Periods of quadratic twists of elliptic curves

Vivek Pal*

with an appendix by Amod Agashe†

Abstract

In this paper we prove a relation between the period of an elliptic curve and the period of its real and imaginary quadratic twists. This relation is often misstated in the literature.

1 Introduction

One of the central conjectures in Number Theory is the Birch and Swinnerton-Dyer Conjecture, which predicts how one can obtain arithmetic information from the L-function. A simpler questions is to ask:

> (*) if an elliptic curve satisfies the Birch and Swinnerton-Dyer Conjecture then will its (quadratic) twist also satisfy the Birch and Swinnerton-Dyer Conjecture.

Part two of the Birch and Swinnerton-Dyer Conjecture involves many elliptic curve invariants, namely the order of the Tate-Shafarevich group, the period and the order of the torsion subgroup among other important invariants. In this paper we relate the period of an elliptic curve with the period of its quadratic twists. A relation between the orders of the torsion subgroups has already been proven in [Kwo97]. If a similar result can be drawn for all of the other elliptic curve invariants involved in Part II of the Birch and Swinnerton-Dyer Conjecture then one can prove idea (*). Furthermore, a relation between the arithmetic component group and the regulator, of an elliptic curve and its twist would provide a conjecture for the relation between the order of the Shafarevich-Tate group for an elliptic curve and its twist.

One advantage of idea (*) comes from the fact that quadratic twists of elliptic curves have very different ranks from the original curve. Currently Part two of the Birch and Swinnerton-Dyer Conjecture is only known to be true for families of elliptic curves, usually of low rank; using twists one could possibly extend these results to many different ranks.

*Florida State University, the author was funded by the FSU Office of National Fellowships

†Amod Agashe was supported by the National Security Agency Grant number Hg8230-10-1-0208

In general if F is an elliptic curve, then we denote the invariant differential on F by $\omega(F)$. We will call a global minimal Weierstrass equation of an elliptic curve simply a minimal equation or minimal model, and denote a minimal model of an elliptic curve F by $F_{\min}$.

Let E be an elliptic curve. We use the Birch and Swinnerton-Dyer definition of the period. Recall that this period, denoted by $\Omega(E)$, is defined as:

$$\Omega(E) := \int_{E_{\min}(\mathbb{R})} |\omega(E_{\min})|.$$

Also, recall that the imaginary period, defined up to a sign, is

$$\Omega^-(E) := \int_{\gamma^-} \omega(E_{\min}),$$

where γ^- is a generator of $H_1(E_{\min}, \mathbb{Z})^-$, which is the subgroup of elements in $H_1(E_{\min}, \mathbb{Z})$ which are negated by complex conjugation.

Furthermore, recall that the quadratic twist of an elliptic curve E by a non-zero integer d, denoted by E^d, is defined as an elliptic curve which is isomorphic to E over $\mathbb{Q}(\sqrt{d})$ but not over $\mathbb{Q}$. Hence we can assume that d is square-free. We also know that E^d is unique up to isomorphism.

The main result of this paper is then

Main Result 1.1. *Let E be an elliptic curve and let E^d denote its quadratic twist by a square-free integer d. Then the periods of E and E^d are related as follows:*
If $d > 0$, then

$$\Omega(E^d) = \frac{\tilde{u}}{\sqrt{d}}\Omega(E),$$

and if $d < 0$, then up to a sign,

$$\Omega(E^d) = \frac{\tilde{u}}{\sqrt{d}}c_\infty(E^d)\Omega^-(E),$$

where $\tilde{u}$ is a rational number such that $2\tilde{u} \in \mathbb{Z}$; it depends on E and d, and is defined explicitly in Proposition 2.5 (the elliptic curve E in Proposition 2.5 should be taken as a minimal model of the E in this theorem).

The theorem above is proved as Theorem 3.2 below.

Remark 1.2. $\tilde{u}$ is not always 1 and $2\tilde{u}$ can be divisible by an odd prime number. In Section 4, we give an example where $\tilde{u}$ is 5 and an example where $\tilde{u}$ is 7. Also, in the appendix, there is an example of an optimal elliptic curve for which $\tilde{u}$ has positive 3-adic valuation.

A result similar to the second case of the theorem above was derived in [Aga10, Lemma 2.1] for elliptic curves in short Weierstrass form using an assumption on which primes one can twist by. The result here is proved without restrictions.

The main result of this paper allows for a weaker hypothesis for several results in [Aga10]; the details are discussed in the appendix.

We would like to remark that the formulas in the Main Result have been stated incorrectly in the literature. For example, Amod Agashe informed the author that they are quoted without $\tilde{u}$ as formula (12) on p. 463 in the proof of Corollary 3 in [OS98]; he also mentioned that the proof of Corollary 3 in [OS98] still works even after the formula is corrected to include $\tilde{u}$.

The author would like to thank Amod Agashe for suggesting this problem and for his help in revising several drafts of this paper. Furthermore the reference to Connell's book [Con08] was mentioned to the author by Amod Agashe, who in turn heard about it from Randy Heaton.

2 Quadratic Twists and Minimal Models

First we recall some useful facts. An elliptic curve over $\mathbb{Q}$ can be described in the following general Weierstrass form:

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

with $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$.

In this paper, by an elliptic curve, we mean a curve given by a Weierstrass equation. An elliptic curve will be called minimal if its Weierstrass equation is minimal. Let E be an elliptic curve, and let $\Delta(E), j(E), c_4(E)$ and $c_6(E)$ be the usual Weierstrass invariants of the elliptic curve E. Then the signature of the elliptic curve E is the triple $c_4(E), c_6(E), \Delta(E)$. If p is a prime, then letting v_p denote the standard p-adic valuation, the p-adic signature of E is the triple $v_p(c_4(E)), v_p(c_6(E)), v_p(\Delta(E))$.

Remark 2.1. A transformation $E \to E'$ of elliptic curves over $\mathbb{Q}$ preserving the Weierstrass equation and the point at infinity is given by:

$$x = u^2x' + r \text{ and } y = u^3y' + u^2sx' + t,$$

for some $u, r, s, t \in \mathbb{Q}$. We will often abbreviate this transformation as the ordered tuple $[u, r, s, t]$. Such a transformation has the following useful properties:

1. $u^4c_4(E') = c_4(E)$
2. $u^6c_6(E') = c_6(E)$
3. $u^{12}\Delta(E') = \Delta(E)$
4. $j(E') = j(E)$
5. $\omega(E') = u\omega(E)$

The above facts can be found in any standard book on elliptic curves, for example see Silverman [Sil92].

Since the period of an elliptic curve depends only on the isomorphism class, for the purpose of proving Main Result 1.1 or for computing $\Omega(E)$, we can assume that E is a minimal model, i.e. $E = E_{\min}$. So henceforth, let E be an elliptic curve given by the minimal equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{E}$$

Lemma 2.2 (Connell)**.** *Let d be a square-free integer. Then a Weierstrass equation for E^d is:*

$$\begin{aligned} &y^2 + a_1xy + a_3y = \\ &\quad = x^3 + \left(a_2d + a_1^2\frac{d-1}{4}\right)x^2 + \left(a_4d^2 + a_1a_3\frac{d^2-1}{2}\right)x + \left(a_6d^3 + a_3^2\frac{d^3-1}{4}\right). \end{aligned} \tag{E^d}$$

Proof. See [Con08, Proposition 4.3.2] and the paragraph preceding it. □

Remark 2.3. The signature for elliptic curve (E^d) is: $c_4(E^d) = c_4(E)\cdot d^2$, $c_6(E^d) = c_6(E)\cdot d^3$ and $\Delta(E^d) = \Delta(E)\cdot d^6$. Let $\alpha = \sqrt{1/d}$. Then the transformation from E to E^d is:

$$\begin{cases} x = \alpha^2 x' \\ y = \alpha^3 y' + \dfrac{a_1\alpha^2(\alpha-1)}{2}x' + \dfrac{a_3(\alpha^3-1)}{2}. \end{cases}$$

Next we recall a proposition from Connell which is displayed below for convenience. It describes $v_p(\Delta)$ for a minimal model of the twist for each prime p.

Proposition 2.4 (Connell)**.** *Recall that E is a minimal elliptic curve over $\mathbb{Q}$ and E^d is its quadratic twist by a square-free integer d. Let Δ be the discriminant of E, let Δ' be the discriminant of E^d_{min}, and for every valuation v on $\mathbb{Z}$ let $\lambda_v = \min\{3v(c_4(E)), 2v(c_6(E)), v(\Delta)\}$. If p is a prime number, then let v_p denote the standard p-adic valuation. Then*

1. *If p is an odd prime divisor of d then:*
   (a) *If $\lambda_{v_p} < 6$ or if $p = 3$ and $v_p(c_6(E)) = 5$, then $v_p(\Delta') = v_p(\Delta) + 6$.*
   (b) *Otherwise $v_p(\Delta') = v_p(\Delta) - 6$.*

   If p is an odd prime not dividing d, then $v_p(\Delta') = v_p(\Delta)$.
2. *If $p = 2$ then:*
   (a) *If $d \equiv 1 \mod 4$, then $v_2(\Delta') = v_2(\Delta)$.*
   (b) *If $d \equiv 3 \mod 4$, then*

i. *If the 2-adic signature of E is $0, 0, c$ $(c \geq 0)$ or $a, 3, 0$ $(4 \leq a \leq \infty)$, then $v_2(\Delta') = v_2(\Delta) + 12$.*

ii. *If the 2-adic signature of E is $4, 6, c$ $(c \geq 6)$ or $a, 9, 12$ $(7 \leq a \leq \infty)$, then $v_2(\Delta') = v_2(\Delta) - 12$.*

iii. *Otherwise $v_2(\Delta') = v_2(\Delta)$.*

(c) *If $d \equiv 2 \mod 4$, let $w = d/2$ then*

i. *If the 2-adic signature of E is $0, 0, c$ $(c \geq 0)$, then $v_2(\Delta') = v_2(\Delta) + 18$.*

ii. *If the 2-adic signature of E is $6, 9, c$ with $(c \geq 18)$ and $2^{-9}c_6(E)w \equiv -1 \mod 4$, then $v_2(\Delta') = v_2(\Delta) - 18$.*

iii. *If $v_2(c_4(E)) = 4, 5$ or $v_2(c_6(E)) = 3, 5, 7$ or the 2-adic signature of E is $a, 6, 6$ with $(a \geq 6)$ and $2^{-6}c_6(E)w \equiv -1 \mod 4$, then $v_2(\Delta') = v_2(\Delta) + 6$.*

iv. *Otherwise $v_2(\Delta') = v_2(\Delta) - 6$.*

Proof. See [Con08, 5.7.3] . □

Proposition 2.5. *Recall that E is a minimal elliptic curve over $\mathbb{Q}$ and E^d is its quadratic twist by a square-free integer d. Let Δ be the discriminant of E, let Δ' be the discriminant of E^d_{min}, and for every valuation v on $\mathbb{Z}$, let $\lambda_v = \min\{3v(c_4(E)), 2v(c_6(E)), v(\Delta)\}$. If p is a prime number, then let v_p denote the standard p-adic valuation. Define u_p for all primes p, as follows (the cases correspond exactly to the cases of Proposition 2.4):*

1. *If p is an odd prime divisor of d, then:*

   (a) *If $\lambda_{v_p} < 6$ or if $p = 3$ and $v_p(c_6(E)) = 5$, then $u_p = 1$.*

   (b) *Otherwise $u_p = p$.*

   If p is an odd prime not dividing d, then $u_p = 1$.

2. *If $p = 2$ then:*

   (a) *If $d \equiv 1 \mod 4$, then $u_2 = 1$.*

   (b) *If $d \equiv 3 \mod 4$, then*

   i. *If the 2-adic signature of E is $0, 0, c$ $(c \geq 0)$ or $a, 3, 0$ $(4 \leq a \leq \infty)$, then $u_2 = 1/2$.*

   ii. *If the 2-adic signature of E is $4, 6, c$ $(c \geq 6)$ or $a, 9, 12$ $(7 \leq a \leq \infty)$, then $u_2 = 2$.*

   iii. *Otherwise $u_2 = 1$.*

   (c) *If $d \equiv 2 \mod 4$, let $w = d/2$, then*

   i. *If the 2-adic signature of E is $0, 0, c$ $(c \geq 0)$, then $u_2 = 1/2$.*

   ii. *If the 2-adic signature of E is $6, 9, c$ with $(c \geq 18)$ and $2^{-9}c_6(E)w \equiv -1 \mod 4$, then $u_2 = 4$.*

iii. *If* $v_2(c_4(E)) = 4, 5$ *or* $v_2(c_6(E)) = 3, 5, 7$ *or the 2-adic signature of* E *is* $a, 6, 6$ *with* $(a \geq 6)$ *and* $2^{-6}c_6(E)w \equiv -1 \mod 4$*, then* $u_2 = 1$.

iv. *Otherwise* $u_2 = 2$.

Let $\tilde{u} = \prod_p u_p$. *Then there exist* $r, s, t \in \mathbb{Q}$ *such that the transformation* $[\tilde{u}, r, s, t]$ *will transform equation* E^d *to a minimal model.*

Proof. The idea of the proof is to apply Proposition 2.4 to the elliptic curve E and then to find a transformation sending E^d to a minimal model.

We claim that $[\tilde{u}, 0, 0, 0]$ transforms E^d to a curve with the correct minimal discriminant. This follows on a case by case basis using Proposition 2.4, Remark 2.3, and Remark 2.1. Take for example the case $1(b)$: this is the case where by Proposition 2.4, $v_p(\Delta(E^d_{\min})) = v_p(\Delta(E)) - 6$. By Remark 2.3, we know that $v_p(\Delta(E^d)) = v_p(d^6\Delta(E)) = v_p(\Delta(E)) + 6$, since here p divides d (and d is square-free). Therefore $v_p(\Delta(E^d_{\min})) = v_p(\Delta(E^d)) - 12$. The transformation which will decrease the valuation of the discriminant by 12 is $[p, 0, 0, 0]$ by Remark 2.1, hence proving the Proposition in this case. Applying a similar process to the other cases will derive the respective u_p. Since the u_ps are coprime to each other, composing the transformations $[u_p, 0, 0, 0]$ will give the transformation $[\tilde{u}, 0, 0, 0]$. Thus the transformation, $[\tilde{u}, 0, 0, 0]$, will send E^d to an elliptic curve E' with the correct minimal discriminant, but which may not have integer coefficients.

We will now show that we can find $r, s, t \in \mathbb{R}$ so that the transformation $[\tilde{u}, r, s, t]$ applied to E^d also gives an integral model for E^d, and therefore a minimal model. Since $E^d_{\min} \cong E'$, we know that there is a transformation $[u, r, s, t]$ that sends E' to $E^d_{\min}$ [Sil92, Cor. 7.8.3]. By comparing discriminants we see that $u = \pm 1$; we can assume $u = 1$ since we can compose this morphism with $[-1, 0, 0, 0]$ to change the sign of u. Composing the morphism $[\tilde{u}, 0, 0, 0]$ with $[1, r, s, t]$ gives the desired morphism, $[\tilde{u}, r, s, t]$, sending E^d to $E^d_{\min}$. □

For the benefit of the reader we remark that often the transformation $[\tilde{u}, 0, 0, 0]$ will in fact transform E^d to an equation with integral coefficients, hence a minimal model, but for our purposes only the u coefficient of the transformation will play a role later.

Corollary 2.6. *We use the notation of Proposition 2.5. Suppose* d *is coprime to* Δ. *Then* $\tilde{u}$ *is a power of* 2. *Moreover if* $d \equiv 1 \mod 4$*, then* $\tilde{u} = 1$.

Proof. Let p be an odd prime. If p does not divide d, then by Proposition 2.5, $u_p = 1$. If p divides d, then $v_p(\Delta) = 0$ since d is coprime to Δ, and so $\lambda_{v_p} < 6$, and thus by Proposition 2.5, $u_p = 1$. In both cases, $u_p = 1$ for odd primes, which proves the first claim of the corollary. If $d \equiv 1 \mod 4$, then by Case 2(a) Proposition 2.5 $u_2 = 1$. The second claim of the corollary follows, since $\tilde{u} = \prod_p u_p = 1$ □

Definition 2.7. We define $E^d_{\min}$ to be the specific minimal model of elliptic curve E^d obtained via Proposition 2.5.

3 Periods

We first prove a relation between the invariant differentials of E and $E^d_{\min}$ and then use this relation to prove the desired relation between the periods in our main result.

Lemma 3.1. *We have:*

$$\omega(E^d) = \frac{\omega(E)}{\sqrt{d}}$$

and

$$\omega(E^d_{min}) = \frac{\tilde{u} \cdot \omega(E)}{\sqrt{d}}.$$

Proof. Using the properties listed in Remarks 2.1 and 2.3 regarding transformations, the transformation taking E to E^d has $u = \alpha = \sqrt{1/d}$. Then by Remark 2.1, $\omega(E^d) = \frac{\omega(E)}{\sqrt{d}}$. By Proposition 2.5, the transformation taking E^d to $E^d_{\min}$ has $u = \tilde{u}$. Then $\omega(E^d_{\min}) = \tilde{u} \cdot \omega(E^d) = \frac{\tilde{u} \cdot \omega(E)}{\sqrt{d}}$. □

We now prove the main result relating the periods.

Theorem 3.2. *Recall that E is a minimal elliptic curve and E^d is its quadratic twist by d. Then the periods of E and E^d are related as follows*
If $d > 0$, then

$$\Omega(E^d) = \frac{\tilde{u}}{\sqrt{d}}\Omega(E).$$

If $d < 0$, then up to a sign,

$$\Omega(E^d) = \frac{\tilde{u}}{\sqrt{d}} c_\infty(E^d)\Omega^-(E),$$

where $c_\infty(E)$ is the number of connected components of $E(\mathbb{R})$.

Proof. We first prove the formula for $d > 0$:

As remarked in the proof of Lemma 3.1, the transformation that takes E to E^d takes $\omega(E)$ to $\sqrt{d}\omega(E^d)$. This transformation sends $E(\mathbb{R})$ bijectively to $E^d(\mathbb{R})$ because the transformation and its inverse are defined over $\mathbb{R}$ (since $d > 0$). Then:

$$\int_{E(\mathbb{R})} |\omega(E)| = \sqrt{d} \int_{E^d(\mathbb{R})} |\omega(E^d)|. \tag{1}$$

Using a similar argument we see that:

$$\int_{E^d(\mathbb{R})} |\omega(E^d)| = \frac{1}{\tilde{u}} \int_{E^d_{\min}(\mathbb{R})} |\omega(E^d_{\min})|. \tag{2}$$

Then from equation (1) and equation (2) we see that:

$$\Omega(E) = \int_{E(\mathbb{R})} |\omega(E)| = \frac{\sqrt{d}}{\tilde{u}}\Omega(E^d).$$

Next we prove the formula for $d < 0$:
We follow the technique used in the proof of [Aga10, Lemma 2.1]. Let $P = (x, y) \in E(\mathbb{R})$ and let σ be the complex conjugation map; then $\sigma(P) = P$. The inverse of the map described in Remark 2.3 is given by:

$$\begin{cases} x' = \dfrac{1}{\alpha^2}x \\ y' = \dfrac{1}{\alpha^3}y - \dfrac{a_1}{2}\left(\dfrac{1}{\alpha^2} - \dfrac{1}{\alpha^3}\right)x - \dfrac{a_3}{2}\left(1 - \dfrac{1}{\alpha^3}\right) \end{cases}$$

where $\alpha = \sqrt{1/d}$. Let T be this map, $T : E^d \to E$.

Claim: $\sigma(T(P)) = -T(P)$.

Proof.

$$\sigma(T(P)) = \sigma\left(\left(\frac{1}{\alpha^2}x, \frac{1}{\alpha^3}y - \frac{a_1}{2}\left(\frac{1}{\alpha^2} - \frac{1}{\alpha^3}\right)x - \frac{a_3}{2}\left(1 - \frac{1}{\alpha^3}\right)\right)\right) =$$

$$= \left(\frac{1}{\alpha^2}x, \frac{-1}{\alpha^3}y - \frac{a_1}{2}\left(\frac{1}{\alpha^2} + \frac{1}{\alpha^3}\right)x - \frac{a_3}{2}\left(1 + \frac{1}{\alpha^3}\right)\right).$$

Using the definition of the negative of a point on an elliptic curve, given in [Sil92, III.2.3]:

$$-T(P) = -\left(\frac{1}{\alpha^2}x, \frac{1}{\alpha^3}y - \frac{a_1}{2}\left(\frac{1}{\alpha^2} - \frac{1}{\alpha^3}\right)x - \frac{a_3}{2}\left(1 - \frac{1}{\alpha^3}\right)\right) =$$

$$= \left(\frac{1}{\alpha^2}x, -\left(\frac{1}{\alpha^3}y - \frac{a_1}{2}\left(\frac{1}{\alpha^2} - \frac{1}{\alpha^3}\right)x - \frac{a_3}{2}\left(1 - \frac{1}{\alpha^3}\right)\right) - a_1\left(\frac{1}{\alpha^2}x\right) - a_3\right)$$

$$= \left(\frac{1}{\alpha^2}x, \frac{-1}{\alpha^3}y - \frac{a_1}{2}\left(\frac{1}{\alpha^2} + \frac{1}{\alpha^3}\right)x - \frac{a_3}{2}\left(1 + \frac{1}{\alpha^3}\right)\right).$$

Then we see that $\sigma(T(P)) = -T(P)$. □

Thus T gives a homeomorphism from $E^d(\mathbb{R})$ to $E(\mathbb{C})^-$, where $E(\mathbb{C})^-$ is the subgroup of points not fixed under complex conjugation. If G is a Lie group, then let G_0 denote the connected component of G containing the identity. Then T also induces a homeomorphism from $E^d(\mathbb{R})_0$ to $E(\mathbb{C})_0^-$. In particular, T gives an isomorphism from $H_1(E^d(\mathbb{R})_0, \mathbb{Z})$ to $H_1(E(\mathbb{C})_0^-, \mathbb{Z})$. By Lemma 4.4 in [AS05], the natural map from $H_1(E^d(\mathbb{R})_0, \mathbb{Z})$ to $H_1(E^d(\mathbb{C}), \mathbb{Z})^+$ is an isomorphism, and by Lemma 5.2 from the appendix, the natural map from $H_1(E^d(\mathbb{C})_0^-, \mathbb{Z})$ to $H_1(E^d(\mathbb{C}), \mathbb{Z})^-$ is an isomorphism. Let γ be a generator of $H_1(E^d(\mathbb{C}), \mathbb{Z})^+$. Then from the statements above, one sees that $T(\gamma)$ is in $H_1(E(\mathbb{C}), \mathbb{Z})^-$ and generates it.

Then it follows that

$$\int_\gamma \omega(E^d) = \int_{T(\gamma)} T(\omega(E^d)) = \frac{1}{\sqrt{d}} \int_{T(\gamma)} \omega(E) = \frac{1}{\sqrt{d}} \Omega^-(E), \tag{3}$$

where the last equality is up to a sign.

Similar to equation (2) we have,

$$\int_{E^d(\mathbb{R})} \omega(E^d) = \frac{1}{\tilde{u}} \int_{E^d_{\min}(\mathbb{R})} \omega(E^d_{\min}), \tag{4}$$

since the transformation in this integral involve only real numbers and thus takes $E^d(\mathbb{R})$ to $E^d_{\min}(\mathbb{R})$.

Using equation (5) from the appendix, equation (3), equation (4), and Lemma 5.1 from the appendix, we see that up to a sign:

$$\begin{aligned} \Omega(E^d) = \int_{E^d_{\min}(\mathbb{R})} \omega(E^d_{\min}) &= \tilde{u} \int_{E^d(\mathbb{R})} \omega(E^d) \\ &= \tilde{u} \cdot c_\infty(E^d) \int_\gamma \omega(E^d) = \frac{\tilde{u}}{\sqrt{d}} c_\infty(E^d) \Omega^-(E), \end{aligned}$$

as was to be shown. □

4 Examples

4.1 Real quadratic twist

Using Sage and GP/Pari we were able to find the following example in which the $\tilde{u}$ in Theorem 3.2 is 5.

Let E be the following elliptic curve

$$E : y^2 = x^3 - x^2 - 6883x + 222137,$$

which is minimal.

By Proposition 2.5, twisting E by $d = 5$ falls in cases 1(b) and 2(a), and so $\tilde{u} = 5$. Then by Theorem 3.2, $\Omega(E^d)/\Omega(E) = \frac{5}{\sqrt{5}} = \sqrt{5}$. We now try to verify this in GP/Pari.

Using Lemma 2.2, we compute the twist by $d = 5$ to be

$$E^d : y^2 = x^3 - 5x^2 - 172075x + 27767125.$$

Using the command ellminimalmodel in GP/Pari we see that one of the minimal models for E^d is then

$$y^2 = x^3 + x^2 - 275x + 1667.$$

For an elliptic curve E we can compute the periods in GP/Pari using the command E.omega[1].

Remark 4.1. The period computed this way is similar to the period we use, but instead of using a minimal model it is defined as $\int_\gamma \omega(E)$, where γ is a generator of $H_1(E(\mathbb{C}), \mathbb{Z})^+$. Therefore we have to first compute a minimal model for E, use that to compute the period in GP/Pari, and then multiply the result by $c_\infty(E)$, the number of connected components, to get the period we desire.

Plotting these elliptic curves in Sage, using plot(E), we can see that both E and E^d have only one connected component, thus $c_\infty(E) = c_\infty(E^d) = 1$.

Then one finds that

$$\Omega(E^d) = \Omega(E^d_{\min}) \approx 2.90253993995\ldots$$

$$\Omega(E) \approx 1.29805532262\ldots$$

So $\Omega(E^d)/\Omega(E) \approx \sqrt{5}$, as expected.

4.2 How the complex period of GP/Pari relates to the imaginary period defined above.

Recall that the imaginary period is defined up to a sign as

$$\Omega^-(E) = \int_\gamma \omega(E),$$

where γ is a generator of $H_1(E_{\min}, \mathbb{Z})^-$. It will be a pure imaginary number since, if σ denotes complex conjugation

$$\sigma(\Omega^-(E)) = \int_{\sigma(\gamma)} \sigma(\omega(E)) = \int_{-\gamma} \omega(E) = -\Omega^-(E).$$

The second equality holds since $\omega(E)$ is defined over $\mathbb{R}$ (in fact over $\mathbb{Q}$) and because $\sigma(\gamma) = -\gamma$.

The complex period computed by GP/Pari (using the command E.omega) is in general not a pure imaginary number. Using the periods given by GP/Pari we can however approximately recover the imaginary period. This is because the two periods computed by GP/Pari (called the real and complex periods) are generators for a lattice, which is also generated by the two periods used in this paper (called the period and the imaginary period). For an elliptic curve E, let Ω_1 and Ω_1^- be the period and imaginary period, respectively, defined in this paper. Let Ω_2 and Ω_2^- be the real and complex periods, respectively, that are computed in GP/Pari for E using the function E.omega. Since the pairs are generators for the same lattice we have, $\Omega_1^- = k_1\Omega_2^- - k_2\Omega_2$ for some $k_1, k_2 \in \mathbb{Z}$. We also know that Ω_1^- is a pure imaginary number and that Ω_2 is a real number, therefore $k_2/k_1 = Re(\Omega_2^-)/\Omega_2$ where $Re(z)$ denotes the real part of the complex number z. Then k_1 and k_2 can be chosen such that $\gcd(k_1, k_2) = 1$. Finding such a k_1 and k_2 gives a way to compute the imaginary period using GP/Pari; however, we can only compute $Re(\Omega_2^-)/\Omega_2$ approximately and hence we can only make a good guess of what k_1 and k_2 are.

4.3 Imaginary quadratic twist

Using Sage and GP/Pari we were able to find the following example in which the $\tilde{u}$ in Theorem 3.2 is 7.

Let E be the following elliptic curve

$$E : y^2 + xy + y = x^3 - 173x + 879,$$

which is minimal.

By Proposition 2.5, twisting E by $d = -7$ falls in cases 1(b) and 2(a); hence $\tilde{u} = 7$. Then by Theorem 3.2, $\Omega(E^d)/\Omega^-(E) = \frac{7}{\sqrt{-7}} = \sqrt{-7}$, up to a sign. We now try to verify this in GP/Pari.

Using Lemma 2.2 we compute the twist by $d = -7$ to be

$$E^d : y^2 + xy + y = x^3 - 2x^2 - 8453x - 301583.$$

Using the command ellminimalmodel in GP/Pari we see that one of the minimal models for E^d is then

$$y^2 + xy = x^3 + x^2 - 3x - 4.$$

Plotting these elliptic curves in Sage, using plot(E), we can see that both E and E^d have only one connected component, thus $c_\infty(E) = c_\infty(E^d) = 1$.

Using Remark 4.1 one finds that

$$\Omega(E^d) = \Omega(E^d_{\min}) \approx 1.73968697697\ldots$$

Following the procedure to compute the imaginary period from Section 4.2 we find that $k_2/k_1 \approx -.50000000000\ldots$. Assuming that this is actually $-1/2$, we get

$$\Omega^-(E) \approx .65753987145\ldots\sqrt{-1}$$

and $\Omega(E^d)/\Omega^-(E) \approx \sqrt{-7}$, as expected.

5 Appendix on periods by Amod Agashe

In Section 5.1, we state and prove some facts about periods that are well known, but whose proof does not seem to be documented in the literature. In Section 5.2, we state a lemma that is used in Section 3. In Section 5.3, we point out the implications of the results of this article to [Aga10].

5.1 Some facts about periods

Let E be an elliptic curve over $\mathbb{Q}$, and let $E_{\min}$ denote an elliptic curve given by a global minimal Weierstrass equation for E. Let $\omega(E_{\min})$ denote the invariant differential on $E_{\min}$. Then recall that the period of E is defined as

$$\Omega(E) = \int_{E_{\min}(\mathbb{R})} |\omega(E_{\min})|.$$

Note that if we take a different global minimal Weierstrass equation for E, call it $E'_{\min}$, then $E_{\min}$ and $E'_{\min}$ are isomorphic to each other over $\mathbb{Q}$ by a transformation of the type $[u, r, s, t]$ (notation as in Remark 2.1) with $u = \pm 1$ (since they have the same discriminant, and the transformation changes the discriminant by a factor of u^{12}, by Remark 2.1). Then the invariant differential of $E'_{\min}$ differs from that of $E_{\min}$ by a factor of u (again, see Remark 2.1), i.e., by ± 1, and so the definition of $\Omega(E)$ given above is independent of the choice of a global minimal Weierstrass equation for E. If two elliptic curves are isomorphic over $\mathbb{Q}$, then they have a common minimal model, and hence they have the same period.

The Néron model of E is the open subscheme of $E_{\min}$ consisting of the regular points (see § III.6 of [Lan91]), and so the period defined above agrees with the period used in the more general version of the Birch and Swinnerton-Dyer conjecture for abelian varieties, as described for example in § III.5 of loc. cit., which uses Néron differentials.

Now as a Lie group, $E_{\min}(\mathbb{R})$ is isomorphic to one or two copies of $\mathbb{R}/\mathbb{Z}$ (see, e.g., [Sil94, Cor. V.2.3.1]). Since the invariant differential has no zeros or poles (see Prop. III.1.5 in [Sil92]), it does not change its sign on any copy of $\mathbb{R}/\mathbb{Z}$, and so on any copy, we have $|\omega(E_{\min})| = \pm\omega(E_{\min})$. If $E_{\min}(\mathbb{R})$ consists of one copy, then we see that up to a sign, $\Omega(E) = \int_{E_{\min}(\mathbb{R})} \omega(E_{\min})$. Now suppose $E_{\min}(\mathbb{R})$ consists of two copies; call them C_1 and C_2. Without loss of generality, assume that C_1 contains the identity, and choose a point P on C_2. Then the translation by P map induces a map from C_1 to C_2 (by continuity arguments) and similarly, translation by $-P$ maps C_2 to C_1. These two maps are inverses to each other, and moreover, $\omega(E_{\min})$ is invariant under translation. Thus we see that the integral of $|\omega(E_{\min})|$ over C_1 is the same as that over C_2 and up to a sign is the integral of $\omega(E_{\min})$ over either component. Thus in this case, up to a sign, $\Omega(E) = 2 \cdot \int_{C_1} \omega(E_{\min})$. In either case, we see that up to a sign,

$$\Omega(E) = \int_{E_{\min}(\mathbb{R})} \omega(E_{\min}). \tag{5}$$

If $\phi : E \to E_{\min}$ is an isomorphism (such an isomorphism exists, of course), then ϕ maps $E(\mathbb{R})$ bijectively to $E_{\min}(\mathbb{R})$ and one sees (by integration by substitution) that

$$\int_{E_{\min}(\mathbb{R})} \omega(E_{\min}) = \int_{E(\mathbb{R})} \phi^* \omega(E),$$

where $\omega(E)$ as usual is the invariant differential on E and ϕ^* denotes the pull-back by ϕ map on differentials. Thus up to a sign,

$$\Omega(E) = \int_{E(\mathbb{R})} \phi^* \omega(E).$$

This definition was used in [ARS06], for example.

Considering that C_1 is homeomorphic to the circle, and the natural map from the first homology group of C_1 to $H_1(E_{\min}(\mathbb{C}), \mathbb{Z})^+$ is an isomorphism (e.g., see Lemma 4.4 in [AS05]), from the discussion two paragraphs above, we get the following lemma:

Lemma 5.1. *Let γ be a generator of the cyclic free abelian group $H_1(E_{\min}(\mathbb{C}), \mathbb{Z})^+$ and let $c_\infty(E_{\min})$ denote the number of connected components in $E_{\min}(\mathbb{R})$. Then up to a sign,*

$$\Omega(E) = c_\infty(E_{\min}) \int_\gamma \omega(E_{\min}).$$

Note that since E and $E_{\min}$ are isomorphic over $\mathbb{R}$, we have $c_\infty(E_{\min}) = c_\infty(E)$. The lemma above is well known, and in fact a more general result for abelian varieties is given as Lemma 8.8 in [Man71]. However, in loc. cit., the author only gives a sketch of the proof of the quoted lemma, and uses the result of Lemma 5.1 above as an input without proof.

5.2 A lemma

In this section, let E be an elliptic curve over $\mathbb{R}$. Recall that $E(\mathbb{C})^-$ denotes the subgroup of $E(\mathbb{C})$ on which complex conjugation acts as multiplication by -1 and $E(\mathbb{C})_0^-$ is the component of $E(\mathbb{C})^-$ containing the identity. The following lemma is an easy adaptation of Lemma 4.4 in [AS05], and is used in Section 3.

Lemma 5.2. *The natural map from $H_1(E(\mathbb{C})_0^-, \mathbb{Z})$ to $H_1(E(\mathbb{C}), \mathbb{Z})^-$ is an isomorphism.*

Proof. Let ψ denote the natural map from $H_1(E(\mathbb{C})_0^-, \mathbb{Z})$ to $H_1(E(\mathbb{C}), \mathbb{Z})^-$. We have the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H_1(E(\mathbb{C})_0^-, \mathbb{Z}) & \longrightarrow & H_1(E(\mathbb{C})_0^-, \mathbb{R}) & \longrightarrow & E(\mathbb{C})_0^- & \longrightarrow & 0 \\ & & \downarrow \psi & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & H_1(E(\mathbb{C}), \mathbb{Z})^- & \longrightarrow & H_1(E(\mathbb{C}), \mathbb{R})^- & \longrightarrow & E(\mathbb{C})^- & & \end{array},$$

where the two vertical arrows on the right are the obvious natural maps, the upper horizontal sequence the exact sequence obtained by viewing the real torus $E(\mathbb{C})_0^-$ as the quotient of the tangent space at the identity by the first integral homology, and the lower horizontal sequence is the exact sequence obtained from the exact sequence

$$0 \to H_1(E(\mathbb{C}), \mathbb{Z}) \to H_1(E(\mathbb{C}), \mathbb{R}) \to E(\mathbb{C}) \to 0$$

of complex analytic parametrization of E by taking anti-invariants under complex conjugation. The middle vertical map is an isomorphism of real vector spaces because if it were not, then its kernel would be an uncountable set that maps to 0 in $E(\mathbb{C})_0^-$ (using the rightmost square in the commutative diagram above), and hence would be contained in $H_1(E(\mathbb{C})_0^-, \mathbb{Z})$, which is countable. The snake lemma then yields an exact sequence

$$0 \to \ker(\psi) \to 0 \to 0 \to \operatorname{coker}(\psi) \to 0,$$

which implies that ψ is an isomorphism, as was to be shown. □

5.3 Some implications

In this section, we point out the implications of the results of this article to [Aga10].

By Corollary 2.6, if d is coprime to the conductor E (or the discriminant of E), then the $\tilde{u}$ in Theorem 3.2 is a power of 2. Note that the D in [Aga10] is $-d$, with $d < 0$. Thus if one replaces the hypothesis (**) in §2 of loc. cit., with the hypothesis that D is coprime to the conductor N of E, then the conclusions of Lemma 2.1, Proposition 2.2, and Corollary 2.4 are valid up to a power of 2. As a consequence (see the discussion after Corollary 2.4 in loc. cit.), we would like to weaken the hypothesis (**) in Conjecture 2.5 of loc. cit. to the hypothesis that D is coprime to N, and thus make the following conjecture:

Conjecture 5.3. *Let E be an optimal elliptic curve over $\mathbb{Q}$ of conductor N and let $-D$ be a negative fundamental discriminant such that D is coprime to N. Recall that E_{-D} denotes the twist of E by $-D$. Suppose $L(E_{-D}, 1) \neq 0$, so that $E_{-D}(\mathbb{Q})$ is finite. Then $|E_{-D}(\mathbb{Q})|^2$ divides $|Ш(E_{-D})| \cdot \prod_{p|N} c_p(E_{-D})$, up to a power of 2, where $Ш(E_{-D})$ denotes the Shafarevich-Tate group of E_{-D} and $c_p(E_{-D})$ denotes the order of the arithmetic component group of E_{-D} at p.*

As mentioned in loc. cit., using the mathematical software sage, with its inbuilt Cremona's database for all elliptic curves of conductor up to 130000, we verified the conjecture above for all triples (N, E, D) such that N and D are positive integers with $ND^2 < 130000$, and E is an optimal elliptic curve of conductor N.

Finally, we remark that Proposition 2.5 explains why the concluding statement of Conjecture 2.5 of [Aga10] does not hold in the example of $(E, D) = (27a1, 3)$ in Table 1 of loc. cit. (this example does not satisfy the hypotheses of the conjecture): using SAGE, we find that $\Delta(E_{\min}) = -3^9$ and $c_6(E_{\min}) = 2^3 \cdot 3^6$, and so by part 1(b) of the proposition, $v_3(\tilde{u}) > 0$. In particular, this is an example of an optimal elliptic curve for which $\tilde{u}$ is not a power of 2. Anyhow, the concluding statement of Corollary 2.4 in loc. cit. does not hold, and so for this pair (E, D), assuming the second part of the Birch and Swinnerton-Dyer conjecture, one does not expect that $|E_{-D}(\mathbb{Q})|^2$ divides $|Ш(E_{-D})| \cdot \prod_{p|N} c_p(E_{-D})$, even up to a power of 2 (see the discussion just before Corollary 2.5 in loc. cit.); rather one expects that $|E_{-D}(\mathbb{Q})|^2$ divides $\tilde{u} \cdot |Ш(E_{-D})| \cdot \prod_{p|N} c_p(E_{-D})$, and so it is not surprising that $|E_{-D}(\mathbb{Q})|^2$ divides $3 \cdot |Ш(E_{-D})| \cdot \prod_{p|N} c_p(E_{-D})$, up to a power of 2.

References

[Aga10] Amod Agashe, *Squareness in the special L-value and special L-values of twists*, Int. J. Number Theory **6** (2010), no. 5, 1091–1111.

[ARS06] Amod Agashe, Kenneth Ribet, and William A. Stein, *The Manin constant*, Pure Appl. Math. Q. **2** (2006), no. 2, part 2, 617–636.

[AS05] A. Agashe and W. A. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484.

[Con08] Ian Connell, *Elliptic curve handbook*, preprint, available at `http://www.ucm.es/BUCM/mat/doc8354.pdf`.

[Kwo97] Soonhak Kwon, *Torsion subgroups of elliptic curves over quadratic extensions*, J. Number Theory **62** (1997), no. 1, 144–162. MR 1430007 (98e:11068)

[Lan91] S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry.

[Man71] J. I. Manin, *Cyclotomic fields and modular curves*, Russian Math. Surveys **26** (1971), no. 6, 7–78.

[OS98] Ken Ono and Christopher Skinner, *Fourier coefficients of half-integral weight modular forms modulo l*, Ann. of Math. (2) **147** (1998), no. 2, 453–470.

[Sil92] J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992.

[Sil94] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.