THE XEDNI CALCULUS AND THE ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM [PRELIMINARY VERSION]

Joseph H. Silverman

Brown University

August 3, 1998 (revised October 5, 1998)

Abstract. Let $E/\mathbb{F}_p$ be an elliptic curve defined over a finite field, and let $S, T \in E(\mathbb{F}_p)$ be two points on E. The *Elliptic Curve Discrete Logarithm Problem* (ECDLP) asks to find an integer m so that $S = mT$ in $E(\mathbb{F}_p)$. In this note we give a new algorithm, dubbed the xedni calculus, which might be used to solve the ECDLP. As remarked by Neal Koblitz, the xedni method is also applicable to the classical discrete logarithm problem for $\mathbb{F}_p^*$ and to the integer factorization problem.

Introduction

Let $E/\mathbb{F}_p$ be an elliptic curve defined over a finite field, and let $S, T \in E(\mathbb{F}_p)$ be two points on E. The *Elliptic Curve Discrete Logarithm Problem* (ECDLP) asks to find an integer m so that $S = mT$ in $E(\mathbb{F}_p)$. This problem is considered to be very difficult to solve if p is large, for which reason it has formed the basis for various cryptographic constructions, such as [8, 14].

Typeset by $\mathcal{A}_\mathcal{M}\mathcal{S}$-TEX

The analogous problem for the multiplicative group $\mathbb{F}_p^*$, called the *Discrete Logarithm Problem* (DLP), has also been much studied. The most efficient method known for solving the DLP is called the *Index Calculus*. However, no practical Index Calculus method has been found for the ECDLP, and indeed it seems likely for both theoretical and practical reasons (see [14, 21]) that the ECDLP does not admit an Index Calculus.

In this note we will describe a new algorithm, dubbed the *Xedni Calculus*, which might be used to solve the ECDLP. I want to stress the word "might" in the previous sentence. A fair test of the Xedni Calculus will require state-of-the-art programming and equipment, and it does not appear that testing small examples with inefficient programs will yield much, if any, useful data. To make a possibly inaccurate analogy from the theory of factorization, the advantages of the number field sieve over the quadratic sieve only become apparent in practice when applied to large examples. Unfortunately, this analogy is incomplete, since it is at least possible to prove that the number field sieve is asymptotically better then the quadratic sieve. For the Xedni Calculus, one of the steps is sufficiently heuristic to so far resist the necessary quantification. The particular step in question is the use of Mestre's congruence/high rank method (in reverse) to increase the likelihood that certain elliptic curves have smaller than expected rank.

To explain the relationship between the Xedni Calculus and the Index Calculus, we first briefly describe the latter. To apply the Index Calculus to the ECDLP, one would first lift the elliptic curve $E/\mathbb{F}_p$ to an elliptic curve $\mathcal{E}/\mathbb{Q}$, next attempt to lift various points from $E(\mathbb{F}_p)$ to $\mathcal{E}(\mathbb{Q})$, and finally use relationships among these lifts to solve the ECDLP. (For details, see for example [21].) The difficulties are twofold. First, one needs to lift $E/\mathbb{F}_p$ to a curve $\mathcal{E}/\mathbb{Q}$ having many independent rational points of small height. Second, one needs to lift points from $E(\mathbb{F}_p)$ to $\mathcal{E}(\mathbb{Q})$. Both of these are very difficult problems, probably more difficult than the original ECDLP. Further, even if one could find curves $\mathcal{E}/\mathbb{Q}$ of very high rank, there are good theoretical reasons for believing that the generators of $\mathcal{E}(\mathbb{Q})$ will never be small enough to allow the lifting problem to be solved in subexponential time.

The Xedni Calculus turns this procedure on its head, whence its name. First we choose points $P_1, \dots, P_r$ in $E(\mathbb{F}_p)$ and lift them to points $Q_1, \dots, Q_r$ having integer coordinates. Next we choose an elliptic curve $\mathcal{E}/\mathbb{Q}$ which goes through the points $Q_1, \dots, Q_r$. This is simple linear algebra, so the problem of lifting curves and points from $\mathbb{F}_p$ to $\mathbb{Q}$ has become trivial because we've lifted the points first and then forced the curve to go through the points. Finally, we check if the points $Q_1, \dots, Q_r$ are dependent in $\mathcal{E}(\mathbb{Q})$. If they are, the ECDLP is almost certainly solved. Thus the goal in the Xedni Calculus is to find an instance where an elliptic curve has *smaller* than the expected rank. This is presumably easier than the Index Calculus problem of producing elliptic curves over $\mathbb{Q}$ of very large rank.

Unfortunately, work of Néron [15] and Masser [11] suggests that a set of points $Q_1, \dots, Q_r$ as constructed above will usually be independent. So we introduce one more crucial idea. Mestre [13] has described a congruence method for producing elliptic curves of large rank. Although partially heuristic, the justification for Mestre's algorithm uses deep methods and conjectures from analytic number theory and arithmetic geometry. We apply Mestre's method *in reverse* to make it more likely that the lifted curve $\mathcal{E}$ has smaller than expected rank.

Now a few words about the organization of this paper. The first part gives a description of the Xedni algorithm. It is entirely self-contained. Interspersed throughout this part are brief "Implementation Notes" and "Theoretical Notes." The former give some ideas for implementing the algorithm, the latter briefly describe the purpose of each step.

The remainder of the paper consists of a number of appendices, some fairly lengthy, giving further information of various sorts, including more detailed theoretical justification and/or implementation strategies for the different steps. The appendices are reasonably independent of one another, so the reader may choose to read only those which are of interest. In other words, a note to "See Appendix XYZ for further details" should be treated as a hypertext link, to be followed if and when the reader actually desires to peruse additional information on the given topic.

Remark. Neal Koblitz [9] has observed that the Xedni Calculus might be applied to computational problems other than the ECDLP, namely to the classical discrete logarithm problem (DLP) for the multiplicative group $\mathbb{F}_p^*$ and to the problem of factoring large integers. We will describe Koblitz' ideas in Appendix K. Note, however, that unless the Xedni Calculus turns out to be more efficient than the Index Calculus or than sieve methods, this remark is of purely theoretical interest, since subexponential methods for solving DLP and integer factorization are already known. On the other hand, Xendi integer factorization appears to be an entirely distinct method from Lenstra's elliptic curve factorization algorithm [10].

Remark. One might also ask if the Xedni Calculus applies to the ECDLP for elliptic curves defined over a field $\mathbb{F}_q$, where $q = p^N$ is a large power of a small prime p, for example $p = 2$. There are two possible ways to proceed. We could take a number field K whose ring of integers R contains a prime $\mathfrak{p}$ satisfying $R/\mathfrak{p} = \mathbb{F}_q$ and apply the Xedni Calculus algorithm directly to obtain lifted points and a lifted curve $\mathcal{E}/K$. If $\mathcal{E}(K)$ has smaller than expected rank, then the ECDLP will be solved. The main difficulty with this approach is that one must perform many algebraic computations in the ring R, which may be very difficult. However, on the bright side, if R contains many primes of small norm (e.g., if 3 and 5 split completely in R), then there are many more small primes to use for Mestre's method, which might help.

A second possibility in this situation is to work over a global function field $K = \mathbb{F}_q(T)$. We thus suppose that the original curve $E/\mathbb{F}_q$ is the reduction of a curve $\mathcal{E}/K$ at $T = 0$, and we construct the lifted points and curve so that $\mathcal{E}$ has a small number of points modulo various primes of $\mathbb{F}_q[T]$. One difficulty with this method is the problem of finding some curves over $\mathbb{F}_q$ having a small number of points, but this would only need to be done once and could then be used for every ECDLP over $\mathbb{F}_q$.

Acknowledgments. I would like to thank Armand Brumer, John Cremona, Jeff Hoffstein, Neal Koblitz, Keith Matthews, Alfred Menezes, David Rohrlich, and Nigel Smart for their many helpful comments and even more helpful criticisms of this work.

Addendum. While writing this note, I received a communication from Jung Hee Cheon (ETRI) and Sang Guen Hahn and Dr. Hwanjoon Kim (KAIST) in which they describe an idea similar to the Xedni Calculus, although without many of the refinements described in this note. I have also been told that Nigel Smart and Nelson Stephens (unpublished) considered some similar ideas a few years ago.

Description of the Xedni Algorithm

Notation.
We set the following notation, which will remain fixed throughout this paper.

$\mathbb{F}_p$ the finite field of p elements, p prime.

$E_p/\mathbb{F}_p$ an elliptic curve defined over $\mathbb{F}_p$, given by a Weierstrass equation

$$E_p : y^2 + a_{p,1}xy + a_{p,3}y = x^3 + a_{p,2}x^2 + a_{p,4}x + a_{p,6}. \qquad (1)$$

N_p $= \#E_p(\mathbb{F}_p)$, the number of points in $E(\mathbb{F}_p)$.

S, T two points in $E_p(\mathbb{F}_p)$.

The *elliptic curve discrete logarithm problem* (ECDLP) is the problem of determining, for a given (p, E_p, S, T), the integer

$$m = m(S,T) = \log_T(S)$$

such that

$$S = mT \quad \text{in } E_p(\mathbb{F}_p).$$

Implementation Note. For simplicity, we will generally assume that the group $E(\mathbb{F}_p)$ is cyclic, and sometime even that N_p is prime.

For any set of r triples $P_i = [x_i, y_i, z_i]$, $1 \le i \le r$, define an r-by-10 matrix $\mathbf{B} = \mathbf{B}(P_1, \dots, P_r)$ of cubic monomials

$$\mathbf{B} = \begin{pmatrix} x_1^3 & x_1^2y_1 & x_1y_1^2 & y_1^3 & x_1^2z_1 & x_1y_1z_1 & y_1^2z_1 & x_1z_1^2 & y_1z_1^2 & z_1^3 \\ x_2^3 & x_2^2y_2 & x_2y_2^2 & y_2^3 & x_2^2z_2 & x_2y_2z_2 & y_2^2z_2 & x_2z_2^2 & y_2z_2^2 & z_2^3 \\ \vdots & & & \ddots & & & \ddots & & & \vdots \\ x_r^3 & x_r^2y_r & x_ry_r^2 & y_r^3 & x_r^2z_r & x_ry_rz_r & y_r^2z_r & x_rz_r^2 & y_rz_r^2 & z_r^3 \end{pmatrix}$$

Thus the i^{th} row of $\mathbf{B}$ consists of the 10 cubic monomials in the three variables x_i, y_i, z_i.

Step 1. Fix an integer $4 \le r \le 9$ and an integer M which is a product of small primes.

Implementation Note. The integer r is the number of points to be lifted. The integer M is the product of the primes for which auxiliary congruence conditions will be imposed. For further details concerning the choice of r, see Appendix J. For the selection of M, see Appendices B and D.

Theoretical Note. It does not appear to be possible to increase the value of r beyond 9, since a general cubic in $\mathbb{P}^2$ is determined by 9 points. Notice the same holds true for the genus 1 curves obtained as a general intersection of two quadrics in $\mathbb{P}^3$.

We also remark that one can restrict to particular cubics. For example, a (general) Weierstrass equation can be forced to go through up to 6 arbitrary points, thereby simplifying some of the subsequent calculations. However, it is probably better to use equations whose coefficients are as small as possible, which means using families of genus 1 curves having the maximum number of undetermined coefficients. This is the reason for our using general cubic curves in $\mathbb{P}^2$.

Step 2. Choose r points

$$P_{M,i} = [x_{M,i}, y_{M,i}, z_{M,i}], \qquad 1 \le i \le r,$$

satisfying:

(i) the first 4 points are $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, and $[1,1,1]$.

(ii) for every prime $\ell | M$, the matrix $\mathbf{B}(P_{M,1}, \dots, P_{M,r})$ has maximal rank modulo ℓ.

Further choose coefficients $u_{M,1}, \dots, u_{M,10}$ so that the points $P_{M,1}, \dots, P_{M,r}$ satisfy the congruence

$$\begin{aligned} &u_{M,1}x^3 + u_{M,2}x^2y + u_{M,3}xy^2 + u_{M,4}y^3 + u_{M,5}x^2z \\ &\quad + u_{M,6}xyz + u_{M,7}y^2z + u_{M,8}xz^2 + u_{M,9}yz^2 + u_{M,10}z^3 \equiv 0 \pmod{M}. \end{aligned} \tag{2}$$

Remark. Condition (i) tells us that $u_{M,1} = u_{M,4} = u_{M,10} = 0$ and that the other coefficients sum to 0 modulo M, but for expository purposes, we will leave all 10 coefficients labeled.

Implementation Note. The idea is to make these choices so that the congruence (2) has the smallest possible number of solutions modulo M subject to conditions (i) and (ii). Note that for any particular prime ℓ, it is easy enough to impose conditions modulo ℓ so as to force (2) to have a small number of solutions modulo ℓ. Then one can use the Chinese Remainder Theorem to find values for the $u_{M,j}$'s modulo M.

The choice of the $P_{M,i}$'s may impose certain constraints on the linear relations satisfied by the subsequent lifted points, so some care is needed in making these choices.

We also note that it may not be useful, or even possible, to impose conditions modulo the very smallest primes. For example, a (smooth) elliptic curve over $\mathbb{F}_2$ can have no more than 5 points, so if $r \ge 6$, then we must take M to be odd. For further information concerning the choice of curves and points modulo M, see Appendix E.

Theoretical Note. Mestre's method [13] for producing elliptic curves of moderately high rank is to impose congruence conditions on the Weierstrass coefficients so as to force the curve to have the maximal number of points modulo ℓ for all small primes (say all $\ell \le 19$ or $\ell \le 37$). Mestre explains why his algorithm works by giving an explicit formula for the rank which involves many deep conjectures and theorems in analytic number theory and arithmetic geometry including especially the conjecture of Birch and Swinnerton-Dyer and the Modularity Conjecture (now largely proven by Wiles [23]). One similarly sees from Mestre's formula that if an elliptic curve has a small number of points modulo ℓ for many small primes, then its rank is likely to be smaller than expected. This is the heuristic justification for Step 2 of the Xedni Calculus. For further details concerning Mestre's method and explicit formula, see Appendix I.

Step 3. Choose r random pairs of integers (s_i, t_i) satisfying $1 \le s_i, t_i < N_p$, and for each $1 \le i \le r$, compute the point $P_{p,i} = (x_{p,i}, y_{p,i})$ defined by

$$P_{p,i} = s_i S - t_i T \in E_p(\mathbb{F}_p).$$

Implementation Note. We will assume that $P_{p,i} \ne 0$ and $P_{p,i} \ne \pm P_{p,j}$ for all $i \ne j$, since otherwise the ECDLP is almost certainly already solved.

Step 4. Make a change of variables in $\mathbb{P}^2$ of the form

$$\begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \alpha_{13} \\ \alpha_{21} & \alpha_{22} & \alpha_{23} \\ \alpha_{31} & \alpha_{32} & \alpha_{33} \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \tag{3}$$

so that the first four points become

$$P_{p,1} = [1,0,0], \quad P_{p,2} = [0,1,0], \quad P_{p,3} = [0,0,1], \quad P_{p,4} = [1,1,1].$$

The equation for E_p will then have the form

$$u_{p,1}x^3 + u_{p,2}x^2y + u_{p,3}xy^2 + u_{p,4}y^3 + u_{p,5}x^2z \\ + u_{p,6}xyz + u_{p,7}y^2z + u_{p,8}xz^2 + u_{p,9}yz^2 + u_{p,10}z^3 = 0.$$

(As in Step 2, we actually have $u_{p,1} = u_{p,4} = u_{p,10} = 0$ and the other $u_{p,i}$'s sum to zero modulo p.)

Implementation Note. The change of variables matrix (3) is easily computed by solving a system of 8 homogeneous equations in 9 variables over the field $\mathbb{F}_p$. If the system turns out to be incompatible, then three of the four points $P_{p,1},\dots,P_{p,4}$ will be collinear, so will sum to O in $E_p(\mathbb{F}_p)$, in which case the ECDLP is almost certainly solved.

Step 5. Use the Chinese Remainder Theorem to find integers $u'_1,\dots,u'_{10}$ satisfying

$$u'_i \equiv u_{p,i} \pmod{p} \quad\text{and}\quad u'_i \equiv u_{M,i} \pmod{M} \qquad \text{for all } 1 \le i \le 10.$$

Step 6. Lift the chosen points to $\mathbb{P}^2(\mathbb{Q})$. In other words, choose points

$$P_i = [x_i, y_i, z_i], \quad 1 \le i \le r,$$

with integer coordinates satisfying

$$P_i \equiv P_{p,i} \pmod{p} \quad\text{and}\quad P_i \equiv P_{M,i} \pmod{M} \quad \text{for all } 1 \le i \le r. \tag{4}$$

In particular, take $P_1 = [1,0,0]$, $P_2 = [0,1,0]$, $P_3 = [0,0,1]$, and $P_4 = [1,1,1]$.

Implementation Note. Note that the congruences (4) take place in $\mathbb{P}^2$. They can be solved using the Chinese Remainder Theorem, and then an extended gcd-type algorithm can be used to find solutions with small coordinates. See Appendix A for details.

Step 7. Let $\mathbf{B} = \mathbf{B}(P_1,\dots,P_r)$ be the matrix of cubic monomials defined earlier. Consider the system of linear equations

$$\mathbf{B}\mathbf{u} = \mathbf{0}. \tag{5}$$

Find a small integer solution $\mathbf{u} = [u_1,\dots,u_{10}]$ to (5) which has the additional property

$$\mathbf{u} \equiv [u'_1, u'_2, \dots, u'_{10}] \pmod{Mp}. \tag{6}$$

Here $u'_1,\dots,u'_{10}$ are the coefficients computed in Step 5.

Let $C_{\mathbf{u}}$ denote the associated cubic curve

$$C_{\mathbf{u}} : u_1x^3 + u_2x^2y + u_3xy^2 + u_4y^3 + u_5x^2z \\ + u_6xyz + u_7y^2z + u_8xz^2 + u_9yz^2 + u_{10}z^3 = 0. \quad (7)$$

Theoretical Note. By construction, we have the following three facts:

- Formula (4) in Step 6 ensures that the points $P_1, \dots, P_r$ are lifts of the original points $P_{p,1}, \dots, P_{p,r}$.
- Formula (6) in Step 7 ensures that the curve $C_{\mathbf{u}}$ is a lift of the original curve E_p (after the change of coordinates from Step 4).
- Formula (5) in Step 7 ensures that the curve $C_{\mathbf{u}}$ contains the points $P_1, \dots, P_r$.

Thus the lifting problems inherent in the Index Calculus do not appear in the Xedni Calculus. (Of course, there is a new problem, namely trying to force the lifted points to be dependent.)

Implementation Note. The existence of a solution to (5) satisfying (6) is guaranteed by condition (ii) in Step 2 and an elementary algebraic lemma. An efficient method to construct small solutions has been described by Matthews [12] as an extension of [6]. See Appendix B for details.

Theoretical Note. It is this step which militates against taking r to have the maximum value of 9, because we would like the coefficients of the curve $C_{\mathbf{u}}$ to be of moderate size. A rough "back-of-the-envelope" calculation suggests that there should exist solutions to (5) and (6) with magnitude

$$\max |u_i| = O\big((Mp)^{3r/(20-2r)}\big).$$

Thus taking $r = 9$ gives coefficients that are $O((Mp)^{27/2})$, while $r = 4, 5, 6$ give coefficients that are $O(Mp)$, $O((Mp)^{3/2})$ and $O((Mp)^{9/4})$ respectively. See Appendix J for further details.

Step 8. Make a change of coordinates to put $C_{\mathbf{u}}$ into standard minimal Weierstrass form with the point $P_1 = [0, 0, 1]$ the point at infinity. Write the resulting equation as

$$E_{\mathbf{u}} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (8)$$

with $a_1, \dots, a_6 \in \mathbb{Z}$, and let $Q_1, Q_2, \dots, Q_r$ denote the images of $P_1, \dots, P_r$ under this change of coordinates (so in particular, $Q_1 = O$). Let $c_4(\mathbf{u})$, $c_6(\mathbf{u})$, and $\Delta(\mathbf{u})$ be the usual quantities [18, III §1] associated to the equation (8).

Implementation Note. A simple algorithm for making this change of coordinates is given in Appendix C (or see [2, Algorithm 7.4.10] or [3]). However, if the coefficients of $C_{\mathbf{u}}$ are very large, we note that it may be possible to implement the remainder of the algorithm (other than some of the optional steps) without finding an explicit equation for $E_{\mathbf{u}}$. Also note that it is worthwhile checking that the resulting equation is minimal at small primes, but one should just assume that the equation is already minimal at all other primes.

Step 9 (Optional). Find a small integer basis $\mathbf{v}_1, \dots, \mathbf{v}_{10-r}$ for the solutions to the system of linear equations (5) in Step 7. For each of the 3^{10-r} choices of integers $\varepsilon_1, \dots, \varepsilon_{10-r} \in \{-1, 0, 1\}$, let

$$\tilde{\mathbf{u}} = \mathbf{u} + \varepsilon_1 Mp\mathbf{v}_1 + \varepsilon_2 Mp\mathbf{v}_2 + \cdots + \varepsilon_{10-r} Mp\mathbf{v}_{10-r}$$

and compute the corresponding elliptic curve $E_{\tilde{\mathbf{u}}}$ and minimal discriminant $\Delta(\tilde{\mathbf{u}})$ as in Step 8. If any $|\Delta(\tilde{\mathbf{u}})|$ is smaller than $|\Delta(\mathbf{u})|$, replace $\mathbf{u}$ by $\tilde{\mathbf{u}}$ and repeat. This will lead to an elliptic curve of the desired form whose discriminant is in some sense locally minimized.

Implementation Note. A small basis for $\mathbf{BU} = \mathbf{0}$ may be found using the LLL algorithm, and indeed will probably already have been determined in Step 7.

Theoretical Note. Mestre [13] has found that his algorithm is most likely to produce curves of high rank if the discriminant is minimized subject to the specified congruence conditions on the coefficients. It is likely that the same will hold true for producing curves of smaller than expected rank, which is the reason for this step. In principle, one could write $|\Delta(\tilde{\mathbf{u}})|$ as a function of the variables $\varepsilon_1, \dots, \varepsilon_{10-r}$ and numerically minimize the resulting function, but the difficulty of this minimization probably outweighs the benefit.

Step 10 (Optional). For some moderate value of L, compute the sum

$$\sum_{\ell \le L,\, \ell \nmid M} \frac{a_\ell(E_{\mathbf{u}})}{\ell - 1}. \tag{9}$$

If (9) is smaller than a pre-determined quantity, return to Step 2 or 3. Otherwise continue with the next step.

Implementation Note. It is probably not worth doing this step unless the values of $a_\ell(E_{\mathbf{u}})$ can be obtained by a simple table lookup, which means precomputing their values. For some suggestions for useful precomputations, see Appendix H.

Theoretical Note. The idea of computing the sum (9) as an indicator of high rank is again due to Mestre [13], and is again based on his explicit formula. Mestre wants high rank, so he discards the curve if the sum is too large; we want low rank, so we discard the curve if the sum is too small. The particular cut-off value needs to be determined experimentally, although by treating the $a_\ell/(\ell-1)$'s as independent random variables, one can get some theoretical idea of the likely spread. For further theoretical details on Mestre's method, see Appendix I.

Step 11. Check if the points $Q_2, \dots, Q_r \in E_{\mathbf{u}}(\mathbb{Q})$ are independent. If they are independent, return to Step 2 or 3. Otherwise compute a relation of dependence

$$n_2 Q_2 + n_3 Q_3 + \cdots + n_r Q_r = O, \tag{10}$$

set

$$n_1 = -n_2 - n_3 - \cdots - n_r,$$

and continue with the next step.

Implementation Note. There are two ways to perform this step. The *Descent Method* chooses a set of auxiliary primes $\mathcal{Q}$, looks at the (easily computed) map

$$E_{\mathbf{u}}(\mathbb{Q})/2E_{\mathbf{u}}(\mathbb{Q}) \longrightarrow \prod_{q \in \mathcal{Q}} E_{\mathbf{u}}(\mathbb{F}_q)/2E_{\mathbf{u}}(\mathbb{F}_q) \cong \mathbb{F}_2^K$$

and uses quadratic reciprocity and linear algebra over $\mathbb{F}_2$. The *Height Method* computes the determinant of the canonical height regulator $\langle Q_i, Q_j \rangle_{2 \le i,j \le r}$ and (if the regulator is approximately 0) uses LLL to find a small linear relation on the columns. The Descent Method will generally be faster, especially if one precomputes the reducible cubic polynomials in $\mathbb{F}_q[X]$ for $q \in \mathcal{Q}$. However, we note that the Height Method is a feasible alternative because it is possible to compute canonical heights without knowing a complete factorization of the discriminant [19, 20]. For details of the Descent Method, see Appendices D and G. For a further discussion of the Height Method, see Appendix F. For precomputation suggestions, see Appendix H.

Theoretical Note. Under the change-of-variables isomorphism $C_{\mathbf{u}} \cong E_{\mathbf{u}}$ from Step 8, we have $P_i \leftrightarrow Q_i$ and $Q_1 = O$. The linear relation (10) is thus equivalent to the linear equivalence of divisors

$$n_2\big((Q_2) - (Q_1)\big) + \big((Q_3) - (Q_1)\big) + \cdots + n_r\big((Q_r) - (Q_1)\big) \sim 0,$$

so we get the relation $n_1(P_1) + n_2(P_2) + \cdots + n_r(P_r) \sim 0$ on $C_{\mathbf{u}}$.

Step 12. Compute

$$s = \sum_{i=1}^{r} n_i s_i \qquad \text{and} \qquad t = \sum_{i=1}^{r} n_i t_i.$$

(Recall $s_1, s_2, \ldots, t_r$ were chosen in Step 3.) If $\gcd(s, N_p) > 1$, return to Step 2 or 3. Otherwise compute an inverse $ss' \equiv 1 \pmod{N_p}$. Then

$$\log_T(S) \equiv s't \pmod{N_p},$$

and the ECDLP is solved.

Implementation Note. Naturally, one should check that $S = mT$ in $E_p(\mathbb{F}_p)$ with $m \equiv s't \pmod{N_p}$. We note that there is a tiny possibility that the system (5) had less than maximal rank modulo p, which could lead to an erroneous value for m.

Theoretical Note. If $1 < \gcd(s, N_p) < N_p$, then one gains some partial information which may be used to help solve the ECDLP. However, for cryptographic purposes one will probably have N_p prime, so this remark is of purely theoretical interest.

This concludes the description of the Xedni Algorithm.

Appendix A. Lifting Points to $\mathbb{Z}$

Step 6 requires us to lift points in $\mathbb{P}^2$ modulo p and modulo M to a (small) point in $\mathbb{P}^2(\mathbb{Q})$. More generally, suppose that we are given points $Q_j = [\alpha_j, \beta_j, \gamma_j]$, $1 \le j \le J$, with integer coordinates and we want to find a point $Q = [\alpha, \beta, \gamma]$ with small coordinates satisfying

$$Q \equiv Q_j \pmod{m_j} \quad \text{in } \mathbb{P}^2 \qquad \text{for all } 1 \le j \le J.$$

We assume the m_j's are pairwise relatively prime, and we let $m = m_1 m_2 \cdots m_J$. The first step is to use the Chinese Remainder Theorem to find integers a, b, c satisfying

$$a \equiv \alpha_j \pmod{m_j}, \quad b \equiv \beta_j \pmod{m_j}, \quad c \equiv \gamma_j \pmod{m_j}, \quad \text{for all } 1 \le j \le J.$$

This gives a point in $\mathbb{P}^2(\mathbb{Q})$ with the desired congruence property. Next we consider the lattice generated by the columns of the matrix

$$\begin{pmatrix} a & m & 0 & 0 \\ b & 0 & m & 0 \\ c & 0 & 0 & m \end{pmatrix}.$$

Using LLL (or some more direct method), we find a small vector $[\alpha, \beta, \gamma]$ in this lattice. Then

$$[\alpha, \beta, \gamma] \equiv d[a, b, c] \pmod{m}$$

for some integer d, so $[\alpha, \beta, \gamma]$ and $[a, b, c]$ represent the same point in $\mathbb{P}^2(\mathbb{Q})$. If $\gcd(d, m) = 1$, then they reduce to the same point mod m, and we are done. Otherwise, we find a (small) basis for the kernel of the matrix and use it to adjust $[a, b, c]$.

Appendix B. Making the Curve Fit the Points

We begin with an elementary algebra lemma which explains why condition (ii) in Step 2 ensures the existence of a solution to (5) satisfying (6).

Lemma. *Let V and W be lattices, let $A : V \to W$ be a linear transformation of rank r, and assume that the quotient W/AV is finite. (Equivalently, assume that $r = \operatorname{rank} W = \operatorname{rank} AV$, or that $A : V \otimes \mathbb{Q} \to W \otimes \mathbb{Q}$ is surjective.) Let*

$$\gamma(A) = \#(W/AV) = \gcd(r \times r \textit{ minors of } A),$$

and for any integer $N \geq 1$, let

$$A_N : V/NV \longrightarrow W/NW$$

be the map induced by A modulo N. Then the following are equivalent.
(i) $\operatorname{rank} A_p = r$ *for every prime* $p|N$.
(ii) $\gcd(N, \gamma(A)) = 1$.
(iii) *The natural map* $\ker(A) \to \ker(A_N)$ *is surjective.*
(iv) *The multiplication-by-N map* $W/AV \xrightarrow{N} W/AV$ *is injective.*

Proof. Consider the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & V & \xrightarrow{N} & V & \longrightarrow & V/NV & \longrightarrow & 0 \\ & & {\scriptstyle A}\downarrow & & {\scriptstyle A}\downarrow & & {\scriptstyle A_N}\downarrow & & \\ 0 & \longrightarrow & W & \xrightarrow{N} & W & \longrightarrow & W/NW & \longrightarrow & 0 \end{array}$$

Applying the Snake Lemma gives the long exact sequence

$$0 \longrightarrow \ker A \xrightarrow{N} \ker A \longrightarrow \ker A_N \longrightarrow \frac{W}{AV} \xrightarrow{N} \frac{W}{AV} \longrightarrow \frac{W}{NW + AV} \longrightarrow 0.$$

Hence

$$\ker A \longrightarrow \ker A_N \longrightarrow \ker\left(\frac{W}{AV} \xrightarrow{N} \frac{W}{AV}\right) \longrightarrow 0,$$

so we see that the map $\ker A \to \ker A_N$ is surjective if and only if the map $W/AV \xrightarrow{N} W/AV$ is injective. This shows that (iii) and (iv) are equivalent. Further, since $\gamma(A) = \#(W/AV)$, it is clear that (iv) and (ii) are equivalent.

Finally, choose bases for V and W and write A as an $r \times n$ matrix with integer coefficients, where $r \le n$. Let $A_1, A_2, \dots, A_k$ be the $r \times r$ submatrices of A. Then condition (ii) says that

$$\gcd(N, \det A_1, \det A_2, \dots, \det A_k) = 1,$$

while condition (i) says that for each prime $p|n$, there is some i so that $\det A_i \not\equiv 0 \pmod{p}$. Hence (i) and (ii) are equivalent.

Now we observe that Step 7 asks us to solve a system of equations $\mathbf{Bu} = \mathbf{0}$ subject to an auxiliary congruence condition $\mathbf{u} \equiv \mathbf{u}' \pmod{Mp}$. Note that the definition of the matrix $\mathbf{B}$ and the congruence conditions in Step 5 tell us that $\mathbf{Bu}' \equiv \mathbf{0} \pmod{Mp}$. In the notation of the Lemma, the vector $\mathbf{u}'$ is in $\ker(\mathbf{B}_{Mp})$, the kernel of the reduction of $\mathbf{B}$ modulo Mp. Further, condition (ii) in Step 2 says that $\mathbf{B}_\ell$ has maximal rank for every prime ℓ dividing M; and since p is a large prime, it is probably true that $\mathbf{B}_p$ will also have maximal rank. (The probability that a randomly chosen matrix 10-by-r matrix has less than maximal rank modulo p is $O(1/p^{11-r})$.) Applying the Lemma, we see that the desired solution almost certainly exists.

Having established the existence of a solution, we need a method to efficiently compute a small solution. We start with the known solution $\mathbf{Bu}' \equiv \mathbf{0} \pmod{Mp}$. Lifting the coordinates of $\mathbf{u}'$ to $\mathbb{Z}$, this means that $\mathbf{Bu}' = Mp\mathbf{v}$ for some vector $\mathbf{v}$ having integer coordinates. The Lemma and our various assumptions tell us that there exists an integer solution to the inhomogeneous equation

$$\mathbf{Bw} = \mathbf{v}, \tag{11}$$

and then the desired solution is $\mathbf{u} = \mathbf{u}' - Mp\mathbf{w}$. So the question comes down to finding a small solution to an inhomogeneous equation such as (11).

I would like to thank Keith Matthews [12] for explaining the following method to me.

Inhomogeneous Equation Algorithm. Let $\mathbf{B}$ be an m-by-n matrix with integer coordinates, and let $\mathbf{b} \in \mathbb{Z}^m$. The following algorithm determines if the inhomogeneous equation $\mathbf{Bx} = \mathbf{b}$ has any solutions, and determines a small solution if solutions exist.

(1) Apply the (Havas-Majewski-Matthews) Hermite Normal form algorithm [6] to the matrix
$$G = \begin{pmatrix} \mathbf{B}^t & 0 \\ \mathbf{b}^t & 1 \end{pmatrix}.$$
Call the result $\mathrm{HNF}(G)$, and let U be the associated unimodular transformation matrix. In other words, $\mathrm{HNF}(G) = UG$.

(2) Compute $H = \mathrm{HNF}(\mathbf{B}^t) = \binom{\mathbf{C}}{0}$, where C consists of the nonzero rows of H.

(3) If the equation $\mathbf{Bx} = \mathbf{b}$ has a solution, then $\mathrm{HNF}(G)$ and U will look like

$$\mathrm{HNF}(G) = \begin{pmatrix} \mathbf{C} & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \text{and} \qquad U = \begin{pmatrix} * & 0 \\ -\mathbf{y}^t & 1 \\ * & 0 \end{pmatrix}, \tag{12}$$

and $\mathbf{y}$ is the desired small solution to $\mathbf{By} = \mathbf{b}$.

(4) If $\mathrm{HNF}(G)$ does not have the form specified in (12), then the original equation has no solutions.

Appendix C. Transforming a Cubic to Weierstrass Form

In this section we briefly describe how to transform a cubic curve in $\mathbb{P}^2$ with a known non-inflexional rational point into a cubic curve in Weierstrass form. Let C be a cubic plane curve given by an equation

$$C : s_1U^3 + s_2U^2V + s_3UV^2 + s_4V^3 + s_5U^2W + s_6UVW + s_7V^2W \\ + s_8UW^2 + s_9VW^2 + s_{10}W^3 = 0$$

We make the following assumptions:

(1) The point $P_0 = [0, 0, 1]$ is on C (equivalently $s_{10} = 0$).

(2) The coefficient $s_8 \neq 0$.

In general, if $[0, 0, 1] \notin C(\mathbb{Q})$, then the known point in $C(\mathbb{Q})$ should first be moved to $[0, 0, 1]$. Then if $s_8 = 0$, the U and V variables should be switched, which has the effect of switching s_8 and s_9. (If both $s_8 = s_9 = 0$, then C is singular at $[0, 0, 1]$.)

Step I. The tangent line to C at P_0 is the line $L_0 : s_8U + s_9V = 0$. Make the transformation

$$U \leftarrow U - s_9V, \qquad V \leftarrow s_8V, \qquad W \leftarrow W.$$

The tangent line is now $L_0 : U = 0$, and C has the form

$$C : s_1U^3 + s_2U^2V + s_3UV^2 + s_4V^3 + s_5U^2W + s_6UVW + s_7V^2W \\ + s_8UW^2 = 0$$

(Note we are abusing notation by writing $s_1, \ldots , s_8$ for the recomputed values, a practice which we will continue in subsequent steps.)

Step II. The intersection of L_0 and C consists of the point P_0 (with multiplicity 2) and the third point $P_1 = [0, -s_7, s_4]$. Make the transformation

$$U \leftarrow U, \qquad V \leftarrow s_7V, \qquad W \leftarrow -s_4V + W.$$

The point P_1 is now at $[0, 1, 0]$, and C has the form

$$C : s_1U^3 + s_2U^2V + s_3UV^2 + s_5U^2W + s_6UVW + s_7V^2W + s_8UW^2 = 0.$$

(Note we are assuming that $s_1 \neq 0$. If $s_1 = 0$, then the line L_0 is already an inflection line to C, which means that we can put C into Weierstrass form directly using a linear transformation of $\mathbb{P}^2$.)

Step III. The tangent line to C at P_1 is the line $L_1 : s_3U + s_7W = 0$. Make the transformation

$$U \leftarrow s_7U, \qquad V \leftarrow V, \qquad W \leftarrow -s_3U + W.$$

The tangent line is now $L_1 : W = 0$, and C has the form

$$C : s_1U^3 + s_2U^2V + s_5U^2W + s_6UVW + s_7V^2W + s_8UW^2 = 0.$$

Step IV. Make the birational transformation

$$U \leftarrow XZ, \qquad V \leftarrow YZ, \qquad W \leftarrow X^2.$$

Canceling X^2Z, we obtain an equation of the form

$$E : s_1XZ^2 + s_2YZ^2 + s_5X^2Z + s_6XYZ + s_7Y^2Z + s_8X^3 = 0.$$

This is in Weierstrass form. Dehomogenizing

$$X \leftarrow -x, \qquad Y \leftarrow y, \qquad Z \leftarrow 1$$

gives the affine form

$$E : s_7y^2 - s_6xy + s_2y = s_8x^3 - s_5x^2 + s_1x.$$

Step V. Make the substitution

$$x \leftarrow \frac{x}{s_8s_7}, \qquad y \leftarrow \frac{y}{s_8s_7^2}.$$

Multiply by $s_8^2s_7^3$ to obtain a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x.$$

Finally, check if E is minimal at small primes and, if not, make an appropriate change of variables to minimize the equation.

Remark. The inverse of the birational transformation in Step IV is the map

$$X \leftarrow UW, \qquad Y \leftarrow VW, \qquad Z \leftarrow U^2.$$

Remark. It is not hard to give a rough upper bound for the size of the coefficients of the curve E in Step IV in terms of the original curve C. More interesting is the expected size of the discriminant of E in Step V. The following table gives the results of some numerical tests. In this table we use the notation

$$\begin{aligned} h(C) &= \log_2 \max |s_i| \\ h_{\mathrm{nm}}(E) &= \tfrac{1}{12} \log_2 |\Delta(E)| \quad \text{for non-minimal equation in Step V} \\ h_c(E) &= \tfrac{1}{12} \log_2 \max\{|c_4|, |c_6|\} \\ h_\Delta(E) &= \tfrac{1}{12} \log_2 |\Delta(E)| \end{aligned}$$

Each line represents the average of 50 trials using s_i's chosen randomly with $\log_2 |s_i|$ smaller than the indicated value for $h(C)$.

$h(C)$	$h_{\mathrm{nm}}(E)/h(C)$	$h_c(E)/h(C)$	$h_\Delta(E)/h(C)$
13.161	8.905	11.065	7.839
19.777	9.145	11.706	8.368
26.413	9.178	11.987	8.640
33.046	9.274	12.268	8.870
39.655	9.289	12.378	8.976
46.333	9.324	12.440	9.026
52.975	9.363	12.547	9.112
59.651	9.380	12.527	9.083

The last three columns of the table seem to be increasing very slowly, so we conclude that if the coefficients of the cubic C are on the order of t bits, then the discriminant of the final Weierstrass equation E will generally have around $110t$ bits. (Remember that $h_\Delta(E)$ is $\log|\Delta|$ divided by 12.)

Appendix D. Checking Independence via 2-Descent

In this section we let $\mathcal{E}/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation

$$\mathcal{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, \dots, a_6 \in \mathbb{Z}, \tag{13}$$

and we let

$$P_i = (x_i, y_i) \in \mathcal{E}(\mathbb{Q}), \quad 1 \le i \le r,$$

be a collection of rational points on $\mathcal{E}$. We will describe a 2-Descent Algorithm which will determine if $P_1, \dots, P_r$ are independent and, if not, will give an equation of dependence. I would like to thank Armand Brumer and John Cremona for suggesting this material to me.

The basic idea is to first check if $P_1, \dots, P_r$ are independent in $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$. If they are, then they are also independent in $\mathcal{E}(\mathbb{Q})$, and we are done. If not, then there is a relation

$$\varepsilon_1 P_1 + \cdots + \varepsilon_r P_r \equiv O \pmod{2\mathcal{E}(\mathbb{Q})} \quad \text{for some } \varepsilon_1, \dots, \varepsilon_r \in \{0, 1\} \text{ not all zero.}$$

This means that there is a point $Q \in \mathcal{E}(\mathbb{Q})$ with

$$2Q = \varepsilon_1 P_1 + \cdots + \varepsilon_r P_r. \tag{14}$$

Note that we can find Q using exact arithmetic, although if $\mathcal{E}(\mathbb{Q})[2] \ne 0$, there will be more than one possible choice for Q. To ease our exposition, we will assume that $\mathcal{E}(\mathbb{Q})[2] = 0$, so Q is uniquely determined. We then pick an index j with $\varepsilon_j = 1$, replace P_j by Q, and repeat the procedure. There are two possibilities.

First, if $P_1, \dots, P_r$ are actually independent, then after just a few iterations we end up with a set of points which are independent in $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$, since each iteration is producing a set of points whose span is strictly larger than the previous set. This allows us to conclude that $P_1, \dots, P_r$ are independent.

Second, if $P_1, \dots, P_r$ are actually dependent, then the above procedure may not terminate. What happens is that each iteration produces a rational point Q which is substituted for one of the points in the current collection. Thus we obtain a potentially infinite sequence of points $P_1, \dots, P_r, Q_1, Q_2, Q_3, \dots$. However, it is easy to check that the heights of these points are bounded, so fairly rapidly we will see some point appearing twice in our list. When this happens, it signals that the original points were dependent, and as long as we have kept a record of the points and relations (14), it is not hard to construct a non-trivial relation among $P_1, \dots, P_r$. (See Appendix G for details.)

There remains the question of determining whether a collection of points is independent in the quotient $\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q})$. The idea is to map into a product of local quotients $\mathcal{E}(\mathbb{Q}_q)/2\mathcal{E}(\mathbb{Q}_q)$ for an appropriately chosen set of small odd primes $q = q_1, q_2, \dots, q_n$. We choose these primes to have the property that $\mathcal{E}(\mathbb{F}_q)[2] \ne 0$, or equivalently, so that the congruence

$$4x^3 + b_2x^2 + 2b_4x + b_6 \equiv 0 \pmod{q} \tag{15}$$

has a solution. (Here b_2, b_4, b_6 are the usual quantities associated to (13), see [18, III §1].) On general principles, the congruence (15) will have exactly one root for approximately 1/2 of all primes, and will have three roots for approximately 1/6 of all primes. For ease of exposition, we will fix one solution $x \equiv \alpha_j \pmod{q_j}$ to (15) for each $1 \le j \le n$; but in practice, if (15) has three roots, it is more efficient to use two of them in the following discussion. Also for simplicity, we will assume that $\mathcal{E}$ has good reduction at q, or equivalently, that (15) does not have a double root.

For any odd prime q, let ψ_q denote the quadratic residue map

$$\psi_q : \mathbb{F}_q^{\times} \longrightarrow \mathbb{F}_2, \qquad \beta \longmapsto \begin{cases} 0 & \text{if } \beta \in \mathbb{F}_q^{\times\,2}, \\ 1 & \text{if } \beta \notin \mathbb{F}_q^{\times\,2}. \end{cases}$$

Now for each $q = q_j$, we let $\alpha = \alpha_j$ and consider the following composition of maps:

$$\begin{array}{ccccccccc} \dfrac{\mathcal{E}(\mathbb{Q})}{2\mathcal{E}(\mathbb{Q})} & \rightarrow & \dfrac{\mathcal{E}(\mathbb{Q}_q)}{2\mathcal{E}(\mathbb{Q}_q)} & \xrightarrow[\text{mod } q]{\text{reduction}} & \dfrac{\mathcal{E}(\mathbb{F}_q)}{2\mathcal{E}(\mathbb{F}_q)} & \rightarrow & \dfrac{\mathbb{F}_q^{\times}}{\mathbb{F}_q^{\times\,2}} & \xrightarrow[\sim]{\psi_q} & \mathbb{F}_2 \\ & & & & (x,y) & \rightarrow & x - \alpha & & \end{array}$$

General theory tells us that each of these maps is a homomorphism (cf. [18, X §4]), so we obtain a homomorphism

$$\phi_q : \frac{\mathcal{E}(\mathbb{Q})}{2\mathcal{E}(\mathbb{Q})} \longrightarrow \mathbb{F}_2, \qquad P = (x,y) \longmapsto \begin{cases} \psi_q(x-\alpha) & \text{if } \operatorname{ord}_q(x) \ge 0, \\ 0 & \text{if } \operatorname{ord}_q(x) < 0. \end{cases}$$

Combining these homomorphisms for $q_1, \dots, q_n$ yields a homomorphism

$$\Phi : \frac{\mathcal{E}(\mathbb{Q})}{2\mathcal{E}(\mathbb{Q})} \longrightarrow \mathbb{F}_2^n, \qquad P \longmapsto (\phi_{q_1}(P), \phi_{q_2}(P), \dots, \phi_{q_n}(P)).$$

Further, the homomorphism Φ is easy to compute, since it involves nothing more than finding some roots modulo q of the polynomial (15) and then computing some quadratic residue symbols modulo the various q's. Finally, we observe that checking whether a set of images $\Phi(P_1), \dots, \Phi(P_r)$ are independent in $\mathbb{F}_2^n$ is simply linear algebra over the finite field $\mathbb{F}_2$, so is fast and easy to implement.

We want to choose n large enough to ensure, or at least make it quite likely, that Φ is injective on the subgroup of $\mathcal{E}(\mathbb{Q})$ generated by the given r points $P_1, \dots, P_r$. Making a reasonable independence assumption, the following proposition gives the answer.

Proposition. *Let $\phi_1, \phi_2, \dots, \phi_n : \mathbb{Z}^r \to \mathbb{F}_2$ be randomly chosen homomorphisms. Then the probability that the induced map*

$$\Phi = (\phi_1, \dots, \phi_n) : (\mathbb{Z}/2\mathbb{Z})^r \longrightarrow \mathbb{F}_2^n$$

is injective is

$$\prod_{i=0}^{r-1} \left(1 - \frac{1}{2^{n-i}}\right).$$

Proof. Since a homomorphism $\mathbb{Z}^r \to \mathbb{F}_2$ must factor as $\mathbb{Z}^r \to (\mathbb{Z}/2\mathbb{Z})^r \to \mathbb{F}_2$, we see that the sample space for the map induced by Φ is the set

$$\Phi \in \mathrm{Home}(\mathbb{Z}^r, \mathbb{F}_2)^n \cong \mathrm{Home}(\mathbb{F}_2^r, \mathbb{F}_2^n).$$

In other words, we may consider Φ to be an r-by-n matrix with coefficients in $\mathbb{F}_2$, and the induced map is injective if and only if the matrix has rank r. Hence the probability that a random Φ induces an injective map is the number of n-by-r matrices over $\mathbb{F}_2$ having rank r divided by the total number of such matrices. Using the standard formulas

$$\#\{n\text{-by-}r \text{ matrices over } \mathbb{F}_2\} = 2^{nr},$$
$$\#\{n\text{-by-}r \text{ matrices over } \mathbb{F}_2 \text{ of rank } r\} = (2^n-1)(2^n-2)(2^n-2^2)\cdots(2^n-2^{r-1}),$$

gives the stated result.

Using this proposition, Table 1 gives the probability that Φ induces an injective map for $r = 4, 6, 9$ and various values of n.

	$n = 9$	$n = 12$	$n = 15$	$n = 18$	$n = 21$
$r = 4$	97.09%	99.63%	99.95%	99.99%	99.99%
$r = 6$	88.18%	98.47%	99.81%	99.98%	99.99%
$r = 9$	28.94%	88.03%	98.45%	99.81%	99.98%

Table 1. Probability That Φ Induces an Injective Map

Appendix E. Selection of Auxiliary Primes

In this section we discuss in more detail the selection of the integer M, the points $P_{M,i}$ and the curve (2) in Steps 1 and 2. More precisely, we begin by fixing a square-free integer M. Then, for each prime $\ell | M$, we choose points

$$P_{\ell,i} = [x_{\ell,i}, y_{\ell,i}, z_{\ell,i}], \qquad 1 \le i \le r,$$

and a cubic congruence

$$E_\ell : u_{\ell,1}x^3 + u_{\ell,2}x^2y + u_{\ell,3}xy^2 + u_{\ell,4}y^3 + u_{\ell,5}x^2z + u_{\ell,6}xyz + u_{\ell,7}y^2z + u_{\ell,8}xz^2 + u_{\ell,9}yz^2 + u_{\ell,10}z^3 \equiv 0 \pmod{\ell}. \quad (16)$$

going through the chosen points. Finally, we use the Chinese Remainder Theorem to combine the mod ℓ points and curves into a points and a curve modulo M.

We set the notation

$$N_\ell = E_\ell(\mathbb{F}_\ell),$$

and we observe that the Hasse-Weil estimate for the first few primes says that $N_2 \le 5$, $N_3 \le 7$, and $N_5 \le 10$.

The first step is to choose the squarefree integer M. A natural choice is to take M to be the product of the first few primes, say all primes $\ell \le L_1$. However, we need to contend with condition (ii) in Step 2, which says that the r-by-10 matrix $\mathbf{B}(P_{\ell,1}, \ldots, P_{\ell,r})$ must have maximal rank (i.e., rank r) modulo ℓ. In particular, the curve $E_\ell/\mathbb{F}_\ell$ must satisfy $N_\ell \ge r$, so if $r \ge 6$, then we must take $2 \nmid M$, and if $r \ge 8$, we must take $3 \nmid M$.

However, even for smaller values of r, we may not want to impose conditions at the very smallest primes. For example, suppose that we take $r = 6$. Then it is possible to choose a curve $E_3/\mathbb{F}_3$ with $N_3 = 6$, but we will not have gained a great deal by doing so, since in any case $\#E(\mathbb{F}_3) \le 7$ for every elliptic curve $E/\mathbb{F}_3$. On the other hand, imposing a condition modulo 3 means that $3|M$, which will make the coefficients of the lifted curve $\mathcal{E}/\mathbb{Q}$ correspondingly larger. There is thus a tradeoff in whether or not to take M divisible by the first few primes. (Of course, if we don't impose a condition modulo 3, say, then it is possible that $\mathcal{E}$ will actually have bad reduction modulo 3, but it's not clear that bad reduction at a few small primes will affect matters very much.) We will thus let

$$M = \prod_{L_0 \le \ell \le L_1} \ell,$$

where the values of L_0 and L_1 need to be experimentally determined. Reasonable choices might be $L_0 = 3$, 5, or 7, and L_1 chosen so that M and p are of the same order of magnitude (or at least, say, $p^{1/2} \le M \le p^{3/2}$). Table 2 gives the value of M for some typical choices of L_0 and L_1.

$L_0 \backslash L_1$	29	43	61	79	101	113	139	163
3	$2^{31.59}$	$2^{52.54}$	$2^{75.63}$	$2^{100.34}$	$2^{126.45}$	$2^{153.47}$	$2^{181.71}$	$2^{210.81}$
5	$2^{30.01}$	$2^{50.95}$	$2^{74.05}$	$2^{98.76}$	$2^{124.87}$	$2^{151.88}$	$2^{180.12}$	$2^{209.22}$
7	$2^{27.68}$	$2^{48.63}$	$2^{71.73}$	$2^{96.44}$	$2^{122.55}$	$2^{149.56}$	$2^{177.80}$	$2^{206.90}$
11	$2^{24.88}$	$2^{45.82}$	$2^{68.92}$	$2^{93.63}$	$2^{119.74}$	$2^{146.75}$	$2^{174.99}$	$2^{204.09}$

Table 2. Values for $M = \prod_{L_0 \le \ell \le L_1} \ell$

Next we come to the more delicate question of choosing a curve E_ℓ and points $P_{\ell,i}$ for each prime $\ell|M$. For any individual prime ℓ (say with $\ell \ge 5$), it is easy enough to search through the curves

$$E_{a,b} : y^2 = x^3 + ax + b, \qquad 0 \le a, b < \ell,$$

and pick out the curves with

$$\#E_{a,b}(\mathbb{F}_\ell) = \max\{\ell + 1 - 2\sqrt{\ell}, r\}.$$

(Note we need to have at least distinct r points.) We can then choose three of the non-zero points in $E_{a,b}(\mathbb{F}_\ell)$ and move them to the points $[1,0,0]$, $[0,0,1]$, and $[1,1,1]$. (Note we already have the point $[0,1,0]$.) However, we need four the points to be independent in the sense that the sum or difference of any two of them cannot equal zero. Thus it is not necessarily enough to have $\#E_{a,b}(\mathbb{F}_\ell) \ge r$, we also need some independence among the points. For moderate values of ℓ, this is not a problem, but it may not be possible for very small values of ℓ. Thus L_0 must be chosen accordingly.

There is one other important consideration in choosing the points and curves to be lifted, namely we must take care that we don't force the lifted points to be independent. It is a reasonable guess that if the N_ℓ's for $L_0 \le \ell \le L_1$ are more-or-less relatively prime to one another, then the choice of particular points modulo ℓ to be lifted will impose fewer independence constraints than if the N_ℓ's have many factors in common.

ℓ	N_ℓ	a	b
7	**7**	**6**	**5**
11	**7**	**2**	**7**
13	7	0	6
	8	**6**	**1**
17	10	6	0
	11	**8**	**14**
19	12	1	2
	13	**0**	**2**
23	**15**	**16**	**9**
	17	17	11
29	20	19	20
	21	3	12
	23	**25**	**8**

ℓ	N_ℓ	a	b
31	21	0	7
	23	**28**	**25**
37	26	8	0
	29	**33**	**21**
41	30	28	26
	31	**21**	**3**
43	**31**	**0**	**18**
47	35	25	3
	37	**12**	**23**
53	40	28	50
	41	**50**	**6**

Table 3. Curves With Small $N_\ell = \#E(\mathbb{F}_\ell)$

Remark. The curve $E/\mathbb{F}_{13}$ in Table 3 with $\#E(\mathbb{F}_{13}) = 8$ is a cyclic group of order 8.

For concreteness, we will take $L_0 = 7$, $L_1 = 53$, and thus $M \approx 2^{60}$. We will also take the curve E_ℓ to be lifted to have the form

$$E_\ell : y^2 = x^3 + ax + b.$$

Table 3 gives a list of suitable curves having small values of N_ℓ. For each ℓ, we precompute and store r points in $E_\ell(\mathbb{F}_\ell)$; or possibly store more than r points and periodically make a new random choice of r points. Note we can also vary the order in which the points are used. We can also change the curve and the points by picking some $u \in \mathbb{F}_\ell^*$ and replacing (a, b) with $(u^4 a, u^6 b)$ and points (x, y) with $(u^2 x, u^3 y)$. This substitution is an isomorphism over $\mathbb{F}_\ell$, so it has no effect on N_ℓ, but it will affect in an unpredictable way the eventual lift $\mathcal{E}/\mathbb{Q}$.

As mentioned above, it might be good to choose the N_ℓ's to be more-or-less relatively prime to one another. For example, choosing the highlighted curves in Table 3 gives N_ℓ's with few common factors, more precisely, it gives

$$M = 18805115359310280 \quad \text{and} \quad \operatorname*{LCM}_{7 \le \ell \le 53} N_\ell = 3767805121080 = \tfrac{1}{4991} M.$$

One disadvantage of this approach is that the N_ℓ's are chosen somewhat larger than they have to be, although the difference in the Mestre sum (9) for the primes $L_0 \le \ell \le L_1$ is not large. For example, if we let a_ℓ denote the value of $\ell + 1 - N_\ell$ for the highlighted N_ℓ's in Table 3, then we have

$$\sum_{7 \le \ell \le 53} \frac{\lfloor 2\sqrt{\ell} \rfloor}{\ell - 1} \approx 5.5887 \qquad \text{and} \qquad \sum_{7 \le \ell \le 53} \frac{a_\ell}{\ell - 1} \approx 4.2758. \tag{17}$$

On the other hand, it's possible that it will be better to choose the N_ℓ's to have many factors in common. For example, at the other extreme we can choose a set of E_ℓ's from Table 3 to satisfy:

$$N_7 = N_{11} = N_{13} = 7, \quad N_{17} = 10, \quad N_{19} = 12, \quad N_{23} = 15, \quad N_{29} = 20,$$
$$N_{31} = 21, \quad N_{41} = 30, \quad N_{47} = 35, \quad N_{53} = 40,$$

and for $\ell = 37$ and 43, choose $(a, b) = (14, 9)$ and $(34, 18)$ respectively, which give curves satisfying $N_{37} = 28$ and $N_{43} = 35$. Then $\mathrm{LCM}\{N_\ell\} = 840$ and $M = \prod N_\ell \approx 10^{16} \approx 2^{53}$. Further, the Mestre sum (17) increases to $4.6712\ldots$.

However, if the N_ℓ's have many common factors, we must be very careful in choosing the points to be lifted so as not to force the lifted points to be automatically independent. To see what can go wrong, we will analyze a tiny example, say where $M = \ell_1\ell_2\ell_3\ell_4$ is a product of 4 primes, and we are lifting $r = 3$ points. We further suppose that all of the N_ℓ's are even, and (to make life easier) that $E_\ell(\mathbb{F}_\ell)$ is cyclic for each $\ell|M$. Note that we have chosen three points $P_{\ell_i,1}, P_{\ell_i,2}, P_{\ell_i,3}$ for each $i = 1, 2, 3$. Consider the maps

$$\varepsilon_\ell : E_\ell(\mathbb{F}_\ell) \to E_\ell(\mathbb{F}_\ell)/2E_\ell(\mathbb{F}_\ell) \cong \mathbb{F}_2.$$

Eventually we will lift to a curve $\mathcal{E}/\mathbb{Q}$ and lift to points $P_1, P_2, P_3 \in \mathcal{E}(\mathbb{Q})$ and check if P_1, P_2, P_3 are independent. One way to check this independence is to look at the image of the map

$$\mathcal{E}(\mathbb{Q})/2\mathcal{E}(\mathbb{Q}) \longrightarrow \prod_\ell \mathcal{E}(\mathbb{F}_\ell)/2\mathcal{E}(\mathbb{F}_\ell),$$

where the product is over some set of primes. (See Appendix D for more details of this procedure.) Since $\mathcal{E}$ reduces modulo ℓ_i to the curve E_{ℓ_i}, and P_j reduces modulo ℓ_i to the point $P_{\ell_i,j}$, we find that if the 3-by-4 matrix

$$\begin{pmatrix} \varepsilon_{\ell_1}(P_{\ell_1,1}) & \varepsilon_{\ell_2}(P_{\ell_2,1}) & \varepsilon_{\ell_3}(P_{\ell_3,1}) & \varepsilon_{\ell_4}(P_{\ell_4,1}) \\ \varepsilon_{\ell_1}(P_{\ell_1,2}) & \varepsilon_{\ell_2}(P_{\ell_2,2}) & \varepsilon_{\ell_3}(P_{\ell_3,2}) & \varepsilon_{\ell_4}(P_{\ell_4,2}) \\ \varepsilon_{\ell_1}(P_{\ell_1,3}) & \varepsilon_{\ell_2}(P_{\ell_2,3}) & \varepsilon_{\ell_3}(P_{\ell_3,3}) & \varepsilon_{\ell_4}(P_{\ell_4,3}) \end{pmatrix} \tag{18}$$

has rank 3 over $\mathbb{F}_2$, then the points P_1, P_2, P_3 are automatically independent. However, the matrix (18) is predetermined by our choice of curves E_{ℓ_i} and points $P_{\ell_i,1}, P_{\ell_i,2}, P_{\ell_i,3}$. So unless we are careful in choosing the curves and points with N_ℓ's having common factors, we may end up forcing the lifted points to be independent. On the other hand, since the primes ℓ dividing M, the curves E_ℓ, and the points $P_{\ell,i}$ may be preselected before the Xendi algorithm is started, it is possible to analyze this choice at the beginning and make sure it doesn't force too many unwanted independence conditions.

Appendix F. Checking Independence Using Heights

An alternative to the descent algorithm (Appendices D and G) for checking independence, one can instead use the theory of canonical heights. This requires moderately high-precision floating point calculations, so is may well be less efficient than using descent, but we briefly describe the method.

The canonical height is a positive definite quadratic form

$$\hat{h} : E(\mathbb{Q})/E(\mathbb{Q})_{\mathrm{tors}} \longrightarrow \mathbb{R}.$$

The associated bilinear form is

$$\langle P, Q\rangle = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q),$$

and the height regulator of a set of points $P_1, \dots, P_r$ is the determinant

$$\operatorname{Reg}(P_1, \dots, P_r) = \det\big(\langle P_i, P_j\rangle\big)_{1\le i,j\le r}.$$

Notice this involves computing $\frac{1}{2}r(r+1)$ individual canonical heights.

The positive definiteness of $\hat{h}$ gives the equivalence

$$P_1, \dots, P_r \text{ are dependent} \iff \operatorname{Reg}(P_1, \dots, P_r) = 0.$$

However, since the canonical height is a (presumably transcendental) real number, we can only check the vanishing condition numerically. Thus the first step is to compute $\operatorname{Reg}(P_1, \dots, P_r)$ accurate to a few decimal places. If it is non-zero, we conclude that $P_1, \dots, P_r$ are independent and go back to choose new points. If the regulator is (approximately) zero, we look for an (approximate) linear relation with small integer coefficients on the columns of the real matrix $\big(\langle P_i, P_j\rangle\big)_{1\le i,j\le r}$. Methods for computing such relations are well known using lattice reduction methods, see for example [2, §2.7].

It remains to explain how to compute the canonical height $\hat{h}(P)$ of a rational point $P \in E(\mathbb{Q})$. This is done using a decomposition into local heights

$$\hat{h}(P) = \lambda_\infty(P) + \sum_{p \text{ prime}} \lambda_p(P).$$

There are two ways to compute the archimedean piece $\lambda_\infty(P)$. The first, due to Tate and the author ([19], see also [4, §3.4]), is a given by a series with recursively generated coefficients. In order to compute $\hat{h}(P)$ accurate to n decimal places, it more than suffices to take $2n + \log\log H(E)$ terms of the series, where $H(E)$ is the magnitude of the largest coefficient of E. So this method is quite suitable for curves whose coefficients are as large as (say) 10^{1000}. The second method of computing λ_∞ is as the value of a theta function. This method has the advantage that the series for theta functions converges quadratically exponentially, but it has the disadvantage that one must first compute various elliptic integrals (which can also be done quadratically using AGM). For details, see for example [2, Algorithm 7.5.7]. It is not clear which method will be faster in practice, but the former is certainly easier to program.

Next comes the computation of the non-archimedean local heights λ_p. If one knows the primes dividing the discriminant Δ of E, then there is a simple algorithm due to the author ([19], see also [4, §3.4] or [2, Algorithm 7.5.6]). Unfortunately, for the curves appearing in the xedni algorithm, the discriminant will generally be much too large to factor, but it turns out that it is usually possible to compute the total contribution of all of the λ_p's without computing them individually. All that is required is to be able to factor the much smaller quantity $\gcd(c_4, c_6)$. (We mention that when putting E into Weierstrass form as described in Appendix C, the final step of clearing the coefficients of y^2 and x^3 will force a common factor into c_4 and c_6, so this known factor can be removed before trying to factor the gcd.) The complete algorithm for computing the total non-archimedean contribution without factoring Δ is described in [20].

Appendix G. Implementation of the 2-Descent Algorithm

In this appendix we give a pseudocode implementation of the 2-Descent Algorithm described theoretically in Appendix D.

IndependentQ(E, P)
Checks if the points in the list P are independent
Input.
    $E = (a_1, a_2, a_3, a_4, a_6)$ an elliptic curve
    $P = (P_1, \ldots, P_r)$ a list of points in $E(\mathbb{Q})$
Output.
    Returns TRUE if $P_1, \ldots, P_r$ are independent in $E(\mathbb{Q})$
    Returns FALSE if $P_1, \ldots, P_r$ are dependent in $E(\mathbb{Q})$

```
PointList = E(Q)[2]
Begin Loop
  If LinearRelationMod2(E, P) = NULL
    Return TRUE
  Else
    (Q, (ε_1, ..., ε_r)) ← LinearRelationMod2(E, P)
    If Q ∈ PointList
      Return FALSE
    Else
      k ← min{i : ε_i = 1}
      Adjoin P_k + E(Q)[2] to PointList
      P_k ← Q
    EndIf
  EndIf
End Loop
```

Remark.. The expected running time of `IndependentQ` is very small. Assuming Lang's height lower bound conjecture, which by work of Fouvry-Nair-Tenenbaum [5] and Hindry-Silverman [7] is at least true for almost all elliptic curves, the worst-case running time for `IndependentQ` is $O(C^r)$ for an absolute constant C. In practice, `IndependentQ` tends to terminate with just a few iterations of the main loop.

LinearRelation(E, P)
Returns a relation for the list of points P
Input.
    $E = (a_1, a_2, a_3, a_4, a_6)$ an elliptic curve
    $P = (P_1, \ldots, P_r)$ a list of points in $E(\mathbb{Q})$
Output.
    A non-zero r-tuple $(d_1, \ldots, d_r) \in \mathbb{Z}^r$ satisfying
    $d_1P_1 + \cdots + d_rP_r = O$, or NULL if no such relation exists.

```
QList ← Empty Set
Do i = 1, 2, ..., r
  Assign LinearRelationSubroutine(E, QList, P_i) to one of:
    (INDEP, Q, m) ← LinearRelationSubroutine(E, QList, P_i)
    (DEP, n, m) ← LinearRelationSubroutine(E, QList, P_i)
  If INDEP
```

```
      Adjoin Q to QList
      M_ij ← m_j for j = 1, 2, ..., i
    Else DEP
      Set A equal to the matrix
```

$$A = \begin{pmatrix} M_{11} & 0 & & \cdots & 0 \\ M_{21} & M_{22} & 0 & \cdots & 0 \\ \vdots & & \ddots & & \\ M_{i-1,1} & M_{i-1,2} & \cdots & \cdots & M_{i-1,i-1} \\ m_1 & m_2 & \cdots & \cdots & m_{i-1} \end{pmatrix}$$

```
      Compute a non-zero solution v ∈ Z^i to vA = 0
      d_j = v_j for j = 1, 2, ..., i − 1
      d_i = n v_i
      d_j = 0 for j = i + 1, ..., r
      Return (d_1, ..., d_r)
    EndIf
  EndDo i
  Return NULL
```

Remark. The routine `LinearRelation` first computes a sequence of relations

$$\begin{aligned} P_1 &= M_{11}Q_1 \\ P_2 &= M_{21}Q_1 + M_{22}Q_2 \\ &\vdots \qquad\qquad \vdots \\ P_{i-1} &= M_{i-1,1}Q_1 + \cdots + M_{i-1,i-1}Q_{i-1} \end{aligned}$$

where $Q_1, \ldots, Q_{i-1}$ are independent modulo $2E(\mathbb{Q})$. Eventually it gets to a P_i such that $P_1, \ldots, P_i$ are dependent, which gives a relation

$$nP_i = m_1Q_1 + \cdots + m_{i-1}Q_{i-1}.$$

Now eliminating the $i-1$ "variables" $Q_1, \ldots, Q_{i-1}$ from these i equations gives a linear relation on $P_1, \ldots, P_i$.

LinearRelationSubroutine(E, Q, R)

If $Q_1, \ldots, Q_k, R$ are independent, returns $(\text{INDEP}, Q_{k+1}, m)$ with $R = \sum_{j=1}^{k+1} m_jQ_j$ and $Q_1, \ldots, Q_{k+1}$ independent modulo $2E(\mathbb{Q})$.
If $Q_1, \ldots, Q_k, R$ are dependent, returns (DEP, n, m) with $nR = \sum_{j=1}^{k} m_jQ_j$.
It is assumed that $Q_1, \ldots, Q_k$ are independent modulo $2E(\mathbb{Q})$

Input.

```
    E = (a_1, a_2, a_3, a_4, a_6) an elliptic curve
    Q = (Q_1, ..., Q_k) a list of points in E(Q), independent mod 2E(Q)
    R a point in E(Q)
```

Output. (One of the following)

```
    (INDEP, Q_{k+1}, (m_1, ..., m_{k+1})) with R = m_1 Q_1 + ··· + m_{k+1} Q_{k+1}
    (DEP, n, (m_1, ..., m_k)) with nR = m_1 Q_1 + ··· + m_k Q_k
```

```
  RList = Empty Set
```

```
$s \leftarrow 0$;  $R_s \leftarrow R$
While $R_s \notin$ RList And LinearRelationMod2$(R, Q_1, \ldots, Q_k) \neq$ NULL
  Adjoin $R_s$ to RList
  /* Compute $R_s + \sum_j \varepsilon_{sj} Q_j = 2R_{s+1}$ */
  $(R_{s+1}, (1, \varepsilon_{s1}, \varepsilon_{s2}, \ldots, \varepsilon_{sk}))$ = LinearRelationMod2$(R_s, Q_1, \ldots, Q_k)$
  /* Increment $s$ and repeat */
  $s \leftarrow s + 1$
EndWhile
If $R_s \in$ RList
  /* $R, Q_1, \ldots, Q_k$ are dependent, compute a relation */
  Find $t < s$ so that $R_t = R_s$
  $n \leftarrow 2^s - 2^t$
  $m_j \leftarrow 2^t \sum_{i=0}^{s-1} 2^i \varepsilon_{ij} - 2^s \sum_{i=0}^{t-1} 2^i \varepsilon_{ij}$ for $j = 1, 2, \ldots, k$
  Return $(\texttt{DEP}, n, (m_1, \ldots, m_k))$
Else
  /* $R, Q_1, \ldots, Q_k$ are independent, write $R = \sum m_j Q_j + m_{k+1} R_s$ */
  $m_j = -\sum_{i=0}^{t-1} 2^i \varepsilon_{ij}$ for $j = 1, 2, \ldots, k$
  Return $(\texttt{INDEP}, R_s, (m_1, \ldots, m_k, 2^s))$
EndIf
```

Remark. The routine `LinearRelationSubroutine` computes a sequence of relations in $E(\mathbb{Q})$ of the form

$$R_i + \sum_{j=1}^{k} \varepsilon_{ij} Q_j = 2R_{i+1}, \qquad i = 0, 1, \ldots.$$

Substituting these relations into one another gives

$$R_0 = -\sum_{j=1}^{k} \left(\sum_{i=0}^{s-1} 2^i \varepsilon_{ij} \right) Q_j + 2^s R_s. \tag{19}$$

If eventually we find an R_s so that $R_s, Q_1, \ldots, Q_k$ are independent modulo $2E(\mathbb{Q})$, then we set $Q_{k+1} = R_s$, and (19) expresses $R = R_0$ in terms of $Q_1, \ldots, Q_{k+1}$.

Conversely, if we eventually find an R_s which duplicates an R_t for some $t < s$, then we use formula (19) with both s and t to write a multiple of $R_t = R_s$ as a linear combination of $Q_1, \ldots, Q_k$:

$$(2^s - 2^t) R_t = \sum_{j=1}^{k} \left(\sum_{i=t}^{s-1} 2^i \varepsilon_{ij} \right) Q_j. \tag{20}$$

Now multiply (19) (with t in place of s) by $2^s - 2^t$ and substitute in (20) to get after some algebra:

$$(2^s - 2^t) R = \sum_{j=1}^{k} \left(2^t \sum_{i=1}^{s-1} 2^i \varepsilon_{ij} - 2^s \sum_{i=0}^{t-1} 2^i \varepsilon_{ij} \right) Q_j.$$

LinearRelationMod2(E, P)
Returns a relation mod $2E(\mathbb{Q})$ for the list of points P
Input.
    $E = (a_1, a_2, a_3, a_4, a_6)$ an elliptic curve
    $P = (P_1, \ldots, P_r)$ a list of points in $E(\mathbb{Q})$
    n, dimension of space with $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathbb{F}_2^n$
    q_{init}, initial prime to use for $E(\mathbb{Q})/2E(\mathbb{Q}) \to E(\mathbb{F}_q)/2E(\mathbb{F}_q)$
Output.
    A non-zero point $Q \in E(\mathbb{Q})$ and an r-tuple $(\varepsilon_1, \ldots, \varepsilon_r) \in \{0,1\}^r$
    so that $\varepsilon_1 P_1 + \cdots + \varepsilon_r P_r = 2Q$, or NULL if no such relation exists.

```
Compute the Weierstrass quantities b_2, b_4, b_6 ([18, III §1])
Let φ(X) = 4X^3 + b_2 X^2 + 2b_4 X + b_6
Let φ'(X) = 12X^2 + 2b_2 X + 2b_4
/* Make a list M of n pairs (q, α) with q prime, φ(α) ≡ 0 (mod q) */
q ← q_init; n_1 ← n
While n_1 > 0
  If φ(X) ≡ 0 (mod q) has one root α
    Adjoin (q, α) to M
    n_1 ← n_1 − 1
  ElseIf φ(X) ≡ 0 (mod q) has three roots α, β, γ
    Adjoin (q, α) and (q, β) to M
    n_1 ← n_1 − 2
  EndIf
  q ← (next prime)
EndWhile
/* Fill an F_2 matrix with image of P_1, ..., P_r in ∏ E(F_q)/2E(F_q) */
A ← (r × n matrix of 0's)
Do j = 1 to r
  x ← x(P_j)
  Do k = 1 to n
    (q, α) ← M_k
    If ord_q(x) ≥ 0 And x ≢ α (mod q) And ((x−α)/q) = −1
      A_jk = 1
    ElseIf x ≡ α (mod q) And (φ'(x)/q) = −1
      A_jk = 1
    EndIf
  EndDo k
EndDo j
/* If A has rank r over F_2, then points are independent */
If rank(A mod 2) = r
  Return NULL
Else
  Compute non-zero ε = (ε_1, ..., ε_r) ∈ {0,1}^r with Aε ≡ 0 (mod 2)
  Q ← DivideByTwo(E, ε_1 P_1 + ε_2 P_2 + ··· + ε_r P_r)
  If Q = NULL
    Return NULL
  Else
```

```
    Return (Q, ε)
  EndIf
EndIf
```

DivideByTwo(E,R)
Divide the point $R \in E(\mathbb{Q})$ by 2
Input.
  $E = (a_1, a_2, a_3, a_4, a_6)$ an elliptic curve
  $R = (\alpha, \beta) \in E(\mathbb{Q})$ a point on E
Output.
  A Point $Q \in E(\mathbb{Q})$ satisfying $R = [2]Q$, or NULL if no such Q

```
Compute the Weierstrass quantities b2, b4, b6, b8 ([18, III §1])
Let F(X) = (X^4 − b4 X^2 − 2 b6 X − b8) − α(4X^3 + b2 X^2 + 2 b4 X + b6)
If F(X) has no roots in Q
  Return NULL
Else
  Compute a root x of F(X)
  Compute
```

$$y = \frac{x^3 - 3\alpha x^2 - (a_1\beta + (a_1^2 + 2a_2)\alpha + a_1a_3 + a_4)x - (a_3\beta + (a_1a_3 + a_4)\alpha + a_3^2 + 2a_6)}{2\beta + a_1\alpha + a_3}$$

```
  Return (x, y)
EndIf
```

Remark. Note that one method to find the (rational) roots of $F(X)$ is to explicitly use the quartic formula. Thus there is no need to use fancy polynomial factorization methods. Also note that this algorithm will generally only be used when we are almost certain that R is in $2E(\mathbb{Q})$, so $F(X)$ will generally have a root. Thus it is not worthwhile doing preliminary tests (e.g., modulo small primes) to check if $F(X)$ is irreducible in $\mathbb{Q}[X]$.

Remark. The routine fails if $2\beta + a_1\alpha + a_3 = 0$, or equivalently, if $2R = O$. Thus a completely general purpose routine should include additional code to divide R by 2 in this special case. For the purposes of the Xedni algorithm, the chances of having $2R = O$ are too small to be worth worrying about, although for safety, one might include an extra line saying:

If $2\beta + a_1\alpha + a_3 = 0$, Return TwoTorsionFlag

Appendix H. Some Useful Precomputations

For each prime ℓ in some range, it might be useful to precompute and store the following quantities:

- Inverses $a^{-1} \bmod \ell$ for each $0 < a < \ell$.
- Quadratic residues $\left(\frac{a}{\ell}\right)$ for each $0 \le a < \ell$.
- Root(s) of $X^3 + ax + b \equiv 0 \pmod{\ell}$ for each $0 \le a, b < \ell$.

In addition, if Step 10 is to be performed, it would be worthwhile precomputing the Fourier coefficients

$$a_\ell(E) = \ell + 1 - \#E_{j,\gamma}(\mathbb{F}_\ell)$$

for each $0 \le j < \ell$ ($j \not\equiv 0, 1728 \pmod{\ell}$) and each $\gamma = \pm 1$. Here $E_{j,\gamma}/\mathbb{F}_\ell$ is any elliptic curve with

$$j(E_{j,\gamma}) = j \qquad \text{and} \qquad -\left(\frac{c_4 c_6}{\ell}\right) = \gamma.$$

In other words, $E_{j,1}$ and $E_{j,-1}$ are isomorphic over $\bar{\mathbb{F}}_\ell$, and they are non-trivial quadratic twists of one another over $\mathbb{F}_\ell$. It is also easy to give a similar classification for the different $\mathbb{F}_\ell$-isomorphism classes of curves with $j = 0$ and $j = 1728$ (at least when $\ell \ge 5$), and for $\ell = 2, 3$ one can simply list all possible curves, but we will not do so here. Once this data is assembled, it then becomes possible to compute $a_\ell(E)$ by simply computing $j(E) \bmod \ell$ and a quadratic residue symbol.

Appendix I. Mestre's Method and Curves of High and Low Rank

In this section we briefly describe Mestre's method [13] for producing elliptic curves of high rank over $\mathbb{Q}$ and explain how a small modification should lead to curves of lower than expected rank. Mestre uses congruence conditions modulo ℓ for small primes $\ell \le L_0$ to force the Fourier coefficients $a_\ell(\mathcal{E})$ of $\mathcal{E}/\mathbb{Q}$ to be as negative as possible. Note that this is equivalent to forcing

$$\#\mathcal{E}(\mathbb{F}_\ell) = \ell + 1 - a_\ell(\mathcal{E})$$

to be as large as possible. Having imposed this condition, he considers curves whose discriminant is as small as possible and computes the auxiliary sum (9). If this sum is not sufficiently negative, he discards $\mathcal{E}$ and picks a new curve. If it is sufficiently negative, he searches for points in $\mathcal{E}(\mathbb{Q})$ near the (real) 2-torsion points and checks them for independence.

The heuristic on which Mestre's algorithm is based appears already in the original formulation of the Birch and Swinnerton-Dyer conjecture, namely if $\mathcal{E}(\mathbb{Q})$ has high rank, then the points in $\mathcal{E}(\mathbb{Q})$ should "spread out" modulo ℓ to force $\mathcal{E}(\mathbb{F}_\ell)$ to be large. Mestre is using the converse of this heuristic, which he justifies with a beautiful explicit formula which we now describe.

Let $\mathcal{E}/\mathbb{Q}$ be an elliptic curve of conductor $N_\mathcal{E}$. The L-series of $\mathcal{E}$ is given, for $\mathrm{Re}(s) > 3/2$, by the infinite product

$$L(\mathcal{E}/\mathbb{Q}, s) = \prod_{\ell | N_\mathcal{E}} (1 - a_\ell(\mathcal{E})\ell^{-s})^{-1} \prod_{\ell \nmid N_\mathcal{E}} (1 - a_\ell(\mathcal{E})\ell^{-s} + \ell^{1-2s})^{-1},$$

and extended analytically to the entire complex plane. For primes $\ell | N_\mathcal{E}$, the Fourier coefficient $a_\ell(\mathcal{E})$ is either 0 or ± 1. For $\ell \nmid N_\mathcal{E}$, we write $a_\ell(\mathcal{E}) = \alpha_\ell(\mathcal{E}) + \bar{\alpha}_\ell(\mathcal{E})$ with $|\alpha_\ell(\mathcal{E})| = |\bar{\alpha}_\ell(\mathcal{E})| = \sqrt{\ell}$, and for any prime power ℓ^m we define $b_{\ell^m}(\mathcal{E}) = \alpha_\ell^m + \bar{\alpha}_\ell^m$.

We will make a particular choice for the function appearing in Mestre's explicit formula, but we note that other choices may yield better numerical estimates. We set

$$F(x) = \max\{0, 1 - |x|\}, \quad \phi(y) = \int_{-\infty}^{\infty} F(x) e^{xyi}\,dx = 2\frac{1 - \cos y}{y^2},$$
$$M(\lambda) = 2\log 2\pi + 2\int_0^\infty \left(\frac{F(x/\lambda)}{e^x - 1} - \frac{e^{-x}}{x}\right) dx.$$

We note that $M(\lambda) = O(1)$, and indeed for $\lambda \ge 1$, we have $2.3 < M(\lambda) < 4.8$.

Theorem. (Mestre's Explicit Formula) *With notation as above, for any* $L \geq 3$,

$$\operatorname{rank}\mathcal{E}(\mathbb{Q}) = \overbrace{\frac{\log N_{\mathcal{E}}}{\log L} - \sum_{\substack{L(\mathcal{E}/\mathbb{Q},1+iy)=0\\ y\neq 0}} \phi(y\log L)}^{\text{Spectral Part}} - \overbrace{2\sum_{\ell^m\leq L} F\left(\frac{\log \ell^m}{\log L}\right)\frac{b_{\ell^m}(\mathcal{E})\log\ell}{\ell^m}}^{\text{Geometric Part}} - M(\log L).$$

Here the first sum is over all zeros of $L(\mathcal{E}/\mathbb{Q}, s)$ *on the line* $\operatorname{Re}(s) = 1$, *other than* $s = 1$, *counted with the appropriate multiplicities, while the second sum is over all prime powers* ℓ^m *less than or equal to* L.

In the geometric part of Mestre's formula, the function F more-or-less averages out to $1/2$ on the interval $\ell^m \leq L$, and most of the sum tends to come from the terms with $m = 1$. In other words, the geometric contribution to the rank in Mestre's formula is approximately

$$-\sum_{\ell\leq L}\frac{a_\ell(\mathcal{E})\log\ell}{\ell}.$$

Mestre's idea to produce curves of elevated rank is to force $a_\ell(\mathcal{E})$ to be as negative as possible for all primes $\ell \leq L_0$, thereby making this term as large as possible. Of course, doing this does not preclude the spectral part of the formula from being negative and thereby cancelling the effect. However, as a practical observation based on Mestre's work, the curves with negative $a_\ell(\mathcal{E})$'s and smallish conductor do seem to have elevated rank.

We now apply Mestre's reasoning in reverse. We are looking at curves which we know to contain r rational points, and we want to increase the likelihood that some curve has small (meaning $\leq r-1$) rank, thereby forcing the r known points to be linearly dependent. We do this by imposing congruence conditions on the Weierstrass coefficients so as to force $a_\ell(\mathcal{E})$ to be as *positive* as possible for primes $L_0 \leq \ell \leq L_1$, thereby making the geometric part of Mestre's formula contribute negatively and encouraging the rank of $\mathcal{E}$ to be lower.

Appendix J. Effects of Varying the Number of Lifted Points

There appear to be two opposing effects to increasing the number r of points to be lifted. Thus as r increases:

- The coefficients $\mathbf{u} = [u_1, \ldots, u_{10}]$ of the curve $C_{\mathbf{u}}$ in Step 7 become larger, and similarly for the coefficients and discriminant of the curve $E_{\mathbf{u}}$ in Step 8.
- The smallest relation satisfied by the r points $P_{p,i} \in E_p(\mathbb{F}_p)$ in Step 3 becomes smaller, hence the smallest possible relation among the points $Q_2, \ldots, Q_r \in E_{\mathbf{u}}(\mathbb{Q})$ in Step 11 becomes smaller.

We can roughly quantify these statements as follows. We start with the effect of r on the coefficients of the curve $C_{\mathbf{u}}$. The coefficients $\mathbf{u}$ form the solution of an $r \times 10$ system of linear equations (5) whose coefficients are cubic monomials in the $[x, y, z]$-coordinates of the lifted points. These $[x, y, z]$-coordinates are lifts of integers modulo Mp, so are roughly on the order of $Mp/2$. Thus $\mathbf{u}$ is the solution of a system of r linear equations in 10 variables whose coefficients are roughly $(Mp/2)^3$. Siegel's Lemma (see, e.g., [22, V §4]) says that there is a solution satisfying

$$\|\mathbf{u}\| \ll (Mp)^{3r/(10-r)}.$$

However, the solution $\mathbf{u}$ is also required to satisfy the congruence condition (6). As explained in Appendix B, this means finding a solution $\mathbf{w}$ to an associated non-homogeneous system of equations and then using $Mp\mathbf{w}$ to form $\mathbf{u}$. Thus the expected size of the solution $\mathbf{u}$ must be multiplied by Mp. Taking this remark into account, we see that there will be solutions satisfying

$$\|\mathbf{u}\| \ll (Mp)^{(10+2r)/(10-r)}.$$

The following table of exponent values suggests why it may be best to choose an intermediate value of r.

r	3	4	5	6	7	8	9
$\frac{10+2r}{10-r}$	$\frac{16}{7}$	3	4	$\frac{11}{2}$	8	13	28

In any case, we see why the cofficients of $C_{\mathbf{u}}$ increase as r increases.

Next we consider the effect of r on the probable relation among the points in Step 3. For simplicity, we will assume that the group $E_p(\mathbb{F}_p)$ is cyclic of prime order N_p. We begin with a precise formulation of the well-known Birthday Phenomenon.

Birthday Lemma. *Let K objects be randomly placed into N boxes. Assume that $N \geq 12$ and $K \geq \sqrt{3N}+1$. Then the probability that some box contains more than one object is greater than*

$$1 - \exp(-K^2/2N).$$

For the convenience of the reader, we include a proof of the Birthday Lemma at the end of this section. We apply the Birthday Lemma to the following situation.

Proposition. *Let G be a cyclic group of order N (written additively), let $r \geq 1$, and let $\kappa > 0$. Let $a_1, \dots, a_r \in G$ be a randomly chosen collection of elements of G. Then the probability of there being integers $n_1, \dots, n_r \in \mathbb{Z}$ satisfying*

$$\sum_{i=1}^{r} n_i a_i = 0 \qquad \text{and} \qquad \max_{1\leq i\leq r} |n_i| \leq 2(2\kappa N)^{1/2r}$$

is greater than

$$1 - \exp(-\kappa).$$

Proof. For any integer X, consider the map

$$F : \{\mathbf{m} : 0 \leq m_i \leq X\} \longrightarrow G, \qquad (m_1, \dots, m_r) \longmapsto m_1 a_1 + \cdots + m_r a_r.$$

We can think of F as randomly distributing the $(X+1)^r$ integer vectors $\mathbf{m}$ into the N boxes labeled by the elements of G. Applying the Birthday Lemma, we see that the probability is greater than

$$1 - \exp(-(X+1)^{2r}/2N)$$

that F is not injective, say $F(\mathbf{m}) = F(\mathbf{m}')$. Then $\mathbf{n} = \mathbf{m} - \mathbf{m}'$ gives the desired integer vector with

$$\sum_{i=1}^{r} n_i a_i = 0 \qquad \text{and} \qquad \max_{1\le i\le r} |n_i| \le 2X.$$

Taking $X = (2\kappa N)^{1/2r}$ gives something slightly stronger than the stated result.

The following table illustrate the proposition by giving the expected size of the coefficients of a relation among r randomly chosen elements in a cyclic group of order N for various values of r and two different probability levels. As can be seen, increasing the probability has only a small effect on the expected size of the smallest relation.

r	3	4	5	6	7	8
$\max \lvert n_i\rvert \le$	$2.90N^{1/6}$	$2.64N^{1/8}$	$2.50N^{1/10}$	$2.41N^{1/12}$	$2.34N^{1/14}$	$2.30N^{1/16}$
Probability $\ge$	99%	99%	99%	99%	99%	99%

r	3	4	5	6	7	8
$\max \lvert n_i\rvert \le$	$1.54N^{1/6}$	$1.65N^{1/8}$	$1.71N^{1/10}$	$1.76N^{1/12}$	$1.79N^{1/14}$	$1.81N^{1/16}$
Probability $\ge$	10%	10%	10%	10%	10%	10%

Now consider the situation in the xedni algorithm. The points $P_{p,1},\dots,P_{p,r}$ chosen in Step 3 are presumably random elements of the (assumed cyclic) group $E_p(\mathbb{F}_p)$ of order N_p, so the proposition tells us that there is probably a relation of the form

$$\sum_{i=1}^{r} n_i P_{p,i} = O \qquad \text{with} \qquad \max_{1\le i\le r} |n_i| = O(N_p^{1/2r}) = O(p^{1/2r}).$$

Further, the big-O constant is fairly small.

Suppose now that we apply the xedni algorithm without imposing Mestre-type conditions at auxiliary primes. If the global points $P_1,\dots,P_r \in C_{\mathbf{u}}(\mathbb{Q})$ are to be dependent, we would hope that the dependence relation would have coefficients on the same order of magnitude as the mod p relation, namely $O(p^{1/2r})$. However, without the Mestre conditions it seems unlikely (i.e., low probability) that the points will be dependent, so we need to see what effect the Mestre condtions have on the expected size of the hypothetical relation on the global points.

We use the notation from Appendix E, and let ℓ denote an auxiliary prime. Note that the chosen set of r points $P_{\ell,1},\dots,P_{\ell,r} \in E(\mathbb{F}_\ell)$ satisfy certain relations in the group $E(\mathbb{F}_\ell)$ of order N_ℓ. We can think of those relations as forming a submodule of $\mathbb{Z}^r$; or, combining all of the auxiliary primes, we consider the *relation module* $\mathcal{R}_M$ defined to be the kernel of the homomorphism

$$\mathbb{Z}^r \longrightarrow \prod_{\ell\mid M} E(\mathbb{F}_\ell), \qquad (n_1,\dots,n_r) \longmapsto \left(\sum_{i=1}^{r} n_i P_{\ell,i}\right)_{\ell\mid M}.$$

If the $P_{\ell,i}$'s were chosen randomly, then we could apply the Birthday Lemma just as above to describe the probable smallest element of the relation module $\mathcal{R}_M$, albeit with the added complication that we are mapping into a product of cyclic groups. However, we have to make an a priori choice of the $P_{\ell,i}$'s, which means that we are in effect making a specific choice of relation module $\mathcal{R}_M$. Note that the hypothetical relation on the global points must necessarily lie in $\mathcal{R}_M$, since the global relation must reduce to a valid local relation modulo each ℓ, so we want to be careful to impose as few constraints as possible.

For example, suppose that we can choose the auxiliary conditions so that the N_ℓ's are pairwise relatively prime, and that we frequently choose new random $P_{\ell,i}$'s. Then $\prod E_\ell(\mathbb{F}_\ell)$ is a cyclic group of order $\prod N_\ell$, so we expect to find a relation (i.e., an element of $\mathcal{R}_M$) whose coefficients are $O(\prod N_\ell^{1/2r})$.

At the other extreme, we consider what happens if the N_ℓ's have common factors. For example, if they are all even and if we choose the $P_{\ell,i}$'s at random, then there is a substantial probability that any relation must have every coefficient divisible by 2. This is quite undesirable, since it means that there cannot be a global relation unless the global curve has non-trivial 2-torsion.

However, in the case that the N_ℓ's have many common factors, we might try to compensate by choosing the $P_{\ell,i}$'s more cleverly. For example, to deal with the even N_ℓ's, we might require that

$$\begin{aligned} P_{\ell,i} &\in 2E_\ell(\mathbb{F}_\ell) \quad \text{for all } i \equiv 0 \pmod{2} \text{ and all } \ell|M \text{ with } N_\ell \text{ even,} \\ P_{\ell,i} &\notin 2E_\ell(\mathbb{F}_\ell) \quad \text{for all } i \equiv 1 \pmod{2} \text{ and all } \ell|M \text{ with } N_\ell \text{ even.} \end{aligned}$$

In this way we force the eventual matrix of $E(\mathbb{Q})/2E(\mathbb{Q})$ in $\prod_{\ell|M} E_\ell(\mathbb{F}_\ell)/2E_\ell(\mathbb{F}_\ell)$ to have rank 1, since it will have alternating rows of all 1's and all 0's. Hence we impose few conditions on an eventual relation of the global points.

The bottom line seems to be as follows. The smallest relation among the global points $P_1, \dots, P_r \in C_{\mathbf{u}}(\mathbb{Q})$, if it exists at all, has coefficients at least as large as

$$O\left(\left(N_p \operatorname*{LCM}_{\ell|M} N_\ell\right)^{1/2r}\right).$$

If the N_ℓ's are more-or-less pairwise relatively prime, then we would hope to eventually find a relation of this size. Otherwise we need to choose the auxiliary points $P_{\ell,i}$ carefully to have any hope of finding a relation of this size.

Proof. (of the Birthday Lemma) The probability that no box contains more than one object is

$$\prod_{k=0}^{K-1}\left(1-\frac{k}{N}\right).$$

We estimate

$$\begin{aligned} -\log\prod_{k=0}^{K-1}\left(1-\frac{k}{N}\right) &= \sum_{k=0}^{K-1}\sum_{j=0}^{\infty}\frac{1}{j}\left(\frac{k}{N}\right)^j \\ &\ge \frac{K(K-1)}{2N}+\frac{(K-1)K(2K-1)}{12N^2} \qquad \begin{cases}\text{taking the } j=1 \\ \text{and } j=2 \text{ terms}\end{cases} \\ &= \frac{K^2}{2N}+\frac{K}{3N}\left\{\frac{K^2}{2N}\left(1-\frac{3}{2K}\right)-\frac{3}{2}\right\}+\frac{K}{12N^2}. \end{aligned}$$

We are given that $K \geq \sqrt{3N} + 1$, so the quantity in braces satisfies

$$\begin{aligned} \frac{K^2}{2N}\left(1 - \frac{3}{2K}\right) - \frac{3}{2} &\geq \frac{3N + 2\sqrt{3N}}{2N} \cdot \left(1 - \frac{3}{2\sqrt{3N}}\right) - \frac{3}{2} \\ &= \frac{\sqrt{3}}{4N}\left(\sqrt{N} - 2\sqrt{3}\right) \\ &\geq 0 \quad \text{since } N \geq 12. \end{aligned}$$

Hence the probability of some box containing more than one object is

$$1 - \prod_{k=0}^{K-1}\left(1 - \frac{k}{N}\right) \geq 1 - \exp(-K^2/2N).$$

Appendix K. Applying Xedni to DLP and Integer Factorization

In this section we describe Neal Koblitz' ideas [9] for applying the Xedni calculus to the discrete logarithm problem for $\mathbb{F}_p^*$ (DLP) and to the integer factorization problem (IFP).

We begin with the DLP. Let $\alpha, \beta \in \mathbb{F}_p^*$. The DLP is the problem of finding an exponent m so that $\alpha = \beta^m$. Koblitz' idea is to use an elliptic curve with split multiplicative reduction at p, since for such a curve, the set of (non-singular) points modulo p is isomorphic to $\mathbb{F}_p^*$. Thus consider the curve

$$E_p : y^2 = x^3 + x^2. \tag{21}$$

The non-singular points $E_p^{ns}(\mathbb{F}_p)$, which means all points except for $(0,0)$, form a group isomorphic to $\mathbb{F}_p^*$ via the map

$$\mathbb{F}_p^* \longrightarrow E_p^{ns}(\mathbb{F}_p), \qquad t \longmapsto \left(\frac{4t}{(t-1)^2}, \frac{4t(t+1)}{(t-1)^3}\right). \tag{22}$$

(See [18, Proposition III.2.5].) Apply this map to α and β to get points $S, T \in E_p^{ns}(\mathbb{F}_p)$. Now use the Xedni Calculus on S, T, E_p to solve the ECDLP for S and T, say $S = mT$, which also gives the solution $\alpha = \beta^m$. Note it won't matter that E_p is singular, since all this means is that the lifted curve $\mathcal{E}/\mathbb{Q}$ has (split) multiplicative reduction at p.

Koblitz' idea for using Xedni to solve the IFP is similar. Suppose that N is an integer that we want to factor. In order to factor N, it suffices to have an algorithm that takes a random integer a and finds a non-zero multiple of the order of a in the multiplicative group $(\mathbb{Z}/N\mathbb{Z})^*$. So suppose we are given a random integer a. Choose r random integers $k_1, \dots, k_r$, say on the same order of magnitude as N, and compute the quantities $b_i \equiv a^{k_i} \pmod{N}$. Now let E_N to be the split multiplicative curve (21) and use the same map (22) as above to map the numbers $b_1, \dots, b_r \in (\mathbb{Z}/N\mathbb{Z})^*$ to points $P_{N,1}, \dots, P_{N,r}$ on the curve $E_N(\mathbb{Z}/N\mathbb{Z})$. Now apply the Xedni Calculus, skipping Step 3, since we've already chosen points $P_{N,1}, \dots, P_{N,r}$ to take the place of the points $P_{p,1}, \dots, P_{p,r}$ in Step 3. Assuming that the Xedni algorithm finds a linear relation $n_1P_1 + \cdots + n_rP_r = 0$ in Step 11, we deduce a relation

$$a^{n_1k_1+\cdots+n_rk_r} \equiv 1 \pmod{N},$$

and hence $\sum n_ik_i$ is the desired multiple of the order of a in $(\mathbb{Z}/N\mathbb{Z})^*$. Finally, we note that if $a^n \equiv 1 \pmod{N}$ and if we take a small divisor m of n, then there is a reasonable probability that $\gcd(a^{n/m} - 1, N)$ will give a non-trivial factor of N.

Appendix L. Using Higher Genus Curves in Xedni

I would like to thank Nigel Smart and Sachar Paulus for suggesting the idea of using higher genus curves. This appendix contains an expanded version of their remarks.

Let $P_1, \dots, P_r \in E_p(\mathbb{F}_p)$ be points constructed as in Step 6 of the Xedni algorithm, but now with r possibly larger than 9. We can use the usual undetermined coefficients procedure to force the P_i's to lie on a curve of higher genus, say either of the form $C : F(X, Y, Z) = 0$ for a homogeneous form F of degree d or of the form $C : Y^2 + aXY + bY = G(X)$ for a polynomial G of degree d. However, we also want C to be related to the elliptic curve E_p. So using the second version, suppose that E_p has the form $Y^2 = f(X)$ for a cubic polynoimal f. Then we construct C to have the form

$$C : Y^2 + paXY + pbY = f(X) + pg(X),$$

where a, b, and the coefficients of g are indeterminates. It is clear that the Jacobian J of C has the property that E_p is a factor (up to isogeny) of $J \bmod p$. Hence if we can find a relation on the points $P_1, \dots, P_r \in C(\mathbb{Q}) \hookrightarrow J(\mathbb{Q})$, then we obtain a relation in $E_p(\mathbb{F}_p)$ and can solve the ECDLP. Unfortunately, there seems no reason why one is more likely to find such relations on higher genus curves, since the advantage of choosing larger r is probably offset by the additional freedom to be independent that points enjoy on higher dimensional abelian varieties. Also, from a practical viewpoint, it is difficult working on abelian varieties of dimension greater than 1. However, if there were some way to further encourage the points to be dependent, for example by forcing their image in $J \equiv E_p \times A \pmod{p}$ to have the form (P, O), then one might gain an advantage in the higher dimensional setting.

References

1. B. Birch, H.P.F. Swinnerton-Dyer, *Elliptic curves and modular functions*, Modular Functions of One Variable (Birch and Kuyk, eds.), Antwerp IV, Springer Lecture Notes 476, Springer-Verlag, 1975, pp. 2–32.
2. H. Cohen, *A Course in Computational Number Theory*, GTM 138, Springer-Verlag, 1993.
3. I. Connell, *Addendum to a paper of Harada and Lang*, J. Algebra **145** (1992), 463–467.
4. J. Cremona, *Algorithms for Modular Elliptic Curves*, 2nd ed., Cambridge University Press, 1997.
5. E. Fouvry, M. Nair, G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro*, Bull. Soc. math. France **120** (485–506), 1992.
6. G. Havas, B.S. Majewski, K.R. Matthews, *Extended gcd and Hermite normal form algorithms via lattice basis reduction*, Experimental Math. **7** (1998), 125–136.
7. M. Hindry, J.H. Silverman, *The canonical height and integral points on elliptic curves*, Invent. Math. **93** (1988), 419–450.
8. N. Koblitz, *Elliptic curve cryptosystems*, Mathematics of Computation **48** (1987), 203–209.
9. ———, *private communications, September 1998.*
10. H. Lenstra, *Factoring integers with elliptic curves*, Annals of Math. **126** (1987), 649–673.
11. D.W. Masser, *Specializations of finitely generated subgroups of abelian varieties*, Trans. AMS **311** (1989), 413–424.
12. K. Matthews, *private communications*, July 31–August 5, 1998.
13. J.F. Mestre, *Formules explicites et minoration de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.
14. 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.

15. A. Néron, *Propriétés arithmétiques et géométriques rattachés à la notion de rang d'une courbe algébrique dans un corps*, Bull. Soc. Math. France **80** (1952), 101–166.
16. D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. **87** (1993), 119–151.
17. ______, *An algorithm to compute $w_3(E)$*, unpublished.
18. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin and New York, 1986.
19. ______, *Computing heights on elliptic curves*, Math. Comp. **51** (1988), 339–358.
20. ______, *Computing canonical heights with little (or no) factorization*, Math. Comp. **66** (1997), 787–805.
21. J.H. Silverman, J. Suzuki, *Elliptic curve discrete logarithms and the index calculus*, ASIACRYPT '98 (Lecture Notes in Computer Science), to appear.
22. J.H. Silverman and J. Tate, *Rational points on elliptic curves*, Springer-Verlag, New York, 1992.
23. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math. **141** (1995), 443–551.

Mathematics Department Box 1917 Brown University Providence, RI 02912 USA
E-mail address: `jhs@math.brown.edu`