Contemporary Mathematics

Abelian Varieties and Finitely Generated Galois Groups

Bo-Hae Im and Michael Larsen

Abstract. This paper surveys the methods that have been used to attack the conjecture, still open, that an abelian variety over a characteristic 0 field with finitely generated Galois group is always of infinite rank.

To Gerhard Frey on the occasion of his 75th birthday

1. Introduction

Let K be a field finitely generated over $\mathbb{Q}$. By Néron's extension [**Ln**, Chapter 6, Theorem 1] of the Mordell-Weil theorem, for every abelian variety A/K, the group $A(K)$ is finitely generated.

We say a field K is *anti-Mordell-Weil* (AMW) if for every non-trivial abelian variety A/K, the group $A(K)$ is of infinite rank.

In 1974, Frey and Jarden [**FyJ**] proved the following theorem:

Theorem 1. *If K is finitely generated over $\mathbb{Q}$ and n is a positive integer, the set of $\boldsymbol{\sigma} := (\sigma_1, \dots, \sigma_n) \in G_K^n$ such that $\bar{K}(\boldsymbol{\sigma})$ is AMW is of Haar measure* 1.

Here $G_K := \mathrm{Gal}(\bar{K}/K)$, and $\bar{K}(\boldsymbol{\sigma})$ denotes the fixed field of $\bar{K}$ under $\langle \boldsymbol{\sigma} \rangle := \langle \sigma_1, \dots, \sigma_n \rangle$. Note that $\langle \sigma_1, \dots, \sigma_n \rangle$ denotes the closure of the subgroup of G_K generated by the σ_i; a closed subgroup of G_K is understood to be *finitely generated* if it is of this form.

In [**Lr**], one of us conjectured that more is true: that in fact $\bar{K}(\boldsymbol{\sigma})$ is AMW for all $\boldsymbol{\sigma}$. This conjecture remains open. In this paper, we will present several different approaches to the problem, review what is known, and discuss some variants and related open problems.

This conjecture can be reformulated as follows:

Bo-Hae Im was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Science, ICT & Future Planning(NRF-2017R1A2B4002619).

Michael Larsen was partially supported by NSF grant DMS-1702152.

CONJECTURE 1. *Every characteristic* 0 *field with finite transcendence degree and finitely generated absolute Galois group is AMW.*

Indeed, $\bar{K}(\boldsymbol{\sigma})$ has a finitely generated Galois group, and every characteristic 0 field with finite transcendence degree and finitely generated absolute Galois group can be written in this form.

This implies the following, apparently stronger, statement:

CONJECTURE 2. *Every characteristic* 0 *field with finitely generated absolute Galois group is AMW.*

Indeed, let K be any characteristic 0 field and $K' := \bar{K}(\boldsymbol{\sigma})$ an algebraic extension of K with a finitely generated absolute Galois group. Any abelian variety over K' is obtained by extension of scalars from an abelian variety over a finitely generated subfield $k \subset K'$. Let k' and $\bar{k}$ denote the algebraic closure of k in K' and $\bar{K}$ respectively. Then $\bar{k}$ is an algebraic closure of k', and there is a natural continuous homomorphism $\pi\colon G_{K'} \to G_{k'}$. As $\bar{k}$ is linearly disjoint with K' over k' and algebraic over k', we have $K' \otimes_{k'} \bar{k} \cong K'\bar{k}$ is a subfield of $\bar{K}$, and every k'-automorphism of $\bar{k}$ extends uniquely to an automorphism of $K'\bar{k}$ which is trivial on K' and thus to an automorphism of $\bar{K}$ which is trivial on K'. We conclude that π is surjective, so $G_{k'}$ is finitely generated. Thus Conjecture 1 for k' implies Conjecture 2.

The following special case of Conjecture 1 remains open, even in the case that $K = \mathbb{Q}$ and A is an elliptic curve:

CONJECTURE 3. *Let A be an abelian variety over a number field K. Then the rank of A is infinite over $\bar{K}(\boldsymbol{\sigma})$ for all $\boldsymbol{\sigma}$.*

There is also a characteristic p version, but some care is needed because a subfield of $\bar{\mathbb{F}}_p$ cannot be AMW because every point in $A(\bar{\mathbb{F}}_p)$ lies in the finite group $A(\mathbb{F}_q)$ for some q and is therefore of finite order. For characteristic p fields, one can define a field K to be AMW if every abelian variety A/K *which is not isotrivial* has infinite rank over K. There are no such abelian varieties over subfields of $\bar{\mathbb{F}}_p$, so the condition is vacuous, and we can formulate:

CONJECTURE 4. *Every field with finitely generated absolute Galois group is AMW.*

Here the absolute Galois group of a field K means $\mathrm{Gal}(\bar{K}/K)$, where $\bar{K}$ is a *separable* closure of K.

The purpose of this paper is to survey what is known about these conjectures and related questions. The emphasis will be on the wide variety of different methods which have been brought to bear, with varying degrees of success, on special cases.

We would like to thank Moshe Jarden for his comments on an earlier version of this paper.

2. Probabilistic Methods

Throughout this paper, a *variety* will be a separated, geometrically reduced scheme over a field; it need not be connected. A *curve* is a variety of dimension 1.

We recall that a field K is *PAC* if every geometrically irreducible variety V over K has a K-point. This implies that $V(K)$ is dense in V. We say K is *ample* (the terms *large* and *anti-mordellic* also appear in the literature) if every non-singular curve has either no K-points or infinitely many. Any K-point on a curve which is irreducible over K but not over some algebraic extension of K must lie in at least two geometric components and therefore must be a singular point. In other words, a K-point on any non-singular curve must lie on a geometrically connected irreducible component of that curve. Thus PAC implies ample.

The "PAC Nullstellensatz" [**FdJ**, Theorem 18.6] asserts that if K is a countable field satisfying the Hilbert irreducibility theorem (e.g., any global field [**Ln**, Chapter 9, Theorem 4.2]), then with probability 1, $\bar{K}(\boldsymbol{\sigma})$ is PAC. It follows that $\bar{K}(\boldsymbol{\sigma})$ is ample. Markus Junker and Jochen Koenigsmann [**JK**], made the following conjecture:

Conjecture 5. *Every infinite field with finitely generated absolute Galois group is ample.*

Arno Fehm and Sebastian Petersen proved [**FP**, Theorem 2.6(a)] that, at least in characteristic 0, every ample field is AMW. This shows that Conjecture 5 implies Conjecture 2 and also gives a new proof of Theorem 1.

The same approach can be used to give a probabilistic analysis of Galois representations coming from the non-torsion part of a non-trivial abelian variety A over a field K finitely generated over $\mathbb{Q}$. Let $V_A := A(\bar{K}) \otimes \mathbb{Q}$, regarded as a space with discrete topology, and consider the representation $\rho_A \colon G_K \to \operatorname{Aut}_{\mathbb{Q}} V_A$. This representation is continuous since

$$V_A := \sum_L A(L) \otimes \mathbb{Q} = \bigcup_L A(L) \otimes \mathbb{Q},$$

where the union (or sum) is taken over all of the (countably many) finite Galois extensions L/K. By Néron's theorem, each summand $A(L) \otimes \mathbb{Q}$ is finite-dimensional.

Every ordered n-tuple $\boldsymbol{\sigma} \in G_K^n$ defines a homomorphism $e_{\boldsymbol{\sigma}} \colon F_n \to G_K$, where F_n is the free group on n generators. The composition $\rho_A \circ e_{\boldsymbol{\sigma}}$ is then a countable sum of finite dimensional $\mathbb{Q}$-representations of F_n, each of which factors through a finite quotient of F_n. It is therefore a direct sum of irreducible $\mathbb{Q}$-representations of F_n which factor through finite quotients. We call such an irreducible representation an *atom*.

By the *generic representation* of F_n we mean the direct sum of a countably infinite number of copies of every atom. Thus, $\rho_A \circ e_{\boldsymbol{\sigma}}$ is always a subrepresentation of the generic representation of F_n.

THEOREM 2. *If K is finitely generated over $\mathbb{Q}$ and n is a positive integer, the set of $\boldsymbol{\sigma} \in G_K^n$ for which the G_K-representation $\rho_A \circ e_{\boldsymbol{\sigma}}$ is generic for all non-trivial A/K has measure* 1.

Note that the space of $G_{\bar{K}(\boldsymbol{\sigma})}$-invariants of V_A is exactly $A(\bar{K}(\boldsymbol{\sigma})) \otimes \mathbb{Q}$, so the infinite multiplicity of the trivial atom in $\rho_A \circ e_{\boldsymbol{\sigma}}$ is equivalent to the infinite rank of A over $\bar{K}(\boldsymbol{\sigma})$.

PROOF. Since there are countably many isomorphism classes of abelian varieties over K, it suffices to prove the statement for a single one. Likewise, it suffices to prove that each atom has infinite multiplicity in V_A with probability 1. We therefore fix an atom $\alpha\colon F_n \to \mathrm{GL}(W)$ which factors through some finite quotient G of F_n (so that W is the representation space of an irreducible rational representation). In particular, G is generated by some n-element subset.

We fix an embedding $\iota\colon G \hookrightarrow \mathsf{A}_N$, $N \geq 4$, such that the restriction of the (unique) irreducible $N-1$-dimensional $\mathbb{Q}$-representation of A_N to G contains W as a subrepresentation. This is possible for all $N \geq |G| + 2$, by composing the regular permutation representation of G with an embedding $S_{|G|} \hookrightarrow \mathsf{A}_N$. Note that S_m embeds in A_N for all $N \geq m + 2 \geq 3$, and the permutation representation of S_m is a subrepresentation of the restriction of the irreducible $N-1$-dimensional representation of A_N.

Since the K-points in any projective space are Zariski-dense, Bertini's theorem implies that there exists a non-singular curve X on A defined over K and passing through the identity 0. Let g be the genus of X. Since there are no rational curves on an abelian variety, we have $g \geq 1$. We fix a non-empty G_K-stable finite subset S of points in $X(\bar{K}) \smallsetminus \{0\}$.

For any $N \geq 2g+2|S|$, we consider the space of meromorphic functions f on X which vanish to order ≥ 2 on every point of S, which are holomorphic except at 0, and which have a pole of order $\leq N$ at 0. By the Riemann-Roch theorem, the projective space of such functions has dimension $N - 2|S| - g$; imposing the condition that $\mathrm{ord}_0 f \geq 1 - N$ or the condition that $\mathrm{ord}_s f \geq 3$ for any specified $s \in S$ defines a projective subspace of codimension 1, while imposing the condition that $\mathrm{ord}_t f \geq 2$ for some $t \in X \smallsetminus (S \cup \{0\})$ defines a projective subspace of codimension 2. The union over t of these codimension 2 subspaces is therefore a subvariety of codimension 1.

It follows that there is a dense open subvariety of functions f on X which have a pole of exact order N at 0, no other poles, zeroes of exact order 2 at each point in S, and no other multiple zeroes. As K-points are Zariski dense in projective space, we can take f to be defined over K. Thus, f defines a morphism $X \to \mathbb{P}^1$ of degree N, which gives a degree N extension of function fields $K(X)/K(\mathbb{P}^1)$.

The Galois group H of the minimal Galois extension of $K(\mathbb{P}^1)$ containing $K(X)$ is a permutation group of degree N, defined up to conjugation. Local monodromy considerations at ∞ and 0 show that H contains an N-cycle and an element of order 2 with $|S|$ 2-cycles (and therefore at least 2 fixed

points, as $N \geq 2|S| + 2$.) If N is prime and sufficiently large, H cannot therefore be contained in the group of affine transformations on the field with N elements. If, in addition, $N > 23$ and N is not of the form $\frac{q^m-1}{q-1}$ for any prime power q and integer $m \geq 2$, then H must contain A_N [**Fe**, Theorem 4.2]. We conclude that there exists an n-tuple $(h_1, \ldots, h_n) \in H^n$ such that

$$\langle h_1, \ldots, h_n \rangle = \iota(G).$$

There is no difficulty choosing an arbitrarily large prime that is not of the form $\frac{q^m-1}{q-1}$. For the latter expression to be prime, either q must be a power of 2, or m must be odd. The number of expressions of the form $\frac{2^{km}-1}{2^k-1}$ less than M is $O(\log^2 M)$; the number of expressions $1 + q + \cdots + q^{2k} < M$ where k is a fixed positive integer and $q \geq 2$ is variable is less than $M^{1/2k} - 1$, so the number if k is allowed to vary is $O(M^{1/2})$, while the number of primes $< M$ grows like $M/\log M$. So we may fix a prime N with $\mathsf{A}_N \subset H \subset S_N$.

Suppose $c \in K \subset \mathbb{P}^1(K)$ such that the kernel G_L of the action of G_K on the N-element set $f^{-1}(c)$ satisfies $G_K/G_L \cong H$. Defining

$$V_c := \operatorname{Span}_{\mathbb{Q}} f^{-1}(c) \subset A(L) \otimes \mathbb{Q},$$

the action of $\operatorname{Gal}(L/K)$ on this space is a quotient of the N-dimensional permutation representation of H, which decomposes as an irreducible $N-1$-dimensional representation and a trivial representation.

If the quotient V_c does not contain the $N-1$-dimensional irreducible, it must have trivial H-action, so $x_1 - x_2 \in A(L)_{\mathrm{tor}}$ for all $x_1, x_2 \in f^{-1}(c)$. By a theorem of Geyer and Jarden [**GJ**, Proposition 1.1], since $x_1 - x_2$ is defined over a bounded degree extension of a given finitely generated field, there are only finitely many possibilities for it, independent of the choice c.

For each $t \in A(\bar{K})_{\mathrm{tor}}$ there are three possibilities for the translation map $\tau_t \colon A \to A$:

(1) $\tau_t(X) \neq X$;
(2) $\tau_t(X) = X$ but $f \circ \tau_t|_X$ and f are distinct;
(3) $f \circ \tau_t|_X = f$

In case (1), $f(x_1) = f(x_2)$ can only happen for finitely many pairs (x_1, x_2), so there are finitely many possibilities for $c = f(x_1)$. In case (2), there are finitely many c for which there exists x_1 with $x_1, x_1 + t \in f^{-1}(c)$.

The set of torsion points t for which case (3) occurs forms a finite subgroup T of A, and the morphism f factors through $X \to X/T$. Since $\deg f = N$ is prime, this means $|T| = 1$ or $|T| = N$. The case $|T| = 1$ means $x_1 - x_2 \in T$ implies $x_1 = x_2$, so this case can be disregarded. This leaves the case $|T| = N$, which implies f is the quotient map by translation by T. This cannot happen, since T acts freely on A and therefore on X, while every degree N morphism from an irreducible curve to $\mathbb{P}^1$ is ramified. Thus, at the cost of excluding finitely many values of c, we may assume that the action of H on V_c contains an irreducible factor of degree $N-1$.

If the composition of $e_{\boldsymbol{\sigma}}$ with the quotient map $G_K \to H$ has image $\iota(G)$, then $\rho_A \circ e_{\boldsymbol{\sigma}}$ contains at least one copy of the atom α. The probability that this occurs for a single value c is at least $N!^{-n}$. However, by Hilbert irreducibility, for every finite sequence $K_1, \dots, K_m$ of finite extensions of K there exists $c \in K \subset \mathbb{P}^1(K)$ such that the kernel G_L of the action of G_K on the N-element set $f^{-1}(c)$ satisfies $G_K/G_L \cong H$, and L is linearly disjoint from $K_1 \cdots K_m$ over K. We define K_{m+1} to be L, and iterate. By linear disjointness, the conditions on the compositions of $e_{\boldsymbol{\sigma}}$ with different maps $G_K \to \mathrm{Gal}(K_i/K)$ are independent. By the second Borel-Cantelli lemma, this implies that with probability 1, the atom α occurs infinitely many times in $\rho_A \circ e_{\boldsymbol{\sigma}}$. □

3. Diophantine Geometry

Let K be any Hilbertian field. Given an abelian variety A/K, a finite group G, and a free $\mathbb{Z}$-module Λ of rank n and an integral representation $G \to \mathrm{Aut}(\Lambda)$, we define $B := \mathrm{Hom}(\Lambda, A) \cong A^n$. The action of G on Λ determines an action of G on B. Note that $\Lambda \subset \mathrm{Hom}(B, A)$, and this embedding is compatible with G-actions, where G acts on $\mathrm{Hom}(B, A)$ through its action on B.

Suppose that the quotient variety B/G contains a rational curve C. Let Y denote the inverse image of C in B. If Y is irreducible, we can apply Hilbert irreducibility to the morphism $f\colon Y \to Y/G = C$ to conclude that for "most" $c \in C(K)$, the inverse image of c in Y consists of a single point $y \in Y$ whose residue field L is a G-extension of K. The embedding of Y in B gives a point of $B(L)$, which we again denote y.

The action of $\mathrm{Gal}(L/K)$ on the Galois orbit of y is compatible with the action of G on B. Composing the embedding of Λ in $\mathrm{Hom}(B, A)$ with the evaluation map on y, we get a G-equivariant map from Λ to $A(L)$. The span of the image in $A(L) \otimes \mathbb{Q}$, regarded as $\mathrm{Gal}(L/K)$-representation is therefore a quotient representation of $W := \Lambda \otimes \mathbb{Q}$ as G-representation. Generically [**IL1**, Proposition 2.1], this span is in fact isomorphic to W as G-representation.

In favorable situations, this construction can be used to give unconditional proofs that $A(\bar{K}(\boldsymbol{\sigma}))$ has infinite rank. If $W^H \neq 0$ for all subgroups of G generated by n elements, then a copy of W in $A(L) \otimes \mathbb{Q}$ guarantees a non-zero element in $A(L \cap \bar{K}(\boldsymbol{\sigma})) \otimes \mathbb{Q}$. By linear disjointness arguments, one can construct an infinite linearly independent sequence of such elements.

In [**Lr**], this idea is implemented in the following concrete form. Suppose E is an elliptic curve over K and a_i and b_i are periodic sequences in K with period 3 such that for all i (or equivalently for $i = 1, 2, 3$),

$$y^2 = (x - a_i)(x - a_{i+1})(x - b_i)(x - b_{i+1})$$

is K-isomorphic to E. For all $c \in K$ distinct from all a_i and b_i, we have

$$\prod_{i=1}^{3} (c - a_i)(c - a_{i+1})(c - b_i)(c - b_{i+1}) \in (K^\times)^2.$$

Thus for all $\sigma \in \mathrm{Gal}(\bar{K}/K)$ there exists $i \in \{1,2,3\}$ such that

$$\sqrt{(c-a_i)(c-a_{i+1})(c-b_i)(c-b_{i+1})} \in \bar{K}(\sigma)$$

Finding such a_i and b_i for a given E amounts to realizing the c-line in E^3/G, where G is the Klein 4-group with each non-zero element inverting two coordinates of E^3.

Ideally, one would like to choose G and Λ such that $\Lambda^G = (0)$ but $\Lambda^H \neq (0)$ for all n-generated subgroups of G, where n is a fixed (possibly large) integer. For any n, such a pair exists; for instance, one can take $G = (\mathbb{Z}/2\mathbb{Z})^{n+1}$, and let Λ denote the quotient of the integral regular representation by its group of G-invariants. Unfortunately, for such pairs (G,Λ), for $n \geq 2$, we do not know if $\mathrm{Hom}(\Lambda, A)/G$ has any rational curves. (There is one exception: for the elliptic curve

$$y^2 = (x-1)(x-\zeta_7)(x-\zeta_7^2)(x-\zeta_7^4),$$

and $n = 2$, the Hamming code gives [**Lr**, Theorem 6] a rational curve on $\mathrm{Hom}(\Lambda, A)/G$.)

There are example of pairs (G,Λ) for which $\mathrm{Hom}(\Lambda, A)/G$ has many rational curves. For instance, a theorem of Eduard Looijenga [**Lo**] shows that if G is a Weyl group and Λ is suitably chosen, this quotient is actually a weighted projective space. On the other hand, examples where most points in $\mathrm{Hom}(\Lambda, A)/G$ lie on rational curves are rare and never too far from the reflection group case [**KL**]. It may also happen that $\mathrm{Hom}(\Lambda, A)/G$ may fail to be uniruled and still have some rational curves. There are some interesting examples of this phenomenon, especially when A is an elliptic curve; for instance most of the smaller sporadic groups can be realized in this way [**IL1**].

On the other hand, there is some evidence that, especially for quotients of higher dimensional abelian varieties by finite groups, rational curves may be the exception rather than the rule. For instance, by a theorem of Gian Petro Pirola [**Pi**], most Kummer surfaces of dimension ≥ 3 have no rational curves. It would be interesting to have a criterion in terms of a positive integer d, a finite group G, and an integral representation Λ of G for whether $\mathrm{Hom}(\Lambda, A)/G$ has a genus 0 curve for all abelian varieties A of dimension d.

Note that if Λ_1 and Λ_2 are integral representations such that the rational representations $W_i := \Lambda_i \otimes \mathbb{Q}$ are isomorphic to one another, then the $\mathrm{Hom}(\Lambda_i, A)$ admit G-equivariant isogenies in both directions, so the existence of genus 0 curves depends only on the underlying rational representation. As a very preliminary step in this direction, in [**IL5**], we gave the following sufficient criterion, extending the result of [**KL**]:

THEOREM 3. *If G has an element g which acts on the Lie algebra of B with eigenvalues $\lambda_i = e^{2\pi i x_i}$, $0 \leq x_i < 1$, and $\sum_i x_i \leq 1$, then B/G has at least one rational curve.*

If G is an alternating group of even degree d and W is the $d-1$-dimensional irreducible representation, then $W^H \neq 0$ for all cyclic subgroups

H of G. Indeed, H is generated by a single element, which cannot be a d-cycle and must therefore have at least two orbits in its action on $\{1, 2, \ldots, d\}$; it follows that W^H has dimension at least 1. Using this construction, in **[IL2]** we proved Conjecture 2 for $n = 1$:

THEOREM 4. *Let A be a non-trivial abelian variety over a field K which is not locally finite, which does not have characteristic 2, and which has (topologically) cyclic Galois group. Then the rank of A over K is infinite.*

4. Combinatorics

According to Conjecture 5, every pointed non-singular curve X/K has infinitely many points over $\bar{K}(\boldsymbol{\sigma})$ for all $\boldsymbol{\sigma}$. This obviously implies the following statement:

CONJECTURE 6. *If K is a finitely generated field over $\mathbb{Q}$ and X is a pointed non-singular curve over K, then for all $\boldsymbol{\sigma}$, there are infinitely many $\bar{K}(\boldsymbol{\sigma})$ points on X.*

For some curves, Conjecture 6 can be proved directly **[IL4]**:

THEOREM 5. *If $a_1, \ldots, a_{2g+2}$ are pairwise distinct elements of any infinite field $K' := \bar{K}(\boldsymbol{\sigma})$, not of characteristic 2, with finitely generated absolute Galois group, then the (non-singular) split hyperelliptic curve*

$$y^2 = (x - a_1) \cdots (x - a_{2g+2})$$

has infinitely many points over K'.

To explain the strategy of proof, we consider the case that the characteristic of K is 0, $g = 1$, and $a_i = 1 - i$ for $i = 1, \ldots, 4$. As $G_{K'} = \langle \boldsymbol{\sigma} \rangle$ is finitely generated, by Kummer theory, $(K')^\times \otimes \mathbb{F}_2$ is finite. Each positive integer n determines a class in this group, so by van der Waerden's theorem, there exist four positive integers in arithmetic progression, a, $a + d$, $a + 2d$, $a + 3d$, all of which are equivalent modulo squares in K'. Thus

$$(a/d)(a/d + 1)(a/d + 2)(a/d + 3) \in (F')^2,$$

so there is a rational point on the curve with $x = a/d$. In the general case, the proof uses the Hales-Jewett Theorem **[HJ**, Theorem 1].

This result implies that if K' is not locally finite, then for any abelian variety A which admits a non-constant K'-morphism from a split hyperelliptic curve X, the rank of A over K' is infinite. In particular, this is the case for all elliptic curves with all 2-torsion points rational.

The other class for which we are aware of a combinatorial proof of Conjecture 6 is projective curves X of the form $ax^n + by^n + cz^n = 0$. By **[BL]**, if $a, b, c \in \mathbb{Q}$ then X has infinitely many points over $\bar{\mathbb{Q}}(\boldsymbol{\sigma})$ for all $\boldsymbol{\sigma}$ provided it has at least one point over $\mathbb{Q}$. In fact, less suffices; it is enough that X has points over every completion of $\mathbb{Q}$. The crucial point is to solve equations of the form $au + bv + cw = 0$, where u, v, w lie in chosen cosets of an arbitrary finite index subgroup of $\mathbb{Q}^\times$. This is done using the circle method.

5. Arithmetic

In this section and the next, we focus on Conjecture 3 in the case that $A = E$ is an elliptic curve. Here we consider methods from arithmetic geometry; in the following section, which is mainly conjectural, we consider what might be hoped for from analytic number theory.

We start with an elliptic curve $E/\mathbb{Q}$. By modularity, we have a good supply of algebraic points on E, namely, the Heegner points.

Let K be an imaginary quadratic field of $\mathbb{Q}$ with discriminant D and N be the conductor of $E/\mathbb{Q}$. For each positive integer c relatively prime to ND, let $\mathcal{O}_c$ be the order of index c in the ring of integers $\mathcal{O}_K$ of K. Then the elliptic curve E with $E(\mathbb{C}) = \mathbb{C}/\mathcal{O}_c$ defines a point on the modular curve $X_0(N)$, and its image P_c on E under the modular parametrization of $X_0(N)$ to E is called the Heegner point of conductor c; it is defined over the ring class field H_c of conductor c. If K satisfies the so-called *Heegner hypothesis*, i.e., all primes dividing the conductor N of E split in K, then there exists a non-torsion Heegner point in the collection of all Heegner points. (See [**Dar**].)

In [**I2**], it is proved that Heegner points span an infinite-dimensional subspace of the Mordell-Weil group $E(H)$ over the compositum H of all ring class fields with conductor prime to ND. In particular, since the ring class fields H_{rp^m}, where r and p are relatively prime to ND, have dihedral Galois group over $\mathbb{Q}$, if an automorphism $\sigma \in G_{\mathbb{Q}}$ does not fix K, then by the norm-compatibility relation among the Heegner points over H_{rp^k}, it can be shown that the rank of E is unbounded over the fixed subfields of H_{rp^m} under σ as m increases. If σ fixes all imaginary quadratic extensions, then automatically the rank of E over the fixed subfield under σ is infinite by an elementary argument. Either way, E has infinite rank over $\bar{\mathbb{Q}}(\boldsymbol{\sigma})$ for $n = 1$.

The same strategy has been applied [**BI**] to extend this result to elliptic curves over global function fields of odd characteristic parametrized by Drinfeld modular curves, and for elliptic curves over totally real fields parametrized by Shimura curves.

If k is a totally real number field and f is a new form on $\mathrm{GL}_2(\mathbb{A}_k)$ of weight 2 with level condition associated with $\mathfrak{c}$, where $\mathbb{A}_k$ denotes the ring of adèles of k and $\mathfrak{c}$ is a non-zero ideal of $\mathcal{O}_k$, then by [**Zh**] there exists an elliptic curve E'/k of conductor $\mathfrak{c}$ such that the L-functions of E' and f coincide up to factors at primes dividing $\mathfrak{c}$ and there exists a Shimura curve X/k and a surjective k-morphism from X to E'. So we say that E/k has a modular parametrization by a Shimura curve if E is k-isogenous to E' arising as above. If K is an imaginary quadratic extension of k such that the discriminant of K/k is prime to $\mathfrak{c}$ and satisfying a splitting or non-splitting property depending on the degree of k over $\mathbb{Q}$, which is the Heegner hypothesis in the case of totally real fields, and if E/k has a modular parametrization, then we can construct Heegner points on E via the isogeny as before.

If k is a global function field of odd characteristic, for any elliptic curve E/k, there exists a morphism from the Drinfeld modular curve $X_0(\mathfrak{c})$ to E, where the conductor of E is $\mathfrak{c} \cdot \infty$ for an ideal $\mathfrak{c}$ of $\mathcal{O}_k$ [**GR**]. We say K/k is an *imaginary quadratic extension* if the place ∞ does not split in K/k. In this case, the Heegner hypotheses for K is the condition that all primes dividing $\mathfrak{c}$ split in K/k. For K satisfying the Heegner hypothesis, we can construct Heegner points via this Drinfeld modular curve parametrization as before.

Although these results are now encompassed by Theorem 4, Heegner point methods, possibly in conjunction with ideas from analytic number theory, remain a viable approach to Conjecture 3 for elliptic curves over suitable global ground fields.

Tim and Vladimir Dokchitser [**DD1**] gave an approach to Conjecture 3 for elliptic curves for general n. Assuming the Birch-Swinnerton-Dyer conjecture, they proved that the conjecture holds if K has a real place or E has non-integral j-invariant.

Their main idea was to show first that there is a quadratic extension M/K where the root number $w(E/M) = -1$ and the rank of $E(M)$ is odd. If a place v of K which is real or nonarchimedean with $v(j(E)) < 0$ is fixed, then they proved that by the weak approximation theorem, M can be taken as a quadratic extension such that the negative contribution of the local root number occurs only above v, so that the global root number $w(E/M)$, which is the product of local root numbers, is -1.

If $G \subset G_K$ is finitely generated, for an odd prime p, they constructed a Galois extension F/K containing M such that $\mathrm{Gal}(F/K) \cong \mathbb{F}_p^r \rtimes C_2$ where C_2 acts by -1, the image of G in $\mathrm{Gal}(F/K)$ has order at most 2, and the primes of M above bad reduction primes of E/K split completely in F. Then, by taking any index p subgroup V of $\mathbb{F}_p^r$, V is a normal subgroup of $\mathrm{Gal}(F/K)$ and $\mathrm{Gal}(F^V/K)$ is isomorphic to the dihedral group of order $2p$. As the image of of G in $\mathrm{Gal}(F/K)$ has order ≤ 2, they got a degree p-extension $L \subseteq F^V$ over K fixed by G and applied the congruence modulo 2-relation among the ranks of E over M, L and K ([**DD2**]) from which they concluded that by the p-parity conjecture,

$$\mathrm{rk}_L E > \mathrm{rk}_K E.$$

6. Analytic Number Theory

The method of §3 is based on the idea that where there are rational curves, there are rational points. However, many varieties without rational curves nevertheless have many rational points. The following conjecture seems to us likely to be true but unlikely to follow from the method of §3:

Conjecture 7. *Let $E/\mathbb{Q}$ be an elliptic curve. For all n there exist infinitely many linearly independent $n+1$-dimensional $\mathbb{F}_2$-subspaces $V_i \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ such that for all i and all non-zero $v \in V_i$, the twist E_v has positive rank over $\mathbb{Q}$.*

This conjecture implies that Conjecture 3 holds for E. Indeed, let $\mathbb{Q}(\sqrt{V_i})$ denote the extension of $\mathbb{Q}$ obtained by taking square roots of coset representatives of all elements of V_i. By Kummer theory, $\mathrm{Gal}(\mathbb{Q}(\sqrt{V_i})/\mathbb{Q})$ is dual to V_i, and the image of $\langle \boldsymbol{\sigma} \rangle$ fixes a subspace of V_i of positive dimension. Thus there exists $v_i \in V_i$ such that $\mathbb{Q}(\sqrt{v_i}) \subset \bar{\mathbb{Q}}(\boldsymbol{\sigma})$. As E_{v_i} has positive rank, the non-trivial eigenspace of the action of $\mathrm{Gal}(\mathbb{Q}(\sqrt{v_i})/\mathbb{Q})$ on $E(\mathbb{Q}(\sqrt{v_i})) \otimes \mathbb{Q}$ has positive rank. By taking points of E in linearly disjoint fields $\mathbb{Q}(\sqrt{v_i})$, we obtain an infinite sequence of elements in $E(\bar{\mathbb{Q}}(\boldsymbol{\sigma})) \otimes \mathbb{Q}$, which can easily be seen to be linearly independent (see, e.g., [**Lr**, Theorem 5]).

It is known [**ILR**] that there are examples of curves E such that Conjecture 7 holds for $n = 1$. The conjecture would hold in general if we knew:

Conjecture 8. *Let $E/\mathbb{Q}$ be an elliptic curve. There exists an infinite dimensional $\mathbb{F}_2$-subspace $V_0 \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ such that for all non-zero $v \in V_0$, the twist E_v has positive rank.*

Using analytic arguments and the known positive density of positive rank quadratic twists of certain elliptic curves over $\mathbb{Q}$ (see, e.g. [**Va**]), we proved [**IL3**] that there exist elliptic curves E over $\mathbb{Q}$ with arbitrarily large finite subspaces $V_0 \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ satisfying the positive rank condition for E. On the other hand, Conjecture 8 would be an easy consequence of the following conjecture:

Conjecture 9. *Let $E_1, \ldots, E_n$ be elliptic curves over $\mathbb{Q}$. Then there exists $d \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ such that the twist of every E_i by d has positive rank.*

By estimating $\sum_{d<N} L'(1, E_d)$, Perelli-Pomykała [**PP**] showed that the proportion of twists of a fixed elliptic curve E by $d < N$ which have analytic rank 1 grows faster than $N^{-\epsilon}$ for all $\epsilon > 0$. The same is true for rank 1 by Kolyvagin's theorem. Choosing $\epsilon < 1/n$, this gives a heuristic argument for Conjecture 9. It would be interesting to try to bound

$$\sum_{d<N} L'(1, (E_1)_d) \cdots L'(1, (E_n)_d)$$

away from zero.

References

[BF] Bary-Soroker, Lior; Fehm, Arno: Open problems in the theory of ample fields. Geometric and differential Galois theories, 1–11, Sémin. Congr., 27, Soc. Math. France, Paris, 2013.

[BL] Bourgain, Jean; Larsen, Michael: A Finitary Hasse Principle for Diagonal Curves, arXiv:1404.2849.

[BI] Breuer, Florian; Im, Bo-Hae: Heegner points and the rank of elliptic curves over large extensions of global fields. *Canad. J. Math.* **60** (2008), no. 3, 481–490.

[DD1] Dokchitser, Tim; Dokchitser, Vladimir: A note on Larsen's conjecture and ranks of elliptic curves. *Bull. Lond. Math. Soc.* **41** (2009), no. 6, 1002–1008.

[DD2] Dokchitser, Tim; Dokchitser, Vladimir: On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math. (2)* **172** (2010), no. 1, 567–596.

[Dar] H. Darmon, Rational points on modular elliptic curves, CBMS Regional Conference Series in Mathematics, 101. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the AMS, Providence, RI, 2004. MR2020572 (2004k:11103)

[FP] Fehm, Arno; Petersen, Sebastian: On the rank of abelian varieties over ample fields. *Int. J. Number Theory* **6** (2010), no. 3, 579–586.

[Fe] Feit, Walter: Some consequences of the classification of finite simple groups. The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), pp. 175–181, Proc. Sympos. Pure Math., 37, Amer. Math. Soc., Providence, R.I., 1980.

[FyJ] Frey, Gerhard; Jarden, Moshe: Approximation theory and the rank of abelian varieties over large algebraic fields. *Proc. London Math. Soc. (3)* **28** (1974), 112–128.

[FdJ] Fried, Michael D.; Jarden, Moshe: Field arithmetic. Third edition. Revised by Jarden. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics, 11. Springer-Verlag, Berlin, 2008.

[GR] Gekeler, Ernst-Ulrich; Reversat, Marc: Jacobians of Drinfeld modular curves. *J. Reine Angew. Math.* **476**(1996), 27–93.

[GJ] Geyer, Wulf-Dieter; Jarden, Moshe: The rank of abelian varieties over large algebraic fields. *Arch. Math. (Basel)* **86** (2006), no. 3, 211–216.

[HJ] Hales, A. W.; Jewett, R. I.: Regularity and positional games. *Trans. Amer. Math. Soc.* **106** (1963), 222–229.

[I1] Im, Bo-Hae: The rank of elliptic curves with rational 2-torsion points over large fields, *Proc. Amer. Math. Soc.* **134** (2006), 1623–1630.

[I2] Im, Bo-Hae: Heegner points and Mordell-Weil groups of elliptic curves over large fields. *Trans. Amer. Math. Soc.* **359** (2007), no. 12, 6143–6154.

[IL1] Im, Bo-Hae; Larsen, Michael: Realizing Rational Representations in Mordell-Weil Groups, arXiv: math/0401209.

[IL2] Im, Bo-Hae; Larsen, Michael: Abelian varieties over cyclic fields. *Amer. J. Math.* **130** (2008), no. 5, 1195–1210.

[IL3] Im, Bo-Hae; Larsen, Michael: Parallelopipeds of positive rank twists of elliptic curves. *Indiana Univ. Math. J.* **60** (2011), no. 1, 311–318.

[IL4] Im, Bo-Hae; Larsen, Michael: Some applications of the Hales-Jewett theorem to field arithmetic. *Israel J. Math.* **198** (2013), no. 1, 35–47.

[IL5] Im, Bo-Hae; Larsen, Michael: Rational curves on quotients of abelian varieties by finite groups. *Math. Res. Lett.* **22** (2015), no. 4, 1145–1157.

[ILR] Im, Bo-Hae; Lozano-Robledo, Álvaro: On products of quadratic twists and ranks of elliptic curves over large fields. *J. Lond. Math. Soc. (2)* **79** (2009), no. 1, 1–14.

[JK] Junker, Markus; Koenigsmann, Jochen: Schlanke Körper. *J. Symbolic Logic* **75** (2010), no. 2, 481–500.

[KL] Kollár, János; Larsen, Michael: Quotients of Calabi-Yau varieties. Algebra, arithmetic, and geometry: in honor of Yu. I. Manin. Vol. II, 179–211, Progr. Math., 270, Birkhäuser Boston, Inc., Boston, MA, 2009.

[Ln] Lang, Serge: Fundamentals of Diophantine geometry. Springer-Verlag, New York, 1983.

[Lr] Larsen, Michael: Rank of elliptic curves over almost separably closed fields. *Bull. London Math. Soc.* **35** (2003), no. 6, 817–820.

[Lo] Looijenga, Eduard: Root systems and elliptic curves. *Invent. Math.* **38** (1976/77), no. 1, 17–32.

[PP] Perelli, A.; Pomykała, J.: Averages of twisted elliptic L-functions. *Acta Arith.* **80** (1997), no. 2, 149–163.

[Pi] Pirola, Gian Pietro: Curves on generic Kummer varieties. *Duke Math. J.* **59** (1989), no. 3, 701–708.

[Va] Vatsal, Vinayak: Rank-one twists of a certain elliptic curve. *Math. Ann.* **311** (1998), no. 4, 791–794.

[Zh] Zhang, Shou-Wu: Heights of Heegner points on Shimura curves. *Ann. of Math.* **153** (2001), no. 1, 27–147.

Department of Mathematical Sciences, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, South Korea

E-mail address: bhim@kaist.ac.kr

Department of Mathematics, Indiana University, Bloomington, IN, 47405, U.S.A.

E-mail address: mjlarsen@indiana.edu