LMS J. Comput. Math. 17 (1) (2014) 58–76
doi:10.1112/S1461157013000259

On a conjecture of Rudin on squares in arithmetic progressions

Enrique González-Jiménez and Xavier Xarles

Abstract

Let $Q(N;q,a)$ be the number of squares in the arithmetic progression $qn+a$, for $n=0,1,\dots,N-1$, and let $Q(N)$ be the maximum of $Q(N;q,a)$ over all non-trivial arithmetic progressions $qn+a$. Rudin's conjecture claims that $Q(N)=O(\sqrt{N})$, and in its stronger form that $Q(N)=Q(N;24,1)$ if $N\geqslant 6$. We prove the conjecture above for $6\leqslant N\leqslant 52$. We even prove that the arithmetic progression $24n+1$ is the only one, up to equivalence, that contains $Q(N)$ squares for the values of N such that $Q(N)$ increases, for $7\leqslant N\leqslant 52$ ($N=8,13,16,23,27,36,41$ and 52).

Supplementary materials are available with this article.

1. *Introduction*

A well-known result by Fermat states that no four squares in arithmetic progression over $\mathbb{Z}$ exist. This result may be reformulated in the following form: in four consecutive terms of a non-constant arithmetic progression, there are at most three squares. Hence, it is natural to ask how many squares there may be in N consecutive terms of a non-constant arithmetic progression.

Following Bombieri, Granville and Pintz [2], given integers q and a, $q\neq 0$, we denote by $Q(N;q,a)$ the number of squares in the arithmetic progression $qn+a$, for $n=0,1,\dots,N-1$ (there is a slight difference between our notation and the one in [2], since our arithmetic progressions begin with $n=0$ instead of $n=1$). Denote by $Q(N)$ the maximum of $Q(N;q,a)$ over all non-trivial arithmetic progressions. Notice that Fermat's result is equivalent to $Q(4)=3$.

As a consequence of Fermat's result, Szemerédi [27] proved, using one of his well-known results on arithmetic progressions, an old conjecture by Erdős [14]: $Q(N)=o(N)$. This bound was improved by Bombieri, Granville and Pintz [2] to $Q(N)=O(N^{2/3+o(1)})$, and by Bombieri and Zannier [3] to $Q(N)=O(N^{3/5+o(1)})$. The so–called Rudin's conjecture ([23, end of § 4.6]) claims that $Q(N)=O(\sqrt{N})$, and in its stronger form (which we call Strong Rudin's conjecture) that:

$$Q(N)=Q(N;24,1)=\sqrt{\tfrac{8}{3}N}+O(1)\quad\text{if } N\geqslant 6.$$

Notice that $Q(5;24,1)=3$, but $Q(5;120,49)=4$ (since $7^2=49, 13^2=169, 17^2=289, 409$, $23^2=529$). (It has been proved in [18] that the first quadratic number field where there are five squares in arithmetic progression is $\mathbb{Q}(\sqrt{409})$; and that the unique non-constant arithmetic progressions of five squares over $\mathbb{Q}(\sqrt{409})$, up to equivalence, is $7^2, 13^2, 17^2, 409, 23^2$.) Therefore $Q(5)=4$, because $Q(5)$ cannot be 5 by Fermat's result.

We will prove that the arithmetic progression $24n+1$ is the only one, up to equivalence, that contains $Q(N)$ squares for the values of N such that $Q(N)$ increases in the interval $7\leqslant N\leqslant 52$ ($N=8,13,16,23,27,36,41$ and 52). This result suggests a Super-Strong Rudin's conjecture: let $\mathcal{GP}_k$ be the kth generalized pentagonal number and assume $a,q\in\mathbb{Z}$, with

Received 30 December 2012; revised 22 July 2013.

2010 Mathematics Subject Classification 11G30, 11B25, 11D45 (primary), 14H25 (secondary).

$\gcd(q,a)$ squarefree and $q>0$; if $N=\mathcal{GP}_k+1\geqslant 8$ for some integer k, then $Q(N)=Q(N;q,a)$ if and only if $(q,a)=(24,1)$.

The following theorem summarizes the main results of this article.

THEOREM 1. *Let N be a positive integer; then:*

(S) *$Q(N)=Q(N;24,1)$ if $6\leqslant N\leqslant 52$;*

(SS) *if $8\leqslant N=\mathcal{GP}_k+1\leqslant 52$ for some integer k, then $Q(N)=Q(N;q,a)$ with $\gcd(q,a)$ squarefree and $q\geqslant 0$ if and only if $(q,a)=(24,1)$.*

1.1. *Notation*

Given any finite subset $I=\{n_0,\dots,n_k\}\subset\mathbb{Z}$, we will always list its elements in increasing order. We denote by $\mathcal{Z}_I$ the set

$$\{(q,a)\in\mathbb{Z}^2 \mid \gcd(q,a) \text{ squarefree}, q\neq 0 \text{ and } qi+a \text{ is a square } \forall i\in I\},$$

and by $z_I=\#\mathcal{Z}_I$ its cardinality.

Given q and a integers, $q\neq 0$, we denote by $\mathcal{S}(q,a)$ the set $\{i\in\mathbb{N} \mid qi+a \text{ is a square}\}$ and, given $N\geqslant 2$, we denote by $\mathcal{S}_N(q,a)$ the set $\mathcal{S}(q,a)\bigcap\{0,1,\dots,N-1\}$. We have:

(i) $\mathcal{S}(24,1)=\{\mathcal{GP}_k\}_{k\in\mathbb{Z}}$ the progression of generalized pentagonal numbers ($\mathcal{GP}_k=k(3k-1)/2$ is the sequence A001318 in [24]);

(ii) $\mathcal{S}(8,1)=\{\mathcal{T}_k\}_{k\in\mathbb{N}}$ the progression of triangular numbers ($\mathcal{T}_k=k(k+1)/2$ is the sequence A000217 in [24]).

We define the following two operations on finite subsets $I\subset\mathbb{Z}$: for any $i\in\mathbb{Z}$, the translated subset $I+i=\{j\in\mathbb{N} \mid j-i\in I\}$; and, for any $r\in\mathbb{Q}^*$ such that $ri\in\mathbb{Z}$ for all $i\in I$, the expanded subset $rI=\{ri \mid i\in I\}$. Denote also by I^s, the symmetric of I, as $I^s=-I+(n_0+n_k)$. We say I is symmetric if $I^s=I$.

We say that two finite subsets I and J of $\mathbb{Z}$ are equivalent, denoted $I\sim J$, if there exists $I=I_0,I_1,\dots,I_k=J$ finite subsets of $\mathbb{Z}$ such that either there exists $j\in\mathbb{Z}$ such that $I_{i+1}=I_i+j$ or there exists $r\in\mathbb{Q}^*$ such that $I_{i+1}=rI_i$, for all $i=1,\dots,k-1$. This is clearly an equivalence relation.

Given a finite subset I of $\mathbb{N}$, we will denote by n_I the positive integer $\sum_{i\in I}2^i$. We have a bijection between the set of finite subsets of $\mathbb{N}$ and $\mathbb{N}$ (the empty set corresponding to 0).

We say that a finite subset I of $\mathbb{N}$ is primitive if $0\in I$, the elements of I are coprime and $n_I\leqslant n_{I^s}$. Notice that any finite subset of $\mathbb{Z}$ is equivalent to a unique primitive one.

2. *Preliminary results and elementary cases*

Let $I=\{n_0,n_1,\dots,n_k\}\subset\mathbb{Z}$ be a finite subset such that $k>1$ and let K be a field. We denote by C_I the curve in $\mathbb{P}^k(K)$ defined by the system of equations

$$C_I:\{(n_{i+2}-n_{i+1})X_{i-1}^2-(n_{i+2}-n_i)X_i^2+(n_{i+1}-n_i)X_{i+1}^2=0\}_{i=1,\dots,k-1}.$$

If the characteristic of the field K is not 2, the curve C_I contains 2^k trivial points $\mathcal{T}_I$ corresponding to the values $X_i^2=1$ for all $i=0,\dots,k$.

The following proposition collects some known and useful facts about the curves C_I that will be used in the following. For a proof see [2].

PROPOSITION 2. *Let $I=\{n_0,n_1,\dots,n_k\}\subset\mathbb{Z}$ be a finite subset such that $k>1$ and let C_I be the associated curve. Then:*

(1) *if K is a field with characteristic 0, then the curve C_I is a non-singular projective curve of genus $g_k=(k-3)2^{k-2}+1$;*

(2) *if $k > 2$, then for any $i \in I$, the natural map $C_I \to C_{I\setminus\{i\}}$ is of degree 2 and it is ramified on the 2^{k-1} points with $X_i = 0$;*
(3) *if J is another finite set with $I \sim J$, then $C_I \cong C_J$, with the isomorphism being the identity or the natural involution in $\mathbb{P}^k$ given by*

$$[x_0 : \ldots : x_k] \mapsto [x_k : \ldots : x_0];$$

(4) *consider the map $\iota : C_I \to \mathbb{P}^k$ defined by $\iota([x_0 : \ldots : x_k]) = [x_0^2 : \ldots : x_k^2]$; there is a natural bijection between $\iota(C_I(\mathbb{Q}) \setminus \mathcal{T}_I)$ and $\mathcal{Z}_I$.*

Thus, in order to compute the set $\mathcal{Z}_I$ we are reduced to computing the set of rational points of the curve C_I.

Observe that, if $I \subset \mathbb{N}$ only has three elements, the corresponding curve C_I is a genus 0 curve. Since it has some rational point, $C_I(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Q})$ and hence $z_I = \infty$.

Now we are going to compute $Q(N)$ for the first values of N by considering the subsets $I \subset \mathbb{N}$ of cardinality 4. In this case the curves C_I have genus 1, and they are isomorphic to an elliptic curve, since they always have some rational points (for example, the points in $\mathcal{T}_I$).

PROPOSITION 3. *Given any subset I of $\{0, 1, \ldots, 6\}$ with four elements, we have that $z_I = \infty$ unless I is equivalent to one of the following five subsets, in which case $z_I = 0$:*

$$\{0,1,2,3\},\ \{0,1,3,4\},\ \{0,1,4,5\},\ \{0,2,3,5\} \quad \textit{and} \quad \{0,1,5,6\}.$$

Proof. To prove that $z_I = 0$ for the given finite sets I in the proposition, one only needs to show that $C_I(\mathbb{Q}) = \mathcal{T}_I$. Or, equivalently, that $\#C_I(\mathbb{Q}) = 8$. Using standard transformations (see Section 3), one may put the corresponding elliptic curves in Weierstrass form, and then compute the Antwerp–Cremona reference [**1**, **13**]. We obtain the elliptic curves `24a1`, `48a3`, `15a3`, `120a2` and `240a3` respectively. All of them have rank 0 and torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Hence $\#C_I(\mathbb{Q}) = 8$ in these cases. For all the other cases, one easily shows that the rank of the corresponding elliptic curve C_I is 1. Therefore, they have an infinite number of points. □

Observe that all the subsets in the proposition with $z_I = 0$ are symmetric subsets. We will see that this is true for any subset with four elements.

COROLLARY 4. *We have $Q(6) = Q(7) = 4$ and $Q(8) = 5$.*

Proof. First of all, we clearly have that $4 = Q(5) \leqslant Q(6) \leqslant 5$. Suppose we have a primitive subset I of 5 elements inside $\{0, 1, 2, 3, 4, 5\}$ such that $z_I > 0$. If I does not contain 5 then $I \setminus \{5\} = \{0, 1, 2, 3, 4\}$, which contains $J = \{0, 1, 2, 3\}$. Since $z_J = 0$ by Proposition 3, $z_I = 0$. So we should have $I = \{0, 1, 2, 3, 4, 5\} \setminus \{i\}$ for $0 < i < 5$, and we have four cases.

If $i = 1$ or $i = 4$, then I contains $\{2, 3, 4, 5\} \sim \{0, 1, 2, 3\}$ or $\{0, 1, 2, 3\}$ respectively, so we are done. If $i = 2$ or $i = 3$, then I contains $\{0, 1, 3, 4\}$ or $\{1, 2, 4, 5\} \sim \{0, 1, 3, 4\}$, and hence, by applying another case of Proposition 3, we conclude.

Now, we are going to prove that $Q(7) = 4$. We proceed with the same strategy. We consider I a primitive subset of $\{0, \ldots, 6\}$ with five elements and we can deduce that $z_I = 0$ if we find a subset J of I with four elements appearing in the list of Proposition 3, hence with $z_J = 0$. We may suppose that $I = \{0, i, j, k, 6\}$ for some $0 < i < j < k < 6$. We have ten cases, but only six cases to consider up to symmetry. The first case $\{0, 1, 2, 3, 6\}$ is Fermat's; the second case $\{0, 1, 2, 4, 6\}$ contains $\{0, 2, 4, 6\} \sim \{0, 1, 2, 3\}$, hence is sorted out again by Fermat's result; $\{0, 1, 2, 5, 6\}$ contains $\{0, 1, 5, 6\}$, $\{0, 1, 3, 4, 6\}$ contains $\{0, 1, 3, 4\}$, $\{0, 1, 3, 5, 6\}$ contains $\{0, 1, 5, 6\}$ and the last subset $\{0, 2, 3, 4, 6\}$ contains $\{0, 2, 4, 6\} \sim \{0, 1, 2, 3\}$.

Now, since $Q(8) \leqslant Q(7)+1 = 5$, to prove $Q(8) = 5$ we only need to exhibit an arithmetic progression with five squares in the first eight terms, and the arithmetic progression $1+24n$ does the job. Note that $\mathcal{S}_8(24,1) = \{0,1,2,5,7\}$. □

So, the first strategy to detect subsets I with cardinality larger than 3 and $z_I = 0$ is to find a subset J of I with four elements such that $z_J = 0$. This can be done by considering the associated elliptic curve E_J and by showing that it only contains the (eight) trivial points $\mathcal{T}_J$. In the next section we will study some necessary conditions for this to happen.

3. *Four squares in arithmetic progressions*

Consider $I = \{n_0, n_1, n_2, n_3\} \subset \mathbb{Z}$, with $n_0 < n_1 < n_2 < n_3$, and let C_I be the corresponding elliptic curve. Let us denote

$$m_0 = \frac{n_1 - n_0}{n_2 - n_1} \quad \text{and} \quad m_1 = \frac{n_3 - n_2}{n_2 - n_1}.$$

Note that they are both strictly positive rational numbers and that the set I is symmetric if and only if $m_0 = m_1$. Dividing by $n_2 - n_1$, the equations of C_I become

$$C_I \ : \ \begin{cases} X_0^2 - (m_0+1)X_1^2 + m_0 X_2^2 = 0, \\ m_1 X_1^2 - (m_1+1)X_2^2 + X_3^2 = 0. \end{cases}$$

We are going to find the Weierstrass equation for these elliptic curves. First, we parametrize the first equation by

$$[X_0 : X_1 : X_2] = [(m_0+1) - 2(m_0+1)t + t^2 \ : \ (m_0+1) - 2t + t^2 \ : \ (m_0+1) - t^2],$$

where $t = (X_2 - X_0)/(X_2 + X_1)$. Next, we substitute X_0, X_1, X_2 in the second equation and we obtain a quartic equation of the curve, depending on a parameter t:

$$C_I : X_3^2 = t^4 + 4m_1 t^3 - 2(m_0 + 4m_1 + 2m_1 m_0 + 1)t^2 + 4m_1(m_0+1)t + (m_0+1)^2.$$

A Weierstrass form of C_I is given by

$$E_I \ : \ y^2 = x(x - m_0 m_1)(x + m_0 + m_1 + 1).$$

Denote by $\phi : C_I \longrightarrow E_I$ the $\mathbb{Q}$-isomorphism that gives this Weierstrass form. Then, if we denote $\phi(\mathcal{T}_I)$ by $\mathcal{F}_I$, we have $\#\mathcal{F}_I = 8$, where the set $\mathcal{F}_I$ is described by Table 1.

LEMMA 5. *The set $\mathcal{F}_I$ is a subgroup of E_I if and only if I is symmetric. Furthermore, if I is not symmetric, then $z_I > 0$.*

Proof. First, observe that the opposites of the non-Weierstrass points on $\mathcal{F}_I$ do not belong to $\mathcal{F}_I$ unless $m_0 = m_1$. Since m_0 and m_1 are strictly positive numbers, $-Q_5 = (-m_0, -m_0(m_1+1)) \in \mathcal{F}_I$ if and only if it is equal to Q_4. This shows one implication. For the other

TABLE 1. $\mathcal{F}_I = \phi(\mathcal{T}_I) = \phi([\pm 1 : \pm 1 : \pm 1 : \pm 1])$.

i	P_i	$Q_i = \phi(P_i)$
0	$[1:1:1:1]$	$\mathcal{O} = [0:1:0]$
1	$[-1:1:-1:1]$	$(0,0)$
2	$[-1:1:1:-1]$	$(m_0 m_1, 0)$
3	$[-1:-1:1:1]$	$(-m_0 - m_1 - 1, 0)$
4	$[1:1:-1:1]$	$(-m_1, -m_1(m_0+1))$
5	$[1:-1:1:1]$	$(-m_0, m_0(m_1+1))$
6	$[-1:1:1:1]$	$(m_0(m_0+m_1+1), -m_0(m_0+1)(m_0+m_1+1))$
7	$[1:1:1:-1]$	$(m_1(m_0+m_1+1), m_1(m_1+1)(m_0+m_1+1))$

one, suppose that $m_0 = m_1$. Then one easily checks that the non-Weierstrass points have order 4, and their doubles are equal to the point $(m_0 m_1, 0)$. That is, $\mathcal{F}_I \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. □

REMARK 6. One may use the isomorphism ϕ in order to find explicitly which arithmetic progressions correspond to the points $-P_4, -P_5, -P_6, -P_7$. Suppose I is primitive, in particular $n_0 = 0$, so it is of the form $\{0, n_1, n_2, n_3\}$, with n_1, n_2 and n_3 coprime. Then the arithmetic progression $a + nq$ given by

$$\begin{cases} a = ((n_1 + n_2 - n_3)^2 - 4n_1 n_2)^2, \\ q = 2^3(n_1 + n_2 - n_3)(n_1 - n_2 - n_3)(n_1 - n_2 + n_3) \end{cases}$$

has squares for $n = 0, n_1, n_2, n_3$. Using this construction, we show in Table 2 the arithmetic progression (q, a) for all the equivalence classes of 4-tuples $I \subset \{0, \dots, N-1\}$, for $5 \leqslant N \leqslant 7$, such that $C_I(\mathbb{Q}) \neq \mathcal{T}_I$. Note that in all of these cases $\operatorname{rank} E_I(\mathbb{Q}) = 1$.

REMARK 7. If I is not symmetric, the subgroup generated by $\mathcal{F}_I$ is infinite, unless $m_1^2+m_1+1$ is a square and $m_0 = -(m_1 + 2 - 2\sqrt{m_1^2 + m_1 + 1})/3$ (or if $m_1^2 + m_1$ is a square and $m_0 = m_1 + 2\sqrt{m_1^2 + m_1}$, which becomes the other case after one interchanges m_0 and m_1). In this case the curve E_I is $\mathbb{Q}$-isomorphic to the curve

$$E_t : y^2 = x(x + 1 + 4t)(x + 16t^3(t + 1)), \quad \text{for some } t \in \mathbb{Q},$$

and

$$\langle P : P \in \mathcal{F}_I \rangle = \mathcal{F}_I \cup \{-P_4, -P_5, -P_6, -P_7\} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Furthermore, the points $-P_4, -P_5, -P_6, -P_7$ correspond to the arithmetic progression with $a = 0$ and $q = 1$. Thus, if we suppose that I is primitive then there exist $s_1, s_2 \in \mathbb{Z}$ such that $n_1 = s_1^2$, $n_2 = s_2^2$ and $n_3 = (s_1 \pm s_2)^2$.

We have seen that if $I \subset \mathbb{Z}$ has four elements, a necessary condition for z_I to be 0 is I being symmetric. In the following, we obtain more necessary conditions, some of them under the Parity Conjecture.

Observe that the number of symmetric subsets with four elements contained in $\{0, 1, \dots, N\}$ may be explicitly computed in terms of N (and it is the sequence A002623 in [24], with $n = N - 3$), and it is almost equal to a polynomial of degree 3 in N:

$$\frac{N^3}{12} - \frac{7N^2}{8} + \frac{35N}{12} - \frac{49}{16} + \frac{(-1)^N}{16}.$$

Since the number of subsets with four elements is a polynomial of degree 4 in N, there are $2/N + O(N^{-2})$ symmetric subsets among all the subsets with four elements. We do not know

TABLE 2. *The arithmetic progression (q, a) for all the equivalence classes of 4-tuples $I \subset \{0, \dots, N-1\}$, for $5 \leqslant N \leqslant 7$, such that $C_I(\mathbb{Q}) \neq \mathcal{T}_I$.*

N	I	An arithmetic progression (q, a) such that $I \subset \mathcal{S}(q, a)$
5	$\{0, 1, 2, 4\}$	$(120, 49)$
6	$\{0, 1, 2, 5\}$	$(24, 1)$
	$\{0, 1, 3, 5\}$	$(168, 121)$
7	$\{0, 1, 2, 6\}$	$(840, 1)$
	$\{0, 1, 3, 6\}$	$(8, 1)$
	$\{0, 2, 3, 6\}$	$(280, 529)$
	$\{0, 1, 4, 6\}$	$(24, 25)$

how many of the equivalence classes of subsets with four elements are symmetric, but we suspect it is of the same order.

Suppose now I is primitive and symmetric, that is $I = \{0, n_1, n_2, n_1 + n_2\}$ with $0 < n_1 < n_2$ coprime integers. Then we have a $\mathbb{Q}$-isomorphism $\psi : C_I \longrightarrow E'_t$ where

$$E'_t \,:\, y^2 = x(x+1)(x+t^2) \quad \text{and} \quad t = n_2/n_1$$

such that $\psi(\mathcal{T}_I) = \{\mathcal{O}, (0,0), (-1,0), (-t^2,0), (\pm t, \pm t(t+1))\}$.

A first remark is that there are plenty of symmetric subsets I with four elements with $z_I > 0$, and even with an infinite number of elements. For example, in the case that the torsion subgroup has more than eight elements, which, by Mazur's theorem, only occurs if the torsion subgroup of $E_t(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, or, equivalently, some of the four 4-torsion points given by the points with x-coordinate equal to $\pm t$ are the double of some rational point. We use the standard formulae (or a 2-descent argument) to obtain that this happens if and only if the x-coordinate and the x-coordinate $+1$ are both squares.

Lemma 8. *Let t be a positive rational number; then*

$$E'_t(\mathbb{Q})_{\text{tors}} \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} & \text{if } t = \left(s - \dfrac{1}{4s}\right)^2, \text{ for some } s \in \mathbb{Q}, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \text{otherwise.} \end{cases}$$

In fact, we may exactly characterize which primitive sets have their corresponding elliptic curve with torsion subgroup of order 16, and even which arithmetic progressions correspond to these new torsion points.

Corollary 9. *Let $I = \{0, n_1, n_2, n_1 + n_2\}$ be a primitive symmetric subset of $\mathbb{N}$. Then the elliptic curve E_I has torsion isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ if and only if n_1, n_2 and $n_1 + n_2$ are squares. The torsion points of E_I correspond to the constant arithmetic progression along with the arithmetic progressions with $a = 0$ and $q = 1$ and with $a = n_1 + n_2$ and $q = -1$.*

Proof. Since $t = n_2/n_1$ is a square, both n_1 and n_2 are squares. Since $t + 1 = (n_1 + n_2)/n_1$ is also a square, $n_3 = n_1 + n_2$ is also a square. Trivially, the arithmetic progression with $(a, q) = (0, 1)$ verifies that $a_{n_i} = a + n_i q = n_i$ are squares, and the one with $(a, q) = (n_1 + n_2, -1)$ verifies that $a_{n_i} = a + n_i q = n_{3-i}$ are also squares, and they correspond to the torsion points of order 8. □

If one wants an infinite number of points in the general symmetric case, there is a two–parametric subfamily of E'_t, with other rational points aside from the trivial ones, which give generically rank 1 elliptic curves.

Example 10. Let z_1 and z_2 be non-zero rational numbers, and consider

$$t = \frac{1}{4}\left(z_1 + \frac{1}{z_1} + z_2 + \frac{1}{z_2}\right) \quad \text{and} \quad x = \frac{-(z_1 + z_2)^2}{4 z_1 z_2}.$$

Then $x(x+1)(x+t^2)$ is a square. Moreover, if $z_1, z_2 \neq \pm 1$, $z_1 \neq \pm z_2$ and $z_1 \neq 1/z_2$, then we obtain a non-trivial point in E'_t.

Now we are going to give a conjectural criterion to be sure that the curve E'_t has odd rank. Recall that the Parity Conjecture claims that any elliptic curve E defined over $\mathbb{Q}$ (or a general number field) has root number $W(E) = -1$ if and only if its group of rational points has odd rank (and, in particular, E has infinitely many rational points). Notice that $W(E)$ is easily computable, even in a family. In our case we have an explicit description.

PROPOSITION 11. *Let $0 < a < b$ be coprime integers, and let $E_{a,b}$ be the elliptic curve defined by*

$$E_{a,b} : y^2 = x(x+a^2)(x+b^2).$$

Then $W(E) = -1$ if and only if $\alpha(a,b) \equiv \mu_2(a,b) \pmod 2$, where

$$\begin{aligned}\alpha(a,b) = &\#\{p \text{ odd prime} \mid p \text{ divides } ab\}\\ &+\#\{p \text{ prime} \mid p \text{ divides } (b^2-a^2) \text{ and } p \equiv 1 \pmod 4\},\end{aligned}$$

$$\mu_2(a,b) = \begin{cases} 0 & \text{if } ab \equiv 4 \pmod 8, \text{ or if } \left[ab \equiv 1 \pmod 2 \text{ and } \dfrac{(b^2-a^2)}{8} \equiv 1 \pmod 2\right],\\ 1 & \text{otherwise.}\end{cases}$$

Proof. Recall that the root number $W(E)$ of an elliptic curve E over $\mathbb{Q}$ is equal to the product of local root numbers $W_p(E)$, where p runs over all the prime numbers and infinity. One always has $W_\infty(E) = -1$, $W_p(E) = 1$ if the curve has good or non-split multiplicative reduction at p, and $W_p(E) = -1$ if the curve has split multiplicative reduction at p. Since a and b are coprime integers, $E_{a,b}$ is minimal at any odd prime. The reduction is good if p does not divide $ab(b^2-a^2)$, and it is split multiplicative if p divides ab, or if p divides b^2-a^2 and -1 is a square modulo p. Hence we obtain $W(E) = (-1)^\beta W_2(E)$, where $\beta = \alpha(a,b)+1$.

Now, to compute $W_2(E)$, we need to carry out a more detailed analysis, since the reduction can be additive in this case. First, one shows by a change of variables that the curve $E_{a,b}$ is isomorphic to the curve given by the equation $y^2+xy+ry = x^3+rx^2$ (this is the so–called Tate normal form), where $r = ab/4(a+b)^2$. Given $s \in \mathbb{Q}$, we denote by $v_2(s)$ the 2-adic valuation of s. The curve has good reduction at 2 (hence $W_2(E) = 1$) if and only if $v_2(r) = 0$, so if $v_2(a) = 2$ or $v_2(b) = 2$. It has split multiplicative reduction (hence $W_2(E) = -1$) if $v_2(r) > 0$, that is, if $v_2(a) > 2$ or $v_2(b) > 2$, and it has additive reduction otherwise.

When the valuation of r is negative, we will consider the original equation of the curve $E_{a,b}$, which is an integral model. We will need the following standard invariants and coinvariants of the Weierstrass equation:

$$j = j(E_{a,b}) = \frac{2^8(a^4+b^4-a^2b^2)^3}{a^4b^4(a+b)^2(a-b)^2}, \quad c_4 = 2^4(a^4+b^4-a^2b^2),$$
$$\Delta = 2^4a^4b^4(a+b)^2(a-b)^2, \quad c_6 = 2^5(a^2+b^2)(2b^2-a^2)(2a^2-b^2).$$

Now, if $v_2(r) = -1$, then $v_2(a) = 1$ or $v(b) = 1$. Therefore the curve has potentially good reduction (since $v_2(j) = 4$), and we can look at the tables in [19]. We obtain $v_2(\Delta) = 8$, $v_2(c_4) = 4$ and $v_2(c_6) = 6$, hence this information is not enough to obtain the sign. We consider $c_6' = c_6/2^6$ and $c_4' = c_4/2^4$, and we compute $2c_6' + c_4' \pmod{16}$. After a case by case computation one obtains that $2c_6' + c_4' \equiv 7 \pmod{16}$, so we are in the case I_1^*. Next, one computes that $2c_6' + c_4' \equiv 23 \neq 7 \pmod{32}$, so $W_2(E) = -1$.

Now, if $v_2(a) = v_2(b) = 0$, we need to take into account the valuations $v_2(a+b)$ and $v_2(a-b)$. First we need to determine when the curve $E_{a,b}$ has potentially multiplicative reduction in order to apply the formulae by Rohrlich [22]. This is equivalent to the case $v_2(j) < 0$. Since in our case $v_2(j) = 8 - 2v_2(a-b) - 2v_2(a+b)$, we have potentially multiplicative reduction if and only if $v_2(a-b) + v_2(a+b) \geqslant 4$. In this case, $W_2(E)$ is computed as follows: if $s \in \mathbb{Q}$, we denote $s2^{-v_2(s)}$ by $\overline{s}$. Then, we obtain that $W_2(E) \equiv -\overline{c_6} \pmod 4$. But observe that

$$\overline{c_6} = \overline{(a^2+b^2)}(2b^2-a^2)(2a^2-b^2) \equiv \overline{(a^2+b^2)} \equiv 1 \pmod 4,$$

hence $W_2(E) = -1$ in this case.

Finally, we need to consider the potentially good reduction case, with $v_2(a) = v_2(b) = 0$. In this case, we have $v_2(a-b) + v_2(a+b) = 3$. Therefore, we obtain that $v_2(\Delta) = 10$, $v_2(c_4) = 4$

and $v_2(c_6) = 6$. One easily shows that the necessary condition $\overline{c_6} \equiv 1 \pmod 4$ for the case I_2^* in the tables of [19] is always satisfied, so we obtain that $W_2(E)$ is 1 in this case.

Therefore we obtain $W_2(E) = 1$ if and only if $v_2(ab) = 0$ and $v_2(a^2 - b^2) = 3$, or $v_2(ab) = 2$. □

COROLLARY 12. *Let $0 < n_1 < n_2$ be coprime integers and $I = \{0, n_1, n_2, n_1 + n_2\}$. Assume that the Parity Conjecture holds for the curve E_{n_1,n_2}, and that $\alpha(n_1, n_2) \equiv \mu_2(n_1, n_2) \pmod 2$. Then $z_I = \infty$.*

REMARK 13. Cohn [10] studied the special symmetric case $\{0, 2, n, n+2\}$ when $n \leqslant 100$. The corollary above gives an arithmetic sufficient condition to determine if there is an arithmetic progression with squares at the positions $\{0, 2, n, n + 2\}$ for any positive integer n. This condition is that the number of odd primes dividing n has the same parity as the number of primes congruent to 1 mod 4 dividing $n^2 - 4$. The disadvantage is that this condition assumes the Parity Conjecture for the elliptic curve $E_{2,n}$. Note that we may suppose that n is odd since in the even case we can reduce $\{0, 2, n, n + 2\}$ to $\{0, 1, n/2, (n + 1)/2\}$.

4. *Five squares in arithmetic progressions: the technique*

We will see in Section 5 that the results of Section 3 are not enough to show Rudin's conjecture even for small values of N. In this section we will study how to prove, for some subsets I with 5 elements, that $z_I = 0$ even if it is not zero for any subset J of I with four elements. Moreover, we will be able to determine $\mathcal{Z}_I$ in some cases.

In order to prove these type of results, we need to be able to compute the rational points of some genus 5 curves whose Jacobians are products of elliptic curves, all of them of rank greater than 0. Hence it is not possible to apply the classical Chabauty method (see [8, 11, 15, 21, 25, 26]). We will instead apply the covering collections technique, as developed by Coombes and Grant [12], Wetherell [28] and others, and specifically a modification of what is now called the elliptic curve Chabauty method developed by Flynn and Wetherell in [16] and by Bruin in [5]. In fact, we will follow the same technique we applied in [17], though a similar technique to the one we used in [18] to study five squares in arithmetic progression over quadratic fields could also be used.

First, we fix the notation. We consider a primitive subset $I \subset \mathbb{N}$ with five elements, and denote by C_I the associated curve as in Proposition 2. We want to show that $z_I = 0$, which is equivalent to show that $C_I(\mathbb{Q})$ only contains the trivial points $\mathcal{T}_I$. Since the genus of C_I is 5, its set of rational points is always finite, hence we may even try to explicitly compute it.

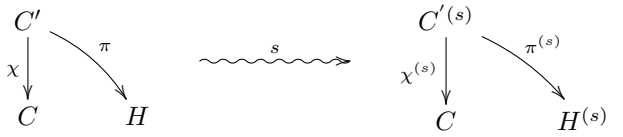
Observe that C_I has five different maps to the elliptic curves corresponding to C_J, for J a subset of I with four elements. As we have already seen in the previous section, the corresponding elliptic curves have all their 2-torsion points defined over $\mathbb{Q}$, a fact that we will use to build unramified coverings of C_I.

The method has two parts. Suppose we have a curve C over a number field K, and an unramified map $\chi : C' \to C$, of degree greater than one, may be defined over a finite extension L of K, along with a nice quotient $C' \to H$, for example a genus 1 quotient. We consider the different unramified coverings $\chi^{(s)} : C'^{(s)} \to C$ which consist of all the twists of the given one. Now, by a classical theorem of Chevalley and Weil [9],

$$C(K) = \bigcup_s \chi^{(s)}(\{P \in C'^{(s)}(L) \ : \ \chi^{(s)}(P) \in C(K)\}),$$

the union being disjoint. Moreover, only a finite number of twists have rational points (the relevant ones), and the (in principle larger) finite set of twists which have points locally everywhere can be explicitly described. The method depends first on being able to compute explicitly a finite set S of twists containing the relevant ones, and second, on being able to

compute all the points $P \in C'^{(s)}(L)$ such that $\chi^{(s)}(P) \in C(K)$ for all $s \in S$, by considering their images in $H^{(s)}(L)$.



In our case, the coverings we are searching for will be defined over $\mathbb{Q}$, but the genus 1 quotients of such coverings are, in general, not defined over $\mathbb{Q}$, but over a quadratic or biquadratic extension. The way we will construct the coverings (factorizing quartic polynomials) will also give us the genus 1 quotients and the field where they are all defined.

In order to construct explicitly the coverings of the curve C_I, we first rewrite the curve as the projectivization (and normalization) of a curve in $\mathbb{A}^3$ given by equations of the form $y_1^2 = p_1(x)$ and $y_2^2 = p_2(x)$, where $p_1(x)$ and $p_2(x)$ are separable degree 4 polynomials with coefficients in $\mathbb{Q}$. This is possible because of the special form of the curve (essentially, because it has two degree 2 maps to elliptic curves that correspond to involutions that commute with each other), and in our case we will see it can be done in ten different ways.

Next, we will consider a factorization of the polynomials $p_i(x)$ as product of two degree 2 polynomials $p_{i,1}(x)$ and $p_{i,2}(x)$ defined over a quadratic field K. This factorization $p_i(x) = p_{i,1}(x)p_{i,2}(x)$ determines an unramified degree 2 covering $\chi : F_i' \to F_i$ of the genus 1 curve F_i given by $y_i^2 = p_i(x)$, as we describe in the next proposition, which summarizes some well-known results.

PROPOSITION 14. *Let F be a genus 1 curve over a number field K given by a quartic model of the form $y^2 = q(x)$, where $q(x)$ is a degree 4 monic polynomial in $K[x]$. Thus, the curve F has two rational points at infinity, and we fix an isomorphism from F to its Jacobian $E = \mathrm{Jac}(F)$ defined by sending one of these points at infinity to the zero point of E. Then:*

1. *any 2-torsion point of the curve E defined over K corresponds to a factorization of the polynomial $q(x)$ as a product of two quadratic polynomials $q_1(x), q_2(x) \in L[x]$, where L/K is an algebraic extension of degree at most 2;*
2. *given such a 2-torsion point P, the degree 2 unramified covering $\chi : F' \to F$ corresponding to the degree 2 isogeny $\phi : E' \to E$ determined by P can be described as the map from the curve F' defined over L, with affine part in $\mathbb{A}^3$ given by the equations $y_1^2 = q_1(x)$ and $y_2^2 = q_2(x)$ and the map given by $\chi(x, y_1, y_2) = (x, y_1y_2)$;*
3. *given any degree 2 isogeny $\phi : E' \to E$, consider the Selmer group $Sel(\phi)$ as a subgroup of $K^*/(K^*)^2$. Let $\mathcal{S}_L(\phi)$ be a set of representatives in L of the image of $Sel(\phi)$ in $L^*/(L^*)^2$ via the natural map. For any $\delta \in \mathcal{S}_L(\phi)$, define the curve $F'^{(\delta)}$ given by the equations $\delta y_1^2 = q_1(x)$ and $\delta y_2^2 = q_2(x)$, and the map to F defined by $\chi^{(\delta)}(x, y_1, y_2) = (x, \delta y_1 y_2)$. Then*

$$F(K) \subseteq \bigcup_{\delta \in \mathcal{S}_L(\phi)} \chi^{(\delta)}(\{(x, y_1, y_2) \in F'^{(\delta)}(L) \mid x \in K \text{ or } x = \infty\}).$$

In order to apply the method to a 5-tuple $I \subset \mathbb{N}$, we first explain how to construct models of C_I such as the ones described above. We first need to choose a subset $J = \{n_0, n_1, n_2\} \subset I$ with three elements, which determines a partition $I = J \sqcup \{n_3, n_4\}$ of I, the n_i not necessarily ordered; the following constructions will depend on that choice. Second, we write the equations of C_I in the form

$$C_I : \begin{cases} X_0^2 = (m_0 + 1)X_1^2 - m_0X_2^2, \\ X_3^2 = -m_1X_1^2 + (m_1 + 1)X_2^2, \\ X_4^2 = -m_2X_1^2 + (m_2 + 1)X_2^2, \end{cases}$$

where

$$m_0 = \frac{n_1 - n_0}{n_2 - n_1}, \quad m_1 = \frac{n_3 - n_2}{n_2 - n_1} \quad \text{and} \quad m_2 = \frac{n_4 - n_2}{n_2 - n_1}.$$

Next, we parametrize the first equation as in Section 3:

$$[X_0 : X_1 : X_2] = [(m_0+1) - 2(m_0+1)t + t^2 \,:\, (m_0+1) - 2t + t^2 \,:\, (m_0+1) - t^2],$$

and we substitute in the other two equations, to obtain the new equations of the curve, depending on the parameter t:

$$C_I : \left\{ y_1^2 = p_1(t), y_2^2 = p_2(t) \right\},$$

where, for $i = 1, 2$, $y_i = X_{2+i}$ and

$$p_i(t) = t^4 + 4m_i t^3 - 2(m_0 + 4m_i + 2m_i m_0 + 1)t^2 + 4m_i(m_0+1)t + (m_0+1)^2.$$

For $i = 1, 2$, we have that the genus 1 curve $F_i : y_i^2 = p_i(t)$ is $\mathbb{Q}$-isomorphic to the elliptic curve

$$E_i : y^2 = x(x - m_0 m_i)(x + m_0 + m_i + 1).$$

Now, we need to choose factorizations of the polynomials $p_i(t)$ as a product of two quadratic polynomials over some quadratic extension $K/\mathbb{Q}$. We describe in the next elementary lemma all these factorizations, relating them to the corresponding 2-torsion points in the corresponding elliptic curve E_i.

LEMMA 15. *For $i = 1, 2$, let*

$$D_{i,1} = m_i(1 + m_i), \quad D_{i,2} = (1 + m_i)(m_i + m_0 + 1), \quad D_{i,3} = m_i(m_i + m_0 + 1),$$

and choose a square root $\alpha_{i,j} = \sqrt{D_{i,j}}$. Then the polynomial $p_i(t)$ factorizes over $\mathbb{Q}(\alpha_{i,j})$ as a product of two quadratic polynomials $p_{i,j,+}(t)$ and $p_{i,j,-}(t)$, depending on j, where

$$\begin{aligned}
p_{i,1,\pm}(t) &= t^2 + 2(m_i \pm \alpha_{i,1})t \mp 2\alpha_{i,1}m_0 - 2m_i m_0 - m_0 - 1 - 2m_i \mp 2\alpha_{i,1}, \\
p_{i,2,\pm}(t) &= t^2 + 2(m_i \pm \alpha_{i,2})t + m_0 + 1, \\
p_{i,3,\pm}(t) &= t^2 + 2(m_i \mp \alpha_{i,3})t - m_0 - 1 - 2m_i \pm 2\alpha_{i,3}.
\end{aligned}$$

These factorizations correspond, by Proposition 14, to the 2-torsion points in $E_i(\mathbb{Q})$ with x-coordinate equal to $r_{i,1} = m_0 m_i$, $r_{i,2} = -m_0 - m_i - 1$ and $r_{i,3} = 0$.

By the previous lemma and Proposition 14, one can construct Galois covers of C_I with Galois group $(\mathbb{Z}/2\mathbb{Z})^2$, depending on the choice of the subset $J \subset I$ above and the choice of $j_1, j_2 \in \{1, 2, 3\}$. The coverings can be described as the projectivization (and normalization) of the curve in $\mathbb{A}^5$ given by

$$C' \,:\, \{y_{1,+}^2 = p_{1,j_1,+}(t), y_{1,-}^2 = p_{1,j_1,-}(t), y_{2,+}^2 = p_{2,j_2,+}(t), y_{2,-}^2 = p_{2,j_2,-}(t)\},$$

which is a curve of genus 17, along with the map $\chi : C' \to C_I$ defined as

$$\chi(t, y_{1,+}, y_{1,-}, y_{2,+}, y_{2,-}) = (t, y_{1,+}y_{1,-}, \, y_{2,+}y_{2,-}).$$

These coverings can be defined over $\mathbb{Q}$, although we choose to show them in this form defined over the field $\mathbb{Q}(\alpha_{1,j}, \alpha_{2,j})$, which is at most a biquadratic extension of $\mathbb{Q}$, in order to consider appropriate genus 1 quotients of them.

Next, we choose one genus 1 quotient of the form

$$H_{\pm,\pm} : z^2 = p_{1,j_1,\pm}(t) p_{2,j_2,\pm}(t).$$

There are four such quotients, but depending on the degree of the field $\mathbb{Q}(\alpha_{1,j}, \alpha_{2,j})$ all of them might be conjugate over $\mathbb{Q}$ or there may be two conjugacy classes if the degree is 2 and all of them may be independent if the degree is 1.

For any element $\delta = (\delta_1, \delta_2) \in (\mathbb{Q}^*)^2$, we consider the twist $C'^{(\delta_1,\delta_2)}$ of the cover χ, given by

$$C'^{(\delta_1,\delta_2)} \; : \; \begin{cases} \delta_1 y_{1,+}^2 = p_{1,j_1,+}(t), & \delta_1 y_{1,-}^2 = p_{1,j_1,-}(t) \\ \delta_2 y_{2,+}^2 = p_{2,j_2,+}(t), & \delta_2 y_{2,-}^2 = p_{2,j_2,-}(t) \end{cases},$$

along with the map

$$\chi^{(\delta_1,\delta_2)}(t, y_{1,+}, y_{1,-}, y_{2,+}, y_{2,-}) = (t, \delta_1 y_{1,+} y_{1,-}, \delta_2 y_{2,+} y_{2,-}).$$

We obtain

$$C(\mathbb{Q}) \subseteq \bigcup_{\delta \in \mathfrak{D}} \chi^{(\delta)}(\{(t, y_{1,+}, y_{1,-}, y_{2,+}, y_{2,-}) \in C'^{(\delta)}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})) \;\mid\; t \in \mathbb{P}^1(\mathbb{Q})\}),$$

for some finite subset $\mathfrak{D} \subset (\mathbb{Q}^*)^2$. Proposition 14 allows us to describe the set $\mathfrak{D}$ in terms of the Selmer groups of some isogenies. For any such $\delta = (\delta_1, \delta_2)$, consider the quotients

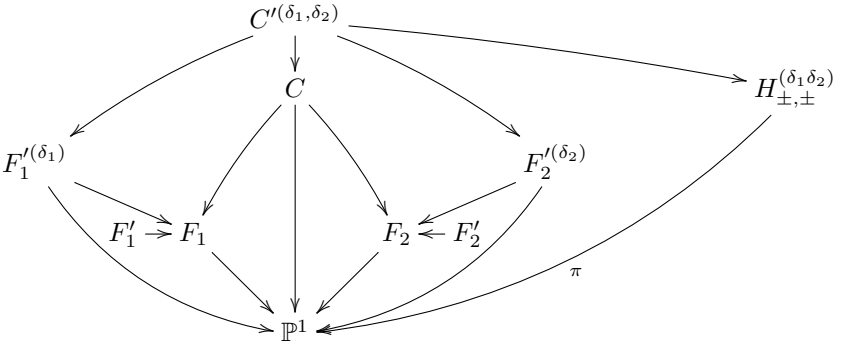
$$H_{\pm,\pm}^{(\delta_1\delta_2)} : \delta_1\delta_2 z^2 = p_{1,j_1,\pm}(t) p_{2,j_2,\pm}(t)$$

which, in fact, only depend on the product $\delta_1\delta_2$. We obtain

$$\{t \in \mathbb{Q} \mid \; \exists Y \in \mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})^4 \text{ such that } (t, Y) \in C'^{(\delta)}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))\}$$

$$\subseteq \{t \in \mathbb{Q} \mid \; \exists w \in \mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}) \text{ such that } (t, w) \in H_{\pm,\pm}^{\delta}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))\}.$$

The following commutative diagram illustrates, for a choice of (j_1, j_2) and a subset $J = \{n_0, n_1, n_2\} \subset I$, all the curves and morphisms involved in our problem.



The vertical map from C to $\mathbb{P}^1$ is the composition of the natural map from C to the conic given by the equation $X_0^2 = (m_0 + 1)X_1^2 - m_0 X_2^2$ with the isomorphism to $\mathbb{P}^1$ given by the parameter t.

Let Υ_I be the group of automorphisms of the curve C_I generated by the automorphisms $\tau_i(x_i) = -x_i$ and $\tau_i(x_j) = x_j$ if $i \neq j$, for $i = 0, \ldots, k$. In the next lemma we describe a finite set $\mathfrak{S} \subset (\mathbb{Q}^*)$ enough to cover all the possible rational values of t giving rational points of C_I, modulo Υ_I.

LEMMA 16. *Let $I \subset \mathbb{N}$ be a 5-tuple. Fix a subset $J = \{n_0, n_1, n_2\} \subset I$ and $j_1, j_2 \in \{1, 2, 3\}$. For any $i = 1, 2$, denote by $\phi_i : E_i' \to E_i$ the 2-isogeny corresponding to the 2-torsion point $(r_{i,j_i}, 0) \in E_i(\mathbb{Q})$. Consider the field $L = \mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})$ and let $\mathcal{S}_L(\phi_i)$ be a set of representatives in L of the image of $Sel(\phi_i)$ in $L^*/(L^*)^2$ via the natural map. Finally, denote by $\widetilde{\mathcal{S}_L}(\phi_1)$ a set of representatives of $Sel(\phi_1)$ modulo the subgroup generated by the image of the trivial points $\mathcal{T}_I$ in this Selmer group. Consider the subset $\mathfrak{S} \subset \mathbb{Q}^*$ defined by*

$$\mathfrak{S} = \{\delta_1\delta_2 \;\mid\; \delta_1 \in \widetilde{\mathcal{S}_L}(\phi_1), \delta_2 \in \mathcal{S}_L(\phi_2)\}.$$

Then, for any point $P = (t, y_1, y_2) \in C_I(\mathbb{Q})$, there exists $\tau \in \Upsilon_I$ and $\delta \in \mathfrak{S}$ such that $\tau(P) = (t', y_1', y_2')$ with $t' \in \pi(H_{\pm,\pm}^{\delta}(L))$ for any sign choice $(\pm, \pm)$.

Proof. We described in the previous paragraph that any point $P = (t, y_1, y_2) \in C_I(\mathbb{Q})$ lifts to a point in $C'^{(\delta_1,\delta_2)}(L)$ for some $\delta_i \in \mathrm{Sel}(\phi_i)$, for $i = 1, 2$. Hence it determines a point in $H^{\delta_1\delta_2}_{\pm,\pm}(L)$ with the first coordinate in $\mathbb{P}^1(\mathbb{Q})$.

If $P \in C_I(\mathbb{Q})$ has image δ_1 in the Selmer group $\mathrm{Sel}(\phi_1)$, then $\tau(P)$ has image $\delta_1\delta_\tau$, if δ_τ is the image of $\tau(T)$ in $\mathrm{Sel}(\phi_1)$ for some trivial point T with corresponding $\delta_1 = 1$. This is true because the automorphisms that belong to Υ_I correspond to the translations by trivial points in the corresponding elliptic curve, if we fix (as we did) the zero point to be a trivial point (see Lemma 11 in [29] for a proof in a special case). But the action of Υ_I in $C_I(\mathbb{Q})$ is transitive on the set of trivial points $\mathcal{T}_I$. □

Now, the method allows us to know for sure if we are able to compute, for some choice of a subset $J = \{n_0, n_1, n_2\} \subset I$ and $j_1, j_2 \in \{1, 2, 3\}$, and for any $\delta \in \mathfrak{S}$, all the points $(t, w) \in H^\delta_{\pm,\pm}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$ with $t \in \mathbb{Q}$ for some choice of the signs $(\pm, \pm)$.

This last computation can be done in two steps as follows.

(1) We first need to determine if there is some point in $H^\delta_{\pm,\pm}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$. In the special case $\delta = (1, 1)$, the point at infinity is always a rational point. But, in general, this curve (which has points locally everywhere for our choices of δ) may have no rational points if it represents an element of the Tate-Shafarevich group of its Jacobian. We use the method described by Bruin and Stoll in [6] and their implementation in `Magma` [4] to determine if this happens.

(2) Second, we choose an isomorphism with its Jacobian $\mathrm{Jac}(H^\delta_{\pm,\pm})$ and then we use the elliptic curve Chabauty technique as developed by Bruin [5] to compute this set if the rank of its group of $\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})$-rational points is less than the degree of $\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})$ over $\mathbb{Q}$. We also need to determine a subgroup of finite index of this group to carry out the elliptic curve Chabauty method. All this is also implemented in `Magma`.

Hence we have 90 possible choices of J, j_1 and j_2, and we need to find one of them where we can carry out these computations for all the elements $\delta \in \mathfrak{S}$. In practice, we only consider the case where the field $\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})$ is at most a quadratic extension of $\mathbb{Q}$, essentially because of the computation of the rank and/or a subgroup of finite index in $\mathrm{Jac}(H^\delta_{\pm,\pm})(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$ is too expensive computationally for number fields of higher degree.

4.1. *The algorithm at work*

We have implemented in `Magma V2.18-8` the algorithm developed above. In the following we describe this algorithm in a few examples. For these 5-tuples $I \subset \mathbb{N}$ we show how it works. In the case that the output of the algorithm is `true` then we obtain $\mathcal{Z}_I$, otherwise we give detailed information about the reasons why the algorithm does not work.

• $I = \{0, 1, 2, 4, 7\}$: this is the first case having no rank zero elliptic quotients. First, we need to choose a subset $J \subset I$, and two values $j_1, j_2 \in \{1, 2, 3\}$ such that the field $L = \mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})$ is of degree less or equal to 2. The subset $J = \{1, 4, 7\}$ and the pair $(j_1, j_2) = (2, 1)$ do the job. In this case $L = \mathbb{Q}(\sqrt{10})$ and we have the following factorizations:

$$p_{1,2,+}(t) = t^2 - 10/3t + 2, \quad p_{2,1,+}(t) = t^2 + 1/3(-2\sqrt{10} - 10)t + 1/3(4\sqrt{10} + 14),$$
$$p_{1,2,-}(t) = t^2 - 6t + 2, \qquad p_{2,1,-}(t) = t^2 + 1/3(2\sqrt{10} - 10)t + 1/3(-4\sqrt{10} + 14).$$

Note that in fact in this case we have $\mathbb{Q}(\alpha_{1,2}) = \mathbb{Q}$. The next step is to compute the set $\mathfrak{S}$ (see Lemma 16). We have $\mathfrak{S} = \{1, 2, 3, 6\}$. Now for any $\delta \in \mathfrak{S}$, we must compute all the points $(t, w) \in H^\delta_{\pm,\pm}(\mathbb{Q}(\sqrt{10}))$ with $t \in \mathbb{P}^1(\mathbb{Q})$ for some sign choice $(\pm, \pm)$, where

$$H^\delta_{\pm,\pm} : \delta w^2 = p_{1,2,\pm}(t)p_{2,1,\pm}(t).$$

For $\delta = 1, 6$, we have that $\mathrm{rank}_{\mathbb{Z}} H^\delta_{+,+}(\mathbb{Q}(\sqrt{10})) = 1$, therefore we can apply elliptic curve Chabauty to obtain the possible values of t. For $\delta = 1$ (respectively $\delta = 6$) we obtain $t = \infty$

(respectively $t = 0$). For the values $t = \infty$ and $t = 0$ we obtain the trivial points $[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1] \in C_I(\mathbb{Q})$. For $\delta = 2, 3$, using the method described by Bruin and Stoll [6] we obtain $H^{\delta}_{-,+}(\mathbb{Q}(\sqrt{10})) = \varnothing$.

The following table shows all the previous data, where the last column shows the arithmetic progression associated to the corresponding t.

δ	Signs	$H^{\delta}_{\text{signs}}(L) = \varnothing$?	$\text{rank}_{\mathbb{Z}} H^{\delta}_{\text{signs}}(L)$	t	(q, a)
1	$(+,+)$	No	1	∞	$(0,1)$
2	$(-,+)$	Yes	–	–	–
3	$(-,+)$	Yes	–	–	–
6	$(+,+)$	No	1	0	$(0,1)$

$I = \{0,1,2,4,7\}, J = \{1,4,7\}, (j_1, j_2) = (2,1), L = \mathbb{Q}(\sqrt{10})$

Looking at the previous table, we obtain $C_I(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1]\}$; and therefore $z_I = 0$ if $I = \{0,1,2,4,7\}$.

• $I = \{0,1,2,5,7\}$: this is the Rudin sequence. Let $J = \{2,5,7\}$ and $(j_1, j_2) = (3,2)$. Then we have $L = \mathbb{Q}(\sqrt{14})$ and $\mathfrak{S} = \{\pm 1, \pm 2, \pm 5, \pm 10\}$. The following table summarizes all the computations made in this case.

δ	Signs	$H^{\delta}_{\text{signs}}(L) = \varnothing$?	$\text{rank}_{\mathbb{Z}} H^{\delta}_{\text{signs}}(L)$	t	(q, a)
1	$(+,+)$	No	1	∞	$(0,1)$
-1	$(+,+)$	No	1	–	–
2	$(+,-)$	No	1	3	$(24,1)$
-2	$(+,-)$	No	1	–	–
5	$(+,-)$	No	1	5/6	$(24,1)$
-5	$(+,-)$	No	1	–	–
10	$(+,+)$	No	1	0	$(0,1)$
-10	$(+,+)$	No	1	–	–

$I = \{0,1,2,5,7\}, J = \{2,5,7\}, (j_1, j_2) = (3,2), L = \mathbb{Q}(\sqrt{14})$

We have that $C_I(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1], [1 : \pm 5 : \pm 7 : \pm 11 : \pm 13]\}$. That is, $\mathcal{Z}_I = \{(24,1)\}$ for $I = \{0,1,2,5,7\}$.

• $I = \{0,1,3,7,8\}$: in this example there are several rational solutions t. Looking at the table below we obtain $\mathcal{Z}_I = \{(120,1)\}$.

δ	Signs	$H^{\delta}_{\text{signs}}(L) = \varnothing$?	$\text{rank}_{\mathbb{Z}} H^{\delta}_{\text{signs}}(L)$	t	(q, a)
1	$(+,+)$	No	1	$\infty, 1$ $4, 5/6$	$(0,1)$ $(120,1)$
-1	$(+,+)$	No	1	$0, 3/2$ $9/5, 3/8$	$(0,1)$ $(120,1)$
2	$(+,+)$	Yes	–	–	–
-2	$(+,+)$	Yes	–	–	–

$I = \{0,1,3,7,8\}, J = \{1,3,7\}, \{j_1, j_2\} = \{3,3\}, L = \mathbb{Q}(\sqrt{7})$

In this case we have obtained $C_I(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1], [1 : \pm 11 : \pm 19 : \pm 29 : \pm 31]\}$.

• $I = \{0,1,4,7,8\}$: in this case we have at least two possible choices of J and (j_1, j_2) where the algorithm works obtaining $z_I = 0$. In the first case $L = \mathbb{Q}(\sqrt{2})$.

δ	Signs	$H^{\delta}_{\text{signs}}(L) = \varnothing$?	$\text{rank}_{\mathbb{Z}} H^{\delta}_{\text{signs}}(L)$	t	(q, a)
1	$(+,+)$	No	1	$0, \infty$	$(0,1)$
3	$(+,+)$	No	1	–	–
7	$(+,+)$	No	1	–	–
21	$(-,+)$	No	1	–	–

$I = \{0,1,4,7,8\}, J = \{1,4,8\}, \{j_1, j_2\} = \{2,2\}, L = \mathbb{Q}(\sqrt{2})$

The second case is more remarkable, since we get $L = \mathbb{Q}$ and the corresponding elliptic curves have rank 0, as the table below shows.

δ	Signs	$H^{\delta}_{\text{signs}}(L) = \varnothing$?	$\text{rank}_{\mathbb{Z}} H^{\delta}_{\text{signs}}(L)$	t	(q, a)
1	$(+,-)$	No	0	$1, \infty$	$(0, 1)$
2	$(+,+)$	Yes	–	–	–
-3	$(+,+)$	No	0	$0, 2$	$(0, 1)$
-6	$(+,+)$	Yes	–	–	–

$I = \{0, 1, 4, 7, 8\}, J = \{1, 4, 7\}, \{j_1, j_2\} = \{2, 1\}, L = \mathbb{Q}$

• $I = \{0, 3, 5, 6, 10\}$: this is the second 5-tuple where the algorithm does not work. The first one is $I = \{0, 1, 2, 6, 10\}$ and the reason is that ten CPU hours was not enough to finish the computations for I. In the following table appear all the subsets $J \subset I$ and pairs (j_1, j_2) such that $L = \mathbb{Q}(\sqrt{D})$ for some $D \in \mathbb{Z}$. Note that in all the previous cases, $p_1(t)$ and $p_2(t)$ do not factorize over $\mathbb{Q}$. Therefore it is enough to check the signs $(+,+)$ and $(-,+)$. For $\delta = 1$ we have computed an upper bound of the rank (denoted by rank*) of the Mordell-Weil group of the Jacobians of the curves $H^1_{+,+}(L)$ and $H^1_{-,+}(L)$, which is greater than 1 in all those cases. Therefore we can not apply elliptic curve Chabauty and the algorithm outputs `false`.

J	$\{j_1, j_2\}$	D	$\text{rank}^*_{\mathbb{Z}} H^1_{+,+}(\mathbb{Q}(\sqrt{D}))$	$\text{rank}^*_{\mathbb{Z}} H^1_{-,+}(\mathbb{Q}(\sqrt{D}))$
$\{0, 5, 10\}$	$\{2, 3\}$	-6	2	2
$\{0, 3, 6\}$	$\{2, 3\}$	10	2	2
$\{0, 6, 10\}$	$\{2, 3\}$	-1	3	2
$\{0, 3, 5\}$	$\{2, 3\}$	2	2	3

$I = \{0, 3, 5, 6, 10\}$

• $I = \{0, 2, 4, 5, 11\}$: this example shows one case where, for all subsets $J \subset I$ of three elements and for all $j_1, j_2 \in \{1, 2, 3\}$, we have that $L = \mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})$ is a biquadratic extension of $\mathbb{Q}$.

• Note that, for all the 5-tuples $I \subset \mathbb{N}$ where our algorithm has worked out, we have obtained $z_I = 0$ or $z_I = 1$, except in the case $I = \{0, 13, 24, 33, 49\}$. The table below shows that $\mathcal{Z}_I = \{(24, 49), (-1, 49)\}$, that is $z_I = 2$.

δ	Signs	$H^{\delta}_{\text{signs}}(L) = \varnothing$?	$\text{rank}_{\mathbb{Z}} H^{\delta}_{\text{signs}}(L)$	t	(q, a)
1	$(+,+)$	No	1	$\infty, 0$	$(0, 1)$
				$-12, -2/11$	$(-1, 49)$
6	$(+,+)$	No	1	-12	$(-1, 49)$
10	$(+,-)$	No	0	$2, 12/11$	$(-1, 49)$
11	$(+,-)$	No	0	$2, 12/11$	$(-1, 49)$
14	$(+,-)$	No	1	$12/11$	$(-1, 49)$
21	$(+,+)$	No	1	$16/3$	$(24, 49)$
				-12	$(-1, 49)$
35	$(+,-)$	No	0	$2, 12/11$	$(-1, 49)$
154	$(+,-)$	No	0	$2, 12/11$	$(-1, 49)$

$I = \{0, 13, 24, 33, 49\}, J = \{0, 13, 24\}, \{j_1, j_2\} = \{2, 2\}, L = \mathbb{Q}(\sqrt{165})$

In this case we have obtained

$$C_I(\mathbb{Q}) = \{[1 : \pm 1 : \pm 1 : \pm 1 : \pm 1], [49 : \pm 36 : \pm 25 : \pm 16 : \pm 0], [49 : \pm 361 : \pm 625 : \pm 841 : \pm 1225]\}.$$

5. *Summary of the computations*

One of the main objectives of this article is to prove the Strong Rudin's conjecture up to $N = 52$. For this purpose, we have developed a method based on the computation of the

rational points of the curves C_I associated to finite subsets $I \subset \mathbb{N}$. In Section 1.1, we have shown that under the natural equivalence we can restrict our computations to primitive subsets I.

First, let us consider the case of finite subsets $I \subset \mathbb{N} \cap \{0, \dots, 51\}$ of cardinality 4. There are 270 725 of those subsets, but only 9077 equivalence classes. We have proved in Section 3 that the corresponding curves are elliptic curves over $\mathbb{Q}$. The following table shows the number of curves having a given rank.

rank	0	1	2	3	4
# curves	199	4692	3778	406	2

If we restrict our attention to the symmetric case, we only have 402 equivalence classes.

rank	0	1	2
# curves	190	191	2

The next step is to compute the subsets of five elements. There are 2 598 960 of those subsets of $\{0, \dots, 51\}$, 117 449 equivalence classes. Then we remove all the subsets I in the previous list with a subset J such that $C_J(\mathbb{Q})$ is an elliptic curve of rank 0 and it has only eight torsion points, since in that case $z_I = 0$. After this sieve, 111 338 subsets remain. Now, in Section 4, given a subset $I \subset \mathbb{N}$ with five elements we have developed a method that allows us to determine $C_I(\mathbb{Q})$ in some cases. The method consists of first choosing a subset $J \subset I$ of three elements and $j_1, j_2 \in \{1, 2, 3\}$. There are 90 possible choices. The next step is to compute the finite set $\mathfrak{S}$, then to compute, for any $\delta \in \mathfrak{S}$, all the points $(t, w) \in H^{\delta}_{\pm,\pm}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$ with $t \in \mathbb{P}^1(\mathbb{Q})$ for some sign choice $(\pm, \pm)$. This method has worked out in 26 589 genus 5 curves C_I. For those, there are 26 165 cases such that $C_I(\mathbb{Q}) = \mathcal{T}_I$ and 424 cases such that $C_I(\mathbb{Q}) \neq \mathcal{T}_I$. For the remaining cases, 84 749, our method does not work for different reasons. First, we have bounded our computations for the cases where the fields $\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2})$ are at most quadratic extensions of $\mathbb{Q}$, since the algorithms on `Magma` we are using are better implemented in these number fields. There are 34 548 cases where all the 90 possible choices give biquadratic fields. For the remaining cases, there are 1033 such that `Magma` crashed for some unknown reason or there had not been enough time (maximum of ten CPU hours); we describe below the reasons for the remaining 49 168 cases. For a given case, we need to decide if $H^{\delta}_{\pm,\pm}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$ is empty or not. Then a first reason why our method does not work is:

(BS) `Magma` does not determine if $H^{\delta}_{\pm,\pm}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$ is empty or not.

Now, assuming that we have computed a rational point on $H^{\delta}_{\pm,\pm}(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$, there may be two further reasons:

(Rank) An upper bound for $\operatorname{rank}_{\mathbb{Z}} \operatorname{Jac}(H^{\delta}_{\pm,\pm})(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$ is greater than one. Then, in principle, we can not use the elliptic curve Chabauty method.

(noMW) `Magma` does not determine a subgroup of finite index on the elliptic curve $\operatorname{Jac}(H^{\delta}_{\pm,\pm})(\mathbb{Q}(\alpha_{1,j_1}, \alpha_{2,j_2}))$.

Notice that more than one reason could apply to a given 5-tuple I, making any of the 90 possible choices fail to compute $C_I(\mathbb{Q})$ by our method. The next table shows the number of cases for the corresponding reasons.

(Rank)	: 37394	(Rank)+(noMW)	: 988		
(BS)	: 630	(BS)+(Rank)	: 8526	(Rank)+(noMW)+(BS)	: 1523
(noMW)	: 11	(noMW)+(BS)	: 96		

All these computations (110 305 5-tuples such that the algorithm has finished in less than ten CPU hours) took around 68 days of CPU time on a MacPro4.1 with 2 x 2.26 GHz Quad-Core Intel Xeon.

The first case where we have not been able to determine $C_I(\mathbb{Q})$ is $I = \{0, 1, 2, 6, 10\}$, since ten CPU hours was not enough. The second one is $I = \{0, 3, 5, 6, 10\}$. In this case, our method

does not work since for all the elliptic quotients defined over quadratic fields the rank upper bound is greater than 1.

6. *Consequences and comments*

The main goal of this article is to give new evidence for Rudin's conjectures. First, given a positive integer $N \geqslant 6$, the strong version claims that $Q(N) = Q(N; 24, 1)$. Our strategy to prove this conjecture is recursive, that is, if we know $Q(N)$ for some N then we attempt to compute $Q(N+1)$. We have that $Q(N) \leqslant Q(N+1) \leqslant Q(N)+1$. Therefore we must compute $\mathcal{Z}_I$ for any $I \subset \{0, \ldots, N\}$ such that $\#I = Q(N)+1$. Note that if $z_I = 0$ for any such tuples I, then $Q(N+1) = Q(N)$. Otherwise $Q(N+1) = Q(N)+1$.

In Section 2 we proved $Q(6) = Q(7) = 4$, and $Q(8) = 5$ since $Q(8; 24, 1) = 5$. Following the same strategy we have even proved that $Q(9) = Q(10) = Q(11) = 5$. But it is not enough to show that $Q(12) = 5$, since for $I = \{0, 1, 2, 5, 9, 11\}$ all the genus 1 quotients associated to subsets of I of four elements have positive rank. However, by using the methods in Section 4, we prove that for $J = \{0, 1, 2, 9, 11\}$ we have $z_J = 0$, therefore $z_I = 0$.

Now, in the general case, the strategy we have followed is to consider all the primitive subsets I of five elements in $\{0, \ldots, 51\}$ where we are not able to compute $C_I(\mathbb{Q})$, either using the genus 1 quotients or by the methods in Section 4, as we have described in Section 5. Using this list we recursively compute the list $\mathcal{NC}(k)$ of all the primitive subsets I of k elements, $k \geqslant 6$, such that we are not able to compute $C_I(\mathbb{Q})$, by finding all the primitive subsets I of k elements whose subsets of $k-1$ elements are equivalent to a subset in $\mathcal{NC}(k-1)$ (see Table 3). Note that we have determined $C_I(\mathbb{Q})$ for all the subsets of $\{0, \ldots, 51\}$ with more than ten elements.

Furthermore, using the subsets I with five elements where we have explicitly determined $C_I(\mathbb{Q})$ such that $C_I(\mathbb{Q}) \neq \mathcal{T}_I$, we have explicitly computed, for $N \geqslant 8$, all the arithmetic progressions (q, a) such that $\#\mathcal{S}_N(q, a) = Q(N)$ except[†] for $N = 11, 12$. In Table 4 we summarize these results.

The computations from Table 4 allow us to prove what we have called the Super-Strong Rudin's conjecture up to level 52: consider $8 \leqslant N = \mathcal{GP}_k + 1 \leqslant 52$ for some integer k, then $Q(N) = Q(N; q, a)$ with $\gcd(q, a)$ squarefree and $q > 0$ if and only if $(q, a) = (24, 1)$.

We finish this section by discussing some points concerning the number of non-constant arithmetic progressions having their squares in a subset $I \subset \{0, \ldots, N\}$ with $\#I \geqslant 5$. One consequence of our computations is that, for the subsets I of $\{0, \ldots, 52\}$ with $\#I \geqslant 5$ for which we are able to compute z_I, we have obtained that $z_I \leqslant 1$, except for one case where $z_I = 2$. But it is easy to see that there are plenty of subsets I with $z_I \geqslant 2$.

TABLE 3. *First primitive subsets (in the natural order explained in Section 1.1) with k elements for which we are not able to determine $C_I(\mathbb{Q})$, together with the number of such subsets.*

k	$I \subset \{0, \ldots, 51\}$	Number of I
5	{0, 1, 2, 6, 10}	84 749
6	{0, 1, 2, 7, 12, 15}[‡]	289 752
7	{0, 1, 6, 8, 11, 19, 23}	299 855
8	{0, 1, 3, 11, 17, 22, 23, 30}	69 241
9	{0, 2, 4, 13, 14, 19, 30, 33, 41}	2082
10	{0, 2, 7, 14, 17, 24, 37, 40, 43, 48}	2

[‡] Note that $I = \{0, 1, 2, 7, 12, 15\} \subset \mathcal{S}_{16}(24, 1)$. Therefore $(24, 1) \in \mathcal{Z}_I$, but we are not able to compute the exact value of z_I.

[†]For the 5-tuples $\{0, 1, 2, 6, 10\}, \{0, 3, 5, 6, 10\}, \{0, 2, 4, 5, 11\}, \{0, 2, 5, 7, 11\}, \{0, 1, 5, 8, 11\}$ and $\{0, 1, 6, 8, 11\}$ we have not been able to compute the rational points of the corresponding genus 5 curves.

LEMMA 17. *Consider $a_i, q_i \in \mathbb{Z}$. Then:*
(1) if $q_1 q_2$ is not a square, then the set $\mathcal{S}(q_1, a_1^2) \cap \mathcal{S}(q_2, a_2^2)$ is infinite;
(2) $\mathcal{S}(q_1, a_1^2) \cap \mathcal{S}(q_2, a_2^2) \cap \mathcal{S}(q_3, a_3^2)$ is finite;
(3) if the Bombieri–Lang conjecture is true, there exists some r such that, for any set of r pairs (q_i, a_i) of coprime integers, $\bigcap_{i=1}^{r} \mathcal{S}(q_i, a_i^2)$ has at most four elements.

Proof. The set $\mathcal{S}(q_1, a_1^2) \cap \mathcal{S}(q_2, a_2^2)$ may also be described by the set of integer solutions of the equation

$$x_1^2 - q_1 q_2 x_2^2 = q_2^2 a_1^2 - q_1 q_2 a_2^2,$$

which is a Pell type equation with a solution. Hence it has an infinite number of solutions.

In the case where we have three pairs, we look for integer solutions of an equation giving a genus 1 curve, so it has a finite number of them by Siegel's theorem.

If we have more than three pairs, the resulting curve will be of genus bigger than 1. So, suppose we have r pairs such that $J = \bigcap_{i=1}^{r} \mathcal{S}(q_i, a_i^2)$ has more than four elements, so there is a subset $I \subset J$ with five elements in it. This means that the corresponding curve C_I will have genus 5, and with $\#C_I(\mathbb{Q}) \geqslant 16r + 8$ (and, if $q_i \neq 0$ for all $i \in I$, in fact $\geqslant 16(r+1)$). But thanks to the results from [7], the Bombieri–Lang conjecture implies there is an absolute bound for the number of rational points of genus 5 curves over $\mathbb{Q}$. Hence such an r is upper bounded. □

EXAMPLE 18. Using the ideas of the previous lemma, it is easy to construct one-parametric families of subsets $I \subset \mathbb{N}$ with five elements along with two different and non-constant

TABLE 4. *In the first column k is an integer, in the second $\mathcal{GP}_k$, in the third the integers N between $\mathcal{GP}_k + 1$ and the next generalized pentagonal number, in the fourth the value $Q(N)$, and in the last column the arithmetic progressions $qn + a$ with $\gcd(q, a)$ squarefree and $q > 0$ such that they have $Q(N)$ squares for $n \in \{0, \ldots, N-1\}$.*

k	$\mathcal{GP}_k$	N	$Q(N)$	Arithmetic progressions (q, a)
		8		$(24, 1)$
-2	7	9–10	5	$(24, 1)$, $(120, 1)$
		11		$(24, 1)$, $(120, 1)$, $(8, 1)$
		12		$(24, 1)$, $(120, 1)$, $(8, 1)$, $(24, 25)$, $(120, 49)$, $(40, 1)$, $(168, 1)$
		13–14		$(24, 1)$
3	12	15	6	$(24, 1)$, $(24, 25)$, $(120, 1)$
		16–18		$(24, 1)$
		19–20		$(24, 1)$, $(120, 49)$
-3	15	21	7	$(24, 1)$, $(120, 49)$, $(120, 1)$
		22		$(24, 1)$, $(120, 49)$, $(120, 1)$, $(24, 25)$, $(8, 1)$
		23		$(24, 1)$
4	22	24–25	8	$(24, 1)$, $(120, 49)$
		26		$(24, 1)$, $(120, 49)$, $(24, 25)$
		27–31		$(24, 1)$
-4	26	32–34	9	$(24, 1)$, $(120, 1)$
		35		$(24, 1)$, $(120, 1)$, $(24, 25)$
		36–39		$(24, 1)$
5	35	40	10	$(24, 1)$, $(24, 25)$
		41–49		$(24, 1)$
-5	40	50	11	$(24, 1)$, $(120, 49)$
		51		$(24, 1)$, $(120, 49)$, $(24, 25)$
6	51	52	12	$(24, 1)$

arithmetic progressions taking squares in I. For example, for any integer $s > 1$, we have that

$$\mathcal{S}(s-1,1) \cap \mathcal{S}(s+1,1) \supset \{0, 4s, 4s(4s^2-1), 8s(8s^4-6s^2+1), 8s(32s^6-40s^4+14s^2-1)\}.$$

As a consequence, we get a one-parametric family of genus 5 non-hyperelliptic curves (of the form C_I) having at least $3 \cdot 16 = 48$ points.

Remark 19. If the Bombieri–Lang conjecture holds true then, thanks to the results from [7], we have that there exists a bound $B(g, \mathbb{Q})$ such that any curve of genus g defined over $\mathbb{Q}$ satisfies $\#C(\mathbb{Q}) \leqslant B(g, \mathbb{Q})$. For the special case $g = 5$, Kulesz [20] found a biparametric family of hyperelliptic curves of genus 5 with 24 automorphisms over $\mathbb{Q}$ with at least 96 points, and for some special value he was able to find a genus 5 hyperelliptic curve C defined over $\mathbb{Q}$ with $\#C(\mathbb{Q}) = 120$. For the non-hyperelliptic case, we have that the curve C_I associated to a 5-tuple $I \subset \mathbb{N}$ is of genus 5 and has 16 automorphisms over $\mathbb{Q}$. Example 18 shows a one-parametric family of genus 5 non-hyperelliptic curves with at least $3 \cdot 16 = 48$ points. Furthermore, we found the following curves associated to 5-tuples $I \subset \mathbb{N}$ such that $\#C_I(\mathbb{Q}) \geqslant 5 \cdot 16 = 80$. For this search, we looked for 5-tuples such that they have points corresponding to $\mathcal{S}(24b, a)$ with $a = 1 + 24k$ square for some $b, k \in \mathbb{N}$. Table 5 shows the results we have obtained.

Table 5. *Some 5-tuples I with $z_I \geqslant 4$.*

I	Arithmetic progression (q, a) such that $I \subset \mathcal{S}(q, a)$			
$\{0, 2, 13, 23, 2233\}$	$(240, 1369)$	$(72, 25)$	$(120, 3481)$	$(168, 625)$
$\{0, 5, 19, 70, 1020\}$	$(72, 1)$	$(120, 2209)$	$(552, 961)$	$(24, 169)$
$\{0, 5, 33, 70, 1183\}$	$(1344, 169)$	$(72, 1849)$	$(816, 961)$	$(24, 169)$
$\{0, 17, 52, 147, 290\}$	$(120, 1681)$	$(96, 49)$	$(24, 961)$	$(264, 2401)$

Note that the Bombieri–Lang conjecture implies that, for $k \geqslant 5$, a constant $c(k)$ should exist such that $z_I \leqslant c(k)$ for all $I \subset \mathbb{N}$ with $\#I = k$. In particular, $z_I \leqslant c(5)$ for all $I \subset \mathbb{N}$. The previous examples show that $c(k) \geqslant 2$ and $c(5) \geqslant 4$ (but we believe $c(5) > 4$).

Acknowledgements. We would like to thank Noam Elkies for a useful discussion about Remark 19 and Nils Bruin for fixing a bug in the elliptic curve Chabauty `Magma` routine that appeared on Magma v2.18-7. We would like to express our gratitude to José M. Tornero for carefully reading the whole paper and proposing several corrections. Finally, we would like to thank the anonymous referee for many useful suggestions. The first author was partially supported by grant MTM2012–35849. The second author was partially supported by grant MTM2009–10359.

Data

All the Magma and Sage sources are available as online supplementary material from the publisher's website.

References

1. *Modular Functions of One Variable IV*, Lecture Notes in Mathematics 476 (eds B. J. Birch and W. Kuyk; (Springer, 1975).
2. E. Bombieri, A. Granville and J. Pintz, 'Squares in arithmetic progressions', *Duke Math. J.* 66 (1992) 369–385.
3. E. Bombieri and U. Zannier, 'A note on squares in arithmetic progressions. II', *Atti Accad. Naz. Lincei Cl. Sci. Fis. Mat. Natur. Rend. Lincei* (9) *Mat. Appl.* 13 (2002) 69–75.
4. W. Bosma, J. Cannon, C. Fieker, and A. Steel (eds), 'Handbook of Magma functions, Edition 2.18-8', 2012, http://magma.maths.usyd.edu.au/magma.

5. N. Bruin, 'Chabauty methods using elliptic curves', *J. Reine Angew. Math.* 562 (2003) 27–49.
6. N. Bruin and M. Stoll, 'Two-cover descent on hyperelliptic curves', *Math. Comp.* 78 (2009) 2347–2370.
7. L. Caporaso, J. Harris and B. Mazur, 'Uniformity of rational points', *J. Amer. Math. Soc.* 10 (1997) 1–35.
8. C. Chabauty, 'Sur les points rationnels des courbes algébriques de genre supérieur à l'unité', *C. R. Acad. Sci. Paris* 212 (1941) 882–885.
9. C. Chevalley and A. Weil, 'Un théorème d'arithmétique sur les courbes algébriques', *C. R. Acad. Sci. Paris* 195 (1932) 570–572.
10. J. H. E. Cohn, 'Squares in arithmetical progressions. I, II', *Math. Scand.* 52 (1983) 5–19; 20–23.
11. R F Coleman, 'Effective Chabauty', *Duke Math. J.* 52 (1985) 765–770.
12. K. R. Coombes and D. R. Grant, 'On heterogeneous spaces', *J. London Math. Soc.* (2) 40 (1989) 385–397.
13. J. E. Cremona, *Algorithms for modular elliptic curves* (Cambridge University Press, 1992).
14. P. Erdős, 'Quelques problèmes de théorie des nombres', Monographies de L'Enseignement Mathématique, No. 6, (L'Enseignement Mathématique, Université, Geneva, 1963) 81–135.
15. E. V. Flynn, 'A flexible method for applying Chabauty's Theorem', *Compositio Math.* 105 (1997) 79–94.
16. E. V. Flynn and J. L. Wetherell, 'Covering collections and a challenge problem of Serre', *Acta Arith.* 98 (2001) 197–205.
17. E. González-Jiménez and X. Xarles, 'On symmetric square values of quadratic polynomials', *Acta Arith.* 149 (2011) 145–159.
18. E. González-Jiménez and X. Xarles, 'Five squares in arithmetic progression over quadratic fields', *Rev. Mat. Iberoam.* 29 (2013) 1211–1238.
19. E. Halberstadt, 'Signes locaux des courbes elliptiques en 2 et 3', *C. R. Acad. Sci. Paris Sér.* I *Math.* 326 (1998) 1047–1052.
20. L. Kulesz, 'Courbes algébriques de genre $\geqslant 2$ possédant de nombreux points rationnels', *Acta Arith.* 87 (1998) 103–120.
21. W. McCallum and B. Poonen, 'On the method of Chabauty and Coleman', *Explicit methods in number theory: rational points and Diophantine equations*, Panoramas et Syntèses 36 (Société Mathématique de France, 2012).
22. D. E. Rohrlich, 'Variation of the root number in families of elliptic curves', *Compositio Math.* 87 (1993) 119–151.
23. W. Rudin, 'Trigonometric series with gaps', *J. Math. Mech.* 9 (1960) 203–227.
24. N. Sloane, 'The On-Line Encyclopedia of Integer Sequences', http://oeis.org/.
25. M. Stoll, 'Independence of rational points on twists of a given curve', *Compos. Math.* 142 (2006) 1201–1214.
26. M. Stoll, 'Finite descent obstructions and rational points on curves', *Algebra Number Theory* 1 (2007) 349–391.
27. E. Szemerédi, 'The number of squares in an arithmetic progression', *Studia Sci. Math. Hungar.* 9 (1975) 417.
28. J. L. Wetherell, 'Bounding the number of rational points on certain curves of high rank', PhD Thesis, University of California, Berkeley, 1997.
29. X. Xarles, 'Squares in arithmetic progression over number fields', *J. Number Theory* 132 (2012) 379–389.

Enrique González-Jiménez
Universidad Autónoma de Madrid
Departamento de Matemáticas and
Instituto de Ciencias Matemáticas
(ICMat)
Madrid, Spain

enrique.gonzalez.jimenez@uam.es

Xavier Xarles
Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra Barcelona
Catalonia

xarles@mat.uab.cat