On a problem of Schinzel and Wójcik involving equalities between multiplicative orders

By Francesco Pappalardi and Andrea Susa
Dipartimento di Matematica, Università Roma Tre,
Largo S. L. Murialdo, 1, *I*–00146 *Roma Italia*
e-mail: pappa,susa@mat.uniroma3.it

(*Received* 10 *October* 2005; *revised* ? *??* 2006)

Abstract

Given $a_1, \ldots, a_r \in \mathbb{Q} \setminus \{0, \pm 1\}$, the Schinzel–Wójcik problem is to determine whether there exist infinitely many primes p for which the order modulo p of each $a_1, \ldots, a_r$ coincides. We prove on the GRH that the primes with this property have a density and in the special case when each a_i is a power of a fixed rational number, we show unconditionally that such a density is non zero. Finally, in the case when all the a_i's are prime, we express the density it terms of an infinite product.

Contents

1. *Introduction*

If $a \in \mathbb{Q}^*$ and p is an odd prime such that the p–adic valuation $v_p(a) = 0$ then we define the *order* of a modulo p by

$$\operatorname{ord}_p a = \min \left\{ k \in \mathbb{N} \mid a^k \equiv 1 \bmod p \right\}.$$

In 1992 Schinzel and Wójcik [13] proved that given any rational $a, b \in \mathbb{Q} \setminus \{0, \pm 1\}$, there exist infinitely many primes p such that the following two conditions are satisfied:

(i) $v_p(a) = v_p(b) = 0$;
(ii) $\operatorname{ord}_p a = \operatorname{ord}_p b$.

Clearly the first condition is satisfied for all but finitely many primes and the second is the important one. Whenever we use the symbol $\operatorname{ord}_p a$, we always assume that $v_p(a) = 0$. The proof of Schinzel and Wójcik's result is very ingenious and uses Dirichlet's Theorem for primes in arithmetic progressions. In the last line of their paper, Schinzel and Wójcik conclude by stating the following problem:

Given $a, b, c \in \mathbb{Q} \setminus \{0, \pm 1\}$, do there exist infinitely many primes such that

$$\operatorname{ord}_p a = \operatorname{ord}_p b = \operatorname{ord}_p c?$$

We refer to the above as the Schinzel–Wójcik (SW for short) problem for a, b, c. In general, if $\{a_1, \ldots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$, the SW problem for $\{a_1, \ldots, a_r\}$ is to determine whether there are infinitely many primes p such that

$$\operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r.$$

In [17] Wójcik produced examples having no odd primes with the wanted property. Indeed let $a = e, b = e^2, c = -e^2$ with $e \in \mathbb{Q} \setminus \{0, \pm 1\}$. For any $p \geq 3$, if $\delta = \operatorname{ord}_p e = \operatorname{ord}_p -e^2$, then we have $e^{2\delta} \equiv (-e^2)^\delta \equiv 1(\text{mod } p)$. Therefore $(-1)^\delta \equiv 1(\text{mod } p)$ so that $2 \mid \delta$ and $(e^2)^{\delta/2} \equiv 1(\text{mod } p)$. This implies $\operatorname{ord}_p e^2 \mid \delta/2$ contradicting $\operatorname{ord}_p e^2 = \delta$. However we have the following result due to Wójcik [17]:

THEOREM (Wójcik (1996) [17]). *Let $K/\mathbb{Q}$ be a finite extension and $\alpha_1, \ldots, \alpha_r \in K \setminus \{0, 1\}$ be such that the multiplicative group $\langle \alpha_1, \ldots, \alpha_r \rangle \subset K$ is torsion free. Then the Schinzel* Hypothesis H *implies that there exist infinitely many primes $\mathfrak{p}$ of K of degree* 1 *such that*

$$\operatorname{ord}_{\mathfrak{p}} \alpha_1 = \cdots = \operatorname{ord}_{\mathfrak{p}} \alpha_r.$$

It is an immediate corollary that if $a, b, c \in \mathbb{Q} \setminus \{0, 1\}$ are such that $-1 \notin \langle a, b, c \rangle \subset \mathbb{Q}^*$, then Hypothesis H (see [12]) implies that the SW problem for $\{a, b, c\}$ has an affirmative answer. Note however that the sufficient condition $-1 \notin \langle a, b, c \rangle$ is not always necessary. Indeed consider SW for $\{2, 3, -6\}$. The above theorem does not apply although for $p = 19, 211, 499, 907$ and for many more primes p, one has that $\operatorname{ord}_p 2 = \operatorname{ord}_p 3 = \operatorname{ord}_p -6$. Moreover, empirical data suggest that the SW problem has an affirmative answer. Observe that Wójcik Theorem does not answer the SW problem for sets of the form $\{a, b, -ab\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$. We denote by $\operatorname{li}(x)$ the *logarithmic integral:*

$$\operatorname{li}(x) = \int_2^x dt/\log t.$$

The *Generalized Riemann Hypothesis* (GRH for short) can be applied to the SW problem. Indeed, we have the following:

THEOREM (K. R. Matthews - 1976 [7]). *Given $a_1, \ldots, a_r \in \mathbb{Z}^*$, there exists a constant $C = C(a_1, \ldots, a_r) \in \mathbb{R}^{\geq 0}$ such that if the Generalized Riemann Hypothesis holds, then*

$$\#\{p \leq x \text{ such that } \operatorname{ord}_p a_i = p - 1 \ \forall i = 1, \ldots, r\} = C \operatorname{li}(x) + O\left(x \frac{(\log\log x)^{2^r - 1}}{(\log x)^2}\right).$$

This result is known as the *simultaneous primitive roots Theorem* and admits as an immediate consequence the following:

COROLLARY. *With the above notation, if $C(a_1, \ldots, a_r) \neq 0$ and the GRH holds, then the SW problem has an affirmative answer for $a_1, \ldots, a_r$.*

Further results in [7] imply that $C(a_1, \ldots, a_r) = 0$ if and only if at least one of the following conditions is satisfied:

(i) There exists $1 \leq i_1 < \ldots < i_{2s+1} \leq r$ such that $a_{i_1} \cdots a_{i_{2s+1}} \in \mathbb{Q}^{*2}$;

(ii) There exists $1 \le i_1 < \ldots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3{\mathbb{Q}^*}^2$ and for each prime $q \equiv 1 \bmod 3$ there exists $i \in \{1, \ldots, r\}$ such that a_i is a cube modulo q.

Furthermore each of the conditions above implies that $a_1, \ldots, a_n$ cannot be simultaneously primitive roots for infinitely many primes.

From the above it follows that $C(2, 3, -6) \neq 0$ so that GRH implies that the SW problem has an affirmative answer in this case. The SW problem for $\{4, 3, -12\}$ is still open both on Hypothesis H and on GRH.

The goal of this note is to study the general SW problem assuming the Generalized Riemann Hypothesis.

For given rational numbers $a_1, \ldots, a_r$ not 0 or ± 1, we consider the following function:

$$\mathcal{S}_{a_1,\ldots,a_r}(x) = \{p \le x \mid \operatorname{ord}_p a_1 = \cdots = \operatorname{ord}_p a_r\}. \tag{1·1}$$

We denote by $\Gamma = \langle a_1, \ldots, a_r\rangle$ the subgroup of $\mathbb{Q}^*$ generated by $a_1, \ldots, a_r$, and by $r(a_1, \ldots, a_r) = \operatorname{rank}_{\mathbb{Z}}\langle a_1, \ldots, a_r\rangle$ its rank as abelian group. Clearly $1 \le r(a_1, \ldots, a_r) \le r$. Further let $\Gamma(N) := \Gamma \cdot {\mathbb{Q}^*}^N / {\mathbb{Q}^*}^N$,

$$\tilde{\Gamma}(N) = \left\{ \xi {\mathbb{Q}^*}^N \in \Gamma(N) \text{ such that } [\mathbb{Q}(\sqrt[N]{\xi}) : \mathbb{Q}] \le 2 \text{ and } \operatorname{disc}(\mathbb{Q}(\sqrt[N]{\xi})) \mid N \right\}$$

and $\Gamma_{\underline{k}} := \langle a_1^{\frac{k}{k_1}}, \ldots, a_r^{\frac{k}{k_r}}\rangle$ if $\underline{k} = (k_1, \ldots, k_r) \in \mathbb{N}^r$ and $k = [\underline{k}]$ is the least common multiple of $k_1, \ldots, k_r$. We also use the notation $\mu(\underline{k}) = \mu(k_1) \cdots \mu(k_r)$. The letters p and l will always denote prime numbers.

THEOREM 1. *Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$ and set $\Gamma = \langle a_1, \ldots, a_r\rangle$. Assume that the Generalized Riemann Hypothesis holds for the fields $\mathbb{Q}(\zeta_n, a_1^{1/n_1}, \ldots, a_r^{1/n_r})$ $(n, n_1, \ldots, n_r \in \mathbb{N})$ and that $r(a_1, \ldots, a_r) \ge 2$. Then*

$$\mathcal{S}_{a_1,\ldots,a_r}(x) = \left(\delta_{a_1,\ldots,a_r} + O_{a_1,\ldots,a_r}\left(\frac{(\log\log x)^{2^r-2}}{\log x} \right) \right) \operatorname{li}(x)$$

where

$$\delta_{a_1,\ldots,a_r} = \sum_{\substack{m \in \mathbb{N} \\ \underline{k} \in \mathbb{N}^r}} \frac{\mu(\underline{k})}{\varphi(mk)} \frac{\#\tilde{\Gamma}_{\underline{k}}(mk)}{\#\Gamma_{\underline{k}}(mk)} \tag{1·2}$$

and the notation is the same as above.

When each a_i is the power of the same rational number, the group $\langle a_1, \ldots, a_r\rangle$ has rank one. In this case we write $a_i = a^{h_i}$ for each $i = 1, \ldots, r$ and we note that we can assume that the greatest common divisor $(h_1, \ldots, h_r) = 1$ otherwise we can replace a with $a^{(h_1,\ldots,h_r)}$. Here the Generalized Riemann Hypothesis can be avoided.

THEOREM 2. *Let $a \in \mathbb{Q} \setminus \{0, \pm 1\}$, $h_1, \ldots, h_r \in \mathbb{N}^+$ with $(h_1, \ldots, h_r) = 1$ and $h = [h_1, \ldots, h_r]$. Then the following asymptotic formula holds:*

$$\mathcal{S}_{a^{h_1},\ldots,a^{h_r}}(x) = \left(\delta_{a^{h_1},\ldots,a^{h_r}} + O_{a,h}\left(\frac{(\log\log x)^{\omega(h)+3}}{(\log x)^2} \right) \right) \operatorname{li}(x)$$

where $\omega(h)$ denotes the number of distinct prime factors of h, if $a = \pm b^d$ with $b > 0$ not a power of any rational number and $D(b) = \operatorname{disc}(\mathbb{Q}\sqrt{b})$, then

$$\delta_{a^{h_1},\dots,a^{h_r}}=\prod_{l|h}\left(1-\frac{l^{1-v_l(d)}}{l^2-1}\right)\times\left[1+t_{2,h}\times\left(s_a+t_{D(b),4h}\times\varepsilon_a\prod_{l|2D(b)}\frac{1}{1-\frac{l^2-1}{l^{1-v_l(d)}}}\right)\right]$$

where

$$s_a=\begin{cases}0 & \textit{if } a>0;\\ -\frac{3\cdot 2^{v_2(d)}-3}{3\cdot 2^{v_2(d)}-2} & \textit{if } a<0;\end{cases}\qquad t_{x,y}=\begin{cases}1 & \textit{if } x\mid y;\\ 0 & \textit{otherwise;}\end{cases}$$

and

$$\varepsilon_a=\begin{cases}\left(-\frac{1}{2}\right)^{2^{\max\{0,v_2(D(b)/d)-1\}}} & \textit{if } a>0;\\ \left(-\frac{1}{2}\right)^{2^{2-\max\{1,v_2(D(b)/d)\}}} & \textit{if } a<0 \textit{ and } v_2(D(b))\neq v_2(8d);\\ \frac{1}{16} & \textit{if } a<0 \textit{ and } v_2(D(b))=v_2(8d).\end{cases}$$

In this degenerate case we can give a complete answer to the SW problem.

COROLLARY 3. *Let $a\in\mathbb{Q}\setminus\{0,\pm1\}$ and $h_1,\dots,h_r\in\mathbb{N}^+$. Then $\delta_{a^{h_1},\dots,a^{h_r}}\neq 0$. Therefore the SW problem for $\{a^{h_1},\dots,a^{h_r}\}$ has an affirmative answer.*

Corollary 3 will proven at the end of Section 4.

In the case when $a_1,\dots,a_r$ are all primes we can express the density in terms of an infinite Euler–product.

THEOREM 4. *Let $p_1,\dots,p_r$ be primes. Set*

$$\Lambda_l=-\frac{l(l^r-(l-1)^r-1)}{(l-1)(l^{r+1}-1)}\qquad \textit{and}\qquad \delta=\prod_l(1+\Lambda_l)\,.$$

Then

$$\delta_{p_1,\dots,p_r}=\delta\cdot\left(\sum_{d|p_1\cdots p_r}\left(1-\frac{2-2^{-r}}{3}(1-\eta_d)\right)\prod_{\substack{l|d\\ l>2}}\left(\frac{\Lambda_l}{1+\Lambda_l}\right)\right)$$

where $\eta_1=1$ and

$$\eta_d=\begin{cases}-1 & \textit{if } d\equiv 3 \bmod 4;\\ \mu(d) & \textit{if } d\equiv 1 \bmod 4, d\neq 1;\\ -1/2-1/2^r & \textit{if } d\equiv 2 \bmod 4.\end{cases}$$

2. *Lemmata*

In this section we present some useful results for setting up the proofs.

Let $\Gamma\subseteq\mathbb{Q}^*$ be a finitely generated multiplicative subgroup. The *support* of Γ is product the finite set of primes p which the p–adic valuation $v_p(g)\neq 0$ for some $g\in\Gamma$. That is

$$s_\Gamma=\prod_{\substack{p\\ \exists g\in\Gamma, v_p(g)\neq 0}}p.$$

Furthermore for each prime $p\nmid s_\Gamma$, we define the *order* $\operatorname{ord}_p\Gamma$ of Γ modulo p as the maximum order modulo p of the elements of Γ and the *index* of Γ modulo p by

$$\operatorname{ind}_p\Gamma=(p-1)/\operatorname{ord}_p\Gamma.$$

If we write $\operatorname{ind}_p \Gamma$ or $\operatorname{ord}_p \Gamma$, we always implicitly assume that $p \nmid s_\Gamma$. In particular the *index* of a_i modulo p is defined as $\operatorname{ind}_p a_i = (p-1)/\operatorname{ord}_p a_i$. Once again, if we write $\operatorname{ind}_p a_i$, we assume that $v_p(a_i) = 0$.

We start by an elementary result:

Lemma 5. *Let $a_1 \dots, a_r \in \mathbb{Q}^* \setminus \{\pm 1\}$, $m \in \mathbb{N}$, $k_1, \dots, k_r \in \mathbb{N}$ be squarefree and set $k = [k_1, \dots, k_r]$. If $p \nmid s_{\langle a_1, \dots, a_r \rangle}$, then the conditions:*

(i) $mk_i \mid \operatorname{ind}_p a_i$ *for* $i = 1, \dots, r$*;*
(ii) $mk \mid \operatorname{ind}_p \langle a_1^{k/k_1}, \dots, a_r^{k/k_r} \rangle$

are equivalent.

Proof. First note that

$$(mk_i \mid \operatorname{ind}_p a_i \forall i = 1, \dots, r) \quad \Longleftrightarrow \quad (mk \mid \operatorname{ind}_p a_i^{k/k_i} \forall i = 1, \dots, r).$$

Indeed, if g is a primitive root modulo p and $a_i \equiv g^{\alpha_i} \bmod p$, then $\operatorname{ind}_p a_i = (p-1, \alpha_i)$. Furthermore $mk_i \mid (p-1, \alpha_i)$ for $i = 1, \dots, r$ if and only if $mk \mid p-1$ and $mk \mid \alpha_i k/k_i$ for $i = 1, \dots, r$. This happens if and only if $mk \mid (p-1, \alpha_i k/k_i)$ for $i = 1, \dots, r$ or equivalently if $mk \mid \operatorname{ind}_p a_i^{k/k_i}$ for $i = 1, \dots, r$. Finally

$$\operatorname{ind}_p \langle a_1^{k/k_1}, \dots, a_r^{k/k_r} \rangle = (\operatorname{ind}_p a_1^{k/k_1}, \dots, \operatorname{ind}_p a_r^{k/k_r}).$$

So $mk \mid \operatorname{ind}_p a_i^{k/k_i}$ for $i = 1, \dots, r$ iff $mk \mid \operatorname{ind}_p \langle a_1^{k/k_1}, \dots, a_r^{k/k_r} \rangle$. □

The proof of Theorem 1 uses the Chebotarev Density Theorem. The following version is obtained using the effective version due to Lagarias and Odlyzko [3].

Lemma 6 (Chebotarev Density Theorem). *Let $M \in \mathbb{N}$ and denote by $\mathbb{Q}(\zeta_M, \Gamma^{1/M})$ the extension of the cyclotomic field $\mathbb{Q}(\zeta_M)$ obtained by adding the M–th roots of all the elements in Γ. Then the Generalized Riemann Hypothesis for the Dedekind zeta function of $\mathbb{Q}(\zeta_M, \Gamma^{1/M})$ implies*

$$\#\{p \le x \text{ such that } M \mid \operatorname{ind}_p \Gamma\} = \frac{\operatorname{li}(x)}{\left[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}\right]} + O\big(\sqrt{x} \log(xMs_\Gamma)\big). \qquad \square \quad (2{\cdot}1)$$

To compute the degree $\left[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}\right] = \#\operatorname{Gal}(\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q})$ we need to employ Kummer Theory (see Lang book [4, Chapter VIII, section 8] and also [1]) that allows us to deduce the next result:

Lemma 7. *Let $M \ge 1$ be an integer. With the notation above, we have that*

$$\left[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}\right] = \#\Gamma(M)/\#\tilde{\Gamma}(M)$$

where $\Gamma(M) = \Gamma \cdot \mathbb{Q}^{*M}/\mathbb{Q}^{*M}$ and

$$\tilde{\Gamma}(M) = \left\{ \xi \mathbb{Q}^{*M} \in \Gamma(M) \text{ such that } [\mathbb{Q}(\sqrt[M]{\xi}) : \mathbb{Q}] \le 2 \text{ and } \operatorname{disc}(\mathbb{Q}(\sqrt[M]{\xi})) \mid M \right\} . \square$$

The next lemma is implicit in the work of C. R. Matthews [6]:

Lemma 8. *Assume that $\Gamma \subseteq \mathbb{Q}^*$ is a multiplicative subgroup of rank $s \ge 2$. Let $t \in \mathbb{R}$, $t > 1$. We have the following estimate*

$$\#\{p \mid \operatorname{ord}_p \Gamma \le t\} \ll \frac{t^{1+1/s}}{\log t}, \qquad (2{\cdot}2)$$

where the implied constants may depend on Γ. □

The invariant $\Delta_s(\Gamma)$ of a multiplicative subgroup $\Gamma \subseteq \mathbb{Q}^*$ with $\operatorname{rank}_{\mathbb{Z}}(\Gamma) = s$, is defined as the greatest common divisor of all the minors of size s of the relation matrix of the group of absolute values of Γ (see [1, Section 3.1] for some details).

The next result follows immediately from a result in [1, Section 3.3], where it is stated in the case when M is squarefree. However, it is clear that the proof does not depend on this property.

LEMMA 9. *Let* Γ *and* M *as above, and* $s = \operatorname{rank}_{\mathbb{Z}}(\Gamma)$. *Then*

$$[\mathbb{Q}(\zeta_M, \Gamma^{1/M}) : \mathbb{Q}] \geq \varphi(M)\frac{(M/2)^s}{\Delta_s(\Gamma)}. \qquad \square$$

LEMMA 10. *Let* $r \geq 2$ *and set* $s = \operatorname{rank}_{\mathbb{Z}}(\Gamma_{\underline{k}})$ *where* $\Gamma_{\underline{k}} = \langle a_1^{k/k_1}, \ldots, a_r^{k/k_r}\rangle$, $\underline{k} = (k_1, \ldots, k_r) \in \mathbb{N}^r$ *and* $k = [k_1, \ldots, k_r]$. *Further let* $P(t)$ *denotes the product of all primes up to* t. *Then we have the following:*

$$\sum_{m \leq z} \sum_{k_1,\ldots,k_r | P(t)} \frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk}, \Gamma_{\underline{k}}^{1/km}) : \mathbb{Q}]} = \delta_{a_1,\ldots,a_r} + O\left(\frac{(\log t)^{2^r-2}}{t} + \frac{1}{z^s}\right) \tag{2·3}$$

where the implied constant may depend on $a_1, \ldots, a_r$.

Proof. Let us start by observing that if $s = \operatorname{rank}_{\mathbb{Z}}(\Gamma_{\underline{k}})$, then

$$\Delta_s(\langle a_1^{k/k_1}, \ldots, a_r^{k/k_r}\rangle) \leq k^{s-1} \times \Delta_s(\langle a_1, \ldots, a_r\rangle).$$

Therefore, in virtue of Lemma 9 and since $\varphi(mk) \geq \varphi(m)\varphi(k)$,

$$\frac{1}{[\mathbb{Q}(\zeta_{mk}, \Gamma_{\underline{k}}^{1/km}) : \mathbb{Q}]} \leq \frac{1}{\varphi(m)m^s} \times \frac{2^s\Delta_s(\Gamma_{\underline{k}})}{\varphi(k)k^s} \ll \frac{1}{\varphi(m)m^s} \times \frac{1}{\varphi(k)\cdot k}.$$

Hence

$$\begin{aligned} S_0 &= \sum_{m > z} \sum_{k_1,\ldots,k_r | P(t)} \frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk}, \Gamma_{\underline{k}}^{1/km}) : \mathbb{Q}]} \\ &\ll \sum_{m>z} \frac{1}{\varphi(m)m^s} \sum_{k | P(t)} \mu(k)^2 \sum_{\substack{k_1,\ldots,k_r \\ k=[k_1,\ldots,k_r]}} \frac{1}{\varphi(k)\cdot k} = O\left(\frac{1}{z^s}\right) \end{aligned} \tag{2·4}$$

since for k squarefree

$$\#\{\underline{k} = (k_1, \ldots, k_r) \in \mathbb{N}^r \text{ such that } k = [k_1, \ldots, k_r]\} = (2^r - 1)^{\omega(k)}$$

and the sequence

$$\sum_{k|P(t)} \frac{(2^r-1)^{\omega(k)}}{\varphi(k)\cdot k}$$

converges as $t \to \infty$.

For a similar reason,

$$\begin{aligned} S_1 &= \sum_{m\le z}\sum_{k>t}\mu(k)^2 \sum_{\substack{k_1,\ldots,k_r\\ k=[k_1,\ldots,k_r]}} \frac{1}{[\mathbb{Q}(\zeta_{mk},\Gamma_{\underline{k}}^{1/km}):\mathbb{Q}]} \\ &\ll \sum_{k>t}\mu(k)^2\frac{(2^r-1)^{\omega(k)}}{\varphi(k)\cdot k} = O\left(\frac{(\log t)^{2^r-2}}{t}\right). \end{aligned} \tag{2·5}$$

The last estimate is standard and it can be obtained for example by induction or also as an application of the Wirsing Theorem.

Finally since

$$\sum_{m\le z}\sum_{k_1,\ldots,k_r|P(t)}\frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk},\Gamma_{\underline{k}}^{1/km}):\mathbb{Q}]} = \delta_{a_1,\ldots,a_r} + O(S_0) + O(S_1),$$

we obtain the claim on summing the estimates of (2·4) and (2·5). □

3. *General case: proof of the Theorem 1*

Let m be a positive integer. We need to consider the auxiliary function:

$$\mathcal{S}_{a_1,\ldots,a_r}(x,m) = \{p\le x \mid \operatorname{ind}_p a_1 = \cdots = \operatorname{ind}_p a_r = m\}.$$

It is immediate that

$$\mathcal{S}_{a_1,\ldots,a_r}(x) = \sum_{m\in\mathbb{N}}\mathcal{S}_{a_1,\ldots,a_r}(x,m). \tag{3·1}$$

Note that for $r=1$, the function $\mathcal{S}_a(x,m)$ was considered by L. Murata in 1991 [10] who proved:

Theorem (Murata). *Let $a\ge 2$ be a squarefree natural number and assume that the GRH holds. Then we have, for any $\epsilon>0$*

$$\#\{p\le x \mid \operatorname{ind}_p a = m\} = \left(c_{a,m} + O\left(\frac{m^\epsilon\log\log x+\log a}{\log x}\right)\right)\operatorname{li}(x)$$

where $c_{a,m}$ is a suitable non negative constant, and the constant implied in the O–symbol may depend on ϵ.

The problem of determining when $c_{a,m}=0$ has been addressed by H. Lenstra [5]. A general expression for the constant $c_{a,m}$ has been obtained by S. Wagstaff [14]. These results and also Theorem 1 are proved using the classical method of Hooley [2].

As a side-product of our Theorem 1, we prove implicitly the following result that generalizes Matthews's Theorem and it is an analogue of Murata's Theorem:

Theorem 11. *Let $\{a_1,\ldots,a_r\}\subset\mathbb{Q}\setminus\{0,\pm1\}$, $m\in\mathbb{N}$, assume that the Generalized Riemann Hypothesis holds and that $r(a_1,\ldots,a_r)\ge 2$. Then*

$$\mathcal{S}_{a_1,\ldots,a_r}(x,m) = \left(c_{a_1,\ldots,a_r,m} + O_{a_1,\ldots,a_r,m}\left(\frac{(\log\log x)^{2^r-2}}{\log x}\right)\right)\operatorname{li}(x)$$

where

$$c_{a_1,\ldots,a_r,m} = \sum_{k_1,\ldots,k_r\in\mathbb{N}}\frac{\mu(k_1)\cdots\mu(k_r)}{\varphi(mk)}\frac{\#\tilde{\Gamma}_{\underline{k}}(mk)}{\#\Gamma_{\underline{k}}(mk)} \tag{3·2}$$

and the notation is the same as in Theorem 1. □

Proof of Theorem 1. We estimate the lowerbound and the upperbound separately. For the upperbound note that if $y \in \mathbb{R}$, with $0 \le y \le x$, then

$$\sum_{m \ge y} \mathcal{S}_{a_1,\dots,a_r}(x,m) \ll \left(\frac{x}{y}\right)^{1+1/s} \frac{1}{\log(x/y)}.$$

Indeed if $\operatorname{ind}_p a_1 = \cdots = \operatorname{ind}_p a_r$, then each a_i generates the same group modulo p. Hence in particular, for each $i = 1,\dots,r$, $\operatorname{ind}_p a_i = \operatorname{ind}_p\langle a_1,\dots,a_r\rangle$. So

$$\begin{aligned}\sum_{m \ge y} \mathcal{S}_{a_1,\dots,a_r}(x,m) &\le \#\left\{p \le x \mid \operatorname{ind}_p\langle a_1,\dots,a_r\rangle > y\right\}\\ &\le \#\left\{p \,\middle|\, \operatorname{ord}_p\langle a_1,\dots,a_r\rangle < \frac{x}{y}\right\} \ll \left(\frac{x}{y}\right)^{1+1/s}\frac{1}{\log(x/y)}\end{aligned}$$

by Lemma 8. Therefore we can take $y = (x\log^s x)^{1/(s+1)}$ obtaining

$$\begin{aligned}\mathcal{S}_{a_1,\dots,a_r}(x) &\le \sum_{m \le y} \mathcal{S}_{a_1,\dots,a_r}(x,m) + O\left(\left(\frac{x}{y}\right)^{1+1/s}\frac{1}{\log(x/y)}\right)\\ &= \sum_{m \le y} \mathcal{S}_{a_1,\dots,a_r}(x,m) + O\left(\frac{x}{(\log x)^2}\right).\end{aligned}$$

For each $t \in \mathbb{R}$, $1 \le t \le x$, we further set

$$\mathcal{S}_{a_1,\dots,a_r}(x,m,t) = \#\left\{p \le x \text{ such that } \forall i = 1,\dots,r, m|\operatorname{ind}_p a_i \text{ and } \left(\frac{\operatorname{ind}_p a_i}{m}, P(t)\right) = 1\right\}$$

where, as usual, $P(t)$ denotes the product of all primes up to t. Note that

$$\mathcal{S}_{a_1,\dots,a_r}(x,m) \le \mathcal{S}_{a_1,\dots,a_r}(x,m,t).$$

Furthermore the inclusion exclusion principle yields

$$\sum_{m \le y} \mathcal{S}_{a_1,\dots,a_r}(x,m,t) = \sum_{m \le y}\sum_{k_1,\dots,k_r|P(t)} \mu(k_1)\cdots\mu(k_r)C_m(x;k_1,\dots,k_r) \tag{3·3}$$

where

$$C_m(x;k_1,\dots,k_r) = \#\{p \le x \text{ such that } mk_i \mid \operatorname{ind}_p a_i\ \forall i = 1,\dots,r\}.$$

Let $k = [k_1,\dots,k_r]$ and apply Lemma 5. We deduce that $mk_i \mid \operatorname{ind}_p a_i$ for $i = 1,\dots,r$ if and only if $mk \mid \operatorname{ind}_p\langle a_1^{k/k_1},\dots,a_r^{k/k_r}\rangle$. Therefore

$$C_m(x;k_1,\dots,k_r) = \#\{p \le x \text{ such that } mk \mid \operatorname{ind}_p\langle a_1^{k/k_1},\dots,a_r^{k/k_r}\rangle\}.$$

The Chebotarev Density Theorem in Lemma 6, implies that (3·3) equals

$$\sum_{m \le y}\sum_{k_1,\dots,k_r|P(t)} \mu(k_1)\cdots\mu(k_r)\left[\frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_{mk},\Gamma_{\underline{k}}^{1/km}) : \mathbb{Q}]} + O_{a_1,\dots,a_r}(\sqrt{x}\log(xmk))\right]$$

where $\Gamma_{\underline{k}} = \langle a_1^{k/k_1},\dots,a_r^{k/k_r}\rangle$. Here we used the fact that $s_{\Gamma_{\underline{k}}} = s_{\langle a_1,\dots,a_r\rangle}$. It is easy to see that

$$\begin{aligned}\sum_{m \le y}\sum_{k_1,\dots,k_r|P(t)} \sqrt{x}\log(xmk) &= \sum_{m \le y} O\big(\sqrt{x}2^{tr}\log(xmP(t))\big)\\ &= O\left(x^{(s+3)/(2s+2)}2^{tr}\log^2(xP(t))\right).\end{aligned}$$

Therefore, since $s = r(a_1, \dots, a_r) \ge 2$,

$$\begin{aligned}\mathcal{S}_{a_1,\dots,a_r}(x) &\le \left(\sum_{m\le y}\ \sum_{k_1,\dots,k_r\mid P(t)} \frac{\mu(k_1)\cdots\mu(k_r)}{[\mathbb{Q}(\zeta_{mk},\Gamma^{1/km}):\mathbb{Q}]} + O\left(\frac{1}{\log x}\right)\right)\operatorname{li}(x)\\ &= \left(\delta_{a_1,\dots,a_r} + O\left(\frac{(\log t)^{2^r-2}}{t} + \frac{2^{tr}\log^3(xP(t))}{x^{(s-1)/(2s+2)}} + \frac{1}{\log x}\right)\right)\operatorname{li}(x)\end{aligned}$$

in virtue of Lemma 10 and of the previous discussion. If we choose $t = \log x/(7r\log 2)$, we obtain the upperbound estimate.

As for the lowerbound let $z \in \mathbb{R}$, with $1 \le z \le x$. It is clear that

$$\mathcal{S}_{a_1,\dots,a_r}(x) \ge \sum_{m\le z}\mathcal{S}_{a_1,\dots,a_r}(x,m). \tag{3·4}$$

From the same argument as above we deduce that

$$\sum_{m\le z}\mathcal{S}_{a_1,\dots,a_r}(x,m) = \left[\delta_{a_1,\dots,a_r} + O\left(\frac{(\log\log x)^{2^r-2}}{\log x} + \frac{1}{z^s} + \frac{z\log^3 x}{x^{1/42}}\right)\right]\operatorname{li}(x) + E(x,z) \tag{3·5}$$

where if $t = \log x/(7r\log 2)$, then

$$E(x,z) = O\left(\sum_{m\le z}\#\left\{p\le x \text{ such that } \exists i, l>t, lm\mid \operatorname{ind}_p a_i\right\}\right).$$

In order to estimate the above, for each η_1, η_2 with $t \le \eta_1 < \eta_2 \le x$, we define:

$$E_i(x,m;\eta_1,\eta_2) = \#\left\{p\le x \text{ such that } \exists l\in(\eta_1,\eta_2],\ lm\mid \operatorname{ind}_p a_i\right\}.$$

So

$$E(x,z) \le \sum_{m\le z}\sum_{i=1}^{r}[E_i(x,m;t,\eta) + E_i(x,m;\eta,x)].$$

Note that

$$E_i(x,m;\eta,x) \le \left\{p \text{ such that } \operatorname{ord}_p a_i < \frac{x}{m\eta}\right\}.$$

Applying Lemma 8, we deduce that

$$\sum_{i=1}^{r}\sum_{m\le z}E_i(x,m;\eta,x) \ll \sum_{m\le z}\left(\frac{x}{m\eta}\right)^{1+1/s}\frac{1}{\log(x/m\eta)} = O\left(\frac{x}{\log^2(x/z)}\right), \tag{3·6}$$

if we choose $\eta = (x\log^s x)^{1/(s+1)}$.

To estimate the first term, we use again the Chebotarev Density Theorem in the form given by Lemma 6 and also Lemma 9. So

$$\begin{aligned}\sum_{i=1}^{r}\sum_{m\le z}E_i(x,m;t,\eta) &\le \sum_{i=1}^{r}\sum_{m\le z}\sum_{l\in(t,\eta]}\left(\frac{\operatorname{li}(x)}{[\mathbb{Q}(\zeta_{ml},a_i^{1/ml}):\mathbb{Q}]} + O(\sqrt{x}\log(xml))\right)\\ &= O_{a_1,\dots a_r}\left(\operatorname{li}(x)\sum_{m\le z}\sum_{l>t}\frac{1}{m\varphi(m)}\frac{1}{l^2-l} + \sum_{l<\eta}\sqrt{x}z\log(xzl)\right)\\ &= O_{a_1,\dots a_r}\left(\frac{\operatorname{li}(x)}{t} + \eta\sqrt{x}\log(xz\eta)\right).\end{aligned}$$

To conclude the proof of Theorem 1 it is enough to choose $z = \log x$. □

4. *Degenerate case: proof of Theorem 2 and Corollary 3*

Let

$$\mathcal{N}_a(x,k) = \#\{p \le x \text{ such that } k \mid \operatorname{ord}_p a\}.$$

The function $\mathcal{N}_a(x,k)$ has been studied by several authors: Ballot, Hasse, Moree, Odoni, Pappalardi, Wiertelak and maybe others. Wiertelak [15] was the first to obtain an asymptotic formula for $\mathcal{N}_a(x,k)$ (see also [11]). The proof of Theorem 2 requires the most general result due to Moree [8, Theorem 2].

Lemma 12. *Let $k \in \mathbb{N}^+$ be squarefree and $a \in \mathbb{Q} \setminus \{0, \pm 1\}$. Then the following asymptotic formula holds:*

$$\mathcal{N}_a(x,k) = \left(\kappa_{a,k} + O_{a,k}\left(\frac{(\log\log x)^{\omega(k)+3}}{(\log x)^2}\right)\right) \operatorname{li}(x).$$

Here

$$\kappa_{a,k} = (1+\varepsilon) \prod_{l \mid k} \frac{l^{1-v_l(d)}}{l^2-1} \tag{4·1}$$

where if we write $a = \pm b^d$ with $b \in \mathbb{Q}^{>0}$ not a perfect power, $D(b) = \operatorname{disc}(\mathbb{Q}(\sqrt{b}))$,

$$\varepsilon = \begin{cases} \frac{3(1-\operatorname{sgn}(a))(2^{v_2(d)}-1)}{4} + \varepsilon_a & \textit{if } 2 \mid k \textit{ and } D(b) \mid 4k; \\ \frac{3(1-\operatorname{sgn}(a))(2^{v_2(d)}-1)}{4} & \textit{if } 2 \mid k \textit{ and } D(b) \nmid 4k; \\ 0, & \textit{if } 2 \nmid k \end{cases}$$

and

$$\varepsilon_a = \begin{cases} \left(-\frac{1}{2}\right)^{2^{\max\{0, v_2(D(b)/d)-1\}}} & \textit{if } a > 0; \\ \left(-\frac{1}{2}\right)^{2^{2-\max\{1, v_2(D(b)/d)\}}} & \textit{if } a < 0 \textit{ and } v_2(D(b)) \ne v_2(8d); \\ \frac{1}{16} & \textit{if } a < 0 \textit{ and } v_2(D(b)) = v_2(8d). \end{cases}$$

Proof of Theorem 2. We use the general property that $\operatorname{ord}_p a^s = \operatorname{ord}_p a/(s, \operatorname{ord}_p a)$ and we observe that when $(h_1, \dots, h_r) = 1$ the condition $(h_i, \operatorname{ord}_p a) = (h_j, \operatorname{ord}_p a)$ for all $i, j = 1, \dots, r$ is equivalent to $(h_i, \operatorname{ord}_p a) = 1$ for $i = 1, \dots, r$. The latter condition is equivalent to $(h, \operatorname{ord}_p a) = 1$ where $h = [h_1, \dots, h_r]$. Therefore by the inclusion exclusion principle,

$$\begin{aligned} \mathcal{S}_{a^{h_1},\dots,a^{h_r}}(x) &= \{p \le x \text{ such that } (h, \operatorname{ord}_p a) = 1\} \\ &= \sum_{k \mid h} \mu(k) \#\{p \le x \text{ such that } k \mid \operatorname{ord}_p a\}. \end{aligned}$$

The function above has also been considered by Wiertelak [16] in the special case when a is a positive integer. By Lemma 12, we have

$$\begin{aligned} S_{a^{h_1},\dots,a^{h_r}}(x) &= \sum_{k \mid h} \mu(k) \left(\kappa_{a,k} + O_{a,h}\left(\frac{(\log\log x)^{\omega(h)+3}}{(\log x)^2}\right)\right) \operatorname{li}(x) \\ &= \left(\delta_{a^{h_1},\dots,a_r^{h_r}} + O_{a,h}\left(\frac{(\log\log x)^{\omega(h)+3}}{(\log x)^2}\right)\right) \operatorname{li}(x) \end{aligned}$$

where

$$\delta_{a^{h_1},\dots,a_r^{h_r}} = \sum_{k|h} \mu(k)(1+\varepsilon) \prod_{l|k} \frac{l^{1-v_l(d)}}{l^2-1}.$$

The above equals $\Sigma_1 + \Sigma_2 + \Sigma_3$ where

$$\Sigma_1 = \sum_{k|h} \mu(k) \prod_{l|k} \frac{l^{1-v_l(d)}}{l^2-1} = \prod_{l|h} \left(1 - \frac{l^{1-v_l(d)}}{l^2-1}\right), \tag{4·2}$$

$$\begin{aligned}\Sigma_2 &= \frac{(3(1-\operatorname{sgn}(a))(2^{v_2(d)}-1)}{4} \sum_{\substack{k|h\\2|k}} \mu(k) \prod_{l|k} \frac{l^{1-v_l(d)}}{l^2-1} \\ &= t_{2,h} \times \frac{\operatorname{sgn}(a)-1}{2} \times \frac{3\cdot 2^{v_2(d)}-3}{3\cdot 2^{v_2(d)}-2} \times \prod_{l|h}\left(1-\frac{l^{1-v_l(d)}}{l^2-1}\right) \\ &= t_{2,h} \times s_a \times \prod_{l|h}\left(1-\frac{l^{1-v_l(d)}}{l^2-1}\right) \end{aligned} \tag{4·3}$$

and

$$\Sigma_3 = \varepsilon_a \times \sum_{\substack{k|h\\2|k\\D(b)|4k}} \mu(k) \prod_{l|k} \frac{l^{1-v_l(d)}}{l^2-1}. \tag{4·4}$$

The conditions $2 \mid k$, $D(b) \mid 4k$ are equivalent to the condition $[2, D(b)/(D(b),4)] \mid k$. Furthermore the integer $[2, D(b)/(D(b),4)]$ is squarefree and equals the product of the primes dividing $2D(b)$. Therefore the sum on the right hand side above equals

$$t_{2,h} \times t_{D(b),4h} \times \prod_{l|2D(d)} \frac{-l^{1-v_l(d)}}{l^2-1}\left(1-\frac{l^{1-v_l(d)}}{l^2-1}\right)^{-1} \times \prod_{l|h}\left(1-\frac{l^{1-v_l(d)}}{l^2-1}\right). \tag{4·5}$$

Adding up the expression in (4·2),(4·3),(4·4) and ε_a times (4·5) we obtain the formula for $\delta_{a^{h_1},\dots,a^{h_r}}$ in the statement of Theorem 2. □

Proof of Corollary 3. Note that

$$\prod_{l|h}\left(1-\frac{l^{1-v_l(d)}}{l^2-1}\right) \neq 0$$

so, in order for $\delta_{a^{h_1},\dots,a^{h_r}} = 0$, we should have $2 \mid h$ so that $t_{2,h} = 1$ and

$$s_a + t_{D(b),4h} \times \varepsilon_a \prod_{l|2D(b)} \frac{1}{\left(1-\frac{l^2-1}{l^{1-v_l(d)}}\right)} = -1. \tag{4·6}$$

In the case when $a > 0$, $s_a = 0$ and identity (4·6) boils down to

$$\prod_{l|2D(b)} \left(\frac{l - l^{v_l(d)}(l^2-1)}{l}\right) = -t \times \varepsilon_a = -t \times \left(-\frac{1}{2}\right)^{2^\nu} \tag{4·7}$$

where $\nu \in \{0,1,2\}$ and $t \in \{0,1\}$. First note that the left hand side of (4·7) is in absolute value larger than 1/2. Indeed, we have that

$$\frac{l^{v_l(d)}(l^2-1)-l}{l}\begin{cases} > 1 & \text{if } l>2 \text{ or if } l=2 \text{ and } v_2(d)>0;\\ = \frac{1}{2} & \text{if } l=2 \text{ and } v_2(d)=0.\end{cases}$$

This implies that in order for equality (4·7) to be satisfied we must have $\nu=0$ and $t=1$. But this also implies that $2D(b)=16$ and therefore the left hand side of (4·7) is $-1/2$ while the right hand side is $1/2$.

In the case when $a<0$ identity (4·6) after some calculation boils down to

$$\prod_{\substack{l\mid D(b)\\ l>2}}\left(\frac{l-l^{v_l(d)}(l^2-1)}{l}\right)=2t\times\left(-\frac{1}{2}\right)^{2^\nu}, \tag{4·8}$$

where $\nu\in\{0,1,2\}$, $t\in\{0,1\}$. This forces $t=1$ and $\nu=0$ for otherwise the right hand side of (4·8) would have as denominator a power of 2 which cannot happen on the left hand side. By a similar argument to the above we arrive to a contradiction. This concludes the proof of Corollary 3. □

5. *The Euler product expansion for the density: proof of Theorem 4*

In this section we want to express the density

$$\delta_{a_1,\ldots,a_r}=\sum_{\substack{m\in\mathbb{N}\\ \underline{k}\in\mathbb{N}^r}}\frac{\mu(\underline{k})}{\varphi(mk)}\frac{\#\tilde{\Gamma}_{\underline{k}}(mk)}{\#\Gamma_{\underline{k}}(mk)}$$

as an Euler product. This will allow to compute it with high precision in several cases.

If mk is odd then $\tilde{\Gamma}_{\underline{k}}(mk)$ is trivial while if mk is even any element $\xi\mathbb{Q}^{*mk}\in\tilde{\Gamma}_{\underline{k}}(mk)$ can be written uniquely as $\xi\mathbb{Q}^{*mk}=d^{mk/2}\mathbb{Q}^{*mk}$ where $d\mid s_\Gamma$ (note that here we allow d to be negative in the case when Γ contains also negative rational numbers).

Given a (possibly negative) divisor $d\mid s_\Gamma$, the condition $d^{mk/2}\mathbb{Q}^{*mk}\in\tilde{\Gamma}_{\underline{k}}(mk)$ is equivalent to $D(d)=\operatorname{disc}(\mathbb{Q}(\sqrt{d}))\mid mk$ and $d^{2^{v_2(mk)-1}}\mathbb{Q}^{*2^{v_2(mk)}}\in\Gamma_{\underline{k}_2}(2^{v_2(mk)})$ (here $(\underline{k}_2:=((2,k_1),\ldots,(2,k_r)))$.

With these positions we can rewrite the density as follows:

$$\delta_{a_1,\ldots,a_r}=\sum_{\substack{m\in\mathbb{N}\\ \underline{k}\in\mathbb{N}^r\\ mk\text{ odd}}}\frac{\mu(\underline{k})}{\varphi(mk)\#\Gamma_{\underline{k}}(mk)}+\sum_{d\mid s_\Gamma}\sum_{\substack{m\in\mathbb{N}\\ \underline{k}\in\mathbb{N}^r\\ (m,\underline{k})\in\mathcal{T}_d}}\frac{\mu(\underline{k})}{\varphi(mk)\#\Gamma_{\underline{k}}(mk)}.$$

where

$$\mathcal{T}_d:=\left\{(m,\underline{k})\in\mathbb{N}^{r+1}\text{ such that }2\mid mk,\tilde{d}(v_2(mk))\in\tilde{\Gamma}_{\underline{k}_2}(2^{v_2(mk)})\text{ and }D(d)\mid mk\right\}$$

where we used the notations $\tilde{d}(N):=d^{2^{N-1}}\mathbb{Q}^{*2^N}$.

Let us write $m=m'm''$ and $k_i=k_i'k_i''$ for $i=1,\ldots,r$ where $\gcd(m'[k_1',\ldots,k_r'],d)=1$ and for each prime $l\mid m''[k_1'',\ldots,k_r''], l\mid d$. Then

$$\Gamma_{\underline{k}}(mk)\cong\Gamma_{k_1',\ldots,k_r'}(m'[k_1',\ldots,k_r'])\times\Gamma_{k_1'',\ldots,k_r''}(m''[k_1'',\ldots,k_r'']).$$

Therefore $\delta_{a_1,\dots,a_r} = \delta' \cdot \delta''$ where

$$\delta' = 1 + \sum_{d \mid s_\Gamma} \frac{\displaystyle\sum_{\substack{(m,\underline{k}) \in \mathcal{T}_d \\ c(mk) \mid 2d}} \frac{\mu(\underline{k})}{\varphi(mk)\#\Gamma_{\underline{k}}(mk)}}{\displaystyle\sum_{\substack{(m,\underline{k}) \in \mathbb{N}^{r+1} \\ c(mk) \mid d,\ mk \text{ odd}}} \frac{\mu(\underline{k})}{\varphi(mk)\#\Gamma_{\underline{k}}(mk)}}$$

with $c(n) = \prod_{l \mid n} l$, and

$$\delta'' = \sum_{\substack{m \in \mathbb{N} \\ \underline{k} \in \mathbb{N}^r \\ mk \text{ odd}}} \frac{\mu(\underline{k})}{\varphi(mk)} \frac{1}{\#\Gamma_{\underline{k}}(mk)} = \prod_{l>2} \left(\sum_{\alpha=0}^{\infty} \left(\frac{1}{\varphi(l^\alpha)\Gamma(l^\alpha)} + \frac{1}{\varphi(l^{\alpha+1})} \sum_{\substack{I \in \{1,l\}^r \\ I \neq (1,\dots,1)}} \frac{(-1)^{p(I)}}{\#\Gamma_I(l^{\alpha+1})} \right) \right)$$

$$= \prod_{l>2} \left(\sum_{\alpha=0}^{\infty} \left(\frac{1}{\varphi(l^\alpha)\#\Gamma(l^\alpha)} - \frac{1}{\varphi(l^{\alpha+1})\#\Gamma(l^{\alpha+1})} + \sum_{I \in \{1,l\}^r} \frac{(-1)^{p(I)}}{\varphi(l^{\alpha+1})\#\Gamma_I(l^{\alpha+1})} \right) \right)$$

$$= \prod_{l>2} \left(1 + \frac{1}{l-1} \sum_{\alpha=0}^{\infty} \frac{1}{l^\alpha} \sum_{I \in \{1,l\}^r} \frac{(-1)^{p(I)}}{\#\Gamma_I(l^{\alpha+1})} \right)$$

where $p(I)$ denotes the number of l's in the sequence $I \in \{1,l\}^r$.

If we denote

$$\Lambda_l = \frac{1}{l-1} \sum_{\alpha=0}^{\infty} \frac{1}{l^\alpha} \sum_{I \in \{1,l\}^r} \frac{(-1)^{p(I)}}{\#\Gamma_I(l^{\alpha+1})} \tag{5·1}$$

then

$$\delta' = 1 + {\sum_{d \mid s_\Gamma}}' \Theta(d) \prod_{p \mid d} \frac{\Lambda_p}{1 + \Lambda_p}$$

where $\sum'_{d \mid s_\Gamma}$ means that if Γ contains also negative numbers then the sum is extended also to negative divisors of s_Γ and if $v = \max\{1, v_2(D(d))\}$,

$$\Theta_d = \sum_{\substack{\beta \in \{0,1\} \\ \alpha \geq v-\beta}} \frac{1}{\varphi(2^{\alpha+\beta})} \sum_{\substack{I \in \{1,2\}^r \\ [I] = 2^\beta \\ \tilde{d}(\alpha+\beta) \in \Gamma_I(2^{\alpha+\beta})}} \frac{(-1)^{p(I)}}{\#\Gamma_I(2^{\alpha+\beta})}$$

$$= \sum_{\substack{\alpha \geq v \\ \tilde{d}(\alpha) \in \Gamma(2^\alpha)}} \frac{1}{2^{\alpha-1}\#\Gamma(2^\alpha)} + \sum_{\alpha \geq v-1} \frac{1}{2^\alpha} \sum_{\substack{I \in \{1,2\}^r \\ I \neq (\underline{1}) \\ \tilde{d}(\alpha+1) \in \Gamma_I(2^{\alpha+1})}} \frac{(-1)^{p(I)}}{\#\Gamma_I(2^{\alpha+1})}$$

$$= \sum_{\alpha \geq v-1} \frac{1}{2^\alpha} \sum_{\substack{I \in \{1,2\}^r \\ \tilde{d}(\alpha+1) \in \Gamma_I(2^{\alpha+1})}} \frac{(-1)^{p(I)}}{\#\Gamma_I(2^{\alpha+1})}. \tag{5·2}$$

We have therefore proven the following:

THEOREM 13. *For every prime l let Λ_l be defined as in (5·1) and for every $d \mid s_\Gamma$ let*

Θ_d be defined as in (5·2). Then

$$\delta_{a_1,\dots,a_r} = \left(\prod_{l>2}(1+\Lambda_l)\right)\cdot\left(1+\sum_{d\mid s_\Gamma}\Theta_d\prod_{\substack{l\mid d\\ l>2}}\frac{\Lambda_l}{1+\Lambda_l}\right).$$

We can apply the above statement to the case when the a_i's are distinct primes:

Proof of Theorem 4. For all $\alpha\in\mathbb{N}$, $\#\Gamma_{(1,\dots,1)}(l^{\alpha+1}) = \#\Gamma(l^{\alpha+1}) = l^{r(\alpha+1)}$ while if $I\neq(1,\dots,1)$, then $\#\Gamma_I(l^{\alpha+1}) = l^{r\alpha+p(I)}$. Therefore

$$\sum_{I\in\{1,l\}^r}\frac{(-1)^{p(I)}}{\#\Gamma_I(l^{\alpha+1})} = \frac{1}{l^{r(\alpha+1)}}-\frac{1}{l^{r\alpha}}+\sum_{I\in\{1,l\}^r}\frac{(-1)^{p(I)}}{l^{r\alpha+p(I)}} = \frac{1-l^r+(l-1)^r}{l^{r(\alpha+1)}}$$

which leads to

$$\Lambda_l = -\frac{l(l^r-(l-1)^r-1)}{(l-1)(l^{r+1}-1)}.$$

Furthermore for every $\alpha\geq 1$ we have that $\tilde{d}(\alpha+1)\in\Gamma_I(2^{\alpha+1})$ while $\tilde{d}(1)\in\Gamma_I(2)$ if and only if $d = p_{j_1}\cdots p_{j_t}$ and $I=(i_1,\dots,i_r)$ then $i_{j_1}=\cdots=i_{j_t}=2$.

Hence $\Theta_1=\Lambda_2$ and if $d\neq 1$ and $v=1$ then

$$\Theta_d = \Lambda_2+1-\frac{1}{2^{r-1}}+\sum_{\substack{I\in\{1,2\}^r\\ \tilde{d}(1)\in\Gamma_I(2)}}\frac{(-1)^{p(I)}}{\#\Gamma_I(2)} = \Lambda_2+1-\frac{1}{2^r}\left(1-\mu(d)\right).$$

If $v\neq 1$ so that $d\neq 1$,

$$\Theta_d = \Lambda_2-\sum_{\alpha\leq v-2}\frac{1}{2^\alpha}\sum_{I\in\{1,2\}^r}\frac{(-1)^{p(I)}}{\#\Gamma_I(2^{\alpha+1})} = \begin{cases}\Lambda_2+1-\frac{1}{2^{r-1}} & \text{if } v=2;\\ \Lambda_2+1-\frac{1}{2^r}\left[\frac{3}{2}+\frac{1}{2^r}\right] & \text{if } v=3.\end{cases}$$

Finally, by Theorem 13

$$\delta_{p_1,\dots,p_r} = \prod_l(1+\Lambda_l)\cdot\left(1+\sum_{\substack{d\mid p_1\cdots p_r\\ d\neq 1}}\frac{\Theta_d}{1+\Lambda_2}\prod_{\substack{l\mid d\\ l>2}}\left(\frac{\Lambda_l}{1+\Lambda_l}\right)\right).$$

Since $1+\Lambda_2 = 3/(2^{r+1}-1)$ and since

$$\Theta_d/(1+\Lambda_2) = \begin{cases}1-\frac{(2-2^{-r})}{3}(1-\mu(d)) & \text{if } d\equiv 1 \bmod 4, d\neq 1;\\ 1-\frac{2-2^{-r}}{3}\cdot 2 & \text{if } d\equiv 3 \bmod 4;\\ 1-\frac{2-2^{-r}}{3}\left(\frac{3}{2}+\frac{1}{2^r}\right) & \text{if } d\equiv 2 \bmod 4,\end{cases}$$

after calculations we obtain the statement and this concludes the proof. □

6. *Numerical examples*

In this section we compare numerical data. Table 1 compares the densities $\delta_{a,a^{q_1},\dots,a^{q_s}}$ with $\mathcal{S}_{a,a^{q_1},\dots,a^{q_s}}(10^8)/\pi(10^8)$ where $q_1=2,\dots,q_s$ is the i–th prime, $s=1,\dots,6$ and $a\in\mathbb{Q}\setminus\{0,\pm1\}$ with natural height up to 6.

Table 2 compares the densities $\delta_{p_1,\dots,p_r}$ with $\mathcal{S}_{p_1,\dots,p_r}(10^8)/\pi(10^8)$ where $\{p_1,\dots,p_r\}$ ranges over the subsets of $\{2,3,5,7,11\}$ with $r\geq 2$.

The value of each quantity in the tables has been truncated at the fifth decimal digit.

Table 1. $\delta_{a,a^{q_1},\ldots,a^{q_s}}$ *versus* $\mathcal{S}_{a,a^{q_1},\ldots,a^{q_s}}(10^8)/\pi(10^8)$

$a \setminus q_s$	2	3	5	7	11	13
2	0.29165 0.29166	0.18226 0.18229	0.14429 0.14431	0.12325 0.12326	0.11198 0.11196	0.10334 0.10330
-2	0.29164 0.29166	0.18228 0.18229	0.14429 0.14431	0.12325 0.12326	0.11200 0.11196	0.10332 0.10330
3	0.33336 0.33333	0.27084 0.27083	0.21445 0.21440	0.18322 0.18314	0.16645 0.16635	0.15360 0.15348
-3	0.33335 0.33333	0.08334 0.08333	0.06597 0.06597	0.05635 0.05635	0.05118 0.05118	0.04721 0.04722
3/2	0.33338 0.33333	0.22401 0.22395	0.17732 0.17730	0.15145 0.15144	0.13751 0.13756	0.12687 0.12691
-3/2	0.33331 0.33333	0.22398 0.22395	0.17729 0.17730	0.15152 0.15144	0.13768 0.13756	0.12707 0.12691
4	0.58330 0.58333	0.36454 0.36458	0.28858 0.28862	0.24651 0.24653	0.22398 0.22393	0.20666 0.20660
-4	0.33333 0.33333	0.20832 0.20833	0.16490 0.16493	0.14082 0.14087	0.12788 0.12796	0.11797 0.11806
3/4	0.33330 0.33333	0.27083 0.27083	0.21443 0.21440	0.18323 0.18134	0.16643 0.16635	0.15355 0.15348
-3/4	0.33335 0.33333	0.08332 0.08333	0.06593 0.06597	0.05634 0.05635	0.05119 0.05118	0.04723 0.04722
5	0.33323 0.33333	0.20826 0.20833	0.12157 0.12152	0.10384 0.10380	0.09437 0.09428	0.08709 0.08699
-5	0.33342 0.33333	0.20833 0.20833	0.18661 0.18663	0.15941 0.15941	0.14476 0.14480	0.13354 0.13359
2/5	0.33325 0.33333	0.20837 0.20833	0.17037 0.17035	0.14557 0.14551	0.13226 0.13217	0.12203 0.12194
-2/5	0.33342 0.33333	0.20835 0.20833	0.17036 0.17035	0.14554 0.14551	0.13219 0.13217	0.12196 0.12194
3/5	0.33326 0.33333	0.20831 0.20833	0.15190 0.15190	0.12970 0.12975	0.11780 0.11786	0.10863 0.10874
-3/5	0.33344 0.33333	0.20836 0.20833	0.19099 0.19097	0.16324 0.16312	0.14827 0.14816	0.13679 0.13670
4/5	0.33337 0.33333	0.20837 0.20833	0.12163 0.12152	0.10392 0.10380	0.09440 0.09428	0.08709 0.08699
-4/5	0.33331 0.33333	0.20823 0.20833	0.18654 0.18663	0.15936 0.15941	0.14476 0.14480	0.13357 0.13359
6	0.33330 0.33333	0.22398 0.22395	0.17721 0.17730	0.15135 0.15144	0.13747 0.13756	0.12687 0.12691
-6	0.33335 0.33333	0.22399 0.22395	0.17733 0.17730	0.15156 0.15144	0.13769 0.13756	0.12707 0.12691
5/6	0.33328 0.33333	0.20840 0.20833	0.16172 0.16167	0.13813 0.13809	0.12545 0.12543	0.11572 0.11573
-5/6	0.33322 0.33333	0.20823 0.20833	0.16157 0.16167	0.13799 0.13809	0.12538 0.12543	0.11570 0.11573

Table 2. $\delta_{p_1,\dots,p_r}$ *versus* $\mathcal{S}_{p_1,\dots,p_r}(10^8)/\pi(10^8)$

$p_1,\dots,p_r$		$p_1,\dots,p_r$		$p_1,\dots,p_r$	
$2,3$	0.28295 0.28287	$2,5$	0.27207 0.27213	$2,7$	0.26976 0.26972
$2,11$	0.26844 0.26851	$3,5$	0.28973 0.28959	$3,7$	0.29237 0.29224
$3,11$	0.28908 0.28912	$5,7$	0.27904 0.27913	$5,11$	0.27796 0.27793
$7,11$	0.27617 0.27625				
$2,3,5$	0.11345 0.11336	$2,3,7$	0.11666 0.11656	$2,3,11$	0.11362 0.11366
$2,5,7$	0.10329 0.10327	$2,5,11$	0.10237 0.10239	$2,7,11$	0.10074 0.10081
$3,5,7$	0.11894 0.11893	$3,5,11$	0.11599 0.11604	$3,7,11$	0.11949 0.11942
$5,7,11$	0.10526 0.10529				
$2,3,5,7$	0.05232 0.05230	$2,3,5,11$	0.05041 0.05038	$2,3,7,11$	0.05306 0.05302
$2,5,7,11$	0.04378 0.04377	$3,5,7,11$	0.05379 0.05378	$2,3,5,7,11$	0.02480 0.02479

7. *Conclusion*

It would be interesting to determine (even conjecturally) a characterization of those finite sets of rational numbers for which the SW problem has an affirmative answer. We are unable to do that at present time but it is reasonable to expect that the SW problem has an affirmative answer for $\{a_1,\dots,a_r\}$ if and only if $\delta_{a_1,\dots,a_r}\neq 0$.

We are also unable to characterize the finite sets for which $\delta_{a_1,\dots,a_r}\neq 0$ (which in virtue of Theorem 1 provides on GRH a sufficient condition for the SW problem to have affirmative answer).

However we have the following elementary result:

Proposition 14. *Let* $\{a_1,\dots,a_r\}\subset\mathbb{Q}^*\setminus\{0,\pm1\}$ *be such that the following properties are both satisfied:*

(i) there exist $\omega_1,\dots,\omega_r\in\mathbb{Z}$ *with* $a_1^{\omega_1}\cdots a_r^{\omega_r}=-1$*;*
(ii) there exist $\nu_1,\dots,\nu_r\in\mathbb{Z}$ *with* $\nu_1+\cdots+\nu_r$ *is odd and* $a_1^{\nu_1}\cdots a_r^{\nu_r}=1$.

Then the Schinzel–Wójcik problem for $a_1,\dots,a_r$ *has a negative answer.*

Proof. Assume that $\delta=\operatorname{ord}_p a_1=\ldots=\operatorname{ord}_p a_r$ for some $p>2$. Since $-1=a_1^{\omega_1}\cdots a_r^{\omega_r}$ for suitable $\omega_1,\dots,\omega_r\in\mathbb{Z}$, we have $(-1)^\delta\equiv a_1^{\delta\omega_1}\cdots a_r^{\delta\omega_r}\equiv 1 \bmod p$. This implies that $2\mid\delta$, so for each $i=1,\dots,r$, $a_i^{\delta/2}\equiv -1 \bmod p$. Therefore we have that $1=(a_1^{\nu_1}\cdots a_r^{\nu_r})^{\delta/2}\equiv(-1)^{\nu_1+\cdots+\nu_r} \bmod p$ which is a contradiction to the second hypothesis. □

Note that the two conditions of Proposition 14 can be satisfied simultaneously only if $r\geq 3$. The second condition in Proposition 14 implies in particular that the Matthews constant $C(a_1,\dots,a_r)$ in the introduction is zero.

The only case which is not covered neither by Theorem 1 or by Theorem 2 is when the rank $r(a_1, \ldots, a_r) = 1$ and $-1 \in \langle a_1, \ldots, a_r \rangle$. From Proposition 14 we deduce that this case includes some cases for which the SW problem has negative answer.

A weaker analogue of the SW problem is the question of whether there exist infinitely many primes p such that $\operatorname{ord}_p a_1 \mid \operatorname{ord}_p a_2 \mid \cdots \mid \operatorname{ord}_p a_r$. Maybe there are examples where this problem has affirmative answer, whereas the SW problem has negative answer. For $r = 2$ this problem has been considered by Moree and Stevenhagen [9]. They prove that if $a = a_1/a_2$ and $b = b_1/b_2$, $((a_1, a_2) = (b_1, b_2) = 1)$ are multiplicatively independent rationals, then the set of primes such that $\operatorname{ord}_p a \mid \operatorname{ord}_p b$ is infinite and is equal to the set of primes dividing at least one term of the sequence $b_2\ a_1^n - b_1\ a_2^n$, $n \geq 1$. This is a special case of a theorem due to Pólya. Under GRH this set has a positive density.

Acknowledgement. The authors would like to thank C. David, A. Granville, P. Moree and A. Schinzel for their useful comments. Both authors were sponsored in part by GNSAGA from INDAM.

REFERENCES

[**1**] L. Cangelmi and F. Pappalardi. On the r–rank Artin Conjecture, II. *J. Number Theory* **75** (1999) 120–132.

[**2**] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.* **225** (1967) 209–220.

[**3**] J. C. Lagarias and A. M. Odlyzko. *Effective versions of the Chebotarev density theorem.* Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 409–464. Academic Press, London, 1977.

[**4**] S. Lang. *Algebra. 2nd edition.* Addison-Wesley Publishing Company, Advanced Book Program Reading, MA, 1984. xv+714.

[**5**] H. W. Lenstra Jr. On Artin's conjecture and Euclid's algorithm in global fields. *Invent. Math.* **42** (1977) 201–224.

[**6**] C. R. Matthews. Counting points modulo p for some finitely generated subgroups of algebraic groups. *Bull. London Math. Soc.* **14** (1982) 149–154.

[**7**] K. R. Matthews. A generalisation of Artin's conjecture for primitive roots. *Acta Arith.* **29** (1976) no. 2 113–146.

[**8**] P. Moree. On primes p for which d divides $\operatorname{ord}_p(g)$. *Funct. Approx. Comment. Math.* **33** (2005) 85–95.

[**9**] P. Moree and P. Stevenhagen. A two-variable Artin conjecture. *J. Number Theory* **85** (2000) no. 2 291–304.

[**10**] L. Murata. A problem analogous to Artin's conjecture for primitive roots and its applications. *Arch. Math. (Basel)* **57** (1991) no. 6 555–565.

[**11**] F. Pappalardi. Square free values of the order fuction. *New York J. Math.* **9** (2003) 331–344.

[**12**] A. Schinzel and W. Sierpinski. Sur certaines hypothéses concernant les nombres premiers. *Acta Arith.* **4** (1958) 185–208; Erratum ibid. **5** (1959), 259.

[**13**] A. Schinzel and J. Wòjcik. On a problem in elementary number theory. *Math. Proc. Cambridge Philos. Soc.* **112** (1992) no. 2 225–232.

[**14**] S. S. Wagstaff Jr. Pseudoprimes and a generalization of Artin's conjecture. *Acta Arith.* **41** (1982) no. 2 141–150.

[**15**] K. Wiertelak. On the density of some sets of primes p, for which $n| \operatorname{ord}_p a$. *Funct. Approx. Comment. Math.* **28** (2000) 237–241.

[**16**] K. Wiertelak. On the density of some sets of primes p, for which $(\operatorname{ord}_p b, n) = d$. *Funct. Approx. Comment. Math.* **21** (1992) 69–73.

[**17**] J. Wójcik. On a problem in algebraic number theory. *Math. Proc. Cambridge Philos. Soc.* **119** (1996) no. 2 191–200.