

Supersingular curves defined over finite fields

by

Saeed Tafazolian

(IMPA at Rio de Janeiro)

1 Abstract

More than half a century ago, André Weil proved a formula for the number $N = \#\mathcal{C}(\mathbb{F}_q)$ of rational points on a smooth geometrically irreducible projective curve \mathcal{C} of genus g defined over a finite field \mathbb{F}_q . This formula provides upper and lower bounds on the number of rational points possible. It states that:

$$q + 1 - 2g\sqrt{q} \leq N \leq q + 1 + 2g\sqrt{q}.$$

We say a curve is *maximal* (resp. *minimal*) if it attains the above upper (resp. lower) bound.

By definition an abelian variety in characteristic positive is supersingular if the first crystalline cohomology groups has all slopes equal $1/2$ and a curve is supersingular if its Jacobian is. Maximal and minimal curves are supersingular. Furthermore one can see supersingular curves defined over finite fields are minimal over some extension of the base field. Thus their Newton polygons are also maximal in the sense that all slopes are equal to $1/2$. Finally the p -rank of a curve is exactly equal to the length of the slope zero segment of its Newton polygon. Clearly, the p -rank of a maximal (or minimal) curve is zero.

The Hasse-Witt matrix \mathcal{H} of a non-singular algebraic curve \mathcal{C} over a finite field \mathbb{F}_q is the matrix of the Frobenius mapping (p -th power mapping) with respect to any basis for the differentials of the first kind. It is a $g \times g$ matrix where g is the genus of \mathcal{C} . We know also the dual of Frobenius mapping which is the so-called Cartier operator, denoted by \mathcal{C} , acting on differential 1-forms. As maximal curves are supersingular, we have that the Cartier operator is nilpotent. Furthermore using the acting Frobenius on the first crystalline cohomology, we show the following result:

Theorem 1.1. *Let \mathcal{C} be a curve defined over a finite field with q^2 elements, where $q = p^n$ for some $n \in \mathbb{N}$. If \mathcal{C} is maximal (or minimal) over \mathbb{F}_{q^2} , then $\mathcal{C}^n = 0$.*

Now using Theorem 1.1 and above properties of supersingular curves we can find some classification of maximal and minimal curves as below (see [2]):

Theorem 1.2. *Let $\mathcal{C}(m)$ be the Fermat curve of degree m prime to the characteristic p defined over \mathbb{F}_{q^2} . Then $\mathcal{C}(m)$ is maximal over \mathbb{F}_{q^2} if and only if m divides $q + 1$.*

Theorem 1.3. *Let \mathcal{C} be a curve defined by the equation $y^q - y = f(x)$, where $f(x) \in \mathbb{F}_{q^2}[x]$ is a polynomial of degree d prime to p . If \mathcal{C} is maximal over \mathbb{F}_{q^2} , then the curve \mathcal{C} is isomorphic to the projective curve defined by the following affine equation*

$$y^q + y = x^d \quad \text{with } d \text{ a divisor of } q + 1.$$

Theorem 1.4. *Let \mathcal{C} be a hyperelliptic curve over $\mathbb{F}_{p^{2n}}$ where $q = p^n$. If $\mathcal{C}^n = 0$, then*

$$g(\mathcal{C}) \leq \frac{q}{2}.$$

Moreover, there is a unique maximal hyperelliptic curve over \mathbb{F}_{q^2} of the above genus bound. It can be given for $p > 2$ by the affine equation

$$y^2 = x^q + x,$$

and for $p = 2$ by

$$y^2 + y = x^{q+1}.$$

References

- [1] A. Garcia and S. Tafazolian, *On additive polynomials and certain maximal curves*, Preprint.
- [2] A. Garcia and S. Tafazolian, *Cartier operators and maximal curves*, Preprint.