Séminaires & Congrès
11, 2005, p. 125–141

POINTLESS CURVES OF GENUS THREE AND FOUR

by

Everett W. Howe, Kristin E. Lauter & Jaap Top

***Abstract.* —** A curve over a field k is *pointless* if it has no k-rational points. We show that there exist pointless genus-3 hyperelliptic curves over a finite field $\mathbb{F}_q$ if and only if $q \leqslant 25$, that there exist pointless smooth plane quartics over $\mathbb{F}_q$ if and only if either $q \leqslant 23$ or $q = 29$ or $q = 32$, and that there exist pointless genus-4 curves over $\mathbb{F}_q$ if and only if $q \leqslant 49$.

***Résumé* (Courbes de genre 3 et 4 sans point). —** Une courbe sur un corps k est appelée *une courbe sans point* si elle n'a aucun point k-rationnel. Nous prouvons qu'il existe des courbes hyperelliptiques de genre trois sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 25$, qu'il existe des quartiques planes sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 23$, $q = 29$ ou $q = 32$, et qu'il existe des courbes de genre quatre sans point sur un corps fini $\mathbb{F}_q$ si et seulement si $q \leqslant 49$.

1. Introduction

What is the largest number of rational points there can be on a curve of genus g over a finite field $\mathbb{F}_q$? Researchers have been studying variants of this question for several decades. As van der Geer and van der Vlugt write in the introduction to their biannually-updated survey of results related to certain aspects of this subject, the attention paid to this question is

> motivated partly by possible applications in coding theory and cryptography, but just as well by the fact that the question represents an attractive mathematical challenge. [**4**]

The complementary question — What is the *smallest* number of rational points there can be on a curve of genus g over a finite field $\mathbb{F}_q$? — seems to have sparked little

2000 *Mathematics Subject Classification.* — Primary 11G20; Secondary 14G05, 14G10, 14G15.
***Key words and phrases.* —** Curve, hyperelliptic curve, plane quartic, rational point, zeta function, Weil bound, Serre bound.

interest among researchers, perhaps because of the apparent *lack* of possible applications in coding theory and cryptography for curves with few points. But despite the paucity of applications, there are still mathematical challenges associated with such curves. In this paper, we address one of them:

Problem. — *Given an integer $g \geqslant 0$, determine the finite fields $\mathbb{F}_q$ over which there exists a curve of genus g having no rational points.*

We will call a curve over a field k *pointless* if it has no k-rational points. Thus the problem we propose is to determine, for a given genus g, the finite fields $\mathbb{F}_q$ over which there is a pointless curve of genus g.

The solutions to this problem for $g \leqslant 2$ are known. There are no pointless curves of genus 0 over any finite field; this follows from Wedderburn's theorem, as is shown by [**18**, §III.1.4, exer. 3]. The Weil bound for curves of genus 1 over a finite field, proven by Hasse [**5**], shows that there are no pointless curves of genus 1 over any finite field. If there is a pointless curve of genus 2 over a finite field $\mathbb{F}_q$ then the Weil bound shows that $q \leqslant 13$, and in 1972 Stark [**19**] showed that in fact $q < 13$. For each $q < 13$ there do exist pointless genus-2 curves over $\mathbb{F}_q$; a complete list of these curves is given in [**14**, Table 4].

In this paper we provide solutions for the cases $g = 3$ and $g = 4$.

Theorem 1.1. — *There exists a pointless genus-3 curve over $\mathbb{F}_q$ if and only if either $q \leqslant 25$ or $q = 29$ or $q = 32$.*

Theorem 1.2. — *There exists a pointless genus-4 curve over $\mathbb{F}_q$ if and only if $q \leqslant 49$.*

In fact, for genus-3 curves we prove a statement slightly stronger than Theorem 1.1:

Theorem 1.3. — *There exists a pointless genus-3 hyperelliptic curve over $\mathbb{F}_q$ if and only if $q \leqslant 25$; there exists a pointless smooth plane quartic curve over $\mathbb{F}_q$ if and only if either $q \leqslant 23$ or $q = 29$ or $q = 32$.*

The idea of the proofs of these theorems is simple. For any given genus g, and in particular for $g = 3$ and $g = 4$, the Weil bound can be used to provide an upper bound for the set of prime powers q such that there exist pointless curves of genus g over $\mathbb{F}_q$. For each q less than or equal to this bound, we either provide a pointless curve of genus g or use the techniques of [**8**] to prove that none exists.

We wrote above that the question of how few points there can be on a genus-g curve over $\mathbb{F}_q$ seems to have attracted little attention, and this is certainly the impression one gets from searching the literature for references to such curves. On the other hand, the question has undoubtedly occurred to researchers before. Indeed, the third author was asked this very question for the special case $g = 3$ by both N.D. Elkies and J.-P. Serre after the appearance of his joint work [**1**] with Auer. Also, while it is true that there seem to be no applications for pointless curves, it *can* be useful

to know whether or not they exist. For example, Leep and Yeomans were concerned with the existence of pointless plane quartics in their work [**13**] on explicit versions of special cases of the Ax-Kochen theorem. Finally, we note that Clark and Elkies have recently proven that for every fixed prime p there is a constant A_p such that for every integer $n > 0$ there is a curve over $\mathbb{F}_p$ of genus at most $A_p np^n$ that has no places of degree n or less.

In Section 2 we give the heuristic that guided us in our search for pointless curves. In Section 3 we give the arguments that show that there are no pointless curves of genus 3 over $\mathbb{F}_{27}$ or $\mathbb{F}_{31}$, no pointless smooth plane quartics over $\mathbb{F}_{25}$, no pointless genus-3 hyperelliptic curves over $\mathbb{F}_{29}$ or $\mathbb{F}_{32}$, and no pointless curves of genus 4 over $\mathbb{F}_{53}$ or $\mathbb{F}_{59}$. Finally, in Sections 4 and 5 we give examples of pointless curves of genus 3 and 4 over every finite field for which such curves exist.

Conventions. — By a *curve* over a field k we mean a smooth, projective, geometrically irreducible 1-dimensional variety over k. When we define a curve by a set of equations, we mean the normalization of the projective closure of the variety defined by the equations.

Acknowledgments. — The first author spoke about the work [**8**] at AGCT-9, and he thanks the organizers Yves Aubry, Gilles Lachaud, and Michael Tsfasman for inviting him to Luminy and for organizing such a pleasant and interesting conference. The first two authors thank the editors for soliciting this paper, which made them think about other applications of the techniques developed in [**8**].

In the course of doing the work described in this paper we used the computer algebra system Magma [**2**]. Several of our Magma programs are available on the web: start at

`http://www.alumni.caltech.edu/~however/biblio.html`

and follow the links related to this paper. One of our proofs depends on an explicit description of the isomorphism classes of unimodular quaternary Hermitian forms over the quadratic ring of discriminant -11. The web site mentioned above also contains a copy of a text file that gives a list of the six isomorphism classes of such forms; we obtained this file from the web site

`http://www.math.uni-sb.de/~ag-schulze/Hermitian-lattices/`

maintained by Rainer Schulze-Pillot-Ziemen.

2. Heuristics for constructing pointless curves

To determine the correct statements of Theorems 1.1 and 1.2 we began by searching for pointless curves of genus 3 and 4 over various small finite fields. In this section we explain the heuristic we used to find families of curves in which pointless curves

might be abundant. We begin with a lemma from the theory of function fields over finite fields.

Lemma 2.1. — *Let L/K be a degree-d extension of function fields over a finite field k, let M be the Galois closure of L/K, let $G = \mathrm{Gal}(M/K)$, and let $H = \mathrm{Gal}(M/L)$. Let S be the set of places $\mathfrak{p}$ of K that are unramified in L/K and for which there is at least one place $\mathfrak{q}$ of L, lying over $\mathfrak{p}$, with the same residue field as $\mathfrak{p}$. Then the set S has a Dirichlet density in the set of all places of K unramified in L/K, and this density is*

$$\delta := \frac{\#\cup_{\tau\in G} H^\tau}{\#G}.$$

We have $\delta \geqslant 1/d$, with equality precisely when L is a Galois extension of K. Furthermore, we have $\delta \leqslant 1 - (d-1)/\#G$.

Proof. — An easy exercise in the class field theory of function fields (*cf.* [**6**, proof of Lem. 2]) shows that the set S is precisely the set of places $\mathfrak{p}$ whose Artin symbol $(\mathfrak{p}, L/K)$ lies in the union of the conjugates of H in G. The density statement then follows from the Chebotarev density theorem.

Since H is an index-d subgroup of G, we have

$$\frac{\#\cup_{\tau\in G} H^\tau}{\#G} \geqslant \frac{\#H}{\#G} = \frac{1}{d}.$$

If L/K is Galois then H is trivial and the first relation in the displayed equation above is an equality. If L/K is not Galois then H is a non-normal subgroup of G, so the first relation above is an inequality.

To prove the upper bound on δ, we note that two conjugates H^σ and H^τ of H are identical when σ and τ lie in the same coset of H in G, so when we form the union of the conjugates of H we need only let τ range over a set of coset representatives of the d cosets of H in G. Furthermore, the identity element lies in every conjugate of H, so the union of the conjugates of H contains at most $d \cdot \#H - (d-1)$ elements. The upper bound follows. □

Note that the density mentioned in Lemma 2.1 is a Dirichlet density. If the constant field of K is algebraically closed in the Galois closure of L/K, then the set S also has a natural density (see [**10**]). In particular, the set S has a natural density when L/K is a Galois extension and L and K have the same constant field.

Lemma 2.1 leads us to our main heuristic:

Heuristic. — *Let $C \to D$ be a degree-d cover of curves over $\mathbb{F}_q$, let L/K be the corresponding extension of function fields, and let δ be the density from Lemma 2.1. If the constant field of the Galois closure of L/K is equal to $\mathbb{F}_q$, then C will be pointless with probability $(1-\delta)^{\#D(\mathbb{F}_q)}$. In particular, if $C \to D$ is a Galois cover, then C will be pointless with probability $(1-1/d)^{\#D(\mathbb{F}_q)}$.*

Justification. — Lemma 2.1 makes it reasonable to expect that with probability $1-\delta$, a given rational point of D will have no rational points of C lying over it. Our heuristic follows if we assume that all of the points of D behave independently. □

Consider what this heuristic tells us about hyperelliptic curves. Since a hyperelliptic curve is a double cover of a genus-0 curve, we expect that a hyperelliptic curve over $\mathbb{F}_q$ will be pointless with probability $(1/2)^{q+1}$. However, if the hyperelliptic curve has more automorphisms than just the hyperelliptic involution, it will be more likely to be pointless. For instance, suppose C is a hyperelliptic curve whose automorphism group has order 4. This automorphism group will give us a Galois cover $C \to \mathbb{P}^1$ of degree 4. Then our heuristic suggests that C will be pointless with probability $(3/4)^{q+1}$.

This heuristic suggested two things to us. First, to find pointless curves it is helpful to look for curves with larger-than-usual automorphism groups. We decided to focus on curves whose automorphism groups contain the Klein 4-group, because it is easy to write down curves with this automorphism group and yet the group is large enough to give us a good chance of finding pointless curves. Second, the heuristic suggested that we look at curves C that are double covers of curves D that are double covers of $\mathbb{P}^1$. The Galois group of the resulting degree-4 cover $C \to \mathbb{P}^1$ will typically be the dihedral group of order 8, and the heuristic predicts that C will be pointless with probability $(5/8)^{q+1}$. For a fixed D, if we consider the family of double covers $C \to D$ with C of genus 3 or 4, our heuristic predicts that C will be pointless with probability $(1/2)^{\#D(\mathbb{F}_q)}$. If $\#D(\mathbb{F}_q)$ is small enough, this probability can be reasonably high.

The curves that we found by following our heuristic are listed in Sections 4 and 5.

3. Proofs of the theorems

In this section we prove the theorems stated in the introduction. Clearly Theorem 1.1 follows from Theorem 1.3, so we will only prove Theorems 1.2 and 1.3.

Proof of Theorem 1.3. — The Weil bound says that a curve of genus 3 over $\mathbb{F}_q$ has at least $q + 1 - 6\sqrt{q}$ points, and it follows immediately that if there is a pointless genus-3 curve over $\mathbb{F}_q$ then $q < 33$. In Section 4 we give examples of pointless genus-3 hyperelliptic curves over $\mathbb{F}_q$ for $q \leqslant 25$ and examples of pointless smooth plane quartics for $q \leqslant 23$, for $q = 29$, and for $q = 31$. To complete the proof, we need only prove the following statements:

(1) There are no pointless genus-3 curves over $\mathbb{F}_{31}$.
(2) There are no pointless genus-3 curves over $\mathbb{F}_{27}$.
(3) There are no pointless smooth plane quartics over $\mathbb{F}_{25}$.
(4) There are no pointless genus-3 hyperelliptic curves over $\mathbb{F}_{32}$.
(5) There are no pointless genus-3 hyperelliptic curves over $\mathbb{F}_{29}$.