The Ramanujan Journal (2023) 61:935–956
https://doi.org/10.1007/s11139-022-00697-8

A p-adic study of the Richelot isogeny with applications to periods of certain genus 2 curves

Rudolf Chow[1] · **Frazer Jarvis**[1]

Received: 28 February 2022 / Accepted: 24 December 2022 / Published online: 6 March 2023

Abstract
In this paper, we begin to consider the problem of computing p-adic periods of certain genus 2 curves with totally split reduction, using techniques of the arithmetic–geometric mean. For this, we synthesise the work of Henniart and Mestre on a p-adic arithmetic–geometric mean in genus 1 with the work of Bost and Mestre on a real arithmetic–geometric mean in genus 2 (via the so-called Richelot isogeny). We prove that, for a certain class of p-adic genus 2 curves, the Richelot isogeny plays the same role in the genus 2 theory as the maps appearing in Henniart–Mestre, in that the Richelot isogeny squares the p-adic periods, and leads to a quadratically converging sequence of genus 2 curves. This suggests that this may provide a quadratically convergent method to compute p-adic periods for these curves, once we have a suitably explicit p-adic Tate uniformisation in genus 2.

Keywords p-adic periods · Genus 2 curves · Richelot isogeny

Mathematics Subject Classification 14G20 · 14H42 · 11G20

1 Introduction

Given two numbers $a \geq b > 0$, we set $a_0 = a, b_0 = b$, and define $a_{n+1} = (a_n + b_n)/2$ and $b_{n+1} = \sqrt{a_n b_n}$. The two sequences (a_n) and (b_n) converge quadratically to a common limit $M = M(a, b)$, known as the arithmetic–geometric mean (AGM). The elementary theory is beautifully presented in the article of Cox [6]. If we define

$$I(a, b) = \int_0^{\pi/2} \frac{\mathrm{d}\theta}{\sqrt{a^2 \cos^2 \theta + b^2 \sin^2 \theta}}$$

✉ Frazer Jarvis
a.f.jarvis@sheffield.ac.uk

[1] School of Mathematics and Statistics, University of Sheffield, Sheffield S3 7RH, UK

there is a (fairly complicated) change of variable, known to Gauss, which shows that $I(a,b) = I(\frac{a+b}{2}, \sqrt{ab})$. It follows that

$$I(a,b) = I(a_0,b_0) = I(a_1,b_1) = \cdots = I(M,M) = \frac{\pi}{2M}.$$

Thus we have a quick way to compute the elliptic integrals $I(a,b)$, at least numerically. A change of variable leads to these integrals appearing as $\int \frac{\mathrm{d}x}{\sqrt{P(x)}}$, where P is a quartic polynomial, and where the limits are roots of P. Writing $y^2 = P(x)$, we see that we can evaluate numerically quickly the period integrals for this elliptic curve.

If we write P for the quartic coming from the integral $I(a,b)$ and P' for that coming from $I(a_1,b_1)$, then it turns out that there is a 2-isogeny between the elliptic curves $y^2 = P(x)$ and $y^2 = P'(x)$, which we refer to as the AGM isogeny. If the complex uniformisation of $y^2 = P(x)$ is given by $\mathbb{C}/\mathbb{Z} + \mathbb{Z}\tau$, then $y^2 = P'(x)$ has a complex uniformisation isomorphic to $\mathbb{C}/\mathbb{Z} + \mathbb{Z}.(2\tau)$, i.e. there is a doubling of the period. Indeed, if we use the usual theta functions to embed the elliptic curves into projective space:

$$\theta_3(q) = \sum_{n\in\mathbb{Z}} q^{n^2}, \qquad \theta_4(q) = \sum_{n\in\mathbb{Z}} (-1)^n q^{n^2} \qquad (q = e^{\pi i \tau}),$$

then

$$\theta_3^2(q^2) = \frac{\theta_3^2(q) + \theta_4^2(q)}{2}, \qquad \theta_4^2(q^2) = \theta_3(q)\theta_4(q),$$

so that the AGM process takes q into q^2, which corresponds to a doubling of the period τ.

Gauss understood the behaviour of the algorithm when a and b are not necessarily positive real numbers (issues arise because the square root is no longer well-defined), and Cremona and Thongjunthug [7] explained how to adapt the algorithm for computing periods of real elliptic curves to the complex case.

There is also a p-adic version of the algorithm, due to Henniart and Mestre [11]. It is easy to see that this will not converge unless the two p-adic integers a and b are in the same p-adic disc. This leads to an algorithm for computing the p-adic periods of elliptic curves with split multiplicative reduction defined over non-archimedean complete fields, so that there exists a p-adic uniformisation (they also require that the residue characteristic differs from 2). We will review this below.

Bost and Mestre [3] define a version of the AGM suitable for computing periods of curves of genus 2. This depends on the Richelot isogeny between two curves of genus 2. If we are given a genus 2 curve in the form $y^2 = f(x)$ where $f(x)$ is a sextic, a quadratic splitting is a factorisation of f as a product $f = P_1P_2P_3$ of three quadratics. Corresponding to this factorisation is the Richelot isogeny, a $(2,2)$-isogeny between Jacobians, which we will discuss further below; the algorithm as given by Bost and Mestre computes the periods when the three quadratics are all real. Again, there are issues when the quadratics are complex.

There is also some literature on p-adic periods of curves of genus 2. Given a genus 2 curve X, there is a p-adic uniformisation of the curve (due to Mumford [20]) when X has totally split reduction. Abelian varieties also have p-adic uniformisation (again due to Mumford [21]); the link between the uniformisations of the curves and their Jacobians was explained by Manin and Drinfeld [14]. Teitelbaum used these ideas in his thesis (see [27]) to compute some p-adic periods for some totally split curves over genus 2; subsequently, Kadziela [13] did something similar in his thesis. Neither exploits the arithmetic–geometric mean, and we hope to explain in this article how this might work, thereby giving a quadratically convergent algorithm. However, some details, especially an explicit description of the Mumford uniformisation, remain to be completed, and we intend to consider this further in future work.

2 A p-adic AGM in genus 1

The material in this section follows Henniart–Mestre [11] closely; more details can be found there. We let K denote a non-archimedean complete field of residue characteristic $p > 2$. If we are given a_0 and b_0 in $K^\times$ such that $a/b \equiv 1 \pmod{8\mathfrak{p}}$, where $\mathfrak{p}|p$ denotes the maximal ideal in $\mathcal{O}_K$, then the formulae we gave above for the arithmetic–geometric mean converge quadratically in $K^\times$ (so that the p-adic precision of the agreement of a_n and b_n doubles at each iteration).

We recall Tate's work on p-adic uniformisation. We let E/K denote an elliptic curve with split multiplicative reduction, and suppose it to be of the form $y^2 = x(x+a)(x+a-b)$. Then the j-invariant of E is not an integer of K, and there is a value $q \in \mathfrak{p}$ characterised by $j = q^{-1} + 744 + \cdots$. There is then a p-adic uniformisation $\phi : K^\times/q^{\mathbb{Z}} \xrightarrow{\sim} E$. Further, if $\mathrm{d}x/y$ is the canonical differential on E, and t is the coordinate on $K^\times$, we have $\phi^*(\mathrm{d}x/2y) = u\,\mathrm{d}t/t$; the AGM can be used to compute the value of u; an extension allows us to compute q from a Weierstrass equation for E.

Indeed, as remarked above, the AGM gives a 2-isogeny between E and a curve E' given by $y^2 = x(x+a')(x+a'-b')$, where a' and b' denote (slightly modified versions of) the arithmetic and geometric means of a and b. If E has a p-adic uniformisation, so does E'. We have a diagram

$$\begin{array}{ccc} K^\times/q^{2\mathbb{Z}} & \xrightarrow{f} & K^\times/q^{\mathbb{Z}} \\ \downarrow\wr & & \downarrow\wr \\ E' & \xrightarrow{g} & E. \end{array}$$

The bottom map here is the AGM isogeny, and the vertical maps come from the p-adic uniformisation. There are p-adic theta functions which satisfy the same duplication rules as over $\mathbb{C}$, so that the p-adic period q doubles. The top map is therefore induced by the identity map on $K^\times$.

This leads to a simple way to determine q using the AGM process. After choosing the models for E' and E above, there is an explicit description of the isogeny g, and

$(0, 0)$ is the non-trivial element of the kernel. The non-trivial element in the kernel of f is clearly given by $q \pmod{q^{2\mathbb{Z}}}$.

This leads to the following method. Start with the elliptic curve $E = E_0$ in Weierstrass form for which one wishes to compute the p-adic period q.

Applying the AGM isogeny repeatedly, and p-adic uniformisation, gives a commutative diagram

$$\begin{array}{ccccccc} \cdots & \xrightarrow{f_2} & K^\times/q^{4\mathbb{Z}} & \xrightarrow{f_1} & K^\times/q^{2\mathbb{Z}} & \xrightarrow{f_0} & K^\times/q^{\mathbb{Z}} \\ & & \phi_2\downarrow\wr & & \phi_1\downarrow\wr & & \phi_0\downarrow\wr \\ \cdots & \xrightarrow{g_2} & E_2 & \xrightarrow{g_1} & E_1 & \xrightarrow{g_0} & E_0 \end{array}$$

in which the maps f_n are induced by the identity on $K^\times$, and the bottom maps are explicit isogenies between elliptic curves with explicitly given Weierstrass equations, $E_n : y^2 = x(x + a_n)(x + a_n - b_n)$. The vertical maps coming from Tate's p-adic uniformisation are a little more mysterious. However, were we to extend the diagram infinitely far to the left, we can see that the top sequence would have projective limit $K^\times$, while the bottom one would have a limit curve E_∞ with an explicit equation $y^2 = x^2(x + M)$, where M is the arithmetic–geometric mean $M = M(a_1, b_1)$. The vertical maps are given by a formula of Tate (see, for example, [26], p. 323). These are complicated series, but they degenerate in the limit into a very simple map. Tate's vertical map for a point $w \in K^\times$ and period q involves the p-adic theta series

$$\vartheta(w, q) = (1 - w)\prod_{n=1}^{\infty}(1 - q^n w)(1 - q^n w^{-1})(1 - q^n) = \sum_{n\in\mathbb{Z}}(-1)^n q^{\frac{n^2-n}{2}} w^n,$$

the equality being the Jacobi triple product, and as $q \to 0$, we see that this approaches $1 - w$. This leads to a simple explicit map at infinity, $\phi_\infty : K^\times \longrightarrow E_\infty$, and at each finite stage, the vertical map ϕ_n can be regarded as an approximation of ϕ_∞ agreeing up to precision of order q^{2^n}.

So one can take $P_1 = (0, 0)$ on E_1, explicitly pull it back to P_2 on E_2, then to P_3 on E_3 etc., up to desired precision; then apply ϕ_∞^{-1} to get something in $K^\times$, and this should be the value q. Explicit details and formulae are given in [11]; from the formulae, it is clear that there is a natural right choice of pull back P_{n+1} of P_n which is in the same p-adic disc.

More generally, one can start with any point P_0 on E_0 and carry out this procedure. This gives a p-adic Landen transformation in this setting.

Before moving on to genus 2, we remark that this also allows one to compute tiny Coleman elliptic integrals. So let $E/\mathbb{Q}_p$ be an elliptic curve with an explicit model $y^2 = (x - e_1)(x - e_2)(x - e_3)$ such that $e_2 - e_1 \equiv e_3 - e_1 \pmod{p\mathbb{Z}_p}$. Suppose that P and Q are points on $E(\mathbb{Q}_p)$ inside the same residue disc. Then recall that $\phi : \mathbb{Q}_p^\times/q^{\mathbb{Z}} \longrightarrow E$ has $\phi^*(\mathrm{d}x/2y) = u\,\mathrm{d}t/t$. Properties of Coleman integration now

imply that

$$\int_P^Q \frac{\mathrm{d}x}{2y} = \int_{\phi^{-1}(P)}^{\phi^{-1}(Q)} \phi^* \left(\frac{\mathrm{d}x}{2y}\right) = \int_{\phi^{-1}(P)}^{\phi^{-1}(Q)} u \frac{\mathrm{d}t}{t} = u \operatorname{Log}\left(\frac{\phi^{-1}(Q)}{\phi^{-1}(P)}\right),$$

where Log denotes a branch of the p-adic logarithm.

We record this as an algorithm:

Algorithm 2.1 Let $E/\mathbb{Q}_p$ be an elliptic curve, and $P, Q \in E(\mathbb{Q}_p)$ in the same residue disc.

1. Let $\alpha = e_2 - e_1$, $\beta = e_3 - e_1$.
2. Compute the quantity $u^2 \in \mathbb{Q}_p$ using the AGM, as in [11].
3. Apply the Landen transformation to both P and Q to get $\phi^{-1}(P)$ and $\phi^{-1}(Q)$.
4. Then

$$\int_P^Q \frac{\mathrm{d}x}{2y} = u \operatorname{Log}\left(\frac{\phi^{-1}(Q)}{\phi^{-1}(P)}\right).$$

When programmed in Sage, this converges quadratically, and gives the same result as existing algorithms of Balakrishnan and others, which have linear convergence. (However, we note that our method only applies to those curves with split multiplicative reduction, whereas those already in Sage apply more generally.)

However, the main aim of this paper is to begin to try to extend the algorithm of Henniart and Mestre to curves of genus 2.

3 The Richelot isogeny and periods of curves of genus 2

Richelot ([23]), in 1836, gave a construction for genus 2 curves which has some resemblances to the AGM isogeny for curves of genus 1. In particular, it allows the numerical computation of period integrals of the form

$$\int_a^b \frac{lx + m}{\sqrt{|P(x)|}} \mathrm{d}x,$$

where P is a polynomial of degree 6 with real roots, and a and b are consecutive real roots of P. It resembles Gauss's work on elliptic integrals, but is significantly more complicated. The method was subsequently refined by Königsberger and Humbert, and was given a modern treatment by Bost and Mestre [3], which we follow in this paper.

Let X denote a curve over $\mathbb{C}$ of genus 2. It therefore has a model $y^2 = f(x)$, for some sextic f. Then X has a Jacobian, $J = \mathrm{Pic}^0(X)$, the degree 0 divisors on X, up to linear equivalence.

We shall explain how to construct a new curve X', with Jacobian J', such that there is a $(2, 2)$-isogeny $J' \longrightarrow J$, which shares some of the properties of the AGM isogeny for elliptic curves.

Definition 3.1 A *quadratic splitting* of $f(x)$ is simply a factorisation of f as a product $P_1P_2P_3$ of three quadratics.

For curves of genus 2 over $\mathbb{R}$, there is a natural quadratic splitting, coming from taking pairs of consecutive roots. We shall see below that there is similarly a canonical choice of quadratic splitting for certain totally split genus 2 curves over p-adic fields. However, one of the main obstacles to a nice general theory over the complexes is that there are 15 choices of quadratic splitting over $\mathbb{C}$, and none is necessarily the correct one. The first author partially considers this issue in his thesis [5].

We fix a splitting, $f = P_1P_2P_3$, where $P_i(x) = p_{i2}x^2 + p_{i1}x + p_{i0}$. Then we define

$$\begin{aligned} Q_1 &= [P_2, P_3] = P_2'P_3 - P_2P_3' \\ Q_2 &= [P_3, P_1] = P_3'P_1 - P_3P_1' \\ Q_3 &= [P_1, P_2] = P_1'P_2 - P_1P_2' \end{aligned}$$

(with the bracket notation intended to remind the reader of the Lie bracket). If P_i and P_j are quadratics, the derivatives P_i' and P_j' are linear, but the leading terms in the brackets cancel, so that each Q_k is again quadratic.

If we write $\Delta = \det(p_{ij})$, let X' be defined by the twist

$$\Delta y^2 = Q_1Q_2Q_3.$$

There is a correspondence $Z \subset X \times X'$. Indeed, if we label the coordinates of X' so that they are given by $\Delta y'^2 = Q_1(x')Q_2(x')Q_3(x')$, we let Z be given by

$$\left\{ (x, y, x', y') \;\middle|\; \begin{array}{l} y^2 = P_1(x)P_2(x)P_3(x),\ \Delta y'^2 = Q_1(x')Q_2(x')Q_3(x'), \\ P_1(x)Q_1(x') + P_2(x)Q_2(x') = 0,\ P_1(x)Q_1(x')(x - x') = yy' \end{array} \right\}.$$

That is, Z is defined as the subset of $X \times X'$ by the extra two equations

$$\begin{aligned} P_1(x)Q_1(x') + P_2(x)Q_2(x') &= 0, \\ P_1(x)Q_1(x')(x - x') &= yy'. \end{aligned}$$

Write $\pi_1 : Z \longrightarrow X$, and $\pi_2 : Z \longrightarrow X'$ for the projections. Then the correspondence Z induces a map $\delta_Z : \Omega^1(X') \longrightarrow \Omega^1(X)$ given by composition $\pi_{1*} \circ \pi_2^*$ of the inverse image $\pi_2^* : \Omega^1(X') \longrightarrow \Omega^1(Z)$ and of the trace $\pi_{1*} : \Omega^1(Z) \longrightarrow \Omega^1(X)$. With the extra factor of Δ we added, it turns out (see [3]) that there is an identity

$$\delta_Z\left((lx' + m)\frac{\mathrm{d}x'}{y'}\right) = (lx + m)\frac{\mathrm{d}x}{y}.$$

So if we had used the same labels for both X and X', we would get

$$\delta_Z\left(\frac{\mathrm{d}x}{y}\right) = \frac{\mathrm{d}x}{y}, \qquad \delta_Z\left(\frac{x\,\mathrm{d}x}{y}\right) = \frac{x\,\mathrm{d}x}{y},$$

which explains how the differentials on the curves behave under the correspondence.

The correspondence Z also defines a map $\mathrm{Div}(X') \longrightarrow \mathrm{Div}(X)$ on divisors by the formula $\sum n_i p_i' \mapsto \sum n_i \pi_1 \pi_2^{-1} p_i'$ for points p_i' on X', and this gives a map $g : J' \longrightarrow J$ on degree 0 divisor classes, $g([\sum n_i p_i']) = [\sum n_i \pi_1 \pi_2^{-1} p_i']$. In the same way, Z induces a map $g' : J \longrightarrow J'$ by $g'([\sum n_i p_i]) = [\sum n_i \pi_1 \pi_2^{-1} p_i]$. We will refer to g as the *Richelot isogeny*; then g' is the dual isogeny, in the sense that $g'g = [2]_{J'}$, multiplication by 2 on J', and $gg' = [2]_J$.

We remark that the correspondence Z depends on the choice of ordering of the three quadratics within the splitting, but that all choices give the same isogeny on divisor classes (see [25], sect. 8.4) so give the same map on Jacobians.

The kernel of g is a $(2, 2)$-subgroup, whose three non-zero elements are the divisor classes $[(q_i, 0) - (q_i', 0)]$, where q_i and q_i' are the two roots of Q_i, for each of the quadratics Q_1, Q_2 and Q_3.

Thus we have a map in genus 2 with analogous properties to the AGM isogeny in genus 1. Before moving to the p-adic theory, we briefly explain that this can likewise be viewed as a period-doubling map. This is already explained in [3] in the case of real sextics, using integration. We will explain another approach, which will be more useful when we come to consider the p-adic setting.

We first recall the definition of a theta function. Take a and b to be column vectors in $\mathbb{Q}^2$, and Ω in the Siegel upper half-space $\mathbb{H}_2$ of all 2×2-symmetric complex matrices with positive definite imaginary part. For a pair $z = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$ of complex numbers, we define the *theta function with characteristic* $\begin{bmatrix} a \\ b \end{bmatrix}$ as

$$\theta \begin{bmatrix} a \\ b \end{bmatrix} (z; \Omega) = \sum_{n \in \mathbb{Z}^2} e^{\pi i^t (n+a)\Omega(n+a) + 2\pi i^t (n+a)(z+b)}.$$

These theta functions are analytic in z and satisfy a transformation law. Of particular importance are the functions with $a, b \in \frac{1}{2}\mathbb{Z}^2/\mathbb{Z}^2$. Often formulae just involve the theta constants, where $z = 0$, and then there are 6 pairs (a, b) for which these vanish; the remaining 10 theta functions are as follows:

$$\begin{aligned}
\theta_0(\Omega) &= \theta \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} (\Omega), & \theta_1(\Omega) &= \theta \begin{bmatrix} 0 & 0 \\ 0 & \frac{1}{2} \end{bmatrix} (\Omega), \\
\theta_2(\Omega) &= \theta \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix} (\Omega), & \theta_3(\Omega) &= \theta \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} (\Omega), \\
\theta_4(\Omega) &= \theta \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} (\Omega), & \theta_5(\Omega) &= \theta \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ 0 & 0 \end{bmatrix} (\Omega), \\
\theta_6(\Omega) &= \theta \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix} (\Omega), & \theta_7(\Omega) &= \theta \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & 0 \end{bmatrix} (\Omega), \\
\theta_8(\Omega) &= \theta \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix} (\Omega), & \theta_9(\Omega) &= \theta \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix} (\Omega).
\end{aligned}$$

(Note that the numbering of these is not standardised in the literature, and our numbering is arbitrary.)

Given an equation $y^2 = f(x)$, where f is a sextic, there is some linear transformation taking three given roots to 0, 1 and ∞, respectively. This turns the original sextic into a quintic, giving an equation in *Rosenhain form*

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu).$$

The classical Thomae formulae allow us to write λ, μ and ν in terms of the 10 genus 2 theta constants $\{\theta_0(\Omega), \ldots, \theta_9(\Omega)\}$, where Ω is the period matrix of the Jacobian. We now consider the quadratic splitting

$$P_1(x) = x(x-\lambda), \quad P_2(x) = (x-1)(x-\mu), \quad P_3 = x - \nu.$$

It turns out that when we apply the Richelot isogeny corresponding to this splitting (making appropriate choices for the square roots in the formulae), we get a sextic defining X'; when we move three roots back to 0, 1 and ∞, we get an equation

$$y^2 = x(x-1)(x-\lambda')(x-\mu')(x-\nu'),$$

and we find that the remaining three roots are exactly given by the same functions defining λ, μ and ν as for X, but evaluated at 2Ω rather than Ω (see [5] for more details of the argument, e.g. which roots one moves to 0, 1 and ∞, and which square roots one should take). The proof involves a lengthy calculation with theta function duplication formulae, and simplification via Maple. We should remark that the quadratic splitting here is chosen for compatibility with the p-adic situation below.

Thus the Richelot isogeny is a period-doubling map in the same way as the AGM isogeny in genus 1.

Thus all the ingredients are in place to try to extend the Henniart–Mestre algorithm for finding p-adic periods of elliptic curves to genus 2, except for the p-adic uniformisation theory, which we recall now.

4 *p*-adic uniformisation for genus 2 curves and their Jacobians

Our main reference here is Teitelbaum's paper [27], together with that of Kadziela [13]. We restrict ourselves to the parts of the theory which will be useful for us; see these references for background on rigid analysis and in particular the structure of p-adic domains in terms of the tree for PGL_2. We will assume that the residue characteristic of our field is odd, so that we can write genus 2 curves with a model of the form $y^2 = f(x)$, where f is a sextic.

Just as not every elliptic curve has a p-adic uniformisation, so the same is true in genus 2. Those curves which do have such a uniformisation are the totally split curves; these are also known as Mumford curves. Essentially, these have special fibres with components of genus 0 intersecting at ordinary double points. Whether or not a curve is a Mumford curve can be read off from the equation (see [27], Proposition 9); there

are three kinds of curve whose reduction is just bad enough to be totally split, which Teitelbaum calls Types A, B and C. Modulo the maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the equation must reduce to

$$y^2 = k(x-\alpha)^2(x-\beta)^2(x-\gamma)(x-\delta)$$

with α, β and γ in different residue classes.

- Type A refers to the case where δ is different from α, β and γ;
- Type B refers to the case where $\delta \equiv \gamma$, so that the equation reduces to $y^2 = k(x-\alpha)^2(x-\beta)^2(x-\gamma)^2$ modulo $\mathfrak{p}$;
- Type C refers to the case where $\delta \equiv \alpha$, so that the equation reduces to $y^2 = k(x-\alpha)^3(x-\beta)^2(x-\gamma)$ modulo $\mathfrak{p}$.

Our work, like Teitelbaum's, focuses on Type B; his motivation is that genus 2 modular curves are of this form, since their reduction is known to have ordinary double points, but it is also very useful for us, since the pairing of the roots by residue classes gives us a canonical p-adic quadratic splitting of the sextic.

Indeed, we shall restrict to the case of Type B from now on. (Further, we suspect that the arguments we give in this paper will not extend to the other cases, but this may be a topic for future investigation.)

Thus the Weierstrass points of the curve are canonically partitioned into three pairs, S_1, S_2 and S_3, where these consist of pairs of points whose x-coordinates in the same residue class.

Given a totally split curve X over a complete p-adic field K, Mumford ([20]) explained that there is a p-adic uniformisation for X. There is a Schottky group $\Gamma \subset \mathrm{PGL}_2(K)$, i.e. a group all of whose non-identity elements are hyperbolic in the p-adic sense that their eigenvalues have different valuations, and a rigid analytic isomorphism $\Omega/\Gamma \longrightarrow X$, where $\Omega = \mathbb{P}^1_K - \mathcal{L}$, with $\mathcal{L}$ being the set of limit points of Γ. Ihara showed that Schottky groups are free; Mumford showed that the number of generators of Γ is equal to the genus of X.

We are interested in the case of a curve of genus 2, so our Schottky group is a free group on two generators γ_1 and γ_2.

Mumford ([21]) also explained how to uniformise abelian varieties; the link between the uniformisation of the curve and its Jacobian was given by Manin and Drinfeld [14]. There is a pairing $\Gamma \times \Gamma \longrightarrow K^\times$, given in terms of p-adic theta functions, which allows us to regard Γ as contained in $C_\Gamma = \mathrm{Hom}(\Gamma, K^\times)$. Then the quotient C_Γ/Γ is a uniformisation of the Jacobian J.

The map is fairly explicit. If Ω is as above, then an automorphic form on Γ is a meromorphic function f on Ω such that $f(\omega) = \chi(\alpha) f(\alpha\omega)$ for all $\alpha \in \Gamma$. The constant $\chi(\alpha) \in K^\times$ is the automorphy factor. It is easy to see that χ is a homomorphism $\Gamma \longrightarrow K^\times$.

Automorphic forms are generated by p-adic theta functions, and these are the most important ingredient in the theory. Given $a, b \in \Omega$, we define

$$\Theta(a, b; z) = \prod_{\gamma \in \Gamma} \frac{z - \gamma(a)}{z - \gamma(b)}.$$

This product converges to give a meromorphic function on Ω; if a and b are in the same orbit under Γ, there are no poles or zeros, but otherwise there are simple zeros on Γa and simple poles on Γb. We set

$$u_\alpha(z) = \Theta(a, \alpha(a); z),$$

which are independent of the choice of a, and satisfies $u_{\alpha\beta}(z) = u_\alpha(z)u_\beta(z)$ for all $\alpha, \beta \in \Gamma$. It turns out that $u_\alpha(z)$ is constant if $\alpha \in [\Gamma, \Gamma]$. The automorphy factor of $\Theta(a, b; z)$ is

$$\chi_{a,b}(\alpha) = \frac{u_\alpha(a)}{u_\alpha(b)} = \frac{\Theta(a, \alpha(a); z)}{\Theta(b, \alpha(b); z)}.$$

If we are given a homomorphism $\chi \in \mathrm{Hom}(\Gamma, K^\times)$, then there is a unique automorphic form f_χ on Ω whose automorphy factor is χ. Then the map $C_\Gamma/\Gamma \longrightarrow J$ is given by $\chi \mapsto [(f_\chi)]$, the class of the divisor of f_χ.

The pairing $\Gamma \times \Gamma \longrightarrow K^\times$ is also easy to describe. If α and β are in Γ, then the value of the pairing is

$$\langle \alpha, \beta \rangle = \frac{u_\alpha(z)}{u_\alpha(\beta z)}.$$

Then this is a symmetric pairing on Γ, valued in $K^\times$.

Let's fix generators γ_1 and γ_2 for our Schottky group Γ. Since the pairing factors through $\overline{\Gamma} \times \overline{\Gamma} \longrightarrow K^\times$, where $\overline{\Gamma} = \Gamma/[\Gamma, \Gamma]$, every element can be written $\alpha \equiv \gamma_1^{m_1}\gamma_2^{m_2}$, $\beta \equiv \gamma_1^{n_1}\gamma_2^{n_2}$, and the bilinearity and symmetricity give

$$\langle \alpha, \beta \rangle = \langle \gamma_1, \gamma_1 \rangle^{m_1 n_1} \langle \gamma_1, \gamma_2 \rangle^{m_1 n_2 + m_2 n_1} \langle \gamma_2, \gamma_2 \rangle^{m_2 n_2}$$

In particular, the pairing is determined by the effects on the two generators.

We recall that for genus 2 Mumford curves of Type B, the Weierstrass points were canonically partitioned into three pairs S_1, S_2 and S_3. We label these pairs arbitrarily, following [27], as $S_i = \{P_i^+, P_i^-\}$. Teitelbaum ([27], 2.1) writes down specific generators γ_1 and γ_2, defines γ_3 so that $\gamma_1\gamma_2\gamma_3 = 1$, and defines p-adic periods by

$$q_1 = \langle \gamma_2, \gamma_3 \rangle^{-1}, \qquad q_2 = \langle \gamma_3, \gamma_1 \rangle^{-1}, \qquad q_3 = \langle \gamma_1, \gamma_2 \rangle^{-1}.$$

Clearly these three periods determine the pairing.

Teitelbaum defines "half-periods" by

$$p_1 = \chi_{P_1^+, P_2^+}(\gamma_2), \qquad p_2 = \chi_{P_2^+, P_3^+}(\gamma_3), \qquad p_3 = \chi_{P_3^+, P_1^+}(\gamma_1),$$

and shows that $p_i^2 = q_i^{-1}$. These half-periods are used to construct particular theta functions on the Jacobian.

Once generators are fixed for the free group Γ, there is a natural isomorphism $\mathrm{Hom}(\Gamma, K^\times) \xrightarrow{\sim} (K^\times)^2$, given by $\chi \mapsto (\chi(\gamma_1), \chi(\gamma_2))$. The pairing $\Gamma \times \Gamma \longrightarrow K^\times$

gives a map $\Gamma \hookrightarrow \mathrm{Hom}(\Gamma, K^\times)$, which we might write $\gamma \mapsto \chi_\gamma$. The image of Γ under the isomorphism is generated by

$$(\chi_{\gamma_1}(\gamma_1), \chi_{\gamma_1}(\gamma_2)) = (\langle\gamma_1, \gamma_1\rangle, \langle\gamma_1, \gamma_2\rangle) = (q_2 q_3, q_3^{-1})$$

and

$$(\chi_{\gamma_2}(\gamma_1), \chi_{\gamma_2}(\gamma_2)) = (\langle\gamma_2, \gamma_1\rangle, \langle\gamma_2, \gamma_2\rangle) = (q_3^{-1}, q_1 q_3).$$

Thus the image of Γ is the subgroup

$$H_\Gamma = \{(q_2^a q_3^{a-b}, q_1^b q_3^{b-a}) \mid a, b \in \mathbb{Z}\}.$$

We conclude that there is an isomorphism

$$C_\Gamma / \Gamma \xrightarrow{\sim} (K^\times)^2 / H_\Gamma.$$

Our strategy should now be clear. Given a curve $X_0 = X$ of genus 2, we consider its Jacobian J_0, and uniformisations of both, by a Schottky group Γ_0. We use the Bost–Mestre algorithm to find a Richelot-isogenous curve X_1, inducing a map on Jacobians $J_1 \longrightarrow J_0$ whose kernel is a $(2, 2)$-group, which we know. We pick an element in the kernel, and lift it by a sequence of Richelot isogenies $J_n \longrightarrow J_{n-1} \longrightarrow \cdots \longrightarrow J_1$ to some desired precision, then map this up to the uniformisation C_{Γ_n} / Γ_n, and then to $(K^\times)^2 / H_{\Gamma_n}$, to recover the periods q_i (or equivalently the half-periods p_i).

5 A p-adic study of the Richelot isogeny

Teitelbaum gives a (linearly) convergent algorithm for computing the half-periods of a genus 2 curve. Essentially, this involves finding a p-adic version of the Thomae formulae, and expressing the coefficients in terms of certain p-adic theta series related to those given in the previous section. The theta series have "q-expansions" which are power series in the three half-periods p_1, p_2 and p_3; these are then explicitly inverted to compute the half-periods. (Note that Guitart–Masdeu [10] remark that a Newton scheme method is a better approach to this inversion than the one given in [27].)

Let us record the following:

Lemma 5.1 *If X is a Type B genus 2 curve, and if $X' \longrightarrow X$ is a Richelot isogeny, then X' also has Type B.*

Proof The simplest way to prove this is simply to observe that if $P_i(x) \equiv (x - \alpha_i)^2$, then $(x - \alpha_i)$ is a factor of $P_i'(x)$ over the residue field. Then $Q_1 = P_2' P_3 - P_2 P_3'$ has a factor over the residue field of $x - \alpha_2$ as this is a factor of both P_2 and P_2', and similarly of $x - \alpha_3$ as this is a factor of both P_3 and P_3'. As Q_1 is a quadratic, we see that over the residue field,

$$Q_1 \equiv c_1(x - \alpha_2)(x - \alpha_3).$$

Similarly,

$$Q_2 \equiv c_2(x-\alpha_3)(x-\alpha_1),$$
$$Q_3 \equiv c_3(x-\alpha_1)(x-\alpha_2),$$

so that X', given by $\Delta y^2 = Q_1 Q_2 Q_3$ again has three pairs of repeated roots over the residue field. □

Teitelbaum gives an example of a curve, $X_0(23)$, of genus 2, with the appropriate reduction type (with $p = 23$), and computes the p-adic half-periods. As already noted, there is a canonical choice of quadratic splitting, and therefore a canonical Richelot isogeny to/from a curve $X_0'(23)$, which is easily computed also to have Type B. The first author ([5]) computed this Richelot-isogenous curve for Teitelbaum's example, used Teitelbaum's method to compute the half-periods, and observed that if p_1, p_2 and p_3 were the half-periods of the original curve, then p_1^2, p_2^2 and p_3^2 were the half-periods of the isogenous curve up to fairly high p-adic precision, so the p-adic periods seem to be squared under the isogeny, just as in the case of a real quadratic splitting. We can prove this using the same methods as indicated above. We sketch this (see [5] for more complete details).

Theorem 5.2 *If $X' \longrightarrow X$ is a Richelot isogeny between two Type B genus 2 curves, then the half-periods of X' are the squares of the half-periods of X.*

Proof Essentially we use the argument above, writing our curve in Rosenhain form, applying the Richelot isogeny with a suitable quadratic splitting, and using Thomae formulae to identify coefficients with theta functions. In the p-adic case, Teitelbaum constructs p-adic theta functions (he only gives explicitly four of them – see (25) of [27]; Guitart–Masdeu [10] give $\vartheta_1, \ldots, \vartheta_9$ below), and gives a p-adic version of the Thomae formulae.

There are 10 p-adic theta functions, which are power series in the half-periods p_1, p_2 and p_3:

$$\vartheta_0 = \sum_{i,j\in\mathbb{Z}} p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \qquad \vartheta_1 = \sum_{i,j\in\mathbb{Z}} (-1)^j p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2}$$
$$\vartheta_2 = \sum_{i,j\in\mathbb{Z}} (-1)^i p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2} \qquad \vartheta_3 = \sum_{i,j\in\mathbb{Z}} (-1)^{i+j} p_1^{j^2} p_2^{i^2} p_3^{(i-j)^2}$$
$$\vartheta_4 = \sum_{i,j\in\mathbb{Z}} (-1)^{i+j} p_1^{j^2-j} p_2^{i^2-i} p_3^{(i-j)^2} \qquad \vartheta_5 = \sum_{i,j\in\mathbb{Z}} p_1^{j^2-j} p_2^{i^2-i} p_3^{(i-j)^2}$$
$$\vartheta_6 = \sum_{i,j\in\mathbb{Z}} (-1)^j p_1^{j^2} p_2^{i^2+i} p_3^{(i-j)^2+(i-j)} \qquad \vartheta_7 = \sum_{i,j\in\mathbb{Z}} p_1^{j^2} p_2^{i^2+i} p_3^{(i-j)^2+(i-j)}$$
$$\vartheta_8 = \sum_{i,j\in\mathbb{Z}} (-1)^i p_1^{j^2+j} p_2^{i^2} p_3^{(i-j)^2-(i-j)} \qquad \vartheta_9 = \sum_{i,j\in\mathbb{Z}} p_1^{j^2+j} p_2^{i^2} p_3^{(i-j)^2-(i-j)}$$

If we make a formal substitution $\Omega = \frac{1}{\pi i}\begin{pmatrix} \log p_2 p_3 & -\log p_3 \\ -\log p_3 & \log p_1 p_3 \end{pmatrix}$ into the classical complex theta functions, then in fact, we recover (almost) exactly these p-adic expressions.

Indeed, an easy calculation gives the following:

$$\begin{aligned}
\theta_0(\Omega) &= \vartheta_0, & \theta_1(\Omega) &= \vartheta_1,\\
\theta_2(\Omega) &= \vartheta_2, & \theta_3(\Omega) &= \vartheta_3,\\
\theta_4(\Omega) &= (p_1p_2)^{\frac{1}{4}}\vartheta_4, & \theta_5(\Omega) &= (p_1p_2)^{\frac{1}{4}}\vartheta_5,\\
\theta_6(\Omega) &= (p_2p_3)^{\frac{1}{4}}\vartheta_6, & \theta_7(\Omega) &= (p_2p_3)^{\frac{1}{4}}\vartheta_7,\\
\theta_8(\Omega) &= (p_1p_3)^{\frac{1}{4}}\vartheta_8, & \theta_9(\Omega) &= (p_1p_3)^{\frac{1}{4}}\vartheta_9.
\end{aligned}$$

Thus every complex theta function identity has a p-adic counterpart. Since it was exactly these identities which are used to prove the doubling of the period matrix above, the same calculations work (with very minor modifications owing to the additional factors such as the $(p_ip_j)^{\frac{1}{4}}$ above) to give the result that the Richelot isogeny corresponds to squaring the half-periods p_1, p_2 and p_3. □

This means that there is a commutative diagram like that of Sect. 2:

$$\begin{array}{ccc}
(K^\times)^2/H' & \xrightarrow{f} & (K^\times)^2/H\\
\downarrow\wr & & \downarrow\wr\\
J' & \xrightarrow{g} & J
\end{array}$$

in which g is induced by the Richelot isogeny.

Conjecture 5.3 *f is given by the identity map on $(K^\times)^2$.*

We state this as a conjecture because we do not yet have a good description of the Mumford uniformisation maps. The corresponding result over $\mathbb{C}$ is fairly easy to prove. We begin by noting (see [4], p. 2, or Sect. 6 below) that elements of the Jacobian are essentially parametrised by pairs of points on the curve. Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on a genus 2 curve. Recall also that $\omega_1 = \frac{\mathrm{d}x}{y}$ and $\omega_2 = \frac{x\,\mathrm{d}x}{y}$ are a basis for the differentials on a curve of genus 2. The Abel–Jacobi map, which identifies the Jacobian with a quotient of $\mathbb{C}^2$ by a lattice is given by mapping (P_1, P_2) to

$$(z_1, z_2) = \int_\infty^{P_1} + \int_\infty^{P_2} (\omega_1, \omega_2)$$

where the integral is defined modulo the lattice of periods. This equality implies that

$$dz_1 = \frac{\mathrm{d}x_1}{y_1} + \frac{\mathrm{d}x_2}{y_2}, \qquad dz_2 = \frac{x_1\,\mathrm{d}x_1}{y_1} + \frac{x_2\,\mathrm{d}x_2}{y_2}.$$

(See also [1], p. 36.) Finally, the equality $\delta_Z\left((lx+m)\frac{\mathrm{d}x}{y}\right) = (lx+m)\frac{\mathrm{d}x}{y}$ under the Richelot isogeny of Sect. 3 shows that dz_i is mapped to dz_i under f^*, so that f is the identity.

In the p-adic case, we expect the same to hold, but need a better description of the vertical maps; however, the correspondence between complex and p-adic theta functions suggests that the result should continue to hold. We assume the conjecture in what follows.

As in Sect. 2, we want to iterate this procedure to get a commutative diagram:

$$\begin{array}{ccccccc} \cdots & \xrightarrow{f_2} & (K^\times)^2/H_2 & \xrightarrow{f_1} & (K^\times)^2/H_1 & \xrightarrow{f_0} & (K^\times)^2/H_0 \\ & & \downarrow{\scriptstyle \phi_2} & & \downarrow{\scriptstyle \phi_1} & & \downarrow{\scriptstyle \phi_0} \\ \cdots & \xrightarrow{g_2} & J_2 & \xrightarrow{g_1} & J_1 & \xrightarrow{g_0} & J_0 \end{array}$$

where $H_n = \{(q_2^{2^n a} q_3^{2^n(a-b)}, q_1^{2^n b} q_3^{2^n(b-a)}) \mid a, b \in \mathbb{Z}\}$.

Next, we wish to iterate a sequence of Richelot isogenies. To fix notation, suppose that $X_0 = X$ is given by $y^2 = f_0$, which reduces modulo $\mathfrak{p}$ to $y^2 = (x-\alpha)^2(x-\beta)^2(x-\gamma)^2$. Write $y^2 = P_1 P_2 P_3$ for the corresponding quadratic splitting; i.e. $P_1 = (x-\alpha_1)(x-\alpha_2)$, where α_1 and α_2 are the two roots of f_0 which are congruent to α modulo $\mathfrak{p}$, so that $P_1 \equiv (x-\alpha)^2$, and similarly for P_2 and P_3. As above, when we work out $Q_1 = P_2' P_3 - P_2 P_3'$, we find that $Q_1 \equiv (x-\beta)(x-\gamma)$ etc., up to constant factors. But in fact, we get p-adic convergence, and at a quadratic rate. For this, we write $\alpha = (\alpha_1 + \alpha_2)/2$, so that $\alpha_1 = \alpha + \epsilon_\alpha$ and $\alpha_2 = \alpha - \epsilon_\alpha$, and assume that $\epsilon_\alpha \in \mathfrak{p}^{v_\alpha}$, with ϵ_β, v_β, ϵ_γ and v_γ defined analogously. Write $v = \min\{v_\alpha, v_\beta, v_\gamma\}$. Then a simple manipulation of the quadratic formula shows that the roots of Q_1 are $\beta + \epsilon_\beta'$ and $\gamma + \epsilon_\gamma'$, where $\epsilon_\beta' \in \mathfrak{p}^{2v}$ and $\epsilon_\gamma' \in \mathfrak{p}^{2v}$. Thus an application of the Richelot process leads to pairs of roots which are in a p-adic disc of the square of the radius of the original pairs.

After one iteration, we get a curve $X_1 = X'$ given by $\Delta y^2 = Q_1 Q_2 Q_3$. If we used these quadratics for the next step, we would return to the original curve. Instead, we redistribute the roots, and write the equation of X_1 as $t_1^2 y^2 = P_1^{(1)} P_2^{(1)} P_3^{(1)}$, where $P_1^{(1)}$ denotes the quadratic whose roots are the roots of Q_2 and Q_3 congruent to α, and so on. Then we can repeat the process with these new quadratics to find a curve X_2, and the above argument shows that the curves $X_0 = X, X_1, X_2, \ldots$ converge quadratically to a limit $T^2 y^2 = (x-a)^2(x-b)^2(x-c)^2$. That is, if we write $t_k y^2 = f_k$ for the curve X_k, where f_k is monic, we see that if the pairs of roots of f_0 are congruent mod $\mathfrak{p}$, then the pairs of roots of f_k are congruent mod $\mathfrak{p}^{2^k}$.

Let us record this result:

Proposition 5.4 *The sequence of equations for X_1, X_2, $X_3, \ldots$ converges quadratically.*

We know that the kernel of f is generated by $(q_2 q_3, q_3^{-1})$ and $(q_3^{-1}, q_1 q_3)$, and that the kernel of g by the divisors corresponding to differences of Weierstrass points in the same factor of the quadratic splitting.

We will lift divisors D_1 in the kernel of g_0 using the Richelot isogeny to divisors D_2, D_3, etc., as far as some D_n, which we expect to give the result to our desired precision; at this precision, the curve and divisor will not change further, so we can assume we

are at X_∞, and then lift via ϕ_∞ to $(K^\times)^2$, enabling us to recover information about the periods.

We expect that the divisors can be chosen to converge p-adically also, and this appears to be the case in examples we have calculated. However, as we will explain below, our method for pulling back the Richelot isogeny is very indirect, and we do not yet have a proof.

6 Practical implementation: lifting via the Richelot isogeny

In order to make this into a practical algorithm, we need to be able to lift a divisor through the Richelot isogeny, and then invert a vertical map. So, given a divisor D on a genus 2 curve X, and a Richelot isogeny $g : X' \longrightarrow X$, we need to work out the divisor $g^{-1}(D)$. Further, we want to be able to see that if X' and X are congruent to some p-adic precision, so are the divisors $g^{-1}(D)$ and D.

We now explain how to make the formula for g explicit.

We take a curve of the form $y^2 = P_1P_2P_3$, with Weierstrass points P_1^+, P_1^-, P_2^+, P_2^-, and P_3^+, P_3^-, corresponding to the three quadratics. Then we will be applying our algorithm to the divisor $D_1 = (P_1^+) - (P_1^-)$ (and repeating it for the other pairs).

The formula in Sect. 3 for lifting divisors applies here; since it is a 2-to-1 map, each point will lift to a pair of points, so that we would expect our divisor to be supported at 4 points. However, it is well known, and explained in [4] (pp. 2–3), for example, that any divisor is linearly equivalent to one supported at 2 points. For this, we note that if (x, y) is any point on X, $\mathcal{O} = (x, y) + (x, -y)$ represents the canonical class in $\mathrm{Pic}^2(X)$ (note that any two divisors of this form are linearly equivalent). There is an isomorphism $\mathrm{Pic}^0(X) \xrightarrow{\sim} \mathrm{Pic}^2(X)$ given by sending a divisor D to $D + \mathcal{O}$. The Riemann–Roch theorem tells us that in any divisor class other than $\mathcal{O}$, there is exactly one effective divisor, i.e. a divisor of the form $(P) + (Q)$. The group law on the Jacobian in these terms is beautiful: given one divisor class represented by $(P) + (Q)$, and another represented by $(P') + (Q')$, then (generically, at least) there is a unique cubic $y = m(x)$ passing through each of the points P, Q, P' and Q'. The cubic $y = m(x)$ meets X at two further points, P'' and Q'', and the group law states that

$$((P) + (Q)) + ((P') + (Q')) + ((P'') + (Q'')) = 3\mathcal{O}$$

in $\mathrm{Pic}^6(X)$. The inverse of a divisor $(P) + (Q)$ is $(\overline{P}) + (\overline{Q})$, where, if $P = (x, y)$ lies on the curve, $\overline{P} = (x, -y)$. We will call a divisor *reduced* if it is of the form $(P) + (Q)$.

The dual $\widehat{g}$ of the Richelot isogeny is, as noted above, given by exactly the same correspondence (see [25], Proposition 8.4.12 and Corollary 8.4.14), and $\widehat{g} \circ g = [2]$, multiplication by 2. The strategy is to halve the given divisor D on J, and then apply the dual isogeny $\widehat{g}$. This gives the preimages under the Richelot isogeny. In practice, one needs to find only one halving D_2 with $[2]D_2 = D$; we apply the dual Richelot map to get $g^{-1}(D) = \widehat{g}(D_2)$, and to get the other preimages, we add the divisors in the kernel of g, whose structure we mentioned earlier.

The problem of halving a divisor is called *bisection*, and has been previously studied in various papers on cryptography, in the context of halving divisors for hyperelliptic curves over finite fields. For the particular models which we need, this was essentially done by Miret, Pujolàs and Thériault in [17] (see also the recent preprint of Miret, Pujolàs and Rio [16]). It works well for general curves of genus 2 with sextic models (much of the literature used quintic models). We again write $D = (x_1, y_1) + (x_2, y_2)$ for the original divisor, and $D_2 = (u_1, v_1) + (u_2, v_2)$ for the bisection. There should be 16 bisections D_2. We write $S = u_1 + u_2$ and $P = u_1 u_2$, so that again

$$x^2 - Sx + P = (x - u_1)(x - u_2).$$

Unravelling the explicit group law on the Jacobian means that the bisection process is equivalent to solving

$$f - m^2 = c(x^2 - sx + p)(x^2 - Sx + P)^2,$$

where $m(x)$ is a cubic, c is a constant, and S and P are the sum and product of u_1 and u_2, the x-coordinates of the points in the support of D_2.

It is explained in [17] how to solve this. The cubic m is constrained to be of the form

$$(k_1 x + k_0)(x^2 - sx + p) - (\gamma x + \delta),$$

where $y = \gamma x + \delta$ is the line joining (x_1, y_1) and (x_2, y_2).

By comparing coefficients, [17] explain that one can eliminate S and P, and also c, and get 2 equations relating k_0 and k_1 coming from the equality above in the bottom 2 degrees. After clearing denominators, the resultant of these two equations with respect to k_0 is a degree 32 polynomial in k_1, but there are some trivial factors (coming from the clearing of the denominators) which can be removed, leaving a degree 16 equation for k_1. This degree 16 equation is explicit, but complicated.

We find a bisection for D by solving this degree 16 equation p-adically to get k_1 up to the desired precision, finding k_0 by substituting it into the two equations given, and then recovering S and P. This indirect method works successfully, although one expects as above that there should be a better way. Once the first bisection is identified by this method which gives the preimage $g^{-1}(D)$ congruent to D, since the subsequent curves are increasingly p-adically congruent, one can simply Hensel-lift each solution in turn to get subsequent ones.

Remark 6.1 We hope that in the case where $y^2 = f = P_1 P_2 P_3$, then the degree 16 equation should somehow be expressible as a quartic function of a quartic, reflecting the decomposition of [2] as the product of $\widehat{g} \circ g$. Miret, Pujolàs and Rio ([16]) show at least that the degree 16 equation can naturally be written as the product of four quartics, at least in the case where f is a monic quintic.

At the end of this process, we have a divisor D_n on X_n, which arises by successive pull-backs of a divisor D_1 on X_1 in the kernel of $g_0 : J_1 \longrightarrow J_0$. Assuming our

precision is at the desired level, we know that it will not change with further iterations, and can assume that it is D_∞ on X_∞, up to the desired precision. We then need to lift it to $(K^\times)^2$.

7 $X_0(23)$

In order to begin to test our method, we compared the results with those given in Teitelbaum [27]. Teitelbaum uses the explicit equations for $X_0(23)$, $X_0(29)$ and $X_0(31)$ (computed by Fricke), all of genus 2, and all with Type B reduction. Since most details are given for $X_0(23)$, we have used this curve as our main test.

In Sect. 3.3 of [27], we find the equation for $X = X_0(23)_{/\mathbb{Q}_{23}}$ as

$$y^2 = x^6 - 14x^5 + 57x^4 - 106x^3 + 90x^2 - 16x - 19.$$

We find that

$$y^2 \equiv (x+2)^2(x+5)^2(x+9)^2 \pmod{23},$$

confirming that X has Type B reduction. The Weierstrass points of X are rational over $\mathbb{Q}_{23}(\pi)$, where $\pi^2 = -23$. There are three pairs of roots; Teitelbaum arbitrarily chooses one from each pair, and moves them to 0, 1 and ∞. This converts the curve into one in Rosenhain form:

$$y^2 = x(x-1)(x-\lambda)(x-\mu)(x-\nu).$$

We can suppose $\pi|\lambda$, $\pi|\mu - 1$ and $\pi|\nu^{-1}$ (as we have Type B reduction). Teitelbaum works out an explicit model for a genus 2 curve in Rosenhain form in terms of p-adic theta functions depending only on the half-periods; these resemble the function in the previous section, except that they are really the theta constants, where $w_1 = w_2 = 1$. Teitelbaum uses 4 of the theta functions listed above (the four functions appearing in (25) of [27] are ϑ_1, ϑ_5, ϑ_2 and ϑ_4, respectively, in our numbering) and is able to write down the coefficients λ, μ and ν in terms of these theta functions. Equating the equation for $X_0(23)$ in Rosenhain form with Teitelbaum's explicit model, one can invert the theta functions to work out the half-periods, which Teitelbaum does up to π^{10}. Some formulae are given in [27], and these seem to become complicated quickly. We hope that our method, assuming it can be completed, is more likely to be computationally feasible for larger degree, and will, after a certain point, be faster to implement.

We pulled a divisor in the kernel of $X_1 \longrightarrow X_0$ up to X_2 and X_3, and it certainly appeared to converge quadratically.

Let us give some numerical results. All computations will be modulo π^{20}. We first give the roots of the quadratic in $\mathbb{Q}_{23}(\pi)$; Hensel's Lemma (or Magma) gives their

values as follows:

$$\begin{aligned}
a_0 &= 779959976562 + 33733491857\pi\ ,\\
a_0' &= 779959976562 - 33733491857\pi\ .\\
b_0 &= 241232708350,\\
b_0' &= 41266787476103,\\
c_0 &= 26196575459988 + 649618143166\pi,\\
c_0' &= 26196575459988 - 649618143166\pi.
\end{aligned}$$

We now compute the chain of isogenous curves X_i obtained as above:

$$\begin{aligned}
X_1 : y^2 = {} & 14509968966141x^6 + 13535473244274x^5\\
& - 4366138213591x^4 - 383149059076x^3\\
& + 4532268917237x^2 + 10611945668949x + 11501225120914
\end{aligned}$$

with roots

$$\begin{aligned}
a_1 &= 29969023457189,\ a_1' = 36816510168425,\\
b_1 &= 2703407962350,\quad b_1' = 41130794360331,\\
c_1 &= 37949541236172,\ c_1' = 6221753140751.
\end{aligned}$$

We already know that all the curves X_i's are totally split and their roots lie in the same p-adic discs as those of X_0; indeed one checks that

$$a_1 \equiv a_1' \equiv 18 \mod \pi,\quad b_1 \equiv b_1' \equiv 21 \mod \pi,\quad c_1 \equiv c_1' \equiv 14 \mod \pi.$$

Here is the equation for X_2 and its roots:

$$\begin{aligned}
X_2 : y^2 = {} & 15963560922167x^6 + 8915045081136x^5 + 5655951820305x^4\\
& + 7187214907216x^3 + 9290858991658x^2 + 18116669010963x\\
& - 9470171526445\ ,\\
a_2 &= 15634233532478,\quad a_2' = 38514512500429,\\
b_2 &= 41230679116716,\quad b_2' = 37806965241739,\\
c_2 &= 18164834403771,\quad c_2' = 30030908259387.
\end{aligned}$$

Finally, the equation for X_3 and its roots:

$$\begin{aligned}
X_3 : y^2 = {} & 13413380228472x^6 + 9889873468227x^5 + 11869333871359x^4\\
& + 19069176773695x^3 - 9637185255233x^2\\
& + 2318445679270x - 6104023778492\ ,\\
a_3 &= 6361117409629,\quad a_3' = 6361117409629,
\end{aligned}$$

$$b_3 = 1577149810583, \quad b_3' = 36895404172314,$$
$$c_3 = 23050359306739, \quad c_3' = 15552288918781.$$

In fact,

$$\begin{aligned}
&a_0 \equiv a_0' \pmod{\pi^3}, \quad b_0 \equiv b_0' \pmod{\pi^2}, \quad c_0 \equiv c_0' \pmod{\pi},\\
&a_1 \equiv a_1' \pmod{\pi^6}, \quad b_1 \equiv b_1' \pmod{\pi^4}, \quad c_1 \equiv c_1' \pmod{\pi^2},\\
&a_2 \equiv a_2' \pmod{\pi^{12}}, \; b_2 \equiv b_2' \pmod{\pi^8}, \quad c_2 \equiv c_2' \pmod{\pi^4},\\
&a_3 \equiv a_3' \pmod{\pi^{24}}, \; b_3 \equiv b_3' \pmod{\pi^{16}}, \; c_3 \equiv c_3' \pmod{\pi^8},
\end{aligned}$$

an even stronger form of doubling of π-adic precision than proven above.

Next, let $D_0 \in J_0$ be the zero divisor, and we lift it along the chain of Jacobians. (Note that we will switch between Mumford representations and actual divisors whenever suitable.)

There are three non-zero divisors on J_1 in the kernel of $J_1 \longrightarrow J_0$:

$$\begin{aligned}
Du_1 &= \left[(u_0, 0) + (u_0', 0)\right] = \left[x^2 + 3772686830795x + 4779300317558, 0\right],\\
Dv_1 &= \left[(v_0, 0) + (v_0', 0)\right] = \left[x^2 + 5235734615709x - 20478600731137, 0\right],\\
Dw_1 &= \left[(w_0, 0) + (w_0', 0)\right] = \left[x^2 + 1906593082874x + 1490035220585, 0\right].
\end{aligned}$$

To lift these further onto J_2, we use the bisection method as previously described. That is, we wish to compute

$$Du_1 \longrightarrow \frac{1}{2}Du_1 \longrightarrow Du_2,$$

and write $\hat{g}_1$ for the second map in this composition.

This gives the bisection as

$$\frac{1}{2}Du_1 = [P_1 + P_2] = \left[x^2 + 3772686830795x + 4779300317558, 0\right],$$

where

$$\begin{aligned}
P_1 &= (20843997281321 + 37869416972530\pi, 20700417432520 + 17537234561531\pi),\\
P_2 &= (24338480333321 + 40747895489590\pi, 13552216979968 + 12473332310983\pi).
\end{aligned}$$

Before mapping P_1 and P_2 to J_2, one first has to scale by the square root of the x^6 coefficient of X_1 so that it lies on the curve $y^2 = P_1 Q_1 R_1$ (instead of $T_0 y^2 = U_0 V_0 W_0$ as it currently does). Now mapping the scaled points via the Richelot isogeny, and then rescaling it back gives

$$\hat{g_1}(P_1) = \left[Q_1 + Q_1'\right],$$

where

$$Q_1 = (15588142880255 + 13614777038871\pi, 2026443975492 + 31565145522315\pi),$$
$$Q_1' = (3503913201810 + 37211337310263\pi, 1634554359251 + 10681002910033\pi).$$

Similarly

$$\hat{g_1}(P_2) = \left[Q_2 + Q_2'\right],$$

where

$$Q_2 = (12952102174602 + 17872156829551\pi, 39129102600005 + 23905673565742\pi),$$
$$Q_2' = (34057150363331 + 36281579638141\pi, 36203107768550 + 25761328056179\pi).$$

Combining everything, we have lifted Du_1 to

$$\begin{aligned}\hat{g_1}(Du_1) &= \left[Q_1 + Q_1' + Q_2 + Q_2'\right] \\ &= [x^2 + 36833651358680x + 5787826917764, \\ &\quad 3303842326834x + 16005171221467].\end{aligned}$$

Note that there are four preimages of Du_1, but only one has the property that the support of the divisors are in the same p-adic discs as for Du_1:

$$\begin{aligned}Du_2 = \Big[&x^2 + 570508136719x + 38814447073528, \\ &39947032033123x + 23933496908852\Big].\end{aligned}$$

Similarly, the lifts of Dv_1 and Dw_1 are given by

$$Dv_2 = \left[x^2 + 28747176982521x + 15742432005809, 23856327829181x + 21330178054941\right],$$
$$Dw_2 = \left[x^2 + 14257352574105x + 16172605252402, 41179889101919x + 9512547229701\right].$$

One checks that all the numbers defining the Mumford representation of Du_2 are congruent to those defining the Mumford representation of Du_1 modulo π^2, so that the divisors are the same modulo 23. Similar results hold for Dv_2 and Dv_1, and Dw_2 and Dw_1.

Without a complete theory for the p-adic uniformisation maps, we are not yet able to compute the periods to compare with Teitelbaum's results. If we had such a theory, this lift should already be sufficient to compute the periods modulo π^8; we hope that this method might eventually prove more efficient than existing methods for genus 2 curves with Type B reduction.

Acknowledgements We thank Tobias Berger, John Cremona, Victor Flynn, David Grant, Haluk Şengün and Michael Stoll for their interest in this project, and Jordi Pujolàs for useful discussions relating to Sect. 6 (and in particular, for providing an early draft of [16]). We also thank the anonymous referee for providing a number of useful suggestions which have improved the exposition of the paper.

Data availibility Data sharing is not applicable to this article as no datasets were generated or analysed during the current study.

Declarations

Conflict of interest The first author thanks the University of Sheffield for its support as a graduate student via a Graduate Teaching Assistantship. This work formed part of his thesis ([5]), supervised by the second author. The authors received no further funding from any organisation for this work. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Baker, H.F.: An introduction to the theory of multiply periodic functions. Cambridge University Press, Cambridge (1907)
2. Borcherds, R.E.: Automorphic forms on $O_{s+2,2}(\mathbb{R})$ and infinite products. Invent. Math. **120**, 161–213 (1995)
3. Bost, J.-B., Mestre, J.-F.: Moyenne arithmético-géométrique et périodes des courbes de genre 1 et 2. Gaz. Math. **38**, 36–64 (1988)
4. Cassels, J.W.S., Flynn, E.V.: Prolegomena to a middlebrow arithmetic of curves of genus 2, LMS Lecture Note Series, vol. 230. Cambridge University Press, Cambridge (1996)
5. Chow, R.: The arithmetic-geometric mean and periods of curves of genus 1 and 2, PhD thesis, University of Sheffield (2018)
6. Cox, D.A.: The arithmetic-geometric mean of Gauss. Enseign. Math. **30**, 275–330 (1984)
7. Cremona, J.E., Thongjunthug, T.: The complex AGM, periods of elliptic curves over $\mathbb{C}$ and complex elliptic logarithms. J. Number Theory **133**, 2813–2841 (2013)
8. Flynn, E.V.: Descent via isogeny in dimension 2. Acta Arith. **66**, 23–43 (1994)
9. Grant, D.: Formal groups in genus two. J. Reine Angew. Math. **411**, 96–121 (1990)
10. Guitart, X., Masdeu, M.: Periods of modular GL_2-type abelian varieties and p-adic integration. Exp. Math. **27**, 344–361 (2018)
11. Henniart, G., Mestre, J.-F.: Moyenne arithmético-géométrique p-adique. C. R. Acad. Sci. Paris Sér. I Math. **308**, 391–395 (1989)
12. Hudson, R.W.H.T.: Kummer's quartic surface. Cambridge University Press, Cambridge (1905)
13. Kadziela, S.: Rigid analytic uniformization of curves and the study of isogenies. Acta Appl. Math. **99**, 185–204 (2007)
14. Manin, Y., Drinfeld, V.: Periods of p-adic Schottky groups. J. Reine Angew. Math. **262**(263), 239–247 (1973)
15. Menezes, A., Wu, Y.-H., Zuccherato, R.: An elementary introduction to hyperelliptic curves, technical report CORR 96–19. University of Waterloo, Ontario (1996)
16. Miret, J., Pujolàs, J., Rio, A.: The splitting of multiplication by 2 in genus 2, preprint (2018)
17. Miret, J., Pujolàs, J., Thériault, N.: Bisection for genus 2 curves with a real model. Bull. Belg. Math. Soc. Simon Stevin **22**, 589–602 (2015)
18. Morikawa, H.: Theta functions and abelian varieties over valuation fields of rank one I. Nagoya Math. J. **20**, 1–27 (1962)
19. Morikawa, H.: Theta functions and abelian varieties over valuation fields of rank one II. Nagoya Math. J. **21**, 231–250 (1962)
20. Mumford, D.: An analytic construction of degenerating curves over complete local rings. Compos. Math. **24**, 129–174 (1972)
21. Mumford, D.: An analytic construction of degenerating abelian varieties over complete rings. Compos. Math. **24**, 239–272 (1972)
22. Mumford, D.: Tata lectures on theta II, Progr. in Math. **43** (1984)
23. Richelot, F.: De transformatione integralium Abelianorum primi ordinis commentation. J. Reine Angew. Math. **16**, 221–341 (1837)
24. Silverman, J.: Advanced topics in the arithmetic of elliptic curves. Springer, New York (1994)
25. Smith, B.: Explicit endomorphisms and correspondences, PhD thesis, University of Sydney (2005)

26. Tate, J.: A review of non-Archimedean elliptic functions. In: Coates, J., Yau, S.-T. (eds.) Elliptic curves, modular forms and Fermat's last theorem, pp. 310–332. International Press, Vienna (1997)
27. Teitelbaum, J.: p-adic periods of genus two Mumford-Schottky curves. J. Reine Angew. Math. **385**, 117–151 (1988)