©2018 The Mathematical Society of Japan
J. Math. Soc. Japan
Vol. 70, No. 2 (2018) pp. 823–832
doi: 10.2969/jmsj/07027643

Arithmetic exceptionality of generalized Lattès maps

By Ömer Küçüksakalli and Hurşit Önsiper

(Received Oct. 24, 2016)

Abstract. We consider the arithmetic exceptionality problem for the generalized Lattès maps on $\mathbf{P}^2$. We prove an existence result for maps arising from the product $E \times E$ of elliptic curves E with CM.

Introduction.

This paper concerns the problem of arithmetic exceptionality for the endomorphisms of the projective plane $\mathbf{P}^2$. More precisely, we want to determine morphisms

$$F : \mathbf{P}^2 \to \mathbf{P}^2$$

defined over a number field K, which when reduced mod $\mathfrak{p}$ induce a bijection

$$\bar{F} : \mathbf{P}^2(K_\mathfrak{p}) \to \mathbf{P}^2(K_\mathfrak{p}),$$

where $K_\mathfrak{p} = \mathcal{O}_K/\mathfrak{p}$, for infinitely many primes $\mathfrak{p}$ of K.

The problem of arithmetic exceptionality in its initial form stems from Schur's conjecture to the effect that if a polynomial $f(x) \in \mathbf{Z}[x]$ induces a bijection on $\mathbf{Z}/p\mathbf{Z}$ for infinitely many primes, then it is essentially a composition of linear polynomials, monomials and the Chebyshev polynomials [**GMS03**]. This conjecture was proved by Fried [**Fr70**]. The generalization of this problem to polynomials in two variables defined over number fields has been studied by several authors. It is in this version of the exceptionality problem that one is lead to work with polynomials induced on the quotients (affine two-planes) of simple Lie algebras by the corresponding Weyl groups [**Kü16**].

A natural extension of this problem is obtained when one replaces polynomials with rational functions defined over number fields, hence equivalently with endomorphisms of the projective line $\mathbf{P}^1$. For a detailed analysis of this case, we refer to [**GMS03**].

In this paper we consider the arithmetic exceptionality problem for the generalized Lattès maps on $\mathbf{P}^2$. This version of the problem has some geometric flavor since it is related to the action of those crystallographic reflection groups on $\mathbf{C}^2$ for which $\mathbf{P}^2$ is the quotient. In this vein, for a complete generalization one will definitely need to take into account the actions of the crystallographic reflection groups with weighted projective surfaces $\mathbf{P}(1,1,2)$, $\mathbf{P}(1,1,3)$, $\mathbf{P}(1,1,4)$, $\mathbf{P}(1,2,3)$, $\mathbf{P}(1,3,4)$ as the quotient [**TY82**, Table II].

In Section 1 of the paper, we first recall the basic definitions and results concerning the set-up

2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 20H15, 51F15.
Key Words and Phrases. crystallographic groups, Frobenius map, fixed point.

$$\mathbf{C}^2 \to \mathbf{C}^2/L \simeq E \times E \to (E \times E)/G \simeq \mathbf{P}^2$$

for the action of the crystallographic group $G \ltimes L$. We basically quote the explicit list of these groups and the corresponding quotient maps worked out in [**KTY82**]. Then in the Lemmata 1.4, 1.5 and 1.6, we characterize the fixed points of the corresponding Lattès maps in terms of the quotient map Φ. In Lemma 1.7, we determine the number of fixed points $|\mathrm{Fix}(F_\lambda)|$ of the Lattès map F_λ. Section 2 contains the main results of the paper. In Theorem 2.2, we give precise number theoretic criteria for the reduction modulo a prime of a Lattès map to be bijective on $\mathbf{F}_{p^2}$. This result is applied to prove the following existence theorem for exceptional Lattès maps.

THEOREM 1. *Let E be an elliptic curve defined over a number field with CM and let $F_k : \mathbf{P}^2 \to \mathbf{P}^2$ be the resulting Lattès map under the action of $G = G(m, \ell, 2)$. There exists a positive integer k such that F_k is exceptional.*

1. Generalized Lattès maps.

Lattès maps on $\mathbf{P}^1$ has been a central theme in the work related to the dynamics of rational maps on $\mathbf{P}^1$ [**Mi06**]. We recall that these maps are defined by commutative diagrams of the form

$$\begin{array}{ccc} E & \xrightarrow{\quad\lambda\quad} & E \\ {\scriptstyle\wp}\downarrow & & \downarrow{\scriptstyle\wp} \\ \mathbf{P}^1 & \xrightarrow{\quad F_\lambda\quad} & \mathbf{P}^1 \end{array}$$

where $E = \mathbf{C}/L(\tau), L(\tau) = \mathbf{Z} + \tau\mathbf{Z}$, is an elliptic curve, $\lambda \in \mathrm{End}(E)$ and $\wp$ is the Weierstrass $\wp$-function attached to $L(\tau)$. Observing that $\wp : E \to \mathbf{P}^1$ is the quotient map for the action of $\mathbf{Z}_2 = \langle\sigma\rangle, \sigma(q) = -q$ on E and lifting to the cover

$$\mathbf{C} \longrightarrow E$$

we see that the diagram arises from the action of the discrete group of motions

$$\mathbf{Z}_2 \ltimes L(\tau)$$

on $\mathbf{C}$.

To construct higher dimensional analogues of this set-up, one works with the crystallographic reflection groups in the group $E(n)$ of complex motions of $\mathbf{C}^n$. We recall the following definitions.

DEFINITION 1.1. A discrete subgroup $\Gamma \subset E(n)$ is called a complex crystallographic group if the quotient $\mathbf{C}^n/\Gamma$ is compact.

DEFINITION 1.2. A complex crystallographic group Γ is said to be a crystallographic reflection group if it is finitely generated by reflections.

A crystallographic reflection group $\Gamma \subset E(n)$ has a natural decomposition

$$0 \to L \to \Gamma \to G \to 1$$

where $G \subset U(n)$ is a finite group of unitary reflections and L is a lattice of rank $2n$ in $\mathbf{C}^n$ invariant under G.

In this paper, we are concerned with $n = 2$ case. In this two-dimensional case, we have a detailed analysis of Γ and of the quotient spaces $\mathbf{C}^2/\Gamma$ in [**TY82**], [**KTY82**]. In particular,

- we have a complete list of pairs (G, L) for crystallographic reflection groups in $E(2)$ (up to equivalence of pairs; $(G, L), (G', L')$ if and only if $G' = AGA^{-1}, L' = AL$ for some matrix A) [**TY82**, Table I]
- we know that the quotient spaces $\mathbf{C}^2/\Gamma$ are weighted projective spaces [**TY82**, Table II]

As it appears in [**TY82**, Table I], certain unitary reflection groups G give rise to non-equivalent pairs $(G, L), (G, L')$ with non-isomorphic quotients.

The fact that in arbitrary dimensions n, the quotient space $\mathbf{C}^n/\Gamma$ is a weighted projective space, is proved in [**BS78**] for crystallographic reflection groups for which G can be generated by real reflections. The approach in [**BS78**] and in the expanded version [**BS06**] is via affine root systems. This approach was initiated in [**Lo76**], where one finds a beautiful algebraic geometric analysis of setups of the form

$$Q^\vee \times E \simeq E \times \cdots \times E \longrightarrow \mathbf{P}(n_0, \ldots, n_l)$$

where $Q^\vee$ is the lattice generated by the dual of an affine root system R and W is the Weyl group of R. In these three articles, one finds explicit descriptions of the weights $n_0, \ldots, n_l$ in terms of the invariants of the root system.

For the rest of the paper, we will consider $\Gamma \subset E(2)$ for which the quotient $M = \mathbf{C}^2/\Gamma$ is smooth, which is necessarily $\mathbf{P}^2$ [**TY82**, Corollary 3.3.3]. It is known that there are precisely six such Γ as listed below.

THEOREM 1.3 ([**KTY82**]). *Every two dimensional complex crystallographic group Γ for which $M \cong \mathbf{P}^2$, is conjugate in the affine transformation group to one of the following six groups,*

$$\begin{aligned}
(2,1)_0 &:= G(2,1,2) \ltimes L^2(\tau),\\
(3,1)_0 &:= G(3,1,2) \ltimes L^2(\zeta_6),\\
(4,1)_0 &:= G(4,1,2) \ltimes L^2(i),\\
(6,1)_0 &:= G(6,1,2) \ltimes L^2(\zeta_6),\\
(4,2)_1 &:= G(4,2,2) \ltimes \left\{ L^2(i) + \mathbf{Z}\frac{1+i}{2}\begin{pmatrix}1\\1\end{pmatrix} \right\},\\
(3,3)_0 &:= G(3,3,2) \ltimes \left\{ L^2(\tau)\begin{pmatrix}-1\\1\end{pmatrix} + L^2(\tau)\begin{pmatrix}\zeta_6^2\\\zeta_6\end{pmatrix} \right\},
\end{aligned}$$

where $L(\tau) = \mathbf{Z} + \tau\mathbf{Z}$ *and* $L^2(\tau) = L(\tau)\binom{1}{0} + L(\tau)\binom{0}{1}$, *Im* $\tau > 0, i = \sqrt{-1}, \zeta_6 = \exp(2\pi i/6)$.

Recall that the primitive reflection group $G(m, \ell, 2) \subset U(2)$ is the group generated by

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & \zeta_m \\ \zeta_m^{-1} & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} \zeta_m^{\ell} & 0 \\ 0 & 1 \end{pmatrix}$$

where $\zeta_m = \exp(2\pi i/m)$. The number of elements in such a group is given by $|G(m, \ell, 2)| = 2m^2/\ell$.

In the same article, the corresponding quotient maps

$$\Phi : \mathbf{C}^2 \longrightarrow \mathbf{C}^2/\Gamma \simeq \mathbf{P}^2$$

and the ramification data were given explicitly [**KTY82**, Theorem 3]. The maps Φ are as follows:

Group	The map Φ
$(2,1)_0$	$[\wp(x) + \wp(y) : \wp(x)\wp(y) : 1]$
$(3,1)_0$	$[\wp'(x) + \wp'(y) : \wp'(x)\wp'(y) : 1]$
$(4,1)_0$	$[\wp^2(x) + \wp^2(y) : \wp^2(x)\wp^2(y) : 1]$
$(6,1)_0$	$[\wp'^2(x) + \wp'^2(y) : \wp'^2(x)\wp'^2(y) : 1]$
$(4,2)_1$	$[(\wp(x)\wp(y) + e_1^2)^2 : (\wp(x) + \wp(y))^2 : (\wp(x)\wp(y) - e_1^2)^2]$
$(3,3)_0$	$[\wp'(x) - \wp'(y) : \wp(x) - \wp(y) : \wp'(x)\wp(y) - \wp(x)\wp'(y)]$

where $e_1 = \wp(1/2; L(i))$. On the other hand, Rong [**Ro10**] determined for each of these six groups Γ, all affine maps $\lambda : \mathbf{C}^2 \to \mathbf{C}^2$ giving rise to Lattès maps F_λ, hence equivalently to diagrams of the form

$$\begin{array}{ccc} \mathbf{C}^2 & \xrightarrow{\quad\lambda\quad} & \mathbf{C}^2 \\ \downarrow & & \downarrow \\ E \times E \simeq \mathbf{C}^2/L & \xrightarrow{\quad[\lambda]\quad} & E \times E \simeq \mathbf{C}^2/L \\ \downarrow & & \downarrow \\ \mathbf{P}^2 \simeq (E \times E)/G & \xrightarrow{\quad F_\lambda \quad} & \mathbf{P}^2 \simeq (E \times E)/G \end{array}$$

For simplicity, we consider $\lambda = k$ for some positive integer k. In such a case (x, y) is mapped to (kx, ky) under λ. As a result, we have the following identity

$$F_k(\Phi(x, y)) = \Phi(kx, ky)$$

Now, we are ready to analyze the set of fixed points under the maps F_k for each group $G(m, \ell, 2)$ in Theorem 1.3.

LEMMA 1.4. *Let $G = (m,1)_0$ for some integer $m = 2,3,4,6$ and $L(\tau)$ be the corresponding lattice. For $k \neq -1,0,1$, we have* $\mathrm{Fix}(F_k) = S_1 \cup S_2$ *where*

$$S_1 = \left\{ \Phi\left(\frac{a+b\tau}{k-\zeta_m^c}, \frac{d+e\tau}{k-\zeta_m^f} \right) : a,b,c,d,e,f \in \mathbf{Z} \right\}$$
$$S_2 = \left\{ \Phi\left(\frac{a+b\tau}{k^2-\zeta_m^c}, \frac{k(a+b\tau)}{k^2-\zeta_m^c} \right) : a,b,c \in \mathbf{Z} \right\}.$$

PROOF. Recall that $\Phi(x,y) = \Phi(x',y')$ if and only if there exists $g \in G$ such that $g\binom{x}{y} \equiv \binom{x'}{y'}$ modulo $L^2(\tau)$. There are $2m^2$ elements of G and $\Phi(x,y)$ is equal to $\Phi(x\zeta_m^*, y\zeta_m^*)$ or $\Phi(y\zeta_m^*, z\zeta_m^*)$ for any choice of m^2 pairs of mth roots of unity (not necessarily primitive).

The map F_k acts very nicely on $\Phi(x,y)$, we have $F_k(\Phi(x,y)) = \Phi(kx,ky)$. Supposing $\Phi(x,y)$ is fixed under F_k, we find that $\Phi(kx,ky)$ is equal to any one of the $2m^2$ expressions described above.

To illustrate the idea of the proof, we will consider one of these cases. The other cases are similar. Suppose that $\Phi(kx,ky) = \Phi(y\zeta_m, x)$. Then $kx \equiv y\zeta_m$ and $ky \equiv x$. It follows that $k^2x \equiv ky\zeta_m \equiv x\zeta_m$. From here we find that x is of the form $x = (a+b\tau)/(k^2-\zeta_m)$ for some integers a and b. Note that ζ_m is a unit in $L(\tau)$. Using $kx \equiv y\zeta_m$, we find that $y \equiv (k(a+b\tau)/\zeta_m)/(k^2-\zeta_m)$. Thus

$$\Phi(x,y) = \Phi\left(\frac{a+b\tau}{k^2-\zeta_m}, \frac{k(a+b\tau)/\zeta_m}{k^2-\zeta_m} \right) = \Phi\left(\frac{a+b\tau}{k^2-\zeta_m}, \frac{k(a+b\tau)}{k^2-\zeta_m} \right).$$

Here the last equality follows from the $\Phi(x,y) = \Phi(x,y\zeta_m)$ □

LEMMA 1.5. *Let $G = (4,2)_1$. For $k \neq -1,0,1$, we have* $\mathrm{Fix}(F_k) = S_1 \cup S_2$ *where*

$$S_1 = \left\{ \Phi\left(\frac{a+bi}{k-i^c}, \frac{d+ei}{k-i^f} \right) : a,b,c,d,e,f \in \mathbf{Z} \text{ and } c \equiv f \pmod 2 \right\},$$
$$S_2 = \left\{ \Phi\left(\frac{a+bi}{k^2-(-1)^c}, \frac{i^d k(a+bi)}{k^2-(-1)^c} \right) : a,b,c,d \in \mathbf{Z} \right\}.$$

PROOF. The group $G = (4,2)_1$ has 16 elements and the following are equal:

$$\begin{array}{cccc} \Phi(x,y) & \Phi(-x,y) & \Phi(x,-y) & \Phi(-x,-y) \\ \Phi(ix,iy) & \Phi(-ix,iy) & \Phi(ix,-iy) & \Phi(-ix,-iy) \\ \Phi(y,x) & \Phi(y,-x) & \Phi(-y,x) & \Phi(-y,-x) \\ \Phi(iy,ix) & \Phi(iy,-ix) & \Phi(-iy,ix) & \Phi(-iy,-ix) \end{array}$$

The proof is similar to the previous one. The eight expressions in the first two rows give rise to the fixed points in the set S_1. The parameter d appearing within the description of S_2 is essential because $\Phi(x,y) \neq \Phi(x,iy)$ unlike the case $(4,1)_0$. □

LEMMA 1.6. *Let $G = (3,3)_0$. For $k \neq -1,0,1$, we have* $\mathrm{Fix}(F_k) = S_1 \cup S_2 \cup S_3$ *where*

$$S_1 = \left\{ \Phi\left(\frac{a+b\tau}{k-1}, \frac{c+d\tau}{k-1} \right) : a,b,c,d \in \mathbf{Z} \right\}$$
$$S_2 = \left\{ \Phi\left(\frac{a+b\tau}{k^2-1}, \frac{k(a+b\tau)}{k^2-1} \right) : a,b \in \mathbf{Z} \right\}$$
$$S_3 = \left\{ \Phi\left(\frac{a+b\tau}{k^2+k+1}, \frac{k(a+b\tau)}{k^2+k+1} \right) : a,b \in \mathbf{Z} \right\}.$$

PROOF. The group $(3,3)_0$ has size 6 and the expressions giving rise to fixed points in the sets S_i are as follows:

S_1	S_2	S_3
$\Phi(x,y)$	$\Phi(y,x)$	$\Phi(-(x+y),x)$
	$\Phi(x,-(x+y))$	$\Phi(y,-(x+y))$
	$\Phi(-(x+y),y)$	

The proof is similar to the proof of Lemma 1.4 and omitted. □

For the number-theoretic applications in the next section of this paper, we need to determine $|\mathrm{Fix}(F_\lambda)|$, the number of fixed points of F_λ. If the fixed points are non-degenerate, then it takes a standard application of the Lefschetz fixed point formula to compute $|\mathrm{Fix}(F_\lambda)|$. In the next lemma, we determine $|\mathrm{Fix}(F_\lambda)|$ by a simple calculation which exploits the following explicit description of non-constant holomorphic (hence algebraic) maps $F : \mathbf{P}^n \to \mathbf{P}^n$:

> $F = [f_1 : f_2 : f_3]$ where each f_i is a homogeneous polynomial of the same degree d, and the only common zero of $f_i, i = 1,2,3$ is the origin.

LEMMA 1.7. *Let k be an integer not equal to $-1, 0, 1$. Then*

$$|\mathrm{Fix}(F_k)| \leq k^4 + k^2 + 1.$$

PROOF. Suppose that $F_k = [f_1 : f_2 : f_3]$. Since the topological degree $\deg(F_k) = k^4$, we see that $\deg(f_i) = k^2$. Set $d = k^2$. We want to solve the system (I)

$$f_1(x,y,z) = cx,$$
$$f_2(x,y,z) = cy,$$
$$f_3(x,y,z) = cz.$$

where c is a non-zero constant. We work in $\mathbf{P}^3$, to exploit elementary intersection theory and we consider the system (II)

$$f_1(x,y,z) = xw^{d-1},$$
$$f_2(x,y,z) = yw^{d-1},$$
$$f_3(x,y,z) = zw^{d-1}.$$

by putting $c = w^{d-1}$. In $\mathbf{P}^3$, we have d^3 number of solutions for (II) which is counted with multiplicities. Clearly all of these solutions lie in $\mathbf{P}^3 \setminus \{w = 0\}$, since otherwise

$$f_1 = f_2 = f_3 = 0$$

at such a point giving rise to $x = y = z = 0 = w$ which is impossible. Discarding the trivial solution $[0 : 0 : 0 : 1] \in \mathbf{P}^3$, we see that

$$d^3 - 1 = (d-1)(d^2 + d + 1)$$

solutions project to solutions of (I) in $\mathbf{P}^2$. We observe that if $\zeta^d = \zeta \neq 0$, then $[\zeta x : \zeta y : \zeta z : 1]$ gives a solution of (II) for each solution $[x : y : z : 1]$. Since $[x : y : z] = [\zeta x : \zeta y : \zeta z]$ when projected to $\mathbf{P}^2$, we see that

$$|\mathrm{Fix}(F_k)| \leq \frac{d^3 - 1}{d - 1} = d^2 + d + 1. \qquad \square$$

2. Exceptionality.

Let E be an elliptic curve and let p be a prime at which E has a supersingular reduction. In this case, the map $[p] : E \to E$ reduces to the Frobenius map

$$\mathrm{Frob}_{p^2} : [X : Y : Z] \mapsto [X^{p^2} : Y^{p^2} : Z^{p^2}].$$

Therefore, working with the reduction mod p of the commutative diagram defining F_p and letting $\psi = (\psi_1, \psi_2, \psi_3)$ denote the projection map

$$\psi : E \times E \to \mathbf{P}^2$$

we see that

$$\bar{F}_p \circ \psi = \psi \circ [p] = (\psi_1^{p^2}, \psi_2^{p^2}, \psi_3^{p^2}).$$

Hence it follows that $\bar{F}_p = \mathrm{Frob}_{p^2}$. From this observation, we obtain the following

Lemma 2.1. *Let E be an elliptic curve and let p be a prime at which E has a supersingular reduction. Let L be the number field obtained by adjoining the coordinates of p-torsion points of E to $\mathbf{Q}$ and let $\mathfrak{p}$ be a prime ideal of L lying over p. Then there exists a one-to-one correspondence*

$$\mathbf{P}^2(\mathbf{F}_{p^2}) \longleftrightarrow \overline{\mathrm{Fix}(F_p)}$$

which is given by the reduction modulo $\mathfrak{p}$.

Proof. There are at most $p^4 + p^2 + 1$ fixed points of F_p. On the other hand, we have $\bar{F}_p = \mathrm{Frob}_{p^2}$ and $\mathrm{Fix}(\mathrm{Frob}_{p^2}) = \mathbf{P}^2(\mathbf{F}_{p^2})$. Since $|\mathbf{P}^2(\mathbf{F}_{\ell^2})| = p^4 + p^2 + 1$, the reduction of each fixed point of F_p modulo $\mathfrak{p}$ must reduce to a different fixed point of Frob_{p^2}. $\square$

This correspondence is compatible with the action of F_k and allows us to obtain one of the main results of this paper.

THEOREM 2.2. *Let E be an elliptic curve and let F_k be the resulting map under a crystallographic group of Theorem* 1.3. *Let p be a prime at which E has supersingular reduction. Then the reduced map $\bar{F}_k : \mathbf{P}^2(\mathbf{F}_{p^2}) \to \mathbf{P}^2(\mathbf{F}_{p^2})$ is a permutation if and only if the corresponding condition (or conditions) holds*:

- $G(m,1,2)$: $\gcd(p^{2m}-1,k)=1$,
- $G(4,2,2)$: $\gcd(p^4-1,k)=1$,
- $G(3,3,2)$: $\gcd(p^s-1,k)=1$ *for* $s=1,2,3$.

PROOF. By the lemmata 1.4, 1.5 and 1.6, we see that the fixed points of F_p are of the form

$$\Phi\left(\frac{a+b\tau}{p^s-1}, \frac{c+d\tau}{p^s-1}\right)$$

for some $a,b,c,d \in \mathbf{Z}$ and $s \in \{1,2,3,4,6,8,12\}$. Moreover $F_k : \mathrm{Fix}(F_p) \to \mathrm{Fix}(F_p)$ is well-defined, i.e. if $\alpha \in \mathrm{Fix}(F_p)$ then so is $F_k(\alpha)$.

Suppose that k is an integer satisfying the condition (or conditions) of the group $G(m,\ell,2)$. In other words $\gcd(p^s-1,k)=1$ for one (or several) s. Then there exists an integer k' such that $kk' \equiv 1 \pmod{p^s-1}$ for each s. Then $F_k \circ F_{k'}$ is the identity map on $\mathrm{Fix}(F_p)$. Thus F_k permute $\mathrm{Fix}(F_p)$ and therefore $\bar{F}_k$ permutes $\mathbf{P}(\mathbf{F}_{p^2})$.

Conversely, if $\gcd(p^s-1,k) \neq 1$ for one s, then we can construct a fixed point of F_p which is no longer in $F_k(\mathrm{Fix}(F_p))$. We illustrate this by giving an example for one case. For example, suppose that $G=G(4,2,2)$ and $\gcd(p^4-1,k)=t>1$. Without loss of generality, assume that $\gcd(t,p^2-i)$ is not trivial in $\mathbf{Z}[i]$. Then the element $\Phi(1/(p^2-i), p/(p^2-i))$ is in $\mathrm{Fix}(F_p)$ but it is not in $F_k(\mathrm{Fix}(F_p))$. One can construct similar examples for the other cases. Since $\mathrm{Fix}(F_p)$ is a finite set, this implies that F_k does not permute $\mathrm{Fix}(F_p)$ and therefore $\bar{F}_k$ does not permute $\mathbf{P}^2(\mathbf{F}_{p^2})$. □

COROLLARY 2.3. *Let E be an elliptic curve defined over a number field with CM. Then for each $G(m,\ell,2)$, the map F_{19} is exceptional.*

PROOF. Suppose that E has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field K. Consider the number field $L=K(\zeta_{19}+\zeta_{19}^{-1})$ with

$$\mathrm{Gal}(L/\mathbf{Q}) \simeq \mathbf{Z}_{18}.$$

By Chebotarev's density theorem there are infinitely many primes which remain inert in L. Each such prime p remains inert in both K and $\mathbf{Q}(\zeta_{19}+\zeta_{19}^{-1})$. It follows that E has supersingular reduction at p and the order of p modulo 19 is either 9 or 18. It is now easy to see that each condition $\gcd(p^s-1,19)=1$ with $s \in \{1,2,3,4,6,8,12\}$ of Theorem 2.2 is satisfied for infinitely many primes. □

This corollary proves Theorem 1. We remark that the assumption that E has complex multiplication is essential for the proof of Theorem 1:

Firstly, we do not know if there are infinitely many primes at which E has supersingular reduction. Lang and Trotter [**LT76**] conjectured the distribution of supersingular primes of norms $\leq x$ for a non-CM elliptic curve E over $\mathbf{Q}$ to be asymptotic to

$$c_E \frac{\sqrt{x}}{\log(x)}$$

as x goes infinity, for some positive constant c_E. Serre proved that the density of supersingular primes is zero [**Se81**]. Elkies proved that there is an infinite number of supersingular primes for any elliptic curve $E/\mathbf{Q}$ [**El87**]. Later, he extended his result to an elliptic curve E over any number field with a real embedding [**El89**]. No such result is known in general for other number fields.

Secondly, even if there are infinitely many primes $\{p_1, p_2, \ldots\}$ at which E has supersingular reduction, one may fail to construct an exceptional map F_k by our method. It is possible that the set $\{p_1^s - 1, p_2^s - 1, \ldots\}$ reduced modulo k has only finitely many nonzero terms for each positive integer k. To see that such a set of primes exist, let us define p_i to be congruent to 1 modulo the first i primes. Such a prime p_i exists by the infinitude of primes in arithmetic progressions.

References

[BS78] J. Bernstein and O. Schwarzman, Chevalley's theorem for complex crystallographic Coxeter groups, Funktsional. Anal. i Prilozhen, **12** (1978), 79–80 [Russian].

[BS06] J. Bernstein and O. Schwarzman, Complex crystallographic Coxeter groups and affine root systems, J. Nonlinear Math. Phys., **13** (2006), 163–182.

[El87] N. D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over $\mathbf{Q}$, Invent. Math., **89** (1987), 561–567.

[El89] N. D. Elkies, Supersingular primes for elliptic curves over real number fields, Compositio Math., **72** (1989), 165–172.

[Fr70] M. Fried, On a conjecture of Schur, Michigan Math. J., **17** (1970), 41–55.

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

[KTY82] J. Kaneko, S. Tokunaga and M. Yoshida, Complex crystallographic groups, II, J. Math. Soc. Japan, **34** (1982), 595–605.

[Kü16] Ö. Küçüksakallı, Bivariate polynomial mappings associated with simple complex Lie algebras, J. Number Theory, **168** (2016), 433–451.

[LT76] S. Lang and H. Trotter, Frobenius distributions in GL_2-extensions, Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Math., **504**, Springer-Verlag, Berlin-New York, 1976, iii+274 pp.

[Lo76] E. Looijenga, Root systems and elliptic curves, Invent. Math., **38** (1976/77), 17–32.

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

[Ro10] F. Rong, Lattès maps on $\mathbf{P}^2$, J. Math. Pures Appl. (9), **93** (2010), 636–650.

[Se81] J. P. Serre, Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Études Sci. Publ. Math., **54** (1981), 323–401.

[TY82] S. Tokunaga and M. Yoshida, Complex crystallographic groups, I, J. Math. Soc. Japan, **34** (1982), 581–593.

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

Hurşit ÖNSİPER
Middle East Technical University
Mathematics Department
06800 Ankara, Turkey
E-mail: hursit@metu.edu.tr