Lifting and Elliptic Curve Discrete Logarithms

Joseph H. Silverman*

Mathematics Department, Brown University, Providence, RI 02912 USA
jhs@math.brown.edu

Abstract. The difficulty of the elliptic curve discrete logarithm problem (ECDLP) underlies the attractiveness of elliptic curves for use in cryptography. The index calculus is a lifting algorithm that solves the classical finite field discrete logarithm problem in subexponential time, but no such algorithm is known in general for elliptic curves. It turns out that there are four distinct lifting scenarios that one can use in attempting to solve the ECDLP; the lifting field may be a local field or a global field, and the lifted points may be torsion points or nontorsion points. These choices lead to four quite different ways to try to solve the ECDLP via lifting. None of these approaches has led to a solution to the ECDLP, but each method has its own reasons for failing to work. In this article I survey the four ways of lifting the ECDLP, explain their similarities and their differences, and describe the distinct roadblocks that arise in each case.

Introduction

The *elliptic curve discrete logarithm problem* (ECDLP) has attracted considerable attention since Neal Koblitz [14] and Victor Miller [20] independently proposed its use as the basis for crytography. To date, the best general algorithms for ECDLP are no better than the square root algorithms which are known to be best possible for the discrete logarithm problem in a generic group. This is in marked contrast to the discrete logarithm problem in the multiplicative group of a finite field, for which subexponential algorithms are known.

A number of writers have considered the possibility of solving the ECDLP by lifting to either a p-adic (complete local) field such as $\mathbb{Q}_p$ or to a global field such as $\mathbb{Q}$, see for example [4,5,12,13,26,27,34,35,36]. In this paper we consider the general question of lifting as it relates to the ECDLP. In particular, we observe that there are four, quite distinct, lifting scenarios, depending on whether the lifting field is local or global and whether the lifted point is torsion or nontorsion. This leads to four surprisingly different ways to try to solve ECDLP via lifting. (Actually, five different methods, because the global/nontorsion approach comes in two different flavors.) As we will see, none of these approaches has led to a solution to ECDLP, but as we will also see, the reasons for their failures are quite varied.

* Research supported by NSA H98230-04-1-0064 and NSF DMS-0650017. This article is an expanded version of talks presented at ECC 2007 and SAC 2008.

R. Avanzi, L. Keliher, and F. Sica (Eds.): SAC 2008, LNCS 5381, pp. 82–102, 2009.

Disclaimer. This article is a survey that draws together a number of threads and attempts to present them in a unified and coherent manner. I have endeavored to give credit as appropriate and I apologize to anyone who may feel slighted. Uncredited results are mostly elementary, well-known to experts in the field, and have undoubtedly been discovered and rediscovered by numerous researchers over the past couple of decades, although many have not previously been published.

1 ECDLP and Lifting Problems

In this section we state the ECDLP and various sorts of lifting problems and briefly indicate how each lifting problem might be used to solve ECDLP and why each turns out not to give a practical algorithm. The remainder of this article gives further details and works out several numerical examples that illustrate what is realistically computable and what is not. For ease of exposition, these examples are done with small numbers (e.g., we often consider the ECDLP over $\mathbb{F}_{257}$), but except as noted, all computations that we perform over $\mathbb{F}_{257}$ can be done for cryptographically useful finite fields containing between 2^{130} and 2^{400} elements.

We do not review the basic theory of elliptic curves or elliptic curve cryptography. The reader will find this material amply covered in [2,6,11,21,25,37] and in numerous other books and articles.

We generally let k denote a finite field and K a local or global field to which we lift. Continuing this convention, we use lower case letters to denote quantities defined over the finite field k and the corresponding upper case letters to denote the lifted quantities defined over the local or global field K.

We now state the two problems whose interconnections lie at the heart of our investigation.

Definition 1. *Let e be an elliptic curve defined over a finite field k and let s and t be points in $e(k)$. Assuming that t is in the group generated by s, the* Elliptic Curve Discrete Logarithm Problem (ECDLP) *is the problem of finding an integer m such that $t = ms$.*

Definition 2. *Let e/k be an elliptic curve and let $s_1, \ldots, s_r \in e(k)$. The* Lifting Problem for $(k, e, s_1, \ldots, s_r)$ *is the problem of finding the following quantities*:

- *a field K with subring R.*
- *a maximal ideal $\mathfrak{p}$ of R satisfying $R/\mathfrak{p} \cong k$.*
- *an elliptic curve E/K satisfying $E \bmod \mathfrak{p} \cong e$.*
- *points $S_1, \ldots, S_r \in E(K)$ satisfying $S_i \bmod \mathfrak{p} = s_i$ for $1 \le i \le r$.*

Remark 1. There are many variants of the lifting problem, including:

A. Given e/k, find a lift E/K of e/k and an algorithm that is able to (efficiently) lift some sizable collection of the points in $e(k)$ to points in $E(K)$.

Table 1. ECDLP Options for Lifting Points

	Lift to Torsion Point	**Lift to Nontorsion Point**
p-adic	• preserves unique relation • computationally feasible • cannot move to formal group	• does not preserve relation • can move to formal group • easy to compute
Global	• preserves unique relation • computationally infeasible • can move to complex numbers	• can find $E(K) \twoheadrightarrow E(k)$, hard to lift • can lift (up to 9) points, hard to make them dependent

B. Lifting $(k, e, s_1, \ldots, s_r)$ with the added restriction that $E(K)$ is a finitely generated group of rank strictly less than r.
C. Lifting $(k, e, s_1, \ldots, s_r)$ with the added restriction that the lifted points $S_1, \ldots, S_r$ are torsion points.

Roughly speaking, we can divide the lifting problem into four cases, depending on whether the field K is local or global and depending on whether the lifted point(s) are torsion or nontorsion. This separation into four cases may appear, at first glance, to be somewhat artificial, but as we shall see, each case offers a different path leading to a solution of ECDLP.

Thus suppose that we are given an ECDLP (k, e, s, t) whose solution is $t = ms$. It is very easy to find a lift (K, E, S, T) to a *local* field K with *torsion* points S and T that satisfy the same relation $T = mS$, but this does not seem to help in finding m. On the other hand, if we could instead lift to *torsion* points in a *global* field, then we could solve ECDLP using Diophantine approximation. Unfortunately (or fortunately, depending on your point of view), it does not seem to be feasible to lift to torsion points in a global field because the degree of the field will necessarily be very large.

It is also quite easy to lift to *nontorsion* points S and T in a *local* field. The problem with this scenario is that there are many different lifts and it appears to be hard to lift while preserving the relation $T = mS$. If we could find a relation-preserving lift to nontorsion points, then it would be easy to solve ECDLP by moving to the formal group. (More precisely, let n be the order of the point $s \in e(k)$ and rewrite the relation as $nT = mnS$, then nS and nT are in the formal group, so it is easy to find m using the formal logarithm.) Finally, there are two approaches to lifting to *nontorsion* points over a *global* field K. First, we can easily find E/K with a lift of s to $S \in E(K)$. If we could also find $T \in E(K)$ satisfying $T = mS$, then we could use height functions or descent theory to recover m and solve ECDLP. But it appears to be very difficult to find T. Second, we can easily find a lift of (k, e, s, t) to (K, E, S, T), but then it will almost always be true that S and T are independent points in $E(K)$, so they do not satisfy the relation $T = mS$ and cannot be used to solve ECDLP.

The preceding discussion is summarized in Table 1. The remainder of this article is devoted to expanding on these preliminary remarks.

2 Lifting to a p-adic Nontorsion Point

Let e/k be an elliptic curve defined over a finite field k and let $s \in e(k)$. Let K be a complete local field with ring of integers R, maximal ideal $\mathfrak{p}$, and residue field $R/\mathfrak{p} = k$. The reduction map $E(K) \to e(k)$ is surjective [30, VII.2.1] , and indeed there is an exact sequence

$$0 \longrightarrow E_1(K) \longrightarrow E(K) \longrightarrow e(k) \longrightarrow 0. \tag{1}$$

Hensel's lemma provides an efficient method to calculate a lift of s to $E(K)$. (There are even more efficient methods, but Hensel's lemma suffices for our purposes.) Here is the basic idea.

Hensel's Lemma: Let e/k and E/K be elliptic curves given by Weierstrass equations

$$\begin{aligned} e : f(x,y) &= y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0, \\ E : F(X,Y) &= Y^2 + A_1XY + A_3Y - X^3 - A_2X^2 - A_4X - A_6 = 0, \end{aligned}$$

with $E \bmod \mathfrak{p} = e$, and let $s = (x_1, y_1) \in e(k)$ be a point to be lifted. Also let π be a generator of the ideal $\mathfrak{p}$. Define a sequence of points (X_i, Y_i) satisfying

$$F(X_i, Y_i) \equiv 0 \pmod{\mathfrak{p}^i}, \qquad i = 1, 2, 3, \ldots, \tag{2}$$

as follows:

- Choose any $(X_1, Y_1) \in R^2$ satisfying $X_1 \bmod \mathfrak{p} = x_1$ and $Y_1 \bmod \mathfrak{p} = y_1$. Note that (X_1, Y_1) satisfies (2).
- Suppose that (X_i, Y_i) has been chosen and satisfies (2). Choose $u, v \in R$ satisfying

$$\frac{F(X_i, Y_i)}{\pi^i} + \frac{\partial F}{\partial X}(X_i, Y_i)u + \frac{\partial F}{\partial Y}(X_i, Y_i)v \equiv 0 \pmod{\mathfrak{p}} \tag{3}$$

  and set

$$X_{i+1} = X_i + \pi^i u \qquad \text{and} \qquad Y_{i+1} = Y_i + \pi^i v.$$

  The nonsingularity of e ensures that one of the partial derivatives is nonzero modulo $\mathfrak{p}$, so there will be *many* choices for $u, v \in R$.
- Repeat the previous step to construct a sequence of points (X_i, Y_i) that reduce modulo $\mathfrak{p}$ to s, that satisfy $F(X_i, Y_i) \equiv 0 \pmod{\mathfrak{p}^i}$, and that converge to a point $S \in E(K)$ lifting s.

Remark 2. Notice that the Hensel construction does not yield a particular lift S of s. Instead, at each step, it is necessary to choose values $u, v \in R$ satisfying (3). In practice, only the values of u and v modulo $\mathfrak{p}$ matter, and the value of v mod $\mathfrak{p}$ is determined by the value of u. Thus for each $S_i = (X_i, Y_i)$, there is one lift S_{i+1} for each value of u in $R/\mathfrak{p}$. In other words, the set of lifts of $s \in e(k)$ to $S \in E(K)$ is parameterized by R, with the lifts modulo $\mathfrak{p}^i$ being parametrized by $R/\mathfrak{p}^i$. In particular, if k is a large field, then even the set of lifts modulo $\mathfrak{p}^2$ is large.

Remark 3. Suppose that $t = ms$ and that we are searching for the value of m. As explained above, we can lift e, s, and t to a curve E/K and points $S, T \in E(K)$. Suppose that we manage to do this while maintaining the initial relation, i.e., $T = mS$. The kernel of the reduction-modulo-$\mathfrak{p}$ map, which we denote $E_1(K)$, is called the *formal group*, and there is an exact sequence

$$0 \longrightarrow E_1(K) \longrightarrow E(K) \xrightarrow{\text{red mod } \mathfrak{p}} e(k) \longrightarrow 0.$$

We know that $ns = nt = 0$, so nS and nT are in $E_1(K)$. The significance of this lies in the fact that the formal group comes equipped with an easily computable formal logarithm homomorphism

$$\log_E^f : E_1(K) \longrightarrow K^+.$$

(See [30, chapter IV] for information about formal groups and formal logarithms.)

We apply the formal logarithm to the relation $T = mS$. Since $\log_E^f$ is a homomorphism, we find that

$$\log_E^f(T) = m \log_E^f(S).$$

This allows us to solve for the discrete logarithm

$$m = \frac{\log_E^f(T)}{\log_E^f(S)},$$

unless we are unlucky and $\log_E^f(S) = 0$. Further, it is not hard to prove that for a given s, most lifts S satisfy $\log_E^f(S) \neq 0$.

So why does local-nontorsion lifting fail to solve the ECDLP? The answer lies in our requirement that the lifted points S and T satisfy $T = mS$. Assume for the moment that we have already lifted s to a point modulo $\mathfrak{p}^2$. Then among the many possible lifts of t modulo $\mathfrak{p}^2$, only one of them satisfies the relation $T \equiv mS \pmod{\mathfrak{p}^2}$. So the difficulty of using local-nontorsion lifts to solve the ECDLP is that there are too many lifts, and there is no way known[1] to consistantly lift two points so as to preserve the desired relation.

We illustrate with a small numerical example.

Example 1. We let $p = 257$ and consider the field $k = \mathbb{F}_{257}$ and the elliptic curve and point

$$e : y^2 = x^3 + 23x + 11, \qquad s = (7, 1) \in e(k).$$

It is easy to check that $\#e(k) = 249 = 3 \cdot 83$ and that s has order $n = 83$ in $e(k)$. We lift e to a p-adic curve E in the obvious way,

$$E : Y^2 = X^3 + 23X + 11.$$

We will lift s to a point $S \bmod p^2$.

[1] This is not strictly true; see Section 3 on local-torsion lifts. What we should say is that there is no way known to lift to nontorsion points satisfying $T = mS$.

We write S in the form

$$S = (7 + pu, 1 + pv) \bmod p^2.$$

In order for S to represent a point on E modulo p^2, we need

$$(1 + pv)^2 \equiv (7 + pu)^3 + 23(7 + pu) + 11 \pmod{p^2}.$$

Expanding this gives

$$1 + 2pv \equiv 515 + 170pu \pmod{p^2},$$

so we find that $v \equiv 85u + 1 \pmod{p}$. Thus S has the form

$$S = (7 + pu, 258 + 85pu) = (7 + 257u, 258 + 21845u) \pmod{257^2}. \quad (4)$$

This gives the complete set of lifts of s modulo p^2 with each value of $u \bmod p$ giving a distinct lift.

Now fix a particular mod 257^2 lift of s, say $S = (7, 258)$, and consider a second point $t = (150, 14) \in e(k)$. The ECDLP for (e, s, t) asks us for the integer $0 \le m < 83$ such that $t = ms$ in $e(k)$. (The solution turns out to be $m = 54$, but we will suppose we do not know the answer.) The lifts of t modulo 257^2 are given by the formula

$$T = (150 + pu, 61694 + 72pu) = (150 + 257u, 61694 + 18247u) \pmod{257^2}, \quad (5)$$

where we are free to choose any $u \bmod 257$. Unfortunately, for most choices of u we have $T \neq mS \pmod{257^2}$, so for most choices of u we lose the relation that we are seeking. For example, if we take the obvious lifts $S = (7, 258)$ and $T = (150, 61694)$, then

$$54S \equiv (24565, 25971) \not\equiv T \pmod{257^2}.$$

Indeed, for these lifts the smallest solution to $T \equiv mS \pmod{257^2}$ is $T = 11093S \pmod{257^2}$.

It turns out that the "correct" choice for u in (5) is $u = 95$. Then we get the point $T = (15570, 33681) \bmod 257^2$, and this point T does satisfy $T = 54S \pmod{257^2}$. Further, if we know the point $T = (15570, 33681)$, we can use the formal logarithm to compute as follows.

It turns out to be easier to do computations if we make the change of variables $Z = -X/Y$ and $W = -1/Y$. This brings the identity element to $(Z, W) = (0, 0)$, and the equation of our curve becomes $W = Z^3 + 23ZW^2 + 11W^3$. The formal logarithm for E starts $\log_E^f(Z) = Z + 23Z^7 + \cdots$, so since we are working modulo 257^2, it suffices to use $\log_E^f(Z) \approx Z$. We first compute (in (Z, W) coordinates)

$$83S = (24 \cdot 257 \bmod 257^2, 203 \cdot 257^3 \bmod 257^4),$$
$$83T = (11 \cdot 257 \bmod 257^2, 46 \cdot 257^3 \bmod 257^4).$$

Then

$$\frac{\log_E^f([83]T)}{\log_E^f([83]S)} = \frac{11 \cdot 257}{24 \cdot 257} \equiv 54 \pmod{257}$$

yields the discrete logarithm $m = 54$ that solves $t = ms$.

Of course, for $p = 257$ it was not hard to find the right value for u. But if $p = 257$ is replaced by a large prime, say $p \approx 2^{160}$, then there is no efficient algorithm known for selecting a "correct" value of u, i.e., a value of u for which $T = mS \pmod{p^2}$.

Remark 4. We have just said that there is no efficient way to lift modulo p^2 to points S and T while maintaining the relation $T = mS$, but this is not entirely true. There are actually two situations in which we can perform this lift . The first is when we lift to points S and T that have the same order modulo p^2 as s and t have modulo p. We discuss this situation in more detail in the next section, but we note here that this is the one case in which we cannot multiply S and T by n and still get useful information.

The other situation in which nontorsion local lifting does work and leads to an essentially linear-time solution to the ECDLP is the case that $n = \#E(\mathbb{F}_p) = p$. Elliptic curves with this property are called *anomalous*. In this case s and t have order p, but if we lift them to points S and T modulo p^2 such that S and T do not have order p, then it turns out that $[p]S$ and $[p]T$ automatically satisfy $T = [m]S \pmod{p^2}$. The reason is that if S' and T' are some other lifts, then $S - S'$ and $T - T'$ are in the formal group, so

$$[p](S - S') \equiv O \pmod{p^2} \qquad \text{and} \qquad [p](T - T') \equiv O \pmod{p^2}.$$

For details see [26,27,36]. Thus anomalous curves are not suitable for use in cryptography.

Remark 5. In Example 1 we considered the problem of lifting modulo p^2. For ease of exposition we restricted attention to p^2, but we note that it is easy to repeat the process and lift to higher powers of p. For example, if we take $u = 0$ in (4), then $S = (7, 258)$ and we can work modulo 257^3 to find the collection of lifts

$$S' = (7 + p^2u, 8454530 + 85p^2u) \pmod{257^3}.$$

Continuing in this way, we can lift s to any desired level 257^i as long as we can perform basic arithmetic with numbers of size 257^i. At each stage we have 257 choices for the next lift.

3 Lifting to a p-adic Torsion Point

Let e/k be an elliptic curve defined over a finite field k and let $s \in e(k)$. Let K be a complete local field with ring of integers R, maximal ideal $\mathfrak{p}$, and residue field $R/\mathfrak{p} = k$. The order n of the point s divides $\#e(k)$. In this section we consider the question of lifting s to a point $S \in E(K)$ that also has finite order n. We

have seen in Section 2 that there are many ways of lifting s to $E(K)$, so there are questions of both existence and uniqueness. Both are answered by the following well-known result.

Theorem 1. *Let e/k, E/K, and $s \in e(k)$ be as above, and assume that the order n of s is not divisible by the characteristic p of k. Then there exists a unique n-torsion point $S \in E(K)$ satisfying $S \bmod \mathfrak{p} = s$.*

Proof. We begin with uniqueness. Suppose that $S, S' \in E(K)$ are both n-torsion points that lift s. Then $T = S - S'$ is an n-torsion point that reduces of zero, and now our assumption that $p \nmid n$ implies that $T = O$; see [30, VII.3.1b]. Hence $S = S'$.

Let E be given by a minimal Weierstrass equation

$$E : F(X,Y) = y^2 + A_1xy + A_3y - x^3 - A_2x^2 - A_4x - A_6 = 0.$$

Thus $A_1, \ldots, A_6 \in R$ and the discriminant $\Delta \in R^*$, since by assumption the reduction $E \bmod \mathfrak{p} = e$ is nonsingular. The nth division polynomial of E is a polynomial

$$\psi_n(X) = n^2X^{(n^2-1)/2} + \cdots \in \mathbb{Z}[A_1, \ldots, A_6][X]$$

whose roots are the x-coordinates of the n-torsion points of E. (Strictly speaking, this is only true if n is odd, otherwise a polynomial of a slightly different form is required.) Further, the discriminant of $\psi_n(X)$ has the form $n^\alpha\Delta^\beta$, so in particular $\mathrm{Disc}(\psi_n) \in R^*$. (Another way to see this last fact is to use the earlier observation that the n-torsion of E injects under reduction, hence the roots of $\psi_n(X)$ remain distinct modulo $\mathfrak{p}'$ for every extension K' of K, hence its discriminant is relatively prime to $\mathfrak{p}$.)

We are given that $s = (x_0, y_0)$ is an n-torsion point in $e(k)$, so x_0 is a root of $\psi_n(X) \equiv 0 \pmod{\mathfrak{p}}$. Further, it is a simple root (i.e., $\psi_n'(x_0) \not\equiv 0 \pmod{\mathfrak{p}}$), so Hensel's lemma tells us that there is a (unique) $X_0 \in R$ satisfying

$$X_0 \equiv x_0 \pmod{\mathfrak{p}} \qquad \text{and} \qquad \psi_n(X_0) = 0.$$

Finally, we use the fact that $F(X_0, Y) \equiv 0 \pmod{\mathfrak{p}}$ has the root $Y \equiv y_0 \pmod{\mathfrak{p}}$ and use Hensel's lemma to find a $Y_0 \in R$ satisfying $Y_0 \equiv y_0 \pmod{\mathfrak{p}}$ and $F(X_0, Y_0) = 0$. Then $S = (X_0, Y_0)$ is an n-torsion point in $E(K)$ lifting $s \in E(k)$. □

Remark 6. Theorem 1 assures us that every $s \in e(k)$ of order n can be lifted to an n-torsion point $S \in E(K)$, where K is a complete local field with residue field k. However, the proof relies on properties of the division polynomial $\psi_n(X)$. If n is large, then it is not feasible to explicitly compute ψ_n, since ψ_n has degree $(n^2-1)/2$. Luckly, there is a more direct way to compute the lift. Roughly speaking, we look at the one-parameter family of lifts, and then the condition that S have finite order gives a linear equation for the parameter. The next example illustrates the process.

Example 2. We continue with Example 1. The formula for S,

$$S = (7 + pu, 258 + 85pu) = (7 + 257u, 258 + 21845u) \pmod{257^2},$$

gives a one-parameter collection of lifts of s. That is, we get one lift modulo 257^2 for each value of u. We now add the condition that$83S \equiv 0 \pmod{p^2}$ and use it to pin down a precise value for u. The easiest way to exploit this condition is to write it as $41S \equiv -42S \pmod{p^2}$. It may seem difficult to compute a large multiple of S when S involves the indeterminate quantity u. However, the variable u appears as pu, so its square modulo p^2 is 0. Hence we never need to deal with general polynomails in u. The only expressions that appear have the form $\alpha+\beta pu$ with $0 \le \alpha < p^2$ and $0 \le \beta < p$. Thus the usual elliptic curve addition formula and general methods for computing large multiples (e.g., by binary expansion of the multiplier) work quite well. The results in our case are

$$\begin{aligned} 41S &\equiv (59609 + 12336u, 39178 + 44718u) \pmod{257^2}, \\ -42S &\equiv (40334 + 24415u, 27099 + 63736u) \pmod{257^2}. \end{aligned}$$

The congruence $41S \equiv -42S \pmod{257^2}$ leads to the two congruences

$$\begin{aligned} \frac{x(41S) - x(-42S)}{257} &\equiv -47u + 75 \equiv 0 \pmod{257}, \\ \frac{y(41S) - y(-42S)}{257} &\equiv -74u + 47 \equiv 0 \pmod{257}. \end{aligned}$$

These congruences have the solution $u \equiv 18 \pmod{257}$. Of course, it is no coincidence that there is a simultaneous solution. Substituting into the formula for S yields the unique point

$$S = (4633, 63223) = (7 + 18 \cdot 257, 1 + 246 \cdot 257) \pmod{257^2}$$

satisfying

$$S \in E \pmod{257^2}, \qquad S \equiv (7, 1) \pmod{257}, \qquad 83S \equiv 0 \pmod{257^2}.$$

We apply the same process to the point $t = (150, 14)$ from Example 1. We find that $T = (150+pu, 14+pv)$ is on the curve modulo p^2 if and only if $v = 71u+240$, so the full set of lifts is $T = (257u + 150, 18247u + 61694)$. We now impose the condition $83T \equiv O \pmod{p^2}$ in the form $41T \equiv -42T$. This leads to $u = 47$ and $T = (12229, 60666)$. Then T has order 83 modulo p^2, and one can check that $T \equiv 54S \pmod{257^2}$. However, we cannot ascertain this last formula by computing $83S$ and $83T$ and working in the formal group, because both $83S$ and $83T$ are zero modulo 257^2. And there is no known way to efficiently use the mod 275^2 lifts to compute the discrete logarithm 54 without first moving into the formal group.

4 Lifting to a Global Torsion Point

As we saw in Section 3, if we lift points $s, t \in e(k)$ to torsion points $S, T \in E(K)$, then the relation $t = ms$ is preserved as $T = mS$. However, lifitng to a local field did not help to compute m. In this section we observe that if we can lift to torsion points defined over a global field, for example $\mathbb{Q}$ or a number field, then it is compartively easy to find m from S and T. For example, we can reduce modulo many small primes $\mathfrak{q}$ and find the value of m modulo $\#E(\mathbb{F}_{\mathfrak{q}})$.

However if we try to lift to torsion points defined over $\mathbb{Q}$ or a number field, then we run into a severe restriction.

Theorem 2. (Mazur [17], Merel [18]) *Let $E/\mathbb{Q}$ be an elliptic curve and let $P \in E(\mathbb{Q})_{\text{tors}}$. Then P has order at most 12.*

More generally, for any $d \geq 1$ there is a bound $C(d)$ so that if $K/\mathbb{Q}$ is a number field of degree d and E/K is an elliptic curve with torsion point $P \in E(K)_{\text{tors}}$, then P has order at most $C(d)$.

We can also turn the question around. Thus we lift e to an elliptc curve E, say defined over $\mathbb{Q}$, and we ask how large a number field K is needed in order to get an n-torsion point in $E(K)$. The asymptotic answer is provided by a theorem of Serre.

Theorem 3. (Serre [28,29]) *Let $E/\mathbb{Q}$ be an elliptic curve. There is a constant $c = c(E) > 0$ so that for all integers $n \geq 2$ and any number field K such that $E(K)$ has a torsion point of exact order n, we have*

$$[K : \mathbb{Q}] \geq c \# \operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}) \approx cn^4.$$

Since for cryptographic applications we need points whose order is between 2^{160} and 2^{320}, the theorems of Mazur, Merel, and Serre make it unlikely that lifting to torsion points over global fields will lead to a workable attack on the ECDLP, since it is not feasible to write down such points or to work in the fields over which they are defined.

5 Lifting to a Global Nontorsion Point

The index calculus is the most powerful method known for solving the classical discrete logarithm problem in the multiplicative group of a finite field. Miller's original article [20] briefly mentions some of the difficulties in extending the index calculus to elliptic curve groups. A more detailed analysis is given in [35]. We briefly summarize the results in Section 5.2. An alternative approach to solving the ECDLP tries to force curves to have low rank rather than using curves of high rank. This method, dubbed the xedni calculus, is described in Section 5.3. In the final section we briefly mention another unsuccessful global nontorsion lifting method that exploits the covering of elliptic curves by modular curves and the existence of special points called Heegner points on modular curves.

5.1 Canonical Heights and Global Lifting

The group of rational points $E(K)$ on an elliptic curve over a number field has a canonical height function

$$\hat{h} : E(K) \longrightarrow [0, \infty)$$

possessing a number of very nice properties. (See, e.g., [30, VIII §9] for basic material on $\hat{h}$.) It has been suggested that the existence of the canonical height in some way protects the ECDLP from index calculus methods. In this section we explain why we feel that the mere existence of the canonical height does not, in and of itself, imply that ECDLP should be hard. Our reason for this assertion is that canonical heights exist in a wide variety of situations, including some such as the classical DLP for which the index calculus does work. We then briefly indicate what we feel is the real reason that the index calculus does not work on elliptic curves. A more complete discussion is given in the next section.

In general terms, a *canonical height* on an abelian group G is a function

$$\hat{h} : G \longrightarrow [0, \infty)$$

with the following four properties:

Power Rule. There is a constant $d > 0$ such that

$$\hat{h}(n\alpha) = |n|^d \hat{h}(\alpha) \qquad \text{for all } n \in \mathbb{Z} \text{ and } \alpha \in G.$$

Addition Rule. There is a constant $c_1 = c_1(G) > 0$ such that

$$\hat{h}(\alpha + \beta) \le c_1\big(\hat{h}(\alpha) + \hat{h}(\beta)\big) \qquad \text{for all } \alpha, \beta \in G.$$

Normalization. For any $\alpha \in G$, let $|\alpha|_H$ denote the number of bits it takes to describe the element α. (The "H" stands for Hamming weight.) There are constants $c_2 = c_2(G) > 0$ and $c_3 = c_3(G) > 0$ such that

$$c_2|\alpha|_H \le \hat{h}(\alpha) \le c_3|\alpha|_H \qquad \text{for all } \alpha \in G.$$

Finiteness. For any bound B, the set $\{\alpha \in G : \hat{h}(\alpha) < B\}$ is finite.

We have the following well-known result, which is a version of Fermat's method of descent.

Proposition 1. *Let G be an abelian group. Suppose that there exists a canonical height on G. Further suppose that the quotient group G/nG is finite for some integer $n \ge 2$. Then the group G is finitely generated.*

More precisely, suppose that G/nG is finite for some integer n satisfying $n^d > 2c_1$, where d and c_1 are the constants appearing in the power rule and the addition rule for $\hat{h}$, respectively. Choose coset representatives

$$\alpha_1, \alpha_2, \ldots, \alpha_t \quad \textit{for } G/nG.$$

Then the finite set

$$\left\{\alpha \in G : \hat{h}(\alpha) \le \max_{1 \le i \le t} \hat{h}(\alpha_i)\right\} \tag{6}$$

generates G.

Table 2. Canonical height on multiplicative and elliptic curve groups

	Multiplicative Group	**Elliptic Curve**
Power Rule	$\hat{h}(\alpha^n) = \lvert n\rvert\hat{h}(\alpha)$	$\hat{h}(nP) = n^2\hat{h}(P)$
Addition Rule	$\hat{h}(\alpha\beta) \le \hat{h}(\alpha) + \hat{h}(\beta)$	$\hat{h}(P+Q) \le 2\hat{h}(P) + 2\hat{h}(Q)$
Normalization	Standard	Standard

Proof. We prove the second part and leave the first part as an exercise (or see any standard text). Let S denote the set (6), let G_S denote the subgroup of G generated by S, and let $M = \max_i \hat{h}(\alpha_i)$. We suppose that $G_S \neq G$ and we choose an element $\alpha \in G \setminus G_S$ of minimal canonical height. Notice in particular that $\hat{h}(\alpha) > M$. The image of $-\alpha$ in G/nG is represented by one of the α_i's, say

$$-\alpha \equiv \alpha_k \pmod{nG}.$$

This means that $-\alpha = \alpha_k - n\beta$ for some $\beta \in G$. We compute

$$n^d\hat{h}(\beta) = \hat{h}(n\beta) = \hat{h}(\alpha+\alpha_k) \le c_1\big(\hat{h}(\alpha)+\hat{h}(\alpha_k)\big) \le c_1\big(\hat{h}(\alpha)+M\big) \le 2c_1\hat{h}(\alpha).$$

Thus $\hat{h}(\beta) \le (2c_1/n^d)\hat{h}(\alpha) < \hat{h}(\alpha)$, so by assumption we have $\beta \in G_S$. Thus $\beta = \sum_i m_i\alpha_i$ for some $m_i \in \mathbb{Z}$, which in turn implies that

$$\alpha = n\beta - \alpha_k = n\sum_i m_i\alpha_i - \alpha_k \in G_S,$$

contradicting the assumption that $\alpha \notin G_S$. This proves that $G_S = G$, and hence that S generates G. □

The part of the definition that makes the height "canonical" is the power rule. If the height function only satisfies $\hat{h}(g^n) \gg\ll |n|^d\hat{h}(g)$, one can still easily deduce the conclusion of Proposition 1 that G/nG is finitely generated, although the actual set of generators will be somewhat different.

It is not only elliptic curves that have a canonical height. The ordinary multiplicative group of $\mathbb{Q}$, or more generally of a number field, also has a canonical height. Indeed, the standard Weil height

$$h\left(\frac{a}{b}\right) = \log\max\{|a|,|b|\}, \qquad a,b \in \mathbb{Z},\ \gcd(a,b)=1,$$

is a canonical height on $\mathbb{Q}^*$. Table 2 gives a point-by-point comparision of the canonical heights on multiplicative groups and elliptic curves and shows how they are analogous.

Since we know that the index calculus works when we lift from the multiplicative group $\mathbb{F}_p^*$ to (finitely generated subgroups of) the multiplicative group of $\mathbb{Q}^*$, it does not seem that the mere existence of the canonical height prevents index calculus methods from working on elliptic curves. We must look elsewhere

for the reason. We give a detailed discussion in the next section, but briefly we point out here the following dichotemy that gives a clear distinction between the two situations.

Consider first a finitely generated subgroup of $\mathbb{Q}^*$, say the subgroup

$$G = \langle p_1, p_2, p_3, \ldots, p_r \rangle$$

generated by the first r primes. Similarly, let $E/\mathbb{Q}$ be an elliptic curve whose Mordell–Weil group is given by

$$E(\mathbb{Q}) = \langle P_1, P_2, \ldots, P_r \rangle.$$

In both situations, the canonical height lets us work with linear combinations of the generators. However, when we look at the actual sizes of the generators, we find (assuming some standard conjectures) a striking difference:

$$\max_{1 \le i \le r} \hat{h}(p_i) \approx \log r \qquad \text{and} \qquad \max_{1 \le i \le r} \hat{h}(P_i) \gg r \log r.$$

Thus it is quite reasonable to work with subgroups of $\mathbb{Q}^*$ of rank (say) 10^6 or 10^7, since the Hamming weight of the generators is not very large. But it would be difficult to deal with elliptic curves of such high rank, even if one knew how to find them. Further, there are other conjectures predicting that for "most" elliptic curve, $\max_i \hat{h}(P_i)$ actually grows exponentially in r. Thus it is not the canoncial height, per se, that "protects" elliptic curves from the index calculus. Rather, it is the fact that generating sets for elliptic curve groups have heights (i.e., Hamming weights) that are at least exponentially larger than those for multiplicative groups.

5.2 Elliptic Curves and the Index Calculus (Hard Lift Method)

Let (k, e, s, t) be an ECDLP whose solution $t = ms$ we seek. We also let n denote the order of s (and t) in the group $e(k)$. The idea of the index calculus is to find a number field K and a lift (K, E) of (k, e) for which it is possible to solve the lifting problem

$$E(K) \longrightarrow e(k)$$

for some reasonable fraction of the points in $e(k)$. One way to do this might be to choose E so that the group $E(K)$ has large rank. Of course, the Mordell–Weil theorem tells us that $E(K)$ has finite rank, and indeed for any given field K, it appears to be very difficult to find elliptic curves of very large rank. In any case, we start by showing that if this lifting problem can be solved, then ECDLP can similarly be solved.

Theorem 4. *Let K be a number field and let (K, E) be a lift of (k, e). Let $\mathcal{A}$ be an algorithm that, given a point $u \in e(k)$, has an ϵ-probability of finding a lift $U \in E(K)$ of u. Then there is an algorithm that solves the ECDLP for $e(k)$ in time $O(\epsilon^{-1})$. (The implied constants depend on K and E.)*

Proof. Let r be an upper bound for the rank of the Mordell–Weil group $E(K)$. An upper bound can be given explicitly in terms of the coefficients of E and the discriminant of the field K. (The methods in [30, chapter 10] can easily be used to derive such a bound, or see [23] for a general formulation. The upper bound for r is logarithmic in the coefficients and discriminant of K, so tends to be fairly small.)

Let (k, e, s, t) be an ECDLP to be solved. Choose at random $2(r+1)\epsilon^{-1}$ pairs of integers (a, b) and for each pair compute the point

$$as - bt \in e(k).$$

Applying the algorithm $\mathcal{A}$ to each of these points, we expect to lift at least $r + 1$ of them. Let

$$u_i = a_i s - b_i t \in e(k), \qquad 0 \le i \le r,$$

be the points that we are able to lift and let $U_i \in E(K)$ be the lift of u_i.

The fact that $E(K)$ has rank at most r implies that the points $U_0, \ldots, U_r$ are dependent. Further, it is generally possible to find an equation of dependency

$$m_0 U_0 + m_1 U_1 + \cdots + m_r U_r = 0 \qquad \text{in } E(K). \tag{7}$$

More precisely, we can find the dependence relation using either the theory of canonical heights or the theory of descent. See [34] and the references listed there for details, but as a practical matter we observe that the method will generally work in time that is polynomial in the number of bits in the description of E, K, and $U_0, \ldots, U_r$.

Having produced a relation (7) over the global field K, we use the reduction map $E(K) \to e(k)$ to deduce the relation

$$m_0 u_0 + m_1 u_1 + \cdots + m_r u_r = 0 \qquad \text{in } e(K).$$

Substituting $U_i = a_i s - b_i t$ and rearranging terms gives

$$\left(\sum_{i=0}^{r} m_i a_i\right) s = \left(\sum_{i=0}^{r} m_i b_i\right) t \qquad \text{in } e(k).$$

In other words, we have a relation $As = Bt$ with $A, B \in \mathbb{Z}$. Further, there is a reasonable probability that B will be relatively prime to n. (In practice, n will be a large prime, in which case B is almost certainly prime to n.) Multiplying the relation $As = Bt$ by $B^{-1} \bmod n$ yields the solution $ms = t$ to the ECDLP. □

We next formulate a general notion of an index calculus for a group and relate it to the ideas described in the proof of Theorem 4.

Definition 3. *Let G be a (finitely generated abelian) group. The* relation problem *on G is the problem of finding, for a given set $\{U_0, U_1, \ldots, U_r\}$ of dependent elements of G, a nontrivial relation*

$$m_0 U_0 + m_1 U_1 + \cdots + m_r U_r = 0.$$

Definition 4. *An* index calculus *for a finite group g is a finitely generated group G for which the relation problem can be efficiently solved, a* (*surjective*) *homomorphism*

$$\pi : G \longrightarrow g,$$

and an algorithm that has an ϵ-probability of lifting an element of g to an element of G.

Example 3. Let G is the subgroup of $\mathbb{Q}^*$ generated by the first n primes, say for $n = 10^5$ or $n = 10^6$. It is relatively easy to check if an element of $\mathbb{Q}^*$ is in G, and it is also not hard to solve the relation problem for elements of G. Finally, let $\mathbb{F}_p$ be a finite field with p elements and consider the reduction map

$$G \longrightarrow \mathbb{F}_p^*.$$

For primes p of an appropriate size, there is a nontrivial probability that elements of $\mathbb{F}_p^*$, lifted into the interval $[0, p-1]$, will lie in G. Thus there is an index calculus for $\mathbb{F}_p^*$.

Example 4. We let $p = 257$ and consider the curve and points

$$e : y^2 = x^3 + 23x + 11, \quad s = (7, 1) \in e(\mathbb{F}_{257}), \quad t = (140, 71) \in e(\mathbb{F}_{257}).$$

It is not hard to find a lift $E/\mathbb{Q}$ such that $S = (7, 1) \in E(\mathbb{Q})$, for example

$$E : Y^2 = X^3 + 23X - 503, \qquad S = (7, 1) \in \hat{E}(\mathbb{Q}).$$

In this example it is likely that $\operatorname{rank} E(\mathbb{Q}) = 1$ and that the reduction map $E(\mathbb{Q}) \to e(\mathbb{F}_{257})$ is surjective, so there are points $T \in E(\mathbb{Q})$ whose reduction is $t = (140, 71)$. If we can find such a T, then it is relatively easy to express T as a multiple of S, and hence to solve the ECDLP for s and t. However, although such T exist, there are no known algorithms that efficiently find a T. For this example it turns out that the least complicated value of $T \in E(\mathbb{Q})$ satisfying $T \equiv t \pmod{257}$ is the point

$$T = \left(\frac{62394310869880049863559}{8736078981416085105625}, \frac{4130665692373765369756729240437877}{8165350423947492616771476241718 75} \right).$$

Further, we are lucky that T is so uncomplicated, since it happens that $T = 5S$. If instead T were equal to, say, $51S$, then its coordinates would require numbers with thousands of digits.

Now let G be the group of points $E(\mathbb{Q})$ of an elliptic curve. As we observed during the proof of Theorem 4, there are efficient algorithms based on canonical heights and on descent theory for solving the relation problem in $E(\mathbb{Q})$. Further, for a given elliptic curve $e/\mathbb{F}_p$, it is not hard to find a lift $E/\mathbb{Q}$ such that the reduction map is surjective, and one can even force the rank of $E(\mathbb{Q})$ to be larger than one. (However, it is not known if the rank can be arbitrarily large; the current record for the rank of $E(\mathbb{Q})$ is less than 30.) Thus if one could find an

efficient algorithm $\mathcal{A}$ that had an ϵ-probability of lifting the map $E(\mathbb{Q}) \to e(\mathbb{F}_p)$, then one would have an index calculus and be able to solve ECDLP.

We now briefly sketch the reasons why such an algorithm is unlikely to exist. Our material is taken from [20] and [35] and we refer the reader to those sources for further details. For simplicity, we restrict attention to an elliptic curve e defined over a finite field $\mathbb{F}_p$ and a lift of e to an elliptic curve $E/\mathbb{Q}$. In order to have an index calculus, we need to find an efficient algorithm $\mathcal{A}$ that lifts a significant number of the points of $e(\mathbb{F}_p)$ to points in $E(\mathbb{Q})$.

The complexity of a point $P \in E(\mathbb{Q})$ is measured by its canonical height $\hat{h}(P)$, so we suppose that $\mathcal{A}$ lifts points in $e(\mathbb{F}_p)$ into the set

$$E_B(\mathbb{Q}) = \{P \in E(\mathbb{Q}) : \hat{h}(P) \le B\}.$$

(See [30, VIII §9] for basic material on canonical heights and [31,33] for computational methods.) A conjecture of Lang (proven in many cases, see [10]) says that $\hat{h}(P)$ cannot be too small. A theoretical and experimental analysis given in [35] shows that at best we can expect

$$\#E_B(\mathbb{Q}) \gg\ll \left(\frac{c \log B}{r \cdot \log |\Delta(E)|}\right)^{r/2},$$

where r is the rank of $E(\mathbb{Q})$, $\Delta(E)$ is the discriminat of E, and c is an explicit constant.

In order to lift points from $e(\mathbb{F}_p)$ into $E_B(\mathbb{Q})$, we need $\#E_B(\mathbb{Q})$ to be a nontrivial fractional multiple of p. On the other hand, the fact that E is a lift of e means that $\log |\Delta(E)| \gg \log p$, and a theorem of Mestre [19] (conditional on various standard conjectures) implies that $\log |\Delta(E)| \gg r \log r$. The calculations in [35] then show that if $p \approx 2^{160}$ and if we want $\#E_B(\mathbb{Q}) \ge p/2^{10}$, then we probably need $r \approx 180$ and $B \approx 2^{7830} \approx p^{49}$. The first problem would be to merely find a curve of rank 180. (Mestre's work says roughly that the coefficients of a curve of rank r will be larger than $r^{c'r}$.) However, even if this problem could be solved, we still have no way of lifting points from $e(\mathbb{F}_p)$ to points in $E_B(\mathbb{Q})$.

Remark 7. Although the index calculus does not work on elliptic curves, we mention that it does work on hyperelliptic Jacobian varieties when the genus is sufficiently large compared to the order of the field; see [1] for details.

5.3 Elliptic Curves and the Xedni Calculus (Easy Lift Method)

As described in the previous section, an index calculus for a group g involves a lifting homomorphism $G \to g$ such that G is finitely generated and such that there is an efficient algorithm for lifting many elements of g to elements of G. Thus in the index calculus scenario, we start with the homomorphism $G \to g$ and then select points to lift. In this section we consider the reverse scenario, which we dub the *xedni calculus* (xedni is index reversed). The idea is to first select the points to be lifted, and then to find an appropriate group into which to lift them. We begin with an abstract formulation.

Definition 5. *A* xedni calculus *for a finite abelian group g is an algorithm that has an ϵ-probability of taking a set of elements $u_0, \dots, u_r \in g$ and efficiently finding a finitely generated group G of rank at most r for which the relation problem can be efficiently solved, a (surjective) homomorphism*

$$\pi : G \longrightarrow g,$$

and points $U_0, \dots, U_r \in G$ satisfying $\pi(U_i) = u_i$.

Proposition 2. *Let g be a finite abelian group for which there is a xedni calculus. Then there is an algorithm to solve the discrete logarithm problem on g.*

Proof. Let $s, t \in g$ be a discrete logarithm problem to be solved. Choose at random integers $a_0, \dots, a_r, b_0, \dots, b_r$ and apply the given xedni calculus algorithm to the points

$$u_i = a_i s - b_i t \in g, \qquad 0 \le i \le r.$$

The algorithm will probably be successful in fewer than $2/\epsilon$ attempts. Let $U_0, \dots, U_r \in G$ be the lifts of $u_0, \dots, u_r$ found by the algorithm. The group G has rank at most r, so $U_0, \dots, U_r$ are dependent; and by assumption there is an efficient method for finding a relation $m_0 U_0 + \cdots + m_r U_r = 0$.

The remainder of the proof is the same as the proof of Theorem 4, so we just briefly sketch. Substituting and rearranging yields $(\sum_i m_i a_i)s = (\sum_i m_i b_i)t$. Then multiplying by the inverse of $\sum_i m_i b_i$ modulo the order of s and t gives the desired relation $ms = t$. □

There is a natural way to try to use the xedni calculus to solve the ECDLP. Thus let $e/\mathbb{F}_p$ be an elliptic curve and let $u_0, \dots, u_r \in e(\mathbb{F}_p)$. Writing $u_i = (x_i, y_i) \in \mathbb{F}_p^2$, we lift the u_i to points $U_i = (X_i, Y_i) \in \mathbb{Z}^2$ without regard to the curve.

Suppose that e is given by that Weierstrass equation

$$e : f(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0.$$

Then lifts of e to $\mathbb{Q}$ are given by Weierstrass equations

$$E : F(X, Y) = Y^2 + A_1 XY + A_3 Y - X^3 - A_2 X^2 - A_4 X - A_6 = 0$$

whose coefficients $A_1, \dots, A_6 \in \mathbb{Q}$ are required to satisfy

$$A_1 \equiv a_1,\ A_2 \equiv a_2,\ A_3 \equiv a_3,\ A_4 \equiv a_4,\ A_6 \equiv a_6 \pmod{p}.$$

The formulas $F(X_i, Y_i) = 0$ for $0 \le i \le r$ give $r+1$ linear equations for $A_1, \dots, A_6$, so as long as $r \le 4$, there is a solution $A_1, \dots, A_6 \in \mathbb{Q}$. Further, the fact that $f(x_i, y_i) = 0$ in $\mathbb{F}_p$ means that we can find a solution with $A_i \equiv a_i \pmod{p}$. Then the curve $E/\mathbb{Q}$ defined by $F(X, Y) = 0$ is a lift of e, and we have arranged matters so that the points $u_i \in e(\mathbb{F}_p)$ have lifts to points $U_i \in E(\mathbb{Q})$.

More generally, we can lift e using a general cubic polynomial of two variables, $F(X, Y) = \sum_{j+k \le 3} A_{jk} X^j Y^k$. There are 10 coefficients A_{jk}, so using only linear algebra, we can lift $e/\mathbb{F}_p$ and up to 9 points $u_i \in e(\mathbb{F}_p)$ to an elliptic curve $E/\mathbb{Q}$ and points $U_i \in E(\mathbb{Q})$. If it turns out that (with non-negligible probability) the rank of $E(\mathbb{Q})$ is smaller than the number of lifted points, then the xedni calculus succeeds.

Example 5. We let $p = 257$ and consider the curve and points

$$e : y^2 = x^3 + 23x + 11, \quad s = (7, 1) \in e(\mathbb{F}_{257}), \quad t = (110, 15) \in e(\mathbb{F}_{257}).$$

We write the lifts $E/\mathbb{Q}$ of $e/\mathbb{F}_{257}$ as

$$E : Y^2 = X^3 + (23 + 257\alpha)X + (11 + 257\beta).$$

Substituting $S = (7, 1)$ and $T = (110, 15)$ yields two equations for α and β whose solution gives

$$E : Y^2 = X^3 - \frac{1330433}{103}X + \frac{9277805}{103},$$
$$S = (7, 1) \in E(\mathbb{Q}) \quad \text{and} \quad T = (110, 15) \in E(\mathbb{Q}).$$

However, the points S and T are linearly independent in $E(\mathbb{Q})$, so they cannot be used to solve the ECDLP for s and t in $e(\mathbb{F}_{257})$.

We may view this naive xedni approach to the ECDLP as a specialization process. Thus if we write $U_i = (X_i, Y_i)$ and treat the coordinates X_i and Y_i as indeterminates, then we can create an elliptic curve $\mathcal{E}$ whose coefficients are in the field of rational functions $\mathcal{K} = \mathbb{Q}(X_0, \ldots, X_r, Y_0, \ldots, Y_r)$ and such that $U_i \in \mathcal{E}(\mathcal{K})$. Then the above process involves substituting in particular values for the X_i and Y_i. It is not hard to see that before we substitute values, the points $U_0, \ldots, U_r$ are independent in the group $\mathcal{E}(\mathcal{K})$. Then results of Néron and Masser, as described in the following result, say that most substitutions give specialized points that are independent.

Theorem 5. (Néron [22], Masser [16]) *Let $\mathcal{E}_Z$ be a parameterized family of elliptic curves, where $Z = (Z_1, \ldots, Z_n)$, and let $U_{0,Z}, \ldots, U_{r,Z}$ be parameterized families of points that are linearly independent. Then*

$$\big\{ z \in \mathbb{Q}^n : Q_{1,z}, \ldots, Q_{r,z} \text{ are dependent in } \mathcal{E}_z(\mathbb{Q}) \big\}$$

is a small set (a set of density 0*).*

If we view the coordinates of the points as being the parameters, then the precise statement of Masser's theorem says that the probability that lifted (i.e., specialized) points are linearly dependent is at most $O(1/p)$. Hence the probability that this naive version of the xedni calculus succeeds is negligible.

The reason that the naive xedni calculus does not work is because the lifted points tend to be independent. This suggests imposing further conditions on the lifts in order to make them more likely to be dependent. Mestre [19] has a method, based on the Birch–Swinnerton-Dyer conjecture, for influencing elliptic curves to have *higher* ranker than expected. His idea is to impose congruence conditions on the coefficients of $E/\mathbb{Q}$ for small primes $\ell \le L$ in order to force $\#E(\mathbb{F}_\ell)$ to be large. Since we know that $\#E(\mathbb{F}_\ell) = \ell + 1 - a_\ell$ with $|a_\ell| \le 2\sqrt{\ell}$, Mestre's idea is to require that a_ℓ be close to $-2\sqrt{\ell}$. Mestre used this idea to produce

an elliptic curve with $\operatorname{rank} E(\mathbb{Q}) = 15$, and his idea is still used in algorithms to find curves of high rank.

This led the author to suggest using Mestre's method in reverse to try to influence the lifted curve E to have smaller than expected rank [34]. Thus we impose both the mod p condition that $E/\mathbb{Q}$ is a lift of $e/\mathbb{F}_p$, and also mod ℓ conditions for small primes in order to force $\#E(\mathbb{F}_\ell)$ to be small, i.e., for a_ℓ to be close to $2\sqrt{\ell}$. The hope was that this would cause $E(\mathbb{Q})$ to have smaller rank than expected, which would allow the xedni calculus to succeed.

However, as described in [13], it turns out that there are two difficulties that cause this approach to fail. First, asymptotically one can show using canonical heights, a height specialization theorem [32, III §11] and Lang's height lower bound conjecture [15, page 78] that the lifted points are independent. Second, even for numbers of cryptographic size, experiments show that the rank lowering effect of the small primes is offset by the increased size of the coefficients of E, which negates the (heuristic) application of the Birch–Swinnerton-Dyer conjecture.

5.4 Elliptic Curves and Heegner Point Lifts

We conclude by briefly describing another global lifting method based on entirely different ideas. Suppose that $e/\mathbb{F}_p$ can be lifted to a curve $E/\mathbb{Q}$ with small coefficients. Then we can exploit the fact (Wiles et.al. [3,38,39]) that E is covered by a modular curve, $X_0(N) \to E$, where N is the conductor of E. The curve $X_0(N)$ has special points called Heegner points that are constructed using the theory of complex multiplication, and Deuring's work on CM [7] explains how to lift points in $X_0(\mathbb{F}_p)$ to Heegner points in $X_0(K)$ for certain number fields K. If these Heegner points have a non-negligible probabiilty of being dependent, then one might use their modular interpretation and height formulas of Gross, Zagier, and Kohnen [8,9] to find explicit dependencies without having to explicitly determine the coordinates of the points. This would give a xedni calculus solution to the ECDLP. However, it turns out that the Heegner point lifts are (almost) always independent, although proving their independence is far from trivial. See [24] for details.

6 Summary and Final Remarks

In this paper we have outlined four lifting methods for the ECDLP:

Local-Nontorsion. Lift to nontorsion points in $E(\mathbb{Q}_p)$.
Fails because we lose the relationship $T = mS$.

Local-Torsion. Lift to torsion points in $E(\mathbb{Q}_p)_{\text{tors}}$
The relation $T = mS$ is true, but the method fails because we cannot move into the formal group, and there is no known way to determine m without moving into the formal group.

Global-Torsion. Lift to points in $E(\mathbb{Q})_{\text{tors}}$ or $E(K)_{\text{tors}}$
Fails because $E(\mathbb{Q})_{\text{tors}}$ is too small and $[K : \mathbb{Q}]$ is too large.

Global-Nontorsion. Lift to nontorsion points in $E(\mathbb{Q})$.
Hard Lift Method (*index calculus*):
Fails because there is no known method to lift additional points.
Easy Lift Method (*xedni calculus*):
Fails because the lifted points are independent.

Acknowledgements. I would like to thank Jeff Achter for his comment on lifting the ECDLP to global torsion points, a remark that led me to consider anew the overall question of lifting and the ECDLP.

References

1. Adleman, L.M., DeMarrais, J., Huang, M.-D.A.: A subexponential algorithm for discrete logarithms over hyperelliptic curves of large genus over $GF(q)$. Theoret. Comput. Sci. 226(1-2), 7–18 (1999)
2. Blake, I.F., Seroussi, G., Smart, N.P.: Elliptic Curves in Cryptography. Cambridge University Press, Cambridge (1999)
3. Breuil, C., Conrad, B., Diamond, F., Taylor, R.: On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Amer. Math. Soc. 14, 843–939 (2001)
4. Cheng, Q., Huang, M.-D.: Partial lifting and the elliptic curve discrete logarithm problem. Algorithmica 46(1), 59–68 (2006)
5. Kim, H.J., Cheon, J.H., Hahn, S.G.: On remarks on lifting problems for elliptic curves. Adv. Stud. Contemp. Math (Pusan) 2, 21–36 (2000)
6. Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. Discrete Mathematics and Its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton (2006)
7. Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abh. Math. Sem. Hansischen Univ. 14, 197–272 (1941)
8. Gross, B., Kohnen, W., Zagier, D.: Heegner points and derivatives of L-series. II. Math. Ann. 278, 497–562 (1987)
9. Gross, B.H., Zagier, D.B.: Heegner points and derivatives of L-series. Invent. Math. 84, 225–320 (1986)
10. Hindry, M., Silverman, J.H.: The canonical height and integral points on elliptic curves. Invent. Math. 93, 419–450 (1988)
11. Hoffstein, J., Pipher, J., Silverman, J.H.: An Introduction to Mathematical Cryptography, UTM. Springer, New York (2008)
12. Huang, M.-D., Kueh, K.L., Tan, K.-S.: Lifting elliptic curves and solving the elliptic curve discrete logarithm problem. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 377–384. Springer, Heidelberg (2000)
13. Jacobson, M.J., Koblitz, N., Silverman, J.H., Stein, A., Teske, E.: Analysis of the xedni calculus attack. Designs, Codes and Cryptography 20, 41–64 (2000)
14. Koblitz, N.: Elliptic curve cryptosystems. Mathematics of Computation 48, 203–209 (1987)
15. Lang, S.: Elliptic Curves: Diophantine Analysis. In: Grund. Math. Wiss., vol. 231. Springer, Berlin (1978)

16. Masser, D.: Specializations of finitely generated subgroups of abelian varieties. Trans. Amer. Math. Soc. 311, 413–424 (1989)
17. Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math 47, 33–186 (1977)
18. Merel, L.: Bornes pour la torsion des courbes elliptiques sur les corps de nombres. Invent. Math. 124, 437–449 (1996)
19. Mestre, J.-F.: Formules explicites et minoration de conducteurs de variétés algébriques. Compositio Math. 58, 209–232 (1986)
20. Miller, V.S.: Use of elliptic curves in cryptography. In: Williams, H.C. (ed.) CRYPTO 1985. LNCS, vol. 218, pp. 417–426. Springer, Heidelberg (1986)
21. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (1996)
22. Néron, A.: Problèmes arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps. Bull. Soc. Math. France 80, 101–166 (1952)
23. Ooe, T., Top, J.: On the Mordell–Weil rank of an abelian variety over a number field. J. Pure Appl. Algebra 58(3), 261–265 (1989)
24. Rosen, M., Silverman, J.H.: On the independence of Heegner points associated to distinct quadratic imaginary fields. Journal of Number Theory 127, 10–36 (2007)
25. Rosing, M.: Implementing Elliptic Curve Cryptography. Manning Publications (1998)
26. Satoh, T., Araki, K.: Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Commentarii Math. Univ. St. Pauli 47, 81–92 (1998); Errata. 48, 211–213 (1999)
27. Semaev, I.A.: Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p. Math. Comp. 67, 353–356 (1998)
28. Serre, J.-P.: Abelian l-adic representations and elliptic curves. In: Research Notes in Mathematics, vol. 7. A K Peters Ltd, Wellesley (1998)
29. Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. Invent. Math. 15, 259–331 (1972)
30. Silverman, J.H.: The Arithemtic of Elliptic Curves. In: Graduate Texts in Mathematics, vol. 106. Springer, Heidelberg (1986)
31. Serre, J.-P.: Computing heights on elliptic curves. Math. Comp. 51, 339–358 (1988)
32. Serre, J.-P.: Advanced Topics in the Arithemtic of Elliptic Curves. Graduate Texts in Mathematics, vol. 151. Springer, Heidelberg (1994)
33. Serre, J.-P.: Computing canonical heights with little (or no) factorization. Math. Comp. 66, 787–805 (1997)
34. Serre, J.-P.: The xedni calculus and the elliptic curve discrete logarithm problem. Designs, Codes and Cryptography 20, 5–40 (2000)
35. Silverman, J.H., Suzuki, J.: Elliptic curve discrete logarithms and the index calculus. In: Ohta, K., Pei, D. (eds.) ASIACRYPT 1998. LNCS, vol. 1514, pp. 110–125. Springer, Heidelberg (1998)
36. Smart, N.P.: The discrete logarithm problem on elliptic curves of trace one. J. Cryptology 12, 193–196 (1999)
37. Stinson, D.: Cryptography: Theory and Practice. CRC Press, Boca Raton (1997)
38. Taylor, R., Wiles, A.: Ring-theoretic properties of certain Hecke algebras. Ann. of Math. 141, 553–572 (1995)
39. Wiles, A.: Modular elliptic curves and Fermat's last theorem. Ann. of Math. 141, 443–551 (1995)