Deterministic elliptic curve primality proving for special sequences

Alice Silverberg

UC Irvine

ECC 2012

October 29, 2012

Deterministic Primality Proving

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.

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

Some History of 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 $\tilde{O}(\log^6 N)$.

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

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, where 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.

Pomerance

Carl 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).

The certificate (when $p > 31$) is an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$ with a point of order $2^r > (p^{1/4} + 1)^2$.

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” with a heuristic expected runtime of $\tilde{O}(\log^4 N)$.

Gross

Dick 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.

They use the $\mathcal{O}_K$-module structure of $E(\mathcal{O}_K/(\pi_k))$ (using an elliptic curve E with CM by $\mathcal{O}_K$, and testing primality of $N_{K/\mathbb{Q}}(\pi_k)$).

However, as Pomerance pointed out, the numbers they consider can all be dealt with using classical $p-1$ or $p+1$ primality tests that are more efficient and do not involve elliptic curves.

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

Large Primes

We implemented the algorithm for a certain sequence J_k for all $k \leq 1.2$ million, and found 79 primes.

The largest, $J_{1,111,930}$, has 334,725 decimal digits and more than a million bits.

Large Primes

At the time it was found, it was the largest proven prime p for which no significant partial factorization of $p-1$ or $p+1$ was known (it's now the second largest), and is the largest such prime with a "Pomerance proof".

As of last night, it was the 1500^{th} largest proven prime.

It was superseded by a 377,922 digit prime for which no significant factorization of $p-1$ or $p+1$ is known, found by David Broadhurst in July, who constructed an ECPP primality proof but not a Pomerance proof.

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 $p \pm 1$ methods, which is not the case for our sequence.

Notation

Let

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

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

$$J_k = \mathrm{Norm}_{K/\mathbb{Q}}(j_k) = 1 + 2(\alpha^k + \overline{\alpha}^k) + 2^{k+2} \in \mathbb{N}.$$

Notation

Let

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

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

$$J_k = \mathrm{Norm}_{K/\mathbb{Q}}(j_k) = 1 + 2(\alpha^k + \overline{\alpha}^k) + 2^{k+2} \in \mathbb{N}.$$

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.

Some composite J_k's

Remark

- J_k *is divisible by* 3 *if and only if* $k \equiv 0 \pmod 8$.
- J_k *is divisible by* 5 *if and only if* $k \equiv 6 \pmod{24}$.
- J_k *is divisible by* 17 *if and only if* $k \equiv 54 \pmod{144}$.
- J_k *is not divisible by* 2, 7, *or* 37.

Family of elliptic curves

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 $\mathbb{Q}(\sqrt{-7})$.

The twisting parameters a and points P_a

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 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	$(21, 63)$
$k \equiv 1, 19, 49, 67 \pmod{72}$	-17	$(81, 440)$
$k \equiv 25, 43 \pmod{72}$	-111	$(-633, 12384)$

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

Primality Test (main result)

Theorem

Suppose $k \geq 6$, $k \not\equiv 0 \pmod 8$, *and* $k \not\equiv 6 \pmod{24}$. *With* $P_a \in E_a(\mathbb{Q})$ *as in the Table, the following are equivalent:*

- J_k *is prime.*
- P_a *mod* J_k *has order* 2^{k+1}.

Sufficient condition for primality

The following is a variant of a result in Goldwasser-Kilian and Lenstra.

Proposition

Suppose N is odd, E is an elliptic curve over $\mathbb{Q}$, p is prime, and $\gcd(N, p\,\mathrm{disc}(E)) = 1$. *If $P \in E(\mathbb{Q})$ and P* mod *N has order $p^b > (\sqrt{N/3} + 1)^2$, then N is prime.*

The Proposition implies the easy direction of the Theorem, since $\gcd(J_k, 2\,\mathrm{disc}(E_a)) = 1$ and

$$2^{k+1} > (\sqrt{J_k/3} + 1)^2$$

when $k \geq 6$.

Necessary condition for primality

For the converse, suppose J_k is prime.

Our choice of a ensures that:

$$E_a(\mathbb{Z}/J_k\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k+1}\mathbb{Z}.$$

We need to show that P_a mod J_k has order 2^{k+1}.

Necessary condition for primality

More precisely, let

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

If $k \in S_a$ and j_k is prime in $\mathcal{O}_K$, then (by a result of Stark and Gross) the Frobenius endomorphism of E_a mod j_k is j_k (and not $-j_k$), and

$$\begin{aligned} E_a(\mathbb{Z}/J_k\mathbb{Z}) &\cong E_a(\mathcal{O}_K/(j_k)) \cong \mathcal{O}_K/(j_k - 1) \\ &= \mathcal{O}_K/(2\alpha^k) = \mathcal{O}_K/(\overline{\alpha}\alpha^{k+1}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k+1}\mathbb{Z} \end{aligned}$$

$$\implies 2^{k+1}P = 0 \mod J_k.$$

We compute the sets S_a.

Necessary condition for primality

We also compute sets $T_a \subset \mathbb{Z}^+$ such that if $k \in T_a$ (and J_k is prime) then

$$P_a \notin \alpha E_a(\mathcal{O}_K/(j_k)).$$

Since $2 = \alpha\bar{\alpha}$, it follows that if $k \in S_a \cap T_a$ and J_k is prime, then P_a mod J_k has order 2^{k+1}.

The sets T_P

Suppose a is squarefree and $P \in E_a(K)$.

Definition

The field $K(\alpha^{-1}(P))$ 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

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

Lemma

Suppose j_k is prime. Then

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

The sets T_a

For $a \in \{-1, -5, -6, -17, -111\}$, let $T_a = T_{P_a}$.

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 of main result

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	$(21, 63)$
$k \equiv 1, 19, 49, 67 \pmod{72}$	-17	$(81, 440)$
$k \equiv 25, 43 \pmod{72}$	-111	$(-633, 12384)$

Then $k \in S_a \cap T_a$.

Work in Progress

We are working on generalizations to:

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

Example with E not defined over $\mathbb{Q}$

We are trying to extend the theory to elliptic curves with CM by imaginary quadratic fields of class number > 1 (so E is not defined over $\mathbb{Q}$).

We are in the process of implementing our results for CM by $K = \mathbb{Q}(\sqrt{-15})$. Here, the elliptic curve is defined over the Hilbert class field $H = K(\sqrt{5})$ of K, and we are testing the primality of

$$F_k = N_{K/\mathbb{Q}}\left(1 - 4\alpha^k\right) = 1 - 4\left(\alpha^k + \bar{\alpha}^k\right) - 4^{k+2},$$

where $\alpha = \frac{1+\sqrt{-15}}{2}$.

A general 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 CM 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.*

Strongly nonzero

Definition

Suppose $\pi \in \mathcal{O}_K$, E is an elliptic curve over K, and $P = (x : y : z) \in E(\mathcal{O}_K)$. We say that P is **strongly nonzero** mod π if $\gcd(z, \pi) = 1$.

Remarks

1. *If π is prime, then P is strongly nonzero mod π if and only if $P \neq O$ mod π.*
2. *If P is strongly nonzero mod π, then $P \neq O$ mod β for every prime β of $\mathcal{O}_K$ with $\beta \mid \pi$.*

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

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

Necessary condition for primality

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

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

so

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

as desired.

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.

Finding good k

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 $i = 1, \ldots, s$.

Finding good k

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

But the goal is to determine the “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:

Proposition

The following are equivalent:

- $P \bmod \pi_k \notin \lambda_i E(\mathcal{O}_K/(\pi_k))$,
- (π_k) *splits completely in* $K(E[\lambda_i])/K$ *but does not split completely in* $K(E[\lambda_i], \lambda_i^{-1}(P))/K$.

Constraint

When $K(E[\lambda_i], \lambda_i^{-1}(P))/K$ is an abelian extension, class field theory tells us that the splitting behavior of a prime ideal of $\mathcal{O}_K$ is determined by congruence conditions.

But if $K(E[\lambda_i], \lambda_i^{-1}(P))/K$ is not abelian, then this is not true.

In general, we don't know a good way to characterize the prime ideals of $\mathcal{O}_K$ that split completely in $K(E[\lambda_i])$ but not in $K(E[\lambda_i], \lambda_i^{-1}(P))$, so we lack a concise description of the "good" k.

Constraint

Requiring $K(E[\lambda_i], \lambda_i^{-1}(P))/K$ to be abelian is a very strong constraint; if we assume it, and also assume $P \notin \lambda_i E(K)$, then $E[\lambda_i] \subset E(K)$.

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

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

Example with E not defined over $\mathbb{Q}$

Our example with $K = \mathbb{Q}(\sqrt{-15})$ works because $[H : K] = 2$ and $2 = \alpha\bar{\alpha}$ splits in $K/\mathbb{Q}$ (here, $\alpha = \frac{1+\sqrt{-15}}{2}$).

Letting $\lambda = (2, \alpha)$, a prime ideal of $\mathcal{O}_K$ above 2, it follows that $[H(E[\lambda], \lambda^{-1}(P)) : H] = 2$, so the extension is abelian.

Example with E not defined over $\mathbb{Q}$

We test the primality of $N_{H/\mathbb{Q}}(\beta_k)$ where

$$\beta_k = 1 + 2\left(\frac{\sqrt{5}+\sqrt{-3}}{2}\right)^k.$$

Then $\pi_k = N_{H/K}(\beta_k) = 1 - 4\alpha^k$ has a nice form.

Having such an explicit element β_k of $\mathcal{O}_H$ allows us to determine congruence conditions on k such that the Frobenius of E over $\mathcal{O}_H/(\beta_k)$ is π_k and

$$E(\mathcal{O}_H/(\beta_k)) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4^{k+1}\mathbb{Z}.$$

Deterministic elliptic curve primality proving for special sequences

Alice Silverberg

UC Irvine

ECC 2012

October 29, 2012