Value sets of Lattès maps over finite fields

Ömer Küçüksakallı

PII: S0022-314X(14)00153-X
DOI: 10.1016/j.jnt.2014.04.014
Reference: YJNTH 4866

To appear in: *Journal of Number Theory*

Received date: 13 November 2013
Revised date: 20 April 2014
Accepted date: 22 April 2014

Please cite this article in press as: Ö. Küçüksakallı, Value sets of Lattès maps over finite fields, *J. Number Theory* (2014), http://dx.doi.org/10.1016/j.jnt.2014.04.014

VALUE SETS OF LATTÈS MAPS OVER FINITE FIELDS

ÖMER KÜÇÜKSAKALLI

Abstract. We give an alternative computation of the value sets of Dickson polynomials over finite fields by using a singular cubic curve. Our method is not only simpler but also it can be generalized to the non-singular elliptic case. We determine the value sets of Lattès maps over finite fields which are rational functions induced by isogenies of elliptic curves with complex multiplication.

Introduction

The conditions for arbitrary functions of finite fields $\mathbf{F}_q$ to be bijections are rather complicated. Thus special types of functions are of great interest. One of the most important such family is the Dickson polynomials of the first type

$$D_n(x,a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j}\binom{n-j}{j}(-a)^j x^{n-2j}.$$

It is a well-known fact that $D_n(x,a)$, $a \in \mathbf{F}_q^*$, is a bijection of $\mathbf{F}_q$ if and only if $(n, q^2-1) = 1$ [LN83]. A harder problem is to determine the size of the value set

$$\{D_n(x,a) : x \in (\mathbf{F}_q)\}.$$

If $D_n(x,a)$ is not a bijection, one may ask how far it is away from being a bijection. For an arbitrary polynomial, there is no easy formula giving the cardinality of the value set. However Chou, Gomez-Calderon and Mullen achieve finding a formula for Dickson polynomials [CGM88] by tedious computations. In this paper we will give a shorter proof of this formula by using the singular cubic curve $C : y^2 = 4x^3 + x^2$ and the real cyclotomic fields. Our alternative proof fits into a larger body of work as well. Recently Gassert [Ga14] determined the graphs for polynomials $D_n(x,1)$. The unusual symmetry of such graphs can be explained alternatively by Theorem 1.4.

There is a special family of rational functions, called Lattès maps, whose dynamics over finite fields show more regularities than that of arbitrary rational functions [PG11]. Lattès maps are rational functions covered by elliptic curve endomorphisms and have been studied for over 100 years. See [Mi06] for a nice introduction to Lattès maps over complex numbers. In recent years there have been results over finite fields as well, see [Ug12], [Ug13] for instance. In addition, bijectivity of Lattès maps over finite fields is investigated in [Mü99]. Lattès maps play an important role to solve Schur problem for rational functions [GMS03].

In the second part of this paper we generalize our alternative interpretation for Dickson polynomials to Lattès maps. We give a sufficient and necessary condition

Date: June 3, 2014.

2010 *Mathematics Subject Classification.* Primary 11G20.

Key words and phrases. Dickson polynomial, Lattès map, elliptic curve, complex multiplication, permutation.

for these maps to be bijections. Moreover we show that the value set formula for Dickson polynomials can be generalized to such functions. More precisely we have the following: Let K be an imaginary quadratic field with Hilbert class field H. Let

$$E : y^2 = x^3 + ax + b, \quad a, b \in H$$

be an elliptic curve with complex multiplication by $\mathcal{O}_K$. The uniformization theorem for elliptic curves says that there exists a lattice Λ so that $\wp(z)$ parametrizes E. In other words the map $C/\Lambda \to E$ given by $z \mapsto (\wp(z), \wp'(z))$ is a complex analytic isomorphism. For each $\alpha \in \mathcal{O}_K$, define F_α by

$$F_\alpha(\wp(z)) = \wp(\alpha z)$$

where $F_\alpha(t)$ is a rational function with coefficients from H [Si94, II.2.2]. Suppose that E has good reduction $\bar{E}$ at $\mathfrak{P}$, a prime ideal of H lying over p. Let $\mathfrak{p} = \mathfrak{P} \cap K$ and let $n \geq 1$ be an integer so that $\mathfrak{p}^n$ is principal. Set $q = |\mathcal{O}_K/\mathfrak{p}|^n$, a power of the prime p. Adding a point at infinity, we obtain the projective 1-space $\mathbf{P}^1(\mathbf{F}_{q^m}) = \mathbf{F}_{q^m} \cup \{\infty\}$. For each integer $m \geq 1$, we have a rational map

$$\bar{F}_\alpha : \mathbf{P}^1(\mathbf{F}_{q^m}) \to \mathbf{P}^1(\mathbf{F}_{q^m})$$

where $\bar{F}_\alpha$ is the reduction of the rational function $F_\alpha \in H(t)$ modulo $\mathfrak{P}$. Corollary 2.7 provides a formula which gives the size of the value set $\{\bar{F}_\alpha(x) : x \in \mathbf{F}_{q^m}\}$ in terms of norms of ideals. Using this we give a sufficient and necessary condition for $\bar{F}_\alpha$ being a bijection, see Corollary 2.8.

1. Real Cyclotomic Case

Let $\omega\mathbf{Z}$ be the additive subgroup of $\mathbf{C}$ generated by $\omega = 2\pi i$. Define the function $\phi(z)$ by the series

$$\phi(z) = \sum_{\lambda \in \omega\mathbf{Z}} \frac{1}{(z-\lambda)^2}.$$

The following lemma is key to illustrate the analogy between the real cyclotomic case and the elliptic case.

Lemma 1.1. *The function $\phi(z)$ has the following properties.*

(1) *The series defining $\phi(z)$ converges absolutely and uniformly on every compact subset of $\mathbf{C} - \omega\mathbf{Z}$. It defines a meromorphic function on $\mathbf{C}$ having a double pole with residue 0 at each $\lambda \in \omega\mathbf{Z}$ and no other poles.*

(2) *The Laurent series for $\phi(z)$ about $z = 0$ is given by*

$$\phi(z) = -\sum_{j=0}^{\infty} (2j-1) \frac{B_{2j}}{(2j)!} z^{2j-2}$$

where B_{2j} is the Bernoulli number.

(3) *The function $\phi(z)$ is even and periodic with period $\omega = 2\pi i$. Moreover*

$$\phi(z) = \frac{e^z}{(e^z-1)^2}$$

and there is an algebraic relation between $\phi(z)$ and its derivative $\phi'(z)$

$$\phi'(z)^2 = 4\phi(z)^3 + \phi(z)^2.$$

Proof. (1) Choose $\Lambda = [1, \omega]$. The series defining the Weierstrass $\wp$-function (relative to lattice Λ) converges absolutely and uniformly on every compact subset $\mathbf{C} - \Lambda$ [Si09, VI.3.1]. Note that

$$\left|\frac{1}{(z-\lambda)^2}\right| \leq \left|\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right| + \left|\frac{1}{\lambda^2}\right|.$$

and

$$\sum_{\lambda \in \omega\mathbf{Z}}{}' \left|\frac{1}{\lambda^2}\right| = \frac{2\zeta(2)}{(2\pi)^2} < \infty$$

where the sum is taken over non-zero elements of $\omega\mathbf{Z}$. Since $\omega\mathbf{Z}$ is a subset of Λ, we conclude that the series defining the function $\phi(z)$ converges absolutely and uniformly on every compact subset of $\mathbf{C} - \omega\mathbf{Z}$. Thus it defines a meromorphic function on $\mathbf{C}$ having a double pole with residue 0 at each $\lambda \in \omega\mathbf{Z}$ and no other poles.

(2) Using the Laurent series expansion of $1/(z - k\omega)^2$ about $z = 0$, it is easy to see that

$$2\sum_{j=1}^{\infty}(2j-1)\left(\frac{z}{k\omega}\right)^{2j-2} = \frac{(k\omega)^2}{(z-k\omega)^2} + \frac{(k\omega)^2}{(-z-k\omega)^2}.$$

for each $k \neq 0$ and $0 < |z| < 2\pi$. Using the definition of $\phi(z)$, we see that

$$\phi(z) = \sum_{\lambda \in \omega\mathbf{Z}} \frac{1}{(z-\lambda)^2} = \frac{1}{z^2} + 2\sum_{k=1}^{\infty}\frac{1}{(k\omega)^2}\sum_{j=1}^{\infty}(2j-1)\left(\frac{z}{k\omega}\right)^{2j-2}.$$

Putting $\zeta(2j) = \sum_{k=1}^{\infty} 1/(k^{2j})$, we obtain

$$\phi(z) = \frac{1}{z^2} + 2\sum_{j=1}^{\infty}(2j-1)\frac{\zeta(2j)}{\omega^{2j}}z^{2j-2}.$$

It is a well known fact that

$$\zeta(2j) = -\frac{1}{2}\frac{\omega^{2j}}{(2j)!}B_{2j}$$

for integers $j \geq 1$ [La87, Chapter 4]. This finishes the proof of the second part.

(3) We start with the defining series of Bernoulli numbers

$$\frac{z}{e^z - 1} = \sum_{j=0}^{\infty}\frac{B_j}{j!}z^j.$$

Bernoulli numbers with odd index are zero except B_1 since the function $z/(e^z - 1) + z/2$ is even. Setting $g(z) = 1/(e^z - 1) + 1/2$, we see that

$$g(z) = \sum_{j=0}^{\infty}\frac{B_{2j}}{(2j)!}x^{2j-1}.$$

Since $g'(z) = -\phi(z)$, we obtain $\phi(z) = e^z/(e^z - 1)^2$. Note that $\phi' = -2\phi g$ and $g^2 = \phi + 1/4$. Using these identities, it is easy to establish the algebraic relation $(\phi')^2 = 4\phi^3 + \phi^2$. □

The properties of $\phi(z)$ listed above are very similar to those satisfied by the Weierstrass $\wp$-function [Si09, VI.3.1]. Moreover projective curves parametrized by these functions have similar structures. Consider the curve C given by

$$C : y^2 = 4x^3 + x^2.$$

This is a singular cubic curve which has a node at the origin with two distinct tangent lines $y \pm x = 0$. The non-singular part of C, denoted by C_{ns}, is the set of non-singular points of C. The composition law on elliptic curves makes C_{ns} into an abelian group. Moreover the map $(x, y) \mapsto \frac{y-x}{y+x}$ from C_{ns} to $\mathbf{C}^*$ gives an isomorphism of abelian groups [Si09, III.2.5]. We have the following commutative diagram

$$\begin{array}{ccccc} \mathbf{C}/\omega\mathbf{Z} & \xrightarrow{z \mapsto (\phi(z), \phi'(z))} & C_{\mathrm{ns}} & \xrightarrow{(x,y) \mapsto \frac{y-x}{y+x}} & \mathbf{C}^* \\ & \searrow^{z \mapsto e^z} & & & \nearrow \end{array}$$

The multiplicative group $\mathbf{C}^*$ has a subgroup consisting of elements of norm 1, namely the unit circle. Let us denote the corresponding subgroup by $C_1 \subseteq C_{\mathrm{ns}}$. Note that $\omega/n \in \mathbf{C}/\omega\mathbf{Z}$ corresponds to $\zeta_n = e^{2\pi i/n} \in \mathbf{C}^*$. For each integer n, the endomorphism $[n] : C_1 \to C_1$ is given by $(\phi(z), \phi'(z)) \mapsto (\phi(nz), \phi'(nz))$. The n-torsion subgroup of C_1, denoted $C_1[n]$, is the set of points of order n in C_1,

$$C_1[n] = \{P \in C_1 : [n]P = O\}.$$

For any integer $n \geq 1$, define f_n by the following functional equation

$$f_n(\phi(z)) = \phi(nz) = x([n]P).$$

The function f_n is closely related with the Dickson polynomial. See [LN83, Chapter 7] for a good introduction to this special family of polynomials. We recall that the n-th Dickson polynomial of the first kind $D_n(x, a)$ is defined by

$$D_n(x, a) = \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-a)^j x^{n-2j}. \tag{1.1}$$

In our paper we fix $a = 1$ and use $D_n(x) = D_n(x, 1)$ for simplicity. The fundamental property of Dickson polynomials is its functional equation $D_n(y + y^{-1}) = y^n + y^{-n}$. Observe that

$$D_n\left(\frac{1}{\phi(z)} + 2\right) = D_n(e^z + e^{-z}) = e^{nz} + e^{-nz} = \frac{1}{\phi(nz)} + 2.$$

It follows that

$$f_n(t) = \frac{1}{D_n(\frac{1}{t} + 2) - 2}. \tag{1.2}$$

Since $D_n(t)$ is a polynomial, $f_n(t)$ is a rational function. Moreover its denominator is related with the n-torsion points of C_1. For any positive integer n, define

$$\psi_n(t) = n^2 \prod_{P \in C_1[n]}{}' (t - x(P))$$

where the product is taken over the $[n]$-torsion points of C_1 except the point at infinity. We regard the empty product to be equal to 1, i.e. $\psi_1(t) = 1$.

Lemma 1.2. *Let n be a positive integer. The polynomial $\psi_n(t)$ is a degree $n-1$ polynomial with integer coefficients whose constant term is equal to* 1*. Moreover we have*

$$f_n(t) = \frac{t^n}{\psi_n(t)}.$$

Proof. It is easy to see by (1.2) that the numerator of the rational function $f_n(t)$ can be taken t^n since $\deg(D_n) = n$. Then the denominator is a polynomial of degree $n-1$ with integer coefficients whose constant term is equal to 1.

Observe that the function $\phi(nz)$ has a double pole at every integer multiple of ω/n. Let $\psi_n(t)$ be as above, then

$$\psi_n(\phi(z)) = n^2 \prod_{j=1}^{n-1} \left(\phi(z) - \phi\left(\frac{j\omega}{n}\right)\right)$$

for any integer $n \geq 1$. Similar to the Weierstrass $\wp$-function [Co89, 10.4], $\phi(z_1) = \phi(z_2)$ if and only if $z_1 \pm z_2 \in \omega\mathbf{Z}$. Note that the function $\phi(nz)\psi_n(\phi(z))$ does not have any pole except z such that $2z \in \omega\mathbf{Z}$. However

$$\phi'(z) = -\frac{e^z(e^z+1)}{(e^z-1)^3} = 0$$

if and only if $2z \in \omega\mathbf{Z}$ and $z \notin \omega\mathbf{Z}$. As a result $\phi(z) - \phi(\omega/2)$ has a double zero at points $z = k\omega + \omega/2$ for every integer $k \in \mathbf{Z}$ and the function $\phi(nz)\psi_n(\phi(z))$ has no poles except the points $z \in \omega\mathbf{Z}$. We cancel these poles by translates of $\phi(z)$. Since $\phi(z)$ is never zero, the meromorphic function

$$\frac{\phi(nz)\psi_n(\phi(z))}{\phi(z)^n}$$

has no poles. One can show that this quotient approaches 1 as $\mathrm{Re}(z) \to \pm\infty$ since $\phi(z) = e^z/(e^z-1)^2$. Therefore it is an entire function which is bounded. By Liouville's theorem it must be constant. Comparing the leading terms of both numerator and denominator, we see that it must be equal to 1. This finishes the proof. □

Let n be a positive integer. Consider $C_1[n]_x = \{x(P) : P \in C_1[n]\}$, the set of x-coordinates of n-torsion points of C_1. Note that

$$\phi\left(\frac{j\omega}{n}\right) = \frac{\zeta_n^j}{(\zeta_n^j - 1)^2} = \frac{1}{\zeta_n^j + \zeta_n^{-j} - 2}$$

where $\zeta_n = e^{2\pi i/n}$ is a primitive n-th root of unity. Therefore the n-th real cyclotomic field $\mathbf{Q}(\zeta_n + \zeta_n^{-1})$ can be obtained by adjoining elements of $C_1[n]_x$ to $\mathbf{Q}$. Recall that such a number field can also characterized as the ray class field $\mathbf{Q}_{(n)}$ of $\mathbf{Q}$ of conductor (n) [Co89, § 8]. Thus we have $\mathbf{Q}(C_1[n]_x) = \mathbf{Q}_{(n)}$.

The number of elements in $C_1[n]_x$ play an important role in our proofs. Let us denote the greatest common divisor of integers n_1 and n_2 by (n_1, n_2). We have the following

Lemma 1.3. *For any integer $n \geq 1$, we have $|C_1[n]_x| = (n + (n,2))/2$.*

Proof. Recall that C_1 is a subset of the projective curve $C : y^2 = 4x^3 + x^2$. For points $P_1, P_2 \in \bar{C}_1$, we have $x(P_1) = x(P_2)$ if and only if $P_1 = [\pm 1]P_2$. On the other hand $x(P) = x([\pm 1]P)$ if and only if $P \in C_1[2]$. As a result,

$$|C_1[n]_x| = \frac{|C_1[n] \setminus C_1[(n,2)]|}{2} + |C_1[(n,2)]| = \frac{n-(n,2)}{2} + (n,2).$$

□

The following theorem enables us to see the projective space $\mathbf{P}^1(\mathbf{F}_q)$ as a union of $\mathbf{Z}$-modules where the module action is given by natural group operation on the curve $\bar{C}_1$, the reduction of C_1 modulo p.

Theorem 1.4. *Let $\mathbf{F}_q$ be the finite field of order q and characteristic p. Let $\mathfrak{P}$ be a prime ideal of the ray class field $\mathbf{Q}_{(q^2-1)}$ lying over p. The elements of $C_1[q \pm 1]_x$ belong to $\mathbf{Q}_{(q^2-1)}$. Moreover their reduction modulo $\mathfrak{P}$ gives all elements of $\mathbf{P}^1(\mathbf{F}_q)$ except zero. In other words we have*

$$\mathbf{P}^1(\mathbf{F}_q) = \bar{C}_1[q-1]_x \cup \bar{C}_1[q+1]_x \cup \{0\}.$$

Proof. It is easy to see that $D_p(t) \equiv t^p \pmod{p}$ by (1.1). Let q be a power of p. Since $D_{ab} = D_a \circ D_b$ we have $D_q \equiv t^q \pmod{p}$. It follows by (1.2) that

$$f_q(t) \equiv t^q \pmod{p}.$$

Thus there are precisely $q+1$ distinct solutions of $f_q(t) = t$ in $\mathbf{P}^1(\mathbf{F}_q)$. It follows that $f_q(t) = t$ has $q+1$ distinct solutions on the Riemann sphere $\mathbf{P}^1(\mathbf{C})$ as well.

Given a point $P \in C_1[q \pm 1]$, we have $[q]P = [\pm 1]P$. As a result $f_q(x(P)) = x(P)$. We claim that the set of elements in $\mathbf{P}^1(\mathbf{C})$ satisfying the equation $f_q(t) = t$, except 0, is given by

$$C_1[q-1]_x \cup C_1[q+1]_x.$$

To justify our claim, we show that this union has q distinct elements. If q is even then $C_1[q-1]_x$ and $C_1[q+1]_x$ are disjoint except for infinity. Since $|A \cup B| = |A| + |B| - |A \cap B|$ for arbitrary sets A and B, we see that there are

$$\frac{q-1+1}{2} + \frac{q+1+1}{2} - 1 = q$$

elements in the union by Lemma 1.3. If q is odd then, $C_1[q-1]_x \cap C_1[q+1]_x = C_1[2]_x$. In this case there are

$$\frac{q-1+2}{2} + \frac{q+1+2}{2} - 2 = q$$

elements in the union as well. □

This characterization makes it easier to investigate rational functions induced by endomorphisms of C_1. Given a function $f : \mathbf{P}^1(\mathbf{F}_q) \to \mathbf{P}^1(\mathbf{F}_q)$, we define its value set

$$V_f = \{f(x) : x \in \mathbf{P}^1(\mathbf{F}_q)\}.$$

As an application of the above theorem, we give the following corollary.

Corollary 1.5. *For each integer $n \geq 1$, define the integers*

$$n^- = \frac{q-1}{(n, q-1)}, \quad n^+ = \frac{q+1}{(n, q+1)}$$

and define the constant

$$\eta = \frac{(n^-, 2) + (n^+, 2)}{2} - (n^-, n^+).$$

We have $V_{f_n} = \bar{C}_1[n^-]_x \cup \bar{C}_1[n^+]_x \cup \{0\}$ *and* $|V_{f_n}| = (n^- + n^+)/2 + \eta + 1$.

Proof. The group homomorphism $[n] : C_1[q-1] \to C_1[q-1]$ has kernel $C_1[(n, q-1)]$. Its image is the cyclic subgroup of order $n^- = (q-1)/(n, q-1)$. In other words we have a surjection $f_n : C_1[q-1]_x \twoheadrightarrow C_1[n^-]_x$. It is similar for $[q+1]$-torsion points. Using Theorem 1.4, we conclude that

$$V_{f_n} = \bar{C}_1[n^-]_x \cup \bar{C}_1[n^+]_x \cup \{0\}.$$

Now we want to determine the size of this union. For any point $P \in \bar{C}_1$, the x-coordinate $x(P)$ is never zero. Thus, we have

$$|V_{f_n}| = |C_1[n^-]_x| + |C_1[n^+]_x| - |C_1[(n^-, n^+)]_x| + 1.$$

We obtain the formula given in the corollary by Lemma 1.3. Note that $\eta = 0$ if $n^- + n^+$ is even and $\eta = 1/2$ if $n^- + n^+$ is odd. See Example 1.8. □

The rational function $f_n(t)$ can be obtained from the polynomial $D_n(t)$ via linear substitutions together with $1/t$, see equation (1.2). We conclude that

$$|V_{f_n}| = |V_{D_n}|.$$

A simple consequence of this equality is that f_n is a bijection of $\mathbf{P}^1(\mathbf{F}_q)$ if and only if D_n is a bijection of $\mathbf{P}^1(\mathbf{F}_q)$. Moreover, since both functions fix infinity, the same is true if they are considered as functions of $\mathbf{F}_q$.

Dickson polynomials provide one of the few classes of polynomials over finite fields whose value sets have been determined. The cardinality of the set $\{D_n(x) : x \in \mathbf{F}_q\}$ was first computed by Chou, Gomez-Calderon and Mullen [CGM88]. Using Lemma 1.5 and the above remark, we recover their result.

Corollary 1.6. *The cardinality of the set* $\{D_n(x) : x \in \mathbf{F}_q\}$ *is* $(n^- + n^+)/2 + \eta$.

Since $n^- = (q-1)/(n, q-1)$ and $n^+ = (q+1)/(n, q+1)$, we see from this corollary that D_n is a bijection if and only if $(n, q-1) = 1$ and $(n, q+1) = 1$. This is possible if and only if $(n, q^2-1) = 1$. From this we recover a well-known condition for Dickson polynomials to be bijective [LN83, 7.16].

Corollary 1.7. *The Dickson polynomial* $D_n(x) : \mathbf{F}_q \to \mathbf{F}_q$ *is a bijection if and only if* $(n, q^2-1) = 1$.

We finish this section by giving an example to illustrate our computations.

Example 1.8. Let us consider $\mathbf{F}_9 = \mathbf{F}_3[i]$ where $i^2 = 2$. Let $\mathfrak{P}$ be a prime ideal of $\mathbf{Q}_{(80)}$ lying over 3. By Theorem 1.4, we have $\mathbf{P}^1(\mathbf{F}_9) = \bar{C}_1[8]_x \cup \bar{C}_1[10]_x \cup \{0\}$. The map f_n is a bijection of $\mathbf{P}^1(\mathbf{F}_9)$ if and only if $(n, 80) = 1$. Let us consider $n = 2^k$ so that the resulting map is not bijective. It is easy to compute that $D_2(t) = t^2 - 2$ by the definition of Dickson polynomials (1.1). Using the equation (1.2), we obtain $f_2(t) = t^2/(4t+1)$. We have

$$\underbrace{\{2 \pm i, 1, 2, \infty\}}_{\bar{C}_1[8]_x} \xrightarrow{f_2} \underbrace{\{1, 2, \infty\}}_{\bar{C}_1[4]_x} \xrightarrow{f_2} \underbrace{\{2, \infty\}}_{\bar{C}_1[2]_x} \xrightarrow{f_2} \underbrace{\{\infty\}}_{\bar{C}_1[1]_x} \xrightarrow{f_2} \cdots$$

and

$$\underbrace{\{\pm i, 1 \pm i, 2, \infty\}}_{\bar{C}_1[10]_x} \xrightarrow{f_2} \underbrace{\{1 \pm i, \infty\}}_{\bar{C}_1[5]_x} \xrightarrow{f_2} \cdots$$

The invariants of Corollary 1.5 specified to this example are given in the table below.

n	2^0	2^1	2^2	2^3	$\cdots$
n^-	8	4	2	1	$\cdots$
n^+	10	5	5	5	$\cdots$
η	0	1/2	1/2	0	$\cdots$
$\lvert V_{f_n}\rvert$	10	6	5	4	$\cdots$

2. Elliptic Case

In this section we will use the analogy between $\phi(z) = e^z/(e^z-1)^2$ and Weierstrass $\wp$-function in order to generalize our ideas given in previous section to the elliptic case. We will investigate the structure of projective space $\mathbf{P}^1(\mathbf{F}_q)$ via the torsion points of elliptic curves with complex multiplication. At the end we will find the value sets of Lattès maps which are rational functions induced by isogenies of elliptic curves as an application.

Let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. If $\mathfrak{a}$ is a non-zero ideal of $\mathcal{O}_K$ then the quotient ring $\mathcal{O}_K/\mathfrak{a}$ is finite and the norm of $\mathfrak{a}$ is defined to be $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$. The norm of an element $\alpha \in K$ is given by $N(\alpha) = \alpha\alpha'$ where α' is the complex conjugate of α. It is a well-known fact that $N((\alpha)) = N(\alpha)$ where $(\alpha) = \alpha\mathcal{O}_K$ is the principal ideal generated by α.

Let H be the Hilbert class field of K, and let

$$E : y^2 = x^3 + ax + b, \quad a, b \in H$$

be an elliptic curve with complex multiplication by $\mathcal{O}_K$. The Weierstrass $\wp$-function (relative to Λ) is defined by the series

$$\wp(z) = \frac{1}{z^2} + \sum_{\lambda\in\Lambda}{}' \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)$$

where the sum is taken over all nonzero elements of Λ. The uniformization theorem for elliptic curves says that there exists a lattice Λ so that $\wp(z)$ parametrizes E [Si09, VI.5.1]. In other words the map $C/\Lambda \to E$ given by $(\wp(z), \wp'(z))$ is a complex analytic isomorphism. For each $\alpha \in \mathcal{O}_K$, define F_α by

$$F_\alpha(\wp(z)) = \wp(\alpha z) = x([\alpha]P).$$

This is the analogy with Dickson's polynomial. If $\alpha \in \mathbf{Z}$ then one can compute F_α recursively [Si09, Exercise 3.7]. For general $\alpha \in \mathcal{O}_K$ it is done by Satoh [Sa04] who separates the problem into several cases and gives a recurrence relation for each case. The function F_α can also be computed as follows in a similar fashion with f_n.

Lemma 2.1. *Let O be the point at infinity of E and P_0 be a point on E with $x(P_0) = 0$. Then for any $\alpha \in \mathcal{O}_K$, we have*

$$F_\alpha(t) = \frac{\displaystyle\prod_{[\alpha]P=P_0} (t - x(P))}{\alpha^2 \displaystyle\prod_{[\alpha]P=O}{}' (t - x(P))} \in H(t).$$

Proof. We know that $F_\alpha(t) = A(t)/B(t)$ where A and B are relatively prime polynomials with $\deg(A) = \deg(B) + 1 = N(\alpha)$ [Co89, 10.14]. Moreover $A(t)$ and $B(t)$ are polynomials with coefficients from H [Si94, II.2.2].

Suppose that $E : y^2 = x^3 + ax + b$ is parametrized by $\wp(z)$, relative to the lattice Λ. If $z \notin \Lambda$, then $B(\wp(z)) = 0$ if and only if $\alpha z \in \Lambda$. Recall that the Weierstrass $\wp$-function has a double pole at every lattice point $\lambda \in \Lambda$. As a result $\wp(\alpha z)$ has a double pole at every z such that $\alpha z \in \Lambda$. We have $\wp(z_1) = \wp(z_2)$ if and only if $z_1 \pm z_2 \in \Lambda$ [Co89, 10.4]. Note that the function

$$\wp(\alpha z) \prod_{[\alpha]P=O}{}' \, (\wp(z) - x(P))$$

does not have any pole except z such that $2z \in \Lambda$. If $z \notin \Lambda$, then $\wp'(z) = 0$ if and only if $2z \in \Lambda$ [Co89, 10.5]. Therefore the function above has poles only at lattice points.

In order to cancel these poles, we use translates of $\wp(z)$. Note that the function above has a zero at each z corresponding to a point P such that $[\alpha]P = P_0$. Consider the meromorphic function

$$\frac{\wp(\alpha z) \prod'_{[\alpha]P=O} (t - x(P))}{\prod_{[\alpha]P=P_0} (t - x(P))}.$$

We claim that this quotient has no poles. It is enough to show that the denominator does not introduce any poles other than the lattice points. Let Q_1, Q_2 be two points of E such that $[\alpha]Q_i = P_0$ for $i = 1, 2$. If $x(Q_1) \neq x(Q_2)$ whenever $Q_1 \neq Q_2$ then we are done. Otherwise Q_1 and Q_2 must be inverses of each other. It follows that $P_0 \in E[2]$ and as a result $y(P_0) = 0$. If $P_0 = (\wp(z_0), \wp'(z_0))$, then the numerator of the above quotient has a double zero at z_0. This finishes the proof of our claim.

Therefore the quotient above does not have any poles and therefore it is an entire function. Moreover it is bounded since it is doubly periodic. By Liouville's theorem it must be constant. Comparing the leading terms of the Laurent series of both numerator and denominator, wee see that this constant must be equal to $1/\alpha^2$. □

For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, the group of $\mathfrak{a}$-torsion points of E is defined by

$$E[\mathfrak{a}] = \{P \in E : [\alpha]P = O \text{ for all } \alpha \in \mathfrak{a}\}.$$

Notice that the definition of $E[\mathfrak{a}]$ depends on the isomorphism $\mathcal{O}_K \cong \mathrm{End}(E)$. We always use the isomorphism $[\cdot] : \mathcal{O}_K \to \mathrm{End}(E)$ such that for any invariant differential ω_E of E, $[\alpha]^*\omega_E = \alpha\omega_E$ for all $\alpha \in \mathcal{O}_K$ [Si94, II.1.1]. We simplify our notation for principal ideals by $E[(\alpha)] = E[\alpha]$.

In the previous section we have used maps f_q whose reduction modulo p gives the Frobenius map. Now we construct analogous maps F_π in the elliptic case. Let $\mathfrak{P}$ be a prime ideal of H lying over $\mathfrak{p}$ such that E has good reduction at $\mathfrak{P}$. Consider the isogeny $[p] : E \to E$ which is defined over H. The reduction of $[p]$ modulo $\mathfrak{P}$ is not separable since $[p]^*\omega_E = p\omega_E \equiv 0 \pmod{\mathfrak{P}}$ [Si09, II.4.2c]. Hence

$$\overline{[p]} = \psi \circ \mathrm{Frob}_q$$

where $\mathrm{Frob}_q : \bar{E} \to \bar{E}$ is the Frobenius map given by $(x, y) \mapsto (x^q, y^q)$ and ψ is a separable map [Si09, II.2.12].

Lemma 2.2. *Let $\mathfrak{P}$ be a prime ideal of H lying over p such that E has good reduction at $\mathfrak{P}$. Set $\mathfrak{p} = \mathfrak{P} \cap K$ and suppose that $\mathfrak{p}^n$ is principal for some integer $n \geq 1$. Then there exists a unique element $\pi \in \mathcal{O}_K$ such that $\mathfrak{p}^n = (\pi)$ and $\overline{[\pi]} = \mathrm{Frob}_{N(\pi)}$.*

Proof. If p splits or ramifies in K, then there exists a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ of norm p, not necessarily principal. Let $n > 0$ be an integer such that $\mathfrak{p}^n$ is principal. We have a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E^{\sigma_\mathfrak{p}} \\ \downarrow & & \downarrow \\ \bar{E} & \xrightarrow{\mathrm{Frob}_p} & \bar{E}^{(p)} \end{array}$$

Here $\sigma_\mathfrak{p} = (\mathfrak{p}, H/K)$ is the Artin map, λ is an isogeny and the vertical maps are reduction modulo $\mathfrak{P}$ [Si94, II.5.3]. Our assumption $\mathfrak{p}^n$ is principal implies that $\sigma_\mathfrak{p}^n = 1$. Thus λ^n is an endomorphism of E, say $\lambda^n = [\pi]$ for some $\pi \in \mathcal{O}_K$ of norm p^n. We want to show that $\mathfrak{p}^n$ is generated by π. Following Silverman [Si94, II.5.4], one can show that $\bar{\pi}\bar{\omega}_E = 0$ where $\bar{\pi}$ is the reduction of π modulo $\mathfrak{P}$ and $\bar{\omega}_E$ is a generator of the vector space of differential forms on $\bar{E}$. From this, we conclude that $\pi \equiv 0 \pmod{\mathfrak{P}}$. Therefore $\pi \in \mathfrak{p} = \mathfrak{P} \cap K$.

If p ramifies in $\mathcal{O}_K$, then we must have $(\pi) = \mathfrak{p}^n$ since their norms coincide and $\mathfrak{p}$ is the unique prime ideal over p. Now suppose that p splits in K. Then $\bar{E}$ is not supersingular [La87, Chapter 13] and $\mathrm{Ker}(\overline{[p]})$ is not trivial [Si09, V.3.1]. It follows that $\pi \notin \mathfrak{p}'$ where $\mathfrak{p}'$ is the complex conjugate of $\mathfrak{p}$. Otherwise π will be an element of $(p) = \mathfrak{p}\mathfrak{p}'$ and $\overline{[\pi]}$ cannot be purely inseparable. As a result we have $\pi \in \mathfrak{p} \setminus \mathfrak{p}'$ and $N(\pi) = p^n$. Therefore $(\pi) = \mathfrak{p}^n$.

If p remains prime in K then the curve $\bar{E}$ is supersingular [La87, Chapter 13]. If $\bar{E}$ is supersingular then the map $\overline{[p]}$ is purely inseparable [Si09, V.3.1]. Thus

$$\overline{[p]} = \varepsilon \circ \mathrm{Frob}_{p^2}$$

for some $\varepsilon \in \mathrm{Aut}(\bar{E})$. If we can show that ε is the reduction modulo $\mathfrak{P}$ of some $\varepsilon_0 \in \mathrm{Aut}(E)$ then we can replace $[p]$ by $\varepsilon_0^{-1} \circ [p]$ and be done. It suffices to show that ε commutes with the image of $\mathrm{End}(E)$ inside $\mathrm{End}(\bar{E})$ [Si94, II.5.2]. This can be done by generalizing the proof given in Silverman [Si94, II.5.3]. In this case it is obvious that $\mathfrak{p}^n = (p^n)$ and $\pi = \zeta p^n$ for some $\zeta \in \mathcal{O}_K^*$. □

Similar to the real cyclotomic case, we will use x-coordinates of $\mathfrak{a}$-torsion points of E. We start with counting the elements in the set $E[\mathfrak{a}]_x = \{x(P) : P \in E[\mathfrak{a}]\}$.

Lemma 2.3. *For any ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we have $|E[\mathfrak{a}]_x| = (N(\mathfrak{a}) + N(\mathfrak{a} + (2)))/2$.*

Proof. Two points P_1 and P_2 of an elliptic curve $E : y^2 = x^3 + ax + b$ have the same x-coordinate if and only if $P_1 = [\pm 1]P_2$. Moreover $P = [\pm 1]P$ if and only if $P \in E[2]$. Thus the number of elements in the set $E[\mathfrak{a}]_x$ is given by

$$|E[\mathfrak{a}]_x| = \frac{|E[\mathfrak{a}] \setminus E[\mathfrak{a} + (2)]|}{2} + |E[\mathfrak{a} + (2)]| = \frac{N(\mathfrak{a}) - N(\mathfrak{a} + (2))}{2} + N(\mathfrak{a} + (2)).$$

□

It is a well known fact that the ray class field of K of conductor $\mathfrak{a}$ can be obtained by torsion points on the elliptic curve E. More precisely we have

$$K_{\mathfrak{a}} = H(h(E[\mathfrak{a}]))$$

where h is a Weber function for $E : y^2 = x^3 + ax + b$. It is defined by

$$h(P) = \begin{cases} x(P) & \text{if } ab \neq 0, \\ x(P)^2 & \text{if } b = 0, \\ x(P)^3 & \text{if } a = 0. \end{cases}$$

For details, see Lang [La87, Chapter 10].

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over H with complex multiplication by $\mathcal{O}_K$. Suppose that E has good reduction $\bar{E}$ at $\mathfrak{P}$, a prime ideal of H lying over p. Then there exists a unique element $\pi \in \mathcal{O}_K$ such that $\mathfrak{p}^n = (\pi)$ and $\overline{[\pi]} = \mathrm{Frob}_{N(\pi)}$ by Lemma 2.2. For each integer $m \geq 1$, the elements of $E[\pi^m \pm 1]$ belong to the number field $L = H(E[\pi^{2m} - 1]_x)$. Note that L equals the ray class field of K of conductor $(\pi^{2m} - 1)$ unless $d_K = -3, -4$. Otherwise it is an abelian extension of K containing the ray class field $K_{(\pi^{2m}-1)}$ by Kummer theory [Ne99, IV.3]. Let $\mathcal{P}$ be a prime ideal of L lying over $\mathfrak{P}$. The reduction of elements $E[\pi^m \pm 1]_x$ modulo $\mathcal{P}$ gives all elements of $\mathbf{P}^1(\mathbf{F}_q)$ where $\mathbf{F}_q$ is a finite field of order $q = N(\mathfrak{p})^n$. Then we have the following

Theorem 2.4. *For each integer $m \geq 1$,*

$$\mathbf{P}^1(\mathbf{F}_{q^m}) = \bar{E}[\pi^m - 1]_x \cup \bar{E}[\pi^m + 1]_x.$$

Proof. By Lemma 2.2, there exists $\pi \in \mathcal{O}_K$ such that $\overline{[\pi]} = \mathrm{Frob}_{N(\pi)}$. Set $q = N(\pi)$ and $\beta = \pi^m$. Let $\bar{F}_\beta$ be the reduction of F_β modulo $\mathfrak{P}$. Since we have $F_\beta(t) \equiv t^{N(\beta)} \pmod{\mathfrak{P}}$, there are precisely $q^m + 1$ distinct solutions of $\bar{F}_\beta(t) = t$ in $\mathbf{P}^1(\mathbf{F}_q)$. It follows that $F_\beta(t) = t$ has $q^m + 1$ distinct solutions on the Riemann sphere $\mathbf{P}^1(\mathbf{C})$ as well.

Given a point $P \in E[\beta \pm 1]$, we have $[\beta]P = [\pm 1]P$. If follows that $F_\beta(x(P)) = x(P)$. We claim that the set of elements in $\mathbf{P}^1(\mathbf{C})$ satisfying the equation $F_\beta(t) = t$ is given by

$$E[\beta - 1]_x \cup E[\beta + 1]_x.$$

To justify our claim, we show that this union has $q^m + 1$ distinct elements. Note that $E[\beta - 1] \cap E[\beta + 1] \subseteq E[2]$. If $\mathfrak{b} = (2, \beta - 1)$, then we see by Lemma 2.3 that the number of elements in $E[\beta - 1]_x \cup E[\beta + 1]_x$ is given by

$$\frac{N(\beta - 1) + N(\mathfrak{b})}{2} + \frac{N(\beta + 1) + N(\mathfrak{b})}{2} - N(\mathfrak{b}) = \frac{N(\beta - 1) + N(\beta + 1)}{2}$$

Define $w = (\sqrt{d_K} + d_K)/2$ where d_K is the discriminant of K. Then $\mathcal{O}_K = \mathbf{Z}[w]$ for each K. There exist integers a, b such that $\beta = aw + b$. Moreover

$$N(\beta \pm 1) = q^m + 1 \pm (ad_K + 2b).$$

This finishes the proof. □

Remark 2.5. It is a well known fact that $\mathcal{O}_K^* = \{\pm 1\}$ unless $d_K = -3, -4$. Observe that $E[\pi^m - 1] \cup E[\pi^m + 1] = E[-\pi^m - 1] \cup E[-\pi^m + 1]$. Thus any generator of $\mathfrak{p}^n$ can be chosen to be π if the discriminant of K is not -3 or -4.

Example 2.6. In order to illustrate the situation in case $d_K = -3$, consider the elliptic curve $E : y^2 = x^3 - 1$ which has complex multiplication by $\mathbf{Z}[\zeta_6]$. We want to investigate $\mathbf{F}_7$ by using the torsion points of E. Let $\mathfrak{p} = (\zeta_6 - 3)$, a prime ideal of $\mathcal{O}_K$ lying over $p = 7$. Since $E(\mathbf{F}_7) = \{O, (1,0), (2,0), (4,0)\}$, we see that $E(\mathbf{F}_7) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Observe that $\mathrm{Ker}(\overline{[\pi - 1]}) = E(\mathbf{F}_7)$ if $\overline{[\pi]} = \mathrm{Frob}_p$. The only choice of π such that $N(\pi - 1) = 4$ is when $\pi = (\zeta_6 - 3)\zeta_6^4$. By Theorem 2.4, the projective space $\mathbf{P}^1(\mathbf{F}_7)$ is given by the union $\bar{E}[\pi - 1]_x \cup \bar{E}[\pi + 1]_x$ for $\pi = \pm(\zeta_6 - 3)\zeta_6^4$.

The above theorem enables us to see the projective space $\mathbf{P}^1(\mathbf{F}_{q^m})$ as a union of $\mathcal{O}_K$-modules where the module action is given by natural group operation on the curve $\bar{E}$. Now we investigate the value set $V_{\bar{F}_\alpha} = \{\bar{F}_\alpha(x) : x \in \mathbf{P}^1(\mathbf{F}_q)\}$ using this structure.

Corollary 2.7. *Suppose that $\mathbf{P}^1(\mathbf{F}_{q^m})$ is given by Theorem 2.4. Define the integral ideals*

$$\mathfrak{a}^- = \frac{(\pi^m - 1)}{(\alpha, \pi^m - 1)}, \quad \mathfrak{a}^+ = \frac{(\pi^m + 1)}{(\alpha, \pi^m + 1)}$$

and define the constant

$$\xi = \frac{N(\mathfrak{a}^- + (2)) + N(\mathfrak{a}^+ + (2))}{2} - N(\mathfrak{a}^- + \mathfrak{a}^+).$$

Then $V_{\bar{F}_\alpha} = \bar{E}[\mathfrak{a}^-]_x \cup \bar{E}[\mathfrak{a}^+]_x$ and $|V_{\bar{F}_\alpha}| = (N(\mathfrak{a}^-) + N(\mathfrak{a}^+))/2 + \xi$.

Proof. The group homomorphism $[\alpha] : E[\beta] \to E[\beta]$ has kernel $E[(\alpha, \beta)]$. Therefore we have a surjection $[\alpha] : E[\beta]_x \twoheadrightarrow C_1[(\beta)/(\alpha, \beta)]_x$. Using Theorem 2.4, we conclude that

$$V_{\bar{F}_\alpha} = \bar{E}[\mathfrak{a}^-]_x \cup \bar{E}[\mathfrak{a}^+]_x.$$

Now we want to determine the size of this union. Since $|A \cup B| = |A| + |B| - |A \cap B|$ for arbitrary sets A and B, we have

$$|V_{\bar{F}_\alpha}| = |E[\mathfrak{a}^-]_x| + |E[\mathfrak{a}^+]_x| - |E[(\mathfrak{a}^- + \mathfrak{a}^+)]_x|.$$

Applying Lemma 2.3, we obtain the formula for $|V_{\bar{F}_\alpha}|$. Note that ξ can take values $0, 1/2, 1$ and $3/2$ depending on $\mathfrak{a}^-$ and $\mathfrak{a}^+$. See Example 2.9. □

The conditions for arbitrary functions of finite fields to be bijections are rather complicated. However for the family of functions $\bar{F}_\alpha$, we can give a sufficient and necessary condition.

Corollary 2.8. *Suppose that $\mathbf{P}^1(\mathbf{F}_{q^m})$ is given by Theorem 2.4. Then $\bar{F}_\alpha$ is a bijection of $\mathbf{P}^1(\mathbf{F}_{q^m})$ if and only if $(\alpha, \pi^{2m} - 1) = (1)$.*

Proof. We see from the above corollary that $\bar{F}_\alpha$ is a bijection of $\mathbf{P}^1(\mathbf{F}_{q^m})$ if and only if $(\alpha, \pi^m - 1) = (1)$ and $(\alpha, \pi^m + 1) = (1)$. This is possible if and only if $(\alpha, \pi^{2m} - 1) = (1)$. □

We finish this section by giving an example to illustrate our computations.

Example 2.9. Let $K = \mathbf{Q}(\sqrt{-5})$ and let $j = j(\mathcal{O}_K)$ be its j-invariant. Set $c = 27j/(j - 1728)$. Then the elliptic curve $E_c : y^2 = x^3 - cx - 2c$ has the same j-invariant [La87, Chapter 1]. Thus E_c has complex multiplication by $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$. Under suitable transformations, the curve E_c is isomorphic over $\mathbf{Q}$ to the curve

$$E : y^2 = x^3 - (9\sqrt{5} + 30)x + (36\sqrt{5} + 56).$$

Consider $p = 13$ which remains prime in $\mathcal{O}_K = \mathbf{Z}[\sqrt{-5}]$. Since $\pi = \pm 13$, we have $\mathbf{P}^1(\mathbf{F}_{169}) = \bar{E}[12]_x \cup \bar{E}[14]_x$. Here the elements of $E[13 \pm 1]$ are reduced modulo $\mathcal{P}$, a prime ideal of $K_{(168)}$ lying over 13. By the corollary above $\bar{F}_\alpha$ is a bijection of $\mathbf{P}^1(\mathbf{F}_{169})$ if and only if $(\alpha, 168) = (1)$.

Observe that $N(1+\sqrt{-5}) = 6$ which divides 168. Therefore $\bar{F}_\alpha$ is not a bijection if $\alpha = (1+\sqrt{-5})^n$ for some integer $n \geq 1$. We want to find the size of the value set of $\bar{F}_\alpha$ by using the Corollary 2.7. Set $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ and $\mathfrak{p}_3 = (3, 1+\sqrt{-5})$ which are ideals of norms 2 and 3 respectively. Then $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3'$ is the complex conjugate of $\mathfrak{p}_3$. See the following table for the invariants of Corollary 2.7 specified to this example.

α	1	$1+\sqrt{-5}$	$(1+\sqrt{-5})^2$	$(1+\sqrt{-5})^3$	$(1+\sqrt{-5})^4$	$\cdots$
$\mathfrak{a}^-$	(12)	$(2)\mathfrak{p}_2\mathfrak{p}_3'$	$(2)\mathfrak{p}_3'$	$\mathfrak{p}_2\mathfrak{p}_3'$	$\mathfrak{p}_3'$	$\cdots$
$\mathfrak{a}^+$	(14)	$\mathfrak{p}_2(7)$	(7)	(7)	(7)	$\cdots$
ξ	0	1	$3/2$	$1/2$	0	$\cdots$
$\lvert V_{\bar{F}_\alpha}\rvert$	170	62	33	28	26	$\cdots$

Acknowledgements

We would like to thank the referee for carefully reading our manuscript and giving enlightening comments which helped improving the quality of the paper.

References

[Co89] D. A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication.* A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, (1989).

[CGM88] W. S. Chou, J. Gomez-Calderon, G. L. Mullen, *Value sets of Dickson polynomials over finite fields.* J. Number Theory 30 (1988), no. 3, 334–344.

[Ga14] T. A. Gassert, *Chebyshev action on finite fields.* Discrete Math. 315 (2014), 83–94.

[GMS03] R. M. Guralnick, P. Müller; J. Saxl, *The rational function analogue of a question of Schur and exceptionality of permutation representations.* Mem. Amer. Math. Soc. 162 (2003), no. 773, viii+79 pp.

[La87] S. Lang, *Elliptic functions.* With an appendix by J. Tate. Second edition. Graduate Texts in Mathematics, 112. Springer-Verlag, New York, (1987).

[LN83] R. Lidl, H. Niederreiter, *Finite fields, Encyclopedia of Mathematics and its Applications, Vol. 20.* Cambridge, UK: Cambridge University Press, (1983).

[Mi06] J. Milnor, *On Lattès maps.* Dynamics on the Riemann sphere, 9–43, Eur. Math. Soc., Zürich, (2006).

[Mü99] P. Müller, *Arithmetically exceptional functions and elliptic curves.* Aspects of Galois theory (Gainesville, FL, 1996), 180–201, London Math. Soc. Lecture Note Ser., 256, Cambridge Univ. Press, Cambridge, (1999).

[Ne99] J. Neukirch, *Algebraic number theory.* Springer-Verlag, Berlin, (1999).

[Si94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, New York, (1994).

[Si09] J. H. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, (2009).

[Sa04] T. Satoh, *Generalized division polynomials.* Math. Scand. 94 (2004), no. 2, 161–184.

[PG11] J. W. Park, S. Gao, *Dynamics of $x + x^{-1}$ via elliptic curves.* Preprint. `http://www.math.clemson.edu/~sgao/papers/park_gao.pdf`

[Ug12] S. Ugolini, *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic two.* Contemp. Math., 579 (2012) 187–204.

[Ug13] S. Ugolini, *Graphs associated with the map $x \mapsto x + x^{-1}$ in finite fields of characteristic three and five.* J. Number Theory 133 (2013), no. 4, 1207–1228.

Middle East Technical University, Mathematics Department, 06800 Ankara, Turkey.
E-mail address: `komer@metu.edu.tr`