数理解析研究所講究録
1511 巻 2006 年 129-135

ON A PROBLEM OF SCHINZEL AND WÓJCIK

FRANCESCO PAPPALARDI AND ANDREA SUSA

for the Proceedings of the Analytic Number Theory Meeting - RIMS, Kyoto October 2004

ABSTRACT. Given $a_1, \dots, a_r \in \mathbb{Q} \setminus \{0, \pm 1\}$, the Schinzel–Wójcik problem is to determine whether there exist infinitely many primes p for which the order modulo p of each $a_1, \dots, a_r$ coincides. We propose some results about this problem. For example, the first result is that on the GRH, the primes with this property have a density. The second is that in the special case when each a_i is a power of a fixed rational number, the density exists unconditionally and it is non zero.

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 as

$$\mathrm{ord}_p(a) = \min\left\{k \in \mathbf{N} \mid a^k \equiv 1 \bmod p\right\}.$$

In 1992 Schinzel and Wójcik [5] 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) $\mathrm{ord}_p(a) = \mathrm{ord}_p(b)$.

Clearly the first condition is satisfied for all but finitely many primes and the second is the important one. Whenever we use the symbol $\mathrm{ord}_p(a)$, 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*
>
> $$\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = \mathrm{ord}_p(c)?$$

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

$$\mathrm{ord}_p(a_1) = \cdots = \mathrm{ord}_p(a_r).$$

It is easy to produce examples having no odd primes with the wanted property. Indeed let $a = e, b = e^2, c = -e^2$. For any $p \geq 3$, if $\delta = \mathrm{ord}_p(e) = \mathrm{ord}_p(-e^2)$, then

---

Date: September 5, 2005.
1991 *Mathematics Subject Classification.* 11N37, 11N56.
Key words and phrases. distribution of values of arithmetical function, Chebotarev Density Theorem.
both authors were sponsored in part by G.N.S.A.G.A. from I.N.D.A.M..

we have $e^{2\delta} \equiv (-e^2)^\delta \equiv 1 (\mathrm{mod}\ p)$. Therefore $(-1)^\delta \equiv 1 (\mathrm{mod}\ p)$ so that $2 \mid \delta$ and $(e^2)^{\delta/2} \equiv 1 (\mathrm{mod}\ p)$. This implies $\mathrm{ord}_p(e^2) \mid \delta/2$. However we have the following result due to Wójcik [6]:

Theorem (Wójcik (1996) [6]). *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–Sierpinski* Hypothesis H *implies that there exist infinitely many primes $\mathfrak{p}$ of K of degree 1 such that*

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

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 [4]) implies that the SW problem for $\{a, b, c\}$ has an affirmative answer. Note however that the sufficient condition $-1 \notin \langle a, b, c \rangle$ should not be always necessary. Indeed consider that case of SW for $\{2, 3, -6\}$. The above theorem does not apply although for $p = 19,211,499,907$, one has that $\mathrm{ord}_p(2) = \mathrm{ord}_p(3) = \mathrm{ord}_p(-6)$. Moreover empirical data suggests that the SW problem has an affirmative answer. Observe that Hypothesis H never answers the SW problem for sets of the form $\{a, b, -ab\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$. We denote by $\mathrm{li}(x)$ the *logarithmic integral:*

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

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

Theorem (K. R. Matthews - 1976 [1]). *Given $a_1, \ldots, a_r \in \mathbb{Z}^*$, there exists $A = A(a_1, \ldots, a_r) \in \mathbb{R}^{\geq 0}$ such that if the Generalized Riemann Hypothesis holds, then*

$$\#\{p \leq x \mid \mathrm{ord}_p(a_i) = p - 1\ \forall i = 1, \ldots, r\} = A\,\mathrm{li}(x) + O\left(x \frac{(\log\log x)^{2^r - 1}}{(\log x)^2}\right).$$

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

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

Further results in [1] imply that:

(1) $A(a_1, \ldots, a_r) = 0$ if and only if at least one of the following conditions is satisfied:
   (a) there exists $1 \leq i_1 < \ldots < i_{2s+1} \leq n$ such that
   $$a_{i_1} \cdots a_{i_{2s+1}} \in (\mathbb{Q}^*)^2;$$
   (b) there exists $1 \leq i_1 < \ldots < i_{2s} \leq n$ such that
   $$a_{i_1} \cdots a_{i_{2s}} \in -3(\mathbb{Q}^*)^2$$
   and the set of primes $q \equiv 1 \bmod 3$ for which each a_i is not a cube modulo q is finite.

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

(2) Using the above, it can be checked that $A(2, 3, -6) \neq 0$ so that GRH implies that the SW problem has an affirmative answer in this case.

(3) For any $a, b \in \mathbb{Q} \setminus \{0, \pm 1\}$ it is easy to see that $A(a, b, ab) = 0$. Indeed if $\operatorname{ord}_p a = \operatorname{ord}_p b = p - 1$, then the Legendre symbols $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$. Therefore $\left(\frac{ab}{p}\right) = 1$ and this implies that $\operatorname{ord}_p ab \mid \frac{p-1}{2}$.

(4) The SW problem for $\{4, 3, -1\}$ is still open both on Hypothesis H and on GRH.

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

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

We denote by $\langle a_1, \dots, a_r \rangle$ the subgroup of $\mathbb{Q}^*$ generated by $a_1, \dots, a_r$, and by $r(a_1, \dots, a_r) = \operatorname{rank}_{\mathbb{Z}} \langle a_1, \dots, a_r \rangle$ its rank as abelian group. Clearly

$$1 \le r(a_1, \dots, a_r) \le r.$$

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

Theorem 1. *Let $\{a_1, \dots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$ and assume that the Generalized Riemann Hypothesis holds for the fields $\mathbb{Q}(\zeta_n, a_1^{1/n_1}, \dots, a_r^{1/n_r})$ $(n, n_1, \dots, n_r \in \mathbb{N})$ and that $r(a_1, \dots, a_r) \ge 2$. Then*

$$\mathcal{S}_{a_1,\dots,a_r}(x) = \left(\delta_{a_1,\dots,a_r} + O_{a_1,\dots,a_r}\left(\frac{1}{\log x}\right)\right) \operatorname{li}(x)$$

where if $k = [k_1, \dots, k_r]$,

$$\Gamma = \langle a_1^{\frac{k}{k_1}}, \dots, a_r^{\frac{k}{k_r}} \rangle, \qquad \mathcal{A} = \Gamma \cdot \mathbb{Q}^{*mk} / \mathbb{Q}^{*mk},$$

$N = 2^{v_2(mk)}$ *and*

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

then

$$\delta_{a_1,\dots,a_r} = \sum_{\substack{m \in \mathbb{N} \\ k_1,\dots,k_r \in \mathbb{N}}} \frac{\mu(k_1) \cdots \mu(k_r)}{\varphi(mk)} \frac{\#\mathcal{B}}{\#\mathcal{A}}. \tag{2}$$

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

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

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

where, 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

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

where

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

and

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

The proof of the above formula uses results of P. Moree [2] and others. In this degenerate case we can give a complete answer to the SW problem.

Corollary 3. *Let $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ and $h_1, \ldots, h_r \in \mathbb{N}^+$. Then $\delta_{a^{h_1},\ldots,a^{h_r}} \neq 0$. Therefore the SW problem for $\{a^{h_1}, \ldots, a^{h_r}\}$ has an affirmative answer.*

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

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

It is immediate to see that

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

Note that for $r = 1$, the function $\mathcal{S}_a(x, m)$ was considered by L. Murata in 1991 [3] who proved:

Theorem (Murata). *Let $a \in \mathbb{Z} \setminus \{0, \pm 1\}$, then if the GRH holds,*

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

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

As a side-product of our Theorem 1, we have the following result that generalizes both Matthews and Murata's Theorems:

Theorem 4. *Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q} \setminus \{0, \pm 1\}$, $m \in \mathbb{N}$, assume that the Generalized Riemann Hypothesis holds and that $r(a_1, \ldots, a_r) \geq 2$. Then*

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

where

$$c_{a_1,\ldots,a_r,m} = \sum_{k_1,\ldots,k_r \in \mathbb{N}} \frac{\mu(k_1)\cdots\mu(k_r)}{\varphi(mk)} \frac{\#\mathcal{B}}{\#\mathcal{A}} \tag{4}$$

and the notations are the same as in the statement of Theorem 1. □

2. Numerical Examples

In this section we compare numerical data. The table compares the densities $\delta_{a,a^2,\ldots,a^r}$ with the quantities $\mathcal{S}_{a,a^2\ldots,a^r}(10^8)/\pi(10^8)$ for $r = 2, 3, \ldots, 8$ and $a \in \mathbb{Q} \setminus \{0, \pm 1\}$ with natural height up to 8. Both quantities have been truncated at the fifth decimal digit.

$S_{a,a^2,\ldots,a^r}(10^8)/\pi(10^8)$ $\delta_{a,a^2,\ldots,a^r}$,							
$a \setminus r$	2	3	4	5	6	7	8
2	0.29165	0.18226	0.18226	0.14429	0.14429	0.12325	0.12325
	0.29166	0.18229	0.18229	0.14431	0.14431	0.12326	0.12326
-2	0.29164	0.18228	0.18228	0.14429	0.14429	0.12325	0.12325
	0.29166	0.18229	0.18229	0.14431	0.14431	0.12326	0.12326
3	0.33336	0.27084	0.27084	0.21445	0.21445	0.18322	0.18322
	0.33333	0.27083	0.27083	0.21440	0.21440	0.18314	0.18314
-3	0.33335	0.08334	0.08334	0.06597	0.06597	0.05635	0.05635
	0.33333	0.08333	0.08333	0.06597	0.06597	0.05635	0.05635
3/2	0.33338	0.22401	0.22401	0.17732	0.17732	0.15145	0.15145
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
-3/2	0.33331	0.22398	0.22398	0.17729	0.17729	0.15152	0.15152
	0.33333	0.22395	0.22395	0.17730	0.17730	0.15144	0.15144
4	0.58330	0.36454	0.36454	0.28858	0.28858	0.24651	0.24651
	0.58333	0.36458	0.36458	0.28862	0.28862	0.24653	0.24653
-4	0.33333	0.20832	0.20832	0.16490	0.16490	0.14082	0.14082
	0.33333	0.20833	0.20833	0.16493	0.16493	0.14087	0.14087
3/4	0.33330	0.27083	0.27083	0.21443	0.21443	0.18323	0.18323
	0.33333	0.27083	0.27083	0.21440	0.21440	0.18134	0.18134
-3/4	0.33335	0.08332	0.08332	0.06593	0.06593	0.05634	0.05634
	0.33333	0.08333	0.08333	0.06597	0.06597	0.05635	0.05635
5	0.33323	0.20826	0.20826	0.12157	0.12157	0.10384	0.10384
	0.33333	0.20833	0.20833	0.12152	0.12152	0.10380	0.10380
-5	0.33342	0.20833	0.20833	0.18661	0.18661	0.15941	0.15941
	0.33333	0.20833	0.20833	0.18663	0.18663	0.15941	0.15941
2/5	0.33325	0.20837	0.20837	0.17037	0.17037	0.14557	0.14557
	0.33333	0.20833	0.20833	0.17035	0.17035	0.14551	0.14551
-2/5	0.33342	0.20835	0.20835	0.17036	0.17036	0.14554	0.14554
	0.33333	0.20833	0.20833	0.17035	0.17035	0.14551	0.14551
3/5	0.33326	0.20831	0.20831	0.15190	0.15190	0.12970	0.12970
	0.33333	0.20833	0.20833	0.15190	0.15190	0.12975	0.12975
-3/5	0.33344	0.20836	0.20836	0.19099	0.19099	0.16324	0.16324
	0.33333	0.20833	0.20833	0.19097	0.19097	0.16312	0.16312
4/5	0.33337	0.20837	0.20837	0.12163	0.12163	0.10392	0.10392
	0.33333	0.20833	0.20833	0.12152	0.12152	0.10380	0.10380
-4/5	0.33331	0.20823	0.20823	0.18654	0.18654	0.15936	0.15936
	0.33333	0.20833	0.20833	0.18663	0.18663	0.15941	0.15941

It is easy to see that if r is not prime, then

$$\delta_{a,a^2,\ldots,a^r} = \delta_{a,a^2,\ldots,a^{r-1}}.$$

Indeed the formula for $\delta_{a,a^2,\ldots,a^r}$ in Theorem 2 depends only on the lowest common multiple of the exponents and if r is not prime then $[1,2,\ldots,r] = [1,2,\ldots,r-1]$.

Similarly if r is not prime, for every $x > 1$

$$S_{a,a^2,\ldots,a^r}(x) = S_{a,a^2,\ldots,a^{r-1}}(x).$$

Indeed if $r = st$, then $\operatorname{ord}_p(a^s) = \operatorname{ord}_p(a^t) = \operatorname{ord}_p(a)$ if and only if

$$(\operatorname{ord}_p(a), s) = (\operatorname{ord}_p(a), t) = 1$$

and if that happens then $(\mathrm{ord}_p(a), st) = 1$.

This explains why in the table the third column equals the second, the fifth equals the fourth and the seventh equals the sixth.

3. 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 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). We will address this problem in a future paper.

We conclude with the following elementary result:

Proposition 5. *If $S = \{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{0, \pm 1\}$ is such that:*

i. $-1 \in \langle S \rangle$;

ii. $S \cap \langle S \rangle^2 \neq \emptyset$.

Then the Schinzel & Wójcik problem for S has a negative answer.

Proof. Assume that $\delta = \mathrm{ord}_p(a_1) = \dots = \mathrm{ord}_p(a_r)$ for some prime $p > 2$. 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 $2 \mid \delta$.

If $a_{i_0} \in S \cap \langle S \rangle^2$, then $a_{i_0} = a_1^{2\tau_1} \cdots a_r^{2\tau_r}$ for suitable $\tau_1, \dots, \tau_r \in \mathbb{Z}$. Hence

$$a_{i_0}^{\delta/2} = a_1^{\delta\tau_1} \cdots a_r^{\delta\tau_r} \equiv 1 \bmod p$$

which contradicts to the hypothesis $\mathrm{ind}_p(a_{i_0}) = \delta$. □

We conclude with a series of remarks:

(1) The hypothesis of the Proposition 5 can both be satisfied only if $r \geq 3$.

(2) Condition ii. in Proposition 5 implies in particular that a_{i_0} is a perfect square and therefore the Matthews constant $A(a_1, \dots, a_r)$ in the introduction is zero.

(3) While the condition $-1 \in \langle S \rangle$ in the previous proposition seems necessary in order the have a negative answer to the SW problem (See Wójcik Theorem in the introduction), we are unable to guess whether the second one is necessary.

(4) The only case which is not covered neither by Theorem 1 or by Theorem 2 is $r(a_1, \dots, a_r) = 1$ and $-1 \in \langle a_1, \dots, a_r \rangle$. From Proposition 5 we deduce that this case includes some sets for which the SW problem has negative answer.

(5) The problem of expressing the density $\delta_{a_1,\dots,a_r}$ as an Euler product when the rank $r(a_1, \dots, a_r) > 1$ and the study of the equation

$$\delta_{a_1,\dots,a_r} = 0$$

will be addressed by the authors in a future paper.

REFERENCES

[1] MATTHEWS, K. R., *A generalisation of Artin's conjecture for primitive roots*. Acta Arith. **29** (1976), no. 2, 113–146.
[2] MOREE, P. *On primes p for which d divides* $\mathrm{ord}_p(g)$. arXiv:math.NT/0407421.
[3] MURATA, L. *A problem analogous to Artin's conjecture for primitive roots and its applications*. Arch. Math. (Basel) **57** (1991), no. 6, 555–565.
[4] SCHINZEL, A. AND SIERPINSKI, W., *Sur certaines hypothéses concernant les nombres premiers*. Acta Arith. **4** (1958), 185–208.
[5] SCHINZEL, A. AND WÒJCIK, J., *On a problem in elementary number theory*. Math. Proc. Cambridge Philos. Soc. **112** (1992), no. 2, 225–232.
[6] WÓJCIK, J., *On a problem in algebraic number theory*. Math. Proc. Cambridge Philos. Soc. **119** (1996), no. 2, 191–200.

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ ROMA TRE, LARGO S. L. MURIALDO, 1, I–00146 ROMA ITALIA
E-mail address: pappa,susa@mat.uniroma3.it