

Computing rational torsion on elliptic curves in linear time

Iftikhar Burhanuddin and Ming-Deh Huang

Department of Computer Science,
University of Southern California, Los Angeles, CA 90007.
{burhanud|huang}@usc.edu

Abstract. We present an algorithm to decide whether an elliptic curve over \mathbb{Q}_p has a non-trivial p -torsion part ($\#E(\mathbb{Q}_p)[p] \neq 1$) under certain assumptions. We use this algorithm to efficiently determine $E(\mathbb{Q})_{tors}$ the group of \mathbb{Q} -rational torsion points on an elliptic curve.

1 Introduction

We present a polynomial-time (polynomial in $\log p$) algorithm that decides whether a given elliptic curve over \mathbb{Q}_p has a non-trivial p -torsion part under certain assumptions. In section 2 the good reduction case is considered followed by the bad reduction case. We devise an algorithm to compute $E(\mathbb{Q}_p)[2]$ in section 4 which is used in a linear-time procedure (linear in the logarithm of the coefficients of the elliptic curve equation) to compute $E(\mathbb{Q})_{tors}$ using a p -adic approach.

We do not attempt a self-contained exposition. The background material on elliptic curves can be found in [12]. We borrow freely (but with due acknowledgement and gratitude) from the literature mentioned in the References section.

We would like to thank Sheldon Kamienny, Qing Luo and Wayne Raskind for the helpful discussions. The authors were supported in part by the following NSF grants CCR-9820778 and CCR-0306393.

2 Deciding whether $E(\mathbb{Q}_p)[p]$ is non-trivial

Notation. Let E be an elliptic curve and R a point on it. Then $x(R)$ and $y(R)$ will denote the x and y coordinates of point R respectively. The elliptic curve $E \bmod p$ will be denoted by \overline{E} and a point on it by \overline{R} .

Algorithm 1 *Let E be an elliptic curve over \mathbb{Q}_p given by a minimal Weierstrass equation $y^2 = x^3 + ax + b$ that has good reduction at p , where $p > 2$.*

Input. We are given the coefficients of E , modulo p^2

Output. TRUE if $\#E(\mathbb{Q}_p)[p] = p$ and FALSE if $\#E(\mathbb{Q}_p)[p] = 1$

1. $n \leftarrow \#\overline{E}(\mathbb{F}_p)$
2. If $\gcd(n, p) = 1$ return FALSE
3. Pick $\overline{P} \in \overline{E}(\mathbb{F}_p)[p]$
4. Lift \overline{P} to $P \in E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ using Hensel's lemma [8](Lemma 2.8) such that $P \equiv \overline{P} \pmod{p}$. We only need to determine P modulo p^2
5. Compute $x([p-1]P) \pmod{p^2}$ using the repeated squaring trick [6](page 23) and the group law formulae.
6. If $x([p-1]P) \equiv x(P) \pmod{p^2}$ return FALSE. Otherwise return TRUE

Theorem 1. *The above algorithm works as desired.*

Proof. The short exact sequence $0 \rightarrow E_1(\mathbb{Q}_p) \rightarrow E(\mathbb{Q}_p) \rightarrow \overline{E}(\mathbb{F}_p) \rightarrow 0$ [12](Proposition VII.2.1) gives rise to the following long exact sequence via the extended snake lemma [7](Lemma II.4.1):

$$\begin{aligned} 0 \rightarrow E_1(\mathbb{Q}_p)[l] \rightarrow E(\mathbb{Q}_p)[l] \rightarrow \overline{E}(\mathbb{F}_p)[l] \xrightarrow{\phi} E_1(\mathbb{Q}_p)/lE_1(\mathbb{Q}_p) \\ \rightarrow E(\mathbb{Q}_p)/lE(\mathbb{Q}_p) \rightarrow \overline{E}(\mathbb{F}_p)/l\overline{E}(\mathbb{F}_p) \rightarrow 0 \end{aligned}$$

where $l \in \mathbb{Z}$. Specializing to the case when $l = p$ and using the fact that $E_1(\mathbb{Q}_p) \cong \hat{E}(p\mathbb{Z}_p) \cong \hat{G}_a(p\mathbb{Z}_p)$ is torsion-free [12](Proposition VII.2.2, IV.6.4b) and by abuse of notation denoting $\log_E \circ \lambda \circ \phi$ by ϕ , we get

$$\begin{aligned} 0 \rightarrow E(\mathbb{Q}_p)[p] \rightarrow \overline{E}(\mathbb{F}_p)[p] \xrightarrow{\phi} \hat{G}_a(p\mathbb{Z}_p)/p\hat{G}_a(p\mathbb{Z}_p) \\ \rightarrow E(\mathbb{Q}_p)/pE(\mathbb{Q}_p) \rightarrow \overline{E}(\mathbb{F}_p)/p\overline{E}(\mathbb{F}_p) \rightarrow 0 \end{aligned}$$

If $\gcd(n, p) = 1$ then $\overline{E}(\mathbb{F}_p)[p] = O$ which implies that $E(\mathbb{Q}_p)[p] = O$ from the above long exact sequence.

We next prove a lemma which is vital to the proof of the theorem when $\gcd(n, p) \neq 1$.

Lemma 1. *Let E be an elliptic curve over \mathbb{Q}_p given by a minimal Weierstrass equation of the form $y^2 = x^3 + ax + b$ with good reduction at p (that is $v(a), v(b) \geq 0, v_p(\Delta) = 0$), where $p > 2$ and the discriminant $\Delta = -16(4a^3 + 27b^2)$. If $Q \in E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ and $\overline{Q} \in \overline{E}(\mathbb{F}_p)[p]$ then*

1. $[i]Q \in E(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$, $i = 1, \dots, p-1$
2. $x([i]Q) \not\equiv x([j]Q) \pmod{p}$, $0 < j < i < p$ and $i + j < p$
3. $x([p-k]Q) \equiv x([k]Q) \pmod{p}$ and $y([p-k]Q) \equiv -y([k]Q) \pmod{p}$ (in particular $y([p-k]Q) \not\equiv y([k]Q) \pmod{p}$), $0 < k < p$

4. $[p]Q \in E_i(\mathbb{Q}_p) \setminus E_{i+1}(\mathbb{Q}_p) \Leftrightarrow v_p(x([p]Q)) = -2i \Leftrightarrow v_p(x([p-1]Q) - x(Q)) = i, i \geq 1$
5. $x([p-1]Q) - x(Q) \equiv 0 \pmod{p^2} \Leftrightarrow \phi = 0$, where $\phi : \overline{E}(\mathbb{F}_p)[p] \rightarrow \hat{G}_a(p\mathbb{Z}_p)/p\hat{G}_a(p\mathbb{Z}_p)$

Proof. 1. Suppose $[i]Q \in E_1(\mathbb{Q}_p)$ then $[i]\overline{Q} = O$ which is a contradiction since $\gcd(i, p) = 1$.

2. Suppose $x([i]Q) \equiv x([j]Q) \pmod{p}$. This assumption combined with the fact that $[i]\overline{Q}, [j]\overline{Q} \neq O$ implies that $[i]\overline{Q} = \pm([j]\overline{Q})$ and hence $[i \pm j]\overline{Q} = O$. This is a contradiction as $\gcd(i \pm j, p) = 1$.
3. Let $R := [p-k]Q$. So $\overline{R} = [p-k]\overline{Q} = -[k]\overline{Q}$. Hence $x(\overline{R}) = x([k]\overline{Q})$ and $y(\overline{R}) = -y([k]\overline{Q})$.
4. From part (3) we know that $x([p-k]Q) \equiv x([k]Q) \pmod{p}$. Say $v_p(x([p-k]Q) - x([k]Q)) = i$. We also know that $y([p-k]Q) \not\equiv y([k]Q) \pmod{p}$. From the group law formulae to calculate $[p]Q$ (say using $[k]Q$ and $[p-k]Q$), it follows that $v_p(x([p]Q)) = -2i$ which is equivalent to $v_p(y([p]Q)) = -3i$ [8](proof of Theorem 7.1(c)). And therefore $[p]Q \in E_i(\mathbb{Q}_p) \setminus E_{i+1}(\mathbb{Q}_p)$.
5. $x([p-1]Q) - x(Q) \equiv 0 \pmod{p^2}$ implies $[p]Q \in E_2(\mathbb{Q}_p)$ by part (4). This implies that $\phi(\overline{Q}) = (\log_E \circ \lambda \circ [p])(Q) = 0 \in \hat{G}_a(p\mathbb{Z}_p)/p\hat{G}_a(p\mathbb{Z}_p)$. Here $\lambda(R) = -x(R)/y(R)$, where $R \in E_1(\mathbb{Q})$ and $\log_E(z) = z + O(z^5)$, where $z \in \hat{E}(p\mathbb{Z}_p)$.
(On the other hand $x([p-1]Q) - x(Q) \not\equiv 0 \pmod{p^2}$ implies $[p]Q \in E_1(\mathbb{Q}_p) \setminus E_2(\mathbb{Q}_p)$ by part (4). This implies that $\phi(\overline{Q}) = (\log_E \circ \lambda \circ [p])(Q) \neq 0$). This completes the proof of the lemma.

In second case we pick a point in $\overline{E}(\mathbb{F}_p)[p]$ and lemma 1 tells us that $E(\mathbb{Q}_p)[p]$ being trivial, is equivalent to $x([p-1]P) \equiv x(P) \pmod{p^2}$. Now we observe that when we compute $x([p-1]P)$ by the squaring trick, the denominators are p -adic units (by lemma 1 part (2)) and the group law formulae hold modulo p^2 . This tells us that only the coefficients of elliptic curve E and of the coordinates of the point P modulo p^2 contribute towards the computation.

The worst-case time complexity is $O(T_{pc} + \log^3 p)$ bit operations where T_{pc} is the worst-case time complexity of the point counting algorithm used ([11], [9]). QED.

Remark 1. It is interesting to note that the algorithm uses only 2 digits of p -adic precision.

Remark 2. Given that $\#E(\mathbb{Q}_p)[p] \neq 1$, to efficiently find a non-zero $P \in E(\mathbb{Q}_p)[p]$, is an open problem. When p is small a brute-force procedure using p -division polynomials can be employed to compute the above (see section 4).

Remark 3. If $p > 5$ we have two cases $\gcd(n, p) = 1$ and $n = p$. If $p = 3, 5$ we have a third case — $\gcd(n, p) = p$ and $n \neq p$ — the only instances of which are $n = 2p$ by the Hasse bound. And this is the reason we pick $\overline{P} \in \overline{E}(\mathbb{F}_p)[p]$ in the algorithm.

3 Deciding whether $E(\mathbb{Q}_p)[p]$ is non-trivial (contd.)

We continue our discussion and next consider the case of bad reduction which is characterized by $v_p(\Delta) > 0$. The type of reduction – multiplicative or additive – be determined as follows: E has multiplicative reduction iff $v_p(\Delta) \geq 1$ and $v_p(ab) = 0$ and it has additive reduction iff $v_p(a), v_p(b) \geq 1$ [12](Exer. 7.1b). Let the reduced curve $E \bmod p$ be denoted by \overline{E} and its non-singular part by \overline{E}_{ns} .

Algorithm 2 *Let E over \mathbb{Q}_p be given by a minimal Weierstrass equation be of the form $y^2 = x^3 + ax + b$. We assume that $p > 2$ and E has bad reduction at p .*

Input. We are given the coefficients of E , modulo p^2

Output. TRUE if $\#E_0(\mathbb{Q}_p)[p] = p$ and FALSE if $\#E_0(\mathbb{Q}_p)[p] = 1$

1. $n \leftarrow \#\overline{E}_{ns}(\mathbb{F}_p)$
2. If $\gcd(n, p) = 1$ return FALSE
3. Pick $\overline{P} \in \overline{E}_{ns}(\mathbb{F}_p)$
4. Lift \overline{P} to $P \in E_0(\mathbb{Q}_p) \setminus E_1(\mathbb{Q}_p)$ using Hensel's lemma [8](Lemma 2.8) such that $P \equiv \overline{P} \pmod{p}$. We only need to determine P modulo p^2
5. If $x([p-1]P) \equiv x(P) \pmod{p^2}$ return FALSE. Otherwise return TRUE

Theorem 2. *The above algorithm works as desired.*

Proof. The proof of correctness of the algorithm rests on the following theorem [12](Exercise III.3.5): $\overline{E}_{ns}(\mathbb{F}_p) \cong \mathbb{F}_p^+, \mathbb{F}_p^*$ or $\{t \in L^* \mid N_{L/\mathbb{F}_p}(t) = 1\}$ where $L = \mathbb{F}_p(\alpha_1, \alpha_2)$ and α_1, α_2 are the slopes of tangent lines in the non-split multiplicative reduction case.

The short exact sequence $0 \rightarrow E_1(\mathbb{Q}_p) \rightarrow E_0(\mathbb{Q}_p) \rightarrow \overline{E}_{ns}(\mathbb{F}_p) \rightarrow 0$ gives rise to the following long exact sequence using a train of thought similar to the one found in the proof of Theorem 1.

$$\begin{aligned}
0 &\rightarrow E_0(\mathbb{Q}_p)[p] \rightarrow \overline{E}_{ns}(\mathbb{F}_p)[p] \xrightarrow{\phi} \hat{G}_a(pZZ_p)/p\hat{G}_a(pZZ_p) \\
&\rightarrow E_0(\mathbb{Q}_p)/pE_0(\mathbb{Q}_p) \rightarrow \overline{E}_{ns}(\mathbb{F}_p)/p\overline{E}_{ns}(\mathbb{F}_p) \rightarrow 0
\end{aligned}$$

If $\gcd(n, p) = 1$ then $\overline{E}_{ns}(\mathbb{F}_p)[p] = 0$ which implies that $E_0(\mathbb{Q}_p)[p] = 0$ from the above long exact sequence. This case takes care of split multiplicative reduction as we have $\#\overline{E}_{ns}(\mathbb{F}_p) = \#\mathbb{F}_p^* = p - 1$ and in the non-split case we have $\#\overline{E}_{ns}(\mathbb{F}_p) = 1, p - 1, p + 1, p^2 - 1$.

On the other hand, we are in the additive reduction case $\#\overline{E}_{ns}(\mathbb{F}_p) = \#\mathbb{F}_p^+ = p$ and $E(\mathbb{Q}_p)[p]$ is trivial is equivalent to $x([p-1]P) - x(P) \equiv 0 \pmod{p^2}$. The proof is similar to lemma 1 with $\overline{E}(\mathbb{F}_p)$ replaced by $\overline{E}_{ns}(\mathbb{F}_p)$ and $E(\mathbb{Q}_p)$ replaced by $E_0(\mathbb{Q}_p)$.

The worst-case time complexity is $O(T_{nspc} + \log^3 p)$ bit operations where T_{nspc} is the time complexity of computing $\#\overline{E}_{ns}(\mathbb{F}_p)$. QED.

Next we will use the output of the above algorithm to decide whether $E(\mathbb{Q}_p)[p]$ is non-trivial with the help of the following fact [12](Appendix C, Corollary 15.2.1), [13](Corollary IV.9.2):

Theorem 3. *Let E/\mathbb{Q}_p be an elliptic curve. Then we have the following exact sequence:*

$$0 \rightarrow E_0(\mathbb{Q}_p) \rightarrow E(\mathbb{Q}_p) \rightarrow G \rightarrow 0$$

where if E has split multiplicative reduction over \mathbb{Q}_p , then G is a cyclic group of order $v(\Delta) = -v(j)$, in the additive scenario the group order is at most 4 and in the non-split multiplicative instance it is either 1 or 2.

In order to weed out the bad cases we impose some conditions.

Theorem 4. *Algorithm 2 correctly computes $\#E(\mathbb{Q}_p)[p]$ provided either*

- E has split multiplicative reduction over \mathbb{Q}_p and $\gcd(v_p(\Delta), p) = 1$, or
- E has additive reduction over \mathbb{Q}_p and $G[p] = 0$, or
- E has non-split multiplicative reduction over \mathbb{Q}_p

Proof. Applying the extended snake lemma to the above exact sequence gives us

$$\begin{aligned}
0 &\rightarrow E_0(\mathbb{Q}_p)[p] \rightarrow E(\mathbb{Q}_p)[p] \rightarrow G[p] \rightarrow E_0(\mathbb{Q}_p)/pE_0(\mathbb{Q}_p) \\
&\rightarrow E(\mathbb{Q}_p)/pE(\mathbb{Q}_p) \rightarrow G/pG \rightarrow 0
\end{aligned}$$

And under the assumptions of the theorem $G[p] = 0$. Hence $E_0(\mathbb{Q}_p)[p] = 0 \Leftrightarrow E(\mathbb{Q}_p)[p] = 0$ otherwise $\#E(\mathbb{Q}_p)[p] = p$. QED.

Remark 4. The instances which are left out are analyzed using the fact that $\frac{X}{X_0} | \#G[p]$, where $X_0 = \#E_0(\mathbb{Q}_p)[p]$ and $X = \#E(\mathbb{Q}_p)[p]$:

1. additive reduction, $\#G = 3$ and $p = 3$ (Kodaira types IV, IV^*). In this case if $X_0 = 1$ then $X = 1, 3$ and if $X_0 = 3$ then $X = 3, 9$.
2. split multiplicative and $p | \#G$. In this scenario if $X_0 = 1$ then $X = 1, p$ and if $X_0 = p$ then $X = p, p^2$.

We will assume that a boolean variable BAD is set if we fall into these instances.

4 Computing $E(\mathbb{Q}_p)[2]$

Let $X_0 = \#E_0(\mathbb{Q}_p)[2]$ and $X = \#E(\mathbb{Q}_p)[2]$.

Theorem 5. $E_0(\mathbb{Q}_p)[2] = E(\mathbb{Q}_p)[2]$ provided either

1. E has good reduction at p , or
2. E has split multiplicative reduction and $\gcd(v_p(\Delta), 2) = 1$, or
3. E has additive reduction and $G[2] = 0$, or
4. E has non-split multiplicative reduction $G[2] = 0$, or
5. $E_0(\mathbb{Q}_p)[2] = 4$

Proof. The proof follows for case (i) since $E = E_0$ and $\overline{E}_{ns} = \overline{E}$. Applying the extended snake lemma gives us

$$\begin{aligned} 0 \rightarrow E_0(\mathbb{Q}_p)[2] \rightarrow E(\mathbb{Q}_p)[2] \rightarrow G[2] \rightarrow E_0(\mathbb{Q}_p)/2E_0(\mathbb{Q}_p) \\ \rightarrow E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) \rightarrow G/2G \rightarrow 0 \end{aligned}$$

Either of the cases (ii) – (iv) of the theorem gives us $G[2] = 0$ and therefore $E_0(\mathbb{Q}_p)[2] \cong E(\mathbb{Q}_p)[2]$.

For case (v), using the fact that $\frac{X}{X_0} | \#G[2]$ and $X | 4$ we have if $X_0 = 4$ then $X = 4$. QED.

Remark 5. Also if $X_0 = 1$ then $X = 1, 2, 4$ and if $X_0 = 2$ then $X = 2, 4$. We see that the following are the instances not tackled by the theorem and refer to them as the BAD2 case:

1. split multiplicative: since in this case G is cyclic the bad cases are type I_v , v is even and $X_0 \neq 4$
2. additive reduction: the bad cases are type $III, I_0, I_v^*(v > 0), III^*$ and $X_0 \neq 4$
3. non-split multiplicative: since $|G| = 1, 2$, the bad case is type I_2 reduction and $X_0 \neq 4$

Algorithm 3 Let E be an elliptic curve over \mathbb{Q}_p given by a minimal Weierstrass equation $y^2 = x^3 + ax + b$, where $p > 2$. Suppose we want to compute the points to D digits of p -adic accuracy

Input. We are given the coefficients of E , modulo p^D

Output. $\langle T_i \rangle$, where $T \in E(\mathbb{Q}_p)[2]$ and $i = 1, 2$.

1. $n \leftarrow \#\overline{E}_{ns}(\mathbb{F}_p)$
2. If $\gcd(n, 2) = 1$ and !BAD2 then Return $\langle O \rangle$.
3. Generate non-trivial elements in $\overline{E}_{ns}(\mathbb{F}_p)[2]$, say \overline{P}_i .
4. Lift \overline{P}_i to $P_i \in E_0(\mathbb{Q}_p)[2]$ by a naive procedure using $x^3 + ax + b$.
5. If !BAD2 then Return $\langle P_i \rangle$ and $\langle O \rangle$.
6. If BAD2 then we naively lift \overline{Q} , the singular point on $\overline{E}(\mathbb{F}_p)$ (which is a 2-torsion point) to $Q_j \in E(\mathbb{Q}_p)[2] \setminus E_0(\mathbb{Q}_p)[2]$ using $x^3 + ax + b$. Return $\langle P_i \rangle, \langle Q_j \rangle$ and $\langle O \rangle$.

Theorem 6. *The above algorithm works as desired.*

Proof. We use the fact that the 2-torsion points have 0 as their y -coordinates. Since $E_1(\mathbb{Q}_p)[2] = 0$ and $\mathbb{Z}_p/2\mathbb{Z}_p = 0$, the appropriate application of the snake lemma sequence tells us that $E_0(\mathbb{Q}_p)[2] \cong \overline{E}_{ns}(\mathbb{F}_p)[2]$.

If we are not in the BAD2 case, by theorem 9 we have $E_0(\mathbb{Q}_p)[2] \cong E(\mathbb{Q}_p)[2]$. So if $\gcd(n, 2) = 1$, there are no non-trivial $E(\mathbb{Q}_p)[2]$ points. On the other hand if $\gcd(n, 2) \neq 1$, we might obtain 1 or 3 non-trivial $E(\mathbb{Q}_p)[2]$ points by lifting $\overline{E}_{ns}(\mathbb{F}_p)[2]$ points.

Now if we are in the BAD2 case, there might be a contribution of 0, 1 or 2, $E(\mathbb{Q}_p)[2]$ points from the singular point.

If the curve has good reduction at p , we can use Hensel's lemma (since $x^3 + \overline{a}x + \overline{b}$ has no repeated roots as \overline{E} is a non-singular curve) to lift the points. In the bad reduction case at p we can lift the points in a brute-force fashion. Fixing the prime p , the complexity is $O(D)$ bit operations. QED.

5 Computing $E(\mathbb{Q})_{tors}$

In this section we use the algorithms devised in the previous sections to determine the $E(\mathbb{Q})_{tors}$ group efficiently. We first recall a fact about torsion over $\overline{\mathbb{Q}}$.

Theorem 7. [12](Corollary 6.4b) $E(\overline{\mathbb{Q}})[m] = (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$

The algorithms which are currently in use for this computation are guided by the following theorems due to Nagell-Lutz and Mazur respectively.

Theorem 8. [12](Corollary 7.2) (Nagell-Lutz) Let E/\mathbb{Q} be an elliptic curve with Weierstrass equation

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}$$

Suppose $O \neq P \in E(\mathbb{Q})_{tors}$ then $x(P), y(P) \in \mathbb{Z}$ and either $y(P) = 0$ or $y(P)^2 | (4a^3 + 27b^2)$ is the discriminant of E .

Theorem 9. [12](Theorem 7.5) (Mazur)

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z}, & 1 \leq n \leq 10, 12 \text{ case (i)} \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}, & 1 \leq n \leq 4 \text{ case (ii)} \end{cases}$$

Observe that an elliptic curve over \mathbb{Q} can be transformed into the form which appears in the Nagell-Lutz theorem.

One approach is to do the computation in a brute force fashion using the Nagell-Lutz theorem. The downsides of this method are that it involves factoring Δ and there might be many square divisors of Δ making this naive procedure computationally expensive [2] (page 2). This algorithm was in vogue till Doud [2] discovered his $O(\log^3 C)$ -time algorithm, where $C = \max(|a^3|, |b^2|)$, which used complex-analytic techniques.

The constant C arises by making the observation that the coordinates of the torsion points are $O(C)$ in magnitude. Suppose $P \in E(\mathbb{Q})_{tors}$ then $x(P)$ will be a root of $x^3 + ax + b - y(P)^2$ and by Nagell-Lutz $y(P)^2 | (a^3 + 27b^2)$ which implies $x(P) | (b - (4a^3 + 27b^2)/k)$ for some $k \in \mathbb{Z}$.

Algorithm 4 *Input.* Given an elliptic curve E in the form $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$

Output. $\langle T, t \rangle_i$, where $T \in E(\mathbb{Q})[t]$ and $i = 1, 2$ and these points are the generators of $E(\mathbb{Q})_{tors}$.

Remark 6. In the following algorithm we compute a non-zero element of $E(\mathbb{Q}_p)[p]$ by solving the p -division polynomial in a brute-force fashion to $O(\log_p C)$ p -adic precision. In the BAD case we use the singular point on $\overline{E}(\mathbb{F}_p)$ and a point in $\overline{E}(\mathbb{F}_p)[p]$ otherwise.

Remark 7. Suppose we have $x(P)$, where $P \in E(\mathbb{Q}_p)[p]$, we compute Q , a $2p$ -torsion point by solving p -adically for $x(Q)$ using the following duplication formula:

$$x(P) = \frac{x(Q)^4 - 2ax(Q)^2 - 8bx(Q) + a^2}{4x(Q)^3 + 4ax(Q) + 4b}$$

Remark 8. Suppose we have $x(P)$, where $P \in E(\mathbb{Q}_p)[p]$, we compute Q , a $3p$ -torsion point by solving p -adically for $x(Q)$ using the following triplication formula:

$$\begin{aligned} x(P) &= \lambda^2 - a - x(Q) - x([2]Q) \\ \lambda &= (x([2]Q)^3 - ax([2]Q) - 6x(Q)^2x([2]Q) + 5x(Q)^3 + ax(Q))/(x([2]Q) - x(Q))^2 \end{aligned}$$

Remark 9. In this algorithm before the output is returned we need to check whether a $E(\mathbb{Q}_p)$ point is in $E(\mathbb{Q})$. This is possible because a priori we know the magnitude of the rational torsion points. Also negative integers (which are an infinite power series) are detected by noticing a recurring $p-1$ in the truncated p -adic expansion. They can be recovered as follows: $\sum_{i=0}^{\infty} a_i p^i = -(p - a_0 + \sum_{i=1}^{\log C} (p-1 - a_i)p^i)$, where the left hand side represents the negative integer as a p -adic number.

1. Compute $E(\mathbb{Q})[2]$. Use a small prime ($p = 3, 5, 7$) to compute $E(\mathbb{Q}_p)[2]$. $r \leftarrow \#E(\mathbb{Q})[2] - 1$. Let R_1, \dots, R_r be the x -coordinates of the non-trivial points.
2. If $r = 0$ then
 - (a) For $p = 3, 5, 7$ do the following:
 - i. Compute $\#E_0(\mathbb{Q}_p)[p]$.
 - ii. If BAD then goto step 4.
 - iii. If $\#E_0(\mathbb{Q}_p)[p] == 1$ then goto start of the loop and iterate with next prime.
 - iv. Compute a point Q (Remark 8) and if successful then
 - A. If $p = 5, 7$ then Return $\langle Q, p \rangle$.
 - B. If $p = 3$ and !BAD then Return $\langle Q, p \rangle$.
 - C. If $p = 3$, BAD and $\#E_0(\mathbb{Q}_p)[p] == 1$ then Return $\langle Q, p \rangle$.
 - D. If $p = 3$, BAD and $\#E_0(\mathbb{Q}_p)[p] \neq 1$ then try to compute S , a non-trivial 9-torsion point using the triplication formula (Remark 10). If successful then
 - Return $\langle S, 9 \rangle$
 - else Return $\langle Q, 3 \rangle$
 - (b) Return $\langle O, 1 \rangle$.
3. If $r = 1$ then
 - (a) For $p = 3, 5$ do the following:
 - i. Compute $\#E_0(\mathbb{Q}_p)[p]$.
 - ii. If BAD then goto step 4.
 - iii. If $\#E_0(\mathbb{Q}_p)[p] == 1$ then goto start of the loop and iterate with next prime.

- iv. Compute a point Q (Remark 8). If successful then
 - A. $U \leftarrow R_1 + Q$.
 - B. If $p = 5$ then Return $\langle U, 10 \rangle$
 - C. If $p = 3$ then try and compute V , a non-trivial 12-point using the duplication formula and U (Remark 9). If successful then
 - Return $\langle V, 12 \rangle$
 - else Return $\langle U, 6 \rangle$
 - (b) Try and compute a non-trivial W , a non-trivial 4-torsion point using the duplication formula and R_1 (Remark 9). If successful then
 - try and compute Z , a non-trivial 8-torsion point using the duplication formula and W (Remark 9). If successful then
 - Return $\langle Z, 8 \rangle$
 - else Return $\langle W, 4 \rangle$
 - (c) Return $\langle R_1, 2 \rangle$.
4. If $r = 3$ then
- (a) For $p = 3$ do the following:
 - i. Compute $\#E_0(\mathbb{Q}_p)[p]$.
 - ii. If BAD then goto step 4.
 - iii. If $\#E_0(\mathbb{Q}_p)[p] == 1$ then exit loop.
 - iv. Compute a point Q (Remark 8). If successful then
 - A. $U \leftarrow R_1 + Q$.
 - B. Return $\langle U, 6 \rangle$ and $\langle R_2, 2 \rangle$.
 - (b) For R_1, R_2, R_3 do the following:
 - i. Try and compute W , a non-trivial 4-torsion point using the duplication formula and R_i (Remark 9). If successful
 - then try and compute Z , a non-trivial 8-torsion point using the duplication formula and W (Remark 9). If successful then
 - Return $\langle Z, 8 \rangle$ and $\langle R_{i+1}, 2 \rangle$
 - else Return $\langle W, 4 \rangle$ and $\langle R_{i+1}, 2 \rangle$
 - (c) Return $\langle R_1, 2 \rangle$ and $\langle R_2, 2 \rangle$

Theorem 10. *The above algorithm works as desired*

Proof. Observe that if $\#E(\mathbb{Q})[2] = 4$ then by theorem 7 we are in case (ii) of Mazur’s classification. Conversely suppose case (ii) holds then assuming $\#E(\mathbb{Q})[2] = 1, 2$ leads us to contradictions.

So we first compute points in $E(\mathbb{Q}_p)[2]$ and check to see if we get 1, 2, 4 points in $E(\mathbb{Q})[2]$ (equivalently $x^3 + ax + b$ has 0, 1, 3 roots in \mathbb{Q}).

The algorithm works since the map $E(\mathbb{Q})[p] \rightarrow E(\mathbb{Q}_p)[p]$ is injective and for $p > 2$, $\#E(\mathbb{Q}_p)[p] = 1, p$. We compute the p -adic expansions of the points iteratively modulo p^i using a naive method such that these points make the p -division polynomials vanish modulo p^i .

The rest of the algorithm proceeds in a case-by-case fashion aided by the following implications of Mazur's result, which forms an outline of the algorithm. Let $r = \#E(\mathbb{Q})[2] - 1$ and when we discuss torsion we mean non-trivial torsion.

- $r = 3 \Leftrightarrow$ case (ii) (see above).
- If $r = 0$ then there is either atmost one 5-torsion or atmost one 7-torsion.
- If $r = 0$ and there is a 3-torsion then there is atmost one 9-torsion.
- If $r = 1$ and there is a 5-torsion then there is atmost one 10-torsion.
- If $r = 1$ and there is a 3-torsion then there is atleast one 6-torsion and atmost one 12-torsion.
- If $r = 1$ and there is a 4-torsion then there is atmost one 8-torsion.
- If $r = 3$, there is atmost one 3-torsion.
- If $r = 3$ and there is a 4-torsion then there is atmost one 8-torsion.

The above algorithm runs in $O(\log C)$ -time as the primes involved are small – 3, 5, 7 – and only $O(\log C)$ many p -adic digits are required to recover the integer coordinates.

Remark 10. We resort to brute-force computation of the points since lifting $\overline{E}(\mathbb{F}_p)[p]$ to $E(\mathbb{Q}_p)[p]$ via Hensel's lemma fails due to the presence of repeated roots in the p -division polynomials.

On the other hand, suppose l is a prime different from p that divides $\#\overline{E}(\mathbb{F}_p)$ but $l \neq \#\overline{E}(\mathbb{F}_p)$ then Hensel's lemma can be used to lift $\overline{E}(\mathbb{F}_p)[l]$ points to $E(\mathbb{Q}_p)[l]$ using l -division polynomials by solving linear equations at each level (to determine the p -adic coefficients of the lifted point).

6 Conclusions and future directions

The natural question to ask is whether the algorithms presented in this paper generalize to compute torsion on jacobians of curves over number fields. Although some of the theorems and algorithms seem to carry over in theory, in practice the first objects which will be needed to accomplish this will be explicit formal group laws and logarithm maps for these varieties. In this regard Freije's [3] method to construct the formal group law and logarithm map of the jacobian of an algebraic curve provides a start.

References

- [1] Doud D. *A procedure to calculate torsion of elliptic curves over \mathbb{Q}* . *Manuscripta Mathematica*, 95(1998), 463–469.
- [2] Freije, M. N. *The formal group of the Jacobian of an algebraic curve*. *Pacific J. Math.* 157, 1993, no. 2, 241–255.
- [3] Koblitz, N. *A Course in Number Theory and Cryptography*. GTM 114, Springer-Verlag, 1994.
- [4] Milne, J. S. *Class Field Theory*. Available at <http://jmilne.org/math/>
- [5] Milne, J. S. *Elliptic Curves*. Available at <http://jmilne.org/math/>
- [6] Satoh, T. *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*. *J. Ramanujan Math. Soc.* 15 (2000), no. 4, 247–270.
- [7] Schoof, R. *Counting points on elliptic curves over finite fields*. *Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993)*. *J. Théor. Nombres Bordeaux* 7 (1995), no. 1, 219–254.
- [8] Silverman, J. H. *The Arithmetic of Elliptic Curves*. GTM 106, Springer-Verlag, 1986.
- [9] Silverman, J. H. *Advanced Topics in the Arithmetic of Elliptic Curves*. GTM 151, Springer-Verlag, 1994.