Finite Fields and Their Applications **8,** 166–170 (2002)
doi.10.1006/ffta.2001.0331, available online at http://www.idealibrary.com on IDEAL®

On a Problem of Garcia, Stichtenoth, and Thomas

H. W. Lenstra, Jr.

Department of Mathematics # 3840, University of California, Berkeley, California 94720-3840; and Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, the Netherlands
E-mail: hwl@math.berkeley.edu, hwl@math.leidenuniv.nl

Communicated by Michael Tsfasman

Received September 29, 2000; revised January 22, 2001; published online July 11, 2001

In a recent paper, Garcia, Stichtenoth, and Thomas exhibited, for every finite field E that is not a prime field, an explicit sequence of absolutely irreducible smooth projective curves C_n over E with genus tending to infinity and with $\# C_n(E)/\text{genus}(C_n)$ tending to a positive limit. I show that their construction does not work over prime fields. © 2002 Elsevier Science (USA)

Key Words: finite fields; polynomials; curves with many points.

In a recent paper, Garcia, Stichtenoth, and Thomas [1] proved the following result.

THEOREM 1. *Let E be a finite field, and let q be its cardinality. Denote by $E[X]$ the polynomial ring in one variable X over E, and by $\bar{E}$ an algebraic closure of E. Let m be an integer and $f \in E[X]$, and suppose that*

(i) *$m > 1$, and m divides $q - 1$;*
(ii) *f has degree m, and the leading coefficient of f is an mth power in E;*
(iii) *the number d of factors X in f satisfies* $\gcd(d, m) = 1$;
(iv) *there is a finite set $S \subset \bar{E}$ with $0 \in S$ such that $\{\alpha \in \bar{E}$: there exists $\beta \in S$ with $f(\alpha) = \beta^m\}$ is contained in S.*

Then for each non-negative integer n the equations

$$x_{i+1}^m = f(x_i) \qquad (0 \le i < n)$$

in $x_0, x_1, \ldots, x_n$ define an absolutely irreducible curve over E, and if C_n denotes the normalization of its projective closure then one has

$$\lim_{n\to\infty} \text{genus}(C_n) = \infty, \qquad \lim_{n\to\infty} \frac{\# C_n(E)}{\text{genus}(C_n)} > 0.$$

1071-5797/02 $35.00

This result is a consequence of Theorem 2.2 in [1], with the condition $S \subset E$ replaced by the weaker but still sufficient condition $S \subset \bar{E}$.

If p denotes the characteristic of E, and $q > p$, then $m = (q-1)/(p-1)$ and $f = 1 - (1+X)^m$ satisfy the conditions of Theorem 1, with $S = E$; see Example 2.3 in [1]. Thus, for every finite field E that is not a prime field one obtains an explicit family of curves showing that

$$\limsup_{C} \frac{\# C(E)}{\mathrm{genus}(C)} > 0,$$

with C ranging over all absolutely irreducible smooth projective curves over E, up to isomorphism. For finite prime fields the lim sup is still positive (see [2]), but the authors of [1] failed in their attempts to deduce this from Theorem 1 (see Remark 2.7 in [1]). In the present note I explain this failure by showing that, in the case in which q is prime, no pair m, f satisfying the conditions of Theorem 1 exists. More precisely, I prove the following result.

THEOREM 2. *Let q be a prime number, let E be a finite field of cardinality q, and let $E[X]$ and $\bar{E}$ be as above. Then there do not exist an integer m and a polynomial $f \in E[X]$ that have the following properties*:

(1) $m > 1$, *and m divides $q - 1$*;
(2) *f has degree m, and if $m = q - 1$ then the leading coefficient of f equals* 1;
(3) *the number d of factors X in f satisfies* $0 < d < m$;
(4) *there is a finite set $S \subset \bar{E}$ with $0 \in S$ such that $\{\alpha \in \bar{E}$: there exists $\beta \in S$ with $f(\alpha) = \beta^m\}$ is contained in S.*

I do not know whether this negative result can be extended to sequences of curves that are defined in a more general way. For example, one may replace the equation $x_{i+1}^m = f(x_i)$ by $f_0(x_{i+1}) = f_1(x_i)$, where f_0 and f_1 are polynomials or even rational functions; can one obtain, in this manner, a sequence of curves satisfying the conclusions of Theorem 1, if q is prime? Another problem is to classify, for general q, all pairs m, f that satisfy the conditions of Theorem 1.

For odd q, the pair $m = q - 1, f = 1 - (1+X)^{q-1}$ satisfies all conditions (with $d = 1$, $S = E$), except the condition on the leading coefficient; for $q = 2$, it violates only the condition $m > 1$.

Proof of Theorem 2. Let the notation be as in Theorem 2, and assume that m and f satisfy conditions (1)–(4). I shall derive a contradiction. Write $T = \{\beta^m : \beta \in S\}$. Then T is a finite subset of $\bar{E}$ containing 0, and for each $\alpha \in \bar{E}$ with $f(\alpha) \in T$ one has $\alpha^m \in T$. Define

$$g = \prod_{\gamma \in T} (X - \gamma).$$

This is a polynomial in $\bar{E}[X]$ of degree $t = \# T$. I prove the identity

$$(5) \qquad d \cdot X^{m-1} \cdot g(f) = g(X^m) \cdot f',$$

where f' is the derivative of f with respect to X. If α is a zero of $g(f)$ in $\bar{E}$, then $f(\alpha) \in T$, so $\alpha^m \in T$ and α is a zero of $g(X^m)$, of multiplicity m if $\alpha = 0$; in addition, the multiplicity of α as a zero of $g(f) = \prod_{\gamma \in T} (f - \gamma)$ is at most 1 more than the multiplicity of α as a zero of f'. This implies that the left side of (5) divides the right side. One proves equality by comparing the degree and the coefficient at X^{m+d-1}.

Denote the leading coefficient of f by a. Comparing leading coefficients in (5) one sees that $d \cdot a^t = m \cdot a$. If $a = 1$, then one has $d = m$ in E, contradicting that $0 < d < m < q$ since q is prime. This proves $a \neq 1$, so (2) shows that m is different from $q - 1$. Since m divides $q - 1$, it is at most $(q - 1)/2$, and one has $2m < q$.

Put $X = Y^{-1}$ in (5), divide by $d \cdot a^t = m \cdot a$, and multiply by Y^{m-1+tm}. Retaining, in the result, only the terms that have degree less than $2m$ in Y, one finds that the polynomial $h = a^{-1} \cdot Y^m \cdot f(Y^{-1}) \in E[Y]$ satisfies

$$(6) \qquad h^t + ba^{-1} \cdot Y^m \cdot h^{t-1} \equiv (1 + bY^m) \cdot (h - Yh'/m) \bmod Y^{2m},$$

where b denotes the coefficient of g at X^{t-1} and h' is the derivative of h with respect to Y. Note that h has degree $m - d$ in Y and that $h(0) = 1$.

Define $m' = m$ if $b \neq 0$ and $m' = 2m$ if $b = 0$. From (6) one obtains

$$h^{t-1} \equiv 1 - Yh'/(mh) \bmod Y^{m'}.$$

Let e be the number of factors Y in $h - 1$; then $0 < e \leq m - d$. Viewing the equation modulo Y^{e+1} one sees that $t - 1 \equiv -e/m \bmod q$. Write j for the residue class of $h^{e/m}$ modulo $Y^{m'}$, the exponent e/m being taken modulo q; this is well defined, since from $m' \leq 2m < q$ and $h(0) = 1$ it follows that $h^q \equiv 1 \bmod Y^{m'}$. One has $Yj'/j = ((e/m)Yh'/h \bmod Y^{m'})$, so in terms of j the equation reads $j^{-1} = 1 - Yj'/(ej)$; that is, $1 = j - Yj'/e$. Comparing coefficients at Y^i, $0 \leq i < m'$, one concludes that $j = (1 + cY^e \bmod Y^{m'})$ for some $c \in E$. Let n be the unique integer satisfying $0 < n < q$ and $n \equiv m/e \bmod q$. Then one has

$$h \equiv (1 + cY^e)^n \bmod Y^{m'}.$$

Since $h - 1$ has exactly e factors Y one has $c \neq 0$.

From $n < q$ it follows that the degrees of the non-zero terms of $(1 + cY^e)^n$ are precisely the numbers ie, $0 \leq i \leq n$. I deal first with the case $m' = 2m$. Since h has a non-zero term of degree $m - d$, one must have $m - d = ie$ for some i with $0 \leq i \leq n$. If $i < n$, then $(1 + cY^e)^n$ has also a non-zero term of degree $(i+1)e = m - d + e$, and $m - d + e < 2m = m'$ implies that h has a non-zero term of that degree as well, contradicting that h has degree $m - d$. If $i = n$, then one has $m - d = ne \equiv (m/e)e = m \bmod q$, which is also a contradiction. It follows that $m' = m$, so that $b \neq 0$.

Let $k \in E[Y]$ be such that $h = (1 + cY^e)^n - k \cdot Y^m$; so $k \cdot Y^m$ is the sum of the terms of degree at least m in $(1 + cY^e)^n$. Modulo Y^{2m}, the left side of (6) is

$$(1 + cY^e)^{nt} + (ba^{-1} - tk) \cdot Y^m \cdot (1 + cY^e)^{n(t-1)}$$

$$\equiv (1 + cY^e)^{n-1} + (ba^{-1} - tk) \cdot Y^m \cdot (1 + cY^e)^{-1}$$

since $n(t-1) \equiv -1 \bmod q$ and $nt = n + n(t-1) \equiv n - 1 \bmod q$. The factor $h - Yh'/m$ on the right of (6) equals

$$(1 + cY^e)^n - k \cdot Y^m - (ne/m) \cdot cY^e \cdot (1 + cY^e)^{n-1} + k \cdot Y^m + k' \cdot Y^{m+1}/m$$

$$= (1 + cY^e)^{n-1} + k' \cdot Y^{m+1}/m,$$

since $ne/m \equiv 1 \bmod q$. Substituting this in (6), canceling $(1 + cY^e)^{n-1}$, and dividing by Y^m, one finds

$$(ba^{-1} - tk) \cdot (1 + cY^e)^{-1} \equiv k' \cdot Y/m + b \cdot (1 + cY^e)^{n-1} \bmod Y^m.$$

In particular, one has $ba^{-1} - t \cdot k(0) = b$, which by $a \neq 1$ implies $k(0) \neq 0$. By the definition of k, this shows that $(1 + cY^e)^n$ has a non-zero term of degree m. Since h has degree $m - d$, one concludes that $m - d$ and m are two consecutive degrees of non-zero terms of $(1 + cY^e)^n$. Therefore $e = d$ and e divides m. The congruence $n \equiv m/e \bmod q$ now gives an equality $n = m/e$, and k equals the constant polynomial c^n. Thus, in the congruence just displayed one has $k' = 0$, and multiplying the congruence by $b^{-1} \cdot (1 + cY^e)$ one obtains

$$a^{-1} - b^{-1} \cdot t \cdot c^n \equiv (1 + cY^e)^n \bmod Y^m.$$

This implies that $1 + cnY^e$ is congruent to a constant modulo Y^{e+1}, contradicting $c \neq 0$ and $0 < n < q$. This contradiction completes the proof.

Remark. The identity (5), which forms the key to my proof, admits the following structural interpretation. Denote by $\mathbf{A}^1$ the affine line over $\bar{E}$, and let π, $\rho: \mathbf{A}^1 \to \mathbf{A}^1$ be the maps defined by X^m and f, respectively; these intervene in an obvious way in the definition of the curves C_n in Theorem 1. There are maps $C_n \to \mathbf{P}^1 = \mathbf{A}^1 \cup \{\infty\}$ of degree m^n that are unramified over the complement of T, and this is used in [1] to bound the growth of genus(C_n) as $n \to \infty$. Write, by abuse of notation, T for the divisor $(g) = \sum_{\gamma \in T} \{\gamma\}$ on $\mathbf{A}^1$, and denote by R_π and R_ρ the respective ramification divisors ("differents") of

π and ρ; these are defined by X^{m-1} and f'. With this notation, (5) is, as an identity between divisors, equivalent to $\rho^*T - R_\rho = \pi^*T - R_\pi$.

ACKNOWLEDGMENTS

I thank H. Stichtenoth for bringing the problem addressed here to my attention and J. Flynn for an inspiring discussion.

REFERENCES

1. A. Garcia, H. Stichtenoth, and M. Thomas, On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3** (1997), 257–274.
2. J.-P. Serre, Sur le nombre des points d'une courbe algébrique sur un corps fini, *C. R. Acad. Sci. Paris Sér. I Math.* **269** (1983), 397–402.