Discrete Logarithms and Mordell-Weil Groups

Mohammad Sadek

Abstract

Let E_p be an elliptic curve over a prime finite field $\mathbb{F}_p$, $p \geq 5$, and $P_p, Q_p \in E_p(\mathbb{F}_p)$. The elliptic curve discrete logarithm problem, ECDLP, on E_p is to find $m_p \in \mathbb{F}_p^\times$ such that $Q_p = m_p P_p$ if $Q_p \in \langle P_p \rangle$. We propose an algorithm to attack the ECDLP relying on a Hasse principle detecting linear dependence in Mordell-Weil groups of elliptic curves via a finite number of reductions.

1 Introduction

The elliptic curve discrete logarithm problem, ECDLP, is the basis for elliptic cryptosystyms. Given an elliptic curve E_p defined over the prime field $\mathbb{F}_p, p \geq 5$, with two points $P_p, Q_p \in E(\mathbb{F}_p)$, the difficulty of finding an $m \in \mathbb{F}_p^\times$ such that $Q_p = mP_p$ is the essence of the security of an elliptic cryptosystem. Many algorithms were created to attack the ECDLP, yet only a few were proved to be efficient and they work only for special families of elliptic curves. For example, one can solve the ECDLP on supersingular elliptic curves, [6], and elliptic curves with trace one, [10].

Two of the main approaches to solve the ECDLP depend on finding liftings of elliptic curves. The first attack called the Index Calculus requires one to lift E_p to an elliptic curve E over $\mathbb{Q}$, then lift P_p, Q_p to points $P, Q \in E(\mathbb{Q})$. However, lifting points in $E(\mathbb{F}_p)$ to points in $E(\mathbb{Q})$ might be harder than the ECDLP. The second approach is called the Xedni Calculus which turns the Index Calculus on its head. In order to apply the Xedni Calculus to the ECDLP, one lifts r points in $E(\mathbb{F}_p)$ constructed arbitrarily from P_p and Q_p, $2 \leq r \leq 9$, to points in $\mathbb{P}^2(\mathbb{Q})$, then chooses an elliptic curve E over $\mathbb{Q}$ passing through them and reducing to E_p mod p, which is an easy linear algebra problem, see [9]. If the rank of the lifted elliptic curve E is smaller than r, then one

Mathematics Subject Classification: 14G50, 94A60

can find a dependence relation between the lifted points, hence a dependence relation between P_p, Q_p. Unfortunately, the lifted elliptic curve E turns out to be of higher rank than r. Silverman's idea was to impose auxiliary conditions modulo many small primes to increase the likelihood that the lifted elliptic curve is of smaller rank than r. Yet, it was shown in [4] that the Xedni Calculus is virtually certain to fail as the probability of dependence of the lifted points still seems certainly very low.

There is no known algorithm to find the rank of an elliptic curve over $\mathbb{Q}$. Indeed, we do not know if such an algorithm exists. For a given set of rational points on an elliptic curve E, there are many methods to check if these points are linearly dependent. These methods include heights on elliptic curves, and a two descent algorithm. In [1], the authors showed that linear dependence of rational points on certain abelian varieties over a given number field K is a Hasse property. Namely, some rational points on such an abelian variety satisfy a dependence relation over K if and only if they satisfy dependence relations when reduced modulo all but finitely many primes of K. In fact, they even proved a stronger version of the latter result. More precisely, a dependence relation of rational points holds on these abelian varieties if and only if these points satisfy dependence relations modulo finitely many primes.

In this note, we analyse the aforementioned result in order to write the steps of an algorithm attacking the ECDLP. Given an elliptic curve $E_p/\mathbb{F}_p$ and two points $P_p, Q_p \in E_p(\mathbb{F}_p)$, we construct a finite set S of primes. For the construction of the set S we assume the Generalized Riemann Hypothesis and Szpiro's conjecture. One chooses an elliptic curve $E_q/\mathbb{F}_q$, and two points $P_q, Q_q \in E_q(\mathbb{F}_q)$ for every $q \in S$. Then one finds points $P, Q \in \mathbb{P}^2(\mathbb{Q})$ reducing to P_q, Q_q mod q, and to P_p, Q_p mod p. Afterwards, one selects an elliptic curve passing through P, Q and reducing to E_q mod q, and to E_p mod p. One hopes that linear dependence relations modulo any prime in the set S will force the linear dependence of P, Q in $E(\mathbb{Q})$. In other words, the algorithm enforces the lifted points to be linearly dependent on the chosen elliptic curve by imposing dependence relations modulo several primes.

During the course of constructing S, the Generalized Riemann Hypothesis and Szpiro's conjecture are assumed to bound the primes in S using the expected rank of the lifted elliptic curve r_E, and the expected Szpiro's ratio σ_E. We can use the maximum known rank and Szpiro's ratio to bound these primes, more precisely, $r_E \leq 28$ and $\sigma_E \leq 9.02$. Therefore, the failure of the algorithm might lead to an elliptic curve of larger rank than 28, or higher Szpiro's ratio than 9.2. However, over a prime field $\mathbb{F}_p$ where p is a large prime, the numerical bounds used to define the set S are rather large and beyond our computational power. Therefore, in such case we make S the largest possible set of primes that we can deal with computationally .

2 Detecting dependence relations

In this section we will review the material needed to pursue with our lifting algorithm.

Let E be an elliptic curve defined over a field $\mathbb{Q}$. Thanks to Mordell, one knows that the abelian group of rational points $E(\mathbb{Q})$ of E is finitely generated, hence, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tor}} \times \mathbb{Z}^r$ where $E(\mathbb{Q})_{\mathrm{tor}}$ is the torsion subgroup of $E(\mathbb{Q})$, and r is the rank of the elliptic curve E. Mazur gave a complete classification of the torsion subgroup $E(\mathbb{Q})_{\mathrm{tor}}$ of $E(\mathbb{Q})$, see (Theorem 7.5, §8, Chapter VIII, [7]). More precisely, $E(\mathbb{Q})_{\mathrm{tor}}$ is isomorphic to one of the following fifteen groups:

$$\mathbb{Z}/n\mathbb{Z},\ 1 \le n \le 12,\ n \ne 11;\ \text{or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ 1 \le n \le 4.$$

No such classifying results are known for the rank of elliptic curves. A widely believed conjecture is that the rank is unbounded, more precisely, that elliptic curves of any rank can be found. However the largest rank existing in the literature is bounded below by 28. There is no know algorithm to find a basis for $E(\mathbb{Q})$ for all elliptic curves E.

A Hasse principle for dependence of rational points on an abelian variety of certain type defined over a number field can be found in [1] and the references there. The following theorem is the statement of this local-to-global principle for elliptic curves over $\mathbb{Q}$. Throughout this note, if $P \in \mathbb{P}^2(\mathbb{Q})$, we write P_p for the reduction of P in $\mathbb{P}^2(\mathbb{F}_p)$.

Theorem 2.1. *Let E be an elliptic curve defined over $\mathbb{Q}$. Let $P \in E(\mathbb{Q})$ and let Γ be a subgroup of $E(\mathbb{Q})$. If $P_p \in (\Gamma \bmod p)$ for almost all integer primes p then $P \in \Gamma + E(\mathbb{Q})_{\mathrm{tor}}$. Moreover, if $E(\mathbb{Q})_{\mathrm{tor}} \subset \Gamma$, then the following conditions are equivalent:*

(1) $P \in \Gamma$.
(2) $P_p \in (\Gamma \bmod p)$ for almost all primes p.

The following is a stronger version of the Hasse principle stated above, Theorem 7.7 in [1].

Theorem 2.2. *Let E be an elliptic curve defined over $\mathbb{Q}$. Let $P \in E(\mathbb{Q})$ and let Γ be a subgroup of $E(\mathbb{Q})$. There is a finite set S of prime integers depending on E, P, Γ, and the choice of a basis for $E(\mathbb{Q})$ such that: if $P_p \in \Gamma \bmod p$ for all $p \in S$ then $P \in \Gamma + E(\mathbb{Q})_{\mathrm{tor}}$. Hence if $E(\mathbb{Q})_{\mathrm{tor}} \subset \Gamma$, then the following conditions are equivalent:*

(1) $P \in \Gamma$.
(2) $P_p \in (\Gamma \bmod p)$ for all $p \in S$.

In what follows we define the finite set S. Let $P_1, \ldots, P_s$ be a basis for $E(\mathbb{Q})$. Since Γ is a subgroup of $E(\mathbb{Q})$, it follows that

$$\Gamma = \mathbb{Z}d_1P_1 + \ldots + \mathbb{Z}d_rP_r + \ldots + \mathbb{Z}d_sP_s$$

where $d_i \in \mathbb{Z} \setminus \{0\}$ if $1 \le i \le r$ and $d_i = 0$ if $i > r$. The point $P \in E(\mathbb{Q})$ can be written as a linear combination of the P_i's, namely,

$$P = \sum_{i=1}^{s} n_i P_i, \ n_i \in \mathbb{Z}.$$

Recall that the height pairing on E is

$$\begin{aligned} \langle\ ,\ \rangle &: E \times E \to \mathbb{R} \\ \langle P, Q\rangle &= \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q) \end{aligned}$$

where $\hat{h} : E \to \mathbb{R}$ is the canonical height on E, see (§9, VIII, [7]). Using the bilinearity of the height pairing, one obtains the following equality

$$\langle P, P\rangle = \sum_{i,j} n_i n_j \langle P_i, P_j\rangle.$$

In addition, since the height pairing is positive definite, there is a constant C depending on the basis of $E(\mathbb{Q})$ and the point P such that $|n_i| \le C$ for each $1 \le i \le s$. That the coefficients n_i are bounded absolutely will be used to describe the set S.

For each i, one considers for each prime divisor l of n_i the Kummer extension $L_{i,l} = \mathbb{Q}\left(E[l^{n_i+1}], \frac{1}{l^{n_i}}E(\mathbb{Q})\right)$ where $E[k]$ is the subgroup of k-torsion points and $\dfrac{1}{k}E(\mathbb{Q})$ is the subgroup of k-divisible points in $E(\mathbb{Q})$, i.e., the group of points $Q \in E$ such that $kQ \in E(\mathbb{Q})$. By the above estimation, there is only a finite number of primes l. In [1], the authors used an effective version of Chebotarev's theorem by Lagarias and Odlyzko. Namely, there are effectively computable constants b_1 and b_2 such that every element $\sigma \in \mathrm{Gal}(L_{i,l}/\mathbb{Q})$ is equal to the Frobenius element $\mathrm{Frob}_q \in \mathrm{Gal}(L_{i,l}/\mathbb{Q})$ for an integer prime q such that $q \le b_1 d_{L_{i,l}}^{b_2}$ where $d_{L_{i,l}}$ is the discriminant of $L_{i,l}$.

For each i such that $n_i \neq 0$, we define the following sets

$$\begin{aligned} S_{i,l} &:= \{q : q \le b_1 d_{L_{i,l}}^{b_2} \text{ and } q \text{ is a good prime for } E\}, \\ S_i &:= \bigcup_{l \mid n_i} S_{i,l}. \end{aligned}$$

The set S is defined by

$$S := \bigcup_{1 \le i \le s, n_i \neq 0} S_i.$$

The bounds established by Lagarias and Odlyzko are large. Assuming the Generalized Riemann Hypothesis, GRH, improves these bounds substantially. In what follows, we assume the GRH to modify the bounds existing in the definition of the set S. In particular, the set of primes in S can be bounded using the degree of the extension $L_{i,l}/\mathbb{Q}$ instead of the discriminant $d_{L_{i,l}}$. In the following lemma, we collect different effective versions of Chebotarev's Density Theorem. The Lemma can be found as Theorem 2.2 and Proposition 2.3 in [5].

Lemma 2.3. *Let $L/\mathbb{Q}$ be a finite Galois extension, d_L the absolute value of the discriminant of L. We denote the discriminant and the degree of $L/\mathbb{Q}$ by d_L and n_L respectively. Let C be a conjugacy class of* $\mathrm{Gal}(L/\mathbb{Q})$. *There is an integer prime p such that the Frobenius at p is in C, and such that p satisfies the following bounds.*

a) There is an absolute effectively computable constant A such that $p \leq 2d_L^A$.

Now we assume the GRH.

b) There is an absolute effectively computable constant b such that $p \leq b(\log d_L)^2$. In fact, one may take $b = 70$.

c) If S is a set of prime numbers such that $L/\mathbb{Q}$ is unramified outside of S. For the conjugacy class C in $\mathrm{Gal}(L/\mathbb{Q})$, *there exists a prime number $p \notin S$ such that the Frobenius at p is in C, and such that*

$$p \leq 280 n_L^2 \left(\log n_L + \sum_{q \in S} \log q \right)^2 .$$

The following Lemma will be used to estimate the degree of the Kummer extension used in the definition of S.

Lemma 2.4. *Let $E/\mathbb{Q}$ be an elliptic curve of rank r. Let l be an integer prime and m a positive integer. The field $\mathbb{Q}\left(E[l^{m+1}], \frac{1}{l^m}E(\mathbb{Q})\right)$ is denoted by L. Then $[L:\mathbb{Q}] \leq l^{2(m+1)r}(l^{2(m+1)}-1)(l^{2(m+1)}-l^{m+1})$.*

Proof: The Galois group of the field extension $\mathbb{Q}\left(E[l^{m+1}], \frac{1}{l^{m+1}}E(\mathbb{Q})\right)/\mathbb{Q}(E[l^{m+1}])$ can be viewed as a subgroup of the product $\left(E[l^{m+1}]\right)^r$. Therefore, the degree of the extension is at most $l^{2(m+1)r}$. Now it is known that $\mathrm{Gal}\left(\mathbb{Q}(E[l^{m+1}])/\mathbb{Q}\right) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/l^{m+1}\mathbb{Z})$, where the latter group is of order $(l^{2(m+1)}-1)(l^{2(m+1)}-l^{m+1})$, hence follows the upper bound for $[L:\mathbb{Q}]$. □

The field L in Lemma 2.4 is unramified outside the set of bad primes of E and the prime l, see Proposition 1.5 in (§1, Chapter VIII, [7]).

3 Setup

Recall that for $Q \in \mathbb{P}^2(\mathbb{Q})$ and a prime q, we write Q_q for the reduction of Q mod q.

Let $E/\mathbb{Q}$ be an elliptic curve of rank r with basis $\{P_1, \ldots, P_r\}$. If $Q \in E(\mathbb{Q})$, then we can write $Q = m_1P_1 + \ldots + m_rP_r$. There exists $Q' \in E(\mathbb{Q})$ such that $Q_p = Q'_p$ and $Q' = m'_1P_1 + \ldots + m'_rP_r$ where $0 \leq m'_i \leq p-1$. The latter statement can be obtained by setting m'_i to be the representative of the class containing m_i in the least residue system modulo p. Therefore, throughout this note if E, Q are lifts of $E_p/\mathbb{F}_p, Q_p \in E_p(\mathbb{F}_p)$, we will assume without loss of generality that $Q = m_1P_1 + \ldots + m_rP_r$ where $0 \leq m_i \leq p-1$.

Again, let E_p be an elliptic curve over $\mathbb{F}_p$ and $E/\mathbb{Q}$ a lift of E_p. We will assume that $\#E_p(\mathbb{F}_p) \geq 17$ is prime. Since the torsion subgroup $E_{\text{tor}}(\mathbb{Q})$ injects into $E_p(\mathbb{F}_p)$, it follows from Mazur's classification of torsion subgroups of elliptic curves over $\mathbb{Q}$ that $E_{\text{tor}}(\mathbb{Q}) = \{O\}$. Therefore, all rational points in $E(\mathbb{Q})$ are of infinite order.

In view of Theorem 2.2, if E is an elliptic curve over $\mathbb{Q}$, then $Q \in \Gamma = \langle P \rangle$, i.e., $Q = mP$ for some $m \in \mathbb{Z}$, if and only if $Q_q = m_qP_q$ for every prime q in some finite set S. The set S is defined as follows: For every prime $l \mid m$, define the following set of primes

$$S_l := \left\{ q : q \leq 280n^2 \left(\log n + \sum_{q=l \text{ or } q|\Delta_E} \log q \right)^2 \text{ and } q \text{ is a good prime for } E \right\},$$

where $n \leq l^{2(m+1)r}(l^{2(m+1)} - 1)(l^{2(m+1)} - l^{m+1})$, r is the rank of E, see Lemma 2.4. For the justification of the bound used to define S_l see Theorem 2.2 and Lemma 2.3 (c). Recall that the Generalized Riemann Hypothesis is assumed throughout. Now,

$$S := \bigcup_{l|m} S_l.$$

The difficulty in using Theorem 2.2 to attack the ECDLP lies in the fact that we are given E_p, P_p, Q_p, and E, P, Q are to be created. Thus we need to construct S without being given the lift E. In order to tackle this difficulty, we will make use of the following widely believed conjectures.

Conjecture 3.1 (Lang). *There is an absolute constant $C > 0$ such that for all elliptic curves $E/\mathbb{Q}$ and every infinite point $Q \in E(\mathbb{Q})$*

$$\hat{h}(Q) \geq C\Delta_E.$$

We set $\sigma_E := \dfrac{\log |\Delta_E|}{\log N_E}$ where N_E is the conductor of E. The following theorem was proved in [3]

Theorem 3.2. *For every elliptic curve $E/\mathbb{Q}$ and every infinite point $Q \in E(\mathbb{Q})$,*

$$\log(\Delta_E) \leq (20\sigma_E)^8 \times 10^{1.1+4\sigma_E} \times \hat{h}(Q).$$

It is known that there are only finitely many elliptic curves $E/\mathbb{Q}$ with integral j-invariants such that $\sigma_E \geq 6$. Therefore, Lang's conjecture is proved for this family of elliptic curves. For other elliptic curves, one may assume Szpiro's conjecture to deduce similar results.

Conjecture 3.3 (Szpiro)**.** *For every $\epsilon > 0$, there are only finitely many elliptic curves satisfying $\sigma_E \geq 6 + \epsilon$.*

This implies that σ_E is absolutely bounded as E ranges over all elliptic curves over $\mathbb{Q}$. The record for the largest σ_E is 9.01996..., see for example [2].

We are in a place to modify the set S_l according to the following inequalities:

$$\sum_{q=l \text{ or } q|\Delta_E} \log q \leq \log l + \log \Delta_E \leq \log l + (20\sigma_E)^8 \times 10^{1.1+4\sigma_E} \times \hat{h}(Q),$$

for any infinite point $Q \in E(\mathbb{Q})$. Assuming Lang's conjecture, the set S_l is defined as follows:

$$S_l := \left\{ q : q \leq 280n^2 \left(\log(nl) + (20\sigma_E)^8 \times 10^{1.1+4\sigma_E} \times \hat{h}(Q) \right)^2 \text{ and } q \text{ is a good prime for } E \right\} \quad (1)$$

where Q is an infinite point in $E(\mathbb{Q})$, $n = l^{2(m+1)r}(l^{2(m+1)} - 1)(l^{2(m+1)} - l^{m+1})$, r is the rank of E. Moreover, following the largest known records for σ_E and r, we may assume that $\sigma_E \leq 9.02$ and $r \leq 28$.

4 Remarks on the set S

Let E_p be an elliptic curve defined over the prime field $\mathbb{F}_p$, $p \geq 5$. Let $P_p \in E_p(\mathbb{F}_p)$. In addition, $\#E_p(\mathbb{F}_p) \geq 17$ is prime.

For $P \in \mathbb{P}^2(\mathbb{Q})$, let $h(P) = h(x(P))$, where $h(P)$ and $h(x(P))$ are the absolute logarithmic heights of P and $x(P)$ respectively. Namely, $h(a/b) = \log \max\{|a|, |b|\}$ with a/b in lowest terms. Set $h = h(P)$ where P is the point P_p viewed as a point in $\mathbb{P}^2(\mathbb{Q})$.

Recall that if $E/\mathbb{Q}$ is a lift of $E_p/\mathbb{F}_p$ with rank r whose basis is $P_1, \ldots, P_r$ such that $Q \in E(\mathbb{Q})$, then we can assume without loss of generality that $Q = m_1P_1 + \ldots + m_rP_r$, where $0 \leq m_i \leq p-1$. For every prime divisor l of any of the m_i's, one has $l \leq \sqrt{p-1}$. Moreover, we can define for any such prime l the following set of primes given in (1):

$$S_{l,i} := \left\{ q : q \leq 280n_i^2 \left(\log(n_i l) + (20\sigma_E)^8 \times 10^{1.1+4\sigma_E} \times \hat{h}(P) \right)^2 \text{ and } q \text{ is a good prime for } E \right\}$$

where $n_i = l^{2(m_i+1)r}(l^{2(m_i+1)} - 1)(l^{2(m_i+1)} - l^{m_i+1})$.

It is well known that given an elliptic curve, there exists two constants c_1, c_2 such that $c_1 \leq \hat{h}(P) - h(P) \leq c_2$ for any non-torsion point $P \in E(\mathbb{Q})$. Indeed, the difference between the logarithmic height and the canonical height is relatively small, see for example [8]. Therefore, we can use the logarithmic height $h = h(P)$ of $P \in \mathbb{P}^2(\mathbb{Q})$ as an approximation for the canonical height of P viewed as a point in $E(\mathbb{Q})$ in the definition of $S_{l,i}$.

Furthermore, we can use the bounds 28 and 9.02 for r and σ_E respectively, as these are the largest known bounds in literature. Thus, we have the following set:

$$S'_l = \left\{ q : q \leq 280n^2 \left(\log(nl) + 180.4^8 \times 10^{37.18} \times h\right)^2 \text{ where } n = l^{56p}(l^{2p} - 1)(l^{2p} - l^p) \right\}. \quad (2)$$

Now, we define the set S as:

$$S = \bigcup_{l \leq \sqrt{p-1}} S'_l.$$

The set S is beyond our computational reach. In fact, the largest prime up to the knowledge of the author is the Mersenne prime $2^{57885161} - 1$. Therefore, if p is a large prime, then the set S is not effectively computable. In our algorithm, we will use the largest possible set of primes when the prime p is rather huge, in order to put Theorem 2.2 into practice.

5 Description of the algorithm

In this section, we introduce the steps of our proposed algorithm.

Input. A prime $p \geq 5$, an elliptic curve E_p defined over the prime field $\mathbb{F}_p$, and two points $P_p, Q_p \in E_p(\mathbb{F}_p)$ such that $Q_p = m_p P_p$ for some $m_p \in \mathbb{F}_p^{\times}$. In addition, $\#E_p(\mathbb{F}_p) \geq 17$ is prime.

Output. An elliptic curve E over $\mathbb{Q}$, two points $P, Q \in E(\mathbb{Q})$, a positive integer m, $1 \leq m \leq p-1$, such that E_p is the reduction of E mod p, and P, Q are reduced to P_p, Q_p mod p such that $Q = mP$.

Let E_p be an elliptic curve defined over the prime field $\mathbb{F}_p$, $p \geq 5$. There exists two integers a_p, b_p, where $0 \leq a_p, b_p \leq p-1$, such that the elliptic curve E_p is described by the following Weierstrass equation:

$$y^2 = x^3 + a_p x + b_p.$$

Since $\#E_p(\mathbb{F}_p) \geq 17$ is prime, it follows that any lift $E/\mathbb{Q}$ of $E_p/\mathbb{F}_p$ has no nontrivial rational torsion points.

Step 1. We set P to be the point P_p considered a point in $\mathbb{P}^2(\mathbb{Q})$.

Step 2. Let $S := \bigcup_{l \leq \sqrt{p-1}} S_l'$, where S_l' is defined in (2), if S_l' is effectively computable. Otherwise, we define S to be the set of primes less than or equal to $2^{57885161}-1$. Let $L = \prod_{l \in S} l$. In fact, because L might be an integer that we can not deal with using our computational powers, we may set L to be the product of all prime integers less than a rather convenient large bound. In fact, we can exclude some small primes from S, consequently, the lifted elliptic curve might have bad reduction at those primes.

Step 3. In this step, we construct an elliptic curve $E_l/\mathbb{F}_l$ and two points $P_l, Q_l \in E_l(\mathbb{F}_l)$ for every $l \in S$. If P is the point P_p viewed as a point in $\mathbb{P}^2(\mathbb{Q})$, we set the point P_l to be the reduction of P modulo l. Let E_l be an elliptic curve passing through P_l, and $Q_l \in E_l(\mathbb{F}_l) = m_l P_l$ for some $m_l \in \mathbb{F}_l^\times$.

Remark 5.1. An alternative approach is to consider an elliptic curve $E/\mathbb{Q}$ of positive rank passing through P and we let $Q = m'P$ for some positive integer m'. The elliptic curve E, and the points P, Q are reduced mod l to E_l, P_l, Q_l for every $l \in S$.

Step 4. In this step, we will lift the points P_p, Q_p to points in $\mathbb{P}^2(\mathbb{Q})$. Recall that the point P, this is P_p considered a point in $\mathbb{P}^2(\mathbb{Q})$, is a lift of $P_p \in E_p(\mathbb{F}_p)$ and it is a lift of $P_l \in E_l(\mathbb{F}_l)$ for every $l \in S$. Lift the points Q_p and Q_l to a point Q in the projective plane $\mathbb{P}^2(\mathbb{Q})$, more precisely, the reduction of Q mod p is Q_p, and the reduction mod l is Q_l. This can be performed by the Chinese Remainder Theorem.

Step 5. If E_p and E_l are defined by:

$$\begin{aligned} E_p &: y^2 = x^3 + a_p x + b_p; \\ E_l &: y^2 = x^3 + a_l x + b_l, \end{aligned}$$

we find coefficients a, b mod pL, where $L = \prod_{l \in S} l$, that reduce to a_p, b_p mod p, and to a_l, b_l mod l for every $l \in S$.

Step 6. Consider the equation

$$(1 + u_1 pL)y^2 = x^3 + (a + u_2 pL)x^2 + b + u_3 pL.$$

We find integer coefficients u_1, u_2, u_3 such that the points P, Q are rational points on the elliptic curve E defined by the above equation.

6 Remarks on the elliptic curve E

1) The elliptic curve $E/\mathbb{Q}$ reduces to E_p modulo p, and to E_l modulo l. The points $P, Q \in E(\mathbb{Q})$ reduce modulo p to P_p, Q_p respectively. Moreover, they reduce to the points P_l, Q_l modulo l for every $l \in S$.
2) The elliptic curve $E/\mathbb{Q}$ has no nontrivial rational torsion points. The reason is that $\#E_p(\mathbb{F}_p) \geq 17$ is prime, therefore, the only torsion subgroup that can inject into $E_p(\mathbb{F}_p)$ is the trivial one, see Mazur's classification of torsion subgroups of an elliptic curve over $\mathbb{Q}$. It follows that the points P, Q are infinite points in $E(\mathbb{Q})$.
3) The set S is defined based on the fact that the extension $\mathbb{Q}\left(E[m], \frac{1}{m}E(\mathbb{Q})\right)$ is a finite extension of $\mathbb{Q}$. That the latter field extension is finite lies in the heart of the proof of the weak Mordell-Weil theorem, namely, that $E(\mathbb{Q})/mE(\mathbb{Q})$ is finite.
4) The point $P \in E(\mathbb{Q})$ is an infinite point, hence we can complete the set $\{P\}$ to a basis $\{P_1 := P, P_2, \ldots, P_r\}$ of $E(\mathbb{Q})$. Now the point $Q = n_1P_1 + \ldots + n_rP_r$. We can assume without loss of generality that $0 \leq n_i \leq p-1$ for every i. For every prime $l \leq \sqrt{p-1}$, these include any prime dividing n_i for every i, we construct the set S_l'. The union of those sets is the finite set S. We assumed Szpiro's conjecture to show that a prime in S is bounded by a constant depending on the logarithmic height of P as a point in $\mathbb{P}^2(\mathbb{Q})$, which is an acceptable approximation for the canonical height of P as a point in $E(\mathbb{Q})$. Moreover, this bound depends on Szpiro's ratio and the rank of the elliptic curve. We impose the biggest known values for the rank and the Szpiro's ratio. If the lifted curve E has rank at most 28 and Szpiro's ratio less than 9.02, then we are expecting our algorithm to work. This is because the set S is a very good approximation for the finite set in Theorem 2.2. Therefore, we may predict that $Q = mP$ for some $m, 1 \leq m \leq p-1$, i.e., $Q \in \Gamma = \langle P \rangle$ because for every $q \in S$ one has $Q_q \in \Gamma \bmod q$.
5) Since E is a lifted elliptic curve passing through the points P, Q, it is expected that the rank of E is at least 2, see [4], otherwise the Xedni Calculus method will resolve the ECDLP.
6) The last step is to find m in the dependence relation $Q = mP$. This can be done using either the height method or the 2-descent method, see [9].

References

[1] G. Banaszak and P. Krasoń. On arithmetic in Mordell-Weil groups. *Acta Arithmetica*, 150(4):315–337, 2011.

[2] M. Bennett and S. Yazdani. A local version of Szpiro's conjecture. *Experiment. Math*, 21(2):103–116, 2012.

[3] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Inventiones Mathematicae*, 93:419–450, 1988.

[4] Michael J. Jacobson, Neal Koblitz, Joseph H. Silverman, Andreas Stein, and Edlyn Teske. Analysis of the Xedni calculus attack. *Design, Codes and Cryptography*, 20:41–64, 1999.

[5] S. Lichtenstein. The effective Chebotarev density theorem and modular forms mod $\mathfrak{m}$. *Proc. Amer. Math Soc.*, 136(10):3419–3428, 2008.

[6] A. Menezes, T. Okamoto, and S. Vanstone. Reducing elliptic curve logarihms to a finite field. *IEEE Trans. Inform. Theory*, 39:1639–1646, 1993.

[7] J. Silverman. *The arithmetic of elliptic curves.* GTM 106. Springer-Verlag, New York, 1986.

[8] J. H. Silverman. The difference between the Weil height and the canonical height on elliptic curves. *Math. Comp.*, 55(192):723–743, 1990.

[9] Joseph H. Silverman. The Xedni calculus and the elliptic curve discrete logarithm problem. *Designs, Codes and Cryptography*, 20:5–40, 1999.

[10] N. P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12:193–196, 1999.

Department of Mathematics and Actuarial Science
American University in Cairo
mmsadek@aucegypt.edu