PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 1, *Number* 1, *March* 2016, *pages* 7–15

Peter Stevenhagen

Adelic points of elliptic curves

written by Athanasios Angelakis

1 Introduction

In the first part of his thesis [1], Angelakis studies absolute abelian Galois groups $A_K = \mathrm{Gal}(K^{\mathrm{ab}}/K)$ of number fields K using class field theory. It was already known that for imaginary quadratic number fields K, K' we can have $A_K \cong A_{K'}$, as topological groups, even if K and K' are *not* isomorphic as number fields (Onabe, 1976). Angelakis' striking and very explicit result is the following;

Theorem 1.1 *There exist "many" imaginary quadratic number fields K having*

$$A_K \cong U \stackrel{\mathrm{def}}{=} \widehat{\mathbb{Z}}^2 \times \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z},$$

as topological groups.

In order to make more precise what "many" means, data can be taken from Watkins' table. For example, the imaginary quadratic number fields K having prime class number lower than 100. From these 2356 number fields, 2291 have absolute abelian Galois group A_K isomorphic to U. Numerically, it seems that an imaginary quadratic number field K of class number p has $A_K \cong U$ with probability $1 - \frac{1}{p}$. This observation leads to:

Conjecture 1.2 *100% of all imaginary quadratic number fields K of prime class number have $A_K \cong U$.*

Not much can be proven here, as distribution results both for the occurrence of prime class numbers and for the average splitting behavior in the analysis of A_K, are lacking. However the same techniques can be applied to a different problem that, although at first sight more complicated, does yield proven theorems.

2 Elliptic curves over K

In class field theory, Galois groups arise as quotients of the multiplicative group $\mathbb{A}_K^*$ of K-ideles. Here the interest lies in the adelic point group $E(\mathbb{A}_K)$ of an elliptic curve E defined over a number field K. The distribution of $E(K)$ as finitely generated abelian group is a very hard problem, even over $\mathbb{Q}$.

Even though $\mathbb{A}_K = \prod_{\mathfrak{p}}' K_{\mathfrak{p}}$ is a *restricted* product of all completions $K_{\mathfrak{p}}$ of K, the adelic point group of an elliptic curve E/K equals

$$E(\mathbb{A}_K) = \prod_{\mathfrak{p}} E(K_{\mathfrak{p}}).$$

For "large" $\mathfrak{p}$ there are many different possibilities for the $\mathfrak{p}$-adic group $E(K_{\mathfrak{p}})$. Still, the product is surprisingly rigid:

Theorem 2.1 *Let K be a number field of degree n. Then for 'almost all' elliptic curves E/K, the adelic point group $E(\mathbb{A}_K)$ is topologically isomorphic to the universal group*

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

associated to the degree n of K.

Based on the counting of integral Weierstrass models as in [4], the notion of 'almost all' in this theorem is the following one: for elements a and b in the ring of integers O_K of K satisfying $\Delta(a,b) = -16(4a^3 + 27b^2) \neq 0$, we write $E(a,b)$ for the elliptic curve defined by the affine Weierstrass equation $y^2 = x^3 + ax + b$. Now fix a norm $||.||$ on $\mathbb{R} \otimes_{\mathbb{Z}} O_K^2 \cong \mathbb{R}^{2[K:\mathbb{Q}]}$. Then for any positive real number X, the set B_X of elliptic curves $E(a,b)$ with $||(a,b)|| < X$ is finite. We say that *almost all* elliptic curves over K have some property, if the fraction of elliptic curves $E(a,b)$ in B_X having that property tends to 1 when $X \in \mathbb{R}_{>0}$ tends to infinity.

Our notion of 'almost all' still allows for large numbers of elliptic curves E/K to have adelic point groups different from the universal group in Theorem 2.1, as the following theorem states.

Theorem 2.2 *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 $E(\mathbb{A}_K)$ is a topological group not isomorphic to $\mathcal{E}_n$.*

The adele ring of K naturally decomposes as a product $\mathbb{A}_K = \mathbb{A}_K^{\infty} \times \mathbb{A}_K^{\mathrm{fin}}$, in which $\mathbb{A}_K^{\infty}$ is the product of the archimedean completions of K, and the *ring of finite K-adeles* $\mathbb{A}_K^{\mathrm{fin}} = \prod_{\mathfrak{p}}' K_{\mathfrak{p}}$ is the restricted product (in the sense explained above) of the non-archimedean completions of K. The adelic point group of an elliptic curve E/K decomposes correspondingly as a product

$$E(\mathbb{A}_K) = E(\mathbb{A}_K^{\infty}) \times E(\mathbb{A}_K^{\mathrm{fin}}). \tag{1}$$

The best strategy is to deal with these factors separately.

3 The Structure of $E(\mathbb{A}_K)$

Every completion of K at an infinite prime $\mathfrak{p}$ of K is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$, depending on whether $\mathfrak{p}$ is real or complex. For $\mathfrak{p}$ complex

and E/K an elliptic curve, $E(K_\mathfrak{p})$ is a topological group isomorphic to $(\mathbb{R}/\mathbb{Z})^2$, by the well-known fact that we have $E(K_\mathfrak{p}) \cong \mathbb{C}/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}$ by the complex analytic theory.

For $\mathfrak{p}$ real and E/K an elliptic curve, there are two possible types of groups $E(K_\mathfrak{p})$, and they may be distinguished by looking at the discriminant Δ_E of the elliptic curve. The *sign* of $\Delta(E)$ is well-defined for every real prime $\mathfrak{p} : K \to \mathbb{R}$ of K, and for such $\mathfrak{p}$ we have

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

The following is easily proved

Proposition 3.1 *Let K be a number field of degree n, and E/K an elliptic curve with discriminant $\Delta_E \in K^*/(K^*)^{12}$. Then there exists an isomorphism of topological groups*

$$E(\mathbb{A}_K^\infty) \cong (\mathbb{Z}/2\mathbb{Z})^r \times (\mathbb{R}/\mathbb{Z})^n. \tag{3}$$

Here $r \leq n$ is the number of real primes $\mathfrak{p}$ of K for which we have $\Delta(E) >_\mathfrak{p} 0$.

Let $\mathfrak{p}|p$ be a finite prime of a number field K, and E an elliptic curve defined over K. In explicit terms, E can be given by a minimal Weierstrass equation with coefficients in $O_\mathfrak{p}$. In this way a continuous reduction map $\phi_\mathfrak{p} : E(K_\mathfrak{p}) \longrightarrow \overline{E}(k_\mathfrak{p})$, from $E(K_\mathfrak{p})$ to the finite set of points of the curve $\overline{E}$ described by the reduced Weierstrass equation over the residue class field $k_\mathfrak{p} = O/\mathfrak{p}$, is obtained. The set of points in the non-singular locus $\overline{E}^{\mathrm{ns}}(k_\mathfrak{p})$ of $\overline{E}$ is contained in the image of ϕ, by Hensel's lemma, and it inherits a natural group structure from $E(K_\mathfrak{p})$. Writing $E_0(K_\mathfrak{p}) = \phi^{-1}[\overline{E}^{\mathrm{ns}}(k_\mathfrak{p})]$, yields the exact sequence of topological groups

$$1 \to E_1(K_\mathfrak{p}) \longrightarrow E_0(K_\mathfrak{p}) \longrightarrow \overline{E}^{\mathrm{ns}}(k_\mathfrak{p}) \to 1. \tag{4}$$

The kernel of reduction $E_1(K_\mathfrak{p})$ is a subgroup of finite index in $E(K_\mathfrak{p})$.

For primes of good reduction, we have $E_0(K_\mathfrak{p}) = E(K_\mathfrak{p})$, and $\overline{E}^{\mathrm{ns}}(k_\mathfrak{p}) = \overline{E}(k_\mathfrak{p})$ is the point group of the elliptic curve $\overline{E} = (E \bmod \mathfrak{p})$ over $k_\mathfrak{p}$. For primes of bad reduction, $E_0(K_\mathfrak{p})$ is a strict subgroup of $E(K_\mathfrak{p})$, but it is of *finite* index in $E(K_\mathfrak{p})$ by [3, Chapter VII, Corollary 6.2.]

Lemma 3.2 *Let $T_\mathfrak{p}$ be the torsion subgroup of $E(K_\mathfrak{p})$. Then $T_\mathfrak{p}$ is a finite group, and $E(K_\mathfrak{p})/T_\mathfrak{p}$ is a free $\mathbb{Z}_p$-module of rank $[K_\mathfrak{p} : \mathbb{Q}_p]$.*

If $\mathfrak{p}$ is a prime of good reduction for E, then there exist an isomorphism

$$T_\mathfrak{p}^{non\text{-}p} \cong \overline{E}(k_\mathfrak{p})^{non\text{-}p}$$

between the maximal subgroups of $T_\mathfrak{p}$ and $\overline{E}(k_\mathfrak{p})$ that are of order coprime to $p = \mathrm{char}(k_\mathfrak{p})$.

Taking the product over all non-archimedean primes $\mathfrak{p}$ of K, and using the fact that the sum of the local degrees at the primes over p in K equals $[K : \mathbb{Q}]$, one gets the following.

Lemma 3.3 *For the group of adelic points of an elliptic curve E over a number field K, there is an isomorphism of topological groups*

$$E(\widehat{K}) = \widehat{\mathbb{Z}}^{[K:\mathbb{Q}]} \times \prod_{\mathfrak{p}} T_\mathfrak{p}, \tag{5}$$

with $T_\mathfrak{p} \subset E(K_\mathfrak{p})$ the finite torsion subgroup of $E(K_\mathfrak{p})$.

In order to describe *any* countable product T of cyclic groups, one can write each of the cyclic constituents of T as a product of cyclic groups of prime power order to arrive at the *standard representation*

$$T \cong \prod_{\ell \text{ prime}} \prod_{k=1}^{\infty} (\mathbb{Z}/\ell^k\mathbb{Z})^{e(\ell,k)}. \tag{6}$$

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

$$e(\ell, k) = \dim_{\mathbb{F}_\ell} T[\ell^k]/\left(T[\ell^{k-1}] + \ell T[\ell^{k+1}]\right), \tag{7}$$

so any two groups written in this standard representation (6) are isomorphic if and only if their exponents $e(\ell, k)$ coincide for all prime powers ℓ^k.

The $\mathbb{F}_\ell$-dimensions $e(\ell, k)$ in (7) are either finite, in which case $e(\ell, k)$ is a non-negative integer, or countably infinite. In the latter case write $e(\ell, k) = \omega$. In the case where $e(\ell, k) = \omega$ for *all* prime powers ℓ^k, the group under consideration is

$$T_E = \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z} \tag{8}$$

occurring in Theorem 2.1.

For the product $T = \prod_{\mathfrak{p}} T_{\mathfrak{p}}$ of local torsion groups at the finite primes $\mathfrak{p}$ that occurs in Lemma 3.3, the exponents $e(\ell, k)$, for the number of cyclic summands of prime power order in the standard representation (6) of T_E, have to be determined.

In the analogous situation of the closure T_K of the torsion subgroup of $\widehat{O}^*$ in [2, Section 2.3] that one had $e(\ell, k) = \omega$ for all but finitely many prime powers ℓ^k, and the 'missing' prime powers were characterized in terms of the number of exceptional roots of unity in K. In the elliptic situation, the cyclotomic extension of K generated by the ℓ^k-th roots of unity will be replaced by the ℓ^k-division field

$$Z_E(\ell^k) \stackrel{\text{def}}{=} K(E[\ell^k](\overline{K})) \tag{9}$$

of the elliptic curve E. This is the finite Galois extension of K obtained by adjoining the coordinates of all ℓ^k-torsion points of E to K. More precisely, the following holds:

Lemma 3.4 *Let E/K be an elliptic curve, and $\ell^k > 1$ a prime power for which the inclusion*

$$Z_E(\ell^k) \subset Z_E(\ell^{k+1})$$

of division fields is strict. Then $e(\ell, k) = \omega$ in the standard representation (6) *of the group T.*

It follows from Lemmas 3.3 and 3.4 that for elliptic curves E having the property that for all primes ℓ, the tower of ℓ-power division fields has strict inclusions

$$Z_E(\ell) \subsetneq Z_E(\ell^2) \subsetneq Z_E(\ell^3) \subsetneq \cdots \subsetneq Z_E(\ell^k) \subsetneq \cdots \tag{10}$$

at every level, the group T_E is the universal group $\prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}$ for which $e(\ell, k) = \omega$ in the standard representation (6).

The structure of $E(\mathbf{A}_K)$ is determined by the Galois representation

$$\rho_E : \mathrm{Gal}(\overline{K}/K) \longrightarrow A = \mathrm{Aut}(E(\overline{K})^{\mathrm{tor}})$$

describing the action of the absolute Galois group of K by group automorphisms on the group $E(\overline{K})^{\mathrm{tor}}$ of all torsion points of E. The group A can be explicitly describe as

$$A = \mathrm{Aut}(E(\overline{K})^{\mathrm{tor}}) \cong \lim_{\leftarrow n} \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) = \mathrm{GL}_2(\widehat{\mathbb{Z}}),$$

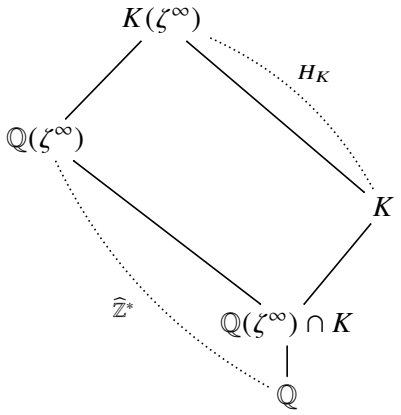
and ρ_E is a continuous homomorphism of profinite groups. The *image of Galois* for the representation ρ_E is the subgroup

$$G = \rho_E[\mathrm{Gal}(\overline{K}/K)] \subset A.$$

For $K = \mathbb{Q}$, Angelakis in [1, Section 4.4] uses a result of Nathan Jones to show that 'almost always' one has $E(\mathbb{A}_{\mathbb{Q}}) = \mathcal{E}$.

For $K \neq \mathbb{Q}$ using that $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \xrightarrow{\det} \widehat{\mathbb{Z}}^*$ and denoting by H_K the Galois group $\mathrm{Gal}(K(\zeta^{\infty})/K)$ (see the figure below), it follows that the image $G \subset \det^{-1}[\mathrm{H_K}]$; this time, one can use the result of Zywina [4] to get that 'almost always' the image $G = \det^{-1}[\mathrm{H_K}]$, which implies that for every prime power $\ell^k > 1$ the inclusion $Z_E(\ell^k) \subset Z_E(\ell^{k+1})$ is strict. From Lemma 3.4 one gets that $e(\ell, k) = \omega$ for T in the standard representation (6). So putting (1), (3), (5) and (8) together, the group $E(\mathbb{A}_K)$ of adelic points of 'almost all' elliptic curves E/K, with n the degree of K, is isomorphic to the "generic group"

$$\mathcal{E} = (\mathbb{R}/\mathbb{Z})^n \times (\widehat{\mathbb{Z}})^n \times \prod_{m=1}^{\infty} \mathbb{Z}/m\mathbb{Z}. \tag{11}$$



References

[1] A. Angelakis, *Universal adelic groups for imaginary quadratic number fields and elliptic curves*, Leiden University & Université Bordeaux I, Doctoral Thesis, Leiden (2015)

[2] A. Angelakis, P. Stevenhagen, *Imaginary quadratic fields with isomorphic abelian Galois groups*, in *ANTS X - Proceedings of the Tenth Algorithmic Number Theory Symposium*, eds. Everett W. Howe and Kiran S. Kedlaya, The Open Book Series Vol 1, (2103) Mathematical Sciences Publisher, Berkeley, pp. 21-39.

[3] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics vol. 106, Second Edition 2009, Springer, Dordrecht.

[4] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), pp. 811-826

Athanasios Angelakis
Max Planck Institut für Mathematik
Vivatsgasse 7
53111 Bonn, Germany
email: math.angelakis@gmail.com