Plane curves with many points over finite fields

Matthew L. Carlin and José Felipe Voloch

The purpose of this paper is to construct plane curves over finite fields which meet the upper bound of [SV] Thm 0.1 (recalled below) for the number of their rational points. We also prove an irreducibility criterion for plane curves.

The upper bound of [SV] Thm 0.1 is the first inequality of the following Theorem in the special case of irreducible curves.

Theorem 1. *Let C be a (possibly reducible) plane algebraic curve defined over $\mathbf{F}_p$, p prime, of degree $d < p$. Suppose that C does not have a linear component defined over $\mathbf{F}_p$. Then $\#C(\mathbf{F}_p) \leq d(d+p-1)/2$. If $\#C(\mathbf{F}_p) \geq d(d+p-1)/2 - (d-1)$, then C is absolutely irreducible.*

Proof: Without loss of generality, we can assume C is reduced, for the conditions are only strengthened in this case. Let $C_1, \ldots, C_m$ be the components of C over $\mathbf{F}_p$ and let d_i be the degree of C_i. By hypothesis $d_i > 1$ for all i. If C_i is absolutely irreducible, then by [SV], Theorem 0.1, $\#C_i(\mathbf{F}_p) \leq d_i(d_i+p-1)/2$, whereas if C_i is not absolutely irreducible, then $\#C_i(\mathbf{F}_p) \leq d_i^2/4$ as follows from the proof of Lemma 3.3 of [RV]. As $d_i^2/4 < d_i(d_i+p-1)/2$, we also get the first bound when C_i is not absolutely irreducible. Now

$$\#C(\mathbf{F}_p) \leq \sum \#C_i(\mathbf{F}_p) \leq \sum d_i(d_i+p-1)/2.$$

From $\sum d_i = d$ we get that

$$\sum d_i(d_i+p-1)/2 = d(d+p-1)/2 - \sum_{i<j} d_i d_j.$$

This, combined with the last inequality, gives the first statement of the theorem. To get the second statement, consider the case that C is not absolutely irreducible. If $m > 1$,

then assume without loss of generality that $d_1 \leq d_i, i > 1$. It follows that

$$\sum_{i<j} d_i d_j \geq d_1(d_2 + \cdots + d_m) \geq 2(d_2 + \cdots + d_m) \geq d_1 + d_2 + \cdots + d_m = d.$$

So $\#C(\mathbf{F}_p) \leq d(d+p-1)/2 - d$. If $m = 1$ then C is irreducible but not absolutely irreducible so, as noted above, $\#C(\mathbf{F}_p) \leq d^2/4$. This implies the requisite inequality unless $p = 2$ and $d = 1$ but then C is absolutely irreducible and this completes the proof.

This result is useful when it easy to check that C contains no lines defined over $\mathbf{F}_p$. The following easy lemma gives a criterion for that to happen.

Lemma. *Let $C/\mathbf{F}_p$ be a plane curve which has no rational points in common with a given line defined over $\mathbf{F}_p$. Then C contains no line defined over $\mathbf{F}_p$.*

Proof: Indeed, if C contains a line defined over $\mathbf{F}_p$, the intersection of this line with the given line will be a rational point common to C and the given line, contrary to the hypothesis.

Remarks:

(i) It may appear that the conditions of the lemma and the theorem are hard to meet but, in fact, we will be using exactly these conditions on the examples below.

(ii) It can also be shown that if, under the assumptions of the theorem, we have $\#C(\mathbf{F}_p) = d(d+p-1)/2$ then C is actually smooth.

Theorem 2. *let p be a prime, $p \equiv 1 \bmod 4$, and c a nonsquare in $\mathbf{F}_p$. Let C be the projective curve defined by*

$$g = (y + cz)^{(p-1)/2} + y^{(p-1)/2} - z^{(p-1)/2} - x^{(p-1)/2} = 0.$$

Then C has $3(p-1)^2/8$ points over $\mathbf{F}_p$.

Proof: Consider first points with $z = 0$. It is clear that there are no points with $z = x = 0$, so assume without loss of generality that $x = 1$. The condition that $(y + c)^{(p-1)/2} + y^{(p-1)/2} = 1$ with $y \in \mathbf{F}_p$ implies that $y = 0$ or $y = -c$, but either of these cases lead to $c^{(p-1)/2} = 1$, which contradicts the assumption that c is a nonsquare in $\mathbf{F}_p$.

Likewise, it can be shown that there are no points with $x = 0$. Now, if $y = 0$, we get $2z^{(p-1)/2} + x^{(p-1)/2} = 0$ which is impossible with $x, z \neq 0$ unless $p = 3$, but since we assumed $p \equiv 1 \bmod 4$, this case doesn't happen.

Now assume without loss of generality that $z = 1$ and also that $x, y \neq 0$. The proof now break into four cases according to the quadratic character of x and y. If x, y are both non-zero squares, they give a point on the curve if and only if $y + c$ is a non-zero square also. The conic $u^2 + c = v^2$ has two rational points at infinity, and no rational point with $u = 0$ or $v = 0$. The other $p - 1$ points lead to $(p - 1)/4$ values of $y = u^2$ satisfying the above conditions and conversely every such y is obtained this way. As there are $(p-1)/2$ choices for x we get $(p-1)^2/8$ points on the curve. Likewise, the cases where both x, y are non-squares or x is a non-square and y is a non-zero square, each contribute $(p - 1)^2/8$ points. The case where y is a non-square and x is a non-zero square lead to $(y+c)^{(p-1)/2} = 3$ which is impossible. So there is a total of $3(p-1)^2/8$ points on the curve over $\mathbf{F}_p$.

Remarks:

(i) Likewise it can be shown that the curves defined by

$$(y + z)^{(p-1)/2} + y^{(p-1)/2} - z^{(p-1)/2} - x^{(p-1)/2} = 0$$

and

$$(cy + z)^{(p-1)/2} + y^{(p-1)/2} - z^{(p-1)/2} - x^{(p-1)/2} = 0$$

both have $3(p - 1)^2/8 - (p - 5)/2$ points over $\mathbf{F}_p$.

(ii) In all these cases theorem 1 and the lemma (with the given line being $x = 0$, say) apply to prove that the curve in question is irreducible and, in the case of the curve of the theorem, even smooth (by a previous remark), since the curve of theorem 2 attains the bound $d(d + p - 1)/2$.

(iii) These curves are all obtained by slicing the surface

$$w^{(p-1)/2} + y^{(p-1)/2} - z^{(p-1)/2} - x^{(p-1)/2} = 0$$

by certain planes. This is a smooth surface with many points for its degree (compare [V]) but it also has many lines. The slicing is done so as to avoid picking up these lines as components.

Theorem 3. *let p be a prime, $p \equiv 3 \bmod 4$, and c a nonsquare in $\mathbf{F}_p$. Let C be the projective curve defined by the affine equation $g(x,y) = (f(x) - f(y))/(x - y)$ where $f(x) = (x + c)^{(p-1)/2} + x^{(p-1)/2}$. Then C has $(p-3)(3p-5)/8$ points over $\mathbf{F}_p$.*

Proof: It is easy to see that C has $(p-3)/2$ rational points at infinity. To compute the affine points, notice that $f(x) = 0$ if $x \in \mathbf{F}_p$ is such that x is a non-zero square and $x+c$ is a non-square or if x is a non-square and $x+c$ is a non-zero square. By an argument identical to one in the proof of theorem 2, there are $(p-1)/2$ such values of x and taking pairs of distinct such values give $(p-1)(p-3)/4$ rational points on C. Further, $f(x) = 2$ if both x and $x+c$ are non-zero squares. Again, there are $(p-3)/4$ such values of x and taking pairs of distinct such values give $(p-7)(p-3)/8$ rational points on C. The same number of points is obtained by looking at $f(x) = -2$. We have thus found $(p-3)(3p-5)/8$ rational points on C. We claim that C has no rational point with $x = 0$. Indeed, $f(0) = -1$ and if $y \neq 0, y \in \mathbf{F}_p, f(y) = 0, \pm 2$, unless $y = -c$ which satisfies $f(y) = 1$, so C has no rational point with $x = 0$ and $y \neq 0$. Finally $(0,0) \notin C$ since $f'(0) \neq 0$. The lemma now gives that C has no rational linear component, so theorem 1 gives that C has at most $(p-3)(3p-5)/8$ points over $\mathbf{F}_p$. As we have seen that C has at least that many points, we conclude the proof.

Remark: Again it follows that C is irreducible and smooth.

In [RVZ] there are examples attaining the upper bound in theorem 1 for all degrees d of the form $p - 1 - 2k$, where k is any divisor of $p - 1$ with $k < (p-1)/2$. Taking $k = (p-1)/4$ gives examples of the same degree as those of theorem 2, but the curves can be shown to be different. The degree of the curves in theorem 3 is $(p-3)/2$ which is not of the form of the examples of [RVZ]. Serre (see [L]) has given constructions of curves of degree 4 for $5 \leq p \leq 23$ attaining the upper bound in theorem 1, but in some cases (such

as $p = 11$) the construction is not explicit. Theorem 3 gives an explicit example for $p = 11$ of a smooth plane quartic (so a curve of genus 3) with 28 rational points.

One only knows improvements to the upper bound in theorem 1 for $d < p/15$ roughly (or for $d > p$, but this is trivial), these come from [SV] or from results such as the Hasse-Weil that apply to all curves. Is it possible that the upper bound in theorem 1 is always attained if d is even and $(p-1)/15 \leq d \leq p-1$?

Acknowledgements: The first author would like to thank the NSF VIGRE program for financial support.

References.

[L] K. Lauter (with an appendix by J-P. Serre), *The maximum or minimum number of rational points on curves of genus three over finite fields*, preprint 2001.

[RV] F. Rodríguez Villegas and J. F. Voloch, *On certain plane curves with many integral points*, Experimental Math. **8** (1999), 57–62.

[SV] Stöhr, K-O. and Voloch, J.F., *Weierstrass Points and Curves over Finite Fields*, Proc. London Math. Soc.(3) **52** (1986), 1–19

[RVZ] F. Rodríguez Villegas, J. F. Voloch and D. Zagier *Constructions of plane curves with many points*, Acta Arith. **XCIX** (2001), 85–96.

[V] Voloch, J.F., *Surfaces in* $\mathbf{P}^3$ *over Finite Fields*, preprint 2001.

Dept. of Mathematics, Univ. of Texas, Austin, TX 78712, USA

e-mail: mcarlin,voloch@math.utexas.edu