RIMS Kôkyûroku Bessatsu **4**
(2007), 189–195

Self-points on an elliptic curve of conductor 14

By

Christian WUTHRICH

Abstract

In order to illustrate the methods used to work with self-points on elliptic curves, we present here the explicit computations on one of the curves of conductor 14.

§ 1. Self-points on elliptic curves

Let $E/\mathbb{Q}$ be an elliptic curve. Denote by N its conductor. There is a modular parametrization

$$\varphi_E \colon X_0(N) \longrightarrow E$$

which is a surjective morphism defined over $\mathbb{Q}$. For any cyclic subgroup C of order N in E, we may consider the point x_C represented by (E, C) in the moduli space $Y_0(N)$. We call the image $P_C = \varphi_E(x_C)$ in E a *self-point* of E. If instead, we choose a couple (E', C') where E' is a curve which is isogenous to E over $\bar{\mathbb{Q}}$ and C' is any cyclic subgroup of E' of order N, we say that $\varphi_E(E', C')$ is a *higher self-point.* The self-point P_C is defined over the field of definition $\mathbb{Q}(C)$ of C; a number field of relatively small degree.

It turns out that the properties of these self-points depend very much on the nature of the curve. For instance they behave differently whether the curve has complex multiplication or not. In case the conductor is a prime number the situation is fairly easy. In [DW07], we prove the following theorem.

Theorem 1. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor $p = N$. Then the point P_C is of infinite order. The only relation among the $p + 1$ self-points is that the sum of all self-points is equal to the image of the cusp $0 \in X_0(p)$, which is known to be a torsion point in $E(\mathbb{Q})$.*

It can be shown that the group generated by the self-points produces a copy of the so-called Steinberg representation in the Mordell-Weil group of E over the Galois closure K of $\mathbb{Q}(C)$.

On the other hand, it is easy to find a self-point which is torsion. Namely there happens to be a curve E of conductor 27, usually labelled 27a2, which admits a cyclic isogeny of degree 27 defined over $\mathbb{Q}$. If C is the kernel of this isogeny, then the self-point P_C must be defined over $\mathbb{Q}$. But the Mordell-Weil group $E(\mathbb{Q})$ is finite of order 3. So P_C is torsion. Note that this curve E has complex multiplication.

We conjecture that all self-points on a curve with non-integral j-invariant are of infinite order. Moreover, we believe that for such curves the following gives all the possible relations among the self-points. Let d be a divisor of N different from N. Let D be any cyclic subgroup of E of order d. There is a degeneracy map $\pi\colon X_0(N) \to X_0(d)$ inducing a map $\pi^*\colon J_0(d) \to J_0(N)$ on Jacobians. Consider the point $x_D = (E, D)$ on $X_0(d)$ and the divisor class

$$\pi^*\big[(x_D) - (\infty)\big] = \sum_{C \supset D} \big[(x_C)\big] - \pi^*\big[(\infty)\big]\,, \tag{1}$$

where the sum runs over all cyclic subgroups C of order N containing D. This divisor class belongs to the image of π^* in $J_0(N)$ and hence in the kernel of the map $\varphi_E\colon J_0(N) \twoheadrightarrow E$ because N is the exact conductor of E. This gives the relation that for any d and D, the sum $\sum_{C \supset D} P_C$ is a torsion point on E.

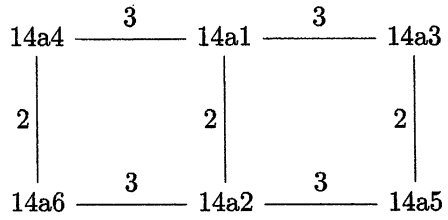
Under some technical conditions, we are able to prove for semi-stable curves and even for some curves with composite conductor that the above relations are the only relations among self-points. See [Wut07]. But the proof is much more involved than the proof of the above theorem. To illustrate the kind of techniques used when dealing with curves whose conductor is not prime, we are treating here in this article one single curve of conductor 14. All the computations have been done using `magma` [BCP97] and pari-gp [PAR06].

§ 2. Self-points on the curve of conductor 14

Let E be the curve 14a1; it is given by the equation

$$E = 14a1 : \; y^2 + xy + y = x^3 + 4x - 6\,.$$

The Mordell-Weil group over $\mathbb{Q}$ contains six points generated by $(9, -33)$. There are six curves in the isogeny class of E linked as shown in the diagram below.(6cm,3cm)[r]



The aim of this section is to prove that there are 24 self-points on this curve, all of infinite order, and that the only relations among these points are given by (1)

The curve 14a1 has non-split multiplicative reduction of type I_6 with $c_2 = 3$ at 2 and split multiplicative reduction of type I_3 with $c_7 = 3$ at 7.

For any d dividing $N = 14$, let K_d be the field inside $\mathbb{Q}(E[d])$ which is fixed by the scalars of the image of the Galois representation

$$\bar{\rho}_d\colon \mathrm{Gal}(\mathbb{Q}(E[d])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}).$$

Write G_d for the Galois group of $K_d/\mathbb{Q}$, which is a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/d\mathbb{Z})$ via $\bar{\rho}_d$.

Since the curve has a 2-torsion point $T = (1, -1)$ defined over $\mathbb{Q}$, the Galois group $G_{14} = \mathrm{Gal}(K_{14}/\mathbb{Q})$ is certainly not equal to $\mathrm{PGL}_2(\mathbb{Z}/14\mathbb{Z})$. The projection onto $\mathrm{PGL}_2(\mathbb{F}_7)$ is surjective since E is semi-stable and there is no isogeny of degree 7, see [Ser96]. The Galois group $G_2 = \mathrm{Gal}(K_2/\mathbb{Q})$ is cyclic with two elements. In fact, K_2 is $\mathbb{Q}(\sqrt{-7})$.

The only proper Galois subextension L in K_7 corresponds to the only proper normal subgroup $\mathrm{PSL}_2(\mathbb{F}_7)$ in $\mathrm{PGL}_2(\mathbb{F}_7)$. To determine L it suffices to note that the map from $\mathrm{Gal}(K_7/\mathbb{Q})$ to $\mathrm{Gal}(L/\mathbb{Q}) = \{\pm 1\}$ sends a Frobenius element at p to $(\frac{p}{7})$, for any prime $p \nmid 14$. By quadratic reciprocity $(\frac{p}{7}) = (\frac{-7}{p})$ and hence $L = \mathbb{Q}(\sqrt{-7}) = K_2$ is contained in K_7. So we see that $K_{14} = K_7$ is an extension with Galois group $\mathrm{PGL}_2(\mathbb{F}_7)$. The self-point P_C is defined over the subextension of K_{14} fixed by the Borel subgroup of $G_{14} \subset \mathrm{PGL}_2(\mathbb{Z}/14\mathbb{Z})$.

If the self-point P_C is constructed with a cyclic subgroup of order 14 containing $T \in E(\mathbb{Q})[2]$, then P_C is defined over a degree 8 extension of $\mathbb{Q}$ inside K_{14}, otherwise over a degree 16 extension inside K_{14} containing $\mathbb{Q}(\sqrt{-7})$. The relations induced by the degeneracy map from $X_0(2)$ are the following: The sum of the 8 self-points of degree 8 is torsion. The remaining 16 self-points form two groups which each sum up to a torsion point. Finally there are the relations coming from $X_0(7)$ involving each 3 points, one of degree 8 and two of degree 16.

For any divisor d of $N = 14$, let V_d be a $\mathbb{Q}$-vector space of maps $f\colon \mathbb{P}^1(\mathbb{Z}/d\mathbb{Z}) \to \mathbb{Q}$. Endowing V_d with the obvious action of $\mathrm{PGL}_2(\mathbb{Z}/d\mathbb{Z})$, it becomes a $\mathbb{Q}[G_d]$-module. Put

$$W_d = \left\{ f \in V_d \,\middle|\, \sum_{x \in \mathbb{P}^1} f(x) = 0 \right\}$$

which is a $\mathbb{Q}[G_d]$-submodule of V_d. For $d = 2$ or 7, the dimension of W_d is $\#\mathbb{P}^1(\mathbb{Z}/d\mathbb{Z}) - 1 = d$.

For $d = 2$, we find that W_2 decomposes as $1 \oplus 1(\sqrt{-7})$ where $1(\sqrt{-7})$ is the 1-dimensional $\mathbb{Q}$-vector space with Galois action by the Dirichlet character associated to $K_2 = \mathbb{Q}(\sqrt{-7})$. Now it is not difficult to show that W_7 is an irreducible $\mathbb{Q}[H_7]$-module

with $H_7 = \mathrm{Gal}(K_7/K_2) = \mathrm{PSL}_2(\mathbb{F}_7)$. The representation W_7 is called a *Steinberg representation.*

Since $\mathbb{P}^1(\mathbb{Z}/14\mathbb{Z}) \cong \mathbb{P}^1(\mathbb{F}_7) \times \mathbb{P}^1(\mathbb{F}_2)$, we find that W_{14} decomposes as

$$W_{14} = W_7 \otimes W_2 = W_7 \oplus W_7(\sqrt{-7})$$

into irreducible $\mathbb{Q}[G_{14}]$-modules. Here $W_7(\sqrt{-7})$ is the twist of W_7 by $1(\sqrt{-7})$.

Proposition 2. *All the self-points P_C on E =*14a1 *are of infinite order.*

Proof. We use first the same approach as in the proof of theorem 1. Fix an embedding of $\bar{\mathbb{Q}}$ into $\bar{\mathbb{Q}}_7$. The curve E has split multiplicative reduction at $p = 7$, so it is isomorphic to a Tate curve $\mathbb{Q}_7^\times / q_E^{\mathbb{Z}}$ with

$$q_E = 6 \cdot 7^3 + 4 \cdot 7^4 + 6 \cdot 7^5 + 7^6 + 3 \cdot 7^7 + \mathbf{O}(7^8)\,.$$

Under this isomorphism the rational 2-torsion point $T = (1, -1)$ corresponds to -1 modulo $q_E^{\mathbb{Z}}$. So there is a cyclic subgroup C_0 of order 14 containing T such that $x_0 = (E, C_0)$ is close to ∞ on $X_0(14)(\bar{\mathbb{Q}}_7)$, i.e. $C_0 \cong \mu[14]$ over $\bar{\mathbb{Q}}_7$. So x_1 belongs to the neighbourhood of ∞ parametrized by q as described in [KM85]. We can apply the formula used in the proof of proposition 3 in [DW07]. We get

$$\log_E(P_{C_0}) = q_E + \frac{a_2}{2} q_E^2 + \frac{a_3}{3} q_E^3 + \cdots = 6 \cdot 7^3 + 4 \cdot 7^4 + 6 \cdot 7^5 + 4 \cdot 7^6 + 4 \cdot 7^7 + \mathbf{O}(7^8)$$

where $\log_E \colon \widehat{E}(pZZ_p) \longrightarrow pZZ_p$ is the formal p-adic logarithm and

$$f_E = \sum_{n \geqslant 0} a_n q^n = q - q^2 - 2q^3 + q^4 + 2q^6 + \cdots$$

is the newform associated to the isogeny class of E. Hence we find that the self-point

$$P_{C_0} = \left(7^{-6} \cdot (1 + 3 \cdot 7 + 4 \cdot 7^2 + 7^3 + 2 \cdot 7^4 + \mathbf{O}(7^5)),\ 7^{-9} \cdot (1 + 7 + 2 \cdot 7^2 + 2 \cdot 7^3 + 7^4 + \mathbf{O}(7^5))\right)$$

is of infinite order in $E(\mathbb{Q}_7)$. So all the self-points conjugate to P_{C_0} are of infinite order; these are exactly the 8 self-points over the degree 8 extension corresponding to cyclic subgroups C of order 14 containing T.

Let now C_1 be a cyclic subgroup of order 14 in E such that its 7-torsion part corresponds to $\mu[7]$ over $\mathbb{Q}_7$, but the 2-torsion part corresponds to $u = \sqrt{q_E}$ and not to $\mu[2]$. Then $x_1 = (E, C_1)$ is not in the neighbourhood of $\infty \in X_0(14)$ parametrized by q. But if we apply the Atkin-Lehner involution w_2 to x_1 we find a point $w_2(x_1)$

which close to ∞ with $q = u$. Note that Atkin and Lehner have shown in [AL70] that $\varphi_E(w_2(x_1)) = -a_2 \cdot \varphi_E(x_1) = P_{C_1}$. Using the same formula as above we find

$$\log_E(P_{C_1}) = u + \frac{a_2}{2}u^2 + \frac{a_3}{3}u^3 + \cdots$$

which converges in $\mathbb{Q}_7(\sqrt{-7})$ as $|u|_7 = 7^{3/2}$. Also the exponential map $\exp_E$ converges and we find a point of infinite order in E defined over $\mathbb{Q}_7(\sqrt{-7})$, the completion of K_2 at the unique place above 7. The conjugates of P_{C_1} are exactly the 16 remaining self-points defined over an extension of degree 16 of $\mathbb{Q}$. □

Theorem 3. *The self-points for* E =14a1 *generate a group of rank* 14 *in* $E(K_{14})$.

In other words we will show that the 10 relations described using (1) are the only relations among the 24 self-points.

Proof. There is a G_{14}-equivariant map

$$\begin{aligned} \iota : V_{14} &\longrightarrow E(K_{14}) \otimes \mathbb{Q} \\ e_C &\longmapsto P_C \end{aligned}$$

where $e_C \colon \mathbb{P}^1(\mathbb{Z}/14\mathbb{Z}) \longrightarrow \mathbb{Q}$ is the map sending C to 1 and all other points to 0. The relations from $X_0(2)$ show that the subspaces consisting of $f \in V_{14}$ such that $f(C) = f(C')$ for all C, C' with $C[2] = C'[2]$. Similarly for $X_0(7)$. We deduce that ι induced a G_{14}-equivariant map from W_{14} to $E(K_{14}) \otimes \mathbb{Q}$. We know that W_{14} splits into two irreducible $\mathbb{Q}[G_{14}]$-modules. By the first part of the proof of the previous proposition, we know that the map from W_7 to the Mordell-Weil group is non-trivial (and hence injective) as there is a self-point of infinite order P_{C_0}. The second part shows that the map from $W_7(\sqrt{-7})$ is injective. So the image of ι has dimension $7+7 = 14$. □

For this curve, we may also compute the self-points explicitly, at least those of degree 8 over $\mathbb{Q}$. The field $\mathbb{Q}(C)$ is defined by a root θ of the polynomial

$$X^8 - 3X^7 + 7X^6 + 7X^5 + 35X^4 + 63X^3 + 77X^2 + 53X - 40.$$

The class group of $\mathbb{Q}(C)$ is of order 2 generated by any of the two primes above 2. The self-point P_C is given by

$$\begin{aligned} x(P_C) = {} & 2^{-6}\cdot 5^{-1}\cdot 7^{-1}\cdot 101^{-1}\cdot(274149\,\theta^7 - 592823\,\theta^6 + 400715\,\theta^5 + 5060363\,\theta^4 \\ & + 10722663\,\theta^3 + 9077635\,\theta^2 - 927367\,\theta - 2264895) \\ y(P_C) = {} & 2^{-9}\cdot 7^{-1}\cdot 101^{-1}\cdot(8040223\,\theta^7 - 31741605\,\theta^6 + 51338609\,\theta^5 + 104708513\,\theta^4 \\ & + 72654981\,\theta^3 - 147056119\,\theta^2 - 245694757\,\theta + 117487875) \end{aligned}$$

Its canonical height is $\hat{h}(P_C) = 1.84388$.

§ 3. Two higher self-points on the curve of conductor 14

We use now the isogenies $E \to E'$ defined over $\mathbb{Q}$ to produce higher self-points $\varphi_E(E', C')$. The higher self-points where E' is 2-isogenous to E do not give us any new points : In fact (E', C') is equal to $w_2(x_C)$, where w_2 is the Atkin-Lehner involution on $X_0(14)$ for some C. So as before $\varphi_E(E', C') = -a_2 \cdot \varphi_E(E, C) = P_C$.

But if we use a 3-isogenies on $E \to E'$, we discover a new points. Fix a cyclic subgroup C of order 14 in E. Let C' be the image of C in E', which is cyclic of order 14 in E'. The self-point $P'_C = \varphi_E(E', C')$ is a point defined over $\mathbb{Q}(C)$, the field of definition of P_C. The point providing from the curve 14a4 is

$$x(P'_C) = 2^{-2}\cdot 5^{-1}\cdot 7^{-1}\cdot 101^{-1}\cdot(-704\,\theta^7+1848\,\theta^6-4235\,\theta^5-3423\,\theta^4-10458\,\theta^3-4970\,\theta^2+11977\,\theta+10925)$$
$$y(P'_C) = 2^{-3}\cdot 7^{-1}\cdot(11\,\theta^7-35\,\theta^6+21\,\theta^5-105\,\theta^4-175\,\theta^3-273\,\theta^2-217\,\theta+93)$$

and the point from the curve 14a3 is

$$x(P''_C) = 5^{-1}\cdot 7^{-1}\cdot 101^{-1}\cdot(368\,\theta^7-1976\,\theta^6+8400\,\theta^5-13464\,\theta^4+24496\,\theta^3+43480\,\theta^2+32016\,\theta+92615)$$
$$y(P''_C) = 5^{-1}\cdot 7^{-1}\cdot 101^{-1}\cdot(-884\,\theta^7-3992\,\theta^6+21100\,\theta^5-87408\,\theta^4-30388\,\theta^3-150160\,\theta^2-678868\,\theta-406215)\,.$$

The canonical heights are $\hat{h}(P'_C) = 1.35464$ and $\hat{h}(P''_C) = 2.62801$ which gives a height determinant of 30.7767. This shows that the three points P_C, P'_C and P''_C are linearly independent. Therefore $\operatorname{rank} E(\mathbb{Q}(C)) \geqslant 3$. We do not know any way of proving the independence of these three points in any other way than explicitly computing the points.

With a 2-descent, we find that the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q}(C))$ is an $\mathbb{F}_2$-vector space of dimension 6. Since the torsion subgroup of $E(\mathbb{Q}(C))$ is still of order six, we deduce that $\operatorname{rank}(E(\mathbb{Q}(C)) \leqslant 5$.

By the formula in [Dok05], we can compute easily that the root number, defined as a product of local root numbers, is $w(E/\mathbb{Q}(C)) = -1$. Using the methods of Shuter in [Shu06], we also find that the 7-Selmer group must have odd rank. Hence unless the Tate-Shafarevich group of E over $\mathbb{Q}(C)$ is infinite, we must believe that the rank of E over $\mathbb{Q}(C)$ is either 3 or 5.

Acknowledgments

I wish to thank Christophe Delaunay for his collaboration on the topic. Also I express my gratitude to Masato Kurihara and Yoshitaka Hachimori for their hospitality during my visit in Japan. The author was supported by a fellowship of the Swiss National Science Foundation during his stay at Keio University.

References

[AL70] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[Dok05] Vladimir Dokchitser, *Root numbers of non-abelian twists of elliptic curves*, Proc. London Math. Soc. (3) **91** (2005), no. 2, 300–324, With an appendix by Tom Fisher.

[DW07] Christophe Delaunay and Christian Wuthrich, *Self-points on elliptic curves of prime conductor*, Preprint, 2007.

[KM85] Nicholas M. Katz and Barry Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies, vol. 108, Princeton University Press, Princeton, NJ, 1985.

[PAR06] The PARI Group, Bordeaux, *PARI/GP, version* `2.3.1`, 2006, available from `http://pari.math.u-bordeaux.fr/`.

[Ser96] Jean-Pierre Serre, *Travaux de Wiles (et Taylor, ...). I*, Astérisque (1996), no. 237, Exp. No. 803, 5, 319–332, Séminaire Bourbaki, Vol. 1994/95.

[Shu06] Micheal Shuter, *Rational Points of Elliptic Curves in p-Division Fields*, preprint in preparation, 2006.

[Wut07] Christian Wuthrich, *Self-points on elliptic curves*, In preparation, 2007.