Counting Rational Points on Supersingular Curves

Beyza Çepni, Hasan Bilgili, Farzin Azar, Mohammad Hamdar

CIMPA-SuSAAN

June 17, 2022

Let p be an odd prime and $q = p^r$ for some $r \in \mathbb{Z}^+$. We are mainly interested in the number of zeros of Artin-Schreir type curves

$$y^q - y = f(x) \text{ where } f(x) \in \mathbb{F}_q[x].$$

over $\mathbb{F}_q$. Mostly, we focus on *supersingular* Artin-Scherier curves.

Linearized Polynomials

A polynomial of the form

$$L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$$

with coefficients in an extension field $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ is called a *q-polynomial* over $\mathbb{F}_{q^m}$. Observe that the L-polynomial of our curve is $\mathbb{F}_q$-linear.

Quadratic Forms

It is well-known that the function from $\mathbb{F}_{q^n}$ to $\mathbb{F}_q$ such that

$$x \mapsto \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(xL(x))$$

is a quadratic form over $\mathbb{F}_q$. The number of zeros of such a quadratic form Q can be written as

$$q^{n-1} + \lambda(q-1)q^{\frac{n+w}{2}-1}$$

where $\lambda \in \{-1, 0, 1\}$ and w is the dimension of

$$\{x \in \mathbb{F}_{q^n} \ : \ Q(x+y) - Q(x) - Q(y) = 0 \ \text{ for all } \ y \in \mathbb{F}_{q^n}\}$$

of Q when q is odd. The dimension of radical of Q has slightly different definition for even characteristic. Note if n and w have different parity (odd/even), then λ has to be 0. Otherwise, it should be ± 1.

Reduction Theorem for Supersingular Curves

Theorem

Let C be a supersingular curve of genus g defined over $\mathbb{F}_q$ with period s. Let n be a positive integer, let $m = gcd(n, s)$ and write $n = m \cdot t$. If q is odd, then we have

$$\#C(\mathbb{F}_{q^n}) - (q^n + 1) =$$

$$\begin{cases} q^{\frac{(n-m)}{2}}[\#C(\mathbb{F}_{q^m}) - (q^m + 1)] & \textit{if } m\cdot r \textit{ is even} \\ q^{\frac{(n-m)}{2}}[\#C(\mathbb{F}_{q^m}) - (q^m + 1)]\frac{(-1)^{(t-1)/2}}{p}t & \textit{if } m\cdot r \textit{ is odd and } p\nmid t \\ q^{\frac{(n-m)}{2}}[\#C(\mathbb{F}_{q^m}) - (q^m + 1)] & \textit{ifm}\cdot r \textit{ is odd and } p|t. \end{cases}$$

If q is even, then we have

$$\#C(\mathbb{F}_{q^n}) - (q^n + 1) =$$

$$\begin{cases} q^{\frac{(n-m)}{2}}[\#C(\mathbb{F}_{q^m}) - (q^m + 1)] & \textit{if } m\cdot r \textit{ is even} \\ q^{\frac{(n-m)}{2}}[\#C(\mathbb{F}_{q^m}) - (q^m + 1)](-1)^{(t^2-1)/8} & \textit{if } m\cdot r \textit{ is odd.} \end{cases}$$

Fibre Products of Artin-Schreier Curves

Consider

$$C: \ y^{q^n} - y = f(x)$$

over $\mathbb{F}_{q^n}$.
For $\alpha \in \mathbb{F}_{q^n}^*$, define

$$H_\alpha = \{x \in \mathbb{F}_{q^n} : \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha x) = 0\}.$$

Then H_α is an additive subgroup of $\mathbb{F}_q$. We can view H_α as a subgroup of $Aut(C)$. $|\mathbb{F}_{q^n}^*/\mathbb{F}_q^*| = \frac{q^n-1}{q-1}$ many α is enough for fibre product.

For

$$y_\alpha = \prod_{\gamma \in H_\alpha} (y + \gamma)$$

we have that

$$C_\alpha := C/H_\alpha : \; y_\alpha^q - y_\alpha = \alpha f(x).$$

Theorem

$$J_C \sim \prod_{\alpha \in \mathbb{F}_{q^n}^* / \mathbb{F}_q^*} J_{C_\alpha}$$

Therefore, the L-polynomial of the curve C is equal to product of the L-polynomials of the curves C_α.

Theorem

$$\#C(\mathbb{F}_{q^m}) - \sum_{\alpha \in \mathbb{F}_{q^m}^*/\mathbb{F}_q^*} \#C_\alpha(\mathbb{F}_{q^m}) = (q^m + 1)\left[1 - \frac{q^n - 1}{q - 1}\right].$$

The polynomial $x^t - a$

Theorem

Let $t \geq 2$ be an integer and $a \in \mathbb{F}_q^*$. Then $x^t - a$ is irreducible if and only if the following two conditions are satisfied:
1. Each prime factor of t divides the order of e of a in $\mathbb{F}_q^*$, but not $(q-1)/e$.
2. If $t \equiv 0 \; mod 4$ then $q \equiv 1 \; mod 4$.

If $q \equiv 3 \bmod 4$ then $q = 2^A u - 1$ with $A \geq 2$ and u is odd. Suppose that condition 1. is satisfied and t is divisible by 2^A. We write $t = Bv$ with $B = 2^{A-1}$ and v is even. Then $x^t - a$ factors as a product of B monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree $t/B = v$.

Theorem

Let

$$F(x) = \sum_{i=0}^{B/2} \frac{(B-i-1)!B}{i!(B-2i)!} x^{B-2i} \in \mathbb{F}_q[x].$$

Then roots $c_1, \ldots, c_B$ *are all in* $\mathbb{F}_q$*, and in* $\mathbb{F}_q[x]$ *we have the canonical factorization*

$$x^t - a = \prod_{j=1}^{B} (x^v - bc_j x^{v/2} - b^2).$$

Results

We counted number of rational points of the curve

$$y^{q^n} - y = \gamma x^{p^h+1} - \alpha \text{ where } \alpha \in \mathbb{F}_{q^m},\ \gamma \in \mathbb{F}_{q^m}^* \text{ and } h \in \mathbb{Z}_{\geq 0}$$

over $\mathbb{F}_{q^m}$, by finding

$$|\{x \in \mathbb{F}_{q^m} \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_p}(\gamma x^{q^h+1}) = \beta\}|$$

for each $\beta \in \mathbb{F}_p$.

Next Aim

Now, one of our aims is to find the 1rational points of the curve

$$y^q - y = x^{q^k+1} + ax^2 + bx + c \text{ where } a, b, c \in \mathbb{F}_q^*, k \in \mathbb{Z}^+.$$

References

1. Rudolf Lidl, Harald Niederreiter, Finite Fields, Addison-Wesley, New York, 1983.

2. Gary McGuire, Emrah Sercan Yilmaz, On the zeta functions of supersingular curves, Finite Fields and Their Applications, Volume 54, Pages 65-79, 2018.

3. Gary McGuire, Emrah Sercan Yilmaz, Divisibility of L-polynomials for a family of Artin-Schreier curves, Journal of Pure and Applied Algebra, Volume 223, Issue 8, Pages 3341-3358, 2019.

4. Emrah Sercan Yilmaz. The Number of Zeros of Quadratic Forms with Two Terms. arXiv preprint arXiv:2001.04764, 2020.

Thank You!