Computability and Complexity in Elliptic Curves and Cryptography
An Algorithm for Finding Elliptic Curves of Prime Order over $\mathbb{F}_p$

Thomas Morrell

AAAS Pacific Division Conference
24-27 June 2012
This is collaborative work with Dr. Liljana Babinkostova (Boise State University), Kevin Bombardier (Wichita State University), Matthew Cole (University of Notre Dame), and Cory Scott (Colorado College).
In public key cryptography, RSA and classical Diffie-Hellman rely upon large key sizes.
In public key cryptography, RSA and classical Diffie-Hellman rely upon large key sizes;
For ECC, key sizes are much smaller.
In public key cryptography, RSA and classical Diffie-Hellman rely upon large key sizes.

For ECC, key sizes are much smaller.

Developments in number theory and technology require use of larger and larger key sizes.
The Case for Using Elliptic Curves in Cryptography

- In public key cryptography, RSA and classical Diffie-Hellman rely upon large key sizes.
- For ECC, key sizes are much smaller.
- Developments in number theory and technology require use of larger and larger key sizes.
- Rate of key size increase less dramatic than for other public key cryptosystems.
In public key cryptography, RSA and classical Diffie-Hellman rely upon large key sizes.

For ECC, key sizes are much smaller.

Developments in number theory and technology require use of larger and larger key sizes.

Rate of key size increase less dramatic than for other public key cryptosystems.

The use of elliptic curves in cryptography necessitates the ability to construct curves of prime order, which are believed to be the most secure in cryptographic applications due to the Silver - Pohlig - Hellman algorithm for computing the discrete logarithm.
Our Motivation

**Conjecture**

\( a \) When \( E \) has CM, the probability that its order \( \#E \) is prime is inversely proportional to \( \lg p \).


\( c \) Babinkostova and Craig, Elliptic Pair of Primes, (in preparation).
Our Motivation

Conjecture

When $E$ has CM, the probability that its order $\#E$ is prime is inversely proportional to $\lg p$.

_________


Definition

An elliptic pair is an ordered pair of prime numbers $(p, q)$ such that the order of $E : y^2 = x^3 + k \mod p$ for some $k \not\equiv 0 \mod p$ is $q$. 
Our Motivation

Conjecture

\( abc \) When \( E \) has CM, the probability that its order \( \#E \) is prime is inversely proportional to \( \lg p \).

---


\(^c\) Babinkostova and Craig, Elliptic Pair of Primes, (in preparation).

Definition

An *elliptic pair* is an ordered pair of prime numbers \((p, q)\) such that the order of \( E : y^2 = x^3 + k \mod p \) for some \( k \not\equiv 0 \mod p \) is \( q \).

Since \( \pi(N) \sim \frac{N}{\lg N} \), this conjecture is equivalent to saying that the number of elliptic pairs is proportional to \( \frac{N}{\lg^2 N} \).
The number of elliptic pairs less than $N$ is approximately

$$A \frac{N}{\lg^2 N},$$

with experiment indicating $A \approx 0.6056$. 
Outline of the Algorithm

Algorithm

Input: A number of bits, $N$, that the prime $p$ should be
Output: An elliptic curve $E$ over $\mathbb{F}_p$ such that $\#E$ is prime

2. Find primitive root $g$ modulo $p$.
3. Compute the order of $E$ : $y^2 = x^3 + g$.
4. Test for primality using Miller-Rabin. If composite, start over and generate a new value for $p$. 
Let $N$ be the number of bits we want our primes $p$ to be:
Analysis of Runtime of Our Algorithm

Let $N$ be the number of bits we want our primes $p$ to be:

- Time required to find single prime $\tilde{O}(N^3)$: expect to have to try $O(N)$ values, each of which can be tested using Miller-Rabin in $\tilde{O}(N^2)$
Analysis of Runtime of Our Algorithm

Let $N$ be the number of bits we want our primes $p$ to be:

- Time required to find single prime $\tilde{O}(N^3)$: expect to have to try $O(N)$ values, each of which can be tested using Miller-Rabin in $\tilde{O}(N^2)$
- Computation of order $\tilde{O}(N^2)$
Analysis of Runtime of Our Algorithm

Let $N$ be the number of bits we want our primes $p$ to be:

- Time required to find single prime $\tilde{O}(N^3)$: expect to have to try $O(N)$ values, each of which can be tested using Miller-Rabin in $\tilde{O}(N^2)$
- Computation of order $\tilde{O}(N^2)$
- Test primality of order: $\tilde{O}(N^2)$
Let $N$ be the number of bits we want our primes $p$ to be:

- Time required to find single prime $\tilde{O}(N^3)$: expect to have to try $O(N)$ values, each of which can be tested using Miller-Rabin in $\tilde{O}(N^2)$
- Computation of order $\tilde{O}(N^2)$
- Test primality of order: $\tilde{O}(N^2)$
- Repeat previous steps until prime order is found ($O(N)$)

The overall complexity is $\tilde{O}(N^4)$. Sieving using small primes and finding values for $p$ of the form $p = x^2 + 3y^2$ can reduce the number of values we have to try down to polynomial in $\log N$. This reduces the overall complexity to $\tilde{O}(N^3)$. 
Analysis of Runtime of Our Algorithm

Let $N$ be the number of bits we want our primes $p$ to be:

- Time required to find single prime $\tilde{O}(N^3)$: expect to have to try $O(N)$ values, each of which can be tested using Miller-Rabin in $\tilde{O}(N^2)$.
- Computation of order $\tilde{O}(N^2)$.
- Test primality of order: $\tilde{O}(N^2)$.
- Repeat previous steps until prime order is found ($O(N)$).

The overall complexity is $\tilde{O}(N^4)$. 
Analysis of Runtime of Our Algorithm

Let \( N \) be the number of bits we want our primes \( p \) to be:

- Time required to find single prime \( \tilde{O}(N^3) \): expect to have to try \( O(N) \) values, each of which can be tested using Miller-Rabin in \( \tilde{O}(N^2) \)
- Computation of order \( \tilde{O}(N^2) \)
- Test primality of order: \( \tilde{O}(N^2) \)
- Repeat previous steps until prime order is found (\( O(N) \))

The overall complexity is \( \tilde{O}(N^4) \)

Sieving using small primes and finding values for \( p \) of the form \( p = x^2 + 3 \) can reduce the number of values we have to try down to polynomial in \( \log N \).

This reduces the overall complexity to \( \tilde{O}(N^3) \)
The order of $E$ when $j = 1728$

**Theorem**

Let $p > 3$ be an odd prime and let $k \not\equiv 0 \mod p$. Let $N_p = \#E(\mathbb{F}_p)$, where $E$ is the elliptic curve $y^2 = x^3 - kx$.

1. If $p \equiv 3 \mod 4$, then $N_p = p + 1$.
2. If $p \equiv 1 \mod 4$, write $p = a^2 + b^2$, where $a, b$ are integers with $b$ even and $a + b \equiv 1 \mod 4$. Then

$$N_p = \begin{cases} 
    p + 1 - 2a & \text{if } k \text{ is a fourth power mod } p \\
    p + 1 + 2a & \text{if } k \text{ is a QR but not a 4th power mod } p \\
    p + 1 \pm 2b & \text{if } k \text{ is a QNR mod } p.
\end{cases}$$

---


Here, QR and QNR denote quadratic residue and quadratic non-residue, respectively.
The order of $E$ when $j = 0$

**Theorem**

Let $p > 3$ be an odd prime and let $k \not\equiv 0 \pmod{p}$. Let $N_p = \#E(\mathbb{F}_p)$, where $E$ is the elliptic curve $y^2 = x^3 + k$.

1. If $p \equiv 2 \pmod{3}$, then $N_p = p + 1$.
2. If $p \equiv 1 \pmod{3}$, write $p = a^2 + 3b^2$,\(^a\) where $a, b$ are integers with $b$ positive and $a \equiv -1 \pmod{3}$.

\(^a\)Most previous authors formulate this theorem using $p = a^2 - ab + b^2$ instead.

Here, CR denotes cubic residue.
We compute \( \#E(\mathbb{F}_p) = p + 1 - \pi - \bar{\pi} \), where \( \pi = 0 \) if \( p \equiv 2 \) mod 3, and \( \pi = -\chi_6(k)^{-1}J(\chi_2, \chi_3) \) otherwise.
We compute $\#E(\mathbb{F}_p) = p + 1 - \pi - \bar{\pi}$, where $\pi = 0$ if $p \equiv 2 \mod 3$, and $\pi = -\chi_6(k)^{-1}J(\chi_2, \chi_3)$ otherwise.

**Corollary**

Let $p \equiv 1 \mod 3$ be a prime and let $k \not\equiv 0 \mod p$. If $\#E(\mathbb{F}_p)$ is prime, then $k$ is neither a QR nor a CR, except in the case where $p = 7$ and $k = 4$. 
We compute $\#E(\mathbb{F}_p) = p + 1 - \pi - \bar{\pi}$, where $\pi = 0$ if $p \equiv 2 \pmod{3}$, and $\pi = -\chi_6(k)^{-1}J(\chi_2, \chi_3)$ otherwise.

**Corollary**

Let $p \equiv 1 \pmod{3}$ be a prime and let $k \not\equiv 0 \pmod{p}$. If $\#E(\mathbb{F}_p)$ is prime, then $k$ is neither a QR nor a CR, except in the case where $p = 7$ and $k = 4$.

Note that in the case $j = 1728$, $\#E(\mathbb{F}_p)$ is always even, so it is not prime.
Computation of $a$ and $b$

The Smith-Cornacchia Algorithm is used to compute integers $a$ and $b$ such that

$$a^2 + db^2 = m$$

for given integers $d$ and $m$.

1. First, we find a value $r_0$ such that $r_0^2 \equiv -d \mod m$. If no such value exists, then there is no solution.

2. Next, we perform the Euclidean algorithm, computing $r_1 \equiv m \mod r_0$, etc.

3. We terminate the algorithm when we reach a value of $r_i < \sqrt{m}$. Then either $a = r_i$, $b = \sqrt{\frac{m-r_i^2}{d}}$ is a solution, or no solution exists.
Computation of $a$ and $b$

The Smith-Cornacchia Algorithm is used to compute integers $a$ and $b$ such that

$$a^2 + db^2 = m$$

for given integers $d$ and $m$.

1. First, we find a value $r_0$ such that $r_0^2 \equiv -d \mod m$. If no such value exists, then there is no solution.

2. Next, we perform the Euclidean algorithm, computing $r_1 \equiv m \mod r_0$, etc.

3. We terminate the algorithm when we reach a value of $r_i < \sqrt{m}$. Then either $a = r_i$, $b = \sqrt{\frac{m-r_i^2}{d}}$ is a solution, or no solution exists.

Since we are working with $m = p$ is prime, the first step can be achieved rapidly using the algorithm of Tonelli and Shanks.
Bröker and Stevenhagen\textsuperscript{1} also suggested an algorithm for generating an elliptic curve of prime order which runs in $\tilde{O}(N^3)$, but it is more difficult to implement.

Comparison to Other Algorithms

Bröker and Stevenhagen\textsuperscript{1} also suggested an algorithm for generating an elliptic curve of prime order which runs in $\tilde{O}(N^3)$, but it is more difficult to implement.

The algorithms have similar forms, but differ in the details:

\begin{itemize}
\item \textbf{Our Algorithm}:
  \begin{itemize}
  \item $p$ is modulus of curve
  \item Most time-consuming step involves finding $N$-bit primes
  \item Test primality of order
  \item Find elliptic curve at end
  \end{itemize}
\item \textbf{Their Algorithm}:
  \begin{itemize}
  \item $p$ is order of curve
  \item Most time-consuming step involves finding appropriate $D \equiv 5 \mod 8$
  \item Try to compute Hilbert class polynomial $P_D$ and find elliptic curve at end
  \end{itemize}
\end{itemize}

Bröker and Stevenhagen\footnote{Bröker and Stevenhagen, \textit{Constructing elliptic curves of prime order}, Contemporary Mathematics: Volume 20, 2007.} also suggested an algorithm for generating an elliptic curve of prime order which runs in $\tilde{O}(N^3)$, but it is more difficult to implement.

The algorithms have similar forms, but differ in the details:

<table>
<thead>
<tr>
<th>Our Algorithm</th>
<th>Their Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p$ is modulus of curve</td>
<td>$p$ is order of curve</td>
</tr>
<tr>
<td>Most time-consuming step</td>
<td>Most time-consuming step</td>
</tr>
<tr>
<td>involves finding $N$-bit primes</td>
<td>involves finding appropriate $D \equiv 5 \mod 8$</td>
</tr>
<tr>
<td>Test primality of order</td>
<td>Try to compute Hilbert class polynomial $P_D$ and</td>
</tr>
<tr>
<td>at end of algorithm</td>
<td>find elliptic curve at end</td>
</tr>
</tbody>
</table>
There are some incomplete results for dealing with the general CM case\(^\text{2,3}\). These are worthy of further investigation and generalization.

---


\(^3\) Rajwade, *Arithmetic on curves with complex multiplication by \(\sqrt{-2}\)*, Proclamations of the Cambridge Philosophical Society, Vol. 64. (1968), pp.659-672.
Future Directions

There are some incomplete results for dealing with the general CM case. These are worthy of further investigation and generalization.

It is unknown whether curves of the form $E : y^2 = x^3 + k$ are less suitable than others for cryptographic purposes, due to their simple form (although there is currently no evidence for this). The other CM curves should be incorporated into the algorithm.

---


Future Directions

There are some incomplete results for dealing with the general CM case.\textsuperscript{23} These are worthy of further investigation and generalization.

It is unknown whether curves of the form $E : y^2 = x^3 + k$ are less suitable than others for cryptographic purposes, due to their simple form (although there is currently no evidence for this). The other CM curves should be incorporated into the algorithm.

We still need a better analysis of the time complexity for finding primes of a given size. It is also probable that there exists a faster algorithm than the one we found.


\textsuperscript{3}Rajwade, \textit{Arithmetic on curves with complex multiplication by $\sqrt{-2}$}, Proclamations of the Cambridge Philosophical Society, Vol. 64. (1968), pp.659-672.
Theorem

If 2 is not a CR, then if \((p, q)\) is an elliptic pair, so is \((q, p)\).

Future Directions

**Theorem**

\textsuperscript{a} If 2 is not a CR, then if \((p, q)\) is an elliptic pair, so is \((q, p)\).


**Conjecture**

If 2 is a CR, then if \((p, q)\) is an elliptic pair, so is \((q, p)\).
Future Directions

**Theorem**

\[a\] If 2 is not a CR, then if \((p, q)\) is an elliptic pair, so is \((q, p)\).

---


**Conjecture**

If 2 is a CR, then if \((p, q)\) is an elliptic pair, so is \((q, p)\).

Can we use these results to prove that the number of elliptic pairs less than \(N\) is proportional to \(\frac{N}{\lg^2 N}\)?
Funding for this project is provided by the National Science Foundation (DMS 1062857) and by Boise State University.