In joint work with Alex Abatzoglou, Drew Sutherland, and Angela Wong, we give necessary and sufficient conditions for the primality of integers in sequences of a special form, using the $\mathcal{O}_K$-module structure of the reductions of an elliptic curve with CM by $\mathcal{O}_K$.

We use this to give deterministic algorithms that very quickly prove the primality or compositeness of the integers in certain sequences, and we implement the algorithms.
M. Agrawal, N. Kayal, & N. Saxena (2002) showed that the primality or compositeness of any integer can be determined in deterministic polynomial time.

With improvements of H. W. Lenstra and C. Pomerance, the time to test an integer $N$ is $\tilde{O}(\log^6 N)$. 
Faster algorithms have long been known for numbers in special sequences, such as:

- Fermat numbers $F_k = 2^{2^k} + 1$ using Pépin’s criterion (1877)
- Mersenne numbers $M_p = 2^p - 1$ using the Lucas-Lehmer test (1930)

These algorithms are deterministic and run in time $\tilde{O}(\log^2 N)$. 
Theorem (Pépin, 1877)

Let $F_k = 2^{2^k} + 1$. The following are equivalent:

- $F_k$ is prime.
- $3$ has order $2^{2^k}$ in $(\mathbb{Z}/F_k\mathbb{Z})^\times$.
- $3^{(F_k - 1)/2} \equiv -1 \pmod{F_k}$.

Our results can be viewed as elliptic curve analogues of this result.
In the mid-1980’s elliptic curves started to be used to give faster algorithms:

- Deterministic algorithm to compute square roots modulo primes (R. Schoof, 1985)
- Integer Factorization (H. W. Lenstra, Jr., 1987)
- Primality Testing (S. Goldwasser & J. Kilian, 1986)
W. Bosma (1985) and D. V. Chudnovsky & G. V. Chudnovsky (1986) gave probabilistic primality tests for numbers in certain sequences, using elliptic curve analogues of classical “$N − 1$” tests, where the group $(\mathbb{Z}/N\mathbb{Z})^\times$ is replaced by CM elliptic curves.
W. Bosma (1985) and D. V. Chudnovsky & G. V. Chudnovsky (1986) gave probabilistic primality tests for numbers in certain sequences, using elliptic curve analogues of classical “$N - 1$” tests, where the group $(\mathbb{Z}/N\mathbb{Z})^\times$ is replaced by CM elliptic curves.

S. Goldwasser & J. Kilian (1986) gave the first general purpose elliptic curve primality proving algorithm, using randomly generated elliptic curves. It runs in expected polynomial time.
Pomerance (1987) showed that for every prime $p$ there exists a certificate of primality that can be checked in time $\tilde{O}(\log^2 p)$ (but it might take exponential time to find the certificate).
Pomerance (1987) showed that for every prime $p$ there exists a certificate of primality that can be checked in time $\tilde{O}(\log^2 p)$ (but it might take exponential time to find the certificate).

D. Gordon (1989) proposed a general purpose compositeness test using supersingular reductions of CM elliptic curves over $\mathbb{Q}$. 
Pomerance (1987) showed that for every prime $p$ there exists a certificate of primality that can be checked in time $\tilde{O}(\log^2 p)$ (but it might take exponential time to find the certificate).

D. Gordon (1989) proposed a general purpose compositeness test using supersingular reductions of CM elliptic curves over $\mathbb{Q}$.

A. O. L. Atkin & F. Morain (1993) developed an improved version of the Goldwasser-Kilian algorithm that uses the “CM method” to construct elliptic curves with complex multiplication, rather than generating elliptic curves at random. It’s faster in practice, but runs in “heuristic polynomial time”.
B. Gross (2005) gave a primality test for Mersenne numbers using an elliptic curve with CM by $\mathbb{Q}(i)$ and supersingular reduction mod every Mersenne prime.
Some History of Primality Testing

- B. Gross (2005) gave a primality test for Mersenne numbers using an elliptic curve with CM by $\mathbb{Q}(i)$ and supersingular reduction mod every Mersenne prime.
- R. Denomme & G. Savin (2008) and A. Gurevich and B. Kunyavskiï (2009, 2012) extended Gross to get primality tests for certain special sequences, including Fermat numbers, using supersingular reductions of elliptic curves with CM by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. 
These results fit into the general framework laid out by Chudnovsky & Chudnovsky.

They use the $\mathcal{O}_K$-module structure of $E(\mathcal{O}_K/(\pi))$, where $E$ is an elliptic curve over $\mathbb{Q}$ with CM by $\mathcal{O}_K$, and $N_{K/\mathbb{Q}}(\pi)$ is tested for primality.

However, as Pomerance pointed out, the numbers they consider can all be dealt with using classical $N - 1$ or $N + 1$ primality tests that are more efficient and do not involve elliptic curves.
Jointly with Alex Abatzoglou, Drew Sutherland, and Angela Wong, we give necessary and sufficient conditions for the primality of integers \( N \) in special sequences. We give a general framework, using arbitrary CM elliptic curves.

We implement our results using elliptic curves with CM by \( \mathbb{Q}(\sqrt{-7}) \) and \( \mathbb{Q}(\sqrt{-15}) \), and obtain deterministic primality and compositeness tests that run in time \( \tilde{O}(\log^2 N) \).
Our work is in the Chudnovsky-Chudnovsky framework, and is an extension of the techniques used by Gross and Denomme-Savin.

However, the integers considered by them can be proved prime using more efficient classical $p \pm 1$ methods. We consider sequences for which that is not the case.
We obtain primes of size more than a million bits.

One of them is the largest proven prime $p$ for which no significant partial factorization of $p - 1$ or $p + 1$ is known.
Let

\[ K = \mathbb{Q}(\sqrt{-7}), \quad \alpha = \frac{1 + \sqrt{-7}}{2} \in \mathcal{O}_K, \]

\[ j_k = 1 + 2\alpha^k \in \mathcal{O}_K, \]

\[ J_k = N_{K/\mathbb{Q}}(j_k) = 1 + 2(\alpha^k + \overline{\alpha}^k) + 2^{k+2} \in \mathbb{N}. \]
Let

\[ K = \mathbb{Q}(\sqrt{-7}), \quad \alpha = \frac{1 + \sqrt{-7}}{2} \in \mathcal{O}_K, \]

\[ j_k = 1 + 2\alpha^k \in \mathcal{O}_K, \]

\[ J_k = N_{K/\mathbb{Q}}(j_k) = 1 + 2(\alpha^k + \overline{\alpha}^k) + 2^{k+2} \in \mathbb{N}. \]

We have

\[ J_1 = J_2 = 11, \quad J_3 = 23, \quad J_4 = 67, \]

\[ J_{k+4} = 4J_{k+3} - 7J_{k+2} + 8J_{k+1} - 4J_k. \]

We give primality/compositeness tests for \( J_k \).
\[ J_k \text{ is divisible by } 3 \text{ if and only if } k \equiv 0 \pmod{8}. \]
\[ J_k \text{ is divisible by } 5 \text{ if and only if } k \equiv 6 \pmod{24}. \]

Consider the family of quadratic twists:

\[ E_a : y^2 = x^3 - 35a^2x - 98a^3. \]

If \( a \in \mathbb{Q}^\times \), then \( E_a \) is an elliptic curve with complex multiplication by \( \mathbb{Q}(\sqrt{-7}) \).
Suppose \( k \geq 6, \ k \not\equiv 0 \pmod{8}, \) and \( k \not\equiv 6 \pmod{24}. \) Choose twisting factor \( a \) and \( P_a \in E_a(\mathbb{Q}) \) as follows.

<table>
<thead>
<tr>
<th>( k )</th>
<th>( a )</th>
<th>( P_a )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( k \equiv 0 \text{ or } 2 \pmod{3} )</td>
<td>( -1 )</td>
<td>( (1, 8) )</td>
</tr>
<tr>
<td>( k \equiv 4, 7, 13, 22 \pmod{24} )</td>
<td>( -5 )</td>
<td>( (15, 50) )</td>
</tr>
<tr>
<td>( k \equiv 10 \pmod{24} )</td>
<td>( -6 )</td>
<td>( (21, 63) )</td>
</tr>
<tr>
<td>( k \equiv 1, 19, 49, 67 \pmod{72} )</td>
<td>( -17 )</td>
<td>( (81, 440) )</td>
</tr>
<tr>
<td>( k \equiv 25, 43 \pmod{72} )</td>
<td>( -111 )</td>
<td>( (−633, 12384) )</td>
</tr>
</tbody>
</table>

Then \( P_a \) generates \( E_a(\mathbb{Q})/\text{torsion} \).
Theorem

The following are equivalent:

- $J_k$ is prime.
- $P_a \mod J_k$ has order $2^{k+1}$.
- $2^k P_a \equiv \left( \frac{-7+\sqrt{-7})a}{2}, 0 \right) \mod j_k$. 

Recall Pépin:

Theorem (Pépin, 1877)

Let $F_k = 2^{2^k} + 1$. The following are equivalent:

- $F_k$ is prime.
- 3 has order $2^{2^k}$ in $(\mathbb{Z}/F_k\mathbb{Z})^\times$.
- $3 \left( \frac{F_k-1}{2} \right) \equiv -1 \pmod{F_k}$.
Theorem

The following are equivalent:

- \( J_k \) is prime.
- \( P_a \mod J_k \) has order \( 2^{k+1} \).
- \( 2^k P_a \equiv \left( \frac{(-7+\sqrt{-7})a}{2}, 0 \right) \mod j_k. \)

Recall Pépin:

**Theorem (Pépin, 1877)**

Let \( F_k = 2^{2^k} + 1 \). The following are equivalent:

- \( F_k \) is prime.
- 3 has order \( 2^{2^k} \) in \( (\mathbb{Z}/F_k\mathbb{Z})^\times \).
- \( 3^{(F_k-1)/2} \equiv -1 \mod F_k. \)
What we really mean by “$P_a \mod J_k$ has order $2^{k+1}$” is:

$2^{k+1}P_a = O \mod J_k$ and $2^k P_a$ is strongly nonzero mod $J_k$,

where

**Definition**

Suppose $E$ is an elliptic curve over a number field $M$ and $\pi \in O_M$. We say that $P \in E(M)$ is **strongly nonzero** mod $\pi$ if one can express $P = (x : y : z) \in E(O_M)$ in such a way that $(z, \pi) = O_M$.

**Remarks**

1. *P is strongly nonzero mod $\pi$ if and only if $P \neq O \mod \beta$ for every prime $\beta | \pi$ in $O_M$.*

2. *In particular, if $\pi$ is prime, then $P$ is strongly nonzero mod $\pi$ if and only if $P \neq O \mod \pi$.*
Our choices of twisting factor imply that when $J_k$ is prime:

$$E_a(O_K/(j_k)) \equiv O_K/(2\alpha^k)$$

$$\equiv O_K/((\bar{\alpha}) \times O_K/(\alpha^{k+1}))$$

$$\equiv \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k+1}\mathbb{Z}.$$

We first show that $J_k$ being prime is equivalent to:

$$2\alpha^k P_a \equiv 0 \mod j_k \text{ and } 2\alpha^{k-1} P_a \text{ is strongly nonzero mod } j_k.$$
We converted the primality test to an efficient algorithm.

We then implemented the algorithm for all \( k \leq 1.2 \text{ million} \), and found 79 primes.

The largest, \( J_{1,111,930} \), has 334,725 decimal digits.
A general framework

Suppose:

- $K$ is an imag. quad. field with Hilbert class field $H$,
- $p_k = p_{(k_1, \ldots, k_t)} \in \mathcal{O}_H$ such that
  \[
  \pi_k := N_{H/K}(p_k) = 1 + \gamma \alpha_1^{k_1} \cdots \alpha_t^{k_t}
  \]
  with $\alpha_1, \ldots, \alpha_t, \gamma \in \mathcal{O}_K$,
- $F_k := N_{H/\mathbb{Q}}(p_k) = N_{K/\mathbb{Q}}(\pi_k)$,
- $E$ is an elliptic curve over $H$ with CM by $\mathcal{O}_K$,
- $P \in E(H)$ has infinite order.
A general framework

Theorem

Suppose $S \subset \mathbb{N}^t$ is such that whenever $k \in S$ and $p_k$ is prime, then

- the Frobenius endomorphism of $E \mod p_k$ is $\pi_k$, and
- $P \mod p_k \not\in \lambda E(\mathcal{O}_H/(p_k))$ for all prime ideals $\lambda | \prod \alpha_i$.

If $k \in S$ and $k \gg_\gamma 0$, then TFAE:

- $p_k$ is prime,
- $(\pi_k - 1)P = 0 \mod p_k$ and for every prime ideal $\lambda | \prod \alpha_i$ there is a point in
  \[
  \frac{(\pi_k - 1)}{\lambda} P
  \]
  that is strongly nonzero mod $p_k$.  


Well known results say that if \( P \mod N \) has sufficiently large order (in terms of \( N \)), then \( N \) is prime.
If the Frobenius endomorphism of $E \mod p_k$ is $\pi_k$, then

\[
E(\mathcal{O}_H/(p_k)) \cong \mathcal{O}_K/(\pi_k - 1) = \mathcal{O}_K/(\gamma\alpha_1^{k_1} \cdots \alpha_s^{k_s})
\]

so

\[
(\pi_k - 1)P = 0 \mod p_k
\]

as desired.

If $P \mod p_k \notin \lambda E(\mathcal{O}_H/(p_k))$ for all $\lambda | \prod \alpha_i$, then

\[
\frac{(\pi_k - 1)}{\lambda} P \not\equiv 0 \mod p_k
\]

as desired.
In our algorithms, the work is in finding a large nice set $S$ such that whenever $k \in S$ and $p_k$ is prime, then:

- the Frobenius endomorphism of $E$ modulo $p_k$ is $\pi_k$,
  and
- $P \mod p_k \notin \lambda E(\mathcal{O}_H/(p_k))$ for all prime ideals $\lambda | \prod \alpha_i$. 
Finding good $k$

For any given $k$, one could check whether $P \mod p_k \not\in \lambda E(O_H/(p_k))$.

But the goal is to determine the “good” $k$ in advance.

This is what allows us to obtain efficient deterministic primality tests.

However, finding a nice description of the $k$ for which $P \mod p_k \not\in \lambda E(O_H/(p_k))$ is constrained by:
Suppose:

- \( \hat{f} : E \to E' := E/E[\bar{\lambda}] \) is the natural isogeny,
- \( f : E' \to E \) is the dual isogeny,
- \( \mathfrak{p} \) is a prime ideal of \( \mathcal{O}_H \).

**Theorem**

The following are equivalent:

- \( P \mod \mathfrak{p} \notin \lambda E(\mathcal{O}_H/\mathfrak{p}) \),
- \( \mathfrak{p} \) splits completely in \( F := H(E[\lambda]) \) and \( \mathfrak{p} \) does not split completely in \( L := F(f^{-1}(P)) \).
When $L/H$ is an abelian extension, class field theory tells us that the splitting behavior in $L$ and $F$ of a prime of $\mathcal{O}_H$ is determined by congruence conditions.

If $L/H$ is not abelian, we do not know a good way to characterize the prime ideals of $\mathcal{O}_H$ that split completely in $F$ but not in $L$.

So we insist that $L/H$ be abelian.

We insist that $L \neq F$, since $p$ splits completely in $F$ but not $L$. 
**Proposition**

If $L/H$ is abelian, $L \neq F$, and $E$ is defined over $\mathbb{Q}(j(E))$, then either

1. 2 splits in $K$ and $\lambda$ is a prime above 2,
2. $\lambda$ is the prime above $p = 2$ or 3, and $p$ ramifies in $K$, or
3. $K = \mathbb{Q}(\sqrt{-3})$ and $\lambda = (2)$.

In the latter two cases, classical $p \pm 1$ primality tests apply.
If $E$ is defined over $\mathbb{Q}$ and one wants a simple description of congruence classes for the “good” $k$, one is restricted to

- $K = \mathbb{Q}(i)$ with $\alpha_i = 1 + i$, or
- $K = \mathbb{Q}(\sqrt{-2})$ with $\alpha_i = \sqrt{-2}$, or
- $K = \mathbb{Q}(\sqrt{-3})$ with $\alpha_i = 2$ or $\sqrt{-3}$, or
- $K = \mathbb{Q}(\sqrt{-7})$ with $\alpha_i = (1 \pm \sqrt{-7})/2$. 
Constraint when $K$ has class number one or two

If we only care about cases where classical $p \pm 1$ tests do not apply, that restricts us to:

For class number one:

$$K = \mathbb{Q}(\sqrt{-7}), \quad \alpha_i = (1 \pm \sqrt{-7})/2.$$ 

For class number two:

$$K = \mathbb{Q}(\sqrt{-15}), \quad \alpha_i = (1 \pm \sqrt{-15})/2.$$
Let $K = \mathbb{Q}(\sqrt{-15})$, which has class number 2 and Hilbert class field $H = K(\sqrt{5})$.

Let
\[
\beta := \frac{\sqrt{5} + \sqrt{-3}}{2}, \quad \alpha := \frac{1 + \sqrt{-15}}{2},
\]
\[
p_k := 1 + 2\beta^k \in \mathcal{O}_H, \quad \pi_k := N_{H/K}(p_k) = 1 - 4\alpha^k.
\]

We test the primality of
\[
F_k = N_{H/\mathbb{Q}}(p_k) = N_{K/\mathbb{Q}}(\pi_k) = 1 - 4 (\alpha^k + \bar{\alpha}^k) - 4^{k+2}.
\]
Example with $K = \mathbb{Q}(\sqrt{-15})$

$E : y^2 = x^3 + Ax + B$

$A = 3234(-16195646845 + 7242913457\sqrt{5})$,

$B = 38416(5395199151946361 - 2412806411180256\sqrt{5})$

Then $E$ has CM by $\mathcal{O}_K$.

$P = (0, 196(-51938421 + 23227568\sqrt{5})) \in E(H)$. 
Example with $K = \mathbb{Q}(\sqrt{-15})$

$S := \{ k \in \mathbb{N} : k \equiv 9, 19, 39, 45, 59, 63, 67,$

$85, 105, 123, 129, 133, 159, 169,$

$173, 181, 183, 221, 223, 225, 229 \pmod{240}\}. $

**Theorem**

If $k \in S$, then the following are equivalent:

- $F_k$ is prime.
- $P \mod p_k$ has order $2^{2k+2}$.
- $2^{2k+1}P \equiv (2643963\sqrt{5} - 5912081, 0) \mod p_k$. 
Example with $K = \mathbb{Q}(\sqrt{-15})$

What we mean by “$P \mod p_k$ has order $2^{2k+2}$” is:

$2^{2k+2}P \equiv 0 \mod p_k$ & $2^{2k+1}P$ is strongly nonzero mod $p_k$.

In fact, we show that $F_k$ being prime is equivalent to:

$4\alpha^k P \equiv 0 \mod p_k$ and $8\alpha^{k-1} P$ is strongly nonzero mod $p_k$.

Under our conditions, if $p_k$ is prime then

$$E(\mathcal{O}_H/(p_k)) \cong \mathcal{O}_K/(4\alpha^k)$$

$$\cong \mathcal{O}_K/(\lambda^2) \times \mathcal{O}_K/(\lambda^{2k+2})$$

$$\cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4^{k+1}\mathbb{Z}.$$
Here, $(2) = \lambda \bar{\lambda}$ where $\lambda = (2, \alpha)$.

Now $F := H(E[\lambda]) = H$ and $L := F(f^{-1}(P))$ has degree 2 over $H$, so $L/H$ is abelian.

Since $L/H$ is abelian and $p_k \in \mathcal{O}_H$ is explicit, we can compute $L$, and use it to determine congruence conditions on $k$ such that the Frobenius of $E$ mod $p_k$ is $\pi_k$ and $P$ mod $p_k \notin \lambda E(\mathcal{O}_H/(p_k))$ (whenever $p_k$ is prime).
So far, we have implemented this for all $k \leq 850,000$. In that range there are exactly 9 prime $F_k$’s, namely when $k = 9, 123, 3585, 16253, 17145, 79023, 100619, 501823,$ and 696123.

The prime $F_{696123}$ has 419,110 decimal digits. It is the largest proven prime $p$ for which no significant partial factorization of $p - 1$ or $p + 1$ is known.

We plan to check all $k \leq 10^6$. 
Deterministic elliptic curve primality proving for special sequences

Alice Silverberg

UC Irvine

GEOCRYPT 2013