Elliptic Curve Discrete Logarithms and the Index Calculus

Joseph H. Silverman[1] and Joe Suzuki[2]

[1] Mathematics Department, Box 1917, Brown University, Providence, RI 02912 USA ⟨jhs@math.brown.edu⟩

[2] Department of Mathematics, Osaka University, Toyonaka, Osaka 560 Japan ⟨suzuki@math.sci.osaka-u.ac.jp⟩

Abstract. The discrete logarithm problem forms the basis of numerous cryptographic systems. The most effective attack on the discrete logarithm problem in the multiplicative group of a finite field is via the index calculus, but no such method is known for elliptic curve discrete logarithms. Indeed, Miller [23] has given a brief heuristic argument as to why no such method can exist. IN this note we give a detailed analysis of the index calculus for elliptic curve discrete logarithms, amplifying and extending miller's remarks. Our conclusions fully support his contention that the natural generalization of the index calculus to the elliptic curve discrete logarithm problem yields an algorithm with is less efficient than a brute-force search algorithm.

0. Introduction

The discrete logarithm problem for the multiplicative group $\mathbb{F}_q^*$ of a finite field can be solved in subexponential time using the *Index Calculus* method, which appears to have been first discovered by Kraitchik [14, 15] in the 1920's and subsequently rediscovered and extended by many mathematicians. (See, for example, [1] and [43], and for a nice summary of the current state-of-the-art, see [29].) For this reason, it was proposed independently by Miller [23] and Koblitz [12] that for cryptographic purposes, one should replace $\mathbb{F}_q^*$ by the group of rational points $E(\mathbb{F}_q)$ on an elliptic curve, thus leading to the *Elliptic Curve Discrete Logarithm Problem*, which we abbreviate as the ECDL problem. Indeed, Victor Miller gives in his article [23, page 423] two reasons why "it is extremely unlikely that an 'index calculus' attack on elliptic curves will ever be able to work." Miller's reasons may be briefly summarized as follows:

(1) It is difficult to find elliptic curves $\mathcal{E}/\mathbb{Q}$ with a large number of small rational points. This observation may be split into two pieces.
   (a) It is difficult to find elliptic curves $\mathcal{E}/\mathbb{Q}$ with high rank.
   (b) It is difficult to find elliptic curves $\mathcal{E}/\mathbb{Q}$ generated by points of small height.

K. Ohta and D. Pei (Eds.): ASIACRYPT'98, LNCS 1514, pp. 110-125, 1998.

(2) Given an elliptic curve $\mathcal{E}/\mathbb{Q}$, a large prime p, and a point $S \in \mathcal{E}(\mathbb{F}_p)$ in the image of the reduction map $\mathcal{E}(\mathbb{Q}) \to \mathcal{E}(\mathbb{F}_p)$, it is difficult to lift S to a point of $\mathcal{E}(\mathbb{Q})$.

Miller [23] devotes three paragraphs giving some rough heuristic reasons to justify these assertions. This lack of an index calculus for the ECDL problem is often cited as a reason for the high security of modern cryptosystems based on ECDL's, as for example in the following excerpt [6].

> Most significantly, no index-calculus-type algorithms are known for the ECDL problem as for the DLP (discrete logarithm problem). For this reason, the ECDL problem is believed to be much harder than either the IFP (integer factorization problem) or the DLP in that no subexponential-time general-purpose algorithm is known.

In view of the importance of the ECDL problem in modern cryptography, it seems worthwhile making a more detailed and in-depth analysis of the possibility of an index calculus for the ECDL problem. That is the purpose of this paper. We will explain how, using a method of Mestre, it is possible to lift an elliptic curve E modulo p to an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ of moderately high rank possessing generators of moderately low height. We will further give both numerical and theoretical evidence which suggests that if p is large, then it will never be possible to use the index calculus on such a curve $\mathcal{E}$ to solve the discrete logarithm problem in $E(\mathbb{F}_p)$. The fundamental reason, already alluded to in Miller's paper, but which we will make much more precise, is that the generators $P_1, \dots, P_r$ on a lifted curve $\mathcal{E}/\mathbb{Q}$ of rank r will necessarily have (logarithmic) height at least

$$\hat{h}(P_i) \geq A + B\log(p) + Cr\log(r)$$

for certain positive constants A, B, C. By way of contrast, the generators (factor basis) for the multiplicative group consists of the first r primes $p_1, p_2, \dots, p_r$ whose (logarithmic) heights

$$h(p_n) = \log(p_n) \leq \log(p_r) \leq C\log(r)$$

are exponentially smaller (as a function of r) than in the elliptic curve situation.

In summary, our theoretical and numerical work fully supports Miller's conclusion that the natural generalization of the index calculus to the elliptic curve discrete logarithm problem yields an algorithm which is less efficient than a brute-force search algorithm.

The detailed contents of this paper are as follows:

Section 1. A brief description of the discrete logarithm problem and the index calculus for the multiplicative group.

Section 2. A discussion of the discrete logarithm problem for elliptic curves and a more detailed description of Miller's obstructions.

Section 3. A theoretical discussion of elliptic curves of high rank, the size of their generators, and the number of points of bounded height.

Section 4. Mestre's method for constructing curves of moderately high rank with generating points of moderately low height, in theory and in practice.

Section 5. The problem of lifing curves and points modulo p to points in $\mathcal{E}(\mathbb{Q})$.

1. The Index Calculus for the Multiplicative Group

In this section we briefly review the index calculus method for solving the discrete logarithm problem in the multiplicative group $\mathbb{F}_p^*$ of a finite field $\mathbb{F}_p$, where p is a fixed large prime. The discrete logarithm problem (DLP) asks:

$$\boxed{\begin{array}{l}\text{Given two elements } \alpha, \beta \in \mathbb{F}_p^*, \\ \text{find } k \text{ such that } \alpha^k = \beta.\end{array}} \qquad \text{(DLP)}$$

Assuming it exists, the value of k satisfying $\alpha^k = \beta$ is denoted by

$$k = \log_\alpha(\beta).$$

The first step in the index calculus is to choose what is known as a *factor basis* consisting of the first r primes,

$$\mathcal{F}_r = \{2, 3, 5, 7, 11, \ldots, p_r\},$$

where we will choose r later. We write $\langle \mathcal{F}_r \rangle$ for the semi-group generated by $\mathcal{F}_r$; that is, $\langle \mathcal{F}_r \rangle$ consists of all integers whose prime divisors are all less than or equal to p_r. Numbers in $\langle \mathcal{F}_r \rangle$ are usually called p_r*-smooth*, and it is vitally important to have an accurate count of how many smooth numbers there are, so we let

$$N(\mathcal{F}_r, B) = \#\{a \in \langle \mathcal{F}_r \rangle \,:\, 1 \le a \le B\}.$$

(This slightly non-classical notation will be useful for comparison with the elliptic curve situation. In the more usual notation, $N(\mathcal{F}_r, B)$ equals $\Psi(B, p_r)$.)

If B is large in comparison to r, then it is quite easy to estimate the size of $N(\mathcal{F}_r, B)$ as the volume of an r-dimensional simplex. Thus

$$N(\mathcal{F}_r, B) = \#\left\{(e_1, \ldots, e_r) \,:\, \begin{array}{c} e_1, \ldots, e_r \ge 0 \\ e_1 \log p_1 + \cdots e_r \log p_r \le \log B \end{array}\right\} \sim \frac{1}{r!} \frac{(\log B)^r}{\prod_i \log p_i}.$$

Then using Stirlings' formula and the prime number theorem (in the form $p_i \sim i \log i$) yields

$$N(\mathcal{F}_r, B) \sim \frac{1}{\sqrt{2\pi r}} \left(\frac{e \log B}{r \log r}\right)^r \qquad \text{for } B \gg r. \tag{1}$$

We have derived this formula for $N(\mathcal{F}_r, B)$ not because it is useful for the index calculus, it isn't, but for later comparison with the elliptic case.

The index calculus begins by computing the powers $\alpha, \alpha^2, \alpha^3, \ldots$ and lifting each of these values from $\mathbb{F}_p$ to $\mathbb{Z}$, say

$$\alpha^j \equiv a_j \pmod{p} \qquad \text{with } 1 \le a_j < p.$$

Each a_j is then checked against $\langle \mathcal{F}_r \rangle$, and if it is in this semi-group, we record the value

$$a_j = \prod_{i=1}^{r} p_i^{e_i(j)}. \tag{2}$$

Notice that since $a_j = \alpha^j$ in $\mathbb{F}_p^*$, and since $\mathbb{F}_p^*$ has order $p-1$, each relation (2) gives a linear equation

$$j \equiv \sum_{i=1}^{r} e_i(j) \log_\alpha(p_i) \pmod{p-1}. \tag{3}$$

We continue computing the powers of α until we obtain r independent linear relations (3), at which point the equations can be solved for the r unknowns $\log_\alpha(p_1), \ldots, \log_\alpha(p_r)$. [Remark. We will neglect the fact that, in practice, the value of r will generally be sufficiently large so as to make it extremely difficult to solve the resulting system of r linear equations, even though they tend to be extremely sparse.]

The final step is to lift the quantities $\beta, \alpha\beta, \alpha^2\beta, \ldots$ to $\mathbb{Z}$, say

$$\alpha^j \beta \equiv b_j \pmod{p} \qquad \text{with } 1 \le b_j < p,$$

until we find a single value of j for which b_j lies in $\langle \mathcal{F}_r \rangle$, say

$$b_j = \prod_{i=1}^{r} p_i^{f_i}.$$

Since $b_j = \alpha^j \beta$ in $\mathbb{F}_p^*$, this yields

$$j + \log_\alpha(\beta) \equiv \sum_{i=1}^{r} f_i \log_\alpha(p_i) \pmod{p-1},$$

and since we already know the values of the $\log_\alpha(p_i)$'s, we recover the desired value of $\log_\alpha(\beta)$.

The key question in implementing the index calculus method is the choice of the number r of primes in the factor base. If r is too small, then it is very unlikely that the a_j's will lie in $\langle \mathcal{F}_r \rangle$; while if r is too large, it will be computationally difficult to determine if a given a_j lies in $\langle \mathcal{F}_r \rangle$. Notice that the latter problem is that of finding the complete factorization of a number $a < p$ by primes at most p_r, which shows how the factorization problem is closely tied into the index calculus.

The probability that a given $1 \le a < p$ lies in $\langle \mathcal{F}_r \rangle$ is approximately equal to $N(\mathcal{F}_r, p)/(p-1)$. Using the approximation (1) and taking $B \gg\ll p$, we find that this quantity is maximized for $r \gg\ll \log p / \log\log p$, which unfortunately leads to a probability which is $\ll p^{-1} \cdot p^{C/\log\log p}$, far too small to be useful. However, it turns out that (1) is not a good approximation in our situation,

because for moderately large values of r, most of the numbers in $N(\mathcal{F}_r, p)$ are of the form $p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ with many of the e_i's equal to 0, and the rest quite small. In geometric terms, most of the numbers in $N(\mathcal{F}_r, p)$ represent points which lie on the boundary of the simplex whose volume is being approximated in the formula (1).

We will not give a detailed analysis here, since the final counting result, although by no means easy, is well-known and amply described in many sources. For example, it is proven in [5] that

$$\Psi\big(x, L(x)^a\big) \approx xL(x)^{-1/2a}, \qquad \text{where} \quad L(x) = \exp(\sqrt{\log x \log\log x}).$$

(Here, as usual, $\Psi(x, y)$ is the number of positive integers less than x whose prime factors are all at most y.) Using a weak form of this result, which suffices for comparison with the elliptic curve case, we see that

$$\text{If } r \approx e^{\sqrt{\log p}}, \text{ then } N(\mathcal{F}_r, p) > p \cdot e^{-\frac{1}{2}\sqrt{\log p}}.$$

Thus a sub-exponential value for r (i.e., r is smaller than any power of p) suffices to give a sub-exponential probability of hitting an element in $\langle \mathcal{F}_r \rangle$. The reason that $N(\mathcal{F}_r, p)$ becomes this large is because the primes $p_1, p_2, \ldots, p_r$ in the rank r factor base are small, satisfying

$$\log p_i \approx \log i \le \log r. \tag{4}$$

We want to emphasize this point because it is fundamentally different from what occurs for elliptic curves, where the elements of a rank r factor base have size on the order of $r \log r$.

Remark.. There are various improvements that are typically used to supplement the index calculus, including storing large factors of the a_j's not factorable in the factor base so as to take advantage of overlaps (birthday phenomenon) and using fancier factorization methods (e.g., based on the number field sieve). At present, we don't see analogous methods for elliptic curves, but even if they exist, they are unlikely to affect our overall analysis, since even saving a square root does not substantially change an exponential running time.

2. The Discrete Logarithm Problem for Elliptic Curves

The discrete logrithm problem for an elliptic curve E over a finite field $\mathbb{F}_p$ is virtually identical to the analogous problem for the multiplicative group. We change notation slightly from the multiplicative case to reflect the fact that the addition law on an elliptic curve is always written additively. We thus assume that our elliptic curve E is given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6$$

whose coefficients lie in the finite field $\mathbb{F}_p$. The discrete logarithm problem for elliptic curves (ECDLP) asks:

Given two points $S, T \in E(\mathbb{F}_p)$, find m such that $S = mT$.	(ECDLP)

Note that group operation is addition in $E(\mathbb{F}_p)$, and we are being asked to compute the integer $m = \log_T(S)$. We also let

$$N = N_p = \#E(\mathbb{F}_p)$$

denote the order of the finite group $E(\mathbb{F}_p)$. There is a polynomial-time algorithm for computing N due to Schoof [30], with improvements by Elkies [8] and Atkins [3], which makes it quite practical to compute N for moderate values of p, say for $p \leq 2^{200}$, and certainly possible for even larger values.

There are various special cases for which the ECDL problem can be solved, including the following:

(1) If $N = p+1$, the so-called "supersingular" case, then the ECDL problem can be reduced to the discrete logarithm problem on the multiplicative group. More generally, if N divides $p^k - 1$, then the ECDL problem can be reduced to the discrete logarithm problem on the multiplicative group of the finite field with p^k elements. Of course, this is only practical if k is not too large. For details, see [20] and [9].

(2) If $N = p$, the so-called "anomalous" case, then the ECDL problem can be reduced to simple addition in $\mathbb{F}_p$, essentially by lifting the curve modulo p^2. See [31], [39], and [28].

(3) If N is divisible by only small primes, then one can use the method of Pohlig and Hellman [25] and Pollard [26] which solves the discrete logarithm problem in time $O(\sqrt{p'})$, where p' is the largest prime divisor of N.

(4) Although not directly relevant, we also mention that the discrete logarithm problem can be solved on the Jacobian J of a curve of genus g provided that $g \gg p$ [2]. The reason is that in this situation, the group $J(\mathbb{F}_p)$ is highly non-cyclic. For cryptographic applications of the elliptic case, one normally chooses E so that $E(\mathbb{F}_p)$ is cyclic of prime order.

Assuming that none of these methods is applicable, it is tempting to try to adapt the index calculus method described in Section 1 directly to the elliptic curve case. Here's a brief summary of how such an index calculus would work.

(1) Choose an elliptic curve $\mathcal{E}/\mathbb{Q}$ which reduces to $E/\mathbb{F}_p$ and which has a reasonably large number of independent rational points, say $P_1, P_2, \ldots, P_r$.

(2) Compute the multiples $S, 2S, 3S, \ldots$ in $E(\mathbb{F}_p)$, and for each j, try to lift jS to a rational point $S_j \in \mathcal{E}(\mathbb{Q})$. That is, $S_j \equiv jS \pmod{p}$. If this is successful, then write S_j as a linear combination

$$S_j = \sum_{i=1}^{r} n_j P_j \qquad \text{in } \mathcal{E}(\mathbb{Q}).$$

(3) After r of the jS's have been lifted, we have r linear equations

$$j = \sum_{i=1}^{r} n_j \log_S(P_j)$$

which can be solved for the individual $\log_S(P_j)$'s.

(4) Next try to lift $T, T+S, T+2S, T+3S, \ldots$ to $\mathcal{E}(\mathbb{Q})$, say that $T+jS$ lifts to T_j. Write

$$T_j = \sum_{i=1}^{r} m_j P_j \qquad \text{in } \mathcal{E}(\mathbb{Q}).$$

Then

$$\log_S(T) + j = \sum_{i=1}^{r} m_j \log_S(P_j),$$

and since we know the values of the $\log_S(P_j)$'s, we recover the desired value of $\log_S(T)$.

There are a number of possible difficulties with putting the above outline into practice. Victor Miller [23, page 423] has given two reasons why "it is extremely unlikely that an 'index calculus' attack on elliptic curves will ever be able to work." His reasons can be briefly summarized as follows (where all quotes are from [23]):

Rank/Height Obstruction. "Unless the rank of the curve can be made very large, and the regulator made fairly small,the probability of a point of $E(\mathbb{F}_p)$ lifting to a point on $\hat{E}(\mathbb{Q})$ whose height is bounded by something reasonable (say a polynomial in $\log p$) is vanishingly small."

Lifting Obstruction. "Even if one could somehow get around the barrier mentioned above, there is still the problem of actually lifting a point." One can try to lift first to a point $(x_1, y_1) \in \hat{E}(\mathbb{Z}/p^k\mathbb{Z})$, but "there are many possible choices for (x_1, y_1). ... Thus, unless there is a new idea, it would seem that this is another barrier, difficult to surmount."

In the remainder of this paper, we are going to analyze in more detail the elliptic index calculus and the obstructions noted by Miller. We begin in the next section with a discussion of the heights of points on elliptic curves.

3. Counting Points on Elliptic Curves Over $\mathbb{Q}$

For this section we briefly forget about elliptic curves over finite fields and discuss the distribution (theoretical, practical, and conjectural) of the rational points on elliptic curves defined over $\mathbb{Q}$. For basic facts about elliptic curves, see for example [18, 33, 34].

Let $\mathcal{E}/\mathbb{Q}$ be an elliptic curve given by a minimal Weierstrass equation

$$\mathcal{E} : y^2 + a_1xy + a_3x = x^3 + a_2x^2 + a_4x + a_6$$

and discriminant $\Delta(\mathcal{E})$. Recall that the height of a rational number $r/s \in \mathbb{Q}$ is defined to be

$$H(r/s) = \max\bigl\{|r|, |s|\bigr\}.$$

The canonical height of a point $P \in \mathcal{E}(\mathbb{Q})$ is then defined to be

$$\hat{h}(P) = \frac{1}{2} \lim_{n\to\infty} \frac{1}{n^2} \log H(x(nP)),$$

and the associated inner product for $P, Q \in \mathcal{E}(\mathbb{Q})$ is

$$\langle P, Q \rangle = \frac{1}{2}\big(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\big).$$

This inner product is positive definite on $\mathcal{E}(\mathbb{Q}) \otimes \mathbb{R}$, and the elliptic regulator of a set of points $P_1, \ldots, P_r \in \mathcal{E}(\mathbb{Q})$ is defined to be

$$\mathrm{Reg}(\mathcal{E}) = \det\big(\langle P_i, P_j \rangle\big)_{1\le i,j\le r}.$$

(Generally, $P_1, \ldots, P_r$ will be set of generators for $\mathcal{E}(\mathbb{Q})/(\mathrm{tors})$, or in numerical examples, an explicitly given set of points. If the set of points is not clear from the context, we will write $\mathrm{Reg}(\mathcal{E}, P_1, \ldots, P_r)$.)

We are interested in counting the number of points in $\mathcal{E}(\mathbb{Q})$ of bounded height, so we set

$$\begin{aligned} N(\mathcal{E}, B) &= \#\{P \in \mathcal{E}(\mathbb{Q}) \,:\, H(x(P)) \le B\}. \\ T(\mathcal{E}) &= \#\mathcal{E}(\mathbb{Q})_{\mathrm{tors}}. \\ r &= r(\mathcal{E}) = \mathrm{rank}\,\mathcal{E}(\mathbb{Q}). \\ \alpha_r &= \pi^{r/2}/((r/2)\Gamma(r/2)) = \text{Volume of unit ball in } \mathbb{R}^r. \end{aligned}$$

Using Sterlings' formula, we have the useful approximation

$$\alpha_r \approx \frac{1}{\sqrt{\pi r}} \left(\frac{2\pi e}{r}\right)^{r/2}. \tag{5}$$

The ordinary and canonical heights are related by

$$\hat{h}(P) = \frac{1}{2} \log H(x(P)) + O_{\mathcal{E}}(1). \tag{6}$$

We will say more later about the dependence of the big-O constant on $\mathcal{E}$, but for now we will ignore its effect (which is negligble in the numerical examples presented below). Then we can estimate $N(\mathcal{E}, B)$ by simply counting lattice points in $\mathbb{R}^r$ relative to the canonical height inner product. Thus

$$\begin{aligned} N(\mathcal{E}, B) &= \#\{P \in \mathcal{E}(\mathbb{Q}) \,:\, H(x(P)) \le B\} \\ &\approx T(\mathcal{E}) \#\{P \in \mathcal{E}(\mathbb{Q}) \,:\, \hat{h}(P) \le \tfrac{1}{2}\log B\} \quad \text{from (6)}, \\ &\approx T(\mathcal{E}) \frac{\alpha_r}{\sqrt{\mathrm{Reg}(\mathcal{E})}} \left(\tfrac{1}{2}\log B\right)^{r/2} \\ &\approx T(\mathcal{E}) \frac{1}{\sqrt{\pi r}} \left(\frac{\pi e \log B}{r \cdot \mathrm{Reg}(\mathcal{E})^{1/r}}\right)^{r/2} \quad \text{from (5)}. \end{aligned}$$

We mention that $T(\mathcal{E}) \le 16$ by Mazur's Theorem [33, VIII.7.5], so the effect from torsion is negligible. In practice, our curves will have trivial torsion, because it has been observed experimentally that the presence of rational torsion makes it more difficult to obtain high rank.

The above formula says that we shouldn't expect to get very many points until $\log B$ and $\mathrm{Reg}(\mathcal{E})^{1/r}$ are of a comparable size, so we need to study the magnitude of the regulator.

A basic result from the geometry of numbers says that (see [17, chapter 5, corollary 7.8])

$$\mathrm{Reg}(\mathcal{E})^{1/r} \ge \left(\frac{\sqrt{3}}{2}\right)^{r-1} \min_{\substack{P\in\mathcal{E}(\mathbb{Q})\\ \hat{h}(P)\neq 0}} \hat{h}(P). \tag{7}$$

Further, there is a conjecture of Lang [18, page 92] which says that for non-torsion points $P \in \mathcal{E}(\mathbb{Q})$,

$$\hat{h}(P) \ge c \log|\Delta(\mathcal{E})|,$$

where the constant c is independent of $\mathcal{E}$. This conjecture has been largely proven [11, 35], albeit with extremely small constants c. Thus, as Miller already observes in [23], it is not possible to get $N(\mathcal{E}, B)$ large unless one chooses

$$\log B \gg r \log|\Delta|.$$

But if $\mathcal{E}$ is the lift of an elliptic curve over $\mathbb{F}_p$, then we'll certainly have $\log|\Delta| \gg \log p$. Then there's the further difficulty that Mestre proves (subject to various "standard" conjectures)

$$\log|\Delta| \gg r \log r,$$

so if we make r large, then the value of Δ (and hence B) will be enormous.

The next step is to see how this theoretical analysis, which is essentially given by Miller [23], compares to actual practice.

4. High Rank Curves With Small Height Points

It is difficult to find elliptic curves over $\mathbb{Q}$ with high rank, as witnessed by the fact that no curves of rank 12 were known before 1982 [22], and even today the highest rank known is 23 [19].

Currently the most successful method for finding curves of high rank is to start on a one or two-parameter family such that every member of the family already contains many independent points, and then specialize to find certain members which possess even higher rank. However, this method is not suitable for our purposes, because we are starting with a curve over $\mathbb{F}_p$ that we want to lift, so we need more freedom than is provided by such a family. Thus we are going to consider an earlier method of Mestre which can be applied in great generality. Mestre's idea is simple to state, although the justification for why it should yield high rank curves depends on much deep mathematics and several unproven conjectures:

Mestre's Construction

In order to produce a curve $\mathcal{E}/\mathbb{Q}$ of high rank, use congruence conditions to choose the coefficients of $\mathcal{E}$ so that $\#\mathcal{E}(\mathbb{F}_\ell)$ is maximized for all (small) primes $\ell = 2, 3, 5, \ldots, \ell_0$, and then so that the discriminant $|\Delta(\mathcal{E})|$ is more-or-less minimized subject to the congruence conditions. Then search for integer points lying close to the rightmost real two-torsion point $(e_1, 0)$, say searching for points (x, y) with $e_1 < x < e_1 + 5000$. We will call a curve chosen according to these criteria a *Mestre curve*. The precise algorithm for constructing Mestre curves is described in [22], and some justification for the algorithm is given in [21].

In his original paper [22], Mestre lists the smallest curves of ranks 4 to 12 which he found using the above method. Two of the listings appear to have typographical errors, and for the remaining curves we gather some information in Table 1, where $P_1, \ldots, P_r$ denotes a basis for $E(\mathbb{Q})$.

Table 1. Data for Mestre's moderate rank curves

r	$\dfrac{(\operatorname{Reg}\mathcal{E})^{1/r}}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\min\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\max\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\dfrac{\log\lvert\Delta\rvert}{r\log r}$
4	0.612	0.772	0.844	2.382
5	0.627	0.840	0.941	2.362
6	0.600	0.937	0.994	2.295
7	0.696	1.032	1.063	2.116
8	0.776	1.103	1.128	2.111
9	0.543	1.051	1.073	2.311
10	0.756	1.091	1.106	2.271
12	0.674	0.916	0.923	2.273
14	0.585	1.018	1.025	2.341

A first observation (from Mestre's paper) is that the curves constructed by his method generally have square-free, or almost square-free, discriminant. This is very reasonable, because Mestre's bound for the rank alluded to above actually has the form

$$r \log r \ll \log(\operatorname{Cond}\mathcal{E}),$$

where the conductor $\operatorname{Cond}\mathcal{E}$ is (essentially) the square-free part of Δ. Thus having a large square dividing the discriminant will make it more difficult for the curve to have large rank.

A second observation, this time from Table 1, is that the independent points constructed by Mestre's method seem to satisfy

$$\hat{h}(P_i) \approx \frac{1}{12}\log|\Delta|.$$

We can justify this observation as follows. Mestre's method yields points $P = (x, y) \in \mathcal{E}(\mathbb{Q})$ which have integer coordinates $x, y \in \mathbb{Z}$ and which are fairly close to the 2-torsion point $T = (e_1, 0)$. The local decomposition of the canonical height says that

$$\hat{h}(P) = \hat{\lambda}_\infty(P) + \sum_p \hat{\lambda}_p(P).$$

(See [34, chapter VI] for the definition and basic properties of the local height functions $\hat{\lambda}_p$.) Assuming that the discriminant Δ is (mostly) square-free and that the coordinates of P are integers, the p-adic local heights add up to give (approximately) $\frac{1}{12}\log|\Delta|$, see [34, VI.4.1]. Further, the fact that P is close to T means that $\hat{\lambda}_\infty(P) \approx \hat{\lambda}_\infty(T)$, which yields

$$\hat{h}(P) \approx \hat{\lambda}_\infty(T) + \frac{1}{12}\log|\Delta|.$$

Finally, the explicit formula [34, VI.3.4] for $\hat{\lambda}_\infty$ shows that

$$\hat{\lambda}_\infty(T) = \log^+|j(\mathcal{E})| + O(1),$$

which will tend to be fairly small. (For explicit estimates, see [36, 37].)

An additional point to make is that the value $\frac{1}{12}\log|\Delta|$ is essentially the smallest possible value for $\hat{h}(P)$ on a Mestre curve, since the fact that the discriminant is square-free means that all of the $\hat{\lambda}_p(P)$'s satisfy

$$\hat{\lambda}_p(P) \ge \frac{1}{12}\operatorname{ord}_p(\Delta)\log p,$$

and if the coordinates of P have denominators and/or P moves further away from e_1, then the value of $\hat{h}(P)$ will tend to increase. It is thus not surprising that the points constructed by Mestre's method tend to be independent, since they represent vectors of approximately the same length L in a lattice whose smallest non-zero vector also has length L. To see why this is true, consider s vectors $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_s \in \mathbb{R}^r$ satisfying $|\mathbf{v}_i - \mathbf{v}_j| \ge L$ and $|\mathbf{v}_i| = L$ for all $i \ne j$. Then the balls of radius L around each $|\mathbf{v}_i|$ are disjoint, and they are contained in a ball of radius $2L$, so a simple volume counting argument shows that $r \ge \log_2(s)$.

The data in Table 1 indicates that

$$\min \hat{h}(P) \approx \frac{1}{12}\log|\Delta(\mathcal{E})| \quad \text{and} \quad \frac{1}{24}\log|\Delta(\mathcal{E})| \le \operatorname{Reg}(\mathcal{E})^{1/r} \le \frac{1}{15}\log|\Delta(\mathcal{E})|. \tag{8}$$

A reasonable assumption, based on this data, would be that it is possible to find Mestre curves of various ranks with

$$\operatorname{Reg}(\mathcal{E})^{1/r} \approx \frac{1}{20}\log|\Delta(\mathcal{E})|. \tag{9}$$

Using this and the other material described above, we obtain the following (heuristic) result:

Heuristic Bound. *Based on the numerical data contained in* [21] *and the above theoretical analysis, it appears to be possible to use Mestre's method to produce elliptic curves* $\mathcal{E}/\mathbb{Q}$ *so that the number of rational points*

$$N(\mathcal{E}, B) = \#\{P \in \mathcal{E}(\mathbb{Q}) \,:\, H(x(P)) \le B\}$$

in $\mathcal{E}(\mathbb{Q})$ *grows like*

$$N(\mathcal{E}, B) \approx \frac{1}{\sqrt{\pi r}} \left(\frac{20\pi e \log B}{r \cdot \log |\Delta(\mathcal{E})|} \right)^{r/2}. \tag{10}$$

Further, it is probably not possible to find elliptic curves such that $N(\mathcal{E}, B)$ *grows significantly faster than this rate.*

Remark.. We also observe from Table 1 that the discriminant tends to satisfy

$$2r \log r \le \log |\Delta(\mathcal{E})| \le 3r \log r,$$

but since for the ECDL problem we will need to impose an extra congruence condition modulo a "large" prime p, we will not use this condition directly. However, it is important to point out that this estimate implies that the generating points on a Mestre curve generally satisfy

$$\hat{h}(P) \approx \frac{1}{12} \log |\Delta(\mathcal{E})| \ge \frac{r \log r}{6}.$$

Comparing this to the analogous estimate (4) for the multiplicative group, we see that the size of the generating elements for a rank r group is exponentially worse in the elliptic curve case!

5. Lifting Mod p Curves to High Rank Curves

It's now time to put into practice the theoretical material contained in the previous sections. Table 2 lists the results of some experiments we performed using Mestre's method to lift a curve over $\mathbb{F}_p$ to a curve of moderate rank. We chose to use $p = 173$ and more-or-less randomly took the curve

$$E : y^2 = x^3 + 42x + 86.$$

(We did choose E so that $\#E(\mathbb{F}_{173}) = 158$ is small, which has the effect of making Mestre's method a little less efficient.) Although not strictly necessary, the algorithm described in [22] uses curves of a slightly different form, so we changed coordinates to the isomorphic curve

$$E : y^2 + y = x^3 + 42x + 129$$

over the field $\mathbb{F}_{173}$. We then used Mestre's method to look for lifts of this curve which have the maximum number of points modulo all primes ≤ 23, and among

these curves looked for independent integral points on the ones having small discriminant. The result was that of 269280 curves tested, there were three examples of rank 6 and three examples of rank 7. The relevant data for these six curves is listed in Table 2.

Table 2. Lifting From Mod 173 To Moderate Rank

r	$\dfrac{(\operatorname{Reg}\mathcal{E})^{1/r}}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\min\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\max\limits_i \dfrac{\hat{h}(P_i)}{\frac{1}{12}\log\lvert\Delta\rvert}$	$\dfrac{\log\lvert\Delta\rvert}{r\log r}$
6	0.702	0.849	0.948	5.823
6	0.722	0.890	0.965	5.859
6	0.673	0.854	0.942	6.252
7	0.670	0.908	0.937	4.651
7	0.686	0.891	0.952	4.712
7	0.672	0.861	0.971	4.956

Comparing Table 2 to Table 1, we see that the relationship between the regulator, the discriminant, and the minimal and maximal heights of the generators are more-or-less the same in both tables. Not surprisingly, what has changed is that for a given rank, the discriminant is much larger in Table 2 than it is in Table 1. This is very reasonable, since Table 1 imposes no prior restrictions on the coefficients of $\mathcal{E}$, while in Table 2 we are forcing the coefficients of $\mathcal{E}$ to have specific values modulo 173. This means that the discriminant of $\mathcal{E}$ should be forced upwards by some power of p.

A reasonable assumption is that $\log|\Delta|$ will grow linearly in both $\log p$ and in $r\log r$ (the latter from Mestre's results and Table 1), say

$$\log|\Delta| \approx c_1 \log p + c_2 r \log r.$$

Fitting the data in Table 2 to this formula (note $p = 173$), we find the best fit is

$$\log|\Delta| \approx 11.93 \log p + 0.26 r \log r. \tag{11}$$

(Note that for our subsequent analysis, it would make little difference if c_1 were to be reduced to, say, 5.)

Now suppose we want to solve the ECDL problem for a given prime p by using Mestre's method to lift $E/\mathbb{F}_p$ to a curve $\mathcal{E}/\mathbb{Q}$ of moderately large rank. Looking at the Heuristic Bound (10), in order to have a reasonable chance of lifting a point of $E(\mathbb{F}_p)$ to a point of $\mathcal{E}(\mathbb{Q})$ of height at most B, we need $N(\mathcal{E}, B)$ fairly close to p, say $N(\mathcal{E}, B) \ge p/2^{10}$. Then (10) and (11) give us the lower bound

$$\log B \ge \frac{r\log(p^{11.93} r^{0.26r})}{20\pi e} \left(\frac{p\sqrt{\pi r}}{2^{10}}\right)^{2/r}. \tag{12}$$

The following table gives, for various values of p, the value of r which minimizes this lower bound and the corresponding lower bound for B.

Table 3. Best Lower Bound for B in (12)

p	r	$B \geq$	$B \geq$
2^{20}	15	$2^{72.63}$	$p^{3.63}$
2^{40}	40	$2^{398.08}$	$p^{9.95}$
2^{80}	87	$2^{1823.54}$	$p^{22.79}$
2^{120}	134	$2^{4297.13}$	$p^{35.81}$
2^{160}	180	$2^{7830.74}$	$p^{48.94}$

We thus see that for any reasonable size prime p (for cryptographic purposes, one would certainly never use a prime smaller than 2^{80}), the smallest allowable B is a substantial power of p. For the sake of argument, we will make the optimistic assumption that we can take $B = p^{20}$, but as the table makes clear, the true value of B is likely to be much larger. We will also suppose, again being optimistic, that it is possible to find a suitable lift $\mathcal{E}/\mathbb{Q}$ whose rank is on the order of 100 to 200, despite the fact that no curves of rank ≥ 24 are currently known.

However, even for $B = p^{20}$ and a curve $\mathcal{E}/\mathbb{Q}$ with known generators $P_1, \ldots, P_r$, we are confronted with the second enormous challenge posed in Miller's paper. Namely, how do we lift a given point on $E(\mathbb{F}_p)$ to a point on $\mathcal{E}(\mathbb{Q})$, even if we know that there is such a lift with height less than p^{20}? Certainly we don't want to check all suitable linear combinations $\sum n_i P_i$, since this is no better than a brute-force search through a set with $N(\mathcal{E}, B)$ elements, and we've chosen B so that $N(\mathcal{E}, B) \gg\ll p$. On the other hand, we could try to lift the given point p-adically, that is, first lift mod p^2, then mod p^3, etc. If we could do this correctly, then when we lift modulo p^{20}, we will have found the desired point in $\mathcal{E}(\mathbb{Q})$, since we know that the x-coordinate of the desired point has height less than p^{20}. Unfortunately, as Miller points out, at each step in this p-adic lifting process, we are faced with p possible lifts for each lift in the previous step. Since there is no (known) method for deciding a priori which of the lifts will lead to an actual point in $\mathcal{E}(\mathbb{Q})$, this method leads to a tree with p^{20} nodes to check, clearly not a feasible task.

Of course, if the lifting problem could be efficiently solved for (say) $p \approx 2^{160}$ and $B = p^{100} \approx 2^{16000}$, either by p-adic or other methods, then it might be feasible to solve "real-world" ECDL problems using the index calculus. However, the numbers involved are so staggeringly large that it seems very unlikely that this lifting problem has a practical solution.

The key point here is that it is necessary to choose B to be a substantial power of p in order to have enough points of height $\leq B$ to cover most of $E(\mathbb{F}_p)$, and for such a large B, there is no method other than a brute force search to find the desired lift of a given point in $E(\mathbb{F}_p)$. If it had been possible to cover $E(\mathbb{F}_p)$ with points of $\mathcal{E}(\mathbb{Q})$ having height at most (say) $\sqrt{p}$, which is essentially what happens for the discrete logarithm problem in the multiplicative group, or even

height at most p, then quite possibly there is a good (i.e., efficient) way of lifting points. But the fact that the generators for $\mathcal{E}(\mathbb{Q})$ have height $\gg\ll r \log r$, as compared with height $\gg\ll \log r$ in the multiplicative case, means that we cannot hope to cover $E(\mathbb{F}_p)$ with points of $\mathcal{E}(\mathbb{Q})$ having such small height. This, then, explains why it is very unlikely that there is an index calculus for elliptic curve discrete logarithms which is directly analogous to the classical index calculus for the multiplicative group.

References

1. Adleman, L., *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, Proc. 20th IEEE Found. Comp. Sci. Symp., 1979, pp. 55–60.
2. L. Adleman, J. DeMarrais and M. Huang,, *A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields*, Algorithmic Number Theory, Lecture Notes in Computer Science, volume 877, Springer-Verlag, 1994, pp. 28–40.
3. A.O. Atkins, *The number of points on an elliptic curve modulo a prime*, preprint, 1988.
4. R. Balasubramanian and N. Koblitz,, *The improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm*, Journal of Cryptology (to appear).
5. Canfield, E.R., Erdös, P., Pomerance, C., *On a problem of Oppenheim concerning 'Factorisation Numerorum'*, Journal Number Theory **17** (1983), 1–28.
6. Certicom White Paper, *Remarks on the security of the elliptic curve cryptosystem*, `www.certicom.com/ecc/wecc3.htm` .
7. T. ElGamal, *A public-key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Transactions on Information Theory **31** (1985), 469–472.
8. N. Elkies, *Explicit isogenies*, preprint, 1991.
9. G. Frey and H. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Mathematics of Computation **62** (1994), 865–874.
10. D. Gordon, *Discrete logarithms in GF(p) using the number field sieve*, SIAM Journal on Discrete Mathematics **6** (1993), 124–138.
11. M. Hindry and J. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450.
12. N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48** (1987), 203–209.
13. ———, *CM-curves with good cryptographic properties*, Advances in Cryptology - CRYPTO '91, Lecture Notes in Computer Science, volume 576, Springler-Verlag, 1992, pp. 279–287.
14. Kraitchik, M., *Théorie des Nombres*, volume 1, Gauthier-Villars, 1922.
15. ———, *Reserches sur la théorie des nombres*, Gauthier-Villars, 1924.
16. B.A. LaMacchia and A.M. Odlyzko, *Computation of discrete logarithms in prime fields*, Designs, Codes and Cryptography **1** (1991), 47–62.
17. S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.
18. ———, *Elliptic Curves: Diophantine Analysis*, Springer-Verlag, New York, 1978.
19. R. Martin and W. McMillen, *An elliptic curve over $\mathbb{Q}$ with rank at least 23*, announcement, June 1997.
20. A. Menezes, T. Okamoto and S. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639–1646.
21. J.F. Mestre, *Formules explicites et minoration de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.
22. ———, *Constructiuon d'une courbe elliptique de rang* ≥ 12, C.R. Acad. Sc. Paris **t. 295** (1982), 643–644.

23. V.S. Miller, *Use of elliptic curves in cryptography*, Advances in Cryptology CRYPTO '85 (Lecture Notes in Computer Science, vol. 218), Springer-Verlag, 1986, pp. 417–426.
24. A. Miyaji, *On ordinary elliptic curve cryptosystems*, Advances in Cryptology - ASIACRYPT '91, Lecture Notes in Computer Science, volume 218, Springer-Verlag, 1993, pp. 460–469.
25. S. Pohlig and M. Hellman, *An improved algorithm for computing logarithms over GF(p) and its cryptographic significance*, IEEE Transactions on Information Theory **24** (1978), 106–110.
26. J. Pollard, *Monte Carlo methods for index computation mod p*, Mathematics of Computation **32** (1978), 918–924.
27. H. H. Rück, *On the discrete logarithms on some elliptic curves*, preprint, 1997.
28. T. Satoh and K. Araki, *Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves*, preprint.
29. O. Schirokauer, D. Weber, and Th. Denny, *Discrete logarithms: The effectiveness of the index calculus method*, Algorithmic Number Theory, (ANTS-II, Talence, France, 1996), Lect. Notes in Computer Sci., vol. 1122, Springer-Verlag, 1996, pp. 337–362.
30. R. Schoof, *Elliptic curves over finite fields and the computation of square roots modulo p*, Math. Comp. **44** (1985), 483–494.
31. I. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Mathematics of Computation **67** (1998), 353–356.
32. V. Shoup, *Lower bounds for discrete logarithms and related problems*, Advances in Cryptology - EUROCRYPT '97, Lecture Notes in Computer Science, volume 1233, Springer-Verlag, 1997, pp. 256–266.
33. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986.
34. ———, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 151, Springer-Verlag, Berlin and New York, 1994.
35. ———, *Lower bound for the canonical height on elliptic curves*, Duke Math. J. **48** (1981), 633–648.
36. ———, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **192** (1990), 723–743.
37. ———, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358.
38. ———, *Computing canonical heights with little (or no) factorization*, Math. Comp. **66** (1997), 787–805.
39. N. Smart, *Announcement of an attack on the ECDLP for anomalous elliptic curves*, preprint, 1997.
40. J. Solinas, *An improved algorithm for arithmetic on a family of elliptic curves*, Advances in Cryptology - CRYPTO '97, Lecture Notes in Computer Science, volume 1294, Springer-Verlag, 1997, pp. 357–371.
41. J. Voloch, *The discrete logarithm problem on elliptic curves and descents*, preprint, 1997.
42. Weber, D., *Computing discrete logarithms with the general number field sieve*, Algorithmic Number Theory, (ANTS-II, Talence, France, 1996), Lect. Notes in Computer Sci., vol. 1122, Springer-Verlag, 1996, pp. 391–403.
43. A.E. Western and J.C.P. Miller, *Tables of Indices and Primitive Roots*, Royal Society Mathematical Tables, vol. 9, Cambridge Univ. Press, 1968.