The AGM-$X_0(N)$ Algorithm

Heegner point lifting with application to elliptic curve point counting

David R. Kohel

School of Mathematics and Statistics
University of Sydney
Elliptic Curves in Cryptography

An elliptic curve $E/\mathbb{F}_p^r$ for cryptography is defined by:

$$E : y^2 + (a_1 x + a_3)y = x^3 + a_2 x^2 + a_4 x + a_6$$

determining a group of points $(x, y)$, where $p$ is the characteristic with $r$ typically in the range $160 \leq r \log_2(p) \leq 240$.

**Small characteristic**

- *Efficient point counting using p-adic lifting.*
- Fast Frobenius for group law.
- Restricted choice in coefficient domain.

**Medium characteristic**.

- Fast Frobenius for group law.
- Word-based operations convenient for software implementation.

**Large characteristic**.

- Ample choice of both characteristic and curve coefficients.
Parametrizations of Elliptic Curves

An elliptic curve admits an invariant called the $j$-invariant, which conversely determines a parametrization of elliptic curves:

$$E : y^2 + xy = x^3 - \frac{36}{j - 12^3}x - \frac{1}{j - 12^3}.$$

Two elliptic curves are isomorphic if and only if they share the same $j$-invariant.

If we specify that the elliptic curve is equipped with a fixed point of order 2, $P = (-1/4, 1/8)$, and that the isomorphism must preserve this point, then we obtain a new parametrization:

$$E : y^2 + xy = x^3 - 128sx^2 - \frac{36s}{64s + 1}x + \frac{512s^2 - s}{64s + 1}.$$

From the $j$-invariant, $j = (256s + 1)^3/s$, of this curve, we see that three such invariants $s$ determine one $j$. 
Parametrizations of Isogenies

The parameter $s = s_1$ determines an isomorphism is the isogeny:

$$E_1 : y^2 + xy = x^3 - 128s_1x^2 - \frac{36s_1}{64s_1 + 1}x + \frac{512s_1^2 - s_1}{64s_1 + 1}.$$ 

$$\downarrow \varphi$$

$$F_1 : y^2 + xy = x^3 - 128s_1x^2 - \frac{327680s_1^2 + 3136s_1 + 5}{16(64s_1 + 1)}x$$

$$+ \frac{(512s_1 + 1)(262144s_1^2 + 1984s_1 + 3)}{64(64s_1 + 1)},$$

consisting of the pair $(E_1, F_1)$ together with a map $\varphi$ of degree 2.

Conversely we can associate an invariant $s$ to any isogeny of degree 2 between elliptic curves; the isogenies are isomorphic if and only if they have the same $s$-invariant.
Elliptic Curve Invariants on $X_0(N)$

The $j$-invariant of an elliptic curve $E$ determines it uniquely up to isomorphism (over some algebraic extension field). The value $j(E)$ can be identified with a point $(j(E))$ on the modular curve $X(1)$ which parametrizes elliptic curves.

In a similar way, $X_0(2)$ classifies pairs $(E_1, E_2)$ of elliptic curves together with an isogeny $\varphi : E_1 \to E_2$ between them. The value of $s = s(\varphi)$ determines a point $(s(\varphi))$ on a curve $X_0(2)$.

Extending this further, we obtain an invariant $t$ which classifies triples of elliptic curves $(E_1, E_2, E_3)$, together with maps $\varphi_1 : E_1 \to E_2$ and $\varphi_2 : E_2 \to E_3$. From this invariant $(t(\varphi_2 \circ \varphi_1))$, on $X_0(4)$, we get an image point on $X_0(2)$

$$s = s(\varphi_1)$$

by forgetting the curve $E_3$. 


Towers of Modular Curves

The modular curves $X_0(2^n)$ classify isogenies of degree $2^n$, and corresponding to the factorization of these isogenies into degree 2 maps, we have induced maps of curves:

<table>
<thead>
<tr>
<th>Curve</th>
<th>Functions</th>
<th>Parametrized objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_0(4)$</td>
<td>$t$</td>
<td>$E_1 	o E_2 	o E_3$</td>
</tr>
<tr>
<td>$X_0(2)$</td>
<td>$s_1 = t(1 + 16t)$</td>
<td>$E_1 	o E_2$</td>
</tr>
<tr>
<td>$X(1)$</td>
<td>$j_1 = (1 + 256s)^3/s$</td>
<td>$E_1$</td>
</tr>
</tbody>
</table>
Modular Correspondences

In the previous example we could have constructed the map from $X_0(4)$ to $X_0(2)$ as follows:

$$
\begin{array}{ccc}
X_0(4) & t & E_1 \rightarrow E_2 \rightarrow E_3 \\
\downarrow & \downarrow & E_2 \rightarrow E_3 \\
X_0(2) & s_2 = t^2/(1 + 16t) &
\end{array}
$$

Thus we get two maps $X_0(4) \rightarrow X_0(2)$.

If $X_0(N)$ is a modular curve determined by the values of an invariant $s$, then associated to a pair of maps $X_0(pN) \rightarrow X_0(N)$, we obtain a map $X_0(pN) \rightarrow X_0(N) \times X_0(N)$, whose image is defined by a polynomial relation $\Phi(s_1, s_2) = 0$.

In the case $N = p = 2$ above, the modular correspondences gives the polynomial relation:

$$
\Phi(s_1, s_2) = s_1^2 - 16(256s_2 + 3)s_1s_2 - s_2 = 0.
$$
Solving Modular Correspondences

Starting with an equation $\Phi(x, y) = 0$ for the image of $X_0(Np)$ in $X_0(N) \times X_0(N)$, such that

$$\Phi(x, y) \cong x^p - y \mod p,$$

we obtain a $p$-adic lifting algorithm as follows.

For a target precision $m$ and initial value $x_1$ in $R = (\mathbb{Z}/p^m\mathbb{Z})[x]/(f(x))$, where $R \to \mathbb{F}_p^n$, for each $i$ we find the unique $x_{i+1}$ such that

$$\Phi(x_i, x_{i+1}) = 0,$$

beginning with the approximation $x_{i+1} = x_i^p$ and applying a Hensel lifting algorithm. The resulting sequence

$$x_1, \ldots, x_r, x_{r+1}, \ldots$$

is preperiodic, converging to the cycle of canonically lifted invariants

$$\tilde{x}_1, \ldots, \tilde{x}_r, \tilde{x}_1, \ldots$$

to the working precision $p^m$. 
Generic Solutions

We note that if $x$ is an indeterminate, then we can solve for the root $y = y(x)$ of $\Phi(x, y)$ in the power series ring $\mathbb{Z}_p[[x]]$. In our setting, the relation $\Phi(x, y) = 0$ has integral coefficients, has $-1$ for the coefficient of $y$, and reduces to $x^p - y \equiv 0 \mod p$, in fact the solution must be of the form

$$y(x) = x^p + a_{p+1}x^{p+1} + a_{p+2}x^{p+2} + \cdots \in \mathbb{Z}[[x]].$$

Then for a particular value $x = x_i$ we obtain $x_{i+1} = y(x_i)$. Moreover, if

$$\lim_{i \to \infty} a_i \to 0,$$

$p$-adically, we find successive polynomial approximations to $y(x)$.

N.B. Using a polynomial product representation, only a finite number of terms is required to obtain a given target precision.
The AGM-$X_0(N)$ Algorithm

Given $E/\mathbb{F}_q$ output $|E(\mathbb{F}_q)| = q - t + 1$.

**Step 1:** Heegner point lifting.

- Initialize $x_1 \equiv (j_1 - j_0)^{-1}$ in $R$ for some $j_0$.
- Apply analytic Frobenius iteration until reaching a precision of one word.
- Hensel lift $x_i$ in word-sized blocks to precision $n/2 + \varepsilon$.

**Step 2:** Determining Frobenius action to find $t$.

- Evaluate a precomputed expression for Frobenius $\pi_i$ in terms of $x_i$.
- Set $v_i = (\pi_i/p)^{-1}$, and compute $v = N(v_i)$ ($= \exp \circ \text{Tr} \circ \log(v_i)$).
- Recover $t \equiv v \mod q$ in the interval $[-2\sqrt{q}, 2\sqrt{q}]$. 

More
The END

Algorithm prototype in Magma:
http://magma.maths.usyd.edu.au/~kohel/magma/

Presentation slides:
Elliptic Curves in Cryptography

The set of points on $E$, together with a point at infinity $O$, forms an abelian group. The group operation is determined by the condition that three points on a line sum to $O$.

An elliptic curve $E$ over $\mathbb{F}_q$, together with a point $P = (x, y)$ of prime order $n$, is used in an ElGamal protocol, analogously to the use of the multiplicative group $\mathbb{F}_q^*$ of a finite field and an element $\alpha \in \mathbb{F}_q^*$ of prime order $n$ dividing $q - 1$.

Public key
\[
\begin{align*}
\text{ElGamal} & \quad \text{E.C. ElGamal} \\
\mathbb{F}_q^* & \quad E \\
\alpha & \quad P \\
\beta = \alpha^k & \quad Q = kP
\end{align*}
\]

In both cases the private key is an integer $k$. Security depends on the difficulty of solving the discrete logarithms $\log_P(Q)$ for $k$. 


History of $p$-Adic Lifting Algorithms

The following table gives a rough sketch of the key $p$-adic lifting algorithms, and an associated modular curve.

<table>
<thead>
<tr>
<th>Year</th>
<th>Algorithm</th>
<th>Modular Curve</th>
<th>Characteristic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1999-2000</td>
<td>Satoh</td>
<td>$X_0(1)$</td>
<td>$p &gt; 3$</td>
</tr>
<tr>
<td>2000-2001</td>
<td>FGH, SST (Satoh)</td>
<td>$X_0(1)$</td>
<td>$p = 2$</td>
</tr>
<tr>
<td>2000-2002</td>
<td>AGM (Mestre)</td>
<td>$X_0(8)$</td>
<td>$p = 2$</td>
</tr>
<tr>
<td>2002</td>
<td>MSST (Gaudry)</td>
<td>$X_0(8)$</td>
<td>$p = 2$</td>
</tr>
</tbody>
</table>

The present work unifies and generalizes these algorithms.
**Parametrizations of Isogenies**

\[
E_1 \xrightarrow{\varphi} F_1 \left( x + \frac{(256s + 1)^2}{4(64s + 1)(4x + 1)}, y - \frac{(256s + 1)^2(8x + 8y + 1)}{8(64s + 1)(4x + 1)^2} \right)
\]

If we then find an isomorphism with an elliptic curve in our parametrized family,

\[
F_1 \cong E_2 : y^2 + xy = x^3 - 128s_2x^2 - \frac{36s_2}{64s_2 + 1}x + \frac{512s_2^2 - s_2}{64s_2 + 1}
\]

we can iterate to form a chain of isogenies:
# Towers of Modular Curves

<table>
<thead>
<tr>
<th>Curve</th>
<th>Functions</th>
<th>Parametrized objects</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_0(32)$</td>
<td>$y^2 = 4x^3 + x$</td>
<td>$E_1 \to E_2 \to E_3 \to E_4 \to E_5 \to E_6$</td>
</tr>
<tr>
<td></td>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>$X_0(16)$</td>
<td>$v = y/(1 + 4x^2)$</td>
<td>$E_1 \to E_2 \to E_3 \to E_4 \to E_5$</td>
</tr>
<tr>
<td></td>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>$X_0(8)$</td>
<td>$u = v/(1 + 4v^2)$</td>
<td>$E_1 \to E_2 \to E_3 \to E_4$</td>
</tr>
<tr>
<td></td>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>$X_0(4)$</td>
<td>$t = u/(1 - 4u)^2$</td>
<td>$E_1 \to E_2 \to E_3$</td>
</tr>
<tr>
<td></td>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>$X_0(2)$</td>
<td>$s = t(1 + 16t)t$</td>
<td>$E_1 \to E_2$</td>
</tr>
<tr>
<td></td>
<td>$\downarrow$</td>
<td>$\downarrow$</td>
</tr>
<tr>
<td>$X(1)$</td>
<td>$j = (1 + 256s)^3/s$</td>
<td>$E_1$</td>
</tr>
</tbody>
</table>

Return
Generic Solutions

As an example we consider the modular correspondence equation

\[ \Phi(s_1, s_2) = s_1^2 - 16 (256s_2 + 3) s_1 s_2 - s_2 = 0, \]

for \( X_0(4) \to X_0(2) \times X_0(2) \). We obtain a generic power series solution

\[ s_2(s_1) = s_1^2 - 48s_1^3 + 2304s_1^4 - 114688s_1^5 + 5898240s_1^6 + \cdots \]

We can express this as a power product in the form

\[ s_2(s_1) = s_1^2 (1 - 3 (2^4 s_1)) (1 + 9 (2^4 s_1)^2) (1 - (2^4 s_1)^3) (1 + 87 (2^4 s_1)^4) \cdots \]

Since \( 2^{4i} \) converges to 0 in the 2-adic ring \( \mathbb{Z}_2 \), we only need to consider \( m/4 \) of these terms to evaluate this expression to precision \( m \).
Canonical Lifts

The Heegner point lifting algorithm succeeds for all but the finite number of supersingular curves. The invariants of the supersingular curves are poles of the generic solution to the modular correspondence.

A supersingular curve has $j = 0$ in characteristic 2, 3 or 5, has $j = -1$ for $p = 7$, and $j = 5$ for $p = 13$. If $j_0$ is a supersingular $j$-invariant, we have choosen a modular function $x$ such that the initial value $x \equiv (j - j_0)^{-1} \mod p$ forms the starting point of the lifting algorithm.

For any ordinary curve the algorithm yields the unique $p$-adic canonical lift of the Heegner point on the curve.
Determining Frobenius action

Associated to an elliptic curve

\[ y^2 + xy = x^3 + a_2 x^2 + a_4 x + a_6 \]

we can form the invariant differential \( dx/(2y + x) \).

A map \( \phi_i : E_i \to E_{i+1} \) over \( K \) induces a map \( \phi_i^*(dx/(2y + x)) = \pi_i dx/(2y + x) \) for some \( \pi_i \) in \( K \).