

On computing rational torsion on elliptic curves

Iftikhar A. Burhanuddin
Department of Computer Science
University of Southern California
Los Angeles, CA 90007
burhanud@usc.edu

Ming-Deh Huang
Department of Computer Science
University of Southern California
Los Angeles, CA 90007
huang@usc.edu

ABSTRACT

We introduce an l -adic algorithm to efficiently determine the group of rational torsion points on an elliptic curve. We also make a conjecture about the discriminant of the m -division polynomial of an elliptic curve.

1. INTRODUCTION

Let K be a number field and E an elliptic curve over K then the Mordell-Weil theorem [11](Theorem VIII.6.7) tells us that $E(K)$ the group of K -rational points is finitely generated. This implies that $E(K)_{tors}$ the group of K -rational torsion is finite. In this extended abstract we will focus on the case when $K = \mathbb{Q}$. A theorem of Mazur [11](Theorem VIII.7.5) tells us about the groups which can appear as $E(\mathbb{Q})_{tors}$.

One approach to do elliptic curve rational torsion computation is by using the Nagell-Lutz theorem [11](Corollary VIII.7.2) in a brute force fashion. The downsides of this method are that it involves factoring the discriminant of the elliptic curve and also this discriminant might have many square divisors making this procedure computationally expensive. This naive method was in vogue till Doud [7] discovered the first polynomial time algorithm which used complex analytic techniques and ran in cubic time, where the size of input is the size of the coefficients of the elliptic curve.

A softly quadratic time algorithm ('softly' - where logarithmic factors are ignored) was proposed by Garcia-Selfa et al [9], where they compute with the Tate Normal Form of an elliptic curve. Their procedure uses Loos' root-finding algorithm as a blackbox routine and does not use any information about how the discriminant of F_m (polynomials which arise in this algorithm) are related to the discriminant of the elliptic curve. And hence a different prime is selected to compute the roots of F_m for each m .

In section 3 we present an algorithm to compute $E(\mathbb{Q})_{tors}$ with a worst case softly quadratic running time. A random-

ized version of the algorithm has an expected softly linear time complexity. Section 4 is devoted to time complexity analysis of these procedures.

The basic idea of our algorithm is given an elliptic curve E over \mathbb{Q} we view it as a curve over \mathbb{Q}_l and using Hensel's lemma compute $E(\mathbb{Q}_l)[m]$, the \mathbb{Q}_l -rational m -torsion points to desired precision, which is dictated by the Nagell-Lutz theorem [11](Corollary VIII.7.2). We then check to see if these points are in $E(\mathbb{Q})[m]$, the group of m -torsion rational points on E . Our algorithm and in particular the choice of the prime l rests on the fact that the prime support of the m -division polynomial equals the prime support of m and the prime support of the discriminant of the elliptic curve. We did not find a reference for it and hence in the next section we prove this for the sake of completeness. This relationship between the discriminants enables us to use a single 'good' prime to compute the m -torsion for all m .

We were curious to know how the $\Delta(f_m)$ the discriminant of f_m the m -division polynomial related to Δ the discriminant of the elliptic curve. So using Magma and Pari-GP we symbolically computed the discriminants of these polynomials for small values of m which led us to make the following conjecture ¹:

$$\Delta(f_m) = \begin{cases} (-1)^{\frac{m-1}{2}} m^{d-1} \Delta^{\frac{d(d-1)}{6}} & m \text{ odd} \\ 2^4 m^{d-4} \Delta^{\frac{d(d-1)}{6}} & m \text{ even} \end{cases}$$

where $d = \deg f_m$. In section 5 we elaborate on how we stumbled upon this interesting formula and prove some lemmas which strengthen it.

We do not attempt a self-contained exposition. The background material on elliptic curves can be found in [11]. We borrow freely but with due acknowledgement and gratitude from the literature mentioned in the References section. We would like to thank Pierrick Gaudry, Sheldon Kamienny, Wayne Raskind and William Stein for helpful discussions. The authors were supported in part by the following NSF grants CCR-9820778 and CCR-0306393.

2. DIVISION POLYNOMIALS

¹On February 1st, 2005 we were informed by Harold M. Stark that our conjectural formula in the odd case is equivalent to Lemma 1 in: Stark, H. M. *A Theorem of Coates-Wiles Revisited*, Seminar on Fermat's Last Theorem. Birkhauser, 1981.

In this section we present definitions and theorems concerning torsion points and polynomials which characterize them. The heart of this section is lemma 3, which forms the basis of our algorithm.

Let K be a number field and \bar{K} its algebraic closure. Let E be an elliptic curve over K given by a Weierstrass equation of the form $y^2 = x^3 + ax + b$, where $a, b \in R$, where R is the ring of integers of K .

THEOREM 1. [11](Corollary 6.4b) $E(\bar{K})[m] = (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$

Define division polynomials Ψ_m recursively as follows [11] (Exercise III.3.7):

$$\begin{aligned}\Psi_1 &= 1, \Psi_2 = 2y, \Psi_3 = 3x^4 + 6ax^2 + 12bx - a^2, \\ \Psi_4 &= (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8bax - 2a^3 - 16b^2)\Psi_2, \\ \Psi_{2k+1} &= \Psi_{k+2}\Psi_k^3 - \Psi_{k-1}\Psi_{k+1}^3, k \geq 2 \\ \Psi_{2k} &= (\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2)\Psi_k/\Psi_2, k \geq 2\end{aligned}$$

Define for $m > 2$

$$f_m = \begin{cases} \Psi_m & m \text{ odd} \\ \Psi_m/\Psi_2 & m \text{ even} \end{cases}$$

Observe that f_m (also referred to as division polynomials) are univariate. The x-coordinates of the m -torsion points of E correspond to the roots of f_m in the following way [1](Corollary III.7): Let $P \in E(\bar{K})$, such that P is not a 2-torsion point. Then $P \in E[m] \Leftrightarrow f_m(x(P)) = 0$.

Let $d = \deg f_m$, which is equal to $\frac{m^2-1}{2}$, m odd and $\frac{m^2-4}{2}$, m even and the leading coefficient of f_m is m , when m is odd and $m/2$ otherwise, where $m > 2$.

Next we'll define the discriminant of a polynomial and related notions [6](Section 3.3.2) and then prove a few lemmas about the discriminants of the division polynomials.

Let S be an integral domain with quotient field L , and let \bar{L} be its algebraic closure. Let $g \in S[X]$ with $n = \deg(g)$ and $lc(g)$ be its leading coefficient, and let α_i be the roots of g in \bar{L} . Define the discriminant of g to be

$$\Delta(g) = (-1)^{\frac{n(n-1)}{2}} R(g, g')/l(g)$$

where $R(g, g')$ is the resultant of g, g' . Then we have

$$\Delta(g) = lc(g)^{n-1+\deg(g')} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2$$

Let $f = x^3 + ax + b$ and so $\Delta(f) = -(4a^3 + 27b^2)$. The discriminant of the elliptic curve is defined to be $\Delta(E) = -16(4a^3 + 27b^2)$ (also denoted as Δ). From here on we'll assume that E is an elliptic curve over \mathbb{Q} given by $y^2 = x^3 + ax + b$, with $a, b \in \mathbb{Z}$. This implies that the division polynomials have integral coefficients and hence their discriminants $\Delta(f_m) \in \mathbb{Z}$, which is clear from the definition of the discriminant in terms of the Sylvester matrix [6](Lemma 3.3.4).

LEMMA 1. Let $m = 2k + 1 > 1$ be an integer.

1. $f | f'_m$
2. $2^2 | f'_m$
3. $m | f'_m$
4. $m^{d-1} | \Delta(f_m)$

PROOF. 1. We'll prove this by induction on m . $f'_3 = 12f$ and the base case holds. Suppose $f | f'_i$ for all odd $i < m$. Let's assume k is odd (in the even case a similar argument applies). We have $\Psi_{2k+1} = f_{2k+1} = f_{k+2}f_k^3 - (f_{k-1}\Psi_2)(f_{k+1}\Psi_2)^3 = f_{k+2}f_k^3 - f_{k-1}f_{k+1}^3\Psi_2^4 = f_{k+2}f_k^3 - 2^4 \cdot f_{k-1}f_{k+1}^3f^2$. Now $f'_{2k+1} = f'_{k+2}f_k^3 + 3 \cdot f_{k+2}f_k^2f'_k - 2^4 \cdot (f_{k-1}f_{k+1}^3)'f^2 - 2^5 \cdot f_{k-1}f_{k+1}^3ff'$. f divides f'_{k+2} and f'_k by the inductive assumption and hence f divides each of the terms in f'_{2k+1} . In particular f exactly divides f'_{2k+1} , otherwise f_{2k+1} would have repeated roots.

2. The argument is similar to the one above for part 1.
3. We know that for every m , $m | (\Psi_m^2)'$ and $p \nmid \Psi_m^2$, where p is an odd prime, [5] (Theorem 1, Corollary 1). Suppose $m = \prod_i p_i$, where p_i are odd primes. From the above, $m | \Psi_m \Psi'_m$ which implies $p_i | \Psi_m \Psi'_m$. Also $p_i \nmid \Psi_m$. Therefore $p_i | \Psi'_m$ and so $m | \Psi'_m$.
4. This follows from part 3, $lc(f_m) = m$ and the matrix definition of the discriminant, where the coefficients of f'_m are repeated on $\frac{m^2-1}{2}$ rows.

□

LEMMA 2. Let $m = 2k > 2$ be an integer.

1. $k | \Delta(f_m)$
2. $2^2 | f'_m$
3. $m | \Delta(f_m)$

PROOF. 1. Recall that $lc(f_m) = k$ and the coefficient of x^{d-1} in f_m is 0. Consider the matrix associated to $R(f_m, f'_m)$. The first column of this matrix has k at entry $(1, 1)$ and $k \frac{m^2-4}{2}$ at $(\frac{m^2-4}{2}, 1)$ and 0 elsewhere. The second column of this matrix has k at entry $(2, 2)$ and $k \frac{m^2-4}{2}$ at $(\frac{m^2-4}{2} + 1, 2)$ and 0 elsewhere. Hence $k^2 | R(f_m, f'_m)$ and $k | \Delta(f_m)$ by the definition of discriminant.

2. $2^2 | f'_m$ and the base case holds. Suppose $2^2 | f'_i$ for all even $i < m$. Now $f'_{2k} = (f_{k+2}f_{k-1}^2 - f_{k-2}f_{k+1}^2)f'_k + (f'_{k+2}f_{k-1}^2 + f_{k+2} \cdot 2 \cdot f_{k-1}f'_{k-1} - f'_{k-2}f_{k+1}^2 - f_{k-2} \cdot 2 \cdot f_{k+1}f'_{k+1})f_k$. Let's assume that k is odd (similar analysis for the even case). From the previous lemma we know that 2^2 divides f'_k, f'_{k+2}, f'_{k-2} . By the inductive hypothesis 2^2 also divides f'_{k-1}, f'_{k+1} . Hence $2^2 | f'_m$.

3. Follows from part 1 and 2.

□

LEMMA 3. *Prime support of $\Delta(f_m) = \text{prime support of } m \cup \text{prime support of } \Delta$, where $m > 2$ is an integer*

PROOF. We know that 2 and m divide $\Delta(f_m)$ (lemma 1, 2). So it suffices to prove that when $(m, p) = 1$ the prime support of $\Delta(f_m)$ equals the set of primes where E has bad reduction over \mathbb{Q} .

Consider E to be an elliptic curve over \mathbb{Q}_p . We'll take a minimal Weierstrass equation denoted again by E and let its discriminant be Δ . Let L be a finite extension of \mathbb{Q}_p . Let $\mathfrak{p} = (\pi)$ be the prime over p in the ring of integers of L , \mathbb{F}_p the residue field and e the ramification index.

Let $x = u^2x' + r, y = u^3y' + su^2x' + t$ be a change of coordinates giving a minimal Weierstrass equation for E/L denoted by E' . The discriminant Δ' for E' satisfies $v_{\mathfrak{p}}(\Delta') = v_{\mathfrak{p}}(u^{-12}\Delta)$.

Let x_i and $x'_i, 1 \leq i \leq d$ be the roots of the m -division polynomial associated to E and E' respectively. For $i \neq j$, we have $v_{\mathfrak{p}}(x'_i - x'_j) = v_{\mathfrak{p}}(\frac{x_i - r}{u^2} - \frac{x_j - r}{u^2}) = v_{\mathfrak{p}}(\frac{x_i - x_j}{u^2})$ and so $v_{\mathfrak{p}}(x_i - x_j) = 2v_{\mathfrak{p}}(u) + v_{\mathfrak{p}}(x'_i - x'_j)$

Next let's consider the valuation of the discriminant of the m -division polynomial associated to E over \mathbb{Q}_p :

$$\begin{aligned} v_{\mathfrak{p}}(\Delta(f_m)) \\ = (2d - 2)v_{\mathfrak{p}}(lc(f_m)) + 2 \sum_{1 \leq i < j \leq d} (2v_{\mathfrak{p}}(u) + v_{\mathfrak{p}}(x'_i - x'_j)) \end{aligned}$$

So let's assume $(m, p) = 1$. Observe that $v_{\mathfrak{p}}(\cdot) = ev_p(\cdot)$. Since $v_p(m) = 0$, we have $v_{\mathfrak{p}}(lc(f_m)) = v_{\mathfrak{p}}(m) = 0$ when m is odd and when m is even, we have $v_{\mathfrak{p}}(lc(f_m)) = v_{\mathfrak{p}}(m/2) = 0$.

Case 1. Let E be an elliptic curve with potential good reduction over \mathbb{Q}_p . Let $L = \mathbb{Q}_p(E(\overline{\mathbb{Q}_p})[m])$ be a finite extension of \mathbb{Q}_p over which E has good reduction [12](Proposition IV.10.3) which means $v_{\mathfrak{p}}(\Delta') = 0$ and so $v_{\mathfrak{p}}(u) = v_{\mathfrak{p}}(\Delta)/12$.

Moreover the reduction modulo \mathfrak{p} map $E(L)[m] \rightarrow \overline{E}(\mathbb{F}_p)[m]$ is injective [11](Proposition VII.3.1 b) and hence $v_{\mathfrak{p}}(x'_i - x'_j) = 0$ for all $i \neq j$ and so $v_{\mathfrak{p}}(\Delta(f_m)) = d(d - 1)/6 \cdot v_{\mathfrak{p}}(\Delta)$ which implies that

$$v_p(\Delta(f_m)) = \frac{d(d-1)}{6} \cdot v_p(\Delta)$$

So if p is a prime of good reduction for E/\mathbb{Q} then $p \nmid \Delta(f_m)$ and if p is a prime of bad (additive) reduction then $p \mid \Delta(f_m)$.

Case 2. Let E be an elliptic curve with potential multiplicative reduction over \mathbb{Q}_p . Let $L \supset \mathbb{Q}_p(E(\overline{\mathbb{Q}_p})[m])$ be a finite extension of \mathbb{Q}_p over which E has (split) multiplicative reduction which means $v_{\mathfrak{p}}(\Delta') > 0$ and $v_{\mathfrak{p}}(c'_4) = 0$. We know that $v_{\mathfrak{p}}(c'_4) = v_{\mathfrak{p}}(u^{-4}c_4)$ so $v_{\mathfrak{p}}(u) = v_{\mathfrak{p}}(c_4)/4$. Also $j = c_4^3/\Delta$ and so $v_{\mathfrak{p}}(c_4) = \frac{1}{3} \cdot (v_{\mathfrak{p}}(\Delta) + v_{\mathfrak{p}}(j))$.

$$\begin{aligned} v_{\mathfrak{p}}(\Delta(f_m)) \\ = \frac{d(d-1)}{6} \cdot (v_{\mathfrak{p}}(\Delta) + v_{\mathfrak{p}}(j)) + \sum_{1 \leq i < j \leq d} 2v_{\mathfrak{p}}(x'_i - x'_j) \end{aligned}$$

Now $v_{\mathfrak{p}}(\Delta) + v_{\mathfrak{p}}(j) = 0$ or > 0 depending on whether E has multiplicative or additive reduction over \mathbb{Q}_p . Also in either case there exist i, j such that $v_{\mathfrak{p}}(x'_i - x'_j) > 0$ (x-coordinates of points which reduce to the singular point). Hence $v_{\mathfrak{p}}(\Delta(f_m)) > 0$ which implies $v_p(\Delta(f_m)) > 0$.

So if p is a prime of bad (additive or multiplicative) reduction for E over \mathbb{Q} then $p \mid \Delta(f_m)$. □

3. ALGORITHM

In this section we present some background material before we introduce our elliptic curve rational torsion algorithm. The methods which are currently in use for this computation are guided by the following theorems due to Nagell-Lutz and Mazur respectively.

THEOREM 2. [11](Corollary VIII.7.2) (Nagell-Lutz) *Let E be an elliptic curve over \mathbb{Q} 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 $y(P)^2 \mid (4a^3 + 27b^2)$.

THEOREM 3. [11](Theorem VIII.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 using a change of coordinates [11](Pages 46-50).

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 $y(P)^2 \mid (4a^3 + 27b^2)$ which implies $x(P) \mid (b - (4a^3 + 27b^2)/k)$ for some $k \in \mathbb{Z}$. Hence the coordinates of the torsion points are $O(C)$ in magnitude, where $C = \max(|a^3|, |b^2|)$.

To compute the points we use a combination of l -adic (and possibly p -adic when $l = p$) lifting techniques, using the following variant of the Hensel's lemma [8](Lemma 2.1).

LEMMA 4. *Let $u \in \mathbb{Z}_p$ and $h \in \mathbb{Z}_p[x]$. Let k be such that $p^k \mid \mid h'(u)$ and assume $p^{n+k} \mid h(u)$ for some $n > k$. Let*

$$\delta = \frac{p^{-k}h(u)}{p^{-k}h'(u)}$$

and $v = u - \delta$. Then $v \equiv u \pmod{p^n}$, $p^{2n} \mid h(v)$ and $p^k \mid \mid h'(v)$.

Hensel's lemma leads to an efficient (almost linear time) method to lift points provided the roots of the polynomial separate early enough (k is bounded by a constant or log of the required p -adic precision), which would ensure that the initialization procedure (where the root is computed modulo p^k) doesn't take more than softly-linear time.

As stated in the Introduction our algorithm works as follows: given an elliptic curve E over \mathbb{Q} we view it as a curve

over \mathbb{Q}_l and (using the appropriate factor of the m -division polynomial) compute the \mathbb{Q}_l -rational m -torsion points to desired precision and then check to see if they are in fact in $E(\mathbb{Q})$. The prime l is chosen such that E over \mathbb{Q}_l has good reduction. The integers m we have to consider are dictated by Mazur's theorem: 2, 3, 4, 5, 7, 8, 9.

Suppose we want to compute the roots of the m -division polynomial. If $l > 2$ is a prime of good reduction which was picked and $l \nmid m$ then the above lemma tells us that the roots of f_m are distinct modulo l and therefore we can lift an \mathbb{F}_l -root of f_m to \mathbb{Q}_l using Hensel's lemma with $k = 0$. On the other hand if p is the prime of good reduction selected and $p^i \mid m$, then we can lift a \mathbb{F}_p -root of f_{p^i} using Hensel's lemma with $k = i$ due to the following fact [10] (Lemma 2.7).

LEMMA 5. Let E be an ordinary 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 $p > 2$ and $ab \neq 0$. Suppose $E(\mathbb{Q}_p^{ur})[p^i] \neq O$. If $P \in E(\mathbb{Q}_p^{ur})[p^i]$ is a non-trivial point, then $v_p(\partial\Psi_{p^i}(x(P))) = i$.

The above lemma will play a role in the algorithm if the good prime chosen happens to be 3, 5 or 7 and we compute 3; 9, 5 and 7 torsion points respectively. In these scenarios the algorithm assumes a p -adic flavor.

The lemma deals with ordinary elliptic curves and so before we apply the lemma we should rule out the supersingular case. The following is a test for supersingularity [1](Page 46): Let E be an elliptic curve over \mathbb{Q}_p that had good reduction at p . E is supersingular iff

- $p \geq 5$ and $\#\overline{E}(\mathbb{F}_p) = p + 1$.
- $p = 2, 3$ and $\#\overline{E}(\mathbb{F}_p) = 1, p + 1$ or $2p + 1$.

Also if E is supersingular then $E(\mathbb{Q}_p)[p] = O$ and hence $E(\mathbb{Q})[p] = O$.

In the below algorithm before the output is returned we need to check whether a $E(\mathbb{Q}_l)$ point is in $E(\mathbb{Q})_{tors}$. 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 $l - 1$ in the truncated l -adic expansion. They can be recovered as follows: $\sum_{i=0}^{\infty} a_i l^i = -(l - a_0 + \sum_{i=1}^{\log_l C} (l - 1 - a_i) l^i)$, where the left hand side represents the negative integer as a l -adic number.

ALGORITHM 1. *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 $E(\mathbb{Q})_{tors}$.

1. Pick a prime $l > 2$ such that $l \nmid \Delta$
2. Compute $E(\mathbb{Q}_l)[2]$ using f

3. $r \leftarrow \#E(\mathbb{Q})[2] - 1$. Let R_1, \dots, R_r be the x -coordinates of the non-trivial points

4. If $r = 0$ then

(a) For $p = 3, 5, 7$ do the following:

- i. If $p \nmid \#\overline{E}(\mathbb{F}_1)$ then goto start of the loop and iterate with next prime
- ii. Compute $Q \in E(\mathbb{Q}_l)[p] \setminus \{O\}$ using f_p
- iii. If $Q \notin E(\mathbb{Q})$ then goto start of the loop and iterate with next prime.
- iv. If $p = 5, 7$ then Return $\langle Q, p \rangle$
- v. If $3^2 \mid \#\overline{E}(\mathbb{F}_1)$ then
 - Compute $S \in E(\mathbb{Q}_l)[9] \setminus E(\mathbb{Q}_l)[3]$ using f_9 . If $S \notin E(\mathbb{Q})$ then Return $\langle Q, 3 \rangle$ else Return $\langle S, 9 \rangle$
 - else Return $\langle Q, 3 \rangle$

(b) Return $\langle O, 1 \rangle$

5. If $r = 1$ then

(a) For $p = 3, 5$ do the following:

- i. If $p \nmid \#E(\mathbb{F}_1)[p]$ then goto start of the loop and iterate with next prime
- ii. Compute $Q \in E(\mathbb{Q}_l)[p] \setminus \{O\}$ using f_p
- iii. If $Q \notin E(\mathbb{Q})$ then goto start of the loop and iterate with next prime
- iv. $U \leftarrow R_1 + Q$
- v. If $p = 5$ then Return $\langle U, 10 \rangle$
- vi. If $4 \nmid \#\overline{E}(\mathbb{F}_1)$ then Return $\langle U, 6 \rangle$
- vii. Compute $V \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$ using f_4
- viii. If $V \in E(\mathbb{Q})$ then
 - Return $\langle V + Q, 12 \rangle$
 - else Return $\langle U, 6 \rangle$

(b) If $4 \nmid \#\overline{E}(\mathbb{F}_1)$ then Return $\langle R_1, 2 \rangle$

(c) Compute $W \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$ using f_4

(d) If $W \in E(\mathbb{Q})$ then

- If $8 \nmid \#\overline{E}(\mathbb{F}_1)$ then Return $\langle W, 4 \rangle$
- Compute $Z \in E(\mathbb{Q}_l)[8] \setminus E(\mathbb{Q}_l)[4]$ using f_8
- If $Z \in E(\mathbb{Q})$ then
 - Return $\langle Z, 8 \rangle$
 - else Return $\langle W, 4 \rangle$

(e) Return $\langle R_1, 2 \rangle$

6. If $r = 3$ then

(a) Do the following:

- i. If $3 \nmid \#\overline{E}(\mathbb{F}_1)$ then exit loop
- ii. Compute a point $Q \in E(\mathbb{Q}_l)[3] \setminus \{O\}$ using f_3
- iii. If $Q \in E(\mathbb{Q})$ then
 - A. $U \leftarrow R_1 + Q$
 - B. Return $\langle U, 6 \rangle$ and $\langle R_2, 2 \rangle$

(b) Do the following:

- i. If $8 \nmid \#\overline{E}(\mathbb{F}_1)$ then Return $\langle R_1, 2 \rangle$ and $\langle R_2, 2 \rangle$
- ii. Compute $W \in E(\mathbb{Q}_l)[4] \setminus E(\mathbb{Q}_l)[2]$ using f_4

iii. If $W \in E(\mathbb{Q})$ then

- If $16 \nmid \# \overline{E}(\mathbb{F}_l)$ then Return $\langle W, 4 \rangle$ and $\langle R_2, 2 \rangle$
- Compute $Z \in E(\mathbb{Q}_l)[8] \setminus E(\mathbb{Q}_l)[4]$ using f_8
- If $Z \in E(\mathbb{Q})$ then
 - Return $\langle Z, 8 \rangle$ and $\langle R_2, 2 \rangle$
 - else Return $\langle W, 4 \rangle$ and $\langle R_2, 2 \rangle$

(c) Return $\langle R_1, 2 \rangle$ and $\langle R_2, 2 \rangle$

LEMMA 6. *The algorithm works as desired*

PROOF. Observe that if $\#E(\mathbb{Q})[2] = 4$ then by theorem 3 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.

Our choice of prime $l > 2$ implies that E has good reduction at l and hence the reduction map $E(\mathbb{Q}_l)[m] \rightarrow \overline{E}(\mathbb{F}_l)[m]$ is injective for all m such that $(m, l) = 1$ [11](Proposition VII.3.1). Moreover the map $E(\mathbb{Q})[p] \rightarrow E(\mathbb{Q}_l)[p]$ is injective.

So we first compute points in $E(\mathbb{Q}_l)[2]$ 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 rest of the algorithm proceeds in a case-by-case fashion aided by the implications of Mazur's result, where we compute the l -adic expansions of the torsion points using Hensel's lemma and ascertain if they lie in $E(\mathbb{Q})$. \square

4. TIME COMPLEXITY ANALYSIS

Let $M(N)$ denote the bit operations required to multiply two numbers of size N . We'll assume that a fast integer multiplication algorithm like Schönhage-Strassen [13] (Theorem 8.24) is used in which case $M(N) = O(N \log N \log \log N) = \mathcal{O}(N)$ (in soft-Oh notation).

An integer of size N can be expressed p -adically using a recursive procedure called radix conversion [13](Theorem 9.17) in $O(M(N \log p) \log N)$ time.

To deterministically find l a prime which does not divide Δ takes $\mathcal{O}(\log^2 \Delta)$ [9]. We compute with f and m -division polynomials, where $m = 3, 4, 5, 7, 8, 9$ and the size of the coefficients of these polynomials are bounded by $O(\log C) = O(\log \Delta)$ [9]. Hence by resorting to a randomized algorithm [13](Corollary 18.12 (ii)) to pick a good prime, the expected running time is $\mathcal{O}(\log \Delta)$.

In either case the magnitude of this prime is $O(\log \Delta)$ [9], [13](Corollary 18.12 (ii)) and hence the time to compute $\# \overline{E}(\mathbb{F}_l)$ (which is unnecessary) is negligible and to find an \mathbb{F}_l -rational root of the division polynomial is $\mathcal{O}(\log \Delta)$.

Once we find an approximate root we use Hensel's lifting to a compute \mathbb{Q}_l -rational root up to $O(\log C) = O(\log \Delta)$ accuracy. Due to the quadratic convergence of the Hensel of lifting, if the desired precision is N then using a recursive algorithm we can half precision at each level and perform lifting in $O(M(N \log l)) = \mathcal{O}(\log \Delta)$ bit operations [8], [13](Theorem 9.26) (assuming the degree of the polynomial is constant).

So the finding the good prime routine dictates the overall running time of the algorithm, which is $\mathcal{O}(\log^2 \Delta)$ deterministic time or an expected running time of $\mathcal{O}(\log \Delta)$.

5. DISCRIMINANT OF DIV POLYNOMIAL

While investigating the discriminant of the m -division polynomials we stumbled upon a precise conjectural formula which expresses $\Delta(f_m)$ in terms of m and the discriminant of the elliptic curve E .

Using Magma running on a Pentium IV 1.80 GHz, 128 MB RAM, Windows XP system we symbolically computed the following discriminants:

m	d	$\Delta(f_m)$	Time
3	4	$-3^3 \Delta^2$	0
4	6	$2^4 \cdot 4^2 \Delta^5$	0
5	12	$5^{11} \Delta^{22}$	0.047 s
6	16	$2^4 \cdot 6^{12} \Delta^{40}$	0.234 s
7	24	$-7^{23} \Delta^{92}$	7.407 s
8	30	$2^4 \cdot 8^{26} \Delta^{145}$	1 m 0.437 s
9	40	$9^{39} \Delta^{260}$	15 m 56.953 s
10	48	$2^4 \cdot 10^{44} \Delta^{376}$	1 h 34 m 37.984 s
11	60	$-11^{59} \Delta^{590}$	13 h 15 m 27.812 s
12	70	$2^4 \cdot 12^{66} \Delta^{805}$	50 h 36 m 25.907 s

Based on the above we make the following conjecture:

CONJECTURE 1.

$$\Delta(f_m) = \begin{cases} (-1)^{\frac{m-1}{2}} m^{d-1} \Delta^{\frac{d(d-1)}{6}} & m \text{ odd} \\ 2^4 m^{d-4} \Delta^{\frac{d(d-1)}{6}} & m \text{ even} \end{cases}$$

In Lemma 3, we showed that the conjecture holds when $(m, p) = 1$ and E is an elliptic curve with potential good reduction over \mathbb{Q}_p . Extending that train of thought we present some results proved in [3] which strengthen the above.

LEMMA 7. *The conjecture holds when $m = p$ an odd prime and E an elliptic curve with potential good reduction over \mathbb{Q}_p .*

PROOF. Let $L = \mathbb{Q}_p(E(\overline{\mathbb{Q}_p})[m])$ be a finite extension of \mathbb{Q}_p over which E has good reduction [12](Proposition IV.10.3) which means $v_p(\Delta') = 0$ and so $v_p(u) = v_p(\Delta)/12$. Also $lc(f_p) = p$.

Case 1. Let \overline{E} over \mathbb{F}_p be a supersingular elliptic curve. So $\overline{E}(\mathbb{F}_p)[p] = O$ and so $E_1(L)[p] \cong E(L)[p]$.

Let t_i be the local parameter of the point whose x -coordinate is x'_i and y -coordinate is positive. In terms of t_i we know that $x'_i = t_i^{-2} - a't_i^2 + O(t_i^3)$ and $y'_i = -t_i^{-3} + a't_i + O(t_i^2)$ [11](Page 113). So $v_p(x'_i - x'_j) = v_p(t_i^{-2} - t_j^{-2}) = v_p(t_i - t_j) + v_p(t_i + t_j) - 2v_p(t_i) - 2v_p(t_j)$.

For each i , $v_p(t_i) > 0$ since the local parameters are elements of the elliptic curve formal group that is elements of maximal ideal of the ring of integers of L . We know that $t_i \neq \pm t_j, 1 \leq$

$i < j \leq \frac{m^2-1}{2}$ and $v_p(t_i) = e/(p^2 - 1) = e/2d$, for all i [2][lemma 4.7]. Now let's consider the addition \oplus of local parameters in the formal group: $t_i \oplus t_j = t_i + t_j +$ higher order terms. Now $v_p(t_i \oplus t_j) = v_p(t_i + t_j)$ since the valuation of the higher order terms is strictly greater than that of the latter. Similarly $v_p(t_i \ominus t_j) = v_p(t_i - t_j)$. Hence $v_p(x'_i - x'_j) = (-2) \cdot e/2d = -e/d$.

$$\begin{aligned} v_p(\Delta(f_p)) &= (2d-2)v_p(p) + \frac{d(d-1)}{6} \cdot v_p(\Delta) + 2 \sum_{1 \leq i < j \leq d} v_p(x'_i - x'_j) \\ &= (2d-2)e + \frac{d(d-1)}{6} \cdot v_p(\Delta) + 2d(d-1)/2 \cdot (-e/d) \\ &= (d-1)e + \frac{d(d-1)}{6} \cdot v_p(\Delta) \end{aligned}$$

Thus $v_p(\Delta(f_p)) = d-1 + \frac{d(d-1)}{6} \cdot v_p(\Delta)$.

Case 2. Let \bar{E} over \mathbb{F}_p be an ordinary elliptic curve. So $\bar{E}(\mathbb{F}_p)[p] = \mathbb{Z}/p\mathbb{Z}$ and the short exact sequence $0 \rightarrow E_1(L)[p] \rightarrow E(L)[p] \rightarrow \bar{E}(\mathbb{F}_p)[p] \rightarrow$ is isomorphic to the short exact sequence $0 \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z} \rightarrow 0$.

Let $\langle Q \rangle = E_1(L)[p]$ and $P \in E(L)[p] \setminus E_1(L)[p]$ then $\Psi_p(X) = \prod_{1 \leq i \leq \frac{p-1}{2}} (X - x(iQ)) \prod_{1 \leq i \leq \frac{p-1}{2}, 0 \leq j \leq p-1} (X - x(iP + jQ))$

Let t_i be the local parameter of the point iQ . We know that $v_p(t_i) = e/(p-1)$ [2](Lemma 4.3).

$$\begin{aligned} x(iP + jQ) &= \left(\frac{y(jQ) - y(iP)}{x(jQ) - x(iP)} \right)^2 - x(iP) - x(jQ) \\ &= \left(\frac{-t_j^{-3} + a't_j + O(t_j^2) - y(iP)}{t_j^{-2} - a't_j^2 + O(t_j^3) - x(iP)} \right)^2 - x(iP) - t_j^{-2} + a't_j^2 + O(t_j^3) \\ &= t_j^{-2} \left(\frac{-1 - y(iP)t_j^3 + a't_j^2 + O(t_j^5)}{1 - x(iP)t_j^2 - a't_j^4 + O(t_j^5)} \right)^2 - x(iP) - t_j^{-2} + a't_j^2 + O(t_j^3) \\ &= t_j^{-2} + 2x(iP) + 2y(iP)t_j + 3x(iP)^2 t_j^2 + 4x(iP)y(iP)t_j^3 + \dots - x(iP) - t_j^{-2} + a't_j^2 + O(t_j^3) \\ &= x(iP) + 2y(iP)t_j + 3x(iP)^2 t_j^2 + a't_j^2 + O(t_j^3) \end{aligned}$$

Let's analyze $\sum_{1 \leq i < j \leq d} 2v_p(x'_i - x'_j)$.

1. $\sum_{1 \leq i < j \leq \frac{p-1}{2}} 2v_p(x(iQ) - x(jQ)) = 2(-2) \cdot \frac{e}{p-1} \cdot \frac{(p-1)(p-3)}{2^3}$
2. $\sum_{1 \leq i, j \leq \frac{p-1}{2}, 0 \leq k \leq p-1} 2v_p(x(iQ) - x(jP + kQ)) = 2(-2) \cdot \frac{e}{p-1} \cdot \frac{(p-1)^2 p}{2^2}$
3. $\sum_{1 \leq i \leq \frac{p-1}{2}, 0 \leq j_1 < j_2 \leq p-1} 2v_p(x(iP + j_1Q) - x(iP + j_2Q)) = 2 \cdot \frac{e}{p-1} \cdot \frac{p(p-1)^2}{2^2}$
4. $\sum_{1 \leq i_1 < i_2 \leq \frac{p-1}{2}, 0 \leq j \leq p-1} 2v_p(x(i_1P + jQ) - x(i_2P + jQ)) = 0$
5. $\sum_{1 \leq i_1 < i_2 \leq \frac{p-1}{2}, 0 \leq j_1 < j_2 \leq p-1} 2v_p(x(i_1P + j_1Q) - x(i_2P + j_2Q)) = 0$
6. $\sum_{1 \leq i_1 < i_2 \leq \frac{p-1}{2}, 0 \leq j_2 < j_1 \leq p-1} 2v_p(x(i_1P + j_1Q) - x(i_2P + j_2Q)) = 0$

$$\sum_{1 \leq i < j \leq d} 2v_p(x'_i - x'_j) = 2(-2) \cdot \frac{e}{p-1} \cdot \frac{(p-1)(p-3)}{2^3} + 2(-2) \cdot \frac{e}{p-1} \cdot$$

$$\frac{(p-1)^2 p}{2^2} + 2 \cdot \frac{e}{p-1} \cdot \frac{p(p-1)^2}{2^2} = -(d-1)e$$

$$\begin{aligned} v_p(\Delta(f_p)) &= (2d-2)v_p(p) + \frac{d(d-1)}{6} \cdot v_p(\Delta) + 2 \sum_{1 \leq i < j \leq d} v_p(x'_i - x'_j) \\ &= (2d-2)e + \frac{d(d-1)}{6} \cdot v_p(\Delta) - (d-1)e \\ &= (d-1)e + \frac{d(d-1)}{6} \cdot v_p(\Delta) \end{aligned}$$

Therefore $v_p(\Delta(f_m)) = d-1 + \frac{d(d-1)}{6} \cdot v_p(\Delta)$. \square

The proof in the scenario where E has potential multiplicative reduction over \mathbb{Q}_p and $m = p$ is tackled using the theory of local heights [3].

6. CONCLUSIONS

The natural question to ask is whether the techniques presented in this paper generalize to compute torsion on jacobians of curves over number fields. Also an analogous conjecture for hyperelliptic curves is being sought working with David Cantor's paper [4] on division polynomials for hyperelliptic curves.

7. REFERENCES

- [1] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press, Cambridge, 1999.
- [2] J. Boxall and D. Grant. Singular torsion points. *Mathematical Research Letters*, 10, 2003.
- [3] I. A. Burhanuddin and M.-D. Huang. Discriminant of the division polynomial of an elliptic curve. *Preprint*, 2004.
- [4] D. G. Cantor. On the analogue of the division polynomials for hyperelliptic curves. *J. Reine Angew. Math.*, 447:91–145, 1994.
- [5] J. W. S. Cassels. A note on the division values of $\mathbf{p}(u)$. *Proc. Cambridge Philos. Soc.*, 45:167–172, 1949.
- [6] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer-Verlag, Berlin, 2000.
- [7] D. Doud. A procedure to calculate torsion of elliptic curves over \mathbb{Q} . *Manuscripta Mathematica*, 95:463–469, 1998.
- [8] M. Fouquet, P. Gaudry, and R. Harley. An extension of satoh's algorithm and its implementation. *J. Ramanujan Math. Soc.*, 15:281–318, 2000.
- [9] I. Garcia-Selfa, M. A. Olalla, and J. M. Tornero. Computing the rational torsion of an elliptic curve using tate normal form. *J. Number Theory*, 96:76–88, 2002.
- [10] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *J. Ramanujan Math. Soc.*, 15(4):247–270, 2000.
- [11] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1986.
- [12] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.
- [13] J. von zur Gathen and J. Gerhard. *Modern Computer Algebra*. Cambridge, Cambridge, 1999.