2

The Birch and Swinnerton-Dyer Conjecture

This chapter is about the conjecture of Birch and Swinnerton-Dyer on the arithmetic of abelian varieties. We focus primarily on abelian varieties attached to modular forms.

In the 1960s, Sir Peter Swinnerton-Dyer worked with the EDSAC computer lab at Cambridge University, and developed an operating system that ran on that computer (so he told me once). He and Bryan Birch programmed EDSAC to compute various quantities associated to elliptic curves. They then formulated the conjectures in this chapter in the case of dimension 1 (see [Bir65, Bir71, SD67]). Tate formulated the conjectures in a functorial way for abelian varieties of arbitrary dimension over global fields in [Tat66], and proved that if the conjecture is true for an abelian variety A, then it is also true for each abelian variety isogenous to A.

Suitably interpreted, the conjectures may by viewed as generalizing the analytic class number formula, and Bloch and Kato generalized the conjectures to Grothendieck motives in [BK90].

2.1 The Rank Conjecture

Let A be an abelian variety over a number field K.

Definition 2.1.1 (Mordell-Weil Group). The *Mordell-Weil group* of A is the abelian group $AK)$ of all K-rational points on A.

Theorem 2.1.2 (Mordell-Weil). *The Mordell-Weil group $A(K)$ of A is finitely generated.*

The proof is nontrivial and combines two ideas. First, one proves the “weak Mordell-Weil theorem”: for any integer m the quotient $A(K)/mA(K)$ is finite. This is proved by combining Galois cohomology techniques with standard finiteness theorems from algebraic number theory. The second idea is to introduce the Néron-

Tate canonical height $h : A(K) \to \mathbf{R}_{\geq 0}$ and use properties of h to deduce, from finiteness of $A(K)/mA(K)$, that $A(K)$ itself is finitely generated.

Definition 2.1.3 (Rank). By the structure theorem $A(K) \cong \mathbf{Z}^r \oplus G_{\text{tor}}$, where r is a nonnegative integer and G_{tor} is the torsion subgroup of G. The *rank* of A is r.

Let $f \in S_2(\Gamma_1(N))$ be a newform of level N, and let $A = A_f \subset J_1(N)$ be the corresponding abelian variety. Let $f_1, \ldots, f_d$ denote the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugates of f, so if $f = \sum a_n q^n$, then $f_i = \sum \sigma(a_n) q^n$, for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

Definition 2.1.4 (L-function of A). We define the L-function of $A = A_f$ (or any abelian variety isogenous to A) to be

$$L(A, s) = \prod_{i=1}^{d} L(f_i, s).$$

By Theorem 1.1.4, each $L(f_i, s)$ is an entire function on $\mathbf{C}$, so $L(A, s)$ is entire. In Section **??** we will discuss an intrinsic way to define $L(A, s)$ that does not require that A be attached to a modular form. However, in general we do not know that $L(A, s)$ is entire.

Conjecture 2.1.5 (Birch and Swinnerton-Dyer). *The rank of* $A(\mathbf{Q})$ *is equal to* $\mathrm{ord}_{s=1} L(A, s)$.

One motivation for Conjecture 2.1.5 is the following *formal* observation. Assume for simplicity of notation that $\dim A = 1$. By Theorem 1.1.6, the L-function $L(A, s) = L(f, s)$ has an Euler product representation

$$L(A, s) = \prod_{p \mid N} \frac{1}{1 - a_p p^{-s}} \cdot \prod_{p \nmid N} \frac{1}{1 - a_p p^{-s} + p \cdot p^{-2s}},$$

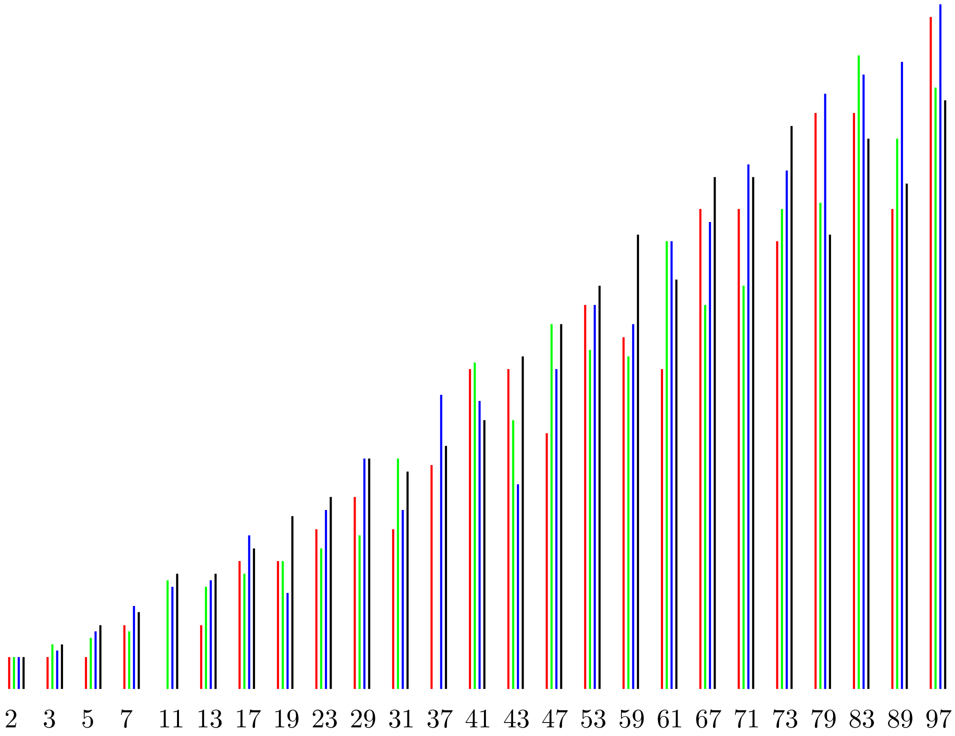
which is valid for $\mathrm{Re}(s)$ sufficiently large. (Note that $\varepsilon = 1$, since A is a modular elliptic curve, hence a quotient of $X_0(N)$.) There is no loss in considering the product $L^*(A, s)$ over only the good primes $p \nmid N$, since $\mathrm{ord}_{s=1} L(A, s) = \mathrm{ord}_{s=1} L^*(A, s)$ (because $\prod_{p \mid N} \frac{1}{1 - a_p p^{-s}}$ is nonzero at $s = 1$). We then have *formally* that

$$\begin{aligned} L^*(A, 1) &= \prod_{p \nmid N} \frac{1}{1 - a_p p^{-1} + p^{-1}} \\ &= \prod_{p \nmid N} \frac{p}{p - a_p + 1} \\ &= \prod_{p \nmid N} \frac{p}{\#A(\mathbf{F}_p)} \end{aligned}$$

The intuition is that if the rank of A is large, i.e., $A(\mathbf{Q})$ is large, then each group $A(\mathbf{F}_p)$ will also be large since it has many points coming from reducing the elements of $A(\mathbf{Q})$ modulo p. It seems likely that if the groups $\#A(\mathbf{F}_p)$ are unusually large, then $L^*(A, 1) = 0$, and computational evidence suggests the more precise Conjecture 2.1.5.

Example 2.1.6. Let A_0 be the elliptic curve $y^2 + y = x^3 - x^2$, which has rank 0 and conductor 11, let A_1 be the elliptic curve $y^2 + y = x^3 - x$, which has rank 1 and conductor 37, let A_2 be the elliptic curve $y^2 + y = x^3 + x^2 - 2x$, which has rank 2 and conductor 389, and finally let A_3 be the elliptic curve $y^2 + y = x^3 - 7x + 6$, which has rank 3 and conductor 5077. By an exhaustive search, these are known to be the smallest-conductor elliptic curves of each rank. Conjecture 2.1.5 is known to be true for them, the most difficult being A_3, which relies on the results of [**?**].

The following diagram illustrates $|\#A_i(\mathbf{F}_p)|$ for $p < 100$, for each of these curves. The height of the red line (first) above the prime p is $|\#A_0(\mathbf{F}_p)|$, the green line (second) gives the value for A_1, the blue line (third) for A_2, and the black line (fourth) for A_3. The intuition described above suggests that the clumps should look like triangles, with the first line shorter than the second, the second shorter than the third, and the third shorter than the fourth—however, this is visibly not the case. The large Mordell-Weil group over $\mathbf{Q}$ does not increase the size of every $E(\mathbf{F}_p)$ as much as we might at first suspect. Nonetheless, the first line is no longer than the last line for every p except $p = 41, 79, 83, 97$.



Remark 2.1.7. Suppose that $L(A, 1) \neq 0$. Then assuming the Riemann hypothesis for $L(A, s)$ (i.e., that $L(A, s) \neq 0$ for $\mathrm{Re}(s) > 1$), Goldfeld [Gol82] proved that the Euler product for $L(A, s)$, formally evaluated at 1, converges but *does not* converge to $L(A, 1)$. Instead, it converges (very slowly) to $L(A, 1)/\sqrt{2}$. For further details and insight into this strange behavior, see [Con03].

Remark 2.1.8. The Clay Math Institute has offered a one million dollar prize for a proof of Conjecture 2.1.5 for elliptic curves over $\mathbf{Q}$. See [Wil00].

Theorem 2.1.9 (Kolyvagin-Logachev). *Suppose $f \in S_2(\Gamma_0(N))$ is a newform such that $\mathrm{ord}_{s=1} L(f, s) \leq 1$. Then Conjecture 2.1.5 is true for A_f.*

Theorem 2.1.10 (Kato). *Suppose $f \in S_2(\Gamma_1(N))$ and $L(f,1) \neq 0$. Then Conjecture 2.1.5 is true for A_f.*

2.2 Refined Rank Zero Conjecture

Let $f \in S_2(\Gamma_1(N))$ be a newform of level N, and let $A_f \subset J_1(N)$ be the corresponding abelian variety. We remark that the definitions, results, and proofs in this section are all true exactly as stated with $X_1(N)$ replaced by $X_0(N)$.

The following conjecture refines Conjecture 2.1.5 in the case $L(A,1) \neq 0$. We recall some of the notation below, where we give a formula for $L(A,1)/\Omega_A$, which can be computed up to something called the Manin index.

Conjecture 2.2.1 (Birch and Swinnerton-Dyer). *Suppose $L(A,1) \neq 0$. Then*

$$\frac{L(A,1)}{\Omega_A} = \frac{\#Ш(A) \cdot \prod_{p \mid N} c_p}{\#A(\mathbf{Q})_{\mathrm{tor}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tor}}}.$$

In order to give a formula for $L(A,1)/\Omega_A$ it will be easiest to work with the dual $A_f^\vee$ of A_f, which we view naturally as a quotient of $J_1(N)$ as follows. Dualizing the map $A_f \hookrightarrow J_1(N)$ we obtain a surjective map $J_1(N) \to A_f^\vee$, where $A = A_f^\vee$ is the dual of A_f.

The map $J_1(N) \to A$ induces a map $\mathcal{J} \to \mathcal{A}$ on Néron models. Pullback of differentials defines a map

$$\mathrm{H}^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}}) \to \mathrm{H}^0(\mathcal{J}, \Omega^1_{\mathcal{J}/\mathbf{Z}}). \tag{2.2.1}$$

One can show that there is a q-expansion map

$$\mathrm{H}^0(\mathcal{J}, \Omega^1_{\mathcal{J}/\mathbf{Z}}) \to \mathbf{Z}[[q]] \tag{2.2.2}$$

which agrees with the usual q-expansion map after tensoring with $\mathbf{C}$. (For us $X_1(N)$ is the curve that parameterizes pairs $(E, \mu_N \hookrightarrow E)$, so that there is a q-expansion map with values in $\mathbf{Z}[[q]]$.)

Let φ_A be the composition of (2.2.1) with (2.2.2).

Definition 2.2.2 (Manin Index). The *Manin index* c_A of A is the index of $\varphi_A(\mathrm{H}^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}}))$ in its saturation. I.e., it is the order of the quotient group

$$\left(\frac{\mathbf{Z}[[q]]}{\varphi_A(\mathrm{H}^0(\mathcal{A}, \Omega^1_{\mathcal{A}/\mathbf{Z}}))}\right)_{\mathrm{tor}}.$$

Manin made the following conjecture when $\dim A = 1$:

Conjecture 2.2.3 (Agashe, Stein). *$c_A = 1$.*

This conjecture is false if A is not required to be attached to a newform. For example, Adam Joyce, a student of Kevin Buzzard, found an $A \subset J_1(431)$ (and also $A' \subset J_0(431)$) whose Manin constant is 2. Here A is isogenous over $\mathbf{Q}$ to a product of two elliptic curves.

Definition 2.2.4 (Real Components). Let c_∞ be the number of connected components of $A(\mathbf{R})$.

If A is an elliptic curve, then $c_\infty = 1$ or 2, depending on whether the graph of the affine part of $A(\mathbf{R})$ in the plane $\mathbf{R}^2$ is connected. In general, there is a simple formula for c_∞ in terms of the action of complex conjugation on $\mathrm{H}_1(A(\mathbf{R}), \mathbf{Z})$, which can be computed using modular symbols. The formula is

$$\log_2(c_\infty) = \dim_{\mathbf{F}_2} A(\mathbf{R})[2] - \dim(A).$$

Definition 2.2.5 (Real Volume). The *real volume* of $A(\mathbf{R})$ is the volume of $A(\mathbf{R})$ with respect to a measure obtained by wedging together a basis for $\mathrm{H}^0(\mathcal{A}, \Omega^1)$.

Let

$$\Phi : \mathrm{H}_1(X_1(N), \mathbf{Z}) \to \mathrm{Hom}(\mathbf{C}f_1 + \cdots \mathbf{C}f_d, \mathbf{C})$$

be the period mapping on homology induced by integrating homology classes on $X_0(N)$ against the $\mathbf{C}$-vector space spanned by the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-conjugates f_i of f, normalized so that $\Phi(\{0,\infty\})(f) = L(f,1)$.

Theorem 2.2.6. *We have the following equality of rational numbers:*

$$\frac{L(A,1)}{\Omega_A} = \frac{1}{c_\infty \cdot c_A} \cdot [\Phi(H_1(X_0(N), \mathbf{Z}))^+ : \Phi(\mathbf{T}\{0,\infty\})].$$

For V and W lattices in a $\mathbf{R}$-vector space M, the lattice index $[V : W]$ is by definition the absolute value of the determinant of a change of basis taking a basis for V to a basis for W, or 0 if W has rank smaller than the dimension of M.

Proof. Let $\tilde{\Omega}_A$ the measure of $A(\mathbf{R})$ with respect to a basis for $S_2(\Gamma_1(N), \mathbf{Z})[I_f]$, where I_f is the annihilator in $\mathbf{T}$ of f. Note that $\tilde{\Omega}_A \cdot c_A = \Omega_A$, where c_A is the Manin index. Unwinding the definitions, we find that

$$\tilde{\Omega}_A = c_\infty \cdot [\mathrm{Hom}(S_2(\Gamma_1(N), \mathbf{Z})[I_f], \mathbf{Z}) : \Phi(H_1(X_0(N), \mathbf{Z}))^+].$$

For any ring R the pairing

$$\mathbf{T}_R \times S_2(\Gamma_1(N), R) \to R$$

given by $\langle T_n, f\rangle = a_1(T_n f)$ is perfect, so $(\mathbf{T}/I_f) \otimes R \cong \mathrm{Hom}(S_2(\Gamma_1(N), R)[I_f], R)$. Using this pairing, we may view Φ as a map

$$\Phi : H_1(X_1(N), \mathbf{Q}) \to (\mathbf{T}/I_f) \otimes \mathbf{C},$$

so that

$$\tilde{\Omega}_A = c_\infty \cdot [\mathbf{T}/I_f : \Phi(H_1(X_0(N), \mathbf{Z}))^+].$$

Note that $(\mathbf{T}/I_f) \otimes \mathbf{C}$ is isomorphic as a ring to a product of copies of $\mathbf{C}$, with one copy corresponding to each Galois conjugate f_i of f. Let $\pi_i \in (\mathbf{T}/I_f) \otimes \mathbf{C}$ be the projector onto the subspace of $(\mathbf{T}/I_f) \otimes \mathbf{C}$ corresponding to f_i. Then

$$\Phi(\{0,\infty\}) \cdot \pi_i = L(f_i, 1) \cdot \pi_i.$$

Since the π_i form a basis for the complex vector space $(\mathbf{T}/I_f) \otimes \mathbf{C}$, if we view $\Phi(\{0,\infty\})$ as the operator "left-multiplication by $\Phi(\{0,\infty\})$, then

$$\det(\Phi(\{0,\infty\})) = \prod_i L(f_i, 1) = L(A, 1),$$

Letting $H = H_1(X_0(N), \mathbf{Z})$, we have

$$\begin{aligned}
[\Phi(H)^+ : \Phi(\mathbf{T}\{0,\infty\})] &= [\Phi(H)^+ : (\mathbf{T}/I_f) \cdot \Phi(\{0,\infty\})] \\
&= [\Phi(H)^+ : \mathbf{T}/I_f] \cdot [\mathbf{T}/I_f : \mathbf{T}/I_f \cdot \Phi(\{0,\infty\})] \\
&= \frac{c_\infty}{\tilde{\Omega}_A} \cdot \det(\Phi(\{0,\infty\})) \\
&= \frac{c_\infty c_A}{\Omega_A} \cdot L(A,1),
\end{aligned}$$

which proves the theorem.

□

References

[AS] A. Agashe and W. A. Stein, *The manin constant, congruence primes, and the modular degree*, In progress.

[Bir65] B. J. Birch, *Conjectures concerning elliptic curves*, Proceedings of Symposia in Pure Mathematics, VIII, Amer. Math. Soc., Providence, R.I., 1965, pp. 106–112. MR 30 #4759

[Bir71] B. J. Birch, *Elliptic curves over* $\mathbf{Q}$*: A progress report*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 396–400.

[BK90] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[CF99] J. B. Conrey and D. W. Farmer, *Hecke operators and the nonvanishing of L-functions*, Topics in number theory (University Park, PA, 1997), Math. Appl., vol. 467, Kluwer Acad. Publ., Dordrecht, 1999, pp. 143–150. MR 2000f:11055

[Con03] K. Conrad, *Partial Euler products on the critical line*, Preprint (2003).

[Gol82] D. Goldfeld, *Sur les produits partiels eulériens attachés aux courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **294** (1982), no. 14, 471–474. MR 84d:14031

[Kna92] A. W. Knapp, *Elliptic curves*, Princeton University Press, Princeton, NJ, 1992.

[Li75] W-C. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.

[SD67] P. Swinnerton-Dyer, *The conjectures of Birch and Swinnerton-Dyer, and of Tate*, Proc. Conf. Local Fields (Driebergen, 1966), Springer, Berlin, 1967, pp. 132–157. MR 37 #6287

[Tat66] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1965/66, pp. Exp. No. 306, 415–440.

[Wil00] A. J. Wiles, *The Birch and Swinnerton-Dyer Conjecture*, `http://www.claymath.org/prize_problems/birchsd.htm`.