A remark on prime (non)congruent numbers

Evink, Tim; Top, Jaap; Top, Jakob Dirk

Published in:
Quaestiones mathematicae

DOI:
10.2989/16073606.2021.1977410

Quaestiones Mathematicae

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tqma20

A remark on prime (non)congruent numbers

Tim Evink, Jaap Top & Jakob Dirk Top

To cite this article: Tim Evink, Jaap Top & Jakob Dirk Top (2022) A remark on prime (non)congruent numbers, Quaestiones Mathematicae, 45:12, 1841-1853, DOI: 10.2989/16073606.2021.1977410

To link to this article: https://doi.org/10.2989/16073606.2021.1977410

Published online: 01 Nov 2021.

Quaestiones Mathematicae 2022, 45(12): 1841–1853

https://doi.org/10.2989/16073606.2021.1977410

A REMARK ON PRIME (NON)CONGRUENT NUMBERS

Tim Evink

Institute of Algebra and Number Theory, Ulm University, Helmholtzstr. 18, 89081 Ulm, Germany.
E-Mail tim.evink@uni-ulm.de

Jaap Top*

Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands.
E-Mail j.top@rug.nl

Jakob Dirk Top

Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands.
E-Mail j.d.top@rug.nl

Abstract. This paper discusses prime numbers that are (resp. are not) congruent numbers. Particularly the only case not fully covered by earlier results, namely primes of the form $p = 8k + 1$, receives attention.

Mathematics Subject Classification (2020): 11G05, 11A41, 11R11, 11N32.

Key words: Congruent number, elliptic curve, Selmer group, Shafarevich-Tate group, Bouniakowsky's conjecture.

1. Introduction. A congruent number is, by definition, a positive integer n that occurs as the area of a rectangular triangle with rational side lengths. In other words, nonzero $a, b, c \in \mathbb{Q}$ should exist such that $a^2 + b^2 = c^2$ and $ab/2 = n$. A classical, equivalent definition is that $n > 0$ is a congruent number precisely when an arithmetic progression $(x-n, x, x+n)$ consisting of three rational squares exists. There is an abundance of literature on congruent numbers, particularly because of their connection to the arithmetic of elliptic curves and to modular forms. For example, the textbook [13] describes many of the spectacular results on congruent numbers. Part of it is also discussed in [30], and various centuries old results including some that already appeared in Leonardo Pisano's *Liber Quadratorum* published in 1225, can be found in [8, Chapter XVI]. Many investigations regarding (non)congruent numbers start with the standard and well-known observation (1) ⇔ (2) ⇔ (3), with

*Corresponding author.

(1) n is a congruent number;

(2) $E^{(n)}\colon y^2 = x^3 - n^2x$ contains a point $(a, b) \in E^{(n)}(\mathbb{Q})$ with $b \neq 0$;

(3) $E^{(n)}\colon y^2 = x^3 - n^2x$ contains $P \in E^{(n)}(\mathbb{Q})$ of infinite order.

In the present note we collect some information regarding prime numbers that are congruent numbers or noncongruent numbers. Concretely:

- We review known results, including detailed references to in some cases very classical sources (the remainder of the present section).
- We recall the equivalence of various conditions that imply a prime $p \equiv 1 \bmod 8$ to be a noncongruent number and reformulate this in a way allowing one to obtain a density result on the number of such primes (Proposition 2.1 and Corollary 2.6).
- By comparing a 2-descent over $\mathbb{Q}$ with a 2-descent over $\mathbb{Q}(\sqrt{p})$ we obtain a new and relatively general approach towards obtaining classical results on a class of primes $p \equiv 1 \bmod 8$ not being congruent numbers (Propositions 2.3 and 2.5 as well as Corollary 2.6).
- The only primes for which no unconditional general statement on being or not being a congruent number is known to date, are the $p \equiv 1 \bmod 8$ ones not in the class referred to above. We present some data useful for predicting density statements in this case (Section 3).
- We show how a conjecture of Bouniakowsky implies the existence of infinitely many primes $p \equiv 1 \bmod 8$ that are congruent numbers. Moreover we estimate the number of primes below any bound b that our construction is predicted to give (Proposition 3.1 and Remark 3.2).

Recognizing whether a prime is a congruent number or not, is also the topic of the 2006 master's thesis [11]. The detailed explanation given there allows us to remain brief on some issues here.

Historically, $p = 2$ is the subject of [1, Proposition XII, pp. 114–116]: Peter Barlow already in 1811 showed that 2 is not a congruent number. As for the odd primes p, probably the earliest result not restricted to a single prime is due to A. Genocchi (1855, [10, pp. 314–315], see also T. Nagell's 1929 expository text [17, pp. 16–17]): no prime $p \equiv 3 \bmod 8$ is a congruent number. The same result with a totally different and much less elementary proof is presented in [31, Proposition 5]. In contrast, *every* prime $p \equiv 5, 7 \bmod 8$ turns out to be a congruent number. This is observed in a short paper by N.M. Stephens [24, bottom of p. 183]; a detailed proof can be found in [16].

The situation for $p \equiv 1 \bmod 8$ is less complete. L. Bastien [3] in 1915 announced that, writing $p = a^2 + b^2$ as a sum of two squares, if the Legendre symbol $\left(\frac{a+b}{p}\right)$ equals -1 then p is not a congruent number. The same result can be deduced from a theorem by Michael J. Razar (1974): although his condition on p looks different at first sight and the notion "congruent number" does not occur in the paper, from [19, Thm 2] and the remarks on "first descent" contained in the text it is immediate that if one of the following conditions holds:

(a) $p \equiv 1 \bmod 16$ and 2 is not a 4th power modulo p;

(b) $p \equiv 9 \bmod 16$ and 2 is a 4th power modulo p,

then p is not a congruent number. Yet another way to formulate this result, is presented in J.B. Tunnell's 1983 paper [31, Proposition 6]: if the prime $p \equiv 1 \bmod 8$ is written as $p = a^2 + 4b^2$ for integers a, b, then $16 \nmid p - 1 + 4b \Rightarrow$ p is not a congruent number. Tunnell's proof is very different from Razar's. Again an alternative way to formulate and prove the same result one finds in the 2006 master's thesis of Brett Hemenway [11, p. 41]. He shows, writing $p \equiv 1 \bmod 8$ as $p = a^2 + b^2$ for integers a, b, that if $(a + b)^2 \equiv 9 \bmod 16$ then p is not a congruent number. His proof (in fact similar to Razar's but more detailed) consists of a 2-descent on the elliptic curve given by $y^2 = x^3 + 4p^2x$; this curve is 2-isogenous to the one with equation $y^2 = x^3 - p^2x$. Although involving different curves, this is very much in the spirit of [29]. The last way we mention of formulating an equivalent result is a special case of [18, Theorem 1.1(1)]: if for a prime $p \equiv 1 \bmod 8$ the Legendre symbol $\left(\frac{1+i}{p}\right) = -1$ (here $i \in \mathbb{F}_p$ is a square root of -1), then p is not a congruent number.

In the next section we discuss the equivalence of the criteria above. In particular this allows one to find the density of the involved set of primes. We also sketch how, apart from the fact that all primes $\equiv 5, 7 \bmod p$ are congruent numbers, the results mentioned here can be verified by comparing 2-descents over $\mathbb{Q}$ and over $\mathbb{Q}(\sqrt{p})$; this unified approach, inspired by [9] and in particular by Propositions 5.5-5.6 in *loc. sit.*, is somewhat different from what one finds in earlier literature. The last section contains results and some data regarding primes $p \equiv 1 \bmod 8$ *not* satisfying the equivalent conditions described above.

2. Equivalences and Selmer groups.

Consider a prime number $p \equiv 1 \bmod 8$. The congruence condition implies that -1 is a fourth power modulo p and that 2 is a square modulo p. Moreover, one can write $p = a^2 + b^2$ for integers a, b of which one is odd and the other is divisible by 4. The equivalences mentioned in the introduction are included in the next result. It uses a certain Galois extension $N/\mathbb{Q}$, namely the splitting field over $\mathbb{Q}$ of the minimal polynomial $x^4 - 2x^2 + 2$ of $\alpha := \sqrt{1 + i}$; this minimal polynomial has zeroes $\pm\alpha$ and $\pm\beta$ with $(\alpha\beta)^2 = 2$. Hence $N = \mathbb{Q}(\sqrt{2}, \alpha)$ and the Galois group $\mathrm{Gal}(N/\mathbb{Q})$ is the dihedral group of order 8, with generators ρ (of order 4) defined by $\alpha \mapsto \beta \mapsto -\alpha$ and σ (of order 2) defined by $\alpha \mapsto \beta \mapsto \alpha$. Note $\mathrm{Gal}(N/\mathbb{Q}(\sqrt{-2})) = \langle\rho\rangle$ (cyclic group of order 4; $(\alpha^3 - \alpha)\beta$ is a square root of -2 and is fixed by ρ). The element ρ^2 is the unique nontrivial element in the center of $\mathrm{Gal}(N/\mathbb{Q})$; the field of invariants under ρ^2 equals $\mathbb{Q}(i, \sqrt{2})$ which is the 8-th cyclotomic field. In particular, ρ^2 being in the center implies that a Frobenius element as appearing in part (7) of the next result, is well-defined (and not only defined up to conjugacy).

PROPOSITION 2.1. *For a prime $p \equiv 1 \bmod 8$ the following statements are equivalent.*

(1.) *For $j \in \mathbb{Z}$ with $j^2 \equiv -1 \bmod p$ one has $\left(\frac{1+j}{p}\right) = -1$.*

(2.) *For $r \in \mathbb{Z}$ with $r^2 \equiv 2 \bmod p$ one has $\left(\frac{1+r}{p}\right) = -1$.*

(3.) *For $r \in \mathbb{Z}$ with $r^2 \equiv 2 \bmod p$ one has $(-1)^{(p-1)/8} \cdot \left(\frac{r}{p}\right) = -1$.*

(4.) *Writing $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$, one has $\left(\frac{a+b}{p}\right) = -1$.*

(5.) *Writing $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$, one has $(a+b)^2 \equiv 9 \bmod 16$.*

(6.) *Writing $p = a^2 + 4c^2$ with $a, c \in \mathbb{Z}$, one has $16 \nmid p - 1 + 4c$.*

(7.) *The (unique) Frobenius element in $G := \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{1+i})/\mathbb{Q})$ corresponding to p equals the generator of the center of G.*

(8.) *With M the normal closure of $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbb{Q}$ which is a dihedral extension of degree 8, the (unique) Frobenius element in $\mathrm{Gal}(M/\mathbb{Q})$ corresponding to p equals the generator of the center.*

Proof. (1.)⇔(2.): this is also shown in [19, Lemma 2]. If $i, r \in \mathbb{F}_p$ satisfy $i^2 = -1$ and $r^2 = 2$, then one has $(1+i)(1+r) = (1+\zeta)^2$ for $\zeta \in \mathbb{F}_p^\times$ of order 8. The result follows.
(1.)⇔(3.): with $\zeta \in \mathbb{F}_p$ as above, note that $i := \zeta^2$ satisfies $i^2 = -1$ and $r := \zeta\cdot(1-i)$ has the property $r^2 = 2$. Therefore

$$(-1)^{(p-1)/8} \cdot \left(\frac{r}{p}\right) = \left(\frac{\zeta}{p}\right) \cdot \left(\frac{r}{p}\right) = \left(\frac{\zeta^2 \cdot (1-i)}{p}\right) = \left(\frac{1+i}{p}\right).$$

(1.)⇔(4.): this is also shown in [11, §5.4.1], for completeness we recall the proof. In $p = a^2 + b^2$ we can and will assume a is odd. Using the Jacobi symbol and in particular reciprocity for it, one finds the property $\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{a^2+b^2}{a}\right) = 1$, hence with $i := (b \bmod p)/(a \bmod p) \in \mathbb{F}_p$ a primitive 4th root of unity $\left(\frac{a+b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{1+i}{p}\right) = \left(\frac{1+i}{p}\right)$.
(4.)⇔(5.): this also follows using [11, §5.4.1], we repeat the calculation.

$$\left(\frac{a+b}{p}\right) = \left(\frac{p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{(a+b)^2 + (a-b)^2}{a+b}\right) = (-1)^{\left((a+b)^2-1)\right)/8},$$

from which the result is immediate.
(5.)⇔(6.): as before, write $p = a^2 + b^2$ with a odd. The assumption $p \equiv 1 \bmod 8$ implies $4|b$. With $b = 2c = 4d$ one obtains congruences $(a+b)^2 \equiv a^2 + 8ad \equiv a^2 + 8d \equiv p + 4c \bmod 16$ and the result follows.
(1.)⇔(7.): use the notations preceding the statement of Proposition 2.1, and fix an embedding $\mathbb{Q}(\zeta) \subset \mathbb{Q}_p$. One has $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta, \alpha) = N$ where ζ is a primitive 8th root of unity, $i = \zeta^2$, and each consecutive extension has degree 2. Note that $\mathbb{Q}(\zeta)$ is the field of invariants of the generator ρ^2 of the center of

Gal($N/\mathbb{Q}$). The condition $p \equiv 1 \bmod 8$ is equivalent to p splitting completely in $\mathbb{Q}(\zeta)$. Hence p-adically one obtains $\mathbb{Q}_p(\zeta) = \mathbb{Q}_p$ with the extension obtained by adjoining a square root of $1+i \in \mathbb{Q}_p$. This extension is nontrivial precisely when a Frobenius at p acts nontrivially on N, hence as ρ^2. Since $1+i$ is a square in $\mathbb{Q}_p$ iff $\left(\frac{1+I}{p}\right) = 1$ where I denotes the reduction of i in the residue field $\mathbb{F}_p$ of $\mathbb{Q}_p$, this proves the result.

(2.)⇔(8.): the minimal polynomial of $\gamma := \sqrt{1+\sqrt{2}}$ over $\mathbb{Q}$ equals $x^4 - 2x^2 - 1$ with zeroes $\pm\gamma$ and $\pm\delta$, where $(\gamma\delta)^2 = -1$. The splitting field M fits in a tower $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(\zeta) \subset \mathbb{Q}(\zeta, \gamma) = M$ where ζ is a primitive 8th root of unity and each consecutive extension has degree 2. The remainder of the argument is analogous to the proof of (1.)⇔(7.), with now $1+\sqrt{2}$ taking the role of $1+i$. □

REMARK 2.2. Note that the fields N and M appearing here are isomorphic; this provides a direct proof of (7.)⇔(8.). This elementary observation is in fact the special case $(Q, a, b, x, y, z) = (\mathbb{Q}, -1, 2, 1, 1, 1)$ of [26, Cor. 5.2].

Several of the conditions appearing in Proposition 2.1 play a role in various papers on 8-rank of class groups. For example, [12, Theorem 2] states for primes $p \equiv 1 \bmod 8$ that the class number of $\mathbb{Q}(\sqrt{-p})$ is not divisible by 8 precisely when condition (5.) holds. This equivalence was already observed by Gauss in a letter to Dirichlet dated 30 May 1828. Similarly, reformulating [6, Theorem 1] yields that for primes $p \equiv 1 \bmod 8$ the class number of $\mathbb{Q}(\sqrt{-p})$ is not divisible by 8 precisely when condition (6.) holds. Included in [2, Main Theorem] as well as in part of [25, Thm 1], the same class number criterion is shown to be equivalent to (1.). A reason for these relations with class numbers can be found as a special case of [32, Theorem 1.1]. Still other equivalent criteria as well as many of the ones above are listed in [15, Lemma-Def. 1] and [32, Thm 4.2]. As an additional, related and very accessible text in the same spirit we refer to [7].

Alternatively, the conditions (1.)–(8.) can be expressed in terms of a Rédei symbol (see, e.g., [26, Sections 4,6] for a precise definition, notation, and relevant examples). They are equivalent to the statement $[-1, 2, p] = -1$.

We now provide some details regarding the 2-descent calculations for the elliptic curves involved. For any prime number p, write

$$E^{(p)} \colon y^2 = x^3 - p^2 x.$$

The curve $E^{(p)}/\mathbb{Q}$ has good reduction away from $\{2, p\}$. With notations as in, e.g., [22, Ch. X §1] take $S = \{2, p, \infty\}$ and denote $\mathbb{Q}(S) = \mathbb{Q}(S, 2) := \{x \in \mathbb{Q}^*/\mathbb{Q}^{*2} : v(x) \equiv 0 \bmod 2 \text{ for all } v \notin S\}$ which is an elementary 2-group generated by the classes of $-1, 2$, and p. With

$$H := \{(c_1, c_2, c_3) \in \mathbb{Q}(S) \times \mathbb{Q}(S) \times \mathbb{Q}(S) \;:\; c_1 c_2 c_3 = 1\},$$

one has the Kummer homomorphism $\delta \colon E^{(p)}(\mathbb{Q}) \to H$ with kernel $2E^{(p)}(\mathbb{Q})$ given by

$$\delta(a,b) = \begin{cases} (a+p, a, a-p) & \text{for } b \neq 0; \\ (2, -p, -2p) & \text{for } a = -p; \\ (p, -1, -p) & \text{for } a = 0; \\ (2p, p, 2) & \text{for } a = p. \end{cases}$$

One has local versions $\delta_v\colon E^{(p)}(\mathbb{Q}_v) \to H_v$ of this, obtained by replacing $\mathbb{Q}$ by the completion $\mathbb{Q}_v$. The inclusion $\mathbb{Q} \subset \mathbb{Q}_v$ induces maps $E^{(p)}(\mathbb{Q})/2E^{(p)}(\mathbb{Q}) \to E^{(p)}(\mathbb{Q}_v)/2E^{(p)}(\mathbb{Q}_v)$ as well as $\mathbb{Q}(S) \to \mathbb{Q}_v^*/\mathbb{Q}_v^{*2}$ and $H \to H_v$; they will all be denoted as ι_v. The 2-Selmer group $S^2(E^{(p)}/\mathbb{Q}) \subset H$ is given by

$$S^2(E^{(p)}/\mathbb{Q}) := \left\{c = (c_1, c_2, c_3) \in H \;:\; \iota_v(c) \in \delta_v(E^{(p)}(\mathbb{Q}_v))\,\forall\, v \in S\right\}.$$

It fits in a short exact sequence

$$0 \to E^{(p)}(\mathbb{Q})/2E^{(p)}(\mathbb{Q}) \xrightarrow{\delta} S^2(E^{(p)}/\mathbb{Q}) \longrightarrow Ш(E^{(p)}/\mathbb{Q})[2] \to 0$$

where $Ш(E^{(p)}/\mathbb{Q})[2]$ is the 2-torsion in the Shafarevich-Tate group of $E^{(p)}/\mathbb{Q}$. To ease notation, for fields F an element $cF^{*2} \in F^*/F^{*2}$ will simply be denoted c. A short calculation shows:

- $\delta_\infty(E^{(p)}(\mathbb{R}))$ is generated by $(1, -1, -1)$;
- $\delta_p(E^{(p)}(\mathbb{Q}_p))$ is generated by $(2, -p, -2p)$, $(p, -1, -p)$ for $p \neq 2$;
- $\delta_2(E^{(p)}(\mathbb{Q}_2))$ has generators $(2, -p, -2p)$, $(p, -1, -p)$, $(5, 1, 5)$ for $p \neq 2$. Here, apart from 2-torsion one may use the point $(\frac{1}{4}, \frac{1}{8}\sqrt{1 - 16p^2}) \in E^{(p)}(\mathbb{Q}_2)$.

An immediate consequence is the following.

PROPOSITION 2.3. $\dim_{\mathbb{F}_2} S^2(E^{(p)}/\mathbb{Q}) = \begin{cases} 4 & \textit{if } p \equiv 1 \bmod 8; \\ 2 & \textit{if } p \equiv 3 \bmod 8; \\ 3 & \textit{if } p \equiv 5, 7 \bmod 8. \end{cases}$

Proof. We only sketch the case $p \equiv 1 \bmod 8$, the other cases are analogous. Since $p \equiv 1 \bmod 8$, one has that $-1, 2$ are squares in $\mathbb{Q}_p$ hence the δ_p-image is generated by $(1, p, p)$ and $(p, 1, p)$. Similarly, the δ_2-image has generators $(2, -1, -2)$, $(1, -1, -1)$, $(5, 1, 5)$. Considering the δ_∞-image one observes that the first coordinate of any $c \in S^2(E^{(p)}/\mathbb{Q})$ is one of $\{1, 2, p, 2p\}$. Now consider the possibilities: if $c = (1, a, a)$, then the local conditions at $2, p$ imply $a \in \{\pm 1, \pm p\}$, giving 4 elements. For $c = (2, a, 2a)$ again one finds $a \in \{\pm 1, \pm p\}$, and the same conclusion holds for $c = (p, a, ap)$ and $c = (2p, a, 2ap)$. □

Using Monsky's result (predicted by Stephens) asserting that primes $p \equiv 5, 7 \bmod 8$ are congruent numbers, the following is a consequence.

COROLLARY 2.4. *For any odd prime* $p \not\equiv 1 \bmod 8$ *one has*

$$Ш(E^{(p)}/\mathbb{Q})[2] = (0) \;\; \textit{and} \;\; \textit{rank}\, E^{(p)}(\mathbb{Q}) = \begin{cases} 0 & \textit{if } p \equiv 3 \bmod 8, \\ 1 & \textit{if } p \equiv 5, 7 \bmod 8. \end{cases}$$

Proof. Since $\operatorname{rank} E^{(p)}(\mathbb{Q}) = \dim_{\mathbb{F}_2} E^{(p)}(\mathbb{Q})/2E^{(p)}(\mathbb{Q}) - 2$, the exact sequence for S^2 implies

$$\operatorname{rank} E^{(p)}(\mathbb{Q}) + \dim_{\mathbb{F}_2} Ш(E^{(p)}/\mathbb{Q})[2] = \dim_{\mathbb{F}_2} S^2(E^{(p)}/\mathbb{Q}) - 2.$$

Together with Proposition 2.3 this implies the corollary for the primes $p \equiv 3 \bmod 8$. Since Monsky's result shows that $E^{(p)}/\mathbb{Q}$ has positive rank for $p \equiv 5, 7 \bmod 8$, the corollary also follows in those cases. □

In the remainder of this section let $K = \mathbb{Q}(\sqrt{p})$. Over K the curve $E^{(p)}$ is isomorphic to

$$E \colon y^2 = x^3 - x.$$

Moreover $\operatorname{rank} E(K) = \operatorname{rank} E(\mathbb{Q}) + \operatorname{rank} E^{(p)}(\mathbb{Q})$, corresponding to the decomposition of $E(K) \otimes \mathbb{Q}$ into eigenspaces for $\operatorname{Gal}(K/\mathbb{Q})$. It is well known that $\operatorname{rank} E(\mathbb{Q}) = 0$ (equivalently, 1 is not a congruent number, a fact already stated by Fibonacci in 1225 and a consequence of a result of Fermat; a detailed proof is also presented in [1]). Hence

$$\operatorname{rank} E^{(p)}(\mathbb{Q}) = \operatorname{rank} E(K).$$

In some cases $p \equiv 1 \bmod 8$, the bound $\operatorname{rank} E(K) \leq \dim_{\mathbb{F}_2} S^2(E/K) - 2$ involving the 2-Selmer group of E over $K = \mathbb{Q}(\sqrt{p})$ gives a stronger bound for $\operatorname{rank} E^{(p)}(\mathbb{Q})$ than the one using $S^2(E^{(p)}/\mathbb{Q})$. In such a case it follows that $Ш(E^{(p)}/\mathbb{Q})[2]$ is nontrivial.

PROPOSITION 2.5. *Let $p \equiv 1 \bmod 8$ be prime, and let $j \in \mathbb{Z}$ satisfy $j^2 \equiv -1 \bmod p$. Then* $\dim_{\mathbb{F}_2} S^2(E/\mathbb{Q}(\sqrt{p})) = \begin{cases} 4 & \text{if } \left(\frac{1+j}{p}\right) = 1, \\ 2 & \text{if } \left(\frac{1+j}{p}\right) = -1. \end{cases}$

The next result is for the most part a consequence of Proposition 2.5. In particular it includes the statement already announced in Bastien's 1915 paper [3], on certain primes not being congruent numbers:

COROLLARY 2.6. *Let $p \equiv 1 \bmod 8$ be a prime satisfying the equivalent conditions given in Proposition 2.1. Then rank $E^{(p)}(\mathbb{Q}) = 0$ and $Ш(E^{(p)}/\mathbb{Q})[2] \cong (\mathbb{Z}/2\mathbb{Z})^2$. In particular, p is not a congruent number.*

The set of primes discussed here has natural density 1/8.

Proof. Most of this is immediate from Propositions 2.3 and 2.5 by the argument sketched above. The assertion about the density is obtained by applying Chebotarëv's density theorem (see, e.g. [27]) in the situation of Proposition 2.1(7). □

Proof. (of Proposition 2.5). The elliptic curve E has good reduction away from 2, so we take $S = \{\mathfrak{p}_2, \mathfrak{q}_2, \infty_1, \infty_2\}$, with $\mathfrak{p}_2, \mathfrak{q}_2$ the primes over 2 in $K = \mathbb{Q}(\sqrt{p})$ and ∞_1, ∞_2 the two real embeddings. As with $E^{(p)}/\mathbb{Q}$, set $K(S) = \{x \in K^*/K^{*2} : v(x) \equiv 0 \bmod 2 \text{ for all } v \notin S\}$ and $H = \{(c_1, c_2, c_3) : K(S) \times K(S) \times K(S) : c_1 c_2 c_3 = 1\}$. The Kummer homomorphism $\delta \colon E(K) \to H$ is then given by

$$\delta(a,b) = \begin{cases} (a+1, a, a-1) & \text{for } b \neq 0; \\ (2, -1, -2) & \text{for } a = -1; \\ (1, -1, -1) & \text{for } a = 0; \\ (2, 1, 2) & \text{for } a = 1. \end{cases}$$

Regarding the local images $\delta_v(E(K_v))$, note that the completion K_v equals $\mathbb{Q}_2$ for $v \in \{\mathfrak{p}_2, \mathfrak{q}_2\}$ and $K_v = \mathbb{R}$ for $v \in \{\infty_1, \infty_2\}$. Observe:

- $\delta_v(E(\mathbb{R}))$ is generated by $(1, -1, -1)$ for $v \in \{\infty_1, \infty_2\}$,
- $\delta_v(E(\mathbb{Q}_2))$ has generators $(2, -1, -2)$, $(1, -1, -1)$, $(-3, 1, -3)$ for $v \in \{\mathfrak{p}_2, \mathfrak{q}_2\}$.

The group $K(S)$ fits in an exact sequence

$$0 \to R_S^*/R_S^{*2} \to K(S) \to \mathrm{Cl}(R_S)[2] \to 0,$$

where R_S is the ring of S-integers of K. We have $\mathrm{Cl}(R_S)[2] = 0$ since $\mathrm{Cl}(R_S)$ is a quotient of the class group $\mathrm{Cl}_K = \mathrm{Cl}(\mathcal{O}_K)$ and K has odd class number. Here the standard notation $\mathcal{O}_K$ for the ring of integers of K is used. As R_S^* has rank 3 and torsion subgroup $\{\pm 1\}$ it follows that $K(S)$ has $\mathbb{F}_2$-dimension 4. We now describe a convenient basis of $K(S)$.

Given $c \in K(S)$ and $v \in S$, write $\mathrm{im}_v(c)$ for the image of c under $K(S) \to K_v^*/K_v^{*2}$. Note that a fundamental unit of K has negative norm (the narrow Hilbert class field of K has odd degree). Choose a fundamental unit $\varepsilon \in \mathcal{O}_K^*$ with $\infty_1(\varepsilon) > 0$, so $\infty_2(\varepsilon) < 0$. Since $\varepsilon\overline{\varepsilon} = -1$, $\mathrm{im}_{\mathfrak{p}}(\varepsilon) = \mathrm{im}_{\mathfrak{q}}(\overline{\varepsilon})$ for $\mathfrak{p}$ and $\mathfrak{q}$ conjugate, and $\mathrm{im}_{\mathfrak{p}_2}(\varepsilon) \subset \langle -1, 3\rangle \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$, precisely one of $\mathfrak{p}_2$, $\mathfrak{q}_2$ is unramified in $K(\sqrt{\varepsilon})$. By interchanging the two if necessary we may and will assume that $\mathfrak{p}_2$ is unramified in $K(\sqrt{\varepsilon})$. Equivalently, this means $\mathrm{im}_{\mathfrak{p}_2}(\epsilon) \in \{1, -3\}$, and of course $\mathrm{im}_{\mathfrak{q}_2}(\epsilon) = -\mathrm{im}_{\mathfrak{p}_2}(\epsilon)$. In terms of a Rédei symbol as in [26], in fact $\mathrm{im}_{\mathfrak{p}_2}(\epsilon) = 1 \Leftrightarrow [p, -1, 2] = 1$.
Take k any odd multiple of the order of $[\mathfrak{p}_2] \in \mathrm{Cl}_K$ and write $\mathfrak{p}_2^k = (x_2)$ for some $x_2 \in K$. Multiplying x_2 by $\pm\varepsilon$ if necessary we may assume x_2 has positive norm and that $\mathfrak{q}_2$ is unramified in $K(\sqrt{x_2})$, so $x_2 \cdot \overline{x_2} = 2^k$ and $\mathrm{im}_{\mathfrak{q}_2}(x_2) \in \{1, -3\}$. These choices yield $K(S) = \langle -1, \varepsilon, x_2, y_2\rangle$, with $y_2 = \overline{x_2}$. Moreover $\mathrm{im}_{\infty_m}(x_2) = \mathrm{im}_{\infty_m}(y_2)$ is independent of $m \in \{1, 2\}$ and it equals the Rédei symbol $[p, 2, -1]$. Rédei reciprocity [26, Theorem 1.1] implies in particular $[p, 2, -1] = [p, -1, 2]$, so $\mathrm{im}_{\infty_1}(x_2) = 1 \Leftrightarrow \mathrm{im}_{\mathfrak{p}_2}(\epsilon) = 1$. Again using Rédei reciprocity one has, for $j \in \mathbb{Z}$ such that $j^2 \equiv -1 \bmod p$, the equality $[p, 2, -1] = [2, -1, p] = \left(\frac{1+j}{p}\right)$ (note that this is exactly the example discussed in [26, Section 6]). For c any of these generators and $v \in S$, this means that the following tables give $\mathrm{im}_v(c) \in K_v^*/K_v^{*2}$.

Case $\left(\frac{1+j}{p}\right) = 1$ (with $j \in \mathbb{Z}$ such that $j^2 \equiv -1 \bmod p$):

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	∞_1	∞_2
-1	-1	-1	-1	-1
ε	1	-1	1	-1
x_2	$2a$	a	1	1
y_2	a	$2a$	1	1

Here $a = \mathrm{im}_{\mathfrak{q}_2}(x_2) \in \langle -3\rangle \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$.

To compute $S^2(E/K) = \{c \in H : \iota_v(c) \in \delta_v(E(K_v)) \;\forall\, v \in S\}$ in this situation, write $S^2(E/K) = \delta(E(K)[2]) \oplus A$ with

$$A = \{c \in S^2(E/K) \;:\; \iota_{\mathfrak{p}_2}(c) \in \langle(-3, 1, -3)\rangle\}.$$

Let $c = (c_1, c_2, c_3) \in A$. As c_1 is totally positive it follows that $c_1 \in \langle x_2, y_2\rangle$. Considering both possibilities for $\mathrm{im}_{\mathfrak{p}_2}(x_2)$ one finds that $\mathrm{im}_{\mathfrak{p}_2}(c_1) \subset \langle -3\rangle$ implies $c_1 \in \langle y_2\rangle$. The $\mathfrak{p}_2$-adic and $\mathfrak{q}_2$-adic images of c_2 result in $c_2 \in \langle\varepsilon\rangle$. Hence A consists of at most four elements. One checks that $(y_2, 1, y_2), (1, \varepsilon, \varepsilon) \in A$ regardless of $a = \mathrm{im}_{\mathfrak{q}_2}(x_2) \in \{1, -3\}$. As a consequence $\dim_{\mathbb{F}_2} A = 2$ and therefore $\dim_{\mathbb{F}_2} S^2(E/K) = 4$ in this situation.

The other case is $\left(\frac{1+j}{p}\right) = -1$ (again $j^2 \equiv -1 \bmod p$). Here one has

	$\mathfrak{p}_2$	$\mathfrak{q}_2$	∞_1	∞_2
-1	-1	-1	-1	-1
ε	-3	3	1	-1
x_2	$2a$	a	-1	-1
y_2	a	$2a$	-1	-1

with $a = \mathrm{im}_{\mathfrak{q}_2}(x_2) \in \langle -3\rangle \subset \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$. As before, one uses the decomposition $S^2(E/K) = \delta(E(K)[2]) \oplus A$ in which one takes the subgroup $A = \{c \in S^2(E/K) : \iota_{\mathfrak{p}_2}(c) \in \langle(-3, 1, -3)\rangle\}$.

Let $c = (c_1, c_2, c_3) \in A$. Considering the $\mathfrak{p}_2$-adic image shows that either $c_2 = y_2$ and $a = 1$ which is inconsistent with the possibilities for $\iota_{\mathfrak{q}_2}(c)$, or $c_2 = \varepsilon y_2$ and $a = -3$ (again, inconsistent with $\iota_{\mathfrak{q}_2}(c)$), or $c_2 = 1$. Since c_1 is totally positive, one has $c_1 \in \{1, -x_2, -y_2, x_2y_2\}$. The possibility $c_1 = -x_2$ is excluded by considering the $\mathfrak{p}_2$-image, and in the same way $c_1 = -y_2$ is impossible because of the $\mathfrak{q}_2$-image. Since also $c_1 = x_2y_2$ is not compatible with $c \in A$, it follows that $c_1 = 1$ and therefore $A = (0)$, so $\dim_{\mathbb{F}_2} S^2(E/K) = 2$, completing the proof. □

3. Examples. A remarkable result by J.B. Tunnell [31] (here restricted to odd integers n) states, in a version proposed by N.D. Elkies, that

$$n \text{ is a congruent number}$$
$$\Downarrow$$
$$2x^2 + y^2 + 8z^2 = n \text{ has as many solutions in } \mathbb{Z}^3 \text{ with } 2|z \text{ as with } 2 \nmid z.$$

This gives an easy method for showing that certain integers are *not* congruent numbers. Applying this to the primes $p \equiv 1 \bmod 8$ below some bound b such that p does not satisfy the conditions given in Proposition 2.1 one obtains (we used Magma [4] for this and further calculations) the following table.

b :	2000	4000	6000	8000	10000	12000
$\pi(b)$:	303	550	783	1007	1229	1438
$\#p \equiv 1 \bmod 8$ & $\left(\frac{1+i}{p}\right) = 1$:	30	62	93	116	146	172
$\#p$ not congruent number:	19	41	62	78	99	122

As a consequence of [32, Theorem 1.1] the primes p discussed here (i.e., $p \equiv 1 \bmod 8$ and $\left(\frac{1+i}{p}\right) = 1$ and p is not a congruent number) have the property

$Ш(E^{(p)}/\mathbb{Q})[2^\infty] \supsetneq (\mathbb{Z}/2\mathbb{Z})^2$. In particular this implies that $Ш(E^{(p)}/\mathbb{Q})$ contains a subgroup $(\mathbb{Z}/4\mathbb{Z})^2$. For the 172 primes below 12000 contributing to the table, which form a set that begins and ends as $\{113, 337, 409, \ldots\ldots, 11897, 11969\}$, a simple Magma test confirms this as well:

```
E:=EllipticCurve([-p^2,0]);
MordellWeilShaInformation(E : ShaInfo);
```

The table suggests that at least 1/12-th of the set of all primes has the property described here. We note that this is in agreement with a result of Koymans and Milovic [14, Theorem 5] who show, conditionally on a conjecture regarding short character sums, that

$$\liminf_{b\to\infty} \frac{\#\{p \le b \ :\ (\mathbb{Z}/4\mathbb{Z})^2 \hookrightarrow Ш(E^{(p)}/\mathbb{Q})\}}{\#\{p \le b\}} \ge \frac{1}{16}.$$

If the converse of Tunnell's theorem as well as the observed density holds (as would be a corollary of the Birch and Swinnerton-Dyer conjecture) as well as the observed density $\ge 1/12$ holds, then at most 1/6-th of the set of primes $p \equiv 1 \bmod 8$ consists of congruent numbers. In comparing the result of Koymans and Milovic [14] with our data we use that for $p \not\equiv 1 \bmod 8$ the group $Ш(E^{(p)}/\mathbb{Q})$ contains no nontrivial torsion elements of 2-power order; this follows from Proposition 2.3 together with Monsky's result [16] and it is also observed in [7, Section 6].

Concerning primes $p \equiv 1 \bmod 8$ that *are* congruent numbers, a Magma test yields the following data.

bound b :	2000	4000	6000	8000	10000	12000	14000
$\#p \le b, \equiv 1 \bmod 8$:	68	129	186	243	295	341	400
$\#p$ congruent number :	11	21	31	38	47	50	58

The 58 primes $\{41, 137, 257, \ldots\ldots, 9377, \ldots\ldots, 13513, 13841, 13921\}$ here all result in $\mathrm{rank} E^{(p)}(\mathbb{Q}) = 2$ and hence $Ш(E^{(p)}/\mathbb{Q})[2] = (0)$. Indeed, Magma quickly finds two independent points except in one case: for $p = 9377$ a point of infinite order with $x = -\frac{6635776}{4225}$ is easily found. To obtain a second, independent rational point one needs to increase the `Effort` parameter in `MordellWeilShaInformation`, resulting in the points with

$$x = \frac{9377 \cdot (46111436236957655053256122338300576234143337)^2}{28100967414057580762568605652421621908428616^2}.$$

Not surprisingly, our data is consistent with the list of congruent numbers $n < 10000$ available from [23]. It is conceivable that using e.g. higher descents combined with our idea to do this over $\mathbb{Q}(\sqrt{p})$, a precise density result for primes $p \equiv 1 \bmod 8$ satisfying $(\mathbb{Z}/4\mathbb{Z})^2 \subset Ш(E^{(p)}/\mathbb{Q})$ may be obtained.

In contrast, the question whether or not infinitely many primes $p \equiv 1 \bmod 8$ are congruent numbers seems much harder. We finish this paper by showing that a special case of Bouniakowsky's conjecture implies the existence of infinitely many such primes. Recall that Bouniakowsky's conjecture from 1854 (see [5, p. 328]) states that if $g(x) \in \mathbb{Z}[x]$ is irreducible, has leading coefficient > 0, and the gcd of all values $\{g(m) \ : \ m \in \mathbb{Z}\}$ equals 1, then $g(m)$ is claimed to be a prime number for infinitely many $m \in \mathbb{Z}$. Note that this is a very early special case of Schinzel's Hypothesis H formulated in [20, p. 188].

PROPOSITION 3.1. *The polynomial* $f(x) := 8x^4+16x^3+12x^2+4x+1$ *satisfies the conditions in Bouniakowsky's conjecture, so* $f(\mathbb{Z})$ *is supposed to contain infinitely many prime numbers.*

If $n \in f(\mathbb{Z}) \setminus \{1\}$, *then* $n \equiv 1 \bmod 8$ *and* n *is a congruent number.*

Proof. It is not difficult to verify that $f(x) \in \mathbb{Z}[x]$ is irreducible (in fact, up to a a factor 2 it equals the 8-th cyclotomic polynomial evaluated in $2x+1$). Clearly the leading coefficient is positive, and since $f(0) = 1$ the gcd of the values $f(k)$ equals 1. This shows the first part of the proposition.

For integers k, note that $f(k) \equiv 4(k^2+k)+1 \bmod 8 = 1 \bmod 8$. Also, $2f(k) = (2k+1)^4+1$ which implies $f(k) \geq 1$ whenever $k \in \mathbb{Z}$ and $f(k) = 1 \Leftrightarrow k \in \{-1, 0\}$ (assuming k is real). Hence to complete the proof, take $n = f(k)$ with $k \in \mathbb{Z} \setminus \{-1, 0\}$, so that $n \geq f(1) = 41$ (because $f(x) = f(-x-1)$ and $x \mapsto f(x)$ increases for $x > -\frac{1}{2}$). Then

$$\begin{aligned} a &:= 2n \cdot (2k+1)^2, \\ b &:= 16 \cdot (k^2+k)^2(2k^2+2k+1)^2 = n^2 - (2k+1)^4, \\ c &:= n^2 + (2k+1)^4 \end{aligned}$$

are positive integers satisfying $a^2+b^2 = c^2$, hence they arise as lengths of a right-angled triangle with area n times a square. This implies that n is a congruent number. □

REMARK 3.2. Of the 58 prime numbers $p \equiv 1 \bmod 8$ with $p < 14000$ that are congruent numbers, 4 are in $f(\mathbb{Z})$. Note that $f(\mathbb{Z})$ contains only 5 integers in the interval $[2, 14000]$. A special case of a conjecture of P.T. Bateman and R.A. Horn predicts the number of integers $1 \leq k \leq b$ such that $f(k)$ is prime: it should grow $\sim \frac{C(f)}{4} b/\ln(b)$ with $C(f) = \prod_p \frac{p-\omega(p)}{p-1}$ and $\omega(p) = 4$ for $p \equiv 1 \bmod 8$ while $\omega(p) = 0$ otherwise. An approximation $C(f) \approx 5.358$ one obtains using [21].

Since $f(\frac{u}{v}) = \left((2\frac{u}{v}+1)^4+1\right)/2 = \frac{1}{v^4}\left((2u+v)^4+v^4\right)/2$, the proof of Proposition 3.1 shows that integers represented by the binary form

$$\left((2u+v)^4+v^4\right)/2 = 8u^4+16u^3v+12u^2v^2+4uv^3+v^4$$

(except those coming from $v = 0$, from $u = 0$, and from $u = -v$) are congruent numbers. Such numbers are $\equiv m^4 \bmod 8$, so whenever m is odd they are $\equiv 1 \bmod 8$. Below the bound 14000 this yields 9 prime congruent numbers, namely

41, 313, 353, 1201, 3593, 4481, 7321, 8521, 10601.

Applying [28, Theorem 1] to the binary form given here yields a constant $C > 0$ such that up to any bound B it attains at least $C\sqrt{B}$ square-free values; by construction these are congruent numbers $\equiv 1 \bmod 8$ since for v even, the number would be divisible by 8 hence it would not be square-free. It seems that this is slightly stronger than what would be obtained starting from $(2uv)^2+(u^2-v^2)^2 = (u^2+v^2)^2$, i.e., from the binary form $uv(u+v)(u-v)$.

REFERENCES

1. PETER BARLOW, *An Elementary Investigation of the Theory of Numbers with its Application to the Indeterminate and Diophantine Analysis, the Analytical and Geometrical Division of the Circle, and several other Curious Algebraical and Arithmetical Problems,* The Royal Military Academy, London, 1811.
2. PIERRE BARRUCAND AND HARVEY COHN, Note on primes of type $x^2 + 32y^2$, class number, and residuacity, *J. Reine Angew. Math.* **238** (1969), 67–70.
3. L. BASTIEN, Nombres congruents, *Intermédiaire des Mathématiciens,* **22** (1915), 231–232.
4. WIEB BOSMA, JOHN CANNON, AND CATHERINE PLAYOUST, The Magma algebra system. I. The user language, Computational algebra and number theory (London, 1993), *J. Symbolic Comput.* **24**(3–4) (1997), 235–265.
5. V. BOUNIAKOWSKY, Sur les diviseurs numériques invariables des fonctions rationnelles entières. (Lu le 4 août 1854), *Mém. Acad. Impériale Sci. de Saint-Pétersbourg, 6-ème série. Sciences math. phys.* **VI** (1857), 305–329.
6. EZRA BROWN, The class number of $\mathbb{Q}(\sqrt{-p})$, for $p \equiv 1 (\bmod 8)$ a prime, *Proc. Amer. Math. Soc.* **31** (1972), 381–383.
7. NILS BRUIN AND BRETT HEMENWAY, On congruent primes and class numbers of imaginary quadratic fields, *Acta Arith.* **159**(1) (2013), 63–87.
8. L.E. DICKSON,, *History of the theory of numbers. Vol. II: Diophantine analysis,* Carnegie Institution, Washington, 1920.
9. TIM EVINK, GERT-JAN VAN DER HEIDEN, AND JAAP TOP, Two-descent on some genus two curves, *Indag. Math. (N.S.)* **32**(4) (2021), 883–900. https://doi.org/10.1016/j.indag.2021.06.004
10. ANGELO GENOCCHI, Sopra tre scritti inediti di Leonardo Pisano pubblicati da B. Boncompagni: Note Analitiche, *Annali di Scienze Matematiche e Fisiche* **6** (1855), 161–185, 218–250, 273–320, 345–362.
11. BRETT HEMENWAY, *On recognizing congruent primes,* Simon Fraser University, Burnaby, 2006. http://summit.sfu.ca/item/6418
12. PIERRE KAPLAN, Divisibilité par 8 du nombre des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et réciprocité biquadratique, *J. Math. Soc. Japan* **25** (1973), 596–608.
13. NEAL KOBLITZ, *Introduction to elliptic curves and modular forms,* Graduate Texts in Mathematics, Second edition, Vol. 97, Springer-Verlag, New York, 1993.
14. P. KOYMANS AND D.Z. MILOVIC, Spins of prime ideals and the negative Pell equation $x^2 - 2py^2 = -1$, *Compos. Math.*, **155**(1) (2019), 100–125.
15. DELANG LI AND YE TIAN, On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D\colon y^2 = x^3 - D^2x$, *Acta Math. Sin. (Engl. Ser.)* **16**(2) (2000), 229–236.

16. PAUL MONSKY, Mock Heegner points and congruent numbers, *Math. Z.* **204**(1) (1990), 45–67.

17. TRYGVE NAGELL, *L'Analyse indéterminée de degré supérieur*, Vol. 39, Gauthier-Villars, Paris, 1929.

18. YI OUYANG AND SHENXING ZHANG, On second 2-descent and non-congruent numbers, *Acta Arith.*, **170**(4) (2015), 343–360.

19. MICHAEL J. RAZAR, A relation between the two-component of the Tate-Šafarevič group and $L(1)$ for certain elliptic curves, *Amer. J. Math.* **96**, (1974), 127–144.

20. A. SCHINZEL AND W. SIERPIŃSKI, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208; erratum 5 (1958), 259.

21. DANIEL SHANKS, On numbers of the form n^4+1, *Math. Comput.* **15** (1961), 186–189.

22. JOSEPH H. SILVERMAN, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, Second edition, Vol. 106, Springer, Berlin, 2009.

23. N.J.A. SLOANE AND SIMON PLOUFFE, *The encyclopedia of integer sequences*, Academic Press, Inc., San Diego, CA, 1995. https://oeis.org/A006991/b006991.txt

24. N.M. STEPHENS, Congruence properties of congruent numbers, *Bull. London Math. Soc.* **7** (1975), 182–184.

25. PETER STEVENHAGEN, Divisibility by 2-powers of certain quadratic class numbers, *J. Number Theory* **43**(1) (1993), 1–19.

26. ———, Redei reciprocity, governing fields, and negative Pell, *Math. Proc. Cambridge Philos. Soc.* (2021), 1–28. https://doi.org/10.1017/S0305004121000335

27. P. STEVENHAGEN AND H.W. LENSTRA, JR., Chebotarëv and his density theorem, *Math. Intelligencer* **18**(2) (1996), 26–37.

28. C.L. STEWART AND J. TOP, On ranks of twists of elliptic curves and power-free values of binary forms, *J. Amer. Math. Soc.* **8**(4) (1995), 943–973.

29. ROEL J. STROEKER AND JAAP TOP, On the equation $Y^2 = (X+p)(X^2+p^2)$, *Rocky Mountain J. Math.* **24**(3) (1994), 1135–1161.

30. JAAP TOP AND NORIKO YUI, *Congruent number problems and their variants*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., Vol. 44, pp. 613–639, Cambridge Univ. Press, Cambridge, 2008.

31. J.B. TUNNELL, A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.* **72**(2) (1983), 323–334.

32. ZHANGJIE WANG, Congruent elliptic curves with non-trivial Shafarevich-Tate groups, *Sci. China Math.* **59**(11) (2016), 2145–2166.

Received 11 May, 2021 and in revised form 23 August, 2021.