ACTA ARITHMETICA
199.3 (2021)

Adelic point groups of elliptic curves

by

ATHANASIOS ANGELAKIS (Athens) and PETER STEVENHAGEN (Leiden)

1. Introduction. Since the early 20th century, it has been a standard technique to study number fields K in terms of their completions $K_\mathfrak{p}$ at primes $\mathfrak{p}$, both finite and infinite. In the 1940s, all these completions were combined by Chevalley in the adele ring $\mathbf{A}_K$ of K. This is a restricted direct product of completions, with the integrality restriction in place to make $\mathbf{A}_K$ locally compact, a property that all completions $K_\mathfrak{p}$ have, and that is essential in harmonic analysis. The adele ring and its unit group, the idele group, play an essential role in Tate's derivation of the functional equations of Hecke L-functions and the idelic formulation of class field theory [3].

It is a natural question whether $\mathbf{A}_K$ characterizes the number field K, i.e., whether non-isomorphic number fields can have topologically isomorphic adele rings. Given the direct relation of $\mathbf{A}_K$ to basic invariants of the number field such as the zeta function ζ_K of K and and the absolute abelian Galois group G_K^{ab} of K, this question neatly fits in a series of identical questions for ζ_K, for G_K^{ab} and for the absolute Galois group G_K itself. It turns out that, whereas the topological group G_K does characterize K up to isomorphism by the Neukirch–Uchida theorem [6, 12.2.1], its maximal abelian quotient G_K^{ab}, the adele ring $\mathbf{A}_K$ and the zeta function ζ_K do not; see [1, Section 1.4] for an extensive discussion and bibliography.

Non-isomorphic number fields with identical zeta functions or isomorphic adele rings are very rare, and they do not exist for small degrees. Finding non-isomorphic number fields with isomorphic absolute abelian Galois groups is even harder, and so far it has only been achieved for imaginary quadratic fields. Somewhat surprisingly, even though there are infinitely many isomorphism types of G_K^{ab} for imaginary quadratic K, we know that, at least conjecturally [2, Conjecture 7.1], many of them share the same 'minimal' isomorphism type.

2020 *Mathematics Subject Classification*: Primary 11G05, 11G07; Secondary 11F80.
Key words and phrases: elliptic curves, adelic points, Galois representation.
Received 25 October 2017; revised 8 January 2021.
Published online 20 July 2021.

DOI: 10.4064/aa171025-27-3

For elliptic curves E defined over a number field K, it is also standard to view them over the completions $K_{\mathfrak{p}}$ to study their reduction properties, but less so over the adele ring $\mathbf{A}_K$, maybe because it is not a field. Still, it is a perfectly natural question what the *adelic point group* $E(\mathbf{A}_K)$ of E over $\mathbf{A}_K$ looks like, and to what extent it characterizes E/K. In view of Lemma 2.1 below, we can define it as the product

$$E(\mathbf{A}_K) = \prod_{\mathfrak{p}\leq\infty} E(K_{\mathfrak{p}}) \tag{1}$$

of the point groups of E over all completions of K, both finite and infinite. This yields an uncountable abelian group that contains all $\mathfrak{p}$-adic point groups as subgroups, and continuously surjects onto the point groups $\overline{E}(k_{\mathfrak{p}})$ at all primes of good reduction. It is in a natural way a compact topological group.

In view of the fact that elliptic curves E/K still give rise to basic open questions such as the effective computation of $E(K)$, the finiteness of its Tate–Shafarevich group, and the 'average behavior' of $E(K)$, it may come as a surprise that the adelic point group $E(\mathbf{A}_K)$ not only admits a very explicit description as a compact topological group, but this description is also almost universal in the sense that most E over a given number field K give rise to the *same* adelic point group.

Theorem 1.1. *Let K be a number field of degree n. Then for almost all elliptic curves E/K, the adelic point group $E(\mathbf{A}_K)$ is topologically isomorphic to the universal group*

$$\mathcal{E}_n = (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$$

associated to the degree n of K.

The notion of 'almost all' in Theorem 1.1 is the same as in [10], and is based on the counting of elliptic curves over K given by short affine Weierstrass models

$$E_{a,b} : y^2 = x^3 + ax + b \tag{2}$$

with integral coefficients $a, b \in \mathcal{O}_K$ satisfying

$$\Delta_E = \Delta(a,b) = -16(4a^3 + 27b^2) \neq 0.$$

To define it, we fix a norm $\|\cdot\|$ on the real vector space $\mathbf{R} \otimes_{\mathbf{Z}} \mathcal{O}_K^2 \cong \mathbf{R}^{2n}$ in which $\mathcal{O}_K^2$ embeds as a lattice. Then for any positive real number X, the set S_X of elliptic curves $E_{a,b}$ with $\|(a,b)\| < X$ is finite, and we say that *almost all* elliptic curves over K have some property if the fraction of elliptic curves $E_{a,b}$ in S_X having that property tends to 1 when $X \in \mathbf{R}_{>0}$ tends to infinity.

As the elliptic curves E/K having complex multiplication (CM) over $\overline{K}$ have their j-invariants inside a finite subset of K, almost all elliptic curves over K are without CM. This allows us to disregard CM-curves in the proof of Theorem 1.1, but we will see in Remark 4.2 that this distinction is hardly relevant.

Our proof of Theorem 1.1 is in three steps. The first, in Section 2, only uses the standard theory of elliptic curves from [9]. It shows that the connected component $E_{\mathrm{cc}}(\mathbf{A}_K)$ of the zero element is a subgroup of $E(\mathbf{A}_K)$ isomorphic to $(\mathbf{R}/\mathbf{Z})^n$, and that it splits off in the sense that we have a decomposition

$$E(\mathbf{A}_K) \cong E_{\mathrm{cc}}(\mathbf{A}_K) \times E(\mathbf{A}_K)/E_{\mathrm{cc}}(\mathbf{A}_K).$$

The totally disconnected group $E(\mathbf{A}_K)/E_{\mathrm{cc}}(\mathbf{A}_K)$ is profinite, and can be analyzed by methods resembling those we employed for the multiplicative group $\mathbf{A}_K^*$ in the class-field-theoretic setting of [2]. It fits in a split exact sequence

$$0 \to T_{E/K} \to E(\mathbf{A}_K)/E_{\mathrm{cc}}(\mathbf{A}_K) \to \widehat{\mathbf{Z}}^n \to 0$$

of $\widehat{\mathbf{Z}}$-modules, with n the degree of K. Here $T_{E/K}$ is the closure of the torsion subgroup of $E(\mathbf{A}_K)/E_{\mathrm{cc}}(\mathbf{A}_K)$, and we can write $E(\mathbf{A}_K)$ as a product

$$E(\mathbf{A}_K) \cong (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times T_{E/K} \tag{3}$$

in which only $T_{E/K}$ depends on the choice of the particular elliptic curve E over K.

In a second step, we show in Section 3 that the *torsion closure* $T_{E/K}$, which is a countable product of finite cyclic groups, is isomorphic to the group $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$ for those E that satisfy a condition in terms of the division fields associated to E/K. Whether this condition is satisfied can be read off from the Galois representation associated to the torsion points of E. The final step concluding the proof of Theorem 1.1, in Section 4, uses recent results of Jones and Zywina [5, 10] to show that this condition is met for almost all elliptic curves over K.

The notion of 'almost all' from Theorem 1.1 still allows for many E/K having adelic point groups *different* from the universal group $\mathcal{E}_n$. Such non-generic adelic point groups can be characterized by a finite set of prime powers ℓ^k for which cyclic direct summands of order ℓ^k are 'missing' from $T_{E/K}$. It is easy (Lemma 5.1) to produce elliptic curves for which $E(\mathbf{A}_K)$ has prescribed missing summands by base changing any given elliptic curve to an appropriate extension field. It is much harder to construct elliptic curves with non-generic adelic point groups over a *given* number field K. Theorem 5.4 shows that, for given K, there are only finitely many prime powers ℓ^k for which cyclic direct summands of order ℓ^k can be missing from adelic point groups of elliptic curves E/K. For $K = \mathbf{Q}$, the only prime power is $\ell^k = 2$, and this is used in Theorem 5.6 to prove an explicit version of the following result.

THEOREM 1.2. *Let K be a number field of degree n. Then there exist infinitely many elliptic curves E/K that are pairwise non-isomorphic over an algebraic closure of K, and for which $E(\mathbf{A}_K)$ is a topological group not isomorphic to $\mathcal{E}_n$.*

2. Structure of adelic point groups. Let E be an elliptic curve over a number field K. As $\mathbf{A}_K$ is a K-algebra inside the full product $\prod_{\mathfrak{p}\leq\infty} K_{\mathfrak{p}}$, the adelic point group $E(\mathbf{A}_K)$ naturally embeds into $\prod_{\mathfrak{p}\leq\infty} E(K_{\mathfrak{p}})$. The justification for our definition (1) is the following.

LEMMA 2.1. *The natural inclusion $E(\mathbf{A}_K) \to \prod_{\mathfrak{p}\leq\infty} E(K_{\mathfrak{p}})$ is an isomorphism.*

Proof. The ring $\mathbf{A}_K$ consists of elements $(x_{\mathfrak{p}})_{\mathfrak{p}}$ that are almost everywhere integral, i.e., for which we have $x_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$ for almost all finite primes $\mathfrak{p}$ of K, with $\mathcal{O}_{\mathfrak{p}} \subset K_{\mathfrak{p}}$ the local ring of integers at $\mathfrak{p}$. For E given by a projective model $E_{a,b}$ as in (2), every $K_{\mathfrak{p}}$-valued point of E with $\mathfrak{p}$ finite can be written with coordinates in $\mathcal{O}_{\mathfrak{p}}$. It follows that every element in $\prod_{\mathfrak{p}\leq\infty} E(K_{\mathfrak{p}})$ is actually in $E(\mathbf{A}_K)$. ∎

As the structure of $E(K_{\mathfrak{p}})$ is different for archimedean and non-archimedean $\mathfrak{p}$, we treat these cases separately.

For archimedean primes, $K_{\mathfrak{p}}$ is either $\mathbf{R}$ or $\mathbf{C}$. At complex places, $E(K_{\mathfrak{p}})$ is isomorphic to $(\mathbf{R}/\mathbf{Z})^2$, as we have $E(\mathbf{C}) \cong \mathbf{C}/\Lambda$ for some lattice $\Lambda \subset \mathbf{C}$. At real places, the two possibilities for $E(K_{\mathfrak{p}})$ are

$$E(K_{\mathfrak{p}}) \cong \begin{cases} \mathbf{R}/\mathbf{Z} & \text{if } \Delta_E <_{\mathfrak{p}} 0, \\ \mathbf{R}/\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} & \text{if } \Delta_E >_{\mathfrak{p}} 0, \end{cases} \tag{4}$$

depending on the sign of the discriminant $\Delta_E \in K^*$ under $\mathfrak{p} : K \to \mathbf{R}$.

PROPOSITION 2.2. *Let K be a number field of degree n, and E/K an elliptic curve with discriminant $\Delta_E \in K^*/(K^*)^{12}$. Then we have an isomorphism of topological groups*

$$\prod_{\mathfrak{p}|\infty} E(K_{\mathfrak{p}}) \cong (\mathbf{R}/\mathbf{Z})^n \times (\mathbf{Z}/2\mathbf{Z})^r.$$

Here $r \leq n$ is the number of real primes $\mathfrak{p}$ of K for which $\Delta_E >_{\mathfrak{p}} 0$.

Proof. Let K have r_1 real and r_2 complex primes; then $\prod_{\mathfrak{p}|\infty} E(K_{\mathfrak{p}})$ is the product of $r_1 + 2r_2 = n$ circle groups $\mathbf{R}/\mathbf{Z}$ and r copies of $\mathbf{Z}/2\mathbf{Z}$, with $r \leq r_1 \leq n$. ∎

To obtain the non-archimedean part $\prod_{\mathfrak{p}<\infty} E(K_{\mathfrak{p}})$ of $E(\mathbf{A}_K)$, we take $\mathfrak{p}$ finite and $E = E_{a,b}$ as in (2), and consider the continuous reduction map

$\phi_{\mathfrak{p}} : E(K_{\mathfrak{p}}) \to \overline{E}(k_{\mathfrak{p}})$ to the finite set of points of the reduced curve $\overline{E}$ over $k_{\mathfrak{p}} = \mathcal{O}_K/\mathfrak{p}$. The set of points in the non-singular locus $\overline{E}^{\mathrm{ns}}(k_{\mathfrak{p}})$ is contained in the image of $\phi_{\mathfrak{p}}$ and inherits a natural group structure from $E(K_{\mathfrak{p}})$. For $E_0(K_{\mathfrak{p}}) = \phi^{-1}[\overline{E}^{\mathrm{ns}}(k_{\mathfrak{p}})]$ we obtain an exact sequence of topological groups

$$1 \to E_1(K_{\mathfrak{p}}) \to E_0(K_{\mathfrak{p}}) \to \overline{E}^{\mathrm{ns}}(k_{\mathfrak{p}}) \to 1, \tag{5}$$

so the kernel of reduction $E_1(K_{\mathfrak{p}})$ is a subgroup of finite index in $E_0(K_{\mathfrak{p}})$. For primes of good reduction, the sequence simply reads

$$1 \to E_1(K_{\mathfrak{p}}) \to E(K_{\mathfrak{p}}) \to \overline{E}(k_{\mathfrak{p}}) \to 1, \tag{6}$$

and for $\mathfrak{p}$ of bad reduction, $E_0(K_{\mathfrak{p}}) \subsetneq E(K_{\mathfrak{p}})$ is a subgroup of *finite* index [9, VII.6.2]. Either way, $E_1(K_{\mathfrak{p}}) \subset E(K_{\mathfrak{p}})$ is a subgroup of finite index.

We can describe $E_1(K_{\mathfrak{p}})$ using the formal group of E as in [9, Chapter IV]. More precisely, the elliptic logarithm $\log_{\mathfrak{p}} : E_1(K_{\mathfrak{p}}) \to \mathcal{O}_{\mathfrak{p}}$ has a finite kernel of p-power order, and its image, which is an open additive subgroup of the valuation ring $\mathcal{O}_{\mathfrak{p}} \subset K_{\mathfrak{p}}$, is non-canonically isomorphic to $\mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]}$. As $E(K_{\mathfrak{p}})$ contains a finitely generated $\mathbf{Z}_p$-module of free rank $[K_{\mathfrak{p}} : \mathbf{Q}_p]$ as a subgroup of finite index, its torsion subgroup $T_{\mathfrak{p}} \subset E(K_{\mathfrak{p}})$ is finite, and $E(K_{\mathfrak{p}})/T_{\mathfrak{p}}$ is a free $\mathbf{Z}_p$-module of rank $[K_{\mathfrak{p}} : \mathbf{Q}_p]$. If we non-canonically write

$$E(K_{\mathfrak{p}}) \cong \mathbf{Z}_p^{[K_{\mathfrak{p}}:\mathbf{Q}_p]} \times T_{\mathfrak{p}} \tag{7}$$

and take the product over all non-archimedean primes $\mathfrak{p}$ of K, we can use the fact that the sum of the local degrees at the primes over p in K equals $n = [K : \mathbf{Q}]$ to obtain the following non-archimedean analogue of Proposition 2.2.

PROPOSITION 2.3. *Let E be an elliptic curve over a number field K of degree n. Then we have an isomorphism of topological groups*

$$\prod_{\mathfrak{p}<\infty} E(K_{\mathfrak{p}}) = \widehat{\mathbf{Z}}^n \times \prod_{\mathfrak{p}<\infty} T_{\mathfrak{p}},$$

where $T_{\mathfrak{p}} = E(K_{\mathfrak{p}})^{\mathrm{tor}}$ is the finite torsion subgroup of $E(K_{\mathfrak{p}})$. ∎

In order to combine Propositions 2.2 and 2.3, we define the profinite group

$$T_{E/K} = \prod_{\mathfrak{p}\le\infty} T_{\mathfrak{p}} \tag{8}$$

as a product of finite groups $T_{\mathfrak{p}}$ given by

$$T_{\mathfrak{p}} = \begin{cases} E(K_{\mathfrak{p}})^{\mathrm{tor}} & \text{if } \mathfrak{p} \text{ is finite,} \\ \mathbf{Z}/2\mathbf{Z} & \text{if } \mathfrak{p} \text{ is real and } \Delta_E >_{\mathfrak{p}} 0, \\ 1 & \text{otherwise.} \end{cases} \tag{9}$$

With this definition, the adelic point group of E over the number field K of degree n is a topological group that can be written, as promised in (3), as

$$E(\mathbf{A}_K) \cong (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times T_{E/K}.$$

In this decomposition, $(\mathbf{R}/\mathbf{Z})^n$ is the connected component $E_{\mathrm{cc}}(\mathbf{A}_K)$ of the zero element in $E(\mathbf{A}_K)$, and in the totally disconnected profinite group

$$E(\mathbf{A}_K)/E_{\mathrm{cc}}(\mathbf{A}_K) \cong \widehat{\mathbf{Z}}^n \times T_{E/K},$$

$T_{E/K}$ is the *closure* of the torsion subgroup. Thus, the isomorphism type of $E(\mathbf{A}_K)$ is determined by the degree n of K and the structure of the *torsion closure* $T_{E/K}$.

3. Structure of the torsion closure. Let T be any group that is obtained as a countable product of finite abelian or, equivalently, finite cyclic groups. Then there are usually many ways to represent T as a product. The group $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$ occurring in Theorem 1.1 is for instance isomorphic to $\prod_{m=2020}^{\infty} \mathbf{Z}/m\mathbf{Z}$, to $(\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z})^2$, and even to $\prod_p \mathbf{F}_p^*$. Our choice is arbitrary, but requires only few characters to write it down.

In order to understand this notational ambiguity, and to deal with it, we can represent a countable product T of finite cyclic groups in a more canonical way. Writing each of the cyclic constituents as a product of cyclic groups of prime power order and taking the cyclic groups of each prime power order together, we arrive at its *standard representation*

$$T = \prod_{\ell \text{ prime}} \prod_{k=1}^{\infty} (\mathbf{Z}/\ell^k\mathbf{Z})^{e(\ell^k)}.$$

The exponents $e(\ell^k)$ are invariants of T, as they can be defined intrinsically in terms of T as

$$e(\ell^k) = \dim_{\mathbf{F}_\ell} T[\ell^k]/(T[\ell^{k-1}] + \ell T[\ell^{k+1}]).$$

We call $e(\ell^k)$ the *ℓ^k-rank* of T. Clearly, two countable products of finite cyclic groups are isomorphic if and only if their ℓ^k-ranks coincide for *all* prime powers $\ell^k > 1$.

The ℓ^k-rank $e(\ell^k)$ of T is either finite, in $\mathbf{Z}_{\geq 0}$, or countably infinite. In the latter case we write $e(\ell^k) = \omega$, and note that we may identify

$$(\mathbf{Z}/\ell^k\mathbf{Z})^{\omega} = \mathrm{Map}(\mathbf{Z}_{>0}, \mathbf{Z}/\ell^k\mathbf{Z})$$

with the group of $\mathbf{Z}/\ell^k\mathbf{Z}$-valued functions on the set $\mathbf{Z}_{>0}$ of positive integers.

The group $T_{\max} = \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$ occurring in Theorem 1.1 has $e(\ell^k) = \omega$ for all prime powers ℓ^k, as there are infinitely many integers m that are exactly divisible by ℓ^k. Leaving out finitely many m from the product, or having each m occur twice, does not change the isomorphism type. As there are infinitely many primes p for which $p-1$ is exactly divisible by ℓ^k, by the classical theorem of Dirichlet on primes in arithmetic progressions, we also have $T_{\max} \cong \prod_p \mathbf{F}_p^*$, as claimed above.

In order to finish the proof of Theorem 1.1, we need to show that for given K, almost all E/K have the property that the torsion closure $T_{E/K}$ in (8) has infinite ℓ^k-rank for *all* prime powers $\ell^k > 1$, making $T_{E/K}$ isomorphic to $T_{\max}$.

In order to determine $e(\ell^k)$ for $T_{E/K}$, we need to count how many cyclic direct summands of order ℓ^k occur in $T_{\mathfrak{p}} = E(K_{\mathfrak{p}})^{\mathrm{tor}}$ at finite primes $\mathfrak{p}$ of K. This can be done by studying the splitting behavior of $\mathfrak{p}$ in the ℓ^k-*division fields*

$$Z_{E/K}(\ell^k) := K(E[\ell^k](\overline{K})) \tag{10}$$

of E over K. The ℓ^k-torsion subgroup $E(K_{\mathfrak{p}})[\ell^k] \subset T_{\mathfrak{p}}$ is full, i.e., isomorphic to $(\mathbf{Z}/\ell^k\mathbf{Z})^2$, if and only if $\mathfrak{p}$ splits completely in $K \subset Z_{E/K}(\ell^k)$. This leads to the following criterion for $T_{E/K}$ to have $e(\ell^k) = \omega$.

Lemma 3.1. *Let E/K be an elliptic curve, and $\ell^k > 1$ a prime power for which the inclusion*

$$Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$$

of division fields is strict. Then $T_{E/K}$ in (8) *has infinite ℓ^k-rank.*

Proof. Let $\mathfrak{p}$ be a finite prime of K that splits completely in the division field $Z_{E/K}(\ell^k)$, but not in the division field $Z_{E/K}(\ell^{k+1})$. Then $E(K_{\mathfrak{p}})$ has full ℓ^k-torsion, but not full ℓ^{k+1}-torsion. This implies that the finite group $T_{\mathfrak{p}}$ contains a subgroup isomorphic to $(\mathbf{Z}/\ell^k\mathbf{Z})^2$ but not one isomorphic to $(\mathbf{Z}/\ell^{k+1}\mathbf{Z})^2$, and therefore has at least one cyclic direct summand of order ℓ^k.

By our assumption, the set of primes $\mathfrak{p}$ that split completely in $Z_{E/K}(\ell^k)$, but not in $Z_{E/K}(\ell^{k+1})$, is infinite and of positive density

$$[Z_{E/K}(\ell^k) : K]^{-1} - [Z_{E/K}(\ell^{k+1}) : K]^{-1} > 0.$$

For all $\mathfrak{p}$ in the infinite set thus obtained, the group $T_{\mathfrak{p}}$ has a cyclic direct summand of order ℓ^k. It follows that $T_{E/K} = \prod_{\mathfrak{p}\leq\infty} T_{\mathfrak{p}}$ has infinite ℓ^k-rank. ∎

We conclude from Lemma 3.1 that for an elliptic curve E having the property that for all primes ℓ, the tower of ℓ-power division fields

$$Z_{E/K}(\ell) \subset Z_{E/K}(\ell^2) \subset Z_{E/K}(\ell^3) \subset \cdots \tag{11}$$

has strict inclusions at every level, $T_{E/K}$ is isomorphic to $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$. In this situation, $E(\mathbf{A}_K)$ is isomorphic to the universal group

$$\mathcal{E}_n = (\mathbf{R}/\mathbf{Z})^n \times \widehat{\mathbf{Z}}^n \times \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}, \tag{12}$$

in degree n, and E/K is *generic* in the sense of Theorem 1.1.

4. Universality of $\mathcal{E}_n$. In order to finish the proof of Theorem 1.1, it suffices to show that for almost all E defined over a fixed number field K, the extension $Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$ in the tower (11) of ℓ-power division fields is strict for all prime powers $\ell^k > 1$. In order to see this for a given E/K, we look at the Galois representation

$$\rho_{E/K} : G_K = \mathrm{Gal}(\overline{K}/K) \to \mathfrak{A}_K = \mathrm{Aut}(E(\overline{K})^{\mathrm{tor}}) \tag{13}$$

on the group $E(\overline{K})^{\mathrm{tor}}$ of its $\overline{K}$-valued torsion points. The group $\mathfrak{A}_K$ is isomorphic to $\varprojlim_m \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z}) = \mathrm{GL}_2(\widehat{\mathbf{Z}})$, since $E(\overline{K})^{\mathrm{tor}}$ is obtained as an injective limit

$$E(\overline{K})^{\mathrm{tor}} = \varinjlim_m E(\overline{K})[m] \cong \varinjlim_m \left(\frac{1}{m}\mathbf{Z}/\mathbf{Z}\right)^2 = (\mathbf{Q}/\mathbf{Z})^2.$$

The composition

$$\phi = \det \circ \rho_{E/K} : G_K \to \widehat{\mathbf{Z}}^*$$

does not depend on the choice of basis and gives the action of G_K on the maximal cyclotomic extension $K \subset K^{\mathrm{cyc}} = K(\zeta_\infty)$ of K: for $\sigma \in G_K$ and ζ a root of unity, we have $\sigma(\zeta) = \zeta^{\phi(\sigma)}$.

The restriction of the action of G_K to the m-torsion subgroup $E(\overline{K})[m]$ of $E(\overline{K})^{\mathrm{tor}}$ is described by the reduction

$$\rho_{E/K,m} : G_K \to \mathrm{Aut}(E(\overline{K})[m]) \cong \mathrm{GL}_2(\mathbf{Z}/m\mathbf{Z})$$

of $\rho_{E/K}$ modulo m, and the invariant field of $\ker \rho_{E/K,m}$ is the m-division field $Z_{E/K}(m) = K(E(\overline{K})[m])$ of E over K. In particular, we have an equivalence

$$Z_{E/K}(\ell^k) = Z_{E/K}(\ell^{k+1}) \iff \ker \rho_{E/K,\ell^k} = \ker \rho_{E/K,\ell^{k+1}}. \tag{14}$$

In case $\rho_{E/K}$ is *surjective*, all extensions $Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$ have degree

$$\ell^4 = \#\ker[\mathrm{GL}_2(\mathbf{Z}/\ell^{k+1}\mathbf{Z}) \to \mathrm{GL}_2(\mathbf{Z}/\ell^k\mathbf{Z})], \tag{15}$$

and in this case $E(\mathbf{A}_K)$ is isomorphic to the universal group $\mathcal{E}_n$ in (12).

It is certainly not true that the *Galois image* $\rho_{E/K}[G_K]$ is always equal to the full automorphism group $\mathfrak{A}_K = \mathrm{Aut}(E(\overline{K})^{\mathrm{tor}})$. There is however the basic result, due to Serre [8], that $\rho_{E/K}[G_K]$ is an *open* subgroup of $\mathfrak{A}_K$ if E is without CM, i.e., if E does *not* have complex multiplication over $\overline{K}$. In particular, the index of $\rho_{E/K}[G_K]$ in $\mathfrak{A}_K \cong \mathrm{GL}_2(\widehat{\mathbf{Z}})$ is always finite for E without CM. As observed in the introduction, elliptic curves defined over K with CM over $\overline{K}$ have their j-invariants in some *finite* subset of K. This is because for any number field K, there are only finitely many imaginary quadratic orders $\mathcal{O}$ for which the j-invariant $j(\mathcal{O})$ lies in K. As a consequence, almost all elliptic curves over K are without CM.

We first look at the case $K = \mathbf{Q}$, which is somewhat particular as there is a special complication that prevents $\rho_{E/K}$ in all cases from being surjective. In order to describe it, we let

$$\chi_2 : \mathfrak{A}_{\mathbf{Q}} = \mathrm{Aut}(E(\overline{\mathbf{Q}})^{\mathrm{tor}}) \to \mathrm{Aut}(E[2](\overline{\mathbf{Q}})) \cong \mathrm{GL}_2(\mathbf{Z}/2\mathbf{Z}) \cong S_3 \to \{\pm 1\}$$

be the non-trivial quadratic character that maps an automorphism of $E(\overline{\mathbf{Q}})^{\mathrm{tor}}$ to the sign of the permutation by which it acts on the three non-trivial 2-torsion points of E. For $\sigma \in G_{\mathbf{Q}}$, the sign of this permutation for $\rho_{E/\mathbf{Q}}(\sigma)$ is reflected in the action of σ on the subfield $\mathbf{Q}(\sqrt{\Delta}) \subset Z_{E/K}(2)$ that is generated by the square root of the discriminant $\Delta = \Delta_E$ of the elliptic curve E, and is given by

$$\chi_2(\rho_{E/\mathbf{Q}}(\sigma)) = \sigma(\sqrt{\Delta})/\sqrt{\Delta}.$$

The Dirichlet character $\widehat{\mathbf{Z}}^* \to \{\pm 1\}$ corresponding to $\mathbf{Q}(\sqrt{\Delta})$ can be seen as a character

$$\chi_\Delta : \mathfrak{A}_{\mathbf{Q}} \cong \mathrm{GL}_2(\widehat{\mathbf{Z}}) \xrightarrow{\det} \widehat{\mathbf{Z}}^* \to \{\pm 1\}$$

on $\mathfrak{A}_{\mathbf{Q}}$. It is different from the character χ_2, which does not factor via the determinant map $\mathfrak{A}_{\mathbf{Q}} \xrightarrow{\det} \widehat{\mathbf{Z}}^*$ on $\mathfrak{A}_{\mathbf{Q}}$.

The *Serre character* $\chi_E : \mathfrak{A}_{\mathbf{Q}} \to \{\pm 1\}$ associated to E is the non-trivial quadratic character obtained as the product $\chi_E = \chi_2\chi_\Delta$. By construction, it vanishes on the Galois image $\rho_{E/\mathbf{Q}}(G_{\mathbf{Q}}) \subset \mathfrak{A}_{\mathbf{Q}}$, so the Galois image is never the full group $\mathfrak{A}_{\mathbf{Q}}$. In the case where we have $\rho_{E/\mathbf{Q}}(G_{\mathbf{Q}}) = \ker \chi_E$, we say that E is a *Serre curve.*

If E is a Serre curve, then the Galois image is of index 2 in the full group $\mathfrak{A}_{\mathbf{Q}} \cong \mathrm{GL}_2(\widehat{\mathbf{Z}})$, and for every prime power $\ell^k > 1$, the extension

$$Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$$

of division fields for E in Lemma 3.1 has the degree ℓ^4 from (15) for odd ℓ, and at least degree ℓ^3 for $\ell = 2$. In particular, the hypothesis of Lemma 3.1 on E is satisfied for all prime powers ℓ^k in case E is a Serre curve. Nathan Jones [5] proved in 2010 that, in the sense of our Theorem 1.1, almost all elliptic curves are Serre curves. This implies the case $K = \mathbf{Q}$ of Theorem 1.1, treated in [1].

THEOREM 4.1. *For almost all elliptic curves $E/\mathbf{Q}$, the adelic point group $E(\mathbf{A}_{\mathbf{Q}})$ is isomorphic to $\mathbf{R}/\mathbf{Z} \times \widehat{\mathbf{Z}} \times \prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$.* ∎

In order to deal with the case $K \neq \mathbf{Q}$, we need an analogue of Jones' result stating that for almost all E over K, the Galois image $\rho_{E/K}[G_K] \subset \mathfrak{A}_K$ is large. As quadratic extensions of a number field $K \neq \mathbf{Q}$ are mostly non-cyclotomic, there is no Serre character here. However, for number fields K that are not linearly disjoint from the maximal cyclotomic extension

$\mathbf{Q}^{\mathrm{cyc}} = \mathbf{Q}(\zeta_\infty)$ of $\mathbf{Q}$, the natural embedding

$$\mathrm{Gal}(K^{\mathrm{cyc}}/K) \to \mathrm{Gal}(\mathbf{Q}^{\mathrm{cyc}}/\mathbf{Q}) = \widehat{\mathbf{Z}}^*$$

will not be an isomorphism, and will identify $\mathrm{Gal}(K^{\mathrm{cyc}}/K)$ with some open subgroup $H_K \subset \widehat{\mathbf{Z}}^*$ of index equal to the field degree of the extension $\mathbf{Q} \subset (K \cap \mathbf{Q}^{\mathrm{cyc}})$. In this case, the Galois image $\rho_{E/K}[G_K] \subset \mathfrak{A}_K$ is contained in the inverse image $\det^{-1}[H_K]$ of H_K under the determinant map $\det : \mathfrak{A}_K \to \widehat{\mathbf{Z}}^*$. We say that the Galois image for an elliptic curve E over $K \neq \mathbf{Q}$ is *maximal* if

$$\rho_{E/K}[G_K] = \det^{-1}[H_K]. \tag{16}$$

For $K \neq \mathbf{Q}$, Zywina [10] proved in 2010 that, in the sense of our Theorem 1.1, almost all elliptic curves E/K have maximal Galois image. This allows us to finish the proof of our main theorem.

Proof of Theorem 1.1. The case $K = \mathbf{Q}$ is Theorem 4.1. For $K \neq \mathbf{Q}$, Zywina's result implies in particular that

$$\rho_{E/K}[G_K] = \det^{-1}[H_K] \subset \mathfrak{A}_K$$

contains $\ker[\det] \cong \mathrm{SL}_2(\widehat{\mathbf{Z}})$ for almost all E. It follows that for prime powers $\ell^k > 1$, the degree of the extension $Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$ for these E is maybe not the maximal possible degree ℓ^4 that we have in (15), but it is still at least

$$\ell^3 = \#\ker[\mathrm{SL}_2(\mathbf{Z}/\ell^{k+1}\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/\ell^k\mathbf{Z})]. \tag{17}$$

This implies that $T_{E/K}$ is the 'maximal' group $\prod_{m=1}^{\infty} \mathbf{Z}/m\mathbf{Z}$, and $E(\mathbf{A}_K)$ the generic group $\mathcal{E}_n$. ■

REMARK 4.2. Even though, for the purpose of Theorem 1.1, we can disregard all elliptic curves E/K having CM, one can show that also these curves typically have generic adelic point group, at least if we choose for K the field of definition $\mathbf{Q}(j(E))$ of E. This is because in the CM case the relevant extension of division fields $Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1})$ from Lemma 3.1 has generic degree ℓ^2, and can be described explicitly in terms of the ray class fields of conductor ℓ^k and ℓ^{k+1} associated to the CM-order of E.

5. Non-generic point groups. If the adelic point group $E(\mathbf{A}_K)$ is non-generic, there is a prime power $\ell^k > 1$ for which the inclusion of division fields

$$Z_{E/K}(\ell^k) \subset Z_{E/K}(\ell^{k+1}) \tag{18}$$

is an equality. In case we can freely choose our ground field K, it is easy to force equality in (18) and construct elliptic curves E/K for which the torsion closure $T_{E/K}$ has ℓ^k-rank equal to 0 for *any* prescribed finite set of prime powers ℓ^k. It suffices to take m in the following lemma divisible by the appropriate powers ℓ^{k+1}.

LEMMA 5.1. *Let $E/\mathbf{Q}$ be any elliptic curve, $m \in \mathbf{Z}_{>0}$ an integer, and*

$$K = Z_{E/\mathbf{Q}}(m) = \mathbf{Q}(E[m](\overline{\mathbf{Q}}))$$

the m-division field of E over $\mathbf{Q}$. Then E is an elliptic curve defined over K, and $T_{E/K}$ has ℓ^k-rank 0 for every prime power $\ell^k > 1$ for which ℓ^{k+1} divides m.

Proof. Suppose $\ell^{k+1} > \ell$ divides m. Then the full ℓ^{k+1}-torsion subgroup $E(\overline{K})[\ell^{k+1}]$ is contained in $E(K)$, so none of the torsion subgroups $T_{\mathfrak{p}}$ of the non-archimedean point groups $E(K_{\mathfrak{p}})$ in (7) will have a cyclic direct summand of order ℓ^k. As K contains an ℓ^{k+1}th root of unity, it has no real primes, so by the definition (9) the torsion closure $T_{E/K} = \prod_{\mathfrak{p}\leq\infty} T_{\mathfrak{p}}$ has ℓ^k-rank 0. ∎

In view of Lemma 5.1, a more interesting question is which non-generic adelic point groups can occur over a *given* number field K, such as $K = \mathbf{Q}$. To realize non-generic adelic point groups, we need elliptic curves E/K and primes ℓ for which the tower of ℓ-power division fields

$$Z_{E/K}(\ell) \subset Z_{E/K}(\ell^2) \subset Z_{E/K}(\ell^3) \subset \cdots \tag{19}$$

from (11) does *not* have strict inclusions at every level.

To ease notation, we write $G_{\ell^k} = \mathrm{Gal}(Z_{E/K}(\ell^k)/K)$ for the Galois group over K of the ℓ^k-division field, and $M_{\ell^k} = E[\ell^k](\overline{K})$ for the group of ℓ^k-torsion points of $E(\overline{K})$. As M_{ℓ^k} is free of rank 2 over $\mathbf{Z}/\ell^k\mathbf{Z}$ and G_{ℓ^k} acts faithfully on M_{ℓ^k}, we have an inclusion

$$G_{\ell^k} \subset \mathrm{Aut}(M_{\ell^k}) \cong \mathrm{GL}_2(\mathbf{Z}/\ell^k\mathbf{Z}), \tag{20}$$

and we can view $\lim\limits_{\leftarrow k} G_{\ell^k}$ as a subgroup of $\mathrm{Aut}(\lim\limits_{\rightarrow k} M_{\ell^k}) \cong \mathrm{GL}_2(\mathbf{Z}_\ell)$.

The Galois group of the $(k-1)$-st extension in the tower (19) is the ℓ-group arising as the kernel

$$K_{\ell^k} = \ker[G_{\ell^k} \to G_{\ell^{k-1}}] \quad (k \geq 2) \tag{21}$$

of the surjection induced by the restriction map

$$\varphi_{\ell^k} : \mathrm{Aut}(M_{\ell^k}) \to \mathrm{Aut}(M_{\ell^{k-1}}),$$

so we have

$$K_{\ell^{k+1}} = 1 \iff Z_{E/K}(\ell^k) = Z_{E/K}(\ell^{k+1}). \tag{22}$$

Triviality of the kernels $K_{\ell^{k+1}}$ needed to obtain non-generic point groups can only arise for a finite number of initial values of $k \geq 1$, with $\ell = 2$ playing a special role.

PROPOSITION 5.2. *Let ℓ be an odd prime, and suppose $K_{\ell^N} \neq 1$ for some $N \geq 2$. Then $K_{\ell^k} \neq 1$ for all $k > N$. For $\ell = 2$, the same is true if $N \geq 3$.*

Proof. Write $\sigma_N \in K_{\ell^N} \setminus \{1\}$ for $N \geq 2$ as $\sigma_N = 1 + \ell^{N-1}x$ with $x \neq \ell y \in \mathrm{End}(M_{\ell^N})$. If $\sigma_k \in G_{\ell^k}$ for $k > N$ maps to σ_N under the restriction map $G_{\ell^k} \twoheadrightarrow G_{\ell^N}$, we have $\sigma_k = 1 + \ell^{N-1}x_k$ with $x_k \neq \ell y_k \in \mathrm{End}(M_{\ell^k})$, and

$$\sigma_k^\ell = 1 + \ell^N x_k + \sum_{i=2}^{\ell} \binom{\ell}{i} \ell^{i(N-1)} x_k^i = 1 + \ell^N x_k \in \mathrm{End}(M_{\ell^k}). \tag{23}$$

Indeed, the number of factors ℓ in the coefficient $\binom{\ell}{i}\ell^{i(N-1)}$ is for $i = 2, 3, \ldots, \ell - 1$ at least $1 + 2(N-1) \geq N + 1$ if we have $N \geq 2$, and for $i = \ell$ in the final coefficient $\ell^{\ell(N-1)}$ it is $\ell(N-1) \geq N+1$ if we either have $\ell \geq 3$, $N \geq 2$ or $\ell = 2$, $N \geq 3$. Assuming we are in this situation, we see that σ_k^ℓ is in $K_{\ell^{N+1}} \setminus \{1\}$. Repeating the argument, we find that if σ_k is raised $k - N$ times to the power ℓ, we end up with an element $1 + \ell^{k-1}x_k \in K_{\ell^k} \setminus \{1\}$, showing $K_{\ell^k} \neq 1$. ∎

In view of Proposition 5.2, it makes sense to focus on the kernels K_{ℓ^2} and K_8 in (21).

PROPOSITION 5.3. *Suppose K is a number field linearly disjoint from the ℓ^2th cyclotomic field $\mathbf{Q}(\zeta_{\ell^2})$, with ℓ an odd prime. Then for all elliptic curves E/K, the tower* (19) *has strict inclusions at all levels.*

Proof. On account of Proposition 5.2, it suffices to show that $K_{\ell^2} = \ker[\pi : G_{\ell^2} \to G_\ell]$ is non-trivial for all elliptic curves E/K. By the hypothesis on K, the determinant map $G_{\ell^2} \xrightarrow{\det} (\mathbf{Z}/\ell^2\mathbf{Z})^*$ is surjective. As ℓ is odd, we can pick $c \in G_{\ell^2}$ such that $\det(c)$ generates $(\mathbf{Z}/\ell^2\mathbf{Z})^*$. Applying π, we find that $\det(\pi(c))$ generates $\mathbf{F}_\ell^* = (\mathbf{Z}/\ell\mathbf{Z})^*$.

Suppose that K_{ℓ^2} is trivial, making π an isomorphism. Then the order of $\pi(c)$ equals the order of c, which is divisible by the order $\ell(\ell-1)$ of $(\mathbf{Z}/\ell^2\mathbf{Z})^*$. Let $s \in G_\ell$ be a power of $\pi(c)$ of order ℓ. Then $s \in G_\ell \subset \mathrm{Aut}(M_\ell) \cong \mathrm{GL}_2(\mathbf{F}_\ell)$, when viewed as a 2×2-matrix over the field $\mathbf{F}_\ell$, is a non-semisimple matrix with double eigenvalue 1. As $\pi(c)$ centralizes this element, its eigenvalues cannot be distinct, and we find that $\det(\pi(c))$ is a square in $\mathbf{F}_\ell^*$, a contradiction. (This neat argument is due to Hendrik Lenstra.) ∎

We can now show that, in contrast to Lemma 5.1, there are only few ways in which adelic point groups of E/K can be non-generic if we fix the base field K.

THEOREM 5.4. *Let K be a number field. Then there exists a finite set Σ_K of powers of primes $\ell \mid 2 \cdot \mathrm{disc}(K)$ such that for every elliptic curve E/K and for every prime power $\ell^k \notin \Sigma_K$, the torsion closure $T_{E/K} \subset E(\mathbf{A}_K)$ has infinite ℓ^k-rank.*

Proof. Suppose there exists a prime power ℓ^k and an elliptic curve E/K for which T_E does not have infinite ℓ^k-rank. Then $K_{\ell^{k+1}} = 1$ in (22) for the associated tower (19). If ℓ is odd, K is not linearly disjoint from $\mathbf{Q}(\zeta_{\ell^2})$ by Proposition 5.3, so ℓ divides $\operatorname{disc}(K)$. This leaves us with finitely many possibilities for ℓ.

If ℓ is odd, we have $K_{\ell^N} = 1$ for $2 \le N \le k+1$ by Proposition 5.2, hence

$$Z_{E/K}(\ell^{k+1}) = Z_{E/K}(\ell). \tag{24}$$

As $Z_{E/K}(\ell^{k+1})$ contains a primitive ℓ^{k+1}st root of unity and $Z_{E/K}(\ell)$ is of degree at most $\#\operatorname{GL}_2(\mathbf{F}_\ell) < \ell^4$ over K, we can effectively bound k, say by $3 + \operatorname{ord}_\ell(n)$, for K of degree n. For $\ell^k = 2^k > 4$, the argument is similar, using $Z_{E/K}(2^{k+1}) = Z_{E/K}(4)$ instead of (24). ∎

The proof of Theorem 5.4 is constructive and yields a set Σ_K of prime powers ℓ^k, but it does not automatically yield the *minimal* set $\Sigma_K^{\min}$. By Lemma 5.1, the minimal set $\Sigma_K^{\min}$ for K can include any given set of prime powers if we take K sufficiently large. Finding $\Sigma_K^{\min}$ for any given K is however a non-trivial matter.

For $K = \mathbf{Q}$, one can take $\Sigma_{\mathbf{Q}}$ containing only powers of $\ell = 2$, and simple Galois theory shows that $\Sigma_{\mathbf{Q}} = \{2, 4, 8\}$ is actually large enough: no equality

$$Z_{E/\mathbf{Q}}(2^{k+1}) = Z_{E/\mathbf{Q}}(4)$$

can hold for $k \ge 4$, because $Z_{E/\mathbf{Q}}(2^{k+1})$ would then contain a cyclic subfield $\mathbf{Q}(\zeta_{32} + \zeta_{32}^{-1})$ of degree 8 over $\mathbf{Q}$, whereas $G_4 = \operatorname{Gal}(Z_{E/K}(4)/\mathbf{Q}) \subset \operatorname{GL}_2(\mathbf{Z}/4\mathbf{Z})$ has no elements of order divisible by 8. It is relatively easy to show that $\Sigma_{\mathbf{Q}}$ does contain 2, as there is the following classical construction of a family of elliptic curves $E/\mathbf{Q}$ for which $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4)$. See also [4, Theorem 1.7].

Proposition 5.5. *For every $r \in \mathbf{Q}^*$, the elliptic curve $E_r/\mathbf{Q}$ defined by the affine Weierstrass equation*

$$E_r : y^2 = x\big(x^2 - 2(1-4r^4)x + (1+4r^4)^2\big)$$

has division fields $Z_{E_r/\mathbf{Q}}(2) = Z_{E_r/\mathbf{Q}}(4) = \mathbf{Q}(i)$. Conversely, every elliptic curve $E/\mathbf{Q}$ with $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$ is $\mathbf{Q}$-isomorphic to E_r for some $r \in \mathbf{Q}^*$.

Proof. Let $E/\mathbf{Q}$ be defined by a Weierstrass equation $y^2 = f(x)$, and suppose that $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$. Then $f \in \mathbf{Q}[x]$ is a monic cubic polynomial with splitting field $Z_{E/\mathbf{Q}}(2) = \mathbf{Q}(i)$, so f has one rational root, and two complex conjugate roots in $\mathbf{Q}(i) \setminus \mathbf{Q}$. After translating x over the rational root, we may take 0 to be the rational root of f, leading to the model

$$E : f(x) = x(x-\alpha)(x-\overline{\alpha}) \tag{25}$$

for some $\alpha \in \mathbf{Q}(i) \setminus \mathbf{Q}$. Note that each such α does define an elliptic curve over $\mathbf{Q}$, and the $\mathbf{Q}$-isomorphism class of E depends on α up to conjugation and up to multiplication by the square of a non-zero rational number.

The equality $Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$ means that the 4-torsion of E is defined over $\mathbf{Q}(i)$, or equivalently the 2-torsion subgroup $E[2](\mathbf{Q}(i))$ of E is contained in $2 \cdot E(\mathbf{Q}(i))$. In terms of the complete 2-descent map [9, Proposition 1.4, p. 315] over $K = \mathbf{Q}(i)$, which embeds $E(K)/2E(K)$ in a subgroup of $K^*/(K^*)^2 \times K^*/(K^*)^2$, the inclusion $E[2](\mathbf{Q}(i)) \subset 2 \cdot E(\mathbf{Q}(i))$ amounts to the statement that all differences between the roots of f are squares in $\mathbf{Q}(i)$. In other words, we have $Z_{E/\mathbf{Q}}(2) = Z_{E/\mathbf{Q}}(4) = \mathbf{Q}(i)$ if and only if α and $\alpha - \overline{\alpha}$ are squares in $\mathbf{Q}(i)$.

Writing $\alpha = (a+bi)^2$ with $ab \neq 0$, we can scale $a+bi$ inside the $\mathbf{Q}$-isomorphism class of E by an element of $\mathbf{Q}^*$, and flip signs of a and b. Thus we may take $\alpha = (1+qi)^2$, with q a positive rational number. The fact that $\alpha - \overline{\alpha} = 4qi = (q/2)(2+2i)^2$ is a square in $\mathbf{Q}(i)$ implies that $q/2 = r^2$ for some $r \in \mathbf{Q}^*$. Substituting $\alpha = (1+2ir^2)^2$ in the model (25), we find that E is $\mathbf{Q}$-isomorphic to

$$E_r : y^2 = x\big(x^2 - 2(1-4r^4)x + (1+4r^4)^2\big). \tag{26}$$

As we have shown that E_r has $Z_{E_r/\mathbf{Q}}(2) = Z_{E_r/\mathbf{Q}}(4) = \mathbf{Q}(i)$, this proves the proposition. ∎

As the j-invariant $j(E_r)$ of the elliptic curve given by (26) is a non-constant function of r, the family $\{E_r/\mathbf{Q}\}_{r\in\mathbf{Q}^*}$ is non-isotrivial, and represents infinitely many distinct isomorphism classes over $\overline{\mathbf{Q}}$. This yields the following explicit version of Theorem 1.2.

THEOREM 5.6. *Let E_r be as above, and K be a number field of degree n. Then all elliptic curves E_r/K with $r \in \mathbf{Q}^*$ have adelic point groups $E_r(\mathbf{A}_K)$ that are not isomorphic to the topological group $\mathcal{E}_n$.*

Proof. We show that for any $r \in \mathbf{Q}^*$, the torsion closure $T_{E_r/K} = \prod_\mathfrak{p} T_\mathfrak{p}$ from (8) has 2-rank equal to 0. As $T_{E_r/K}$ is intrinsically defined as the closure of the torsion subgroup of $E_r(\mathbf{A}_K)/E_{r,\mathrm{cc}}(\mathbf{A}_K)$, this implies that $E_r(\mathbf{A}_K)$ is not isomorphic to $\mathcal{E}_n$.

As E_r has by construction a non-complete 2-torsion subgroup $E(\mathbf{R})[2] = \langle(0,0)\rangle$ over the unique archimedean completion $\mathbf{R}$ of $\mathbf{Q}$, its discriminant $\Delta(E_r)$ is a negative rational number. By the definition (9), we therefore have $T_\mathfrak{p} = 1$ for all infinite primes $\mathfrak{p}$ of K.

For $\mathfrak{p}$ a finite prime of K, there are two cases. If $K_\mathfrak{p}$ contains i, and therefore $Z_{E_r/K}(4) = K(i)$, the complete 4-torsion of E_r is $K_\mathfrak{p}$-rational, and $E_r(K_\mathfrak{p})$ has no direct summand of order 2. In the other case, where $K_\mathfrak{p}$ does not contain i, we have $E(K_\mathfrak{p})[2] = \langle(0,0)\rangle$. As all 4-torsion points of E_r are $K_\mathfrak{p}(i)$-rational, we can pick a point $P \in E_r(K_\mathfrak{p}(i))$ of order 4 for which $2P$ is a 2-torsion point $T \in E_r(K_\mathfrak{p}(i))$ that is *not* $K_\mathfrak{p}$-rational. Write σ for the non-trivial automorphism of $K_\mathfrak{p} \subset K_\mathfrak{p}(i)$. Then the point $Q = P + P^\sigma \in E_r[4](K_\mathfrak{p}(i))$ is $K_\mathfrak{p}$-rational and satisfies $2Q = T + T^\sigma = (0,0)$. It follows that $E(K_\mathfrak{p})[4] = \langle Q\rangle \cong \mathbf{Z}/4\mathbf{Z}$ has no direct summand of order 2, and the same is then true for $E(K_\mathfrak{p})$. This shows that no $T_\mathfrak{p}$ has a direct summand of order 2, and completes the proof. ∎

REMARK 5.7. It follows from the tables of Rouse and Zureick-Brown [7] and [4, Proposition 3.8] that for *all* elliptic curves $E/\mathbf{Q}$, the inclusion $Z_{E/\mathbf{Q}}(4) \subset Z_{E/\mathbf{Q}}(8)$ is strict, and therefore, by Proposition 5.2, for such E we have $K_{2^{k+1}} \neq 1$ in (22) for all $k \geq 2$. This implies that for $K = \mathbf{Q}$,

$$\Sigma_{\mathbf{Q}}^{\min} = \{2\}$$

is the minimal set of prime powers in Theorem 5.4.

REMARK 5.8. Both in Lemma 5.1 and in Theorem 5.6, the only value of the ℓ^k-rank of $T_{E/K}$ different from the generic value $e(\ell^k) = \omega$ is $e(\ell^k) = 0$. This is no coincidence, as there is the purely algebraic fact that if a group G acts on a free module M of rank 2 over $\mathbf{Z}/\ell^{k+1}\mathbf{Z}$ in such a way that the module of invariants M^G has a direct summand of order ℓ^k, then there exists an element $g \in G$ such that $M^{\langle g\rangle}$ has a cyclic direct summand of order ℓ^k. Thus, if E/K is an elliptic curve for which $T_\mathfrak{p} \subset T_{E/K}$ has a cyclic direct summand of order ℓ^k for a *single* finite prime $\mathfrak{p}$, then we are in the situation above, with $G \subset G_{\ell^{k+1}}$ the decomposition group of $\mathfrak{p}$ acting on $M = M_{\ell^{k+1}}$ as in (20). It then follows that for the infinitely many primes $\mathfrak{p}$ of K that are unramified in $K \subset Z_{E/K}(\ell^{k+1})$ with Frobenius element in $G_{\ell^{k+1}}$ conjugate to the element $g \in G$ above, $T_\mathfrak{p}$ also has a cyclic direct summand of order ℓ^k, leading to the implication

$$e(\ell^k) \neq 0 \implies e(\ell^k) = \omega$$

for the ℓ^k-ranks of $T_{E/K}$.

References

[1] A. Angelakis, *Universal adelic groups for imaginary quadratic number fields and elliptic curves*, PhD thesis, Leiden Universiteit & Université de Bordeaux, 2015; https://open-access.leidenuniv.nl/handle/1887/34990.

[2] A. Angelakis and P. Stevenhagen, *Imaginary quadratic fields with isomorphic abelian Galois groups*, in: ANTS X—Proc. Tenth Algorithmic Number Theory Sympos., Open Book Ser. 1, Math. Sci. Publ., Berkeley, CA, 2013, 21–39.

[3] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic Number Theory*, Academic Press, London, 1967.

[4] H. B. Daniels and Á. Lozano-Robledo, *Coincidences of division fields*, arXiv:1912.05618 (2019).

[5] N. Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. 362 (2010), 1547–1570.

[6] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields*, 2nd ed., Grundlehren Math. Wiss. 323, Springer, Berlin, 2008.

[7] J. Rouse and D. Zureick-Brown, *Elliptic curves over* $\mathbb{Q}$ *and 2-adic images of Galois*, Res. Number Theory 1 (2015), art. 12, 34 pp.

[8] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.

[9] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, Dordrecht, 2009.

[10] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. London Math. Soc. 42 (2010), 811–826.

Athanasios Angelakis
Department of Mathematics
National Technical University of Athens
9 Iroon Polytexneiou St.
15780 Zografou, Attiki, Greece
E-mail: ath.angelakis@gmail.com

Peter Stevenhagen
Mathematisch Instituut
Leiden Universiteit
Postbus 9512
2300 RA Leiden, The Netherlands
E-mail: psh@math.leidenuniv.nl