Advances in Mathematics of Communications
Volume 8, No. 4, 2014, 427–436
doi:10.3934/amc.2014.8.427

SOME REMARKS ON PRIMALITY PROVING AND ELLIPTIC CURVES

Alice Silverberg

Department of Mathematics
University of California, Irvine
Irvine, CA 92697-3875, USA

(Communicated by Neal Koblitz)

Abstract. We give an overview of a method for using elliptic curves with complex multiplication to give efficient deterministic polynomial time primality tests for the integers in sequences of a special form. This technique has been used to find the largest proven primes N for which there was no known significant partial factorization of $N-1$ or $N+1$.

1. Introduction

In this article we will make some remarks on a technique for using elliptic curves to give efficient deterministic primality tests for integers in very special sequences. The goal is to explain, and put in context, some recent uses of this method [4, 30, 5, 1] that were inspired by papers of Benedict Gross (2005) [17] and Robert Denomme and Gordan Savin (2008) [11]. The implementations run in quasi-quadratic time, and are useful for proving the primality of large primes in certain sequences to which classical $p \pm 1$ tests do not apply.

In §2 we give a very brief history of some of the more relevant aspects of primality testing. We state Gross's result in §4, and give a proof of it that runs parallel to the proof of Pépin's primality test for Fermat numbers. We continue in §5 with results of Denomme and Savin that use similar techniques. In §7 we give highlights of a general framework for using CM elliptic curves to obtain fast deterministic primality tests, for which proofs will be given in [5]. In §6 and §8 we state concrete applications of the general framework (with proofs, details, and implementations given in [4, 30, 5, 1]). The primality testing theorems have been phrased in parallel ways to try to make clear how they are all related.

2. Brief history

Primality proving has a long and illustrious history. We will only touch on some very special aspects, and refer the reader to [24] for a nice short article by Carl Pomerance on primality testing, the book [10] for an excellent detailed exposition by Richard Crandall and Pomerance, and Hendrik Lenstra's ICM article [21] for historical remarks on elliptic curve primality testing.

2010 *Mathematics Subject Classification:* Primary 11Y11; Secondary 11G05, 14K22.
Key words and phrases: Primality, elliptic curves, complex multiplication.
This work was supported by the National Science Foundation under grant CNS-0831004.

To test an integer n for primality using trial division takes time $O(\sqrt{n})$. Fast primality tests used in practice are probabilistic; they make use of randomly chosen input, output "prime" on all prime inputs, and might (rarely) give the wrong answer for composite inputs. The Miller-Rabin (probabilistic) primality test runs in (polynomial) time $\tilde{O}(\log^2 n)$.

The "AKS" deterministic primality test of Manindra Agrawal, Neeraj Kayal, and Nitin Saxena (2002) [6] showed for the first time that the primality or compositeness of any integer can be determined in deterministic polynomial time. With improvements to AKS due to Lenstra and Pomerance [23], the time to test an integer n is $\tilde{O}(\log^6 n)$.

Fast deterministic algorithms (that run in time $\tilde{O}(\log^2 n)$) have long been known for numbers in special sequences, such as:

- Fermat numbers $2^{2^k}+1$ using Pépin's criterion (1877),
- Mersenne numbers 2^k-1 using the Lucas-Lehmer test (1930).

As Pomerance points out in [24], the following idea of Lucas "has been the basis of essentially all of primality testing".

Theorem 1 (Lucas, 1876)**.** *If $a \in \mathbb{Z}$, $a^{n-1} \equiv 1 \pmod{n}$, and $a^{(n-1)/p} \not\equiv 1 \pmod{n}$ for all primes $p|(n-1)$, then n is prime.*

In other words, if a has order $n-1$ in $(\mathbb{Z}/n\mathbb{Z})^\times$ then n is prime. As Pomerance puts it in [24], "The Lucas idea may be summed up as follows: build up a group so large that n must be prime."

Since the mid-1980's, elliptic curves have been used in algorithmic number theory to give deterministic algorithms that are faster than earlier algorithms that did not use elliptic curves, beginning with Réne Schoof's algorithm (1985) [26] for computing square roots modulo primes, and followed shortly thereafter by Lenstra's algorithm for factoring integers using elliptic curves (1987) [22].

In his 1985 Masters thesis "Primality testing using elliptic curves" [8], Wieb Bosma gave sufficient conditions for primality of numbers of special forms, using elliptic curve analogues of Lucas' test, where arithmetic in the group $(\mathbb{Z}/n\mathbb{Z})^\times$ is replaced by arithmetic in the reduction mod n of an elliptic curve with complex multiplication (CM) by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. This gives a probabilistic primality test.

David Chudnovsky and Gregory Chudnovsky (1986) [9] also used CM elliptic curves to give sufficient conditions for the primality of integers in certain sequences, and thereby gave a probabilistic primality test. They also proposed using higher dimensional varieties, including abelian varieties with complex multiplication.

Shafi Goldwasser and Joe Kilian (1986) [12, 13] gave the first general purpose elliptic curve primality proving algorithm, using randomly generated elliptic curves. It runs in expected polynomial time. Daniel Gordon (1989) [14] proposed a general purpose compositeness test using CM elliptic curves over $\mathbb{Q}$ with supersingular reduction. Oliver Atkin and François Morain (1993) [7] developed an improved version of the Goldwasser-Kilian algorithm that is faster in practice, but its expected polynomial runtime of $\tilde{O}(\log^4 n)$ is only heuristic.

3. Complex multiplication (CM)

We give some very brief remarks about elliptic curves with complex multiplication.

If E is an elliptic curve over a number field, $\mathfrak{p}$ is a prime of good reduction, and E has CM (i.e., $\mathrm{End}(E)$ is an order in an imaginary quadratic field), then one can

write down a formula for the number of points on E modulo $\mathfrak{p}$, in terms of E and $\mathfrak{p}$ (see [15, 16, 28, 25, 27]). An example that goes back to Gauss is the following. If E is $y^2 = x^3 - x$, then $\mathrm{End}(E) \cong \mathbb{Z}[i]$, where $i = \sqrt{-1}$ can be viewed as an endomorphism of E via $(x, y) \mapsto (-x, iy)$. If p is an odd prime, then

$$|E(\mathbb{F}_p)| = \begin{cases} p+1 & \text{if } p \equiv 3 \pmod 4, \\ p+1-2u & \text{if } p \equiv 1 \pmod 4, \end{cases}$$

where u is obtained by factoring $p = \pi\bar{\pi}$ in $\mathbb{Z}[i]$ in such a way that $\pi = u + vi \equiv 1 \pmod{2+2i}$. The two cases are the cases of supersingular and ordinary reduction, respectively.

4. Primality tests for Fermat and Mersenne numbers

We next present two proofs in parallel, in order to show the relationship between a classical primality test and the elliptic curve tests we are concerned with in this paper. The classical result is Pépin's test for primality of Fermat numbers, while the elliptic curve result is Gross's test for primality of Mersenne numbers. We present proofs designed to highlight the parallel structure, with arithmetic in the group of points on an elliptic curve over a finite field taking the place of arithmetic in the group $(\mathbb{Z}/n\mathbb{Z})^\times$.

Let $F_k := 2^{2^k} + 1$, the k-th Fermat number. It is known that the first five Fermat numbers $F_0, \ldots, F_4$ are prime, while $F_5, \ldots, F_{32}$ and many others are composite. The largest that is currently known to be composite is $F_{2,543,548}$. Complete factorizations of F_k are only known for $k \leq 11$. No factors of F_{24} are currently known. Using the prime number theorem, one can obtain a heuristic argument that there are only finitely many Fermat primes.

Let $M_k := 2^k - 1$, the k-th Mersenne number. If M_k is prime then k is prime. There are 48 Mersenne numbers that are known to be prime. The largest one, $M_{57,885,161}$, is also the largest known prime number. A heuristic argument using the prime number theorem gives the conjecture that there are infinitely many Mersenne primes.

Theorem 2 (Pépin, 1877)**.** *Let $F_k = 2^{2^k} + 1$. The following are equivalent:*

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

Sketch of proof. If F_k is prime, then the group $(\mathbb{Z}/F_k\mathbb{Z})^\times$ is cyclic of order $F_k - 1 = 2^{2^k}$, and 3 is a generator (since 3 is not a square mod F_k). Thus, 3 has order $F_k - 1$, and equivalently $3^{(F_k-1)/2} \equiv -1 \pmod{F_k}$ (the unique element of order 2 in $(\mathbb{Z}/F_k\mathbb{Z})^\times$).

Conversely, if 3 has order $F_k - 1$ in $(\mathbb{Z}/F_k\mathbb{Z})^\times$, then the subgroup generated by 3 is, in a sense, too big to fail to have F_k prime. This is Lucas' test with $n = F_k$, $a = 3$, and $p = 2$. □

Theorem 3 (Gross, 2005 [17])**.** *Let $M_k = 2^k - 1$, with odd $k \geq 3$. Let E denote the elliptic curve $y^2 = x^3 - 12x$ and let $P = (-2, 4) \in E(\mathbb{Q})$. The following are equivalent:*

(i) *M_k is prime.*
(ii) $(\frac{M_k+1}{2})P \equiv (0, 0) \pmod{M_k}$.

(iii) *P has order M_k+1 in $E(\mathbb{Z}/M_k\mathbb{Z})$.*

Sketch of proof. If M_k is prime, then (using the theory of elliptic curves over finite fields) one can show that E mod M_k is supersingular, and $E(\mathbb{Z}/M_k\mathbb{Z})$ is a cyclic group of order $M_k+1=2^k$ generated by P. Then $(\frac{M_k+1}{2})P \equiv (0,0) \pmod{M_k}$, the unique element of order 2 in $E(\mathbb{Z}/M_k\mathbb{Z})$.

Conversely, if P mod M_k has order $M_k+1=2^k$, then P mod q has that order for some prime divisor q of M_k. Thus, $M_k+1 \le |E(\mathbb{F}_q)| \le q+1+2\sqrt{q}$ using Hasse's bound, so $q \mid M_k \le q+2\sqrt{q}$. It follows that $q=M_k$ is prime. This is basically an analogue for elliptic curves of Lucas' test, with $n=M_k$, $a=P$, and $p=2$, and with M_k+1 serving the role played by $n-1$ in Lucas' test. Here, it is the subgroup generated by P that is too big for M_k to fail to be prime. □

5. Examples with CM by $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$

Denomme and Savin [11], extending the work of Gross, gave an elliptic curve analogue of the Pépin test for Fermat numbers, and also gave primality tests for other sequences.

Theorem 4 (Denomme-Savin, 2008 [11])**.** *Let E denote the elliptic curve $30y^2 = x^3-x$, which has CM by $\mathbb{Z}[i]$, let $P=(5,2)\in E(\mathbb{Q})$, and for $k\ge 2$ let $f_k := 2^{2^{k-1}}+i \in \mathbb{Z}[i]$ and $F_k = f_k\bar{f}_k = 2^{2^k}+1$. Then the following are equivalent:*

(i) *F_k is prime.*
(ii) $(1+i)^{2^k-1}P \equiv (0,0) \pmod{f_k}$.

The proof uses that whenever F_k is prime, then P generates the cyclic $\mathbb{Z}[i]$-module

$$E(\mathbb{Z}[i]/(f_k)) \cong \mathbb{Z}[i]/((1+i)^{2^k}).$$

Conversely, if F_k is composite and $p<\sqrt{F_k}$ is a prime divisor of F_k, one applies the Hasse bound to $E(\mathbb{Z}/p\mathbb{Z}) = E(\mathbb{Z}[i]/(\pi))$ where $p=\pi\bar{\pi}$. If (ii) holds then the point P mod π generates too large a $\mathbb{Z}[i]$-submodule of $E(\mathbb{Z}[i]/(\pi))$ for E mod π to satisfy the Hasse bound.

Theorem 5 (Denomme-Savin, 2008 [11])**.** *Let E denote the elliptic curve $y^2 = 30x^3+\frac{1}{4}$, which has CM by $\mathbb{Z}[\rho]$ where $\rho=\frac{-1+\sqrt{-3}}{2}$, let $P=(\frac{1}{2},2)\in E(\mathbb{Q})$, and for $\ell\ge 2$ let $k_\ell := -1-3^{2^{\ell-1}}\rho \in \mathbb{Z}[\rho]$ and $K_\ell := k_\ell\overline{k_\ell} = 3^{2^\ell} - 3^{2^{\ell-1}}+1$. Then the following are equivalent:*

(i) *K_ℓ is prime.*
(ii) $(\sqrt{-3})^{2^\ell-1}P \equiv (0,\pm\frac{1}{2}) \pmod{k_\ell}$.

Here, if K_ℓ is prime, then P generates the cyclic $\mathbb{Z}[\rho]$-module

$$E(\mathbb{Z}[\rho]/(k_\ell)) \cong \mathbb{Z}[\rho]/((\sqrt{-3})^{2^\ell}).$$

Theorem 6 (Denomme-Savin, 2008 [11])**.** *Let E denote the elliptic curve $7y^2 = x^3+1$, which has CM by $\mathbb{Z}[\rho]$, let $P=(3,2)\in E(\mathbb{Q})$, and for $k\ge 2$ let $j_k := \rho+2^{2^{k-1}}\bar{\rho} \in \mathbb{Z}[\rho]$ and $J_k := j_k\bar{j_k} = 2^{2^k} - 2^{2^{k-1}}+1$. Then the following are equivalent:*

(i) *J_k is prime.*
(ii) $2^{2^{k-1}-1}P \equiv (-\rho^r,0) \pmod{j_k}$ *with* $r\in\{0,1,2\}$.

If J_k is prime, then the point P generates the cyclic $\mathbb{Z}[\rho]$-module

$$E(\mathbb{Z}[\rho]/(j_k)) \cong \mathbb{Z}[\rho]/(2^{2^{k-1}}).$$

Using similar methods, Yu Tsumura (2011) [29] obtained similar results for the sequence $2^p \pm 2^{(p+1)/2} + 1$ using elliptic curves with CM by $\mathbb{Q}(i)$. Alexander Gurevich and Boris Kunyavskiĭ (2009, 2012) [18, 19] extended the framework of Gross and Denomme-Savin to give deterministic primality tests for numbers of the form $g^2 2^{2n-1} - g2^n + 1$ and $g^2 2^{2n} - g2^n + 1$. They also considered other algebraic groups, as did Masanari Kida (2004) [20]. The CM elliptic curves in all these tests have CM by $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$.

As pointed out by Pomerance (see [24]), the numbers considered by Gross, Denomme-Savin, etc. can all be dealt with using classical $p-1$ or $p+1$ primality tests à la Lucas and Pépin that are more efficient and do not involve elliptic curves.

6. CM elliptic curves over $\mathbb{Q}$

In joint work with Alex Abatzoglou, Drew Sutherland, and Angela Wong, we extend the above work to a general framework. We implement our results to test primality even in sequences for which classical $p \pm 1$ primality tests do not apply.

Using CM elliptic curves defined over $\mathbb{Q}$, the methods of Gross and Denomme-Savin extend nicely only for elliptic curves with CM by $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-3})$, or $\mathbb{Q}(\sqrt{-7})$. The reason that this is so is briefly explained in §7.2 below (see [5] for details). We also explain why CM by $\mathbb{Q}(\sqrt{-7})$ is the only case not amenable to $p \pm 1$ primality tests. In [4] we implement a primality testing algorithm that uses elliptic curves with CM by $\mathbb{Q}(\sqrt{-7})$, for a sequence that does not succumb to classical $p \pm 1$ tests; in this section we state the theorem on which our algorithm relies.

Let $\alpha = \frac{1+\sqrt{-7}}{2}$, $j_k = 1 + 2\alpha^k$, and $J_k = j_k \bar{j_k} = 1 + 2(\alpha^k + \overline{\alpha}^k) + 2^{k+2} \in \mathbb{N}$. An equivalent definition of the sequence J_k is to let $J_k = 2^{k+2} + 1 + T_k$ where $T_0 = 4$, $T_1 = 2$, and $T_{k+1} = T_k - 2T_{k-1}$. Heuristics using the prime number theorem imply the conjecture that infinitely many J_k are prime. Theorem 8 below gives primality/compositeness tests for the sequence J_k.

Remarks 7. (a) J_k is divisible by 3 if and only if $k \equiv 0 \pmod 8$.
(b) J_k is divisible by 5 if and only if $k \equiv 6 \pmod{24}$.

For $0 \neq a \in \mathbb{C}$, let E_a denote the elliptic curve $y^2 = x^3 - 35a^2x - 98a^3$. Given $k > 1$ with $k \not\equiv 0 \pmod 8$ and $k \not\equiv 6 \pmod{24}$, choose a and $P \in E_a(\mathbb{Q})$ as follows:

k	a	P
$k \equiv 0$ 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	$(-633, 12384)$

Theorem 8 (Abatzoglou-Silverberg-Sutherland-Wong, 2012)**.** *Suppose $k \geq 6$, $k \not\equiv 0 \pmod 8$, $k \not\equiv 6 \pmod{24}$, and a and P are as in the table. Then the following are equivalent:*

(i) *J_k is prime.*
(ii) $2^k P \equiv \left(\frac{(-7+\sqrt{-7})a}{2}, 0\right)$ *in* $E_a \mod j_k$.

(iii) *P has order 2^{k+1} in $E_a(\mathbb{Z}/J_k\mathbb{Z})$.*

If J_k is prime, then as $\mathbb{Z}[\alpha]$-modules we have

$$\begin{aligned} E_a(\mathbb{Z}[\alpha]/(j_k)) &\cong \mathbb{Z}[\alpha]/(2\alpha^k) \\ &\cong \mathbb{Z}[\alpha]/(\overline{\alpha}) \times \mathbb{Z}[\alpha]/(\alpha^{k+1}). \end{aligned}$$

Thus as groups we have $E_a(\mathbb{Z}/J_k\mathbb{Z}) = E_a(\mathbb{Z}[\alpha]/(j_k)) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k+1}\mathbb{Z}$.

7. A general framework

In [5] we give a general framework that extends the above results to arbitrary CM elliptic curves. We state the main result in Theorem 11 below. We follow that with a justification for why CM by $\mathbb{Q}(\sqrt{-7})$ and $\mathbb{Q}(\sqrt{-15})$ are the only cases of elliptic curves with CM by fields of class number one or two that do not succumb to $p \pm 1$ tests and to which the methods of Gross and Denomme-Savin extend "nicely".

If M is a number field, let $\mathcal{O}_M$ denote its ring of integers.

7.1. General result.

Definition 9. Suppose E is an elliptic curve over a number field M and J is an ideal of $\mathcal{O}_M$ that is prime to $\mathrm{disc}(E)$. We say that $P \in E(M)$ is *strongly nonzero* mod J if one can express $P = (x : y : z) \in E(\mathcal{O}_M)$ in such a way that the ideals (z) and J are relatively prime. We say that P is *nonzero* mod J, and write $P \not\equiv O_E$ mod J, if one can express $P = (x : y : z) \in E(\mathcal{O}_M)$ in such a way that $z \notin J$; otherwise we say P is zero mod J and write $P \equiv O_E$ mod J.

Remark 10. (a) A point P is strongly nonzero mod J if and only if P is nonzero mod λ for every prime ideal $\lambda \mid J$ in $\mathcal{O}_M$.

(b) In particular, if J is prime, then P is strongly nonzero mod J if and only if $P \not\equiv O_E$ mod J.

Suppose:

(i) K is an imaginary quadratic field with Hilbert class field H,
(ii) $\alpha_1, \ldots, \alpha_s, \gamma \in \mathcal{O}_K - \{0\}$; $k = (k_1, \ldots k_s) \in \mathbb{N}^s$,
(iii) $\pi_k := 1 + \gamma\alpha_1^{k_1} \cdots \alpha_s^{k_s} \in \mathcal{O}_K$,
(iv) $\mathfrak{p}_k$ is an ideal of $\mathcal{O}_H$ such that $\mathrm{N}_{H/K}(\mathfrak{p}_k) = (\pi_k)$,
(v) $F_k := \mathrm{N}_{H/\mathbb{Q}}(\mathfrak{p}_k) = \mathrm{N}_{K/\mathbb{Q}}(\pi_k)$,
(vi) E is an elliptic curve over H with CM by $\mathcal{O}_K$ and discriminant prime to F_k.
(vii) $F_k > 16\,\mathrm{N}_{K/\mathbb{Q}}(\gamma^2)$,
(viii) $L_k \in \mathbb{Z}^+$ is defined by $L_k\mathbb{Z} = (\frac{\pi_k - 1}{\gamma}) \cap \mathbb{Z}$.

Note that if F_k is prime, then $\mathfrak{p}_k$ is a prime ideal of $\mathcal{O}_H$. If $\mathfrak{p}_k$ is a prime ideal, then F_k is a prime power p^r with $r \mid [H : \mathbb{Q}] = 2h$. Since testing primality of a number that is known to be a prime power is not difficult, the next result can be viewed as essentially a primality test for F_k.

Theorem 11. *Retain the notation and assumptions above. Suppose that whenever the ideal $\mathfrak{p}_k$ is prime, then:*

(a) the Frobenius endomorphism of E over the field $\mathcal{O}_H/\mathfrak{p}_k$ is π_k, and
(b) for every prime ideal λ of $\mathcal{O}_K$ that divides $(\alpha_1 \cdots \alpha_s)$ we have P mod $\mathfrak{p}_k \notin \lambda E(\mathcal{O}_H/\mathfrak{p}_k)$.

Then the following are equivalent:

(i) *$\mathfrak{p}_k$ is prime.*

(ii) $(\pi_k - 1)P \equiv O_E \mod \mathfrak{p}_k$, *and for every prime ideal* λ *of* $\mathcal{O}_K$ *that divides* $(\alpha_1 \cdots \alpha_s)$ *there is a point in* $\frac{(\pi_k-1)}{\lambda}P$ *that is strongly nonzero mod* $\mathfrak{p}_k$.

Suppose further that $\alpha_1 \cdots \alpha_s$ *is not divisible by any rational prime that splits in* K, *and that* $F_k > 16\,\mathrm{N}_{K/\mathbb{Q}}(\gamma \prod_\lambda \lambda)^2$ *where* λ *runs over the prime ideals of* $\mathcal{O}_K$ *that divide* $(\alpha_1 \cdots \alpha_s)$ *and are ramified in* $K/\mathbb{Q}$. *Then the following are equivalent:*

(i) $\mathfrak{p}_k$ *is prime.*

(ii) $L_k \gamma P \equiv O_E \mod \mathfrak{p}_k$, *and* $\frac{L_k}{p}\gamma P$ *is strongly nonzero mod* $\mathfrak{p}_k$ *for every prime* $p \mid \mathrm{N}_{K/\mathbb{Q}}(\alpha_1 \cdots \alpha_s)$.

Well known results say that if $E/\mathbb{Q}$ is an elliptic curve, $P \in E(\mathbb{Q})$, and $P \bmod N$ has sufficiently large order (in terms of N), then N is prime. This can easily be generalized to the above setting, to give one direction of the proof. For the converse direction, if $\mathfrak{p}_k$ is prime and the Frobenius endomorphism of $E \bmod \mathfrak{p}_k$ is π_k, then

$$E(\mathcal{O}_H/\mathfrak{p}_k) \cong \mathcal{O}_K/(\pi_k - 1) = \mathcal{O}_K/(\gamma\alpha_1^{k_1} \cdots \alpha_s^{k_s})$$

so $(\pi_k - 1)P \equiv O_E \bmod \mathfrak{p}_k$ as desired. If $P \bmod \mathfrak{p}_k \notin \lambda E(\mathcal{O}_H/\mathfrak{p}_k)$, then $\frac{(\pi_k-1)}{\lambda}P \not\equiv O_E \mod \mathfrak{p}_k$ as desired. The dependence on γ is hidden in the assumption that F_k is sufficiently large compared to γ. Full details are given in [5].

In our algorithms in [4, 30, 5, 1], the work is in finding a large nice set S such that whenever $k \in S$ and $\mathfrak{p}_k$ is prime, then:

(a) the Frobenius endomorphism of $E \bmod \mathfrak{p}_k$ is π_k, and

(b) $P \bmod \mathfrak{p}_k \notin \lambda E(\mathcal{O}_H/\mathfrak{p}_k)$ for all prime ideals $\lambda \mid \frac{\pi_k - 1}{\gamma}$ (i.e., for all $\lambda \mid \prod \alpha_i$).

Finding the k's that satisfy (a) is doable. More problematic is (b).

7.2. CONSTRAINTS ON K. For any given k, one could check whether $P \bmod \mathfrak{p}_k \notin \lambda E(\mathcal{O}_H/\mathfrak{p}_k)$ for all prime ideals λ dividing $\prod \alpha_i$. But the goal is to determine in advance the "good" k. This is what allows us to obtain efficient deterministic primality tests. However, finding a nice description of the k for which $P \bmod \mathfrak{p}_k \notin \lambda E(\mathcal{O}_H/\mathfrak{p}_k)$ is constrained by the following. Suppose:

- $\hat{f} : E \to E' := E/E[\bar{\lambda}]$ is the natural isogeny,
- $f : E' \to E$ is the dual isogeny,
- $F := H(E[\lambda])$,
- $L := F(f^{-1}(P))$.

We prove the next result in [5].

Theorem 12. *The following are equivalent:*

(i) $P \mod \mathfrak{p}_k \notin \lambda E(\mathcal{O}_H/\mathfrak{p}_k)$.

(ii) $\mathfrak{p}_k$ *splits completely in* F *and* $\mathfrak{p}_k$ *does not split completely in* L.

When the extension L/H is abelian, 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 $\mathfrak{p}_k$ splits completely in F but not L. In [5] we show that if L/H is abelian and $L \neq F$ then $F = H$, and we prove:

Proposition 13. *If* $F = H$, E *is defined over* $\mathbb{Q}(j(E))$, *and* p *is the rational prime below* λ, *then either:*

(i) $p = 2$, *and* 2 *splits in* K, *or*

(ii) $p = 2$ *or* 3, *and* p *ramifies in* K, *or*

(iii) $K = \mathbb{Q}(\sqrt{-3})$ *and* $\lambda = (2)$.

In the latter two cases, $\lambda = \bar{\lambda}$ so classical $p \pm 1$ primality tests apply.

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

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

If we are only interested in cases where $\lambda \neq \bar{\lambda}$ in order to obtain sequences to which $p \pm 1$ tests do not apply, and we take (for simplicity) E defined over $\mathbb{Q}(j(E))$, that restricts us to

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

if K has class number one (which is the case we handle in [4] and in §6 above), and

$$K = \mathbb{Q}(\sqrt{-15}) \quad \text{with} \quad \alpha_i = (1 \pm \sqrt{-15})/2$$

if K has class number two (which is the case we handle in [5] and in §8 below).

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

Theorem 14 (Abatzoglou-Silverberg-Sutherland-Wong, 2012 [5])**.** *Let*

$$\alpha = \tfrac{1+\sqrt{-15}}{2},$$

let E be the elliptic curve $y^2 = x^3 + a_4 x + a_6$ where

$$\begin{aligned} a_4 &= -3234(16195646845 - 7242913457\sqrt{5}), \\ a_6 &= 14^4(5395199151946361 - 2412806411180256\sqrt{5}) \end{aligned}$$

(with CM by $\mathbb{Z}[\alpha]$), and let

$$P = (0, -14^2(51938421 - 23227568\sqrt{5})) \in E(\mathbb{Q}(\sqrt{5})).$$

Let $f_k = 1 - 4\alpha^k$ and $F_k = f_k \bar{f}_k = 1 - 4(\alpha^k + \bar{\alpha}^k) + 4^{k+2} \in \mathbb{N}$. Let $\beta = \frac{\sqrt{5}+\sqrt{-3}}{2}$ and $p_k = 1 + 2\beta^k$. Let

$$\begin{aligned} S := \{k \in \mathbb{N} : k \equiv\ & 9, 19, 27, 31, 39, 45, 59, 63, 67, 81, 85, 105, 123, 129, \\ & 133, 141, 159, 169, 173, 181, 183, 201, 211, 221, 223, 225, 229, 237 \pmod{240}\}. \end{aligned}$$

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

(i) *F_k is prime.*
(ii) *$2^{2k+1}P \equiv (7(377709\sqrt{5} - 844583), 0)$ mod p_k.*
(iii) *$2^{2k+2}P \equiv O_E \mod p_k$ and $2^{2k+1}P$ is strongly nonzero mod (p_k).*
(iv) *$4\alpha^k P \equiv O_E$ mod p_k and $8\alpha^{k-1}P$ is strongly nonzero mod (p_k).*

This follows from Theorem 11. Let $H = \mathbb{Q}(\sqrt{-3}, \sqrt{5})$, the Hilbert class field of K. If k is odd then $f_k = \mathrm{N}_{H/K}(p_k)$ and $F_k = \mathrm{N}_{H/\mathbb{Q}}(p_k)$. Let $\lambda = (2, \alpha)$, the ideal of $\mathbb{Z}[\alpha]$ generated by 2 and α. Then $(2) = \lambda\bar{\lambda}$. We can show that if $k \in S$ and p_k is prime, then as $\mathbb{Z}[\alpha]$-modules we have

$$\begin{aligned} E(\mathcal{O}_H/(p_k)) &\cong \mathbb{Z}[\alpha]/(4\alpha^k) \\ &\cong \mathbb{Z}[\alpha]/(\bar{\lambda}^2) \times \mathbb{Z}[\alpha]/(\lambda^{2k+2}) \end{aligned}$$

and $P \bmod p_k \notin \lambda E(\mathcal{O}_H/(p_k))$. (When F_k is prime, we have $E(\mathcal{O}_H/(p_k)) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4^{k+1}\mathbb{Z}$ as groups.)

Remarks 15. (a) F_k is divisible by 3 if and only if k is even.
(b) F_k is divisible by 5 if and only if $k \equiv 2 \pmod 4$.
(c) F_k is divisible by 7 if and only if $k \equiv 16 \pmod{24}$.
(d) F_k is divisible by 11 if and only if $k \equiv 48 \pmod{60}$.
(e) F_k is divisible by 31 if and only if $k \equiv 6$ or $12 \pmod{15}$.
(f) F_k is divisible by 61 if and only if $k \equiv 1 \pmod{30}$.

9. Large primes

We implemented Theorem 8 for all $k \leq 1.2$ million. In that range there are exactly 79 prime J_k's. The largest, $J_{1,111,930}$, has 334,725 decimal digits [2].

We implemented Theorem 14 for all $k \leq$ one million. In that range there are exactly 9 prime F_k's. The largest, $F_{696,123}$, has 419,110 decimal digits [3], and is the largest proven prime p for which there is no known significant partial factorization of $p-1$ or $p+1$.

Acknowledgements

I thank Alexander Abatzoglou, Andrew Sutherland, and Angela Wong, with whom the work in [4, 5] was jointly undertaken, and I thank them, Robert Denomme, and the referees for helpful comments. I thank the organizers of GeoCrypt 2013 for giving me the opportunity to present the results.

References

[1] A. Abatzoglou, A CM elliptic curve framework for deterministic primality proving on numbers of special form, Ph.D thesis, University of California at Irvine, 2014.
[2] A. Abatzoglou, A. Silverberg, A. V. Sutherland and A. Wong, available online at http://primes.utm.edu/primes/page.php?id=106847
[3] A. Abatzoglou, A. Silverberg, A. V. Sutherland and A. Wong, available online at http://primes.utm.edu/primes/page.php?id=117544
[4] A. Abatzoglou, A. Silverberg, A. V. Sutherland and A. Wong, Deterministic elliptic curve primality proving for a special sequence of numbers, in *Algorithmic Number Theory*, Math. Sci. Publ., 2013, 1–20.
[5] A. Abatzoglou, A. Silverberg, A. V. Sutherland and A. Wong, A framework for deterministic primality proving using elliptic curves with complex multiplication, *Math. Comp.*, to appear.
[6] M. Agrawal, N. Kayal and N. Saxena, Primes is in P, *Ann. Math.*, **160** (2004), 781–793.
[7] A. O. L. Atkin and F. Morain, Elliptic curves and primality proving, *Math. Comp.*, **61** (1993), 29–68.
[8] W. Bosma, *Primality Testing with Elliptic Curves*, Doctoraalscriptie Report, University of Amsterdam 85–12, 1985, available online at http://www.math.ru.nl/~bosma/pubs/PRITwEC1985.pdf
[9] D. V. Chudnovsky and G. V. Chudnovsky, Sequences of numbers generated by addition in formal groups and new primality and factorization tests, *Adv. Appl. Math.*, **7** (1986), 385–434.
[10] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, Second edition, Springer, New York, 2005.
[11] R. Denomme and G. Savin, Elliptic curve primality tests for Fermat and related primes, *J. Number Theory*, **128** (2008), 2398–2412.
[12] S. Goldwasser and J. Kilian, Almost all primes can be quickly certified, in *STOC '86 — Proc. 18th Annual ACM Symp. Theory Computing*, 1986, 316–329.
[13] S. Goldwasser and J. Kilian, Primality testing using elliptic curves, *J. ACM*, **46** (1999), 450–472.
[14] D. M. Gordon, Pseudoprimes on elliptic curves, in *Théorie des nombres*, de Gruyter, Berlin, 1989, 290–305.

[15] B. H. Gross, *Arithmetic on Elliptic Curves with Complex Multiplication*, Springer, Berlin, 1980.
[16] B. H. Gross, Minimal models for elliptic curves with complex multiplication, *Compositio Math.*, **45** (1982), 155–164.
[17] B. H. Gross, An elliptic curve test for Mersenne primes, *J. Number Theory*, **110** (2005), 114–119.
[18] A. Gurevich and B. Kunyavskiĭ, Primality testing through algebraic groups, *Arch. Math. (Basel)*, **93** (2009), 555–564.
[19] A. Gurevich and B. Kunyavskiĭ, Deterministic primality tests based on tori and elliptic curves, *Finite Fields Appl.*, **18** (2012), 222–236.
[20] M. Kida, Primality tests using algebraic groups, *Exper. Math.*, **13** (2004), 421–427.
[21] H. W. Lenstra, Jr., Elliptic curves and number-theoretic algorithms, in *Proc. Int. Congr. Math.*, Amer. Math. Soc., Providence, 1987, 99–120.
[22] H. W. Lenstra, Jr., Factoring integers with elliptic curves, *Ann. Math.*, **126** (1987), 649–673.
[23] H. W. Lenstra, Jr. and C. Pomerance, Primality testing with Gaussian periods, available online at `http://www.math.dartmouth.edu/~carlp/aks041411.pdf`, 2011.
[24] C. Pomerance, Primality testing: variations on a theme of Lucas, *Congr. Numer.*, **201** (2010), 301–312.
[25] K. Rubin and A. Silverberg, Point counting on reductions of CM elliptic curves, *J. Number Theory*, **129** (2009), 2903–2923.
[26] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.*, **44** (1985), 483–494.
[27] A. Silverberg, Group order formulas for reductions of CM elliptic curves, in *Proc. Conf. Arith. Geom. Crypt. Coding Theory*, Amer. Math. Soc., Providence, 2010, 107–120.
[28] H. Stark, Counting points on CM elliptic curves, *Rocky Mountain J. Math.*, **26** (1996), 1115–1138.
[29] Y. Tsumura, Primality tests for $2^p + 2^{\frac{p+1}{2}} + 1$ using elliptic curves, *Proc. Amer. Math. Soc.*, **139** (2011), 2697–2703.
[30] A. Wong, *Primality Test Using Elliptic Curves with Complex Multiplication by* $\mathbb{Q}(\sqrt{-7})$, Ph.D thesis, University of California at Irvine, 2013.

Received for publication January 2014.

E-mail address: asilverb@uci.edu