Math. Proc. Camb. Phil. Soc. (2026), **180**, 389–401
doi:10.1017/S0305004125101758
First published online 3 November 2025

On The Schinzel–Wójcik Problem Under Hypothesis H

BY M. ANWAR
Department of Mathematics, Faculty of Science, Ain Shams University, Abbassia, Cairo 11566, *Egypt.*
Department of Mathematics, Pennsylvania State University, University Park, PA 16802, *USA.*
e-mail: mohamedanwar@sci.asu.edu.eg

(*Received* 19 *September* 2024*; revised* 08 *August* 2025*; accepted* 22 *August* 2025)

Abstract

Given r non-zero rational numbers $a_1, \dots, a_r$ which are not ± 1, we complete, under *Hypothesis H*, a characterisation of the Schinzel–Wójcik r-rational tuples (i.e. r-tuples of rational numbers for which the Schinzel–Wójcik problem has an affirmative answer) which satisfy that the sum of the exponents of the positive elements a_i in the representation of -1 in terms of the elements a_i in the multiplicative group $\langle a_1, \dots, a_r \rangle \subset \mathbb{Q}^*$ is even whenever $-1 \in \langle a_1, \dots, a_r \rangle$.

2020 Mathematics Subject Classification: 11A07 (Primary); 11A15 (Secondary)

1. *Introduction*

Given $a_1, \dots, a_r \in \mathbb{Q}^* \setminus \{\pm 1\}$, we say that the Schinzel–Wójcik problem has an affirmative answer if there exist infinitely many primes p such that they have the same multiplicative order modulo p.

In 1992, *Schinzel–Wójcik* proved that

THEOREM 1·1 [9]. *Given any $a, b \in \mathbb{Q}^* \setminus \{\pm 1\}$, there exist infinitely many primes p such that* $\operatorname{ord}_p a = \operatorname{ord}_p b$.

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 concluded by stating the following problem:

> Given $a, b, c \in \mathbb{Q}^* \setminus \{\pm 1\}$, do there exist infinitely many primes p with the property that $\operatorname{ord}_p a = \operatorname{ord}_p b = \operatorname{ord}_p c$?

In 1996, Wójcik produced a family of triplets of rational numbers (a, b, c) for which the above property is not satisfied for any odd prime p (see [10]). Here is another family of non-rational triplets in cyclotomic extensions, let $a_1 = \zeta_n a$, $a_2 = a$, $a_3 = a^n$ such that $a \in \mathbb{Q}(\zeta_n)^*$ is not a root of unity and $n > 2$. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Q}(\zeta_n)$ such that $v_{\mathfrak{p}}(a_j) = 0$ for all $j = 1, 2, 3$. If $d = \operatorname{ord}_{\mathfrak{p}}(a_1) = \operatorname{ord}_{\mathfrak{p}}(a_2) = \operatorname{ord}_{\mathfrak{p}}(a_3)$, then $\zeta_n^d = (a_1/a_2)^d \equiv 1 (\operatorname{mod} \mathfrak{p})$. Therefore n divides d. Hence $a^d = a_3^{d/n} \not\equiv 1 (\operatorname{mod} \mathfrak{p})$ but also $a^d = a_2^d \equiv 1 (\operatorname{mod} \mathfrak{p})$ which is a contradiction. Finally, (a_1, a_2, a_3) is an example of a triplet of non-rational numbers for

© The Author(s), 2025. Published by Cambridge University Press on behalf of The Cambridge Philosophical Society.

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

which the Schinzel–Wójcik problem has negative answer. However, we have the following result proved by Wójcik [10] under the assumption of Schinzel's *Hypothesis H* as in [8]:

HYPOTHESIS 1·2 (**Schinzel's Hypothesis H, 1958**). *Let $f_1, \dots, f_k \in \mathbb{Z}[x]$ be irreducible polynomials with positive leading coefficients and such that* $\gcd(f_1(n)\cdots f_k(n) \mid n \in \mathbb{N}) = 1$. *Then there are infinitely many $t \in \mathbb{N}$ such that $f_1(t), \dots, f_k(t)$ are all prime.*

THEOREM 1·3 [10]. *Let $K/\mathbb{Q}$ be a finite extension and $a_1, \dots, a_r \in K \setminus \{0, 1\}$ be such that the multiplicative group $\langle a_1, \dots, a_r\rangle \subset K$ is torsion-free. Then, Schinzel's Hypothesis H implies that there exist infinitely many prime ideals $\mathfrak{p}$ of degree one such that* $\operatorname{ord}_{\mathfrak{p}} a_1 = \cdots = \operatorname{ord}_{\mathfrak{p}} a_r$.

Also, in 2009, F. Pappalardi and A. Susa proved that:

PROPOSITION 1·4 [7]. *Let $\{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ be such that both the following properties are satisfied*:

(i) *there exist $\omega_1, \dots, \omega_r \in \mathbb{Z}$ with $a_1^{\omega_1} \cdots a_r^{\omega_r} = -1$; and*
(ii) *there exist $v_1, \dots, v_r \in \mathbb{Z}$ with $v_1 + \cdots + v_r$ odd and $a_1^{v_1} \cdots a_r^{v_r} = 1$.*

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

In the case where $S = \{a_1, \dots, a_r\} \subset \mathbb{Z}$, under the assumption of the *Generalised Riemann Hypothesis* for suitable number fields, in 1976, K. Matthews proved [5] that $\mathcal{P}_S = \{p \text{ prime} \mid \forall a \in S, a \text{ is a primitive root modulo } p\}$ is finite if and only if at least one of the two following conditions is satisfied:

(1) there exist $1 \le i_1 < \cdots < i_{2s+1} \le r$ such that $a_{i_1} \cdots a_{i_{2s+1}} \in \mathbb{Q}^{*2}$;
(2) there exist $1 \le i_1 < \cdots < i_{2s} \le r$ such that $a_{i_1} \cdots a_{i_{2s}} \in -3\mathbb{Q}^{*2}$, and for all primes $\ell \equiv 1 \bmod 3$ there exists at least one element of S which is a cube modulo ℓ.

In 2017, F. Pappalardi and M. Anwar proved [2] that the same characterisation holds in the case of $\{a_1, \dots, a_r\} \subset \mathbb{Q}$, under the assumption of *Hypothesis H*.

The aim of this paper is to prove a sufficient condition of the Schinzel–Wójcik problem under *Hypothesis H*. We shall prove:

THEOREM 1·5. *Let $\{a_1, \dots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ be such that*:

(i) *there exist $v_1, \dots, v_r \in \mathbb{Z}$ such that $-1 = a_1^{v_1} \cdots a_r^{v_r}$ with $\sum' v_i \equiv 0 \pmod 2$, where $\sum'$ means that the sum runs over the positive a_i, and*
(ii) *for every $v_1, \dots, v_r \in \mathbb{Z}$, if $a_1^{v_1} \cdots a_r^{v_r} = 1$, then $v_1 + \cdots + v_r \equiv 0 \pmod 2$.*

Then *Hypothesis H* implies the existence of infinitely many prime numbers q such that

$$\operatorname{ord}_q a_1 = \operatorname{ord}_q a_2 = \cdots = \operatorname{ord}_q a_r.$$

Throughout this paper, the notation $\sum'$ denotes that the summation is taken only over the positive values of a_i, and this convention will be used consistently.

The conditions (i) and (ii) in Theorem 1·5 are satisfied by many families of rational numbers, for example, $\{-a^2, a^{-1}, b^2, b^{-2}\}$ and $\{-a^2, a^{-1}b^{-1}, b\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$, where a, b are coprime rational numbers except $0, 1, -1$.

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

Note that the new contribution of this work is solving the case $-1 = a_1^{v_1} \cdots a_r^{v_r}$ for some $v_1, \ldots, v_r \in \mathbb{Z}$ with $\sum' v_i \equiv 0 (\mathrm{mod}\, 2)$, and that the only remaining case is when $\sum' v_i \equiv 1 (\mathrm{mod}\, 2)$ for any such identity.

In light of Theorem 1·3 and Proposition 1·4, Theorem 1·5, under *Hypothesis H*, completes a characterisation of the Schinzel–Wójcik r-rational tuples (i.e. r-tuples of rational numbers for which the Schinzel–Wójcik problem has an affirmative answer) which satisfy that the sum of the exponents of the positive elements a_i in the representation of -1 in terms of the a_i's in the multiplicative group $\langle a_1, \ldots, a_r \rangle \subset \mathbb{Q}^*$ is even whenever $-1 \in \langle a_1, \ldots, a_r \rangle$. (Note that if $-1 = \prod a_i^{v_i}$ for some $v_1, \ldots, v_r$ with $\sum' v_i$ even, then the sum of the exponents of the positive a_i's in any representation of -1 has to be even.) More precisely,

THEOREM 1·6. *Let* $\{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ *such that if* $-1 = a_1^{v_1} \cdots a_r^{v_r}$ *for some* $v_1, \ldots, v_r \in \mathbb{Z}$, *then the sum of the exponents of the positive* a_i*'s is even. Assuming Hypothesis H, then the Schinzel–Wójcik problem has an affirmative answer for* $\{a_1, \ldots, a_r\}$ *if and only if at least one of the following two conditions is satisfied*:

(i) $-1 \notin \langle a_1, \ldots, a_r \rangle$;

(ii) *for every* $v_1, \ldots, v_r \in \mathbb{Z}$, *if* $a_1^{v_1} \cdots a_r^{v_r} = 1$, *then* $v_1 + \cdots + v_r \equiv 0 \,(\mathrm{mod}\, 2)$.

This characterisation was originally introduced by M. Anwar in his Ph.D. thesis [**1**] in 2018 for all r-tuples of odd rational numbers—that is, rational numbers whose denominators are supported only at odd primes—for which the Schinzel–Wójcik problem admits an affirmative answer. However, a gap was later identified in the proof. In 2021, Olli Järviniemi established the same characterisation for all r-rational tuples, under the assumption of the *generalised Riemann hypothesis* [**4**].

Remark 1·7. The proof of Theorem 1·3 relies on Artin's reciprocity law, more precisely on the following consequence of the latter for power-residue symbols ([**3**], page 51). Let K be an algebraic number field and $\mathfrak{m}$, $\mathfrak{p}$, $\mathfrak{q}$ ideals of K. We write $\mathfrak{p} \sim \mathfrak{q} \,(\mathrm{mod}\, \mathfrak{m})$ if $(\mathfrak{p}, \mathfrak{q}, \mathfrak{m}) = 1$ and there exist totally positive integers α, β of K such that $(\alpha\beta, \mathfrak{m}) = 1$, $\alpha \equiv \beta \,(\mathrm{mod}\, \mathfrak{m})$ and $(\alpha)\mathfrak{p} = (\beta)\mathfrak{q}$.

Assume now that $k \in \mathbb{N}$, $\zeta_k \in K$, $\gamma \in K$ and let $\mathfrak{f}$ be the conductor of the extension $K(\sqrt[k]{\gamma})/K$ denoted further by $\mathfrak{f}\left(K(\sqrt[k]{\gamma})/K\right)$. If ideals $\mathfrak{p}$,$\mathfrak{q}$ of K satisfy $\mathfrak{p} \sim \mathfrak{q} \,(\mathrm{mod}\ \mathfrak{f})$, then

$$\left[\frac{\gamma}{\mathfrak{p}}\right]_k = \left[\frac{\gamma}{\mathfrak{q}}\right]_k$$

provided the kth-power-residue symbols are defined.

Let us conclude the introduction by giving a brief sketch of the proof of the main theorem. To do so, we first set some notation. Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ be such that $-1 = a_1^{v_1} \cdots a_r^{v_r}$ for some $v_1, \ldots, v_r \in \mathbb{Z}$ with $\sum' v_i \equiv 0 \,(\mathrm{mod}\ 2)$. Let

$$\mathcal{L} = \{\ell \text{ prime} \mid v_\ell(a_j) \neq 0 \text{ for some } j \in \{1, \ldots, r\}\}.$$

Write

$$\mathcal{L} = \{\ell_1, \ldots, \ell_m\}$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

and for all $j = 1, \ldots, r$,

$$a_j = (-1)^{e_{0j}} \ell_1^{e_{1j}} \ell_2^{e_{2j}} \cdots \ell_m^{e_{mj}}, \tag{1·1}$$

where $e_{0j} = 0$ or 1 and $e_{ij} \in \mathbb{Z}$ for all $1 \le i \le m$, $1 \le j \le r$. We furthermore decompose the ℓ_i's in $(\mathbb{Q}^{mc})^*$, the cyclotomic closure of $\mathbb{Q}$,

$$\ell_i = \zeta_w^{b_i} \pi_1^{a_{i1}} \cdots \pi_n^{a_{in}} \quad (1 \le i \le m) \tag{1·2}$$

with $w \in \mathbb{N}$, b_i, $a_{ij} \in \mathbb{Z}$, $(b_1, \ldots, b_m, w) = 1$, where $\pi_1, \pi_2, \ldots$ is a multiplicative basis of $(\mathbb{Q}^{mc})^*$ (see Lemma 2·1) and $\pi_1, \ldots, \pi_n \in \mathbb{Q}(\zeta_g)$ for some $g \in \mathbb{Z}^+$.

For some suitable positive integer k, the main points in the proof are the following:

(1) there exists a prime ideal $\mathfrak{q}_0$ in $\mathbb{Q}(\zeta_k)$ such that

$$\left[\frac{a_i}{\mathfrak{q}_0}\right]_k = -1 \quad \text{for all } i = 1, \ldots, r;$$

(2) there exist infinitely many pairs of primes (p,q) satisfying $q = kp + 1$ and

$$a_j^p \equiv -1 \pmod{q} \quad \text{for all } j = 1, 2, \ldots, r.$$

Hence,

$$\operatorname{ord}_q a_1 = \operatorname{ord}_q a_2 = \cdots = \operatorname{ord}_q a_r = 2p.$$

Using Lemma 2·2, we will be able to prove that for any integers $x_1, \ldots, x_n$ and every $t \in \mathbb{Z}$ such that $(t, F) = 1$, there exists a prime ideal $\mathfrak{q}_0$ in $\mathbb{Q}(\zeta_k)$ such that

$$\left[\frac{\pi_i}{\mathfrak{q}_0}\right]_k = \zeta_k^{x_i} \ (1 \le i \le n), \quad N\mathfrak{q}_0 \equiv t \pmod{F},$$

where $F \in \mathbb{Z}$ such that $k \mid F$ and $N = N_{\mathbb{Q}(\zeta_k)/\mathbb{Q}}(\cdot)$. A main ingredient in the proof is to choose ζ_k suitably so that this implies 1 above. This corresponds to proving the solvability of a system of linear congruences. We show in Lemma 2·4 that a solution exists. Consequently, the second claim can be achieved using Lemma 2·3 which guarantees the existence of a polynomial $f_1(x)$ such that

$$(p, q) = \left(f_1(x), \frac{f_1(x) - 1}{k}\right)$$

is a pair of primes for infinitely many $x \in \mathbb{Z}$, using *Hypothesis H*. Furthermore, if $q = f_1(x)$ is prime for some positive integer x, then $q = N\mathfrak{q}'$, $\mathfrak{q}' \sim \mathfrak{q}_0^{-1} \pmod{F}$. Using Remark 1·7 and the first point, one can easily see that

$$a_j^{\frac{q-1}{k}} \equiv \left[\frac{a_j}{\mathfrak{q}'}\right]_k = \left[\frac{a_j}{\mathfrak{q}_0}\right]_k^{-1} = -1 \pmod{\mathfrak{q}'} \quad (1 \le j \le r).$$

Consequently,

$$a_j^p \equiv -1 \pmod{\mathfrak{q}'} \quad \text{for all } j = 1, 2, \ldots, r,$$

which completes the second claim.

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

The paper is organised as follows. Section 2 includes some prior lemmas. Section 3 presents the proof of the main Theorem 1·5. Finally, Section 4 presents a family of examples that shows that the applied strategy is not applicable in the case that the sum of the exponents of the positive elements a_i in the representation of -1 in terms of the a_i's in the multiplicative group $\langle a_1, \ldots, a_r \rangle \subset \mathbb{Q}^*$ is odd whenever $-1 \in \langle a_1, \ldots, a_r \rangle$.

2. *Lemmata*

In this section, we introduce a series of lemmata crucial to the proof of Theorem 1·5. The first lemma is due to W. May. Its proof follows from the corollary to theorem 2 in [**6**]. The second and third lemmas are due to J. Wojcik [**10**].

LEMMA 2·1. *Let K be an algebraic number field. Let K^{mc} denote the cyclotomic closure of the field K. In the field K^{mc} there is a multiplicative basis i.e. such sequence $\pi_1, \pi_2, \ldots$, that any non-zero element of K^{mc} is represented uniquely as $\zeta \prod_{s=1}^{t} \pi_s^{x_s}$, where x_s are rational integers and ζ is a root of unity.*

LEMMA 2·2. *Let K, K_1 be algebraic number fields such that $K \subset K_1 \subset K^{mc}$ and $k, F \in \mathbb{Z}$ such that $k|F$. Assume that $\pi_1, \ldots, \pi_n, \zeta_k \in K_1$, where $\pi_1, \ldots, \pi_n$ are elements of the multiplicative basis described in Lemma 2·1. Let G be the subgroup of the multiplicative group of residue classes mod F corresponding to the field $K_1 \cap \mathbb{Q}(\zeta_F)$. Finally let $\bar{t} \in G$ denote the residue class mod F containing $t \in \mathbb{Z}$. For all rational integers $x_1, \ldots, x_n$ and every $\bar{t} \in G$ there exist infinitely many prime ideals $\mathfrak{q}$ of degree one of K_1 such that*

$$\left[\frac{\pi_i}{\mathfrak{q}}\right]_k = \zeta_k^{x_i} \quad (1 \le i \le n), \qquad N\mathfrak{q} \equiv t \,(\mathrm{mod}\, F).$$

LEMMA 2·3. *Let K_2 be a normal field and k a positive integer. Assume that n_2 denotes the degree of K_2 and that $g(x)$ is the minimal polynomial of an algebraic integer θ such that $K_2 = \mathbb{Q}(\theta)$. If a prime ideal $\mathfrak{q}_0$ of degree one of K_2 and a positive integer F satisfy the condition*

$$F \equiv 0 \,(\mathrm{mod}\, k(2n_2)!\ \mathrm{disc}\,(g)), \qquad N\mathfrak{q}_0 \equiv 1 \,(\mathrm{mod}\, k), \ (\mathfrak{q}_0, F) = 1, \qquad \left(\frac{N\mathfrak{q}_0 - 1}{k}, F\right) = 1$$

then there exists a polynomial $f_1(x)$ such that the polynomials $f_1(x)$ and $f_2(x) = (f_1(x) - 1)/k$ satisfy the assumptions of Hypothesis H. *Moreover, this $f_1(x)$ is such that if $q = f_1(x)$ is prime for some positive integer x, then $q = N\mathfrak{q}'$, $\mathfrak{q}' \sim \mathfrak{q}_0^{-1} \,(\mathrm{mod}\, F)$, where $\mathfrak{q}'$ is a prime ideal of degree one of K_2.*

Define the matrices

$$E_{r\times(m+1)} := \begin{pmatrix} e_{01} & e_{11} & e_{21} & \cdots & e_{m1} \\ \vdots & \vdots & \vdots & & \vdots \\ e_{0r} & e_{1r} & e_{2r} & \cdots & e_{mr} \end{pmatrix} \quad \text{and} \quad A_{(m+1)\times n} := \begin{pmatrix} 0 & 0 & \cdots & 0 \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}.$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

As defined in Section 1, the entries of the matrices E and A are associated with the rational tuple $a_1, \ldots, a_r$.

LEMMA 2·4. *Let $k, w, u \in \mathbb{Z}^+$ be such that $w \mid k$ and $b_1, b_2, \ldots, b_m \in \mathbb{Z}$ where $m \in \mathbb{Z}^+$. Let $\{a_1, \ldots, a_r\} \subset \mathbb{Q}^* \setminus \{\pm 1\}$ such that*:

(i) *there exist $v_1, \ldots, v_r \in \mathbb{Z}$ such that $-1 = a_1^{v_1} \cdots a_r^{v_r}$ with $\sum' v_i \equiv 0 \pmod 2$, and*

(ii) *for every $v_1, \ldots, v_r \in \mathbb{Z}$, if $a_1^{v_1} \cdots a_r^{v_r} = 1$, then $v_1 + \cdots + v_r \equiv 0 \pmod 2$.*

Then the system

$$EA \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \equiv \frac{k}{2} \begin{pmatrix} 1 - e_{01} \\ \vdots \\ 1 - e_{0r} \end{pmatrix} - \frac{k}{w} u\, E \begin{pmatrix} 0 \\ b_1 \\ \vdots \\ b_m \end{pmatrix} \pmod k \tag{2·1}$$

is solvable.

Proof. The first condition implies that there exists v_i for some $i = 1, 2, \ldots, r$ such that v_i is odd and $a_i < 0$. So, without loss of generality we may assume that v_1 is odd and $a_1 < 0$ (i.e., $e_{01} = 1$). Note that a solution exists if and only if a solution exists modulo $p^{v_p(k)}$ for each prime $p \mid k$. We will show how to prove the existence of a solution for $p = 2$; the case $p > 2$ is easier, since in this case the column

$$\frac{k}{2} \begin{pmatrix} 1 - e_{01} \\ \vdots \\ 1 - e_{0r} \end{pmatrix}$$

is $\mathbf{0}$ modulo $p^{v_p(k)}$.

Consider the system (2·1) modulo 2^α, where $\alpha := v_2(k)$ is assumed to be sufficiently large. The system (2·1) takes the form:

$$EA \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} 0 \\ k_2 \\ \vdots \\ k_r \end{pmatrix} - \frac{k}{w} u\, E \begin{pmatrix} 0 \\ b_1 \\ \vdots \\ b_m \end{pmatrix} \pmod{2^\alpha}, \tag{2·2}$$

where for all $i = 1, 2, \ldots, r$,

$$k_i = \frac{k}{2}(1 - e_{0i}) \equiv \begin{cases} 2^{\alpha-1} \pmod{2^\alpha} & \text{if } a_i > 0, \\ 0 \pmod{2^\alpha} & \text{if } a_i < 0. \end{cases}$$

The first condition of Lemma 2·4 implies that

$$\begin{aligned} \mu_0 &:= e_{01}v_1 + \cdots + e_{0r}v_r \equiv 1 \pmod 2, \\ \mu_j &:= e_{j1}v_1 + \cdots + e_{jr}v_r = 0 \text{ for all } j = 1, \ldots, m, \\ \sum_{i=1}^{r} v_i k_i &= 2^{\alpha-1} \sum{}' v_i \equiv 0 \pmod{2^\alpha}. \end{aligned} \tag{2·3}$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

Therefore, replacing Row_1 by $\sum_i v_i \mathrm{Row}_i$ in the system (2·2) and using equations (2·3), we get the following

$$E_1 A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} 0 \\ k_2 \\ \vdots \\ k_r \end{pmatrix} - \frac{k}{w} u\, E_1 \begin{pmatrix} 0 \\ b_1 \\ \vdots \\ b_m \end{pmatrix} \pmod{2^\alpha}, \tag{2·4}$$

where

$$E_1 = \begin{pmatrix} \mu_0 & 0 & 0 & \cdots & 0 \\ e_{02} & e_{12} & e_{22} & \cdots & e_{m2} \\ \vdots & \vdots & \vdots & & \vdots \\ e_{0r} & e_{1r} & e_{2r} & \cdots & e_{mr} \end{pmatrix}.$$

Now, replacing Row_1 by $\mu_0^{-1} \cdot \mathrm{Row}_1$ in the system (2·4), we get

$$E_2 A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} 0 \\ k_2 \\ \vdots \\ k_r \end{pmatrix} - \frac{k}{w} u\, E_2 \begin{pmatrix} 0 \\ b_1 \\ \vdots \\ b_m \end{pmatrix} \pmod{2^\alpha}, \tag{2·5}$$

where

$$E_2 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ e_{02} & e_{12} & e_{22} & \cdots & e_{m2} \\ \vdots & \vdots & \vdots & & \vdots \\ e_{0r} & e_{1r} & e_{2r} & \cdots & e_{mr} \end{pmatrix}.$$

Replacing Row_i by $(-e_{0i} \cdot \mathrm{Row}_1 + \mathrm{Row}_i)$ for $i = 2, 3, \ldots, r$ in the system (2·5), we get

$$E_3 A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} 0 \\ k_2 \\ \vdots \\ k_r \end{pmatrix} - \frac{k}{w} u\, E_3 \begin{pmatrix} 0 \\ b_1 \\ \vdots \\ b_m \end{pmatrix} \pmod{2^\alpha}, \tag{2·6}$$

where

$$E_3 = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & e_{12} & e_{22} & \cdots & e_{m2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & e_{1r} & e_{2r} & \cdots & e_{mr} \end{pmatrix}.$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

Hence, using row operations, the system (2·6) can be written as follows

$$DA\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \equiv \begin{pmatrix} 0 \\ k_2' \\ \vdots \\ k_s' \\ k_{s+1}' \\ \vdots \\ k_r' \end{pmatrix} - \frac{k}{w}u \begin{pmatrix} 0 \\ b_2' \\ \vdots \\ b_s' \\ 0 \\ \vdots \\ 0 \end{pmatrix} \pmod{2^\alpha}, \tag{2·7}$$

where

$$D = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & d_{21} & d_{22} & \cdots & d_{2m} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & d_{s1} & d_{s2} & \cdots & d_{sm} \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & & & & \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}$$

is a row echelon form of E with $s \leq r$ independent rows, $b_i' = d_{i1}b_1 + d_{i2}b_2 + \cdots + d_{im}b_m$ and $k_i' = 0$ or $2^{\alpha-1}$ modulo 2^α for all $i = 2, \ldots, r$. Obtaining a zero row, say row j, through row operations on E corresponds to replacing a_j with a product of powers of the a_i's that equals 1. Hence, by the second condition of Lemma 2·4, we deduce that any sequence of row operations on E resulting in a zero row in D must replace the initial row with an even sum of rows of E. Hence, we get $k_i' = 0$ modulo 2^α for all $i = s+1, s+2, \ldots, r$. Note that α is chosen sufficiently large such that the non-zero rows of D are not zero modulo 2^α.

The rows of the matrix DA are linear combinations of the rows of the matrix A. More precisely,

$$DA = \begin{pmatrix} \mathbf{0} \\ d_{21}\mathrm{Row}_2(A) + d_{22}\mathrm{Row}_3(A) + \cdots + d_{2m}\mathrm{Row}_{m+1}(A) \\ \vdots \\ d_{s1}\mathrm{Row}_2(A) + d_{s2}\mathrm{Row}_3(A) + \cdots + d_{sm}\mathrm{Row}_{m+1}(A) \\ \mathbf{0} \\ \vdots \\ \mathbf{0} \end{pmatrix}.$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

In fact, the rows $\mathrm{Row}_2(DA), \ldots, \mathrm{Row}_s(DA)$ are linearly independent, otherwise there are $c_2, \ldots, c_s$ not all zeros such that

$$c_2\mathrm{Row}_2(DA) + c_3\mathrm{Row}_3(DA) + \cdots + c_s\mathrm{Row}_s(DA) = \mathbf{0}.$$

Hence,

$$f_2\mathrm{Row}_2(A) + f_3\mathrm{Row}_3(A) + \cdots + f_{m+1}\mathrm{Row}_{m+1}(A) = \mathbf{0},$$

where

$$f_i = c_2d_{2,i-1} + \cdots + c_sd_{s,i-1}, \quad \text{for all } i = 2, 3, \ldots, m+1.$$

Equivalently, we have

$$\begin{aligned} f_2a_{11} + f_3a_{21} + \cdots + f_{m+1}a_{m1} &= 0,\\ f_2a_{12} + f_3a_{22} + \cdots + f_{m+1}a_{m2} &= 0,\\ \cdots \quad \cdots \quad \cdots&\\ f_2a_{1n} + f_3a_{2n} + \cdots + f_{m+1}a_{mn} &= 0. \end{aligned}$$

Consequently, using the factorisation of the ℓ_i's in equation (1·2), we get

$$\ell_1^{f_2}\ell_2^{f_3}\cdots\ell_m^{f_{m+1}} = 1.$$

Since $\ell_1, \ell_2, \ldots, \ell_m$ are multiplicatively independent, therefore

$$f_2 = f_3 = \cdots = f_{m+1} = 0.$$

Equivalently,

$$c_2\begin{pmatrix} d_{21}\\ \vdots\\ d_{2m}\end{pmatrix} + c_3\begin{pmatrix} d_{31}\\ \vdots\\ d_{3m}\end{pmatrix} + \cdots + c_s\begin{pmatrix} d_{s1}\\ \vdots\\ d_{sm}\end{pmatrix} = \begin{pmatrix} 0\\ \vdots\\ 0\end{pmatrix}.$$

Since the rows $\mathrm{Row}_2(D), \ldots, \mathrm{Row}_s(D)$ are linearly independent, therefore

$$c_2 = c_3 = \cdots = c_s = 0$$

which contradicts the assumption that not all the c_i are zeros. Therefore, the rows $\mathrm{Row}_2(DA), \ldots, \mathrm{Row}_s(DA)$ are linearly independent.

By applying row and column operations to the system (2·7) and using the method described in [**1**, chapter 2, section 5, p. 17], while noting that the matrix DA has rank $s-1$, we obtain the following comparable system:

$$\begin{pmatrix} g_1x_1'\\ \vdots\\ g_{s-1}x_{s-1}'\end{pmatrix} \equiv \begin{pmatrix} k_2'' - \frac{k}{w}u\,b_2''\\ \vdots\\ k_s'' - \frac{k}{w}u\,b_s''\end{pmatrix} \pmod{2^\alpha}, \tag{2·8}$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

where $g_i = 2^{\beta_i}$ for some positive integer $\beta_i, k_j'' \in \{0, 2^{\alpha-1}\}$ and $b_i'' \in \mathbb{Z}$ for all $i = 1, \ldots, s-1, j = 2, \ldots, s$. For sufficiently large α, satisfying $\beta_i < \alpha$ and $\beta_i < v_2(k/w)$ for all $i = 1, 2, \ldots, s-1$, the system (2·8) is solvable and hence the system (2·2) is so. Therefore, the system (2·1) is solvable.

3. *Proof of Theorem* 1·5

Let $k_0 = gw$, $k = 2k_0$ and choose $K_1 = K_2 = \mathbb{Q}(\zeta_k)$, which is a normal extension. The integers g,w are defined as in equation (1·2).

Put

$$F = k(2\phi(k))!\ \operatorname{disc}(\Phi_k) \prod_{i=1}^{r} N\left(\mathfrak{f}\left(\frac{K_2\left(\sqrt[k]{a_i}\right)}{K_2}\right)\right), \tag{3·1}$$

where ϕ is the Euler totient function, Φ_k is the kth cyclotomic polynomial and $N(\cdot) = N_{K_2/\mathbb{Q}}(\cdot)$.

Further, put $\overline{F} = kF$, $F = F_1F_2$, where F_1 contains prime factors dividing k and $(F_2, k) = 1$. Note that F_2 is odd since k is even. Let t satisfy the system of congruences

$$t \equiv \begin{cases} k+1 \pmod{k^2}, \\ 2 \pmod{F_2}. \end{cases}$$

Consequently,

$$\begin{cases} t \equiv 1 \pmod{k}, \\ t-1 \equiv 1 \pmod{F_2}, \\ \frac{t-1}{k} \equiv 1 \pmod{k}. \end{cases}$$

Therefore,

$$(t, kF_2) = 1, \quad (t-1, F_2) = 1, \quad \left(\frac{t-1}{k}, F_1\right) = 1.$$

Hence,

$$(t, \overline{F}) = 1, \quad t \equiv 1 \pmod{k}, \quad \left(\frac{t-1}{k}, F\right) = 1. \tag{3·2}$$

Lemma 2·4 guarantees the existence of a solution of the system (2·1) for the integers e_{ij}, a_{ij}, b_i introduced in equations (1·1), (1·2) and $u = (t-1)/k$. Let $x_1, x_2, \ldots, x_n \in \mathbb{Z}/k\mathbb{Z}$ be such a solution. Using Lemma 2·2, there exists a prime ideal $\mathfrak{q}_0$ in $K_1 = \mathbb{Q}(\zeta_k)$ of degree one with the properties:

$$\left[\frac{\pi_i}{\mathfrak{q}_0}\right]_k = \zeta_k^{x_i} \quad (1 \le i \le n), \quad N\mathfrak{q}_0 \equiv t \pmod{\overline{F}}, \tag{3·3}$$

where the π_i's are defined as in equation (1·2). Since equations (3·2) and (3·3) imply that $(t-1)/k$ is odd and $(N\mathfrak{q}_0 - 1)/k \equiv (t-1)/k \pmod{k}$, therefore

$$\left[\frac{-1}{\mathfrak{q}_0}\right]_k = (-1)^{\frac{N\mathfrak{q}_0-1}{k}} = (-1)^{\frac{t-1}{k}} = -1 \quad \text{and} \quad \left[\frac{\zeta_w}{\mathfrak{q}_0}\right]_k = \zeta_w^{\frac{N\mathfrak{q}_0-1}{k}} = \zeta_k^{\frac{k}{w}\frac{N\mathfrak{q}_0-1}{k}} = \zeta_k^{\frac{k}{w}u}.$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

Consequently, with the aid of equations (1·1), (1·2) and (3·3), we get

$$\left[\frac{a_j}{\mathfrak{q}_0}\right]_k = \left[\frac{-1}{\mathfrak{q}_0}\right]_k^{e_{0j}} \cdot \prod_{y=1}^{m}\left[\frac{\ell_y}{\mathfrak{q}_0}\right]_k^{e_{yj}} = (-1)^{e_{0j}} \prod_{y=1}^{m}\left(\left[\frac{\zeta_w}{\mathfrak{q}_0}\right]_k^{b_y} \cdot \prod_{i=1}^{n}\left[\frac{\pi_i}{\mathfrak{q}_0}\right]_k^{a_{yi}}\right)^{e_{yj}}$$

$$= \zeta_k^{\frac{k}{2}e_{0j}} \cdot \zeta_k^{\left(\sum_{y=1}^{m} b_y e_{yj}\right)\frac{k}{w}u} \cdot \zeta_k^{\sum_{y=1}^{m}\left(\sum_{i=1}^{n} a_{yi}x_i\right)e_{yj}}.$$

The sum of the three exponents in the previous equation is congruent to $k/2$ modulo k by Lemma 2·4, and hence we obtain

$$\left[\frac{a_1}{\mathfrak{q}_0}\right]_k = -1, \ldots, \left[\frac{a_r}{\mathfrak{q}_0}\right]_k = -1. \tag{3·4}$$

Hence, by equations (3·1), (3·2) and (3·3), we have

$$F \equiv 0 \pmod{k(2\phi(k))!\,\mathrm{disc}(\Phi_k)}, \quad N\mathfrak{q}_0 \equiv 1 \pmod{k}, \ (\mathfrak{q}_0, F) = 1, \quad \left(\frac{N\mathfrak{q}_0 - 1}{k}, F\right) = 1.$$

Using Lemma 2·3, there exists a polynomial $f_1(x)$ such that the polynomials $f_1(x)$ and $f_2(x) = (f_1(x) - 1)/k$ satisfy the assumptions of *Hypothesis H*. By this Hypothesis, there exist infinitely many $x \in \mathbb{N}$ such that $q = f_1(x)$, $p = f_2(x)$ are primes. Again by Lemma 2·3, if $q = f_1(x)$ is a prime number for some $x \in \mathbb{N}$, then

$$q = N\mathfrak{q}' \quad \text{and} \quad \mathfrak{q}_0^{-1} \sim \mathfrak{q}' \pmod{F},$$

where $\mathfrak{q}'$ is a prime ideal of degree one of K_2. Consequently, equation (3·1) implies

$$\mathfrak{q}_0^{-1} \sim \mathfrak{q}' \mod \mathfrak{f}\left(\frac{K_2\left(\sqrt[k]{a_i}\right)}{K_2}\right) \quad \text{for all } 1 \le i \le r.$$

By equations (3·4), then Remark 1·7, the consequence of Artin's reciprocity law, and $(q-1)/k = p$ guarantee

$$a_j^p = a_j^{\frac{q-1}{k}} \equiv \left[\frac{a_j}{\mathfrak{q}'}\right]_k = \left[\frac{a_j}{\mathfrak{q}_0}\right]_k^{-1} = -1 \pmod{\mathfrak{q}'} \quad (1 \le j \le r).$$

Hence,

$$a_j^{2p} \equiv 1 \pmod{q} \quad \text{for all } j = 1, 2, \ldots, r.$$

For all sufficiently large $q = kp + 1$, we have

$$\mathrm{ord}_q\, a_1 = \mathrm{ord}_q\, a_2 = \cdots = \mathrm{ord}_q\, a_r = 2p.$$

4. *Worked example*

In this section, we give a family of examples that shows that the system (2·1) is not solvable in the case that $-1 = a_1^{v_1} \cdots a_r^{v_r}$ for some $v_1, \ldots, v_r \in \mathbb{Z}$ with $\sum' v_i \equiv 1 (\mathrm{mod}\, 2)$.

Consider

$$a_1 = -\ell_1^{-2}\ell_2^{-2}, \qquad a_2 = -\ell_1\ell_2\ell_3^{-1} \qquad \text{and} \quad a_3 = \ell_3^2,$$

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

where ℓ_1, ℓ_2 and ℓ_3 are prime numbers. Clearly, we have

$$a_1^{v_1}a_2^{v_2}a_3^{v_3} = -1 \quad \text{if and only if} \quad v_1 = v_3 \equiv 1 \pmod 2 \text{ and } v_2 = 2v_1 \equiv 0 \pmod 2.$$

In this case, the sum of the exponents of the positive a_i's in the representation of -1 in the multiplicative group $\langle a_1, a_2, a_3\rangle \subset \mathbb{Q}^*$ is odd. Now, we will show the insolvability of the system (2·1) modulo 2^α, which is

$$\begin{pmatrix} 1 & -2 & -2 & 0 \\ 1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 0 & \cdots & 0 \\ a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ a_{31} & a_{32} & \cdots & a_{3n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \equiv 2^{\alpha-1} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} - \frac{k}{w}u \begin{pmatrix} 1 & -2 & -2 & 0 \\ 1 & 1 & 1 & -1 \\ 0 & 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 \\ b_1 \\ b_2 \\ b_3 \end{pmatrix} (\text{mod } 2^\alpha).$$

By applying the row operations mentioned in Lemma 2·4 on E and then multiplying by A, we get the following equivalent system

$$\begin{pmatrix} 0 & 0 & \cdots & 0 \\ c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \equiv 2^{\alpha-1} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} - \frac{k}{w}u \begin{pmatrix} 0 \\ b_1 + b_2 - b_3 \\ 2b_3 \end{pmatrix} (\text{mod } 2^\alpha),$$

which is not solvable.

Note that a_1, a_2 and a_3 satisfy the proved characterisation in [4] by Olli Järviniemi, under the assumption of the *generalised Riemann hypothesis*.

Acknowledgements. The author would like to thank Prof. Francesco Pappalardi for his useful comments. The author also gratefully acknowledges the anonymous reviewers and the editors for their valuable suggestions and constructive feedback, which helped improve the quality and clarity of this work.

This research was financially supported by the Fulbright U.S. Scholar Program, which is sponsored by the U.S. Department of State and the Egyptian-American Fulbright Commission, and was conducted at Pennsylvania State University. Its contents are solely the responsibility of the author and do not necessarily represent the official views of the Fulbright Program, the Government of the United States, or the Egyptian-American Fulbright Commission.

REFERENCES

[1] M. ANWAR. On Schinzel-Wójcik problem. Università degli studi Roma Tre, 2018.
[2] M. ANWAR and F. PAPPALARDI. On simultaneous primitive roots. *Acta Arith.*, **180** (2017), 35–43.
[3] H. HASSE. Bericht Über neuere untersuchungen und problem aus der theorie der algebraischen zahlkörper teil ii: Reziprozitätsgesetz. *Acta Arith.*, **180** (1965), 35–43, Wüzburg-Wien.
[4] O. JÄRVINIEMI. Equality of orders of a set of integers modulo a prime. *Proc. Amer. Math. Soc.*, **149**(09) (2021), 3651–3668.
[5] K. MATTHEWS. A generalisation of Artin's conjecture for primitive roots. *Acta Arith.*, **29**(2) (1976), 113–146.
[6] W. MAY. Multiplicative groups of fields. *Proc. London Math. Soc.* (1972), pages 295–306.
[7] F. PAPPALARDI and A. SUSA. On a problem of Schinzel and Wójcik involving equalities between multiplicative orders. *Math. Proc. Camb. Phil. Soc.* **146**(2) (2009), 303–319.
[8] A. SCHINZEL and W. SIERPIŃSKI. Sur certaines hypothèses concernant les nombres premiers. *Acta Arith.* **4**(3) (1958), 185–208.

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press

[9] A. SCHINZEL and J. WÓJCIK. On a problem in elementary number theory. *Math. Proc. Camb. Phil. Soc.* **112**(2) (1992), 225–232.

[10] J. WÓJCIK. On a problem in algebraic number theory. *Math. Proc. Camb. Phil. Soc.* **119**(2) (1996), 191–200.

https://doi.org/10.1017/S0305004125101758 Published online by Cambridge University Press