Deterministic elliptic curve primality proving for special sequences

Alice Silverberg

UC Irvine

Hawaii Conference in Algebraic Number Theory,
Arithmetic Geometry and Modular Forms
March 8, 2012

Primality Proving

Manindra Agrawal, Neeraj Kayal, & Nitin Saxena (2002) showed that the primality or compositeness of any integer can be determined in deterministic polynomial time.

With improvements of Hendrik Lenstra and Carl Pomerance, the time to test an integer N is $\tilde{O}(\log^6 N)$.

Primality Proving

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 $\tilde{O}(\log^2 N)$.

Primality Testing

As pointed out by Pomerance, essentially all of primality testing is based on:

Theorem (Lucas)

If $a^{N-1} \equiv 1 \pmod{N}$*, and* $a^{(N-1)/p} \not\equiv 1 \pmod{N}$ *for all primes* $p|(N-1)$*, then* N *is prime.*

In other words (according to Carl Pomerance): “Build up a group that is so large that N is forced to be prime.”

Here, the group is

$$\langle a \rangle \subseteq (\mathbb{Z}/N\mathbb{Z})^{\times} = \mathbb{G}_m(\mathbb{Z}/N\mathbb{Z}).$$

Using Elliptic Curves to give faster Algorithms

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)

Bosma

In his 1985 Masters thesis “Primality testing using elliptic curves”, Wieb Bosma gave sufficient conditions for primality of numbers of a special form, using elliptic curve analogues of classical $N - 1$ tests.

The group $(\mathbb{Z}/N\mathbb{Z})^\times$ is replaced by elliptic curves with complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$.

It gives a probabilistic primality test, and does not prove compositeness.

Chudnovsky & Chudnovsky

D. V. Chudnovsky and G. V. Chudnovsky (1986) used elliptic curves with CM by $\mathbb{Q}(\sqrt{-D})$ to give sufficient conditions for the primality of integers in certain sequences

$$s_k = \mathrm{Norm}_{\mathbb{Q}(\sqrt{-D})/\mathbb{Q}}(1 + \alpha_0 \alpha_1^k),$$

defined by algebraic integers $\alpha_0, \alpha_1 \in \mathbb{Q}(\sqrt{-D})$.

They obtained a probabilistic primality test, which they implemented.

They also proposed using higher dimensional algebraic varieties, including abelian varieties with complex multiplication.

Goldwasser & Kilian

Shafi Goldwasser & Joe Kilian (1986) gave the first general purpose elliptic curve primality proving algorithm, using randomly generated elliptic curves.

It runs in expected polynomial time.

Gordon

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

Atkin & Morain

Oliver Atkin and François 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.

The algorithm is faster in practice, but runs in “heuristic polynomial time”.

Gross

Benedict Gross (2005) reinterpreted the Lucas-Lehmer test for Mersenne numbers in terms of the algebraic torus associated to the field $\mathbb{Q}(\sqrt{3})$.

He also gave a primality test for Mersenne numbers using the elliptic curve

$$E : y^2 = x^3 - 12x,$$

which has complex multiplication by $\mathbb{Q}(i)$ and has supersingular reduction modulo every Mersenne prime.

Denomme & Savin

Robert Denomme and Gordan Savin (2008), extending the ideas of Gross, gave primality tests for the Fermat numbers and for the sequences

$$2^{2^\ell} - 2^{2^{\ell-1}} + 1$$

and

$$3^{2^\ell} - 3^{2^{\ell-1}} + 1$$

using elliptic curves with complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$.

Tsumura

Using similar methods, Yu Tsumura (2011) obtained similar results for the sequence

$$2^p \pm 2^{(p+1)/2} + 1$$

using elliptic curves with CM by $\mathbb{Q}(i)$.

Gurevich & Kunyavskiĭ

A. Gurevich and B. Kunyavskiĭ (2009) reinterpreted classical primality tests for numbers of the form $h2^k \pm 1$ and put them in the framework of group schemes.

More recently (2012), they extend the framework of Gross and Denomme-Savin to give deterministic primality tests for numbers of the form

$$g^2 2^{2n-1} - g2^n + 1 \quad \text{and} \quad g^2 2^{2n} - g2^n + 1$$

using elliptic curves with CM by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$.

Gross, Denomme-Savin, Tsumura, Gurevich-Kunyavskiĭ

These results fit into the general framework laid out by Chudnovsky and Chudnovsky.

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.

Zero mod N

If $E \subset \mathbb{P}^2$ is an elliptic curve over $\mathbb{Q}$, we take points $P = (x : y : z) \in E(\mathbb{Q})$ so that $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$.

Definition

- $(x : y : z) = O \bmod N$ means that $N | z$.
- $(x : y : z) \neq O \bmod N$ means that $N \nmid z$.

If $P = O \bmod N$ then $P = O \bmod p$ for all primes $p | N$.

Strongly nonzero

Definition

Suppose E is an elliptic curve over $\mathbb{Q}$ and $P = (x : y : z) \in E(\mathbb{Q})$. We say that P is **strongly nonzero** mod N if $\gcd(z, N) = 1$.

Remarks

1. *If P is strongly nonzero mod N, then $P \neq O$ mod p for every prime $p|N$.*
2. *If N is prime, then P is strongly nonzero mod N if and only if $P \neq O$ mod N.*

Sufficient condition for primality

Proposition (Goldwasser-Kilian, Lenstra)

Suppose

- E *is an elliptic curve over* $\mathbb{Q}$,
- $P \in E(\mathbb{Q})$,
- $N \in \mathbb{Z}^+$ *such that* $\gcd(N, \mathrm{disc}(E)) = 1$,
- $m \in \mathbb{Z}^+$ *such that* $m > (N^{1/4} + 1)^2$,
- $mP = O \bmod N$, *and*
- $\frac{m}{q}P$ *is strongly nonzero mod* N *for all primes* $q|m$.

Then N *is prime.*

Proof

$mP = O \bmod N \implies mP = O \bmod p$ for all primes $p|N$, so the order d_p of P in $E(\mathbb{F}_p)$ divides m.

If $d_p < m$ for some prime $p|N$, then $d_p|\frac{m}{q}$ for some prime $q|m$, so $\frac{m}{q}P = O \bmod p$. This contradicts the hypothesis that $\frac{m}{q}P$ is strongly nonzero mod N for all primes $q|m$. So P has order m in $E(\mathbb{F}_p)$ for every prime $p|N$.

If N is not prime then N has a prime divisor $p \leq \sqrt{N}$, and

$$|E(\mathbb{F}_p)| \geq m > (N^{1/4} + 1)^2 \geq (p^{1/2} + 1)^2 = p + 1 + 2\sqrt{p},$$

contradicting the Hasse bound

$$|E(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}.$$

So N is prime.

Abatzoglou, Silverberg, Sutherland, & Wong

Jointly 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.

We use this to give a deterministic algorithm that very quickly proves the primality or compositeness of the integers N in certain sequences.

The algorithm runs in quasi-quadratic time: $\tilde{O}(\log^2 N)$.

Computations

We implemented the algorithm for a certain sequence and found the first 78 primes in the sequence. We believe that the 16 largest are the largest proven primes p that do not succumb to a classical $p-1$ or $p+1$ test.

Relation to prior work

Our work is in the Chudnovsky and Chudnovsky framework, and is a direct extension of the techniques used by Gross and by Denomme & Savin.

However, the integers considered by Gross, Denomme-Savin, Tsumura, and Gurevich-Kunyavskiĭ can be proved prime using more efficient classical $N \pm 1$ methods.

We consider a sequence for which that is not the case.

Our framework

Suppose (for simplicity) that K is an imaginary quadratic field of class number one, $\lambda_1, \ldots, \lambda_s$ are primes of $\mathcal{O}_K$, $\gamma \in \mathcal{O}_K - \{0\}$, and $k = (k_1, \ldots, k_s) \in \mathbb{N}^s$. Let

$$\Lambda_k = \gamma \lambda_1^{k_1} \cdots \lambda_s^{k_s}, \quad \pi_k = 1 + \Lambda_k, \quad F_k = \mathrm{Norm}_{K/\mathbb{Q}}(\pi_k).$$

Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ and positive rank over K, and fix $P \in E(K)$ of infinite order.

General result

Theorem

Suppose $\Sigma \subset \mathbb{N}^s$ is such that if $k \in \Sigma$ and π_k is prime, then:

- *the Frobenius endomorphism of E modulo π_k is π_k, and*
- *$P \bmod \pi_k \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$ for $i = 1, \ldots, s$.*

If $k \in \Sigma$ and $F_k > 16\,\mathrm{Norm}_{K/\mathbb{Q}}(\gamma)^2$, then F_k is prime if and only if

- *$\Lambda_k P = 0 \bmod \pi_k$, and*
- *$\frac{\Lambda_k}{\lambda_i} P$ is strongly nonzero mod π_k for all i.*

Sufficient condition for primality

To show that F_k is prime, use the result of Goldwasser-Kilian & Lenstra on sufficient conditions for primality.

For the other direction, first note that F_k is prime in $\mathbb{Z}$ if and only if π_k is prime in $\mathcal{O}_K$, since

$$F_k = \mathrm{Norm}_{K/\mathbb{Q}}(\pi_k).$$

The hypotheses

Our hypothesis is that k is in a nice set Σ such that whenever $k \in \Sigma$ and π_k is prime, then:

- the Frobenius endomorphism of E modulo π_k is π_k, and
- $P \bmod \pi_k \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$ for $i = 1, \ldots, s$.

Frobenius endomorphism

If π_k is prime, then the Frobenius endomorphism of E mod π_k corresponds, under the canonical embedding

$$\mathcal{O}_K \hookrightarrow \mathrm{End}(E \bmod \pi_k),$$

to either π_k or $-\pi_k$.

Structure of $E(\mathcal{O}_K/(\pi_k))$

If π_k is prime and the Frobenius endomorphism of E mod π_k is π_k, then

$$E(\mathcal{O}_K/(\pi_k)) \cong \ker(\text{Frob} - 1) \cong \ker(\pi_k - 1)$$
$$= \ker(\Lambda_k) \cong \mathcal{O}_K/(\Lambda_k)$$

so

$$\Lambda_k P = 0 \bmod \pi_k$$

as desired.

Necessary condition for primality

Continue to assume F_k is prime and the Frobenius endomorphism of E mod π_k is π_k.

We have

$$E(\mathcal{O}_K/(\pi_k)) \cong \mathcal{O}_K/(\Lambda_k) = \mathcal{O}_K/(\gamma\lambda_1^{k_1} \cdots \lambda_s^{k_s}).$$

If $P \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$ for $i = 1, \ldots, s$, then

$$\frac{\Lambda_k}{\lambda_i} P \neq 0 \mod \pi_k$$

for all i, as desired.

The goal

Our goal is to find a large nice set Σ such that if $k \in \Sigma$ and π_k is prime, then:

- the Frobenius endomorphism of E modulo π_k is π_k, and
- $P \bmod \pi_k \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$ for $i = 1, \ldots, s$.

Good k

For any given k, one could check whether $P \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$.

The method used by us and by Gross and Denomme-Savin determines a “good" k in advance.

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

Constraint

However, finding a nice description of the k for which $P \bmod \pi_k \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$ is constrained by the following. Let

$$F_i := K(E[\lambda_i]) \quad \subseteq \quad L_i := F_i(\lambda_i^{-1}(P)).$$

Proposition

The following are equivalent:

- $P \bmod \pi_k \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$,
- (π_k) *splits completely in* F_i/K *but does not split completely in* L_i/K.

Constraint

When L_i/K is an abelian extension, class field theory tells us that the splitting behavior in L_i of a prime ideal of $\mathcal{O}_K$ is determined by congruence conditions.

But if L_i/K is not abelian, then this is not true.

In general, we don't know a good way to characterize the prime ideals of K that split completely in F_i but not in L_i, so we lack a concise description of the "good" k.

Constraint

Requiring L_i/K to be abelian is a very strong constraint.

If $P \notin \lambda_i E(K)$, then it follows that $E[\lambda_i] \subset E(K)$.
However, elliptic curves with CM by K have only very limited torsion over K. If E is defined over $\mathbb{Q}$, this only happens when

- $\mathrm{Norm}_{K/\mathbb{Q}}(\lambda_i) = 2$, or
- $j = 0$ and $\mathrm{Norm}_{K/\mathbb{Q}}(\lambda_i) = 3$ or 4.

Constraint

So if E is defined over $\mathbb{Q}$ and one wants a simple description of congruence classes for the "good" k, one is restricted to

- $K = \mathbb{Q}(\sqrt{-7})$ with $\lambda_i = (1 \pm \sqrt{-7})/2$, or
- $K = \mathbb{Q}(\sqrt{-2})$ with $\lambda_i = \sqrt{-2}$, or
- $K = \mathbb{Q}(i)$ with $\lambda_i = 1 + i$, or
- $\mathbb{Q}(\sqrt{-3})$ with $\lambda_i = \sqrt{-3}$ or 2.

A sequence

Recall the framework:

$$\Lambda_k = \gamma\lambda_1^{k_1}\cdots\lambda_s^{k_s}, \quad \pi_k = 1+\Lambda_k, \quad F_k = \mathrm{Norm}_{K/\mathbb{Q}}(\pi_k).$$

Take

$$K = \mathbb{Q}(\sqrt{-7}), \quad s = 1, \quad \lambda_1 = \tfrac{1+\sqrt{-7}}{2}, \quad \gamma = 2,$$

so

$$\pi_k = 1+2\lambda_1^k \in \mathcal{O}_K, \qquad F_k = \pi_k\overline{\pi}_k \in \mathbb{N}.$$

Let's write J_k for F_k, and j_k for π_k.

A sequence

Then

$$J_k = 1 + 2(\lambda_1^k + \overline{\lambda}_1^k) + 2^{k+2}.$$

We have

$$J_1 = J_2 = 11, \quad J_3 = 23, \quad J_4 = 67,$$

and

$$J_{k+4} = 4J_{k+3} - 7J_{k+2} + 8J_{k+1} - 4J_k.$$

Family of elliptic curves

For $a \in \mathbb{Q}^\times$, consider the family of elliptic curves:

$$E_a : y^2 = x^3 - 35a^2x - 98a^3$$

with complex multiplication by $\mathbb{Q}(\sqrt{-7})$.

Twisting parameters a and points P_a

Given k, choose a and P_a as follows.

k	a	P_a
$k \equiv 0$ or $2 \pmod 3$	-1	$(1, 8)$
$k \equiv 4, 7, 13, 22 \pmod{24}$	-5	$(15, 50)$
$k \equiv 10 \pmod{24}$	-6	$(21, 63)$
$k \equiv 1, 19 \pmod{72}$	-17	$(81, 440)$
$k \equiv 25, 43, 49, 67 \pmod{72}$	-111	$(-633, 12384)$

Then $\text{rank}(E_a(\mathbb{Q})) = 1$, and P_a generates $E_a(\mathbb{Q})/\text{torsion}$.

Primality Test for the sequence J_k

Theorem

Suppose $k > 1$.
If $k \equiv 0 \pmod 8$ *or* $6 \pmod{24}$, *then* J_k *is composite.*
Otherwise, the following are equivalent:

- J_k *is prime.*
- $2^{k+1} P_a = 0$ *mod* J_k *and* $2^k P_a$ *is strongly nonzero mod* J_k.

Primality Test for the sequence J_k

To get from the general result to this, the hard work is in finding values of a for which there are many "good" k's, and computing the k's that work for a.

This means determining a good set Σ_a such that if $k \in \Sigma_a$ and j_k is prime, then:

- the Frobenius endomorphism of E_a mod j_k is j_k, and
- $P_a \bmod j_k \notin \lambda_1 E_a(\mathcal{O}_K/(j_k))$.

Generalized Legendre and Jacobi symbols

Definition

If $\alpha \in \mathcal{O}_K$ and π is a prime of $\mathcal{O}_K$, the *(generalized) Legendre symbol* is:

$$\left(\frac{\alpha}{\pi}\right) = \begin{cases} 0 & \text{if } \pi|\alpha, \\ 1 & \text{if } \alpha \text{ is a nonzero square mod } \pi, \\ -1 & \text{otherwise.} \end{cases}$$

The *(generalized) Jacobi symbol* is defined multiplicatively.

Frobenius endomorphism

Suppose a is a squarefree integer. Let

$$S_a := \left\{ k > 1 : \left(\frac{a}{J_k}\right)\left(\frac{j_k}{\sqrt{-7}}\right) = 1 \right\}.$$

Proposition (Gross, Stark)

If $k \in S_a$ and j_k is prime in $\mathcal{O}_K$, then the Frobenius endomorphism of E_a mod j_k is j_k.

The sets T_P

Definition

Suppose a is squarefree and $P \in E_a(K)$. Then the field $K(\lambda_1^{-1}(P))$ has degree 1 or 2 over K, so it can be written in the form $K(\sqrt{\delta_P})$ with $\delta_P \in K$. Let

$$T_P := \left\{k \in \mathbb{Z} : \left(\frac{\delta_P}{j_k}\right) = -1\right\}.$$

For $a \in \{-1, -5, -6, -17, -111\}$, let

$$T_a = T_{P_a}.$$

The sets T_P

Lemma

Suppose a is squarefree, $P \in E_a(K)$, $k \in \mathbb{N}$, and j_k is prime. Then

$$k \in T_P \iff P \notin \lambda_1 E_a(\mathcal{O}_K/(j_k)).$$

The sets T_P

Lemma

$$
\begin{aligned}
T_{-1} &= \mathbb{Z} \\
T_{-5} &= \{k \equiv 3, 4, 7, 8, 11, 13, \\
&\qquad\qquad 14, 15, 16, 17, 20, 22 \pmod{24}\} \\
T_{-6} &= \{k \equiv 1, 5, 10, 12, 15, 19, 20, 21, 22, 23 \pmod{24}\} \\
T_{-17} &= \mathbb{Z} \\
T_{-111} &= \{k \equiv 1, 2, 3, 6 \pmod{8}\}
\end{aligned}
$$

Proof

Given $k \in \mathbb{Z}^{>1}$ with $k \not\equiv 0 \pmod 8$ and $k \not\equiv 6 \pmod{24}$, choose twisting factor a and $P_a \in E_a(\mathbb{Q})$ as in the table:

k	a	P_a
$k \equiv 0$ or $2 \pmod 3$	-1	$(1, 8)$
$k \equiv 4, 7, 13, 22 \pmod{24}$	-5	$(15, 50)$
$k \equiv 10 \pmod{24}$	-6	$(21, 63)$
$k \equiv 1, 19 \pmod{72}$	-17	$(81, 440)$
$k \equiv 25, 43, 49, 67 \pmod{72}$	-111	$(-633, 12384)$

Then $k \in S_a \cap T_a$.

Proof

Since $k \in S_a$, the Frobenius endomorphism of E_a modulo j_k is j_k.

Since $k \in T_a$, we have $P \bmod j_k \notin \lambda_1 E_a(\mathcal{O}_K/(j_k))$.

Now apply the general result with $\Sigma = S_a \cap T_a$.

Recall:

Theorem

Suppose $\Sigma \subset \mathbb{N}^s$ *is such that if* $k \in \Sigma$ *and* π_k *is prime, then:*

- *the Frobenius endomorphism of* E *modulo* π_k *is* π_k*, and*
- $P \bmod \pi_k \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$ *for* $i = 1, \ldots, s$.

If $k \in \Sigma$ *and* $F_k > 16\,\mathrm{Norm}_{K/\mathbb{Q}}(\gamma)^2$*, then* F_k *is prime if and only if*

- $\Lambda_k P = 0 \bmod \pi_k$*, and*
- $\frac{\Lambda_k}{\lambda_i} P$ *is strongly nonzero mod* π_k *for all* i.

Large primes

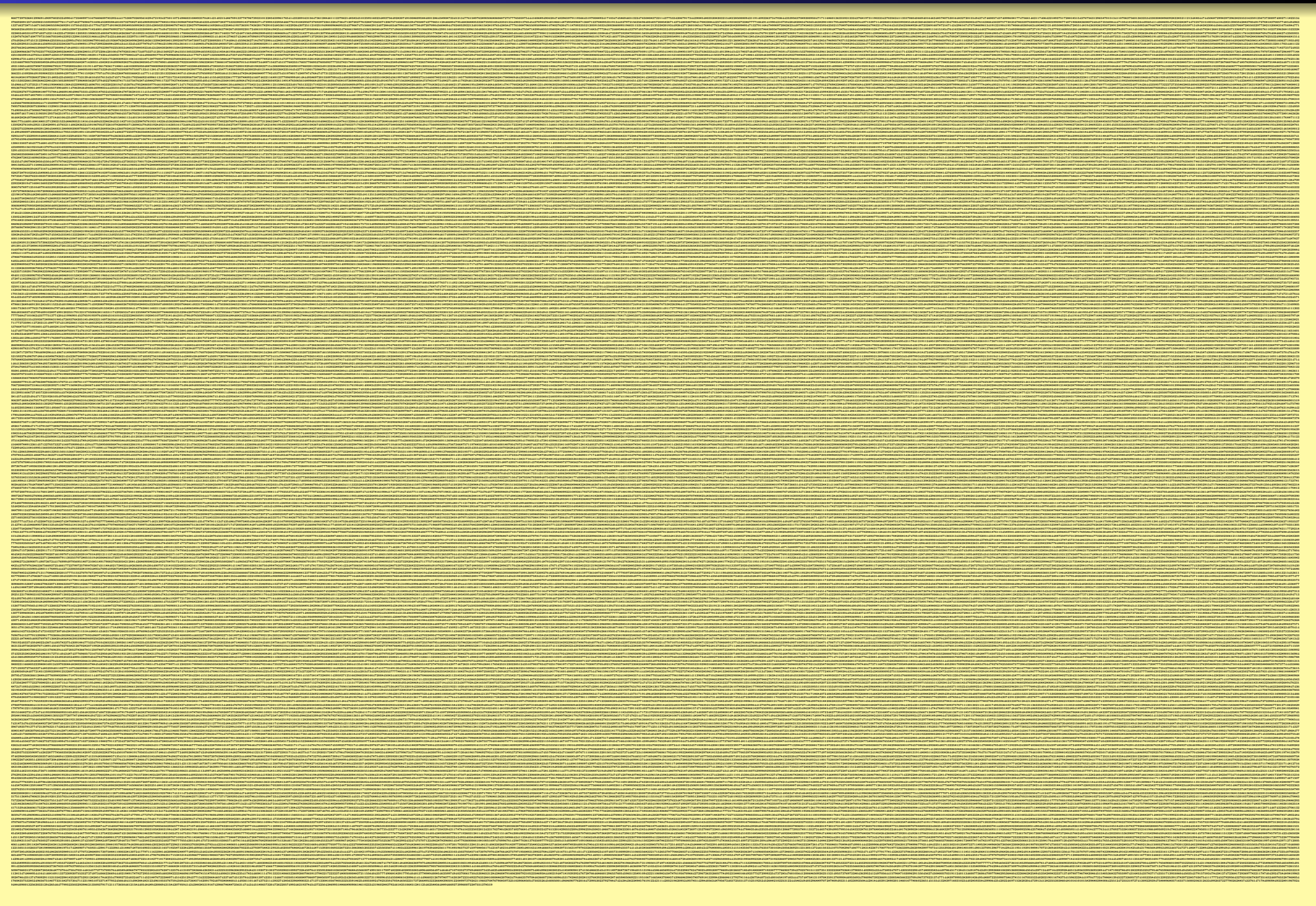
The 16 largest primes we've found so far in the sequence are the largest proven primes that do not succumb to a classical $N - 1$ or $N + 1$ test.

The largest prime J_k we've found so far is $J_{857,637}$ which has 258,176 decimal digits.

In 2000, it would have been the seventh largest prime, with only the Mersenne primes $M_{33}, M_{34}, M_{35}, M_{36}, M_{37}$, and M_{38} ahead of it.

As of Tuesday, it was ranked 2492.

$J_{857,637}$ (all 258,176 digits)



Other sequences

These methods also work for other sequences of the form

$$\begin{aligned}&\mathrm{Norm}_{K/\mathbb{Q}}(1+\gamma\lambda^{k_1}\bar{\lambda}^{k_2})\\&\qquad=1+\mathrm{Trace}_{K/\mathbb{Q}}(\gamma\lambda^{k_1}\bar{\lambda}^{k_2})+\mathrm{Norm}_{K/\mathbb{Q}}(\gamma)2^{k_1+k_2},\end{aligned}$$

with $K=\mathbb{Q}(\sqrt{-7})$ and $\lambda=\frac{1+\sqrt{-7}}{2}$.

Complexity

For numbers N, the algorithm runs in quasi-quadratic time: $\tilde{O}(\log^2 N)$.

For comparison, Goldwasser-Kilian has an expected runtime of $O(\log^{11} N)$, while Atkin-Morain has a heuristic runtime of $\tilde{O}(\log^4 N)$.

Work in Progress

We are working on generalizations to:

- elliptic curves with complex multiplication by fields of class number > 1,
- abelian surfaces with complex multiplication.

Deterministic elliptic curve primality proving for special sequences

Alice Silverberg

UC Irvine

Hawaii Conference in Algebraic Number Theory,
Arithmetic Geometry and Modular Forms
March 8, 2012