MATHEMATICS OF COMPUTATION
Volume 79, Number 270, April 2010, Pages 1171–1190
S 0025-5718(09)02275-3
Article electronically published on October 16, 2009

ON THE EXISTENCE AND NON-EXISTENCE OF ELLIPTIC PSEUDOPRIMES

SIGUNA MÜLLER

ABSTRACT. In a series of papers, D. Gordon and C. Pomerance demonstrated that pseudoprimes on elliptic curves behave in many ways very similar to pseudoprimes related to Lucas sequences. In this paper we give an answer to a challenge that was posted by D. Gordon in 1989. The challenge was to either prove that a certain composite $N \equiv 1 \bmod 4$ did not exist, or to explicitly calculate such a number. In this paper, we both present such a specific composite (for Gordon's curve with CM by $\mathbb{Q}(\sqrt{-7})$), as well as a proof of the non-existence (for curves with CM by $\mathbb{Q}(\sqrt{-3})$). We derive some criteria for the group structure of CM curves that allow testing for all composites, including $N \equiv 3 \bmod 4$ which had been excluded by Gordon. This gives rise to another type of examples of composites where strong elliptic pseudoprimes are not Euler elliptic pseudoprimes.

1. MOTIVATION

1.1. **The challenge.** For a field k of characteristic > 3, an elliptic curve over k may be represented as

$$E(k) = \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \mathcal{O}, \tag{1}$$

where $a, b, \in k$ and $\mathcal{O}$ is the point at infinity. E is nonsingular if the discriminant is nonzero. In this case, $E(k)$ can be naturally made into an additive group with $\mathcal{O}$ being the identity element.

In [4], [5], Gordon defined a necessary but not sufficient test for primality using elliptic curves. Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication (CM) by an order in $K = \mathbb{Q}(\sqrt{-d})$ for $d \in \mathbb{Z}^+$, and suppose E has a rational point $\mathcal{P}$ on E of infinite order. Then, if N is a prime which is inert in K and does not divide the discriminant of E,

$$(N + 1)\mathcal{P} \equiv \mathcal{O} \bmod N. \tag{2}$$

That is, when we view E as an elliptic curve over the finite field $\mathbb{Z}/N\mathbb{Z}$, the image of the point $\mathcal{P}$ has order dividing $N+1$. A composite number N is called an *elliptic pseudoprime* if $\left(\frac{-d}{N}\right) = -1$, N is coprime to the discriminant of E and N satisfies (2). (The concept of the evaluation modulo N for composite N will be made precise in sect. 3.2.)

Received by the editor August 28, 2008 and, in revised form, December 4, 2008 and March 4, 2009.

2000 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11Y40, 11A51.

These pseudoprimes are analogous to Fermat pseudoprimes, which are composites N for which

$$a^{N-1} \equiv 1 \bmod N$$

for a given a. They are also analogous to pseudoprimes for the Lucas-Lehmer test: let D, P, Q be integers such that $D = P^2 - 4Q \neq 0$ and $P > 0$. Then a composite integer N is a Lucas pseudoprime if

$$U_{N-\left(\frac{D}{N}\right)} \equiv 0 \bmod N,$$

where $U = U_k$ is the Lucas U-sequence.

A more profitable view of Lucas pseudoprimes was developed by Grantham in [7] using the field $\mathbb{F}_{p^2}$ (see also [11], [2]), and for the more general case in [8]. He puts the Frobenius automorphism into the center stage of his test. If P and Q are as above, then a composite number N is a Frobenius pseudoprime with respect to $f(x) = x^2 - Px + Q$ if

$$x^N \equiv \begin{cases} P - x \bmod (f(x), N), & \text{if } \left(\frac{D}{N}\right) = -1, \\ x \bmod (f(x), N), & \text{if } \left(\frac{D}{N}\right) = 1. \end{cases}$$

This also shows that elliptic pseudoprimes are analogous to Grantham's (quadratic) Frobenius test.

The Lucas-Lehmer test is a degenerate of the elliptic test, and the Fermat test is a special case of the Lucas test. For this reason, it seems plausible that elliptic pseudoprimes share properties very similar to Fermat and Lucas pseudoprimes. In a series of papers [4, 5, 6], Gordon and Pomerance describe similarities regarding distribution estimates.

This paper deals with an interesting question stated by Gordon in 1989, [4, p. 244]. It is a fundamental and well-known fact that the Fermat test can be strengthened by the 'strong version', resp. the Miller-Rabin test. Similarly, a strong version' of the Lucas test can be formulated.

Gordon defines Euler elliptic pseudoprimes analogously to the regular case. N is an *Euler elliptic pseudoprime* if

$$\begin{cases} \left(\frac{N+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod N, & \text{if } \mathcal{P} = 2\mathcal{Q} \text{ for some } \mathcal{Q} \text{ on } E(\mathbb{Z}_N), \\ \left(\frac{N+1}{2}\right)\mathcal{P} \equiv \text{ a 2-torsion point mod } N, & \text{otherwise.} \end{cases} \tag{3}$$

Gordon also required that $N \equiv 1 \bmod 4$, but we will show below that this is not necessary (but see Remark 4).

If p is a prime, for elliptic curves given by (1) the 2-torsion points in $E(\mathbb{F}_p)$ (points $\mathcal{P}$ such that $2\mathcal{P} = \mathcal{O}$) are of the form $(X, 0)$, where X is a root of $X^3 + AX + B \equiv 0 \bmod p$.

Analogously, *strong elliptic pseudoprimes* are defined as follows [4, 5]:

Definition 1. If N is an elliptic pseudoprime and $N + 1 = 2^s \cdot t$, where t is odd, call N a strong elliptic pseudoprime if

$$(t)\mathcal{P} \equiv \mathcal{O} \bmod N, \quad \text{or}$$
$$(t \cdot 2^r)\mathcal{P} \equiv \text{ a 2-torsion point, for some } r \text{ with } 0 \leq r < s.$$

For Fermat and Lucas pseudoprimes, all strong pseudoprimes fulfill the corresponding Euler criteria, i.e., are Euler pseudoprimes.

TABLE 1. Gordon's Curves with Points

Gordon's CM curves in $\mathbb{F}_p$ for $\left(\frac{-d}{p}\right) = -1$			
	curve	$\mathcal{P}$	$K = \mathbb{Q}(\sqrt{-d})$
(i)	$y^2 = x^3 - 5x$	$(5, 10)$	$\mathbb{Q}(\sqrt{-1})$
(ii)	$y^2 = x^3 - 120x - 448$	$(64, 504)$	$\mathbb{Q}(\sqrt{-2})$
(iii)	$y^2 = x^3 + 3$	$(1, 2)$	$\mathbb{Q}(\sqrt{-3})$
(iv)	$y^2 = x^3 - 3500x - 98000$	$(84, 884)$	$\mathbb{Q}(\sqrt{-7})$
(v)	$y^2 = x^3 - 1056x + 13552$	$(33, 121)$	$\mathbb{Q}(\sqrt{-11})$
(vi)	$y^2 = x^3 - 2432x - 46208$	$(57, 19)$	$\mathbb{Q}(\sqrt{-19})$
(vii)	$y^2 = x^3 - 495360x - 134193024$	$(817, 2537)$	$\mathbb{Q}(\sqrt{-43})$
(viii)	$y^2 = x^3 - 117920x + 15585808$	$(201, 67)$	$\mathbb{Q}(\sqrt{-67})$
(ix)	$y^2 = x^3 = -34790720x + 78984748304$	$(3400, 548)$	$\mathbb{Q}(\sqrt{-163})$

Gordon first asked the surprising question whether this would be true for elliptic pseudoprimes. He poses the challenge, 'The proof does not carry over to elliptic pseudoprimes, and it would be interesting to find a strong elliptic pseudoprime $N \equiv 1 \bmod 4$ which does not pass (3), or prove that none exist.'

1.2. **Our result.** The main result of this paper is an answer to Gordon's challenge. Before stating the result, we need to address a few issues.

Gordon's original definition for pseudoprimes on elliptic curves [4, p. 233] incorporated an explicit addition chain for $N + 1$ (resp. $(N + 1)/2^i$). However, he also notes that, 'the dependence on the addition chain may be eliminated by using a parametrization for which the addition law has no divisions.'

Later [6], the definition was given in terms of the division polynomials. However, our approach will be based on calculations using the addition law, for reasons that will be made clear in sect. 3.2.

As for Fermat pseudoprimes, it is always easier to find a pseudoprime N for *some* point on a given curve. It is much harder to find N where both the curve *and* the point are specified; see sect. 3.2.

Gordon gives an explicit list of suitable curves, *along with an integral point*, for each field of CM with class number 1; see Table 1. For the most part of the paper we concentrate on finding N for this (more challenging setting) where both the curve and the point are specified.

Our main contributions are as follows:

- We show that for Gordon's curve (iv), $E : y^2 = x^3 - 3500x - 98000$ along with its (given) integral point $(84, 884)$, there *is* a composite number that is a *counterexample* to the classical result. Specifically, let

$$\begin{aligned} N &= 676258600736819377469073681570025709 \\ &= 47737 \cdot 275183 \cdot 1212119 \cdot 2489759 \cdot 3178891 \cdot 5366089. \end{aligned}$$

Then $N \equiv 1 \bmod 4$, $\left(\frac{-7}{N}\right) = -1$ and

$$\begin{gathered} (N+1)\,\mathcal{P} \equiv \mathcal{O} \bmod N, \\ \left(\tfrac{N+1}{2}\right)\mathcal{P} \equiv (654609963152984637027391710649598749, 0) \bmod N, \\ 2(654609963152984637027391710649598749, 0) \equiv \mathcal{O} \bmod N. \end{gathered}$$

Therefore, N is a strong elliptic pseudoprime. However, there exists a point

$$\mathcal{Q} = (427631894156657698513741722706642740,$$
$$3492235364925418467988168910950721 58)$$

on $E(\mathbb{Z}/N\mathbb{Z})$ with

$$2\mathcal{Q} \equiv \mathcal{P} \bmod N.$$

Hence, $\mathcal{P}$ 'does not look like a double, but is', contradicting the Euler condition. Here, the computations are done utilizing the modified projective algorithm [3, p. 293] via a left-to-right scan.

- The *opposite* is also true. For the curve (iii) we give an explicit proof that for $E : y^2 = x^3 + B$ and *any* integral point on E, every strong elliptic pseudoprime $N \equiv 1 \bmod 4$ is also an Euler elliptic pseudoprime. We conjecture that the same is true for *all* the other applicable curves (v)-(ix) (those which allow $N \equiv 1 \bmod 4$).
- By drawing from results in [13] for supersingular curves, Gordon observed that $E(\mathbb{F}_p)$ might not be cyclic when p is a prime $\equiv 3 \bmod 4$. This led him to require $N \equiv 1 \bmod 4$. However, we demonstrate that any CM curve by an order in $\mathbb{Q}(\sqrt{-d})$ for $d > 2$ is always cyclic. Hence, the above can be generalized to integers $N \equiv 3 \bmod 4$. In that case, $2^s | N + 1$ for $s > 1$ and one conceivably obtains stronger tests for larger s. We show that even for $s > 1$, counterexamples analogous to the above exist. Moreover, the case $s > 1$ gives rise to yet another type of counterexamples. We exhibit examples of composites N with points that 'look like a double, but aren't'. While the underlying criteria are fairly restrictive we were able to compute counter-examples for *each* type of curve in Gordon's table.

2. Some ideas and observations

2.1. **Recognizing doubles.** Unless stated otherwise, primes will be denoted by p, P, or Q, etc., and composite numbers by N.

As in the traditional setting, we require some (hopefully simple) mechanism to check whether $\mathcal{P}$ is twice another point. For a proof of the following well-known result, see e.g. [9].

Lemma 1. *Let E be an elliptic curve over a field k of characteristic not equal to 2 or 3. Suppose E is given by*

$$y^2 = (x - \alpha)(x - \beta)(x - \gamma) = x^3 + rx^2 + sx + t$$

with α, β, γ in k. For (x_2, y_2) in $E(k)$, there exists (x_1, y_1) in $E(k)$ with $2(x_1, y_1) = (x_2, y_2)$ iff $x_2 - \alpha, x_2 - \beta$ and $x_2 - \gamma$ are squares in k.

When k is a finite field, $E(\overline{k})$ is a torsion group; that is, every point on the curve has finite order. For a non-negative integer n, the set of n-torsion points is

$$E[n] = \{\mathcal{P} \in E(\overline{k}) \,|\, n\mathcal{P} = \mathcal{O}\}. \tag{4}$$

We stress that here the points can have coordinates in the algebraic closure $\overline{k}$, not just k. If $\mathrm{char}(k) \neq 2$, E can be put into the form $y^2 = (x - \alpha)(x - \beta)(x - \gamma)$ with $\alpha, \beta, \gamma \in \overline{k}$. One can easily show [14] that

$$E[2] = \{\mathcal{O}, (\alpha, 0), (\beta, 0), (\gamma, 0)\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2. \tag{5}$$

Hence, the condition of the lemma requires that all 2-torsion points are in k (and not only in $\overline{k}$). This means that $E(k)$ has a subgroup isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. Hence, this approach cannot be used for the challenge curves defined over $k = E(\mathbb{F}_p)$ as they are all cyclic when p is prime. In this situation the problem of recognizing whether a point is a double of something seems to be much more difficult.

The classical analog is furnished by the Jacobi symbol, which however has the well-known practical but unpleasant property: if $\left(\frac{a}{N}\right) = 1$ for some composite N, then a is not necessarily a square modulo N. Being a square would require being such modulo each factor of N. However, we have the following special case, which we shall prove in section 2.4 below.

Lemma 2. *Let $N \equiv 3 \bmod 4$ be a composite integer. If N is an Euler pseudoprime for the base a, i.e., if $a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \bmod N$, then this implies that*

$$\begin{cases} a^{(N-1)/2} \equiv 1 \bmod N, & \textit{iff } a \textit{ is a square modulo } N, \\ a^{(N-1)/2} \equiv -1 \bmod N, & \textit{iff } a \textit{ is not a square modulo } N. \end{cases}$$

For $N \equiv 1 \bmod 4$ (as required) the analogous condition for CM curves reads

$$\begin{cases} \left(\frac{N+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod N, & \text{iff } \mathcal{P} \text{ is a double in } E(\mathbb{Z}_N), \\ \left(\frac{N+1}{2}\right)\mathcal{P} \equiv \text{ a 2-torsion point mod } N, & \text{iff } \mathcal{P} \text{ is not a double in } E(\mathbb{Z}_N). \end{cases} \tag{6}$$

Note that this condition bypasses any Jacobi-like symbols. Also note that since $(N+1)/2$ is odd, (6) in fact constitutes the strong Euler test. Hence, for constructing Gordon's challenge number, the condition is to exhibit a composite that violates (6).

We note that (6) is indeed fulfilled when $N = p$ is a prime. This is Corollary 1 below. The next section shows that we can partially recover a Jacobi-like symbol.

2.2. **Restoring the symbol.** We rely on the well-known fact that $E(\mathbb{F}_p)$ is either cyclic or isomorphic to a sum of two cyclic groups; see e.g. [3].

Lemma 3. *Let E be an elliptic curve over $\mathbb{F}_p$. Then*

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_n \quad \textit{or} \quad \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$$

for some integer $n \geq 1$, or for some integers $n_1, n_2 \geq 1$ with n_1 dividing n_2.

We recall that the *exponent* of a finite abelian group is the largest possible order of an element. In view of the above, the exponent $\exp(E(\mathbb{F}_p))$ of $E(\mathbb{F}_p)$ is n or n_1, according to the above.

We define an analog of the Jacobi symbol for the case that $2 | \exp(E(\mathbb{F}_p))$.

Definition 2. Let E be an elliptic curve over $\mathbb{F}_p$ such that

$$E(\mathbb{F}_p) \simeq \mathbb{Z}_{d_2} \oplus \mathbb{Z}_{d_1},$$

where $d_1 | d_2$ and we include the case $d_1 = 1$. Suppose that $d_2 = 2k$. Let

$$\left[\frac{\mathcal{P}}{p}\right] \equiv k\mathcal{P} \bmod p.$$

Observe that the exponent $\exp(E(\mathbb{F}_p))$ of $E(\mathbb{F}_p)$ is $d_2 = 2k$. The definition allows either cyclic groups (with $d_2 = p+1$ and $d_1 = 1$), or a product of two cyclic groups. In the following, E has no points of order (a multiple of) 4 in $\mathbb{F}_p$.

Lemma 4. *Suppose* $2 \not| k$. *Then*

$$\begin{cases} \left[\frac{\mathcal{P}}{p}\right] \equiv \mathcal{O} \bmod p, & \text{iff } \mathcal{P} \text{ is a double modulo } p, \\ \left[\frac{\mathcal{P}}{p}\right] \equiv \text{ a 2-torsion point} \bmod p, & \text{iff } \mathcal{P} \text{ is not a double modulo } p. \end{cases} \tag{7}$$

Proof. By the structure property, Lemma 3, for p a prime, the values of $\left[\frac{\mathcal{P}}{p}\right]$ can only be either $\mathcal{O}$, or one of the 2-torsion points.

Consider the first assertion in (7). We need to show that points $\mathcal{P}$ that are doubles (of some points in $E(F_p)$) are exactly those with $\left[\frac{\mathcal{P}}{p}\right] \equiv \mathcal{O} \bmod p$. Necessity is clear. Recall that each of $\mathbb{Z}_{d_2} = \mathbb{Z}_{2k}$ and $\mathbb{Z}_{d_1}$ are cyclic. This means that the doubles are the evens in $\mathbb{Z}_{d_2}$. If $2 \not| d_1$, every element is a double in $\mathbb{Z}_{d_1}$. Otherwise, we again have that the doubles are the evens. So, if $\left[\frac{\mathcal{P}}{p}\right] \equiv k\mathcal{P} \equiv \mathcal{O} \bmod p$, then since k is odd, the previous paragraph implies that $\mathcal{P}$ is a double in $E(\mathbb{F}_p)$.

For the second assertion, again necessity is easy. If $\left[\frac{\mathcal{P}}{p}\right] \equiv$ a 2-torsion point modulo p but $\mathcal{P} = 2\mathcal{Q}$, then $k\mathcal{P} \equiv (2k)\mathcal{Q} \equiv \mathcal{O} \bmod p$, a contradiction. Finally, the converse follows from what has already been proved. □

Since for CM curves, $2k = \exp(E(\mathbb{F}_p)) = p + 1$, and k is odd for $p \equiv 1 \bmod 4$, we have

Corollary 1. *Eq.* (6) *is true if* $N \equiv 1 \bmod 4$ *is prime.*

2.3. **Euler vs. doubles.** Schoof [13] showed that for primes p, if $|E(\mathbb{F}_p)| = p + 1$, then either $E(\mathbb{F}_p) \simeq \mathbb{Z}/(p+1)\mathbb{Z}$ or $E(\mathbb{F}_p) \simeq \mathbb{Z}/((p+1)/2)\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. In the latter case, which can only happen if $p \equiv 3 \bmod 4$, any point will satisfy $\left(\frac{p+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod p$, since $\exp(E(\mathbb{F}_p)) = (p+1)/2$ in this case. So Gordon's restriction for the challenge number to be $N \equiv 1 \bmod 4$ is to ensure that the curve is cyclic if N is a prime (but see section 4.2).

Cyclic groups are convenient to work with since doubles are easily recognizable via Euler's criterion. The situation is more complicated for the second case of Lemma 3. As an example, consider the group $G \simeq \mathbb{Z}_{2k} \oplus \mathbb{Z}_2$. Then, if $2|k$, we have $k(x, 1) = (0, 0)$, but $(x, 1)$ is not a double.

At first glance, this property seems promising. Unfortunately the first part of the challenge problem (6) cannot be attacked using this approach.

Lemma 5. *Suppose* $N \equiv 1 \bmod 4$ *is a strong elliptic pseudoprime for the point* $\mathcal{P}$. *Then* $\left(\frac{N+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod N$ *iff* $\mathcal{P}$ *is a double of a point* $\bmod N$.

Proof. This follows since $(N + 1)/2$ is odd. □

2.4. $3 \cdot 1 = 3 \bmod 4$, **but** $3 \cdot 3 = 1 \bmod 4$**.** As described above, in the general case, $\left(\frac{a}{N}\right) = 1$ does not necessarily imply that a is a square modulo N. However, for $N \equiv 3 \bmod 4$, the Euler, resp. strong, test, implies that the symbol conveys the 'correct' information, as stated in Lemma 2. It turns out that congruence conditions modulo 4 play a crucial role.

Proof of Lemma 2. Suppose $a^{(N-1)/2} \equiv \left(\frac{a}{N}\right) \bmod N$. By assumption, $(N - 1)/2$ is odd. So, if $a^{(N-1)/2} \equiv 1 \bmod N$, then also $\left(\frac{a}{P}\right) \equiv a^{(P-1)/2} \equiv 1 \bmod P$ for any prime $P|N$. Hence, a is a square modulo N.

Suppose $a^{(N-1)/2} \equiv -1 \bmod N$. Observe that this implies $\nu_2(P-1) \geq \nu_2(N-1)$ for all $P|N$. Here $\nu_2(k)$ denotes the largest factor of 2 dividing k. We claim that

$$\left(\frac{a}{P}\right) \equiv a^{(P-1)/2} \equiv \begin{cases} -1, & \text{if } \nu_2(P-1) = \nu_2(N-1) = 1, \\ 1, & \text{if } \nu_2(P-1) > \nu_2(N-1) = 1. \end{cases} \tag{8}$$

This can be seen as follows. Let $N - 1 = 2^s t$ with $2 \nmid t$. By hypothesis, $\mathrm{ord}_P(a)$ divides $2^1 t$, but $\mathrm{ord}_P(a)$ does not divide t. So, $\nu_2(\mathrm{ord}_P(a)) = 1$. On the other hand, $\left(\frac{a}{P}\right) = -1$ iff $\nu_2(P-1) = \nu_2(\mathrm{ord}_P(a))$. This establishes the claim.

The important point is that since $N \equiv 3 \bmod 4$, there is some prime $P|N$ with $P \equiv 3 \bmod 4$. By (8), $\left(\frac{a}{P}\right) = -1$, so a is not a square modulo N.

Now, the converse follows from the above, since $a^{(N-1)/2} \equiv \pm 1 \bmod N$ by hypothesis.

Remark 1.

(1) The elliptic analog requires $N \equiv 1 \bmod 4$ and one can indeed have N divisible by a product of an even number of P with all of them equivalent to 3 modulo 4. Moreover, congruence conditions modulo 4 for the elliptic curve setting become less stringent. In general, the group orders are of the form $P + 1 - a$, and not of the fixed form $P - 1$, as for the Fermat test. It is this simple phenomenon that will be crucial to construct a challenge number.

(2) For the general case, i.e., if $N \equiv 1 \bmod 4$ is a strong pseudoprime, one still has property (8), but with the right side replaced by $\nu_2(N-1) = s$ (above, $s = 1$). Specifically [3], if N is a strong pseudoprime and $P|N$, where $P - 1 = 2^{s'} t'$, $2 \nmid t'$, then

$$a^{2^{s'-1}t} \equiv \left(\frac{a}{P}\right) \bmod P. \tag{9}$$

In that case the multiplicative property of the Jacobi symbol is fundamental for the proof that the strong test implies the Euler test.

3. Construction of a challenge number

By Lemma 5 we are aiming at the second case in (6). That is, we try to construct a point $\mathcal{P}$ that looks like a non-double via (6), but which is a double in $E(\mathbb{Z}_N)$.

In terms of the Euler condition this would mean $a^{(N-1)/2} \equiv -1 \bmod N$, but a is indeed a square modulo N. The proof of Lemma 2 reveals the following. For the case that $a^{(N-1)/2} \equiv -1 \bmod N$ one has $\left(\frac{a}{P}\right) = 1$ for $P|N$, provided $\nu_2(P-1) > \nu_2(N-1)$. We would need this condition for all $P|N$, which by the congruence property modulo 4 does not happen. However, group orders of CM curves behave differently.

3.1. Necessary conditions.

In the following, let E have complex multiplication by the field $\mathbb{Q}(\sqrt{-d})$. Specifically, let E and $\mathcal{P}$ be one of the curves together with a point $\mathcal{P}$ on it, as given in Gordon's table, Table 1. In this section we will assume that N is squarefree. This will make it easier to construct a challenge number. Let $e_P(\mathcal{P})$ denote the order of $\mathcal{P}$ on $E(\mathbb{F}_P)$. Suppose we have a composite N with the

following properties:

(10) $\mathcal{P}$ is a double in $E(\mathbb{F}_P)$ for all primes P dividing N,

(11) $\nu_2(e_P(\mathcal{P})) = 1$ for all P dividing N,

(12) for all $P|N$, there is a point of order 4 in $E(\mathbb{F}_P)$,

(13) $\left(\frac{-d}{P}\right) = 1$ and $P \equiv 3 \bmod 4$ for at least one $P|N$.

This is enough for finding a counterexample to the classical result.

Theorem 1. *Let $N \equiv 1 \bmod 4$ be an elliptic pseudoprime. Under the conditions described above, N fulfills Gordon's challenge: N is a strong elliptic pseudoprime which does not pass the Euler analogue. Specifically,*

(14)
$$\left(\frac{N+1}{2}\right)\mathcal{P} \equiv \text{ a 2-torsion point } \bmod N, \text{ but } \mathcal{P} = 2\mathcal{Q} \text{ for some } \mathcal{Q} \text{ in } E(\mathbb{Z}_N).$$

Proof. Clearly, $\mathcal{P}$ needs to be a double in $E(\mathbb{F}_P)$ for all $P|N$. This is (10). Theorem 2 below shows that a necessary condition for the latter is (12). Given that $(N+1)\mathcal{P} \equiv \mathcal{O} \bmod N$, eq. (11) is necessary and sufficient to obtain $\left(\frac{N+1}{2}\right)\mathcal{P} \equiv$ a 2-torsion point modulo N. Condition (13) will be shown in Lemma 9. □

We would like to stress that conditions (10), (11), and (12) are usually mutually exclusive. Experimentally we observe that requiring a point of order 4 'typically' leads to high factors of 2, in both $|E(\mathbb{F}_P)|$, as well as $e_P(\mathcal{P})$. It is quite fortunate that we found enough primes for which all the above conditions are fulfilled.

3.2. **Implementation.** Recall that the curve discriminant is $\Delta = -16(27b^2 + 4a^3)$ and the discriminant of the cubic is $D = -(27b^2 + 4a^3)$. Hence, if p is coprime to D, then

$$\left(\frac{\Delta}{p}\right) = \left(\frac{D}{p}\right). \tag{15}$$

Recall that E has CM by an order in $K = \mathbb{Q}(\sqrt{-d})$. In [4, Table 1], Gordon lists the respective j-invariants of each curve. For our purposes, the relationships involving D are more revealing. We see by inspection that

Proposition 1. *For $d \geq 3$,*

$$\left(\frac{-d}{p}\right) = \left(\frac{D}{p}\right). \tag{16}$$

For $d = 1$, $\left(\frac{-d}{p}\right) = \left(\frac{-1}{p}\right)$, but $\left(\frac{D}{p}\right) = \left(\frac{5}{p}\right)$, and for $d = 2$, $\left(\frac{-d}{p}\right) = \left(\frac{-2}{p}\right)$, but $\left(\frac{D}{p}\right) = \left(\frac{2}{p}\right)$.

3.2.1. *The algorithm.* In the following, we consider the particular curve E and point $\mathcal{P}$ from Gordon's Table 1, [4]:

$$y^2 = x^3 - 3500x - 98000, \quad \mathcal{P} = (84, 448). \tag{17}$$

E has complex multiplication by $\mathbb{Q}(\sqrt{-7})$ and hence, $\left(\frac{-7}{p}\right) = -1$ for primes $p \equiv 3, 5, 6 \bmod 7$. We wish to find a composite N such that $\left(\frac{-7}{N}\right) = -1$, $N \equiv 1 \bmod 4$, and N fulfills (14).

We adapted Erdös' construction mechanism (see, e.g., [1]) by incorporating the conditions above. Erdös' idea was to construct an integer L for which there are a very large number of primes P such that $P-1$ divides L. Suppose that the product of some of these primes is, say, $C = P_1 \cdot \cdots \cdot P_k \equiv 1 \bmod L$. Then each $P_j - 1$ divides L, which divides $C - 1$, and hence C is a Carmichael number by Korselt's criterion [3, p.122].

In our case, for $L = 17272710 = 2 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$, we generated a set S of primes q for which

$$e_q(\mathcal{P}) \text{ divides } L, \tag{18}$$

$$q \text{ satisfies all 4 conditions (10)-(13).} \tag{19}$$

The goal is to get S large enough to contain a subset $\mathsf{T} \subset \mathsf{S}$ with

$$N = \prod_{P \in \mathsf{T}} \equiv -1 \bmod L, \quad \left(\frac{-7}{N}\right) = -1, \quad N \equiv 1 \bmod 4.$$

Any such N will be an elliptic pseudoprime, since $e_P(\mathcal{P})|L|N+1$ for all $P|N$. Moreover, by Theorem 1, N will in fact be a challenge number.

The choice of L is based on the heuristics given for Carmichael numbers N, [1], which guarantee to find N as a product of primes of some set. The difference to the above is that for Carmichael numbers, S is the set of primes with $P-1|L$, and $N \equiv 1 \bmod L$. This condition is much easier than the one above. If $\lambda(L)$ is the Carmichael function which is the largest order of any number modulo L, it is suggested that a size of $|S| > \lambda(L)$ should be sufficient to find a Carmichael number N. For Carmichael numbers, this bound can be improved but we used it as a starting point for our case.

3.2.2. *Underlying theory.* The conditions (10)-(13) are very restrictive. The first few primes q that we found via brute-force are: 617, 1723, 2731, 3191, 6547, 11087, 13103, 21683, 21839, 47737, 49727, 49739, 51679, 52361, 60679, 63719 and then there is a jump and the next ones are 117721, 133169, 145531, 232681, 275183, 281353, 306431, 341879, 373463. Then it seemed that the primes died out. In fact, the next one is not until 607319.

At this point, we only collected 26 primes q, but $\lambda(L) = 36$. Clearly, this required speeding up the algorithm. The approach we took is as follows:

(1) Let $D_e(L)$ be the set of even divisors of L. Sort $D_e(L)$.
(2) Let q be a prime. For each $o \in D_e(L)$ test, if $o\mathcal{P} \equiv \mathcal{O} \bmod q$, but $\left(\frac{o}{2}\right)\mathcal{P} \not\equiv \mathcal{O} \bmod q$. The first o that fulfills this secures (18) and (11) since $2||L$. If there is no such $o \in D_e(L)$, discard q. Since there are only 128 elements in $D_e(L)$, this step is quite fast, but eliminates a lot of unsuccessful prime candidates q.
(3) Testing condition (12) can easily be done for CM curves; see Theorem 3 and its corollary. A necessary and sufficient condition for the existence of a point of order 4 in $E(\mathbb{F}_p)$ is that $p \equiv 3 \bmod 4$. This settles the case $\left(\frac{-d}{p}\right) = -1$.

    Moreover, step (12) can be simplified for any curve E of the form (1) over $\mathbb{F}_p$, when $x^3 + ax + b \equiv 0 \bmod p$ has three roots in $\mathbb{F}_p$. This can be seen as follows.

Recall that $E(\overline{\mathbb{F}}_p)$ is a torsion group where $\overline{\mathbb{F}}_p$ is the algebraic closure of $\mathbb{F}_p$. Here we are interested in points that contain coordinates in $\mathbb{F}_p$ itself (and not only in $\overline{\mathbb{F}}_p$).

Lemma 6. *Let $d > 2$. Suppose that the cubic $x^3 + ax + b$ has three roots α, β, γ in $\mathbb{F}_p$. Then there is a point of order 4 in $E(\mathbb{F}_p)$ if and only if one of the following is true:*

$$\left(\tfrac{\alpha-\beta}{p}\right) = \left(\tfrac{\alpha-\gamma}{p}\right) = 1, \quad \text{or} \tag{20}$$

$$\left(\tfrac{\beta-\alpha}{p}\right) = \left(\tfrac{\beta-\gamma}{p}\right) = 1, \quad \text{or} \tag{21}$$

$$\left(\tfrac{\gamma-\alpha}{p}\right) = \left(\tfrac{\gamma-\beta}{p}\right) = 1. \tag{22}$$

Proof. The hypothesis implies that all the 2-torsion points are in $E(\mathbb{F}_p)$. A necessary condition to get a point of order 4 is that (at least) one of these is a double of some point in $E(\mathbb{F}_p)$. That is, one of $(\alpha, 0), (\beta, 0), (\gamma, 0)$ must be the double of another point. The rest follows from Lemma 1 since 0 is trivially a square. □

Since the cubic has three roots in $\mathbb{F}_p$, this implies that $E(\mathbb{F}_p)$ has a subgroup isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, and hence is not cyclic. Then, by Theorem 3, necessarily $\left(\frac{-d}{p}\right) = 1$ (and not -1).

Note that generally for $\left(\frac{-d}{p}\right) = 1$ one could theoretically obtain points of order 4 when $\mathbb{Z}_2$ is a subgroup of $E(\mathbb{F}_p)$, but $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is not. This would require additional methods for recognizing whether or not $4 | \exp(E(\mathbb{F}_p))$. From Theorem 3 and Corollary 3 below this cannot happen. Hence, Lemma 6 covers the remaining open case $\left(\frac{-d}{p}\right) = 1$.

(4) As mentioned, testing whether $\mathcal{P}$ is a double of something is difficult when Lemma 1 cannot be applied. Essentially, Koblitz showed in [10, eq.(9.3)] that $\mathcal{Q} = (0, y_0) \in E(F_p)$ is a double of some point in $E(F_p)$ iff

$$(A - m^2)^2 - 4(B + 2my_0) \equiv 0 \bmod p. \tag{23}$$

Here, A, B, C are determined by

$$y^2 = x^3 + Ax^2 + Bx + C.$$

Koblitz considers the special case that $y^2 \equiv (x - \alpha)(x - \beta)(x - \gamma)$ with (essentially) $\alpha, \beta, \gamma \in \mathbb{F}_p$. This explains the occurrence of the x^2 term above and then leads to a proof of Lemma 1.

From the proof in [10, p. 49] it is clear that (23) holds for the more general setting that the three roots of the cubic don't all have to be in $\mathbb{F}_p$.

Lemma 7. *Let E be any curve with equation $y^2 = x^3 + Ax^2 + Bx + C$. Then $\mathcal{P} = (x_0, y_0) \in E(\mathbb{F}_p)$ is a double of a point in $E(\mathbb{F}_p)$ iff*

$$m^4 - 2A'm^2 - 8y_0m - 4B' + A'^2 = 0$$

has a solution in $\mathbb{F}_p$, where A', B' are given below.

Proof. Let e_1, e_2, e_3 be the roots of $x^3 + Ax^2 + Bx + C = x^3 + ax + b$, where we allow $e_i \in E(\overline{\mathbb{F}}_p)$. Then $\mathcal{P} = (x_0, y_0) \in 2E(\mathbb{F}_p) \setminus \mathcal{O}$ iff the point with x-coordinate 0, $\mathcal{P}' = (0, y_0) \in 2E'(\mathbb{F}_p) \setminus \mathcal{O}$. Here, $(0, y_0)$ is a point on the

curve E' with equation $y^2 = \big(x-(e_1-x_0)\big)\big(x-(e_2-x_0)\big)\big(x-(e_3-x_0)\big) = x^3 + A'x^2 + B'x + C'$. We get

$$A' = -(e_1-x_0) - (e_2-x_0) - (e_3-x_0) = -e_1 - e_2 - e_3 + 3x_0 = 3x_0 + A,$$
$$B' = (e_1-x_0)(e_2-x_0) + (e_1-x_0)(e_3-x_0) + (e_2-x_0)(e_3-x_0)$$
$$= 3x_0^2 + 2Ax_0 + B.$$

Since $x_0 = 0$ for $\mathcal{P}' = (0, y_0) \in E'(\mathbb{F}_p)$ we can apply condition (23) for the curve E'. This gives the above statement. □

In particular, for $L = 17272710$, we have $\lambda(L) = 36$. The counterexamples (p. 1173 and Example 1) were obtained from the set $\mathsf{S} = \{617, 1723, 2731, 3191, 6547, 11087, 13103, \ldots, 3178891, 3277387, 3815891, 5366089\}$ with $|\mathsf{S}| = 45$.

The computations were done on a Dell D610 laptop during several weeks of the summer of 2008. We never optimized the implementation but only used infrequent access to the UW license server to (periodically) run Maple 11.

3.3. **Implementational issues.**

3.3.1. *Given* $\mathcal{P}$. To find our counterexample we apply the elliptic curve arithmetic to construct $E(\mathbb{Z}_N)$, something that is not a true elliptic curve, when N is a composite number. Generally, when the nature of N is not known, it is customary to deal with pseudocurves (see e.g. [3] and the remarks given there).

Definition 3. For $a, b \in \mathbb{Z}_N$ with $(N, 6) = 1$ and $(4a^3 + 27b^2, N) = 1$, an elliptic pseudocurve over $\mathbb{Z}_N$ is a set

$$E(\mathbb{Z}_N) = \{(x, y) \in \mathbb{Z}_N \times \mathbb{Z}_N : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}. \tag{24}$$

For composite N, the group law operations might fail due to non-invertible elements modulo N. This is the basis for Lenstra's factorization algorithm. In our case, this complicates the construction of counterexamples. Clearly, the concept of elliptic multiplication on a pseudocurve depends on the addition chain used.

Gordon [5] distinguished between two methods.

- 'Method A' uses the standard left-to-right addition chain. The interesting feature about this is that this is really analogous to a strong pseudoprimality test. In fact, the left-to-right (LTR) algorithm calculates all points of the form $\left(\frac{N+1}{2^j}\right)\mathcal{P}$, and if one of these points is a 2-torsion point modulo P for some $P|N$, but is not such modulo another prime factor, then the y-coordinate of the point is divisible by P, and so N will be partially factored during the inversion step in the next doubling. A similar situation arises for the side-steps if one uses the right-to-left (RTL) doubling and multiplication algorithm, but this would result in twice as many pseudoprimes.

  We have not been able to construct counterexamples that allow computation of both $\left(\frac{N+1}{2}\right)\mathcal{P} \bmod N$ and $(N+1)\,\mathcal{P} \bmod N$ without exposing a factor of N. Instead, we used the following.
- 'Method B' [5, p. 296] is a test that does not use inversions. We used the group operations, but for projective coordinates, to avoid inversions. More precisely, for most of the paper we have applied the Modified Projective (MP) Algorithm [3, p. 293], which also avoids inversions but has a lower operation count than projective coordinates.

For the Modified Projective (MP) Algorithm we present $\mathcal{P}$ in projective coordinates as $(84, 448, 1)$. The algorithm first computes $MP((84, 448, 1), m)$, which gives $m\mathcal{P} \bmod N$ in the modified projective presentation. If the output is (m_1, m_2, m_3), then the affine representation requires computing the one inverse $m_3^{-1} \bmod N$. If this inverse does not exist, we discard N.

3.3.2. *Free choice of $\mathcal{P}$.* The factors of N while computing $\left(\frac{N+1}{2^j}\right)\mathcal{P}$ arise from the fact that the orders of $\mathcal{P}$ modulo different $P|N$ might be different. E.g.,

Example 1. For $N = 122993650064325419922521978 9 = \prod_{i=1}^{6} P_i$ and $\mathcal{P} = (84, 884)$ we get

$$\left[\frac{N+1}{2}\right]\mathcal{P} \equiv \begin{cases} [34, 0], & \text{for } P_1 = 617, \\ [70, 0], & \text{for } P_2 = 13103,\ P_3 = 21839, \text{ and } P_5 = 60679, \\ [3802, 0], & \text{for } P_4 = 49739, \\ [2277701, 0], & \text{for } P_6 = 2308121. \end{cases}$$

Using the Chinese Remainder Theorem, this gives rise to the non-trivial 2-torsion point modulo N,

$$\left[\frac{N+1}{2}\right]\mathcal{P} \equiv [10137989263313622228028033508, 0] \bmod N.$$

This would be a counterexample to the Euler test, since

$$2(867839202842227778545409802, 359719680740619525660418872) \equiv \mathcal{P} \bmod N.$$

Example 2 illustrates a 2-torsion point that is the same modulo each $P_i|N$. Hence, any of the above evaluation methods are successful and don't expose a factor of N. The key is that the order of $\mathcal{Q}$ is the same $(= 6)$ for each $P|N$.

Example 2. As above, let $E : y^2 = x^3 - 3500x - 98000$ which has CM by $\mathbb{Q}(\sqrt{-7})$. We choose the point $\mathcal{Q} = (4216, 194)$ and $N = 4661 = 59 \cdot 79$. Then $\left(\frac{-7}{N}\right) = -1$, $N \equiv 1 \bmod 4$, and

$$\begin{aligned} &(4661 + 1)\mathcal{Q} \equiv \mathcal{O} \bmod 4661, \\ &\left(\frac{4661+1}{2}\right)\mathcal{Q} \equiv \begin{cases} (11, 0) \bmod 59, \\ (11, 0) \bmod 79, \end{cases} \equiv (11, 0) \bmod 4661, \\ &2(11, 0) \equiv \mathcal{O} \bmod N. \end{aligned}$$

However,

$$2\mathcal{R} \equiv \mathcal{Q} \bmod N \text{ for } \mathcal{R} = (199, 1112).$$

Again, while $\mathcal{Q}$ looks like a non-double via the Euler analog, it actually is a double of $\mathcal{R}$.

4. Proof of non-existence

4.1. **Doubles and points of order 4.** Recall Definition 2 and Lemma 4. We explore a connection between doubles and points of order 4.

Clearly, for every k with $2k = \exp(E(\mathbb{F}_p))$,

$$\begin{cases} \left[\frac{\mathcal{P}}{p}\right] \equiv \mathcal{O} \bmod p, & \text{iff } \nu_2(e_p(\mathcal{P})) < \nu_2(\exp(E(\mathbb{F}_p))), \\ \left[\frac{\mathcal{P}}{p}\right] \equiv \text{a 2-torsion point mod } p & \text{iff } \nu_2(e_p(\mathcal{P})) = \nu_2(\exp(E(\mathbb{F}_p))). \end{cases} \tag{25}$$

Theorem 2. *Suppose* $\left(\frac{N+1}{2}\right)\mathcal{P} \equiv$ 2-torsion mod N *for some integer* $N \equiv 1 \bmod 4$. *If* $4 \not| \exp(E(\mathbb{F}_P))$ *for* $P|N$, *then* $\mathcal{P}$ *be cannot be a double in* $E(\mathbb{F}_P)$.

Proof. The hypothesis is that $2 \not| k$, where k is as above. From Lemma 4 and (25), $\mathcal{P}$ is a double iff

$$\left[\frac{\mathcal{P}}{P}\right] \equiv \mathcal{O} \bmod P \text{ iff } \nu_2(e_P(\mathcal{P})) < \nu_2(\exp(E(\mathbb{F}_P))).$$

However, $\nu_2(e_P(\mathcal{P})) = 1$ since $\left(\frac{N+1}{2}\right)\mathcal{P} \equiv$ 2-torsion mod P, and $\nu_2(\exp(E(\mathbb{F}_P))) \leq 1$ by hypothesis, a contradiction. □

4.2. **CM curves and group structure.** This section deals with the existence of points of order 4 in $E(\mathbb{F}_p)$. We will be investigating the number of zeros of the cubic

$$x^3 + ax + b = 0 \tag{26}$$

in $\mathbb{F}_p$.

Proposition 2. *Let* $D_C = -2^4 \cdot 3^3 \cdot D$, *where* D *is the discriminant of* (26).

1. *If* $p \equiv -\left(\frac{D_C}{p}\right) \bmod 3$, *then there is only one root of this cubic. In particular,* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ *is not a subgroup of* $E(\mathbb{F}_p)$.
2. *If* $p \equiv \left(\frac{D_C}{p}\right) \bmod 3$, *then* (26) *has either* 0 *or* 3 *solutions. In the former case,* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ *is not a subgroup of* $E(\mathbb{F}_p)$; *in the latter case it is.*

Proof. The statements concerning the number of solutions of (26) were shown by Callier (see [15]). Clearly, by (5), $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ is a subgroup iff the cubic has three roots in $\mathbb{F}_p$. □

In [13], Schoof essentially showed the following result for supersingular curves:

Lemma 8. *Consider any supersingular curve over* $\mathbb{F}_p$. *Then,*

- *for* $p \equiv 1 \bmod 4$, $E(\mathbb{F}_p)$ *is always cyclic;*
- *for* $p \equiv 3 \bmod 4$, *there are two cases:*

$$\begin{cases} E(\mathbb{F}_p) \simeq \mathbb{Z}_{(p+1)/2} \oplus \mathbb{Z}_2 & \text{when } E(\mathbb{F}_p)[2] \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2, \\ E(\mathbb{F}_p) \text{ is cyclic} & \text{otherwise.} \end{cases}$$

For $p \equiv 3 \bmod 4$ the condition is whether or not all the 2-torsion points are in $\mathbb{F}_p$. Equivalently, $E(\mathbb{F}_p)$ is not cyclic iff the cubic (26) has 3 solutions in $\mathbb{F}_p$. In this case, any point will satisfy $\left(\frac{p+1}{2}\right)\mathcal{P} \equiv 0 \bmod p$. This was Gordon's motivation for requiring the challenge number to be congruent to $1 \bmod 4$. However, this restriction is for $d > 2$ not necessary, as Theorem 3 below shows.

Theorem 3. (1) *Let* E *have CM by* $\mathbb{Q}(\sqrt{-d})$ *where* $d \geq 3$. *Then* $E(\mathbb{F}_p) \simeq \mathbb{Z}_{p+1}$ *and hence is cyclic.*

(2) *If* $\left(\frac{-d}{p}\right) = 1$, *then* (26) *has either* 0 *or* 3 *solutions. Moreover,* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ *is a subgroup of* $E(\mathbb{F}_p)$ *iff* (26) *has* 3 *solutions.*

Proof. (1) We show that $p \equiv -\left(\frac{D_C}{p}\right) \bmod 3$. Then the result will follow from Proposition 2 and Lemma 8.

Since E has CM, $\left(\frac{-d}{p}\right) = -1$. Then $\left(\frac{-3}{p}\right) = -\left(\frac{-d}{p}\right)\left(\frac{-3}{p}\right) = -\left(\frac{D}{p}\right)\left(\frac{-3}{p}\right) = -\left(\frac{D_C}{p}\right)$, where we used (16). Hence,

$$-\left(\frac{D_C}{p}\right) = \begin{cases} 1, & \text{for } p \equiv 1 \bmod 3, \\ -1, & \text{for } p \equiv -1 \bmod 3, \end{cases}$$

which gives the desired result.

(2) This follows analogously, since $\left(\frac{-d}{p}\right) = 1$ gives $p \equiv \left(\frac{D_C}{p}\right) \bmod 3$. □

Corollary 2. *Suppose* $\left(\frac{-d}{p}\right) = -1$. *A necessary and sufficient condition for the existence of a point of order 4 in* $E(\mathbb{F}_p)$ *is that* $p \equiv 3 \bmod 4$.

Proof. This follows immediately from Theorem 3. □

Corollary 3. *Suppose* $\left(\frac{-d}{p}\right) = 1$. *A necessary condition for the existence of a point of order* 4 *in* $E(\mathbb{F}_p)$ *is that* (26) *has* 3 *solutions. If we denote these by* α, β, γ, *respectively, then there is a point of order* 4 *iff one of the three conditions* (20)-(22) *is fulfilled.*

Proof. By Theorem 3, (26) can only have 0 or 3 solutions. Clearly, if it has no solutions, then there are no (non-trivial) 2-torsion points in $E(\mathbb{F}_p)$. Hence, there are no points of order 4. The rest follows from Lemma 6. □

Lemma 9. *Suppose there is a composite* $N \equiv 1 \bmod 4$ *with* $\left(\frac{-d}{N}\right) = -1$. *A necessary condition for the existence of a point of order* 4 *in* $E(\mathbb{F}_P)$ *for all primes* $P|N$ *is that for at least one of these,* $\left(\frac{-d}{P}\right) = 1$ *and* $P \equiv 3 \bmod 4$.

Proof. On the one hand we need an odd number of (not necessarily different) primes with $\left(\frac{-d}{P}\right) = -1$. By Corollary 2, for each of these, $P \equiv 3 \bmod 4$. If all primes $P|N$ are of this form, then $N \equiv 3 \bmod 4$ as well. Hence, we need at least one P as stated. □

Remark 2. We investigated all types of curves in Gordon's table, Table 1 (which allow $N \equiv 1 \bmod 4$). For each of the curves with $d \in \{2, 11, 19, 43, 163\}$ it seems that points of order 4 in $E(\mathbb{F}_p)$ for p prime with $\left(\frac{-d}{p}\right) = 1$ can only occur for $p \equiv 1 \bmod 4$. We used Corollary 3 to test all primes up to 10^6. The conditions that $\left(\frac{-d}{p}\right) = 1$ and $p \equiv 3 \bmod 4$ seem to be conflicting conditions for points of order 4. However, we observe that the curve (iv) does satisfy these conditions.

4.3. **The special case of CM by** -3**.** Throughout the remainder of this section we consider the curve

$$y^2 = x^3 + B. \tag{27}$$

Then $\Delta = -16 \cdot 27 \cdot B^2$ and $\left(\frac{-d}{p}\right) = \left(\frac{\Delta}{p}\right) = \left(\frac{-3}{p}\right) = -1$ for $p \equiv 2 \bmod 3$.

Necessary properties pertaining to points of order 4 will show that this curve does not lead to any counterexamples, as above.

For the case $\left(\frac{-d}{p}\right) = 1$, all we know is that $|E(\mathbb{F}_p)| = p + 1 - a$ for some a. Given a specific prime p, Schoof's algorithm [12] works well in practice. Alternatively, for CM curves, $|E(\mathbb{F}_p)|$ can be determined even more efficiently. However, Theorem

3 implies that possibly $\exp(E(\mathbb{F}_p)) \neq |E(\mathbb{F}_p)|$. Hence, we need another method to decide whether or not there is a point of order 4 in $E(\mathbb{F}_p)$.

We give a different condition for the existence of points of order 4, which includes Corollary 2 as a special case. It reveals a relationship between $\left(\frac{-d}{p}\right)$ and $p \bmod 4$ for both $\left(\frac{-d}{p}\right) = 1$ and -1.

Proposition 3. *Let E be given by* (27)*. A necessary condition for the existence of a point of order* 4 *in $E(\mathbb{F}_p)$ is that $p \bmod 3$ equals $p \bmod 4$. In particular, for $\left(\frac{-d}{p}\right) = 1$, necessarily $p \equiv 1 \bmod 4$, and for $\left(\frac{-d}{p}\right) = -1$, necessarily $p \equiv -1 \bmod 4$.*

Proof. Clearly, a necessary condition for the existence of a point of order 4 is that one of the 2-torsion points is a double of something in $\mathbb{F}_p$. We may assume that at least one of the 2-torsion points is in $\mathbb{F}_p$, because otherwise we are done. Then this point is of the form $(x_0, 0)$ where x_0 is a solution of $x^3 + B = 0$ in $\mathbb{F}_p$.

Hence, there has to be a point $(x, y) \in \mathbb{F}_p$ such that

$$2(x, y) = (x_0, 0).$$

In particular, the y-coordinate of $2(x, y)$ has to be 0.

If the curve is given in the form (1), the standard doubling formulas yield the y-coordinate of $2(x, y)$ as the degree 6 polynomial

$$\frac{x^6 + 5x^4a + 20x^3b - 5x^2a^2 - 4axb - a^3 - 8b^2}{8y(x^3 + ax + b)}, \tag{28}$$

and we ask when this has a root in $\mathbb{F}_p$. For the curve $y^2 = x^3 + B$, the condition simplifies to solving

$$x^6 + 20x^3B - 8B^2 \equiv 0 \bmod p,$$

which again reduces to solving the quadratic equation

$$y^2 + 20By - 8B^2 \equiv 0 \bmod p.$$

This is equivalent to solving

$$(2y + 20B)^2 \equiv (20^2 + 32)B^2 \bmod 4p.$$

After changing notation, this reduces to

$$y^2 \equiv (2b)^2 108 \bmod 4p.$$

Since $108 = 2^2 \cdot 3^3$, we conclude that a necessary condition for the existence of a point of order 4 is that

$$\left(\frac{3}{p}\right) = 1.$$

Recall that $d = 3$. If, firstly $\left(\frac{-d}{p}\right) = \left(\frac{-3}{p}\right) = 1$, then what we just showed implies $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right) = 1$ and necessarily $p \equiv 1 \bmod 4$ (actually, $p \equiv 1 \bmod 12$). Analogously, if $\left(\frac{-d}{p}\right) = \left(\frac{-3}{p}\right) = -1$, then necessarily $p \equiv -1 \bmod 4$ (or, more precisely, $p \equiv -1 \bmod 12$). □

Theorem 4. *For $d = 3$ there is no composite integer $N \equiv 1 \bmod 4$ that is a strong elliptic pseudoprime but violates the Euler condition* (14).

Proof. Again, by Lemma 5, it suffices to consider the second assertion in (14). So we need to show there cannot be a point $\mathcal{P}$ that doesn't looks like a double but is. As above, the condition $\left(\frac{N+1}{2}\right)\mathcal{P} = 2 -$ torsion mod N implies $\nu_2(e_P(\mathcal{P})) = 1$ and $\exp(\mathbb{F}_P) = 2k$ for all $P|N$. From Theorem 2, a necessary condition for $\mathcal{P}$ to be a double in $E(\mathbb{F}_P)$ is that $4|\exp(E(\mathbb{F}_P))$. Hence, there needs to be a point of order 4 in each $E(\mathbb{F}_P)$.

By Proposition 3, if $\left(\frac{-d}{N}\right) = -1$, then $N \equiv -1 \bmod 4$. This is a contradiction to the challenge $N \equiv 1 \bmod 4$. □

4.4. **Other CM curves.** We described necessary conditions for the existence of points of order 4. Remark 2 seems to indicate that Proposition 3 generalizes to the other curves (v)-(ix) (those that are by Theorem 3 cyclic). We formulate this as

Conjecture 1. *Let E be any of the curves of type (v)-(ix). Then points of order 4 in $E(\mathbb{F}_p)$ for $\left(\frac{-d}{p}\right) = 1$ are only possible for $p \equiv 1 \bmod 4$.*

This is true for all primes up to 10^6. If this is true in general, the exact same reasoning as above would give the following.

Consequence. For any of the curves of type (iii), as well as (v)-(ix), it follows that any strong elliptic pseudoprime $N \equiv 1 \bmod 4$ is also an Euler elliptic pseudoprime.

5. The general case

5.1. **On an observation of Gordon for $N \equiv 3 \bmod 4$.** Recall that Gordon observed that if $\exp(E(\mathbb{F}_N))$ is $\frac{N+1}{2}$, when N is a prime, then always $\left(\frac{N+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod N$. He noted that, 'this can only happen for $N \equiv 3 \bmod 4$'.

However, the strong version of an elliptic pseudoprime test is only 'stronger' than the Euler version when $4|N+1$. The 'stronger' condition for the Fermat test utilizes the celebrated fact that whenever $a^{2^{i+1}t} \equiv 1 \bmod N$ for some prime $N = 2^s \cdot t + 1$ with t odd, then necessarily $a^{2^i t} \equiv \pm 1 \bmod N$. However, this poses strong restrictions on the primes $P|N$. For the case that $a^t \equiv 1 \bmod N$, we see that $\nu_2(\mathrm{ord}_P(a)) = 0$, while for the case $a^{2^i t} \equiv -1 \bmod N$, $\nu_2(\mathrm{ord}_P(a)) = i + 1$, and this is the same constant value for all $P|N$. This property distinguishes Fermat pseudoprimes from strong pseudoprimes.

Hence, we expect that the strong elliptic version would be equally stronger. By Theorem 3, Gordon's restriction that $N \equiv 1 \bmod 4$ is not necessary for $d > 2$.

5.2. **$\mathcal{P}$ doesn't look like a double, but is.** The question arises whether the above approach for $N \equiv 1 \bmod 4$ would yield similar results for $N \equiv 3 \bmod 4$. As above, we aim at

$$\left(\frac{N+1}{2}\right) \equiv 2\text{-torsion mod } N, \text{ but } \mathcal{P} \text{ is a double.} \tag{29}$$

The following incorporates the case $2||N+1$, but is more stringent for $2^s|N+1$ for larger s, where $N + 1 = 2^s \cdot t$ with t odd.

Lemma 10. *Let $N+1 = 2^s \cdot t$ with $2 \nmid t$ an elliptic pseudoprime. If*

$$\mathcal{P} \text{ is a double in } E(\mathbb{F}_P) \text{ for all primes } P \text{ dividing } N, \tag{30}$$

$$\nu_2(e_P(\mathcal{P})) = s \text{ for all } P \text{ dividing } N, \tag{31}$$

$$\text{for all } P|N, \text{ there is a point of order } 2^{s+1} \text{ in } E(\mathbb{F}_P), \tag{32}$$

$$\left(\frac{-d}{P}\right) = 1 \text{ and } P \equiv 2^s + 1 \bmod 2^{s+1} \text{ for at least one } P|N, \tag{33}$$

then N fulfills (29).

Proof. The proof is analogous to the one for Theorem 1. The condition $P \equiv 2^s + 1 \bmod 2^{s+1}$ ensures that $2^s || N+1$, i.e., that $2 \nmid t$. □

These conditions are very restrictive. By Conjecture 1, we can only expect to find such numbers for the curve (iv). In the following, we give an example for $s = 2$ (the easiest case for $N \equiv 3 \bmod 4$), but for a point $\mathcal{P}$ of our choosing. We have not been able to find a counterexample for Gordon's point $(84, 448)$.

Example 3. Consider Gordon's curve $E : y^2 = x^3 - 3500x - 98000$ with CM by $\mathbb{Q}(\sqrt{-7})$. Let $\mathcal{P} = (172472, 139758)$ and

$$N = 245699 = 277 \cdot 887.$$

Here, $\left(\frac{-7}{N}\right) = -1$ and $2^2 || N+1$. Then

$$(N+1)\mathcal{P} \equiv \mathcal{O} \bmod N,$$

$$\left(\frac{N+1}{2}\right)\mathcal{P} \equiv (152634, 0) \bmod N.$$

So N is a strong elliptic pseudoprime and $\mathcal{P}$ appears to be a non-double. However,

$$2(190103, 153439) \equiv \mathcal{P} \bmod N$$

for $(190103, 153439) \in E(\mathbb{Z}_N)$.

In this example, $\mathcal{P}$ has order 12 modulo each factor, and hence modulo N. Hence, any addition chain can be used to compute the above result.

We have the following refinement of Conjecture 1, which we verified for all primes up to 10^5.

Conjecture 2. *Let $s \geq 1$ and E be any curve of type (iii), resp. (v)-(ix). Then points of order 2^{s+1} in $E(\mathbb{F}_p)$ for $\left(\frac{-d}{p}\right) = 1$ can only occur for $p \equiv 1 \bmod 2^{s+1}$.*

By Lemma 10, this would lead to the general result, which includes the above for $N \equiv 1 \bmod 4$.

Consequence. Under Conjecture 2 there are no points that 'don't look like a double but are', for any of the curves of type (iii), as well as (v)-(ix).

5.3. $\mathcal{P}$ **looks like a double, but isn't.** In the following we are interested in a point $\mathcal{P}$ that looks like a double via (6), but isn't.

Remark 3. This concept may seem to be analogous to 'pseudosquares' [16, p.412]. However, these are integers that 'behave' like a square modulo certain primes. In our case we rely on properties of composites to ensure the required conditions.

According to Lemma 5 this cannot occur for $N \equiv 1 \bmod 4$.

Lemma 11. *Suppose $N \equiv 3 \bmod 4$ is an elliptic pseudoprime such that for all $P|N$,*

$$\nu_2(e_P(\mathcal{P})) = \nu_2\left(\frac{N+1}{2^l}\right) \tag{34}$$

for some $l \geq 1$. Then N is a strong elliptic pseudoprime. Specifically,

$$\left(\frac{N+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod N,$$
$$\left(\frac{N+1}{2^{l+1}}\right)\mathcal{P} \equiv \textit{some } 2\text{-torsion point} \bmod N.$$

Proof. This follows directly from the hypothesis. □

Any such point $\mathcal{P}$ looks like a double. However, it does *not* have to be a double, as the following example shows.

Example 4. Consider Gordon's curve (iii), $y^2 = x^3 + 3$ with point $\mathcal{P} = (1, 2)$ and $d = 3$. For $N = 83139622019 = 41 \cdot 83 \cdot 4177 \cdot 5849$ we have $\left(\frac{-3}{N}\right) = -1$, $N \equiv 7 \bmod 8$ and

$$\left(\frac{N+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod N,$$
$$\left(\frac{N+1}{4}\right)\mathcal{P} \equiv (10491607602, 0) \bmod N.$$

However, $\mathcal{P}$ is not a double in $E(\mathbb{F}_P)$ for the prime factors $P|N$, $41, 4177, 5849$, so it is not a double modulo N. Specifically, $E(\mathbb{F}_{41})$ has generator $(17, 18)$. But $(1, 2) = 15(17, 18)$ and since 15 is odd, we see that $(1, 2)$ is not a double in $E(\mathbb{F}_{41})$.

Note that we have shown in Theorem 4 that for this type of curve there are *no* composites that lead to the situation '$\mathcal{P}$ doesn't look like a double, but is'.

Remark 4. It seems to be easier to construct counterexamples for a point of the form, 'looks like a double, but isn't'. In fact, $\mathcal{P}$ only needs to be a non-double for (at least one) prime factor of N. Note that Gordon's initial challenge $N \equiv 1 \bmod 4$ (while based on a different argument) would not allow this.

Remark 5. In this section, any 2-torsion point is nontrivial in the sense that it is not the same in each $E(\mathbb{F}_P)$. Here, the computations utilize the Chinese Remainder Theorem and the fact that $E(\mathbb{Z}_{n_1 n_2}) \simeq E(\mathbb{Z}_{n_1}) \oplus E(\mathbb{Z}_{n_2})$ for odd integers with n_1, n_2 with $(n_1, n_2) = 1$. As in Example 2 and Example 4, this can be avoided by constructing a point that has the same order in each $E(\mathbb{F}_P)$ for all $P|N$. This can be done via a simple modification of the algorithm described above (but this would result in points different from those given by Gordon).

Table 2 gives such counterexamples for *each* of Gordon's curves, along with the respective given point on it. In all cases, $\left(\frac{-d}{N}\right) = -1$, $\left(\frac{N+1}{2}\right)\mathcal{P} \equiv \mathcal{O} \bmod N$, but there is no point $\mathcal{Q}$ with $\mathcal{P} \equiv 2\mathcal{Q} \bmod N$.

TABLE 2

strong but not Euler: non-doubles appear to be doubles			
curve	$\mathcal{P}$	N	$\left(\frac{N+1}{2^{l+1}}\right)\mathcal{P} \bmod N$
(i)	(5,10)	9090870127122419 = $61 \cdot 997 \cdot 1289 \cdot 3851 \cdot 30113$	(4036547764918982, 0) $(l = 1)$
(ii)	(64,504)	120917159 = $11 \cdot 19 \cdot 41 \cdot 103 \cdot 137$	(6959692, 0) $(l = 2)$
(iii)	(1,2)	83139622019 = $41 \cdot 83 \cdot 4177 \cdot 5849$	(10491607602, 0) $(l = 1)$
(iv)	(84,884)	32759 = $17 \cdot 41 \cdot 47$	(2345, 0) $(l = 2)$
(v)	(33,121)	16142173358219 = $17 \cdot 257 \cdot 991 \cdot 1429 \cdot 2609$	(15389548052101, 0) $(l = 1)$
(vi)	(57,19)	26583876053828615339 = $23 \cdot 41 \cdot 1213 \cdot ... \cdot 3407$	(6809585105401582053, 0) $(l = 1)$
(vii)	(817, 2537)	5470919= $89 \cdot 61471$	(4589876, 0) $(l = 2)$
(viii)	(201, 67)	51952080584902915346365 79= $53 \cdot 83 \cdot ... \cdot 218651$	(3604099946727828526761 69, 0) $(l = 1)$
(iv)	(3400,548)	41153384804755859 = $17 \cdot 137 \cdot 389 \cdot 147629 \cdot 307691$	(29011658891746501, 0) $(l = 1)$

SUMMARY

This paper gives an answer to a question about certain types of elliptic pseudoprimes, showing that they do exist in certain cases and not in others. While we were able to generalize Gordon's original challenge to any composite integers N, we were not able to provide a proof of the nonexistence of certain composites to all types of curves.

ACKNOWLEDGEMENT

The author would like to thank the referee for many insightful and helpful remarks that helped improve both the content and presentation of this paper.

REFERENCES

1. W. R. Alford, Andrew Granville, and Carl Pomerance, *There are infinitely many Carmichael numbers*, Annals of Mathematics **139** (1994), 703–722, URL: `http://cr.yp.to/bib/entries.html#1994/alford`.
2. Daniel Bleichenbacher, *Efficiency and security of cryptosystems based on number theory*, Ph.D. thesis, 1996, URL: `http://www.bell-labs.com/user/bleichen/diss/thesis.html`.
3. Richard Crandall and Carl Pomerance, *Prime numbers*, A computational perspective. Springer-Verlag, New York, 2001. MR2002a:11007
4. Daniel M. Gordon, *On the number of elliptic pseudoprimes*, Math. Comp. **52** (1989), no. 185, 231–245. MR946604 (89f:11169)
5. ———, *Pseudoprimes on elliptic curves*, Théorie des nombres (Quebec, PQ, 1987), de Gruyter, Berlin, 1989, pp. 290–305. MR1024570 (91g:11158)
6. Daniel M. Gordon and Carl Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), no. 196, 825–838. MR1094951 (92h:11081)
7. Jon Grantham, *A probable prime test with high confidence*, Journal of Number Theory **72** (1998), 32–47, URL: `http://www.pseudoprime.com/jgpapers.html`. MR1643284 (2000e:11160)

8. ———, *Frobenius pseudoprimes*, Mathematics of Computation **70** (2001), 873–891, URL: `http://www.pseudoprime.com/pseudo.html`. MR1680879 (2001g:11191)
9. Anthony W. Knapp, *Elliptic curves*, Mathematical Notes, vol. 40, Princeton University Press, Princeton, NJ, 1992. MR1193029 (93j:11032)
10. Neal Koblitz, *Introduction to elliptic curves and modular forms*, second ed., Graduate Texts in Mathematics, vol. 97, Springer-Verlag, New York, 1993. MR1216136 (94a:11078)
11. Siguna Müller, *On QF-pseudoprimes and second-order recurrence sequences*, Contributions to general algebra, 12 (Vienna, 1999), Heyn, Klagenfurt, 2000, pp. 299–310. MR1777670 (2001e:11016)
12. René Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), no. 170, 483–494. MR777280 (86e:11122)
13. ———, *Counting points on elliptic curves over finite fields*, J. Théor. Nombres Bordeaux **7** (1995), no. 1, 219–254, Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993). MR1413578 (97i:11070)
14. Lawrence C. Washington, *Elliptic curves: Number theory and cryptography*, Discrete Mathematics and Its Applications, Chapman & Hall/CRC, May 2003.
15. H. C. Williams and C. R. Zarnke, *Some algorithms for solving a cubic congruence modulo p*, Utilitas Math. **6** (1974), 285–306. MR0389730 (52 #10561)
16. Hugh C. Williams, *Édouard Lucas and primality testing*, John Wiley & Sons Inc., New York, 1998, A Wiley-Interscience Publication. MR2000b:11139

Department of Mathematics, RH 311, University of Wyoming, Laramie, Wyoming 82071

E-mail address: `smuller@uwyo.edu`