MODELS OF CURVES: THE BIRCH AND SWINNERTON-DYER FORMULA

HOLLY GREEN

1. The statement

Notation 1.1.
- K a number field of discriminant Δ_K
- E/K an elliptic curve
- $|\cdot|_v$ the normalised absolute value on K_v (for v a place of K)
- q_v the cardinality of the residue field of K_v

Conjecture 1 (Birch and Swinnerton-Dyer part II)**.** *Assuming* $Ш_E$ *is finite and that* $L(E,s)$ *has an analytic continuation to* $\mathbb{C}$*, its lead coefficient at* $s=1$ *is*

$$\frac{\#Ш_E \cdot \mathrm{Reg}_E \cdot C_E}{\#E(K)^2_{\mathrm{tors}} \cdot \sqrt{|\Delta_K|}}.$$

Todays focus is the product of local terms C_E, which is model dependent.

Definition 1.2. Fix an non-zero differential ω on E. Then

$$C_E \ := \ \prod_{v\nmid\infty} c_{E/K_v}\Big|\frac{\omega}{\omega_v^0}\Big|_v \cdot \prod_{\substack{v|\infty\\ K_v\cong\mathbb{R}}} \int_{E(K_v)} |\omega|_v \cdot \prod_{\substack{v|\infty\\ K_v\cong\mathbb{C}}} \int_{E(K_v)} |\omega\wedge\bar{\omega}| \ = \ \prod_v C_{E/K_v}(\omega)$$

where $c_{E/K_v} = [E(K_v):E_0(K_v)]$ is a *Tamagawa number* and ω_v^0 is a *Néron differential.*

If $E: y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ is a minimal Weierstrass equation over K_v, then

$$\omega_v^0 = \pm\frac{dx}{2y+a_1x+a_3}.$$

Example 1.3. Let $E/\mathbb{Q}: y^2 = x^3+17^{12}$, $\Delta_E = -2^3\cdot 3^3\cdot 17^{24}$. This is minimal over $\mathbb{Q}_p$, and so $\omega_p^0 = \frac{dx}{2y}$, whenever $p\neq 17$.

Let $y = 17^6 Y$, $x = 17^4 X$. Then $E: Y^2 = X^3+1$ is minimal over $\mathbb{Q}_{17}$ and

$$\omega_{17}^0 = \frac{dX}{2Y} = 17^2\frac{dx}{2y}.$$

Remark 1.4. When $K=\mathbb{Q}$, E has a global minimal Weierstrass equation (e.g. $E: y^2 = x^3+1$ in the example above). Therefore, there's a canonical choice of ω which gives

$$C_E = \prod_p c_{E/\mathbb{Q}_p}\cdot \int_{E(\mathbb{R})} |\omega|.$$

Remark 1.5. Each local term $C_{E/K_v}(\omega)$ depends on the choice of ω, but C_E doesn't. To see this: for $\alpha\in K^\times$, $C_{E/K_v}(\alpha\omega) = |\alpha|_v C_{E/K_v}(\omega)$ and $\prod_v |\alpha|_v = 1$.

Date: March 6th 2024.

Where does this term come from? (From my understanding).

Recall that $L(E,s) = \prod_{v\nmid\infty} L(E, q_v^{-s})^{-1}$. The non-Archimedean terms appearing in the Birch and Swinnerton-Dyer conjecture arise naturally as v-adic integrals.

Lemma 1.6 (Tate, [5] Theorem 5.2)**.** *Given $v \nmid \infty$,*

$$L_v(E, q_v^{-1})^{-1} \int_{E(K_v)} |\omega^0|_v = c_{E/K_v} \Big| \frac{\omega}{\omega_v^0} \Big|_v.$$

In the 1950's, before the formulation of the Birch and Swinnerton-Dyer conjecture, the Tamagawa number of a semisimple algebraic group was receiving a lot of attention. It is possible that Birch and Swinnerton-Dyer tried to mimic this construction for elliptic curves as follows:

$$\prod_v \int_{E(K_v)} |\omega|_v \underset{\text{add convergence factors}}{\overset{\text{doesn't converge}}{\rightsquigarrow}} \prod_{v\nmid\infty} L_v(E, q_v^{-1})^{-1} \int_{E(K_v)} |\omega|_v \cdot \prod_{v|\infty} \int_{E(K_v)} |\omega|_v = C_E.$$

It's worth noting that when $v \nmid 2\Delta_E\infty$ (i.e. E/K_v has good reduction), Lemma 1.6 reduces to

$$\left(\frac{\#\tilde{E}(k_v)}{q_v} \right)^{-1} \int_{E(K_v)} |\omega^0|_v = \Big| \frac{\omega}{\omega_v^0} \Big|_v$$

where the factors $\#\tilde{E}(k_v)/q_v$ were the quantities initially of interest to Birch and Swinnerton-Dyer.

2. Tamagawa numbers

Notation 2.1.
- $\mathcal{K}$ a non-Archimedean local field, e.g. $\mathbb{Q}_p$
- $\mathcal{O}_\mathcal{K}$ ring of integers, e.g. $\mathbb{Z}_p$
- k residue field, e.g. $\mathbb{F}_p$, of cardinality q
- $A/\mathcal{K}$ an abelian variety; $C/\mathcal{K}$ a smooth, proper, geometrically connected curve

The Birch and Swinnerton-Dyer conjecture can be stated more generally for abelian varieties (due to Tate). The product of local terms has a natural generalisation, and at non-Archimedean places the terms are computed from the 'Néron model' for A (see [4, Chapter IV, §5] for a definition) – the correct analogue of a minimal regular model for an elliptic curve.

Definition 2.2. A *Néron model* of A is a smooth, separated, finite type group scheme $\mathcal{A}/\mathcal{O}_\mathcal{K}$ with generic fibre A, satisfying (the Néron mapping property):

if $\mathcal{Y}$ is a smooth, separated $\mathcal{O}_\mathcal{K}$-scheme, then any $\mathcal{K}$-morphism $\mathcal{Y}_\mathcal{K} \to A$ can be extended uniquely to an $\mathcal{O}_\mathcal{K}$-morphism $\mathcal{Y} \to \mathcal{A}$.

Definition 2.3. Let $\mathcal{A}/\mathcal{O}_\mathcal{K}$ denote a Néron model for A. Let $\Phi_A := \mathcal{A}_s/\mathcal{A}_s^0$ (the Néron component group/the component group scheme of the special fibre of $\mathcal{A}$). Then

$$c_{A/\mathcal{K}} := \#\Phi_A(k) = \#\Phi_A(\bar{k})^{\mathrm{Gal}(\bar{k}/k)}.$$

Remark 2.4. (1). Néron models always exist.

(2). The Néron model of $E/\mathcal{K}$ is the smooth part of its minimal regular model and $\Phi_E(k) \cong E(\mathcal{K})/E_0(\mathcal{K})$ (Néron, see [4]). We therefore recover the previous definition of the Tamagawa number, i.e. $c_{E/\mathcal{K}} = [E(\mathcal{K}) : E_0(\mathcal{K})]$.

For higher dimensional A, it is infeasible to compute defining equations in projective space and so the computation of a Néron model is out of scope.

If $A = \operatorname{Jac} C$, it turns out that the Néron model can be described in terms of the minimal regular model of C (a theorem of Raynaud, [3, Theorem 9.5.4]). This allows us to compute the Tamagawa number for such an A as follows.

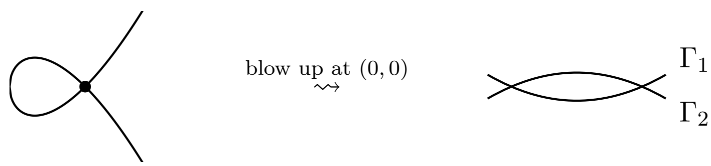
Theorem 2.5 ([2] Theorem 1.1)**.** *Let $\mathcal{C}/\mathcal{O}_\mathcal{K}$ be a minimal regular model for C. Write $I = \{\Gamma_1, \ldots, \Gamma_n\}$ for the irreducible components of $\mathcal{C}_s$ base-changed to $\bar{k}$ and $m_i \in \mathbb{N}$ for the multiplicity of Γ_i. Define (extending linearly)*

$$\alpha : \mathbb{Z}^I \longrightarrow \mathbb{Z}^I \qquad\qquad \beta : \mathbb{Z}^I \longrightarrow \mathbb{Z}$$
$$\Gamma_i \longmapsto \textstyle\sum_{1 \le j \le n} (\Gamma_i \cdot \Gamma_j)\Gamma_j \qquad\qquad \Gamma_i \longmapsto m_i.$$

Then $\Phi_{\operatorname{Jac} C}(\bar{k}) \cong \ker(\beta)/\operatorname{im}(\alpha)$. In particular,

$$c_{\operatorname{Jac} C/\mathcal{K}} = \#\ker(\beta)/\operatorname{im}(\alpha)^{\operatorname{Gal}(\bar{k}/k)}.$$

Example 2.6. (Elliptic curve type I_2) Let $E : y^2 = x^3 + 2x^2 + p^2$ over $\mathbb{Q}_p$ for p odd. This is a minimal Weierstrass equation for E whose reduction is a nodal cubic curve. Blowing up once here yields the minimal regular model:

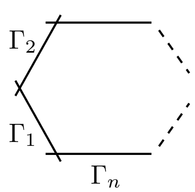


Write $I = \{\Gamma_1, \Gamma_2\}$, $m_1 = m_2 = 1$ and $(\Gamma_1 \cdot \Gamma_2) = (\Gamma_2 \cdot \Gamma_1) = 2$ and $(\Gamma_1 \cdot \Gamma_1) = (\Gamma_1 \cdot \Gamma_2) = -2$. Then $\ker(\beta) = \langle \Gamma_2 - \Gamma_1 \rangle_\mathbb{Z}$ and $\operatorname{im}(\alpha) = \langle 2(\Gamma_2 - \Gamma_1) \rangle_\mathbb{Z}$ (since $\alpha(\Gamma_1) = 2(\Gamma_2 - \Gamma_1) = -\alpha(\Gamma_2)$. Therefore,

$$\Phi(\bar{k}) \cong \mathbb{Z}/2\mathbb{Z} = \{0, \Gamma_2 - \Gamma_1\}.$$

- If $\operatorname{Gal}(\bar{k}/k)$ acts trivially (for the given curve this corresponds to $\left(\frac{2}{p}\right) = +1$), then $c_{\operatorname{Jac} C/\mathcal{K}} = 2$.
- If $\operatorname{Gal}(\bar{k}/k)$ acts non-trivially, (for the given curve this corresponds to $\left(\frac{2}{p}\right) = -1$), then $c_{\operatorname{Jac} C/\mathcal{K}} = 2$ too.

Example 2.7. (Elliptic curve type I_n, $n \ge 3$)



Here $I = \{\Gamma_1, \ldots, \Gamma_n\}$. $\forall i$, we have $m_i = 1$. Then

$$\begin{aligned} \ker(\beta) &= \langle \Gamma_1 - \Gamma_2,\, \ldots,\, \Gamma_{n-1} - \Gamma_n \rangle_\mathbb{Z} \\ &= \langle \Gamma_1 - 2\Gamma_2 + \Gamma_3,\, \ldots,\, \Gamma_{n-2} - 2\Gamma_{n-1} + \Gamma_n,\, \Gamma_{n-1} - \Gamma_n \rangle_\mathbb{Z} \end{aligned}$$

Write M for the intersection pairing matrix. Then $\alpha : \mathbf{a} = (a_1, \ldots, a_n) \to \mathbf{a} \cdot M$.

M has $n-1$ linearly independent columns and we can show that $\operatorname{im}(\alpha)$ is

$$\langle \Gamma_1 - 2\Gamma_2 + \Gamma_3,\, \ldots,\, \Gamma_{n-2} - 2\Gamma_{n-1} + \Gamma_n,\, n(\Gamma_{n-1} - \Gamma_n) \rangle_\mathbb{Z}.$$

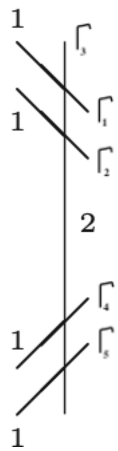
Therefore $\Phi(\bar{k}) \cong \mathbb{Z}/n\mathbb{Z} = \{i(\Gamma_{n-1} - \Gamma_n) : i = 0, \ldots n\}$.

- If $\operatorname{Gal}(\bar{k}/k)$ acts trivially, then $c_{\operatorname{Jac} C/\mathcal{K}} = n$.
- If $\operatorname{Gal}(\bar{k}/k)$ acts non-trivially, then when n is odd $\Rightarrow$ $c_{\operatorname{Jac} C/\mathcal{K}} = 1$ and when n is even $\Rightarrow$ $c_{\operatorname{Jac} C/\mathcal{K}} = 2$.

$$M = \begin{bmatrix} -2 & 1 & 0 & \cdots & 0 & 1 \\ 1 & -2 & 1 & \ddots & \ddots & 0 \\ 0 & 1 & -2 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 & 0 \\ 0 & \ddots & \ddots & 1 & -2 & 1 \\ 1 & 0 & \cdots & 0 & 1 & -2 \end{bmatrix}.$$

Example 2.8. (Elliptic curve type I_n^*)

Let $n = 0$, i.e. potential good reduction: acquires good reduction over a field extension.



Here $I = \{\Gamma_1, \Gamma_2, \Gamma_3, \Gamma_4, \Gamma_5\}$. $\forall i \neq 3$ we have $m_i = 1$ and $m_3 = 2$. Clearly,

$$\ker(\beta) = \langle \Gamma_1 \overset{\lambda_1}{-} \Gamma_2, \Gamma_2 \overset{\lambda_2}{-} \Gamma_4, \Gamma_4 \overset{\lambda_3}{-} \Gamma_5, \Gamma_3 \overset{\lambda_4}{-} 2\Gamma_1 \rangle_{\mathbb{Z}} = \langle \lambda_1, \lambda_2, \lambda_1 + \lambda_3, \lambda_4 \rangle_{\mathbb{Z}}.$$

The intersection pairing matrix is

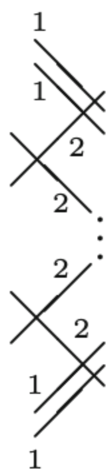
$$M = \begin{bmatrix} -2 & 0 & 1 & 0 & 0 \\ 0 & -2 & 1 & 0 & 0 \\ 1 & 1 & -2 & 1 & 1 \\ 0 & 0 & 1 & -2 & 0 \\ 0 & 0 & 1 & 0 & -2 \end{bmatrix}$$

which has 4 linearly independent columns. We can show that $\mathrm{im}(\alpha)$ is

$\langle \lambda_4, 2\lambda_1 + \lambda_4, -3\lambda_1 - 2\lambda_2 - \lambda_3 - 2\lambda_4, 2\lambda_1 + 2\lambda_2 + \lambda_4 \rangle_{\mathbb{Z}} = \langle \lambda_4, 2\lambda_1, \lambda_1 + \lambda_3, 2\lambda_2 \rangle_{\mathbb{Z}}$.

Therefore $\Phi(\bar{k}) \cong (\mathbb{Z}/2\mathbb{Z})^2$.

Let $n \geq 1$, i.e. potential multiplicative reduction: acquires multiplicative reduction over a field extension.



A similar computation gives that

$$\Phi(\bar{k}) \cong \begin{cases} \mathbb{Z}/4\mathbb{Z} & n \text{ odd,} \\ (\mathbb{Z}/2\mathbb{Z})^2 & n \text{ even.} \end{cases}$$

References

[1] B. J. Birch, H. P. Swinnerton-Dyer. *Notes on elliptic curves. II.* (1965).
[2] S. Bosch, Q. Liu. *Rational points of the group of components of a Néron model.* (1999).
[3] S. Bosch, W. Lütkebohmert, M. Raynaud. *Néron models.* (1990).
[4] J. Silverman. *Advanced topics in the arithmetic of elliptic curves.* (1994).
[5] J. Tate. *Algorithm for determining the type of a singular fiber in an elliptic pencil.* (1975).