Modular Forms

Kenneth A. Ribet William A. Stein

December 5, 2003

Contents

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 $A(K) \cong \mathbf{Z}^r \oplus G_{\mathrm{tor}}$, 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 2.4 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

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

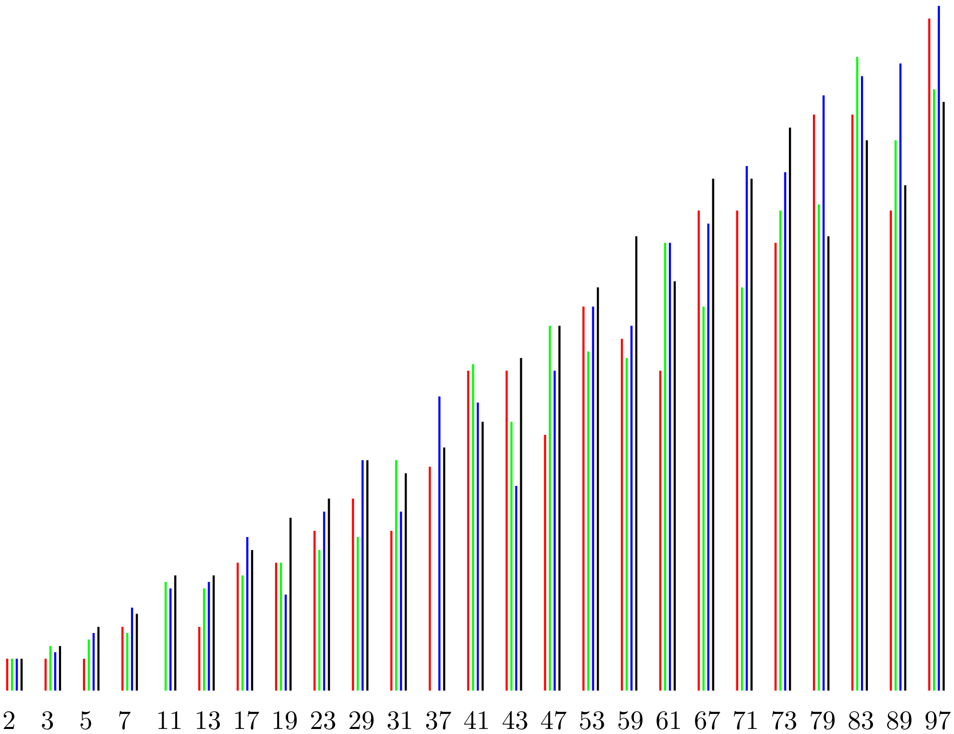
which is valid for $\mathrm{Re}(s)$ sufficiently large. (Note that $\varepsilon = 1$, since A is a modular elliptic curve, hence a quotient of $X_0(N)$.) There is no loss in considering the product $L^*(A, s)$ over only the good primes $p \nmid N$, since $\mathrm{ord}_{s=1} L(A, s) = \mathrm{ord}_{s=1} L^*(A, s)$ (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 [GZ86].

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.

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 an vinteger, which we call the Manin index. Note that the definitions, results, and proofs in this section are all true exactly as stated with $X_1(N)$ replaced by $X_0(N)$, which is relevant if one wants to do computations.

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

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

By Theorem 2.1.10, the group Ш(A) is finite, so the right hand side makes sense. The right hand side is a rational number, so if Conjecture 2.2.1 is true, then the quotient $L(A, 1)/\Omega_A$ should also be a rational number. In fact, this is true, as we will prove below (see Theorem 2.2.11). Below we will discuss aspects of the proof of rationality in the case that A is an elliptic curve, and at the end of this section we give a proof of the general case.

In to more easily understanding $L(A, 1)/\Omega_A$, it will be easiest to work with $A = A_f^\vee$, where $A_f^\vee$ is the dual of A_f. We view A naturally as a quotient of $J_1(N)$ as follows. Dualizing the map $A_f \hookrightarrow J_1(N)$ we obtain a surjective map $J_1(N) \to A_f^\vee$. Passing to the dual doesn't affect whether or not $L(A, 1)/\Omega_A$ is rational, since changing A by an isogeny does not change $L(A, 1)$, and only changes Ω_A by multiplication by a nonzero rational number.

2.2.1 The Number of Real Components

Definition 2.2.2 (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. For example, Figure 2.2.1 shows the real points of the elliptic curve defined by $y^2 = x^3 - x$ in the three affine patches that cover $\mathbf{P}^2$. The completed curve has two real components.

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

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

2.2.2 The Manin Index

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

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

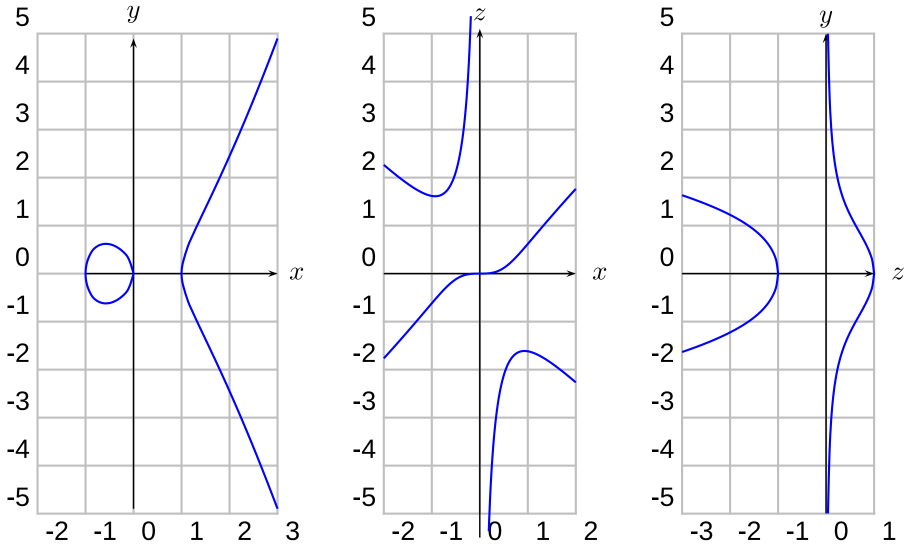


FIGURE 2.2.1. Graphs of real solutions to $y^2z = x^3 - xz^2$ on three affine patches

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 2.2.3 (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

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

Open Problem 2.2.4. Find an algorithm to compute c_A.

Manin conjectured that $c_A = 1$ when $\dim A = 1$, and I think $c_A = 1$ in general.

Conjecture 2.2.5 (Agashe, Stein). $c_A = 1$.

This conjecture is false if A is not required to be attached to a newform, even if $A_f \subset J_1(N)^{\mathrm{new}}$. 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. Also, the Manin index for $J_0(33)$ (viewed as a quotient of $J_0(33)$) is divisible by 3, because there is a cusp form in $S_2(\Gamma_0(33))$ that has integer Fourier expansion at ∞, but not at one of the other cusps.

Theorem 2.2.6. *If $f \in S_2(\Gamma_0(N))$ then the Manin index c of $A_f^\vee$ can only divisible by* 2 *or primes whose square divides N. Moreover, if $4 \nmid N$, then* $\mathrm{ord}_2(c) \leq \dim(A_f)$.

The proof involves applying nontrivial theorems of Raynaud about exactness of sequences of differentials, then using a trick with the Atkin-Lehner involution, which was introduced by Mazur in [Maz78], and finally one applies the "q-expansion principle" in characteristic p to deduce the result (see [AS]). Also, Edixhoven claims he can prove that if A_f is an elliptic curve then c_A is only divisible by 2, 3, 5, or 7. His argument use his semistable models for $X_0(p^2)$, but my understanding is that the details are not all written up.

2.2.3 The Real Volume Ω_A

Definition 2.2.7 (Real Volume). The *real volume* Ω_A of $A(\mathbf{R})$ is the volume of $A(\mathbf{R})$ with respect to a measure obtained by wedging together a basis for $\mathrm{H}^0(\mathcal{A}, \Omega^1)$.

If A is an elliptic curve with *minimal* Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

then one can show that

$$\omega = \frac{dx}{2y + a_1x + a_3} \tag{2.2.3}$$

is a basis for $\mathrm{H}^0(\mathcal{A}, \Omega^1)$. Thus

$$\Omega_A = \int_{A(\mathbf{R})} \frac{dx}{2y + a_1x + a_3}.$$

There is a fast algorithm for computing Ω_A, for A an elliptic curve, which relies on the quickly-convergent Gauss arithmetic-geometric mean (see [Cre97, §3.7]). For example, if A is the curve defined by $y^2 = x^3 - x$ (this is a minimal model), then

$$\Omega_A \sim 2 \times 2.622057554292119810464839589.$$

For a general abelian variety A, it is an open problem to compute Ω_A. However, we can compute Ω_A/c_A, where c_A is the Manin index of A, by explicitly computing A as a complex torus using the period mapping Φ, which we define in the next section.

2.2.4 The Period Mapping

Let

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

be the *period mapping* on integral 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. Extend Φ to $\mathrm{H}_1(X_1(N), \mathbf{Q})$ by $\mathbf{Q}$-linearity. We normalize Φ so that $\Phi(\{0, \infty\})(f) = L(f, 1)$. More explicitly, for $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q})$, we have

$$\Phi(\{\alpha, \beta\})(f) = -2\pi i \int_\alpha^\beta f(z)dz.$$

The motivation for this normalization is that

$$L(f, 1) = -2\pi i \int_0^{i\infty} f(z)dz, \tag{2.2.4}$$

which we see immediately from the Mellin transform definition of $L(f, s)$:

$$L(f, s) = (2\pi)^s \Gamma(s)^{-1} \int_0^{i\infty} (-iz)^s f(z) \frac{dz}{z}.$$

2.2.5 Manin-Drinfeld Theorem

Recall the Manin-Drinfeld theorem, which we proved long ago, asserts that $\{0, \infty\} \in \mathrm{H}_1(X_0(N), \mathbf{Q})$. We proved this by explicitly computing $(p+1-T_p)(\{0, \infty\})$, for $p \nmid N$, noting that the result is in $\mathrm{H}_1(X_0(N), \mathbf{Z})$, and inverting $p+1-T_p$. Thus there is an integer n such that $n\{0, \infty\} \in \mathrm{H}_1(X_0(N), \mathbf{Z})$.

Suppose that $A = A_f^\vee$ is an elliptic curve quotient of $J_0(N)$. Rewriting (2.2.4) in terms of Φ, we have $\Phi(\{0, \infty\}) = L(f, 1)$. Let ω be a minimal differential on A, as in (2.2.3), so $\omega = -c_A \cdot 2\pi i f(z) dz$, where c_A is the Manin index of A, and the equality is after pulling ω back to $\mathrm{H}^0(X_0(N), \Omega) \cong S_2(\Gamma_0(N))$. Note that when we defined c_A, there was no factor of $2\pi i$, since we compared ω with $f(q)\frac{dq}{q}$, and $q = e^{2\pi i z}$, so $dq/q = 2\pi i dz$.

2.2.6 The Period Lattice

The *period lattice* of A with respect to a nonzero differential g on A is

$$\mathcal{L}_g = \left\{ \int_\gamma g : \gamma \in \mathrm{H}_1(A, \mathbf{Z}) \right\},$$

and we have $A(\mathbf{C}) \cong \mathbf{C}/\mathcal{L}_g$. This is the Abel-Jacobi theorem, and the significance of g is that we are choosing a basis for the one-dimensional $\mathbf{C}$-vector space $\mathrm{Hom}(\mathrm{H}^0(A, \Omega), \mathbf{C})$, in order to embed the image of $\mathrm{H}_1(A, \mathbf{Z})$ in $\mathbf{C}$.

The integral $\int_{A(\mathbf{R})} g$ is "visible" in terms of the complex torus representation of $A(\mathbf{C}) = \mathbf{C}/\mathcal{L}_g$. More precisely, if $\mathcal{L}_g$ is not rectangular, then $A(\mathbf{R})$ may be identified with the part of the real line in a fundamental domain for $\mathcal{L}_g$, and $\int_{A(\mathbf{R})} g$ is the length of this segment of the real line. If $\mathcal{L}_g$ is rectangular, then it is that line along with another line above it that is midway to the top of the fundamental domain.

The real volume, which appears in Conjecture 2.2.1, is

$$\Omega_A = \int_{A(\mathbf{R})} \omega = -c_A \cdot 2\pi i \int_{A(\mathbf{R})} f.$$

Thus Ω_A is the least positive real number in $\mathcal{L}_\omega = -c_A \cdot 2\pi i \mathcal{L}_f$, when the period lattice is not rectangular, and twice the least positive real number when it is.

2.2.7 The Special Value $L(A, 1)$

Proposition 2.2.8. *We have $L(f, 1) \in \mathbf{R}$.*

Proof. With the right setup, this would follow immediately from the fact that $z \mapsto -\overline{z}$ fixes the homology class $\{0, \infty\}$. However, we don't have such a setup, so we give a direct proof.

Just as in the proof of the functional equation for $\Lambda(f, s)$, use that f is an eigenvector for the Atkin-Lehner operator W_N and (2.2.4) to write $L(f, 1)$ as the sum of two integrals from $i/\sqrt{N}$ to $i\infty$. Then use the calculation

$$\begin{aligned}\overline{2\pi i \int_{i/\sqrt{N}}^{i\infty} \sum_{n=1}^{\infty} a_n e^{2\pi i n z} dz} &= -2\pi i \sum_{n=1}^{\infty} a_n \overline{\int_{i/\sqrt{N}}^{i\infty} e^{2\pi i n z} dz} \\ &= -2\pi i \sum_{n=1}^{\infty} a_n \overline{\frac{1}{2\pi i n} e^{-2\pi n/\sqrt{N}}} \\ &= 2\pi i \sum_{n=1}^{\infty} a_n \frac{1}{2\pi i n} e^{2\pi n/\sqrt{N}}\end{aligned}$$

to see that $\overline{L(f,1)} = L(f,1)$. □

Remark 2.2.9. The BSD conjecture implies that $L(f,1) \geq 0$, but this is unknown (it follows from GRH for $L(f,s)$).

2.2.8 Rationality of $L(A,1)/\Omega_A$

Proposition 2.2.10. *Suppose $A = A_f$ is an elliptic curve. Then $L(A,1)/\Omega_A \in \mathbf{Q}$. More precisely, if n is the smallest multiple of $\{0,\infty\}$ that lies in $\mathrm{H}_1(X_0(N),\mathbf{Z})$ and c_A is the Manin constant of A, then $2n \cdot c_A \cdot L(A,1)/\Omega_A \in \mathbf{Z}$.*

Proof. By the Manin-Drinfeld theorem $n\{0,\infty\} \in \mathrm{H}_1(X_0(N),\mathbf{Z})$, so

$$n \cdot L(f,1) = -n \cdot 2\pi i \cdot \int_0^{i\infty} f(z)dz \in -2\pi i \cdot \mathcal{L}_f = \frac{1}{c_A}\mathcal{L}_\omega.$$

Combining this with Proposition 2.2.8, we see that

$$n \cdot c_A \cdot L(f,1) \in \mathcal{L}_\omega^+,$$

where $\mathcal{L}_\omega^+$ is the submodule fixed by complex conjugation (i.e., $\mathcal{L}_\omega^+ = \mathcal{L} \cap \mathbf{R}$). When the period lattice is not rectangular, Ω_A generates $\mathcal{L}_\omega^+$, and when it is rectangular, $\frac{1}{2}\Omega_A$ generates. Thus $n \cdot c_A \cdot L(f,1)$ is an integer multiple of $\frac{1}{2}\Omega_A$, which proves the proposition. □

Proposition 2.2.10 can be more precise and generalized to abelian varieties $A = A_f^\vee$ attached to newforms. One can also replace n by the order of the image of $(0) - (\infty)$ in $A(\mathbf{Q})$.

Theorem 2.2.11 (Agashe, Stein). *Suppose $f \in S_2(\Gamma_1(N))$ is a newform and let $A = A_f^\vee$ be the abelian variety attached to f. Then we have the following equality of rational numbers:*

$$\frac{|L(A,1)|}{\Omega_A} = \frac{1}{c_\infty \cdot c_A} \cdot [\Phi(H_1(X_1(N),\mathbf{Z}))^+ : \Phi(\mathbf{T}\{0,\infty\})].$$

Note that $L(A,1) \in \mathbf{R}$, so $|L(A,1)| = \pm L(A,1)$, and one expects, of course, that $L(A,1) \geq 0$.

For V and W lattices in an $\mathbf{R}$-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 $\tilde{\Omega}_A$ be 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. □

Remark 2.2.12. Theorem 2.2.11 is false, in general, when A is a quotient of $J_1(N)$ not attached to a single $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-orbit of newforms. It could be modified to handle this more general case, but the generalization seems not to has been written down.

2.3 General Refined Conjecture

Conjecture 2.3.1 (Birch and Swinnerton-Dyer). *Let* $r = \mathrm{ord}_{s=1} L(A, s)$. *Then* r *is the rank of* $A(\mathbf{Q})$, *the group* $\text{Ш}(A)$ *is finite, and*

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

2.4 The Conjecture for Non-Modular Abelian Varieties

Conjecture 2.3.1 can be extended to general abelian varieties over global fields. Here we discuss only the case of a general abelian variety A over $\mathbf{Q}$. We follow the discussion in [Lan91, 95-94] (Lang, Number Theory III), which describes Gross's formulation of the conjecture for abelian varieties over number fields, and to which we refer the reader for more details.

For each prime number ℓ, the ℓ-adic *Tate module* associated to A is

$$\mathrm{Ta}_\ell(A) = \varprojlim_n A(\overline{\mathbf{Q}})[\ell^n].$$

Since $A(\overline{\mathbf{Q}})[\ell^n] \cong (\mathbf{Z}/\ell^n\mathbf{Z})^{2\dim(A)}$, we see that $\mathrm{Ta}_\ell(A)$ is free of rank $2\dim(A)$ as a $\mathbf{Z}_\ell$-module. Also, since the group structure on A is defined over $\mathbf{Q}$, $\mathrm{Ta}_\ell(A)$ comes equipped with an action of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$:

$$\rho_{A,\ell} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{Aut}(\mathrm{Ta}_\ell(A)) \approx \mathrm{GL}_{2d}(\mathbf{Z}_\ell).$$

Suppose p is a prime and let $\ell \neq p$ be another prime. Fix any embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$, and notice that restriction defines a homorphism $r : \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Let $G_p \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ be the image of r. The inertia group $I_p \subset G_p$ is the kernel of the natural surjective reduction map, and we have an exact sequence

$$0 \to I_p \to \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p) \to 0.$$

The Galois group $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$ is isomorphic to $\widehat{\mathbf{Z}}$ with canonical generator $x \mapsto x^p$. Lifting this generator, we obtain an element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, which is well-defined up to an element of I_p. Viewed as an element of $G_p \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, the element Frob_p is well-defined up I_p and our choice of embedding $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_p$. One can show that this implies that $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ is well-defined up to I_p and conjugation by an element of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.

For a G_p-module M, let

$$M^{I_p} = \{x \in M : \sigma(x) = x \text{ all } \sigma \in I_p\}.$$

Because I_p acts trivially on M^{I_p}, the action of the element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on M^{I_p} is well-defined up to conjugation (I_p acts trivially, so the "up to I_p" obstruction vanishes). Thus the characteristic polynomial of Frob_p on M^{I_p} is well-defined, which is why $L_p(A,s)$ is well-defined. The *local L-factor* of $L(A,s)$ at p is

$$L_p(A,s) = \frac{1}{\det\left(I - p^{-s}\,\mathrm{Frob}_p^{-1} \,|\, \mathrm{Hom}_{\mathbf{Z}_\ell}(\mathrm{Ta}_\ell(A), \mathbf{Z}_\ell)^{I_p}\right)}.$$

Definition 2.4.1. $L(A,s) = \displaystyle\prod_{\text{all } p} L_p(A,s)$

For all but finitely many primes $\mathrm{Ta}_\ell(A)^{I_p} = \mathrm{Ta}_\ell(A)$. For example, if $A = A_f$ is attached to a newform $f = \sum a_n q^n$ of level N and $p \nmid \ell \cdot N$, then $\mathrm{Ta}_\ell(A)^{I_p} = \mathrm{Ta}_\ell(A)$. In this case, the Eichler-Shimura relation implies that $L_p(A,s)$ equals $\prod L_p(f_i,s)$, where the $f_i = \sum a_{n,i} q^n$ are the Galois conjugates of f and $L_p(f_i,s) = (1 - a_{p,i} \cdot p^{-s} + p^{1-2s})^{-1}$. The point is that Eichler-Shimura can be used to show that the characteristic polynomial of Frob_p is $\prod_{i=1}^{\dim(A)} (X^2 - a_{p,i}X + p^{1-2s})$.

Theorem 2.4.2. $L(A_f,s) = \prod_{i=1}^{d} L(f_i,s)$.

2.5 Numerical Evidence for the Conjectures

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).

[Cre97] J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[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

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR 87j:11057

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

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR 93a:11048

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

[Maz78] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[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`.