COMPUTING MODULAR POLYNOMIALS

DENIS CHARLES AND KRISTIN LAUTER

1. Introduction

The ℓ^{th} modular polynomial, $\phi_\ell(x, y)$, parameterizes pairs of elliptic curves with an isogeny of degree ℓ between them. Modular polynomials provide the defining equations for modular curves, and are useful in many different aspects of computational number theory and cryptography. For example, computations with modular polynomials have been used to speed elliptic curve point-counting algorithms ([BSS99] Chapter VII).

The standard method for computing modular polynomials consists of computing the Fourier expansion of the modular **j**-function and solving a linear system of equations to obtain the integral coefficients of $\phi_\ell(x, y)$ ([Elk98]). The computer algebra package MAGMA [BC03] incorporates a database of modular polynomials for ℓ up to 59.

The idea of the current paper is to compute the modular polynomial directly modulo a prime p, without first computing the coefficients as integers. Once the modular polynomial has been computed for enough small primes, our approach can also be combined with the Chinese Remainder Theorem (CRT) approach as in [ALV03] to obtain the modular polynomial with integral coefficients or with coefficients modulo a much larger prime using Explicit CRT. Our algorithm does not involve computing Fourier coefficients of modular functions.

The idea of our algorithm is as follows. Mestre's algorithm, Methode de graphes [Mes86], uses the ℓ^{th} modular polynomial modulo p to navigate around the connected graph of supersingular elliptic curves over $\mathbb{F}_{p^2}$ in order to compute the number of edges (isogenies of degree ℓ) between each node. From the graph, Mestre then obtains the ℓ^{th} Brandt matrix giving the action of the ℓ^{th} Hecke operator on modular forms of weight 2. The main idea of our algorithm is to do the reverse: we compute the ℓ^{th} modular polynomial modulo p by computing all the isogenies of degree ℓ between supersingular curves modulo p via Vélu's formulae. Specifically, for a given **j**-invariant of a supersingular elliptic curve over $\mathbb{F}_{p^2}$, Algorithm 1 computes $\phi_\ell(x, j)$ modulo p by computing the $\ell + 1$ distinct subgroups of order ℓ and computing the **j**-invariants of the $\ell + 1$ corresponding ℓ-isogenous elliptic curves. Algorithm 2 then uses the connectedness of the graph of supersingular elliptic curves over $\mathbb{F}_{p^2}$ to move around the graph, calling Algorithm 1 for different values of j until enough information is obtained to compute $\phi_\ell(x, y)$ modulo p via interpolation.

There are several interesting aspects to Algorithms 1 and 2. Algorithm 1 does not use the factorization of the ℓ-division polynomials to produce the subgroups of order ℓ. Instead we generate independent ℓ-torsion points by picking random points with coordinates in a suitable extension of $\mathbb{F}_p$ and taking a scalar multiple which is the group order divided by ℓ. This turns out to be more efficient than factoring the ℓ^{th} division polynomial for large ℓ. This approach also gives as a corollary a very fast way to compute a random ℓ-isogeny of an elliptic curve over a finite field for

2000 Mathematics Subject Classification. Primary: 11G18, 11Y16. Secondary: 14H52, 14G50.

large ℓ.

Algorithm 2 computes $\phi_\ell(x,y)$ modulo p by doing only computations with supersingular elliptic curves in characteristic p even though $\phi_\ell(x,y)$ is a general object giving information about isogenies between elliptic curves in characteristic 0 and ordinary elliptic curves in characteristic p. The advantage that we gain by using supersingular elliptic curves is that for all but at most 4 of the isomorphism classes of supersingular elliptic curves, we can show that the full ℓ-torsion is defined over an extension of degree $O(\ell)$ of the base field $\mathbb{F}_{p^2}$, whereas in general the field of definition can be of degree $O(\ell^2)$.

2. Local computation of $\phi_\ell(x,j)$

The key ingredient of the algorithm is the computation of the univariate polynomial $\phi_\ell(x,j)$ modulo a prime p given a **j**-invariant j. We describe the method to do this here.

Algorithm 1
Input: Two distinct primes p and ℓ, and j the **j**-invariant of a supersingular elliptic curve E over a finite field $\mathbb{F}_q$ of degree at most 2 over a prime field of characteristic p.
Output: The polynomial $\phi_\ell(x,j) = \prod_{E' \ \ell\text{-isogenous to } E}(x - j(E')) \in \mathbb{F}_{p^2}[x]$.

Step 1 Find the generators P and Q of $E[\ell]$:
- (a) Let n be such that $\mathbb{F}_q(E[\ell]) \subseteq \mathbb{F}_{q^n}$.
- (b) Let $S = \sharp E(\mathbb{F}_{q^n})$, the number of $\mathbb{F}_{q^n}$ rational points on E.
- (c) Set $s = S/\ell^k$, where ℓ^k is the largest power of ℓ that divides S (note $k \geq 2$).
- (d) Pick two points P and Q at random from $E[\ell]$:
  - (i) Pick two points U, V at random from $E(\mathbb{F}_{q^n})$.
  - (ii) Set $P' = sU$ and $Q' = sV$, if either P' or Q' equals $\mathcal{O}$ then repeat step (i).
  - (iii) Find the smallest i_1, i_2 such that $\ell^{i_1}P' \neq \mathcal{O}$ and $\ell^{i_2}Q' \neq \mathcal{O}$ but $\ell^{i_1+1}P' = \mathcal{O}$ and $\ell^{i_2+1}Q' = \mathcal{O}$.
  - (iv) Set $P = \ell^{i_1}P'$ and $Q = \ell^{i_2}Q'$.
- (e) Using Shanks's Baby-steps-Giant-steps algorithm check if Q belongs to the group generated by P. If so repeat step (d).

Step 2 Find the **j**-invariants $j_1, \cdots, j_{\ell+1}$ in $\mathbb{F}_{p^2}$ of the $\ell+1$ elliptic curves that are ℓ-isogenous to E.
- (a) Let $G_1 = \langle Q \rangle$ and $G_{1+i} = \langle P + (i-1) * Q \rangle$ for $1 \leq i \leq \ell$.
- (b) For each i, $1 \leq i \leq \ell+1$ compute the **j**-invariant of the elliptic curve E/G_i using Vélu's formulas.

Step 3 Output $\phi_\ell(x,j) = \prod_{1 \leq i \leq \ell+1}(x - j_i)$.

The following lemma gives the possibilities for the value of n in Step (1a).

Lemma 2.1. *Let $E/\mathbb{F}_q$ be an elliptic curve, and let ℓ be a prime not equal to the characteristic of $\mathbb{F}_q$. Then $E[\ell] \subseteq E(\mathbb{F}_{q^n})$ where n is a divisor of either $\ell(\ell-1)$ or ℓ^2-1.*

Proof : The Weil-pairing tells us that if $E[\ell] \subseteq \mathbb{F}_{q^n}$ then $\mu_\ell \subseteq \mathbb{F}_{q^n}$ ([Sil86] Corollary 8.1.1). We seek, however, an upper bound on n, to do this we use the Galois representation coming from the ℓ-division points of E. Indeed, we have an *injective* group homomorphism ([Sil86] Chapter III, §7)

$$\rho_\ell : \mathrm{Gal}(\mathbb{F}_q(E[\ell])/\mathbb{F}_q) \to \mathrm{Aut}(E[\ell]) \cong \mathrm{GL}_2(\mathbb{F}_\ell).$$

The Galois group $\mathrm{Gal}(\mathbb{F}_q(E[\ell])/\mathbb{F}_q)$ is cyclic, thus by ρ_ℓ the possibilities for $\mathrm{Gal}(\mathbb{F}_q(E[\ell])/\mathbb{F}_q)$ are limited to cyclic subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$. We study the following map

$$\mathrm{GL}_2(\mathbb{F}_\ell) \xrightarrow{\psi} \mathrm{SL}_2(\mathbb{F}_\ell) \longrightarrow \mathrm{PSL}_2(\mathbb{F}_\ell),$$

where the map ψ is given by $\psi(M) = \frac{1}{\det M} M$. By a theorem of Dickson (see [Hup67] Hauptsatz 8.27) the cyclic subgroups of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ are either of order ℓ or of cardinality dividing $(\ell \pm 1)/k$, where $k = \gcd(\ell - 1, 2)$. If C is a cyclic subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ then its image in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is annihilated by either ℓ or $\ell \pm 1$. Since the image is obtained by quotienting out by scalars and then a group of order 2, C is annihilated by either $\ell(\ell-1)$ or $(\ell-1)(\ell+1) = \ell^2 - 1$. Thus the degree of the field extension containing the ℓ-torsion points on E must divide either $\ell(\ell-1)$ or ℓ^2-1. $\square$

We will try step (1) with $n = \ell^2 - 1$, if steps (1d - 1e) do not succeed for some K (a constant) many trials, we repeat with $n = \ell(\ell-1)$. The analysis that follows shows that a sufficiently large constant K will work.

For step (1b) we do not need a point counting algorithm to determine S. Since E is a supersingular elliptic curve, we have the following choices for the trace of Frobenius a_q:

$$a_q = \begin{cases} 0 & \text{if } E \text{ is over } \mathbb{F}_p \\ 0, \pm p, \pm 2p & \text{if } E \text{ is over } \mathbb{F}_{p^2}. \end{cases}$$

Not all the possibilities can occur for certain primes, but we will not use this fact here (see [Sch87]). If the curve is over $\mathbb{F}_{p^2}$ we can determine probabilistically the value of a_q as follows. Pick a point P at random from $E(\mathbb{F}_q)$ and check if $(q + 1 + a_q)P = \mathcal{O}$. Since the pairwise gcd's of the possible group orders divide $4p$ which is $O(\sqrt{\sharp E(\mathbb{F}_q)})$, with high probability only the correct value of a_q will annihilate the point. Thus in $O(\log^{2+o(1)} q)$ time we can determine with high probability the correct value of a_q. Once we know the correct trace a_q, we can find the roots (in $\overline{\mathbb{Q}}$), π and $\overline{\pi}$, of the characteristic polynomial of the Frobenius $\phi^2 - a_q\phi + q$. Then the number of points lying on E over the field $\mathbb{F}_{q^n}$ is given by $q^n + 1 + \pi^n + \overline{\pi}^n$, this gives us S.

Note: We could have used a deterministic point counting algorithm to find $\sharp E(\mathbb{F}_q)$ but this would have cost $O(\log^6 q)$ field operations.

Next, we analyze the probability with which step (1d) succeeds.

Lemma 2.2. *For a random choice of the points U and V in step (1d i) the probability that step (1d ii) succeeds is at least*

$$\left(1 - \frac{1}{\ell^2}\right)^2.$$

Proof : As a group $E(\mathbb{F}_{q^n}) \cong \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/MN\mathbb{Z}$, where $N = \ell N'$ since ℓ-torsion points of E are $\mathbb{F}_{q^n}$ rational. Using this isomorphism one sees that the probability that $sU = \mathcal{O}$ is bounded above by $\frac{N'}{N}\frac{MN'}{MN} = \frac{1}{\ell^2}$. $\square$

At the end of step (1d) we have two random ℓ-torsion points of E namely, P and Q. The probability that Q belongs to the cyclic group generated by P is $\frac{\ell}{\ell^2} = \frac{1}{\ell}$. Thus with high probability we will find in step (1e) two generators for $E[\ell]$.

Lemma 2.3. *The expected running time of Step 1 is $O(\ell^{4+o(1)} \log^{2+o(1)} q)$.*

Proof : The finite field $\mathbb{F}_{q^n}$ can be constructed by picking an irreducible polynomial of degree n. A randomized method that requires on average $O\big((n^2 \log n + n \log q) \log n \log\log n\big)$ operations over $\mathbb{F}_q$ is given in [Sho94]. Thus the field can be constructed in $O(\ell^{4+o(1)} \log^{2+o(1)} q)$ time since $n \leq \ell^2$. Step (1d) requires picking a random point on E. We can do this by picking a random element in $\mathbb{F}_{q^n}$ treating it as the x-coordinate of a point on E and solving the resulting quadratic equation for the y-coordinate. Choosing a random element in $\mathbb{F}_{q^n}$ can be done in $O(\ell^2 \log q)$ time. Solving the quadratic equation can be done probabilistically in $O(\ell^2 \log q)$ field operations. Thus to pick a point on E can be done in $O(\ell^{4+o(1)} \log^{2+o(1)} q)$ time. The computation in steps (1d i – iv) computes integer multiples of a point on the elliptic curve, where the integer is at most q^n, and this can be done in $O(\ell^{4+o(1)} \log^{2+o(1)} q)$ time using the repeated squaring method and fast multiplication. Shanks's Baby-steps-giant-steps algorithm for a cyclic group G requires $O(\sqrt{|G|})$ group operations. Thus step (1e) runs in time $O(\ell^{\frac{5}{2}+o(1)} \log^{1+o(1)} q)$, since the group is cyclic of order ℓ. $\square$

Let C be a subgroup of E, Vélu in [Vel71] gives explicit formulas for determining the equation of the isogeny $E \to E/C$ and the Weierstrass equation of the curve E/C. Let E is given by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and let S be a set of representatives for $(C - \{\mathcal{O}\})/\pm 1$. We define the following two functions in $\mathbb{F}_q(E)$ for $Q = (x, y)$ a point on $E - \{\mathcal{O}\}$ define

$$\begin{aligned} g^x(Q) &= 3x^2 + 2a_2x + a_4 - a_1y \\ g^y(Q) &= -2y - a_1x - a_3, \end{aligned}$$

and set

$$\begin{aligned} t(Q) &= \begin{cases} g^x(Q) & \text{if } Q = -Q \text{ on } E; \\ 2g^x(Q) - a_1g^y(Q) & \text{otherwise,} \end{cases} \\ u(Q) &= (g^y(Q))^2 \\ t &= \sum_{Q \in S} t(Q) \\ w &= \sum_{Q \in S} (u(Q) + x(Q)t(Q)). \end{aligned}$$

Then the curve E/C is given by the equation

$$Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6$$

where

$$\begin{aligned} &A_1 = a_1, A_2 = a_2, A_3 = a_3, \\ &A_4 = a_4 - 5t, A_6 = a_6 - (a_1^2 + 4a_2)t - 7w. \end{aligned}$$

From the Weierstrass equation of E/C we can easily determine the $\mathbf{j}$-invariant of E/C. It is clear that this procedure can be done using $O(\ell)$ elliptic curve operations for each of the groups G_i, $1 \leq i \leq \ell + 1$. Thus step 2 can be done in $O(\ell^{4+o(1)} \log^{1+o(1)} q)$ time steps. Step 3 requires only $O(\ell)$ field operations and so the running time of the algorithm is dominated by the running time of steps 1 and 2. Note that the polynomial obtained at the end of Step 3 $\phi_\ell(x, j)$ has coefficients in $\mathbb{F}_{p^2}[x]$ since all the curves ℓ-isogenous to E are supersingular and hence their $\mathbf{j}$-invariants belong to $\mathbb{F}_{p^2}$. In summary, we have the following:

Theorem 2.4. *Algorithm 1 computes $\phi_\ell(x,j) \in \mathbb{F}_{p^2}[x]$, in fact, the list of roots of $\phi_\ell(x,j)$, and has an expected running time of $O(\ell^{4+o(1)} \log^{2+o(1)} q)$.*

For our application of Algorithm 1 we will need the dependence of the running time in terms of the quantity n. We make the dependence explicit in the next theorem.

Theorem 2.5. *With notation as above, Algorithm 1 computes $\phi_\ell(x,j) \in \mathbb{F}_{p^2}[x]$ together with the list of its roots and has an expected running time of $O(n^{2+o(1)} \log^{2+o(1)} q + \sqrt{\ell} n^{1+o(1)} \log^{1+o(1)} q + \ell^2 n^{1+o(1)} \log q)$.*

In the case of ordinary elliptic curve, step (1) of Algorithm 1 can still be used, once the number of points on $E/\mathbb{F}_q$ has been determined, by Lemma 2.1 the degree of the extension, n, is still $O(\ell^2)$. This leads to the following two results:

Corollary 2.6. *If $E/\mathbb{F}_q$ is an elliptic curve, we can pick a random ℓ-torsion point on $E(\overline{\mathbb{F}}_q)$ in time $O(\ell^{4+o(1)} \log^{2+o(1)} q + \log^{6+o(1)} q)$.*

Corollary 2.7. *If $E/\mathbb{F}_q$ is an elliptic curve, we can construct a random ℓ-isogenous curve to E in time $O(\ell^{4+o(1)} \log^{2+o(1)} q + \log^{6+o(1)} q)$.*

3. Computing $\phi_\ell(x,y) \mod p$

In characteristic $p > 2$ there are exactly

$$S(p) = \left\lfloor \frac{p}{12} \right\rfloor + \epsilon_p$$

supersingular **j**-invariants where

$$\epsilon_p = 0, 1, 1, 2 \text{ if } p \equiv 1, 5, 7, 11 \mod 12.$$

In this section we provide an algorithm for computing $\phi_\ell(x,y) \mod p$ provided $S(p) \geq \ell + 1$. The description of the algorithm follows:

Algorithm 2
Input: Two distinct primes ℓ and p with $S(p) \geq \ell + 1$.
Output: The polynomial $\phi_\ell(x,y) \in \mathbb{F}_p[x,y]$.

(1) Find the smallest (in absolute value) discriminant $D < 0$ such that $\left(\frac{D}{p}\right) = -1$.
(2) Compute the Hilbert Class polynomial $H_D(x) \mod p$.
(3) Let j_0 be a root of $H_D(x)$ in $\mathbb{F}_{p^2}$.
(4) Set $i = 0$.
(5) Compute $\phi_i = \phi_\ell(x, j_i) \in \mathbb{F}_{p^2}$ using Algorithm 1.
(6) Let j_{i+1} be a root of ϕ_k for $k \leq i$ which is not one of $j_0, \cdots, j_i$.
(7) If $i < \ell$ then set $i = i + 1$ and repeat Step 5.
(8) Writing $\phi_\ell(x,y) = x^{\ell+1} + \sum_{0 \leq k \leq \ell} p_k(y) x^k$, we have $\ell + 1$ systems of equations of the form $p_k(j_i) = v_{ki}$ for $0 \leq k, i \leq \ell$. Solve these equations for each $p_k(y)$, $0 \leq k \leq \ell$.
(9) Output $\phi_\ell(x,y) \in \mathbb{F}_p[x,y]$.

We argue that the above algorithm is correct and analyze the running time. For step 1, we note that if $p \equiv 3 \mod 4$, then $D = -4$ works. Otherwise, -1 is a quadratic residue and writing (without loss of generality) D as $-4d$, we are looking for the smallest d such that $\left(\frac{d}{p}\right) = -1$. A theorem of Burgess ([Bur62]) tells us that $d \ll p^{\frac{1}{4\sqrt{e}}}$, and under the assumption of GRH the estimate of

Ankeny ([Ank52]) gives $d \ll \log^2 p$. Computing $H_D(x) \mod p$ can be done in $O(d^2(\log d)^2)$ time [LL90] §5.10. Thus step 2 requires $O(\sqrt{p}\log^2 p)$ time , and under the assumption of GRH requires $O\big(\log^4 p(\log\log p)^2\big)$ time. Since $\left(\frac{D}{p}\right) = -1$ all the roots of $H_D(x)$ are supersingular **j**-invariants in characteristic p. $H_D(x)$ is a polynomial of degree $h(\sqrt{-D})$, the class number of the order of discriminant D, and this is $\ll |D|^{\frac{1}{2}+\epsilon}$, by Siegel's theorem. Finding a root of $H_D(x) \in \mathbb{F}_{p^2}$ can be done in $O(d^{1+\epsilon}\log^{2+o(1)} p)$ time using probabilistic factoring algorithms, where $d = |D|$. The graph with supersingular **j**-invariants over charactertistic p as vertices and ℓ-isogenies as edges is connected (see [Mes86]), consequently, we will always find a **j**-invariant in step 6 that is not one of $j_0, \cdots, j_i$. Thus the loop in steps $(5)\cdots(7)$ is executed exactly $\ell + 1$ times under the assumption that $S(p) \geq \ell + 1$. Even though Algorithm 1 requires $\tilde{O}(\ell^4 \log^2 q)$ time[1] in the worst case, we will argue that for *almost all* of the iterations of the loop it actually runs in $\tilde{O}(\ell^3 \log^2 q)$ time.

Lemma 3.1. *Let $E_1, \cdots, E_{S(p)}$ be the supersingular elliptic curves (unique up to isomorphism) defined over $\mathbb{F}_{p^2}$. Then for all but (possibly) four elliptic curves the extension degree*

$$[\mathbb{F}_{p^2}(E_i[\ell]) : \mathbb{F}_{p^2}],\ 1 \leq i \leq S(p)$$

divides $6(\ell - 1)$.

Proof : Let $E/\mathbb{F}_{p^2}$ be a supersingular curve and let t be the trace of Frobenius. Then the Frobenius map ϕ satisfies

$$\phi^2 - t\phi + p^2 = 0.$$

Suppose $t = \pm 2p$, then the characteristic equation of Frobenius factors as $(\phi \pm p)^2$. Thus the action of Frobenius on the vector space of ℓ-torsion points is not irreducible. In particular, there is a non-zero eigenspace $V \subseteq E[\ell]$, where ϕ acts as multiplication by $\pm p$. Thus there is a non-zero vector $v \in V$ whose orbit under Frobenius is of size dividing $\ell - 1$. Let P be the ℓ-torsion point corresponding to v. Then $[\mathbb{F}_{p^2}(P) : \mathbb{F}_{p^2}]$ divides $\ell - 1$. Since E is supersingular, its embedding degree is 6, thus the extension $\mathbb{F}_{p^2}(E[\ell])/\mathbb{F}_{p^2}(P)$ is of degree dividing 6. The number of isomorphism classes of elliptic curves with trace 0 or $\pm p$ over $\mathbb{F}_{p^2}$ is at most 4 by a theorem of Schoof [Sch87], this proves the result. □

Thus, except for possibly 4 iterations of the loop in steps $(5)\cdots(7)$, Algorithm 1 can be run with the quantity $n = 6(\ell - 1)$ (and we can test efficiently if this value of n works). Thus Algorithm 1 runs in expected time $O(\ell^{3+o(1)}\log^{2+o(1)} p)$ for all except (possibly) 4 iterations of the loop. Thus the loop runs in expected time $O(\ell^{4+o(1)}\log^{2+o(1)} p)$.

Writing the modular polynomial $\phi_\ell(x, y)$ as $x^{\ell+1} + \sum_{0\leq k\leq \ell} p_k(y)x^k$, we know that $p_0(y)$ is monic of degree $\ell + 1$ and $\deg(p_k(y)) \leq \ell$ for $1 \leq k \leq \ell$. Thus at the end of the loop in steps $(5)\cdots(7)$ we have enough information to solve for the $p_k(y)$ in step (8). We are solving $\ell+1$ systems of equations, each requiring an inversion of a matrix of size $(\ell+1)\times(\ell+1)$. This can be done in $O(\ell^4 \log^{1+o(1)} p)$ time. Since the polynomial $\phi_\ell(x, y) \mod p$ is the reduction of the classical modular polynomial, a polynomial with integer coefficients, the polynomial that we compute has coefficients in $\mathbb{F}_p$. Thus we have proved the following theorem:

Theorem 3.2. *Given ℓ and p distinct primes such that $S(p) \geq \ell + 1$, Algorithm 2 computes $\phi_\ell(x, y) \in \mathbb{F}_p[x, y]$ in expected time $O(\ell^{4+o(1)}\log^{2+o(1)} p + \log^4 p \log\log p)$ under the assumption of GRH.*

Hence, we can compute $\phi_\ell(x, y)$ modulo a prime p in $\tilde{O}(\ell^4 \log^2 p + \log^4 p)$ time if $p \geq 12\ell + 13$.

[1] We use the soft-Oh $\tilde{O}$ notation when we ignore factors of the form $\log \ell$ or $\log\log p$.

Remark 3.3. If one is allowed to pick the prime p, such as would be the case if we are computing ϕ_ℓ over the integers using the Chinese Remainder Theorem combined with this method, then one can eliminate the assumption of GRH in the above theorem. For example, for primes $p \equiv 3 \mod 4$ the **j**-invariant 1728 is supersingular. Thus in step (3) of Algorithm 2, we can start with $j_0 = 1728$ for any such prime. Hence we do not need the GRH to bound D in the analysis of the running time of the algorithm.

Acknowledgements: We would like to thank Igor Shparlinski and Steven Galbraith for useful suggestions and comments on an earlier draft of the paper. The first author would like to thank Microsoft Research for providing a stimulating research environment for this work.

References

[ALV03] Agashe, A.; Lauter, K.; Venkatesan, R.; *Constructing Elliptic Curves with a known number of points over a prime field*, in Lectures in honour of the 60th birthday of Hugh Cowie Williams, Fields Institute Communications Series, **42**, 1-17, 2003.

[Ank52] Ankeny, N., C.; *The least quadratic non-residue*, Annals of Math., (2), **55**, 65-72, 1952.

[BSS99] Blake, I.; Seroussi, G.; Smart, N.; *Elliptic Curves in Cryptography*, Lond. Math. Soc., Lecture Note Series, **265**, Cambridge University Press, 1999.

[BC03] Bosma, W.; Cannon, J.; *Handbook of MAGMA functions,* Sydney, 2003.

[Bur62] Burgess, D., A.; *On character sums and primitive roots*, Proc. London Math. Soc., **III**, **12**, 179-192, 1962.

[Elk98] Elkies, Noam; *Elliptic and modular curves over finite fields and related computational issues*, in Computational Perspectives on Number Theory: Proceedings of a Conference in Honor of A.O.L. Atkin (D.A. Buell and J.T. Teitelbaum, eds.), AMS/International Press, 21-76, 1998.

[Hup67] Huppert, Bertram; *Endliche Gruppen I*, Die Grundlehren der Mathematischen Wissenschaften, Band **134**, Springer-Verlag, 1967.

[LL90] Lenstra, A., K.; Lenstra, H., W., Jr.; *Algorithms in Number Theory*, Handbook of Theoretical Computer Science, Vol. **A**. Elsevier, 673-715, 1990.

[Mes86] Mestre, J.-F.; *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields, Nagoya Univ., Nagoya, 217-242, 1986.

[Sch87] Schoof, René; *Nonsingular Plane Cubic Curves over Finite Fields*, J. Combinatorial Theory, **46**, 2, 183-208, 1987.

[Sho94] Shoup, Victor; *Fast construction of irreducible polynomials over finite fields*, J. Symbolic Computation, **17**, 371-391, 1994.

[Sil86] Silverman, Joseph, H.; *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag, 1986.

[Vel71] Vélu, Jacques; *Isogénies entre courbes elliptiques*, C. R. Acad. Sc. Paris, **273**, 238-241, 1971.

Department of Computer Science, University of Wisconsin-Madison, Madison, WI - 53706.
E-mail address: `cdx@cs.wisc.edu`

Microsoft Research, One Microsoft Way, Redmond, WA - 98052.
E-mail address: `klauter@microsoft.com`