Computation of the p-adic period via 3-isogenies for $p = 2 \pmod 3$

Hubert Dubé *
Department of Mathematics, McGill University
hubert.dube@mail.mcgill.ca

September 12, 2015

Abstract

In this document, we attempt to replicate Mestre and Henniart's technique for computing the p-adic period for elliptic curves over $\mathbb{Q}_p$ described in [HM89]. While their article did so by considering towers of 2-isogenous curves and the p-adic analogue to the arithmetic-geometric mean, we do so by considering 3-isogenies on $\mathbb{Q}_p$ for $p = 2 \pmod 3$ instead. We produce an alternative algorithm and provide an example to demonstrate its effectiveness.

This document is the result of a Summer research project under the immensely insightful guidance of professor Henri Darmon and was made possible by the National Science and Engineering Council's Undergraduate Student Research Awards (NSERC USRA).

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}_p$ given by the standard Weierstrass planar equation $y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}_p$. Suppose the j-invariant of E to be non-integral, i.e. $|j| > 1$. John Tate has demonstrated in [Tat74] that there exists an $\mathbb{Q}_p(\sqrt{-c_6})$-isomorphism $\mathbb{Q}_p^\times/q^\mathbb{Z} \cong E$ for some $|q| < 1$. We call q the p-adic period and we call $E(q) = \mathbb{Q}_p^\times/q^\mathbb{Z}$ the Tate curve. Let ψ be such an isomorphism. Then we also have $\psi^* (\omega(E)) = u \, \mathrm{d}t/t$ where $u^2 \in \mathbb{Q}_p^\times$ and $\mathrm{d}t/t$ is $E(q)$'s canonical differential.

Mestre and Henniart published in 1989 an algorithm for computing the p-adic period of a curve E which roughly goes as follows. First, one performs a change of variable to obtain a planar equation $y^2 = x(x+A_0)(x+A_0-B_0)$. By considering a modified arithmetic-geometric sequence $(A_n, B_n)_{n\geq 0}$, one produces a tower of curves

$$E_0 \leftarrow E_1 \leftarrow \cdots \leftarrow E_n \leftarrow E_{n+1} \leftarrow \cdots .$$

where $E_n : y^2 = x(x + A_n)(x + A_n - B_n)$ linked together via 2-isogenies. By reversing these isogenies properly, one is able to start from a point $P \in E_0$, get to $P_\infty \in E_\infty$ and compute the value t for which $\psi(t) = P$. A slight modification of this algorithm permits one to compute the period q.

In this document, we therefore consider chains of 3-isogenies to compute the p-adic period. The core idea of the algorithm follows closely the model of Mestre and Henniart. However, for simplicity's sake, we consider only primes of the form $p = 2 \pmod 3$ in order to have unique cube roots in $\mathbb{Q}_p$. This heavily simplifies the reversing action of isogenies. To see why this restriction implies uniqueness of cube roots, it is enough to see that the map $x \mapsto x^3$ is injective in $\mathbb{F}_p$ since $x^3 - 1$ has a unique root. Furthermore, the quantity u is computed using Mestre and Henniart's original algorithm on the arithmetic-geometric mean.

2 The $\mathbb{Q}_p$-rational subgroup of order 3

Mestre and Henniart's algorithm is powerful due to its inherent simplicity which follows from a great choice of Weierstrass form. The planar equation chosen is a fantastic one to study 2-torsion subgroups as all order

*This paper was made possible thanks to the NSERC Undergraduate Student Research Award under the supervision of professor Henri Darmon.

2 points of E become immediately obvious and easy to work with. With that in mind, we seek to find a similar form for rational 3-torsion subgroups of $E(\mathbb{Q}_p)$. This proves to be difficult as though the subgroup may be rational, its elements may not be.

Let $E(K)$ be an elliptic curve over K (with characteristic different from 2 and 3) and let $G = \{\mathcal{O}, P, -P\}$ be a subgroup of $E(L)$ for some finite extension $L \supset K$ where we write $P = (x_0, y_0)$. Under the fair assumption that E has planar equation

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

we note that $[2]P = -P = (x_0, -y_0)$. For any $\sigma \in \mathrm{Gal}(L/K)$, we have $P^\sigma = (\sigma(x_0), \sigma(y_0)) = (x_0, \pm y_0)$, and therefore $x_0 \in K$. Up to a change of variable

$$(x, y) \mapsto (x - x_0, y),$$

we may assume $P = (0, t)$ for some $t \in L$. In particular, we have $t^2 = a_6$, and therefore L is, at most, a quadratic extension of K. Furthermore, a simple computation shows that

$$0 = x([2]P) = \frac{a_4^2}{4a_6} - a_2 \quad \Longrightarrow \quad a_4^2 - 4a_2a_6 = 0,$$

which means that we may find $\alpha, \beta, \gamma \in K$ such that

$$a_2x^2 + a_4x + a_6 = \gamma(\alpha x + \beta)^2.$$

Therefore, not only is the order 3 group G K-rational, but the above formula permits one to display it in an obvious manner. We have the following equation for E:

$$E : y^2 = x^3 + \gamma(\alpha x + \beta)^2,$$

where the obvious order 3 group is given by $\{\mathcal{O}, (0, \beta\sqrt{\gamma}), (0, -\beta\sqrt{\gamma})\}$. In general, however, there is no unique way to define α, β and γ unless we require more conditions and thus we will usually simply have equations of the form $y^2 = x^3 + ax^2 + bx + c$ with the extra assumption that $b^2 - 4ac = 0$.

3 The 3-descent on $\mathbb{Q}_p$ for $p \equiv 2 \pmod 3$

Let E_0 be an elliptic curve defined over $\mathbb{Q}_p$ for $p \equiv 2 \pmod 3$ of the form $E : y^2 = x^3 + a_0x^2 + b_0x + c_0$ where $b_0^2 - 4a_0c_0 = 0$ as above. Assume further that $j(E)$ is non-integral such that there exists $q \in \mathbb{Q}_p$ such that $E(\mathbb{Q}_p) \cong E(q) = \mathbb{Q}_p^\times / q^{\mathbb{Z}}$, and that the group $\{\mathcal{O}, (0, \sqrt{c_0}), (0, -\sqrt{c_0})\}$ is generated by a primitive cubic root of unity ζ_3 in $E(q)$.

Define then for $n \geq 0$

$$\begin{aligned}
\tilde{a}_n &= -\frac{a_n}{3}, \\
\tilde{b}_n &= \frac{1}{243}\left(8a_n^2 - 27b_n\right), \\
\tilde{c}_n &= -\frac{1}{19683}\left(16a_n^3 - 108a_nb_n + 729c_n\right)
\end{aligned}$$

as well as the following quantity:

$$r_n = \frac{1}{9}\left[\kappa_n - \frac{54b_n - 16a_n^2}{\kappa_n} - 4a_n\right], \qquad \text{where } \kappa_n = (432a_nb_n - 2916c_n - 64a_n^3)^{1/3}.$$

The advantage of working in a p-adic field with $p = 2 \pmod 3$ is that we have a guarantee on the uniqueness of κ_n as there exists at most only two rational 3-torsion groups on elliptic curves. Finally, we define

$$\begin{aligned}
a_{n+1} &= \tilde{a}_n + 3r_n, \\
b_{n+1} &= \tilde{b}_n + 2r_n\tilde{a}_n + 3r_n^2, \\
c_{n+1} &= \tilde{c}_n + r_n\tilde{b}_n + r_n^2\tilde{a}_n + r_n^3
\end{aligned}$$

and

$$E_{n+1} : y^2 = x^3 + a_{n+1}x^2 + b_{n+1}x + c_{n+1},$$

where again we have the property that $b_{n+1}^2 - 4a_{n+1}c_{n+1} = 0$.

This sequence of elliptic curves is used to define the chain of isogenies

$$E_0 \xleftarrow{\varphi_1} E_1 \xleftarrow{\varphi_2} \cdots \xleftarrow{\varphi_n} E_n \xleftarrow{\varphi_{n+1}} \cdots$$

which are isogenies $\varphi_n : E_n \longrightarrow E_{n-1}$ given by the equations

$$\begin{aligned} x_{n-1} &= \frac{3(x_n + r_{n-1})^3 + 4a_n(x_n + r_{n-1})^2 + 6b_n(x_n + r_{n-1}) + 12c_n}{3(x_n + r_{n-1})^2}, \\ y_{n-1} &= y_n \left(1 - \frac{2(b_n(x_n + r_{n-1}) + 4c_n)}{(x_n + r_{n-1})^3}\right). \end{aligned} \tag{3.1}$$

For every $n \geq 0$, we have that E_n is isomorphic to $E\left(q^{3^n}\right)$ via a uniquely defined map ψ_n for which $\psi_n^*(\omega_n) = u\,\mathrm{d}t/t$.

As n goes to infinity, the equation for E_n tends to the curve E_∞ whose equation is given by $y^2 = x^3 - \frac{3}{4u^2}x^2 + \frac{1}{6u^4}x - \frac{1}{108u^6}$. We denote by ψ_∞ the isomorphism from $\mathbb{Q}_p^\times$ to $E_\infty \setminus \left(1/(3u^2), 0\right)$ given by

$$X(t) = \left(\frac{t}{u^2(1-t)^2} + \frac{1}{3u^2}\right), \qquad Y(t) = \frac{t(1+t)}{2u^3(1-t)^3}.$$

The algorithm for computing the p-adic period then relies on inverting the φ_n in such a way that the parameter t from two consecutive Tate curves is preserved, i.e. we have $t_n \in E\left(q^{3^n}\right)$ for which $\varphi_{n+1}(\psi_{n+1}(t_{n+1})) = \psi_n(t_n)$ such that $t_\infty = t_n \pmod{q^{3^n}}$. Because we only want to compute q and not an arbitrary parameter for any given point on the curve E_0, we only need to invert the abscissa coordinate of the isogeny.

The three possible inverses to the first equation in (3.1) are the three roots to the polynomial

$$3(X + r_{n-1})^3 + (4a_n - 3x_{n-1})(X + r_{n-1})^2 + 6b_n(X + r_{n-1}) + 12c_n \tag{3.2}$$

and the one preserving the parameter in $E\left(q^{3^n}\right)$ will be the root x_n whose p-adic distance from x_{n-1} is smallest.

For any curve E with $|j| > 1$, the algorithm is thus as follows:

1. Using Mestre and Henniart's algorithm [HM89], compute the quantity u associated with E. Then, transform the equation of E to the form discussed above using Hensel's lemma. We denote this isomorphic curve E_0.

2. Using the formulas above, compute E_1 and let $x_1 = r_0$. By repeatedly solving equation (3.2), compute x_∞ to the desired degree of precision.

3. Finally, with u and x_∞ known, compute the p-adic period via

$$q = 1 + \frac{3 + \sqrt{-3(1 - 12u^2x_\infty)}}{6u^2x_\infty - 2}.$$

The square root is chosen in such a way that $|q| < 1$.

We note that if one makes an erronous choice of square root, one ends up with q^{-1} rather than the desired period. Therefore inverting the result will give rise to q.

Finally, given an arbitrary point $P_0 \in E_0$, it is equally easy to compute $t \in E(q)$ such that $\psi_0(t) = P_0$ by letting $x_0 = x(P_0)$ and starting in E_0 instead.

4 Application to a curve

Let E be the modular curve $X_1(11)$ whose equation is $y^2+y=x^3-x^2$ with $j(E)=-4096/11$. This example was worked out in Mestre and Henniart's original paper and as we will see here, the new algorithm still yields the same answer. The parameter u^2 is computed using the algorithm provided in [HM89], while x_∞ and q are both computed using this new algorithm. We also compute the abscissa x_0 of the 3-torsion point using Hensel's lemma. The quantities a_1, b_1 and c_1 are then a byproduct of this computation.

These computations yield the follwing results, here computed to an accuracy of $\mathcal{O}(11^{64})$, similar to what was done in Mestre and Henniart's paper:

$$\begin{aligned}
x_0 &= 3.26656418aaaa704a5a515700977876a07284a917753659457327263915207498 9\ldots\\
a_1 &= 8.67858242aaaa121969644020511419 92a723975a06a75635007a77a55470a264\ldots\\
b_1 &= a.012119641261096372525970a667831561680286725384034541061161398a689\ldots\\
c_1 &= a.7a78a553340462649017115a3109651a15397751953a44348561099932807500\ldots\\
u^2 &= 3.663a634a3355328016575911937 88a10218097976820538364 7a372a83514524\ldots\\
x_\infty &= 5.288a825517860a5a59549a94016a023095227941563107437539829a272a9919\ldots\\
q &= 0.835809210a029a177264090910424a74845992542398373657759354 8a31a068\ldots
\end{aligned}$$

Computations where performed in the number theoretic programming language PARI/GP Calculator, version 2.7.2. Here we wrote $\sum a_j p^j$ as the string $a_{-n}\ldots a_{-1}\ a_0\ .\ a_1\ a_2\ldots$ with the letter a denoting the decimal value 10 as is usual in hexadecimal notation.

5 Closing remarks and further research

Clearly this algorithm does not provide the level of simplicity that [HM89] did and therefore does not immediately provide a useful alternative to the computation of the p-adic period. It is also limiting due to the restriction that $p=2 \pmod 3$, though extending the result to all primes $p\neq 2,3$ depends solely on properly defining the cube root function in $\mathbb{Q}_p$. Furthermore, by restricting our study to the classical Weierstrass form of the elliptic curve, we were unable to provide a powerful way to study 3-torsion subgroups and their associated 3-isogenies. The sequences that resulted from this study were complicated and did not appear to have any sort of meaningful interpretation. In particular, this prevents (or renders very difficult) the analysis of convergence of the various sequences involved in the algorithm.

It seems like before tackling higher order rational torsion subgroups, we should study the rational 3-torsion subgroups in more depth. Perhaps we could find simplified formulas by considering alternative forms to elliptic curves, such as the Hessian form of elliptic curves, namely curves of the form

$$x^3+y^3+z^3=3dxyz,$$

or the Jacobi quartic of the form

$$y^2=ex^4+2ax^2z^2+z^4.$$

In any case, the goal is to obtain a planar equation involving a polynomial equation whose roots are the coordinates of all 3-torsion points of any given curve.

Note that any attempt at repeating the result for 5-isogenies, or, for that matter, for n-isogenies with $n>4$, can prove itself to be extremely difficult as it involves solving an n-th order polynomial equation.

As a closing note, I, the author, would like to thank professor Henri Darmon for the patient guidance, encouragement and insightful advice he has provided over the course of the Summer. This document would not have been possible without his help and I am extremely grateful for it.

References

[HM89] Guy Henniart and Jean-François Mestre. Moyenne arithmético-géométrique p-adique. *CR Acad. Sci. Paris Sér. I*, 308:391–395, 1989.

[Ser71] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15(4):259–331, 1971.

[Sil99] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic Curves*. Springer-Verlag, New York, 1999. Graduate Texts in Mathematics.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, New York, second edition, 2009. Graduate Texts in Mathematics.

[Tat74] John T Tate. The arithmetic of elliptic curves. *Inventiones mathematicae*, 23(3-4):179–206, 1974.

[Vél71] Jacques Vélu. Isogénies entre courbes elliptiques. *CR Acad. Sci. Paris Sér. AB*, 273:A238–A241, Juillet 1971.