mathbb{F}_{3^5}\big) = 519$.

We here take $r = n = 11$ and $\ell(x) = l_3(x)l_{11}(x)$. Hence

$$\mathcal{R}_\ell(x^{11}) = 1 + 2x^2 + x^3 + x^5 + x^6 = (2 + x)^3\big(2 + x^2 + x^3\big)$$

We summarize the results obtained in this section in Table 7.

q	r	$g(\mathfrak{C})$	$\#\mathfrak{C}\big(\mathbb{F}_q\big)$	old entry
3^5	2	4	306	
3^5	11	5	364	364
3^5	2	6	345	
3^5	11	15	519	

TABLE 7. Examples of curves with many points over $\mathbb{F}_{243}$.

References

[1] A García and H. Stichtenoth, *A Class of Polynomials over Finite Fields*, Finite Fields and Their Applications **5** (1999), 424–435.

[2] A. Garzón, *Euclidean Algorithm and Kummer Covers with many Points*, Revista Colombiana de Matemáticas **37** (2003), no. 1, 37–50.

[3] A. Garzón and A. García, *On Kummer Covers with many Points over Finite Fields*, Journal of Pure and Applied Algebra **185** (2003), 177–192.

[4] H Niederreiter and C.P Xing, *Rational Points on Curves over Finite Fields. Theory and Applications*, LMS Lecture Note Series 285, Cambridge University Press, 2001.

[5] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, Germany, 1993.

[6] G. Van der Geer and M. Van der Vlugt, *Kummers Covers with many Points*, Finite Fields and their Appl. (2000), 327–341.

[7] ———, *Tables with many Points*, 2013, available in *http://manypoints.org.*

(Recibido en noviembre de 2012. Aceptado en septiembre de 2013)

Departamento de Matemáticas
Universidad del Valle
Facultad de Ciencias
Carrera 13 No 100-00
Cali, Colombia
e-mail: alvaro.garzon@correounivalle.edu.co
e-mail: horacio.navarro@correounivalle.edu.co

Esta página aparece intencionalmente en blanco