Non-existence of a Curve over $\mathbb{F}_3$ of Genus 5 with 14 Rational Points

Kristin Lauter

klauter@math.lsa.umich.edu

1 Introduction

The purpose of this note is to explain the significance and proof of the theorem alluded to in the title:

Theorem 1 *An absolutely irreducible, smooth, projective curve of genus* 5 *over* $\mathbb{F}_3$ *with* 14 *rational points cannot exist.*

The significance of this statement is best explained by considering the known bounds on the number of rational points on a curve of genus g over the field $\mathbb{F}_q$. Throughout this paper we will use curve to mean an absolutely irreducible, smooth, projective curve. The Weil bound,

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

shows in this case that the number of points must be less than or equal to 21. The Serre bound,

$$\#X(\mathbb{F}_q) \leq q + 1 + g[2\sqrt{q}],$$

shows that it must be less than or equal to 19. Oesterlé's optimization of the bounds from "Weil's explicit formulae" shows that it must be less than or equal to 14, so this theorem distinguishes a case where the Oesterlé bound cannot be met.

As this example illustrates, Oesterlé's bounds are much stronger than the Weil bound when the genus is large compared to q. In fact, Ihara [2] showed that the Weil bound is never attained if g is larger than $\sqrt{q}(\sqrt{q}-1)/2$. In tables for the number of points on curves, the maximum number of points for a given genus is often very close to, but not equal to the Oesterlé bound. Yet at the moment, we have no method for obtaining better bounds. It is possible that for each q, there may be an infinite number of values for the genus such that the Oesterlé bound cannot be met, but for g large, say $g > 4$, the only example known where the bound could not be met was found by Serre in 1983 ([5]). Serre found by hand a choice of trigonometric polynomial such that the upper bound on the number of points for a curve over $\mathbb{F}_2$ of genus 7 is 11. Serre then showed that there does not exist such a curve and that the maximum number of points is actually 10. The theorem stated above provides the second example of a case where the Oesterlé bound is not tight. We obtained this theorem by applying Serre's ideas to other cases in the attempt to produce more examples and to understand the circumstances which lead to the failure of these bounds.

The proof consists of making a finite list of possibilities for the zeta function of such a curve and then ruling them all out. The numerator of the zeta function is the characteristic polynomial of the map induced by the Frobenius endomorphism on the Tate module of the Jacobian variety of the curve. A possibile zeta function is eliminated from the list if the eigenvalues of Frobenius are such that the Jacobian of the curve would be decomposable as a polarized abelian variety, since this is impossible.

I would like to thank Rene Schoof and Jean-Pierre Serre for their help and suggestions.

2 Zeta Functions

In this section we collect a few facts about the zeta function of a curve X, defined over a finite field $\mathbb{F}_q$. It is given by the expression

$$Z(X,t) = \exp(\sum_{n\geq 1} \#X(\mathbb{F}_{q^n})\frac{t^n}{n}).$$

It follows from the proof of the Weil conjectures (see [3], for example) that this power series is actually a rational function,

$$Z(X,t) = \frac{h(t)}{(1-t)(1-qt)},$$

where

$$h(t) = \prod_{i=1}^{g}(1-\alpha_i t)(1-\bar{\alpha}_i t),$$

α_i and $\bar{\alpha}_i$ are the eigenvalues of Frobenius acting on the Tate module of the Jacobian of the curve. Since the α_j have absolute value $\sqrt{q}$, we write

$$\alpha_j = \sqrt{q}e^{i\theta_j}.$$

Setting $N_n = \#X(\mathbb{F}_{q^n})$, the expression

$$N_n = q^n + 1 - \sum_{i=1}^{g}(\alpha_i^n + \bar{\alpha_i}^n)$$

then gives the Weil bound when $n = 1$. We can also write

$$N_n = \sum_{d|n} da_d,$$

where a_d is the number of places of degree d on the curve.

Our goal is to exploit facts about N_n to get constraints on the possibilities for $h(t)$.

3 Bounds from Trigonometric Polynomials

A more detailed explanation of the material in this section along with an explanation of Oesterlé's bounds can be found in [4] or [5]. Given any trigonometric polynomial of the form

$$f(\theta) = 1 + 2\sum_{n=1}^{\infty} c_n \cos(n\theta)$$

where the $\{c_n\}$ are non-negative real numbers not all zero, and $f(\theta) \geq 0$, for all θ, we form the series

$$\Psi_d(t) = \sum_{n=1}^{\infty} c_{nd} t^{nd}.$$

N_m can be rewritten as

$$N_m = 1 + q^m - 2q^{m/2} \sum_{j=1}^{g} \cos(m\theta_j).$$

If we multiply this through by $c_m q^{-m/2}$, sum over m, and substitute in the expression for N_m in terms of the a_d from above, we obtain a bound which will be useful in our argument:

$$(*) \qquad \sum_{d\geq 2} d a_d \Psi_d(q^{-1/2}) \leq g + \Psi_1(q^{1/2}) - (N_1 - 1)\Psi_1(q^{-1/2}).$$

4 Proof of the Theorem

The main tool in the proof is an auxiliary polynomial related to $h(t)$,

$$F(T) = \prod_{i=1}^{g} (T - u_i),$$

where $u_i = \alpha_i + \bar{\alpha}_i$, α_i as in Section 2. The $\{u_i\}$ are all real numbers of absolute value less than or equal to $2\sqrt{q}$, so it follows that $F(T)$ and all of its derivatives have *all* of their roots real and in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. Write $F(T) = \sum_{i=0}^{g} b_i T^i$, so that the $\{b_i\}$ are the elementary symmetric polynomials in the $\{u_i\}$. Define

$$s_n = \sum_{i=1}^{g} u_i^n.$$

Then Newton's identities [1], A IV.65 express the $\{b_i\}$ in terms of the $\{s_n\}$, and the $\{s_n\}$ are in turn integral polynomials in the N_n, so we have the relations:

$$b_1 = -s_1, \quad b_2 = (s_1^2 - s_2), \quad \ldots \quad ,$$

$$0 = s_n + b_1 s_{n-1} + b_2 s_{n-2} + \ldots + n b_n,$$

and

$$s_1 = (q+1) - N_1, \quad s_2 = (q^2+1) - N_2 + 2gq, \quad \ldots \quad ,$$
$$s_5 = (q^5+1) - N_5 + 5q(q^3+1-N_3) + 10q^2 s_1.$$

Now assume that a curve of genus 5 over $\mathbb{F}_3$ with 14 rational points exists. In this case, the above relations lead to the following expression for $F(T)$ in terms of the $\{a_d\}$:

$$F(T) = T^5 + 10T^4 + (a_2+37)T^3 + (10a_2+a_3+62)T^2 + (\tfrac{1}{2}a_2^2 + \tfrac{87}{2}a_2 + 10a_3 + a_4 + 32)T + (5a_2^2 + a_2a_3 + 127a_2 + 46a_3 + 10a_4 + a_5 - 184).$$

The following choice for $\{c_n\}$,

$$c_1 = \frac{\sqrt{3}}{2}, \quad c_2 = \frac{7}{12}, \quad c_3 = \frac{\sqrt{3}}{6}, \quad c_4 = \frac{1}{12},$$

(associated to the trigonometric polynomial $f = \cos^2\theta(1 + \frac{2}{\sqrt{3}}\cos\theta)^2$) when inserted into (*) leads to the bound $a_2 \leq 1$.

Using the condition on the roots of $F(T)$ and its derivatives and the bound $a_2 \leq 1$ obtained above, we check that the only possibility for (a_2, a_3, a_4, a_5) is $(0, 0, 14, 56)$. To start, the possibilities with $a_2 = 1$ are eliminated because the roots of the third derivative would not be such that the second derivative could have all its roots be real. If $a_2 = 1$, then $F'''(T) = 60T^2 + 240T + 228$ and $F''(T) = 20T^3 + 120T^2 + 228T + 144 + 2a_3$, and the roots of F''' do not allow any choice of a_3 such that the maximum is above the x-axis and the minimum is below.

Now suppose a_2 is zero. Then a_3 must be less than or equal to three in order for F'' to have real roots. For each choice of $a_3 = 0, 1, 2, 3$, we make a list of the possibilities for a_4 by checking the sign of the F' at the roots of F''. When F' is evaluated at the smallest root of F'', the value should be negative, the second root should give a positive value, and the third root a negative value. Thus for

$a_3 = 0$, we must have $12 \leq a_4 \leq 16$, for
$a_3 = 1$, we must have $6 \leq a_4 \leq 8$, for
$a_3 = 2$, we must have $a_4 = 0$, and
$a_3 = 3$, is not possible.

The case $a_3 = 2$, $a_4 = 0$ is ruled out since F' would not have all its roots in the correct interval. Similarly, checking the values of F at the roots of F', we find that:

$a_3 = 0$, $a_4 = 12 \Rightarrow a_5 = 72$
$a_3 = 0$, $a_4 = 13 \Rightarrow a_5 = 64$
(**) $a_3 = 0$, $a_4 = 14 \Rightarrow a_5 = 56$
$a_3 = 0$, $a_4 = 15$ or 16, not possible.
$a_3 = 1$, $a_4 = 6 \Rightarrow a_5 = 90$
$a_3 = 1$, $a_4 = 7 \Rightarrow a_5 = 82$
$a_3 = 1$, $a_4 = 8 \Rightarrow a_5 = 73$

Finally, we check that none of the polynomials corresponding to these possibilities have all five of their roots in the correct interval except the one corresponding to (**), which is

$$F(T) = T^5 + 10T^4 + 37T^3 + 62T^2 + 46T + 12.$$

The polynomial $F(T)$ factors as the product of two polynomials

$$r(T) = (T^2 + 4T + 2)(T + 2) \text{ and } s(T) = (T + 1)(T + 3)$$

with coefficients in $\mathbb{Z}$. The polynomials r and s are coprime in the strong sense that their resultant is -1, which is a unit in $\mathbb{Z}$. Now we use a powerful argument due to Serre to show that this is not possible [6], [5].

Lemma 1 *Let $F(T) = \prod_{i=1}^{g}(T - u_i)$ be the polynomial with $u_i = \alpha_i + \bar{\alpha}_i$, $\{\alpha_i\}$ the set of eigenvalues of Frobenius of an absolutely irreducible, smooth, projective curve. Then $F(T)$ cannot be factored as $F(T) = r(T)s(T)$, with r and s non-constant polynomials in $\mathbb{Z}[T]$ such that resultant$(r, s) = \pm 1$.*

Proof: Suppose to the contrary that the polynomial $F(T)$ associated to such a curve can be written as $F(T) = r(T)s(T)$, with r and s non-constant polynomials in $\mathbb{Z}[T]$ with resultant$(r, s) = \pm 1$. This is equivalent by ([1], A IV.73) to the existence of two polynomials, $a, b \in \mathbb{Z}[T]$ such that $ar + bs = 1$. Note that in the case considered above, we can take $a(T) = -(T + 2)$, $b(T) = T^2 + 4T + 3$.

Denote by $Frob$ the Frobenius endomorphism of the Jacobian of the curve, and by V the unique endomorphism satisfying the relation

$$Frob \circ V = V \circ Frob = q.$$

Then the endomorphism $C = Frob + V$ has as characteristic polynomial F^2, and in fact $F(C) = 0$. Consider the two endomorphisms $p = a(C)r(C)$ and $p' = b(C)s(C)$. Then p and p' are idempotents since $pp' = p'p = 0$ and $p+p' = 1$. These two idempotents decompose the Jacobian into a direct sum

$$J = B \oplus B', \text{ where } B = ker\ p,\ B' = ker\ p'.$$

The fact that this decomposition is compatible with the principal polarization of the Jacobian variety follows from the fact that p and p' are Hermitian. Such a decomposition is impossible for a Jacobian variety since it contradicts the irreducibility of the theta divisor. □

Remark 1 *The method detailed above has also lead to the proof that the Oesterlé bound $N = 17$ cannot be met for a curve of genus 7 over $\mathbb{F}_3$. In that case there are two possible zeta functions which must be eliminated by the application of Lemma 1.*

References

[1] N. Bourbaki, *Algèbre*, chap. IV, Herrmann, Paris, 1958.

[2] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, *J. Fac. Sci. Tokyo* **28** (1981), p. 721-724.

[3] J. Milne, *Etale Cohomology.* Princeton University Press: Princeton, NJ, 1980.

[4] R. Schoof, *Algebraic curves and coding theory*, UTM 336, Univ. of Trento, 1990.

[5] J.-P. Serre, *Rational Points on curves over finite fields.* Notes by F. Gouvea of lectures at Harvard University, 1985.

[6] J.-P. Serre, Letter to K. Lauter, December 3, 1997.

Mathematics Subject Classification Numbers: 11R58, 14G10
Key words: rational points on curves over finite fields, zeta functions, Jacobians