

# Deterministic Elliptic Curve Primality Proving for a Special Sequence of Numbers

Alex Abatzoglou, Alice Silverberg,  
Andrew V. Sutherland, Angela Wong

Tenth Algorithmic Number Theory Symposium  
University of California, San Diego  
July 9, 2012

# Recent History of Primality Proving

Agarwal, Kayal, and Saxena (2004) developed the AKS primality test which runs in deterministic polynomial time. The algorithm runs in  $\tilde{O}(k^6)$  time.

One can do even better with special sequences of numbers. Pépin's test, which tests Fermat numbers, and the Lucas-Lehmer test, which tests Mersenne numbers, are both deterministic and run in  $\tilde{O}(k^2)$  time.

# Recent History of Primality Proving

Agarwal, Kayal, and Saxena (2004) developed the AKS primality test which runs in deterministic polynomial time. The algorithm runs in  $\tilde{O}(k^6)$  time.

One can do even better with special sequences of numbers. Pépin's test, which tests Fermat numbers, and the Lucas-Lehmer test, which tests Mersenne numbers, are both deterministic and run in  $\tilde{O}(k^2)$  time.

# History of EC Primality Proving

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

Atkin-Morain (1993) improved upon this algorithm by using elliptic curves with complex multiplication. The Atkin-Morain algorithm has a heuristic expected running time of  $\tilde{O}(k^4)$ .

# Prior Work

Our work fits into a general framework given by D. V. Chudnovsky and G. V. Chudnovsky (1986) who used elliptic curves with complex multiplication by  $\mathbb{Q}(\sqrt{-D})$  to give sufficient conditions for the primality of integers in certain sequences  $\{s_k\}$ , where

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

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

# Prior Work

We extend the work done by Gross (2004) and Denomme-Savin (2008), who used elliptic curves with CM by  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\sqrt{-3})$  to test the primality of Mersenne, Fermat, and other related numbers.

However, as noted by Pomerance, the families of numbers they consider are susceptible to  $N - 1$  or  $N + 1$  primality tests that are more efficient than their tests using elliptic curves.

(see also Gurevich-Kunyavskii (2009, 2012), and Tsumura (2011))

## Prior Work

We extend the work done by Gross (2004) and Denomme-Savin (2008), who used elliptic curves with CM by  $\mathbb{Q}(i)$  or  $\mathbb{Q}(\sqrt{-3})$  to test the primality of Mersenne, Fermat, and other related numbers.

However, as noted by Pomerance, the families of numbers they consider are susceptible to  $N - 1$  or  $N + 1$  primality tests that are more efficient than their tests using elliptic curves.

(see also Gurevich-Kunyavskii (2009, 2012), and Tsumura (2011))

# The Plan

- Introduce a sequence of numbers,  $J_k$ , to test for primality.
- Present primality test that will tell us if  $J_k$  is prime or composite.
- Prove this primality test



# Our Work

We give necessary and sufficient conditions for the primality of integers of the form

$$J_k = N_{\mathbb{Q}(\sqrt{-7})/\mathbb{Q}} \left( 1 + 2 \left( \frac{1 + \sqrt{-7}}{2} \right)^k \right).$$

Initial sequence of  $J_k$ 's:

11, 11, 23, 67, 151, 275, 487, 963, 2039, 4211, ...

# Our Work

We use these conditions to give a deterministic algorithm that very quickly proves the primality or compositeness of  $J_k$ , using an elliptic curve  $E/\mathbb{Q}$  with complex multiplication by the ring of integers of  $\mathbb{Q}(\sqrt{-7})$ .

This algorithm runs in quasi-quadratic time:  $\tilde{O}(k^2)$ .

Note that the sequence of integers  $J_k$  does not succumb to classical  $N - 1$  or  $N + 1$  primality tests.

# Our Work

We use these conditions to give a deterministic algorithm that very quickly proves the primality or compositeness of  $J_k$ , using an elliptic curve  $E/\mathbb{Q}$  with complex multiplication by the ring of integers of  $\mathbb{Q}(\sqrt{-7})$ .

This algorithm runs in quasi-quadratic time:  $\tilde{O}(k^2)$ .

Note that the sequence of integers  $J_k$  does not succumb to classical  $N - 1$  or  $N + 1$  primality tests.

# $k$ 's for which $J_k$ is prime

2	63	467	3779	27140	414349
3	65	489	5537	31324	418033
4	77	494	5759	36397	470053
5	84	543	7069	47294	475757
7	87	643	7189	53849	483244
9	100	684	7540	83578	680337
10	109	725	7729	114730	810653
17	147	1129	9247	132269	857637
18	170	1428	10484	136539	1111930
28	213	2259	15795	147647	
38	235	2734	17807	167068	
49	287	2828	18445	167950	
53	319	3148	19318	257298	
60	375	3230	26207	342647	

# Large Primes We've Found

The largest prime we've found,  $J_{1111930}$ , has 334,725 decimal digits and is more than a million bits. It is currently the 1311<sup>th</sup> largest proven prime.

We believe this is currently the second largest known prime  $N$  for which no significant partial factorization of  $N - 1$  or  $N + 1$  is known and is the largest such prime with a Pomerance proof.

We've checked all  $k \leq 10^6$  and found 78 primes in this range.

# Large Primes We've Found

The largest prime we've found,  $J_{1111930}$ , has 334,725 decimal digits and is more than a million bits. It is currently the 1311<sup>th</sup> largest proven prime.

We believe this is currently the second largest known prime  $N$  for which no significant partial factorization of  $N - 1$  or  $N + 1$  is known and is the largest such prime with a Pomerance proof.

We've checked all  $k \leq 10^6$  and found 78 primes in this range.

# Differences From Chudnovsky-Chudnovsky

Recall Chudnovsky-Chudnovsky only gives sufficient conditions for primality. Our work gives both necessary and sufficient conditions, which allows us to construct a deterministic algorithm.

This is done by selecting explicit elliptic curves  $E/\mathbb{Q}$  and a point  $P \in E(\mathbb{Q})$  such that  $P$  reduces to a point of maximal order  $2^{k+1} \bmod J_k$  whenever  $J_k$  is prime.

## ECPP on $J_k$

Pomerance (1987) showed that for every prime  $p > 31$ , there exists an elliptic curve  $E/\mathbb{F}_p$  with a point of order  $2^r > (p^{1/4} + 1)^2$ . This can be used to establish the primality of  $p$  in  $r$  operations. The algorithm we will be presenting for our numbers  $J_k$  outputs exactly such a primality proof.



# Some Definitions

Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . We take points  $P = [x, y, z] \in E(\mathbb{Q})$  such that  $x, y, z \in \mathbb{Z}$  and  $\gcd(x, y, z) = 1$ .

## Definition

A point  $P = [x, y, z] \in E(\mathbb{Q})$  is *zero mod  $N$*  when  $N \mid z$ ; otherwise  $P$  is *nonzero mod  $N$* .

## Definition

Given a point  $P = [x, y, z] \in E(\mathbb{Q})$ , and  $N \in \mathbb{Z}$ , we say that  $P$  is *strongly nonzero mod  $N$*  if  $\gcd(z, N) = 1$ .

# Some Definitions

Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . We take points  $P = [x, y, z] \in E(\mathbb{Q})$  such that  $x, y, z \in \mathbb{Z}$  and  $\gcd(x, y, z) = 1$ .

## Definition

A point  $P = [x, y, z] \in E(\mathbb{Q})$  is *zero mod  $N$*  when  $N \mid z$ ; otherwise  $P$  is *nonzero mod  $N$* .

## Definition

Given a point  $P = [x, y, z] \in E(\mathbb{Q})$ , and  $N \in \mathbb{Z}$ , we say that  $P$  is *strongly nonzero mod  $N$*  if  $\gcd(z, N) = 1$ .

# Some Definitions

Let  $E$  be an elliptic curve over  $\mathbb{Q}$ . We take points  $P = [x, y, z] \in E(\mathbb{Q})$  such that  $x, y, z \in \mathbb{Z}$  and  $\gcd(x, y, z) = 1$ .

## Definition

A point  $P = [x, y, z] \in E(\mathbb{Q})$  is *zero mod  $N$*  when  $N \mid z$ ; otherwise  $P$  is *nonzero mod  $N$* .

## Definition

Given a point  $P = [x, y, z] \in E(\mathbb{Q})$ , and  $N \in \mathbb{Z}$ , we say that  $P$  is *strongly nonzero mod  $N$*  if  $\gcd(z, N) = 1$ .

# Strongly Nonzero

**Remark** Note the following:

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

# Notation

Let

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

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

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

We can define  $J_k$  recursively, like so:

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

with initial values  $J_1 = J_2 = 11$ ,  $J_3 = 23$ , and  $J_4 = 67$ .

# Notation

Let

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

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

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

We can define  $J_k$  recursively, like so:

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

with initial values  $J_1 = J_2 = 11$ ,  $J_3 = 23$ , and  $J_4 = 67$ .

# Sieving the Sequence $J_k$

When searching for prime  $J_k$  over a large range of  $k$ , we can accelerate this search by sieving out values of  $k$  for which we know  $J_k$  is composite:

## Lemma

- 1  $3 \mid J_k$  if and only if  $k \equiv 0 \pmod{8}$ ,
- 2  $5 \mid J_k$  if and only if  $k \equiv 6 \pmod{24}$ .

# Sieving the Sequence $J_k$

When searching for prime  $J_k$  over a large range of  $k$ , we can accelerate this search by sieving out values of  $k$  for which we know  $J_k$  is composite:

## Lemma

- 1  $3 \mid J_k$  if and only if  $k \equiv 0 \pmod{8}$ ,
- 2  $5 \mid J_k$  if and only if  $k \equiv 6 \pmod{24}$ .



# Elliptic Curves

We would like to consider a family of elliptic curves with complex multiplication by  $\mathbb{Q}(\sqrt{-7})$ .

For  $a \in \mathbb{Q}^\times$ , define the family of quadratic twists

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

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

# The Twisting Parameters $a$ and Points $P_a$

For  $k > 1$  such that  $k \not\equiv 0 \pmod{8}$  and  $k \not\equiv 6 \pmod{24}$ , we can choose a twisting factor  $a$  and a point  $P_a \in E_a(\mathbb{Q})$  as follows:

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

# Primality Test

## Theorem

Fix  $k > 1$  such that  $k \not\equiv 0 \pmod{8}$  and  $k \not\equiv 6 \pmod{24}$ . Based on this  $k$ , choose  $a$  as in the table above, with the corresponding  $P_a \in E_a(\mathbb{Q})$ . The following are equivalent:

- 1  $2^{k+1} P_a$  is zero mod  $J_k$  and  $2^k P_a$  is strongly nonzero mod  $J_k$ ,
- 2  $J_k$  is prime.

# Proof (The “Easy” Direction)

## Proposition (Goldwasser-Kilian, Lenstra)

*Let  $E/\mathbb{Q}$  be an elliptic curve, let  $N$  be a positive integer prime to  $\text{disc}(E)$ , let  $P \in E(\mathbb{Q})$ , and let  $m > (N^{1/4} + 1)^2$ . Suppose  $mP$  is zero mod  $N$  and  $(m/q)P$  is strongly nonzero mod  $N$  for all primes  $q|m$ . Then  $N$  is prime.*

Note that  $2^{k+1} > \left(J_k^{1/4} + 1\right)^2$  for  $k > 2$ . Let  $m = 2^{k+1}$  and  $\frac{m}{q} = 2^k$ . By this proposition, (1)  $\Rightarrow$  (2) of the Theorem.

# Proof (The “Harder” Direction)

Recall  $\alpha = \frac{1+\sqrt{-7}}{2}$  and  $j_k = 1 + 2\alpha^k$ .

- Define a set of  $k$ 's such that if  $j_k$  is prime, then  $E_a(\mathcal{O}_K/(j_k)) \cong \mathcal{O}_K/(2\alpha^k)$ .
- Define another set of  $k$ 's such that if  $j_k$  is prime, then  $P_a \notin \alpha(E_a(\mathcal{O}_K/(j_k)))$ .
- Show that for  $k$ 's in the intersection of the two sets for which  $j_k$  is prime,  $2^{k+1}$  annihilates  $P_a \bmod J_k$ , but  $2^k$  doesn't.

# Frobenius Endomorphism

For prime  $j_k \in \mathcal{O}_K$ , let  $\tilde{E}_a$  denote the reduction of  $E_a \bmod j_k$ .

## Proposition (Stark)

*If  $j_k \in \mathcal{O}_K$  is prime, then the Frobenius endomorphism of  $\tilde{E}_a$  is*

$$\left( \frac{a}{j_k} \right) \left( \frac{j_k}{\sqrt{-7}} \right) j_k.$$

Let  $a$  be a squarefree integer. Define

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

By the Stark result,

### Lemma

*Suppose  $a$  is a squarefree integer,  $k > 1$ , and  $j_k$  is prime in  $\mathcal{O}_K$ .*

- 1  $k \in S_a$  if and only if the Frobenius endomorphism of  $E_a$  over the finite field  $\mathcal{O}_K/(j_k)$  is  $j_k$ .*
- 2 If  $k \in S_a$ , then  $E_a(\mathcal{O}_K/(j_k)) \cong \mathcal{O}_K/(2\alpha^k)$  as  $\mathcal{O}_K$ -modules.*

Let  $a$  be a squarefree integer. Define

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

By the Stark result,

### Lemma

*Suppose  $a$  is a squarefree integer,  $k > 1$ , and  $j_k$  is prime in  $\mathcal{O}_K$ .*

- 1  $k \in S_a$  if and only if the Frobenius endomorphism of  $E_a$  over the finite field  $\mathcal{O}_K/(j_k)$  is  $j_k$ .
- 2 If  $k \in S_a$ , then  $E_a(\mathcal{O}_K/(j_k)) \cong \mathcal{O}_K/(2\alpha^k)$  as  $\mathcal{O}_K$ -modules.



Let  $a$  be a squarefree integer, and suppose that  $P \in E_a(K)$ . Then 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  $\delta_P \in K$ . Assuming  $j_k$  is prime, let

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

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

### Lemma

*Suppose that  $k > 1$ ,  $j_k$  is prime in  $\mathcal{O}_K$ , and  $a$  is a squarefree integer. Suppose that  $P \in E_a(K)$ , and let  $\tilde{P}$  denote the reduction of  $P \bmod j_k$ . Then  $\tilde{P} \notin \alpha \tilde{E}_a(\mathcal{O}_K/(j_k))$  if and only if  $k \in T_P$ .*

# Proof (The “Harder” Direction)

- Define a set  $S_a$  of  $k$ 's such that if  $j_k$  is prime, then  $E_a(\mathcal{O}_K/(j_k)) \cong \mathcal{O}_K/(2\alpha^k)$ .
- Define another set  $T_a$  of  $k$ 's such that if  $j_k$  is prime, then  $P_a \notin \alpha(E_a(\mathcal{O}_K/(j_k)))$ .
- Show that for  $k$ 's in the intersection of the two sets for which  $j_k$  is prime,  $2^{k+1}$  annihilates  $P_a \bmod J_k$ , but  $2^k$  doesn't.

# The Twisting Parameters $a$ and Points $P_a$

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

We considered  $S_a$  and  $T_a$  for a number of values of  $a$ , and found these five values covered all cases of  $k$  that weren't sieved out.

# Proof

Suppose that  $k > 1$  and  $J_k$  is prime. Let  $a$  be as in the table. Then  $k \in S_a \cap T_a$ . Let  $\tilde{P}$  denote the reduction of  $P_a$  mod  $J_k$ , and let  $\beta$  be the annihilator of  $\tilde{P}$  in  $\mathcal{O}_K$ .

Since  $k \in S_a$ , we have  $E_a(\mathcal{O}_K/(J_k)) \cong \mathcal{O}_K/(2\alpha^k)$  and therefore  $\beta \mid 2\alpha^k$ . We also have that

$k \in T_a \Rightarrow \tilde{P} \notin \alpha \tilde{E}_a(\mathcal{O}_K/(J_k))$ . Hence,  $\alpha^{k+1} \mid \beta$ .

Since  $2\alpha^k \mid 2^{k+1}$ , but  $\alpha^{k+1} \nmid 2^k$ , we must have  $2^{k+1}\tilde{P} = 0$  and  $2^k\tilde{P} \neq 0$ . □

# Proof

Suppose that  $k > 1$  and  $J_k$  is prime. Let  $a$  be as in the table. Then  $k \in S_a \cap T_a$ . Let  $\tilde{P}$  denote the reduction of  $P_a$  mod  $J_k$ , and let  $\beta$  be the annihilator of  $\tilde{P}$  in  $\mathcal{O}_K$ .

Since  $k \in S_a$ , we have  $E_a(\mathcal{O}_K/(J_k)) \cong \mathcal{O}_K/(2\alpha^k)$  and therefore  $\beta \mid 2\alpha^k$ . We also have that

$k \in T_a \Rightarrow \tilde{P} \notin \alpha \tilde{E}_a(\mathcal{O}_K/(J_k))$ . Hence,  $\alpha^{k+1} \mid \beta$ .

Since  $2\alpha^k \mid 2^{k+1}$ , but  $\alpha^{k+1} \nmid 2^k$ , we must have  $2^{k+1}\tilde{P} = 0$  and  $2^k\tilde{P} \neq 0$ . □

# Proof

Suppose that  $k > 1$  and  $J_k$  is prime. Let  $a$  be as in the table. Then  $k \in S_a \cap T_a$ . Let  $\tilde{P}$  denote the reduction of  $P_a$  mod  $J_k$ , and let  $\beta$  be the annihilator of  $\tilde{P}$  in  $\mathcal{O}_K$ .

Since  $k \in S_a$ , we have  $E_a(\mathcal{O}_K/(J_k)) \cong \mathcal{O}_K/(2\alpha^k)$  and therefore  $\beta \mid 2\alpha^k$ . We also have that

$k \in T_a \Rightarrow \tilde{P} \notin \alpha \tilde{E}_a(\mathcal{O}_K/(J_k))$ . Hence,  $\alpha^{k+1} \mid \beta$ .

Since  $2\alpha^k \mid 2^{k+1}$ , but  $\alpha^{k+1} \nmid 2^k$ , we must have  $2^{k+1}\tilde{P} = 0$  and  $2^k\tilde{P} \neq 0$ . □

# Conclusion




- We have shown a deterministic algorithm that proves primality or compositeness of our integers  $J_k$ .
- This algorithm runs in time  $\tilde{O}(k^2)$ .
- These  $J_k$  do not succumb to classical  $N \pm 1$  tests.






# Future Work

- We are currently working on extending our results to other elliptic curves with complex multiplication by imaginary quadratic fields of class number  $> 1$ .
- Another possibility we are considering is extending our results to abelian varieties of higher dimension.

# Select Bibliography I

-  D. V. Chudnovsky, G. V. Chudnovsky, *Sequences of numbers generated by addition in formal groups and new primality and factorization tests*, Adv. in Appl. Math **7** no. 4 (1986) 385–434.
-  R. Denomme, G. Savin, *Elliptic Curve Primality Tests for Fermat and Related Primes*, Journal of Number Theory **128** (2008) 2398–2412.
-  B. Gross, *An Elliptic Curve Test for Mersenne Primes*, Journal of Number Theory **110** (2005) 114–119.

# Select Bibliography II

-  A. Gurevich, B. Kunyavskii, *Primality testing through algebraic groups*, Arch. Math. (Basel) **93** (2009) 555–564.
-  A. Gurevich, B. Kunyavskii, *Deterministic primality tests based on tori and elliptic curves*, Finite Fields and Their Applications **18** (2012) 222–236.
-  H. M. Stark, *Counting Points on CM Elliptic Curves*, The Rocky Mountain Journal of Mathematics **26** (1996) 1115–1138.