Acta Academiae Paedagogicae Agriensis, Sectio Mathematicae **30** *(2003) 147–165*

ON THE CONGRUENCE $u_n \equiv c \pmod{\mathfrak{p}}$, WHERE u_n IS A RECURRING SEQUENCE OF THE SECOND ORDER

Andrzej Schinzel (Warsaw, Poland)

Dedicated to the memory of Professor Péter Kiss

1. Introduction

The following assertion has been proved in [1] as a by-product of a study of exponential congruences (Corollary to Theorem 5). Let a sequence u_n of rational integers satisfy the recurrence relation $u_{n+1} = au_n + bu_{n-1}$, where $a^2 + 4b \neq 0$. If the congruence $u_n \equiv c \pmod{p}$ is soluble for almost all primes p and either $b = 0, -1$ or $b = 1$, $a \neq d^3 + 3d$ (d integer), then $c = u_m$ for an integer m.

The aim of this paper is to extend this result as follows.

Theorem 2. *Let K be a number field, u_n a sequence of elements of K satisfying the relation*

$$u_{n+1} = au_n + bu_{n-1}, \quad \text{where } a^2 + 4b \neq 0. \tag{1}$$

If $c \in K$, the congruence $u_n \equiv c \pmod{\mathfrak{p}}$ is soluble for almost all prime ideals $\mathfrak{p}$ of K and either $b = 0, -1$ or $b = 1$, $a = 0$ or $b = 1$, $a^2 + 4 \neq d^2$ (d an integer of K), then $c = u_m$, where m is an integer.

Corollary 1. *Let a sequence u_n of rationals satisfy the recurrence relation* (1). *If $c \in \mathbf{Q}$, the congruence $u_n \equiv c \pmod{p}$ is soluble for almost all primes p and $b = 0$, or ± 1, then $c = u_m$ for an integer m.*

Comparing Corollary 1 with Corollary quoted above from [1] we see that now u_n need not be integers and the condition $a \neq d^3 + 3d$ has disappeared.

Corollary 2. *Let K be an imaginary quadratic field and u_n a sequence of elements of K satisfying the recurrence relation* (1). *If $c \in K$, the congruence $u_n \equiv c \pmod{\mathfrak{p}}$ is soluble for almost all prime ideals $\mathfrak{p}$ of K and $b = 0$, or ± 1, then $c = u_m$ for an integer m.*

Theorem 2 is a consequence of the following theorem concerning exponential congruences.

Theorem 1. *Let K be a number field, $\alpha \in K^*$, $f \in K[z]$, $\deg f \leq 4$. The congruence*

$$f(\alpha^x) \equiv 0 \pmod{\mathfrak{p}}$$

is soluble for almost all prime ideals $\mathfrak{p}$ *of* K*, if and only if one of the following cases holds for a* β *in the splitting field of* f

$$z - \alpha^r \mid f(z), \quad r \in \mathbf{Z} \tag{2}$$

$$\alpha = \beta^2,\ \left(z - \beta^{2r_1+1}\right)\left(z + \beta^{2r_2}\right)\left(z + \beta^{2r_3+1}\right) \mid f(z),\ r_i \in \mathbf{Z}; \tag{3}$$

$$\alpha = \beta^2,\ \left(z - \beta^{2r_1+1}\right)\left(z - \zeta_4^{e_2}\beta^{2r_2}\right)\left(z + \beta^{2r_3+1}\right)\left(z - \zeta_4^{e_4}\beta^{2r_4+1}\right) \mid f(z),\ r_i \in \mathbf{Z},\ e_2e_4 \text{ odd}; \tag{4}$$

$$\alpha = \beta^3,\ (z - \beta^{r_1})(z - \zeta_3^{e_2}\beta^{r_2})(z - \zeta_3^{e_3}\beta^{r_3})(z - \zeta_3^{e_4}\beta^{r_4}) \mid f(z),\ r_i \in \mathbf{Z},\ e_2r_1 \not\equiv 0,\ r_2 \equiv 0,\ e_3r_3 \equiv -1,\ e_4r_4 \equiv 1 \pmod 3; \tag{5}$$

$$\alpha = \beta^4,\ \left(z - \beta^{2r_1+1}\right)\left(z + \beta^{4r_2}\right)\left(z + \beta^{2r_3+1}\right)\left(z + \beta^{4r_4+2}\right) \mid f(z),\ r_i \in \mathbf{Z}; \tag{6}$$

ζ_q *denotes a root of unity of order* q*.*

Remark. In principle one could obtain a similar result for degree f bounded by any number b. However, the number of possibilities increases fast with b and the matter gets out of hand (cf. Theorem 5 in [1]).

Definition. A system of congruences $A_{h0}t_0 + A_{h1}t_1 \equiv 0 \pmod{m_h}$ $(1 \le h \le g)$ is covering, if every integer vector $[t_0, t_1]$ satisfies at least one of these congruences.

Lemma 1. *A system of congruences*

$$A_{h0}t_0 + A_{h1}t_1 \equiv 0 \pmod m \quad (1 \le h \le 4) \tag{7}$$

is covering, if and only if one of the following cases holds:

$$\text{for an } h_0 \le 4 : m \mid (A_{h_0 0}, A_{h_0 1})\,; \tag{8}$$

$$2 \mid m \text{ and for three distinct indices } h_1, h_2, h_3 \le 4 \tag{9}$$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod m,$$
$$A_{h_2 0} \equiv \frac{m}{2}, \quad A_{h_2 1} \equiv 0 \pmod m,$$
$$A_{h_3 0} \equiv 0, \quad A_{h_3 1} \equiv \frac{m}{2} \pmod m;$$

(10) $3 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \varepsilon_1 \frac{m}{3} \pmod{m},$$
$$A_{h_2 0} \equiv \varepsilon_2 \frac{m}{3}, \quad A_{h_2 0} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \varepsilon_3 \frac{m}{3} \pmod{m},$$
$$A_{h_4 0} \equiv -A_{h_4 1} \equiv \varepsilon_4 \frac{m}{3} \pmod{m};$$

where $[\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4] \in \{-1, 1\}^4$.

(11) $4 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_2 0} \equiv \frac{m}{2}, \quad A_{h_2 1} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \varepsilon_3 \frac{m}{4} \pmod{m},$$
$$A_{h_4 0} \equiv -A_{h_4 1} \equiv \varepsilon_4 \frac{m}{4} \pmod{m},$$

where $[\varepsilon_3, \varepsilon_4] \in \{1, -1\}^2$;

(12) $4 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_2 0} \equiv \varepsilon_2 \frac{m}{4}, \quad A_{h_2 1} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_4 0} \equiv \varepsilon_4 \frac{m}{4}, \quad A_{h_4 1} \equiv \frac{m}{2} \pmod{m},$$

where $[\varepsilon_2, \varepsilon_4] \in \{-1, 1\}^2$;

(13) $4 \mid m$ *and for a permutation* (h_1, h_2, h_3, h_4) *of* $(1, 2, 3, 4)$

$$A_{h_1 0} \equiv 0, \quad A_{h_1 1} \equiv \varepsilon_1 \frac{m}{4} \pmod{m},$$
$$A_{h_2 0} \equiv \frac{m}{2}, \quad A_{h_2 1} \equiv 0 \pmod{m},$$
$$A_{h_3 0} \equiv A_{h_3 1} \equiv \frac{m}{2} \pmod{m},$$
$$A_{h_4 0} \equiv \frac{m}{2}, \quad A_{h_4 1} \equiv \varepsilon_4 \frac{m}{4} \pmod{m},$$

where $[\varepsilon_1, \varepsilon_4] \in \{-1, 1\}^2$.

Proof necessity. Since each of the vectors $[1, 0]$ and $[0, 1]$ satisfies one of the congruences (7) we have for some h_1, h_2

$$A_{h_1 0} \equiv 0, \quad A_{h_2 1} \equiv 0 \pmod m.$$

If $h_1 = h_2 = h$ we have the case (8), thus assume $h_2 \neq h_1$. Since each of the vectors $[1, -1]$ and $[1, 1]$ satisfies one of the congruences (7) we have for some j_1, j_2

$$A_{j_1 0} - A_{j_1 1} \equiv 0, \quad A_{j_2 0} + A_{j_2 1} \equiv 0 \pmod m. \tag{14}$$

If $j_i \in \{h_1, h_2\}$ ($i = 1$ or 2), we have the case (9) with $h_3 = j_i$, thus we assume $j_i \notin \{h_1, h_2\}$ ($i = 1, 2$) and distinguish two cases:

$$j_1 \neq j_2 \tag{15}$$

and

$$j_1 = j_2. \tag{16}$$

In the case (15) excluding the case (8) we infer that $A_{h_1 1} \not\equiv 0 \pmod m$, $A_{h_2 0} \not\equiv 0 \pmod m$, $A_{j_1 0} \not\equiv 0 \pmod m$, $A_{j_2 0} \not\equiv 0 \pmod m$. Since each of the vectors $[\pm 2, 1]$, $[1, \pm 2]$ satisfies one of the congruences (7) for $h \in \{h_1, h_2, j_1, j_2\}$ we infer that either

$$2 \mid m, \quad A_{h_1 1} \equiv A_{h_2 0} \equiv \frac{m}{2} \pmod m, \tag{15.1}$$

or

$$3 \mid m, \quad A_{j_i 0} \equiv \varepsilon_{i+2} \frac{m}{3} \pmod m, \quad [\varepsilon_3, \varepsilon_4] \in \{-1, 1\}^2. \tag{15.2}$$

In the case (15.1), since each of the vectors $[\pm 3, 1]$ satisfies one of the congruences (7) for $h \in \{j_1, j_2\}$, we infer that either for an $i \leq 2$, $A_{j_i 0} \equiv \frac{m}{2} \pmod m$, or $4 \mid m$ and $A_{j_i 0} \equiv \varepsilon_{i+2} \frac{m}{4} \pmod m$ ($i = 1, 2$) where $[\varepsilon_3, \varepsilon_4] \in \{-1, 1\}^2$. In the former case we have (9) with $h_3 = j_i$, in the latter case we have (11) with $h_i = j_{i-2}$ ($i = 3, 4$). In the case (15.2), since each of the vectors $[3, 1]$, $[1, 3]$ satisfies one of the congruences (7) for $h \in \{h_1, h_2\}$ we infer that

$$A_{h_1 1} \equiv \varepsilon_1 \frac{m}{3} \pmod m, \quad A_{h_2 0} \equiv \varepsilon_2 \frac{m}{3} \pmod m$$

where $[\varepsilon_1, \varepsilon_2] \in \{-1, 1\}^2$, thus we have the case (10) with $h_i = j_{i-2}$ for $i = 3, 4$.

Consider now the case (16). Excluding (8) we infer that

$$A_{h_1 1} \not\equiv 0 \pmod m,$$
$$A_{h_2 0} \not\equiv 0 \pmod m,$$
$$A_{j_1 0} \equiv A_{j_1 1} \equiv \frac{m}{2} \pmod m.$$

Let $\{j_3\} = \{1,2,3,4\} \setminus \{h_1, h_2, j_1\}$. Since each of the vectors $[1, \pm 2]$, $[\pm 2, 1]$ satisfies one of the congruences (7) we infer that either

$$2 \mid m, \quad A_{h_1 1} \equiv \frac{m}{2} \pmod m, \tag{16.1}$$

or

$$2 \mid m, \quad A_{h_2 0} \equiv \frac{m}{2} \pmod m \tag{16.2}$$

or

$$\begin{aligned} A_{j_3,0} \pm 2A_{j_3,1} &\equiv 0 \pmod m, \\ \pm 2A_{j_3,0} + A_{j_3,1} &\equiv 0 \pmod m. \end{aligned} \tag{16.3}$$

The conditions (16.3) lead to (8) with $h = j_3$, the conditions (16.1) and (16.2) together lead to (9) with $h_3 = j_1$. If (16.1) holds but (16.2) does not, then since each of the vectors $[\pm 2, 1]$ satisfies one of congruences (7) for $h \in \{h_2, j_3\}$, we have

$$\pm 2A_{j_3,0} + A_{j_3,1} \equiv 0 \pmod m, \tag{17}$$

hence

$$\pm 4A_{j_3,0} \equiv 2A_{j_3,1} \equiv 0 \pmod m.$$

If

$$A_{j_3,1} \equiv 0 \pmod m,$$

then either $A_{j_3,0} \equiv 0 \pmod m$, which gives (8) with $h = j_3$, or $A_{j_3,0} \equiv \frac{m}{2} \pmod m$, which gives (9) with $h_2 = j_3$, $h_3 = j_1$. If $A_{j_3,1} \equiv \frac{m}{2} \pmod m$, then (17) implies $4 \mid m$,

$$A_{j_3,0} \equiv \varepsilon_4 \frac{m}{4} \pmod m,$$

which gives (12) with $h_3 = j_1$, $h_4 = j_3$. If (16.2) holds but (16.1) does not, then by symmetry we have (8) or (9) or (13).

Sufficiency of the condition follows from the easily verified fact, that the following systems of congruences are covering:
$0 \equiv 0 \pmod 1$; $t_1 \equiv 0$, $t_0 \equiv 0$, $t_0 + t_1 \equiv 0 \pmod 2$; $t_1 \equiv 0$, $t_0 \equiv 0$, $t_0 + t_1 \equiv 0$, $t_0 - t_1 \equiv 0 \pmod 3$; $t_1 \equiv 0$, $t_0 \equiv 0 \pmod 2$, $t_0 + t_1 \equiv 0$, $t_0 - t_1 \equiv 0 \pmod 4$;

$t_1 \equiv 0,\ t_0 + t_1 \equiv 0 \pmod 2,\ t_0 \equiv 0,\ t_0 + 2t_1 \equiv 0 \pmod 4;\ t_0 \equiv 0,\ t_0 + t_1 \equiv 0 \pmod 2,\ t_1 \equiv 0,\ 2t_0 + t_1 \equiv 0 \pmod 4$.

Lemma 2. *If K is a number field, $\alpha \in K$, $\beta_j \in \overline{\mathbf{Q}}$ $(1 \le j \le l)$, the congruence*

$$\prod_{j=1}^{l} (\alpha^x - \beta_j) \equiv 0 \pmod{\mathfrak{p}} \tag{18}$$

is soluble for almost all prime ideals $\mathfrak{p}$ of the field $K(\beta_1, \dots, \beta_l) =: K_1$ and w is the number of roots of unity contained in K_1, then there exist $\gamma \in K_1$ and a subset H of $\{1, \dots, l\}$ such that

$$\alpha = \zeta_w^a \gamma^e, \tag{19}$$

$$\beta_h = \zeta_w^{b_h} \gamma^{d_h} \quad (h \in H) \tag{20}$$

and the system of congruences

$$t_0 (ad_h - eb_h) + wd_h t_1 \equiv 0 \pmod{we} \quad (h \in H) \tag{21}$$

is covering.

Proof. Let

$$\alpha = \zeta_w^{a_0} \prod_{s=1}^{t} \pi_s^{a_s}, \quad \beta_j = \zeta_w^{b_{j0}} \prod_{s=1}^{t} \pi_s^{b_{js}} \quad (1 \le j \le l), \tag{22}$$

where π_s are elements of the multiplicative basis of the field K_1 (see [1], Lemma 9). Let Q be a unimodular matrix such that

$$[a_1, \dots, a_t]\, Q = [e, 0, \dots, 0], \quad e = (a_1, \dots, a_t) \tag{23}$$

and put

$$[b_{j1}, \dots, b_{jt}]\, Q = [d_{j1}, \dots, d_{jt}]. \tag{24}$$

We choose integers $\eta_2, \dots, \eta_t$ divisible by w such that for all $j \le l$

$$\sum_{s=2}^{t} d_{js}\eta_s = 0 \text{ implies } d_{j_s} = 0 (2 \le s \le t) \tag{25}$$

and set

$$m = \max_{1 \le j \le l} \left| \sum_{s=2}^{t} d_{js}\eta_s \right| + 1. \tag{26}$$

Further we set

$$n = 2^\tau wme \operatorname*{l.c.m.}_{\substack{q \le m+e \\ q \text{ prime}}} (q-1),\ \eta_1 = \frac{n}{e}t_1 + a_0\frac{n}{ew}t_0, \tag{27}$$

where τ is the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K_1$,

$$\varepsilon_0 = -t_0, \quad \begin{bmatrix} \varepsilon_1 \\ \vdots \\ \varepsilon_t \end{bmatrix} = Q \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_t \end{bmatrix}. \tag{28}$$

By Theorem 4 of [1] there exist infinitely many prime ideals $\mathfrak{P}$ of $K_1(\zeta_n)$ such that

$$\left(\frac{\zeta_w}{\mathfrak{P}}\right)_n = \zeta_w^{\varepsilon_0}, \quad \left(\frac{\pi_s}{\mathfrak{P}}\right)_n = \zeta_n^{\varepsilon_s} \quad (1 \le s \le t). \tag{29}$$

Let H be the set of these indices $h \le l$ that for some integers x, t_0, t_1 and for some prime ideal $\mathfrak{P}$ satisfying (29) we have

$$\alpha^x \equiv \beta_h \pmod{\mathfrak{P}}. \tag{30}$$

The congruence (30) gives

$$\left(\frac{\alpha^x}{\mathfrak{P}}\right)_n = \left(\frac{\beta_h}{\mathfrak{P}}\right)_n,$$

hence

$$x\left(\frac{n}{w}a_0\varepsilon_0 + \sum_{s=1}^{t} a_s\varepsilon_s\right) \equiv \frac{n}{w}b_{h0}\varepsilon_0 + \sum_{s=1}^{t} b_{hs}\varepsilon_s \pmod{n}$$

and by (24) and (28)

$$x\left(-\frac{n}{w}a_0t_0 + e\eta_1\right) \equiv -\frac{n}{w}b_{h0}t_0 + \sum_{s=1}^{t} d_{hs}\eta_s \pmod{n}.$$

Substituting the value of η_1 from (27) we obtain

$$0 \equiv nxt_1 \equiv -\frac{n}{w}b_{h0}t_0 + \frac{n}{w}d_{h1}\left(\frac{w}{e}t_1 + \frac{a_0}{e}t_0\right) + \sum_{s=2}^{t} d_{hs}\eta_s \pmod{n}. \tag{31}$$

It follows that

$$\sum_{s=2}^{t} d_{hs}\eta_s \equiv 0 \pmod{m}$$

and, by (26) and (25),

$$\sum_{s=2}^{t} d_{hs}\eta_s = 0, \quad d_{hs} = 0 \ (2 \le s \le t). \tag{32}$$

Hence, by (23) and (24),

$$b_{hs} = \frac{d_{h1}}{e} a_{hs}$$

and putting $a_0 = a$, $b_{h0} = b_h$, $d_{h1} = d_h$

$$\gamma = \prod_{s=1}^{t} \pi_s^{a_s/e}$$

we obtain (20) and (21). Moreover, since the congruence (18) is soluble for almost all prime ideals $\mathfrak{p}$ of K_1 the system of congruences, resulting from (31) and (32)

$$(ad_h - eb_h)\, t_0 + wd_h t_1 \equiv 0 \pmod{we} \quad (h \in H) \tag{33}$$

must be covering.

Remark. The above proof is modelled on the proof of Theorem 5 in [1].

Lemma 3. *If a system of congruences*

$$A_{h0}t_0 + A_{h1}t_1 \equiv 0 \pmod{m} \quad (1 \le h \le g) \tag{34}$$

is covering, $w \mid m$, $d = (m, A_{11}, \dots, A_{g1})$ and $\alpha = \beta^{m/d}$, then the alternative of congruences

$$\alpha^x \equiv \zeta_w^{A_{h0}} \beta^{A_{h1}/d} \pmod{\mathfrak{p}} \quad (1 \le h \le g)$$

is soluble for all prime ideals $\mathfrak{p}$ of $\mathbf{Q}(\zeta_w, \beta)$ for which β is a $\mathfrak{p}$-adic unit.

Proof. Since the system (34) is covering, for every prime ideal $\mathfrak{p}$ there exists an $h \le g$ such that

$$A_{h0} \frac{d\frac{N\mathfrak{p}-1}{w}}{\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right)} + A_{h1} \frac{\operatorname{ind}\beta}{\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right)} \equiv 0 \pmod{m},$$

hence

$$A_{h0}\frac{N\mathfrak{p}-1}{w} + \frac{A_{h1}}{d}\operatorname{ind}\beta \equiv 0 \left(\operatorname{mod} \frac{m}{d}\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right)\right).$$

However

$$\frac{m}{d}\left(\operatorname{ind}\beta, d\frac{N\mathfrak{p}-1}{w}\right) \equiv 0 \ (\operatorname{mod}(\operatorname{ind}\alpha, N\mathfrak{p}-1)),$$

hence the congruence

$$A_{h0}\frac{N\mathfrak{p}-1}{w}+\frac{A_{h1}}{d}\operatorname{ind}\beta \equiv x \operatorname{ind}\alpha \pmod{N\mathfrak{p}-1}$$

is soluble for x and we obtain

$$\alpha^x \equiv \zeta_w^{A_{h0}}\beta^{A_{h1}/d} \pmod{\mathfrak{p}}.$$

Proof of Theorem 1. Necessity.

By Lemma 2 the system (33) is covering, hence we apply Lemma 1 with

$$A_{h0} = ad_h - eb_h, \quad A_{h1} = wd_h.$$

If the case (8) holds, then for a certain $h \in H$

$$ad_h - eb_h \equiv wd_h \equiv 0 \pmod{we},$$

hence $e \mid d_h$ and $b_h \equiv a\frac{d_h}{e} \pmod{w}$, which gives

$$\beta_h = \alpha^{d_h/e}$$

hence (2) holds with $r = d_h/e$.

If the case (9) holds, then for some distinct indices h_1, h_2, h_3

$$ad_{h_1} - eb_{h_1} \equiv 0, \quad wd_{h_1} \equiv \frac{we}{2} \pmod{we},$$

hence $2 \mid e$, $d_{h_1} \equiv \frac{e}{2}c_1$, c_1 odd, $2 \mid a$, $b_{h_1} \equiv \frac{a}{2}c_1 \pmod{w}$;

$$ad_{h_2} - eb_{h_2} \equiv \frac{we}{2}, \quad wd_{h_2} \equiv 0 \pmod{we},$$

hence $d_{h_2} = ec_2$, $c_2 \in \mathbf{Z}$, $b_{h_2} \equiv \frac{w}{2} + ac_2 \pmod{w}$;

$$ad_{h_3} - eb_{h_3} \equiv wd_{h_3} \equiv \frac{we}{2} \pmod{we},$$

hence $d_{h_3} = \frac{e}{2}c_3$, c_3 odd, $b_{h_3} \equiv \frac{w}{2} + ac_3 \pmod{w}$.

This gives (3) with

$$\beta = \zeta_w^{a/2}\gamma^{e/2}, \quad 2r_1 + 1 = c_1, \quad r_2 = c_2, \quad 2r_3 + 1 = c_3.$$

If the case (10) holds, $3 \mid we$ and without loss of generality we may assume that

$$ad_1 - eb_1 \equiv 0, \quad wd_1 \equiv \varepsilon_1\frac{we}{3} \pmod{we},$$

hence $3 \mid e$, $d_1 \equiv \frac{e}{3}\varepsilon_1 \pmod e$, $3 \mid a$, $b_1 \equiv \frac{a}{3}\frac{3d_1}{e} \pmod w$;

$$ad_2 - eb_2 \equiv \varepsilon_2 \frac{we}{3}, \quad wd_2 \equiv 0 \pmod{we},$$

hence $e \mid d_2$, $3 \mid w$, $b_2 \equiv \frac{d_2}{e} - \varepsilon_2 \frac{w}{3} \pmod w$;

$$ad_3 - eb_3 \equiv wd_3 \equiv \varepsilon_3 \frac{we}{3} \pmod{we},$$

hence $d_3 \equiv \varepsilon_3 \frac{e}{3} \pmod e$, $b_3 \equiv \frac{a}{3}\frac{3d_3}{e} - \varepsilon_3 \frac{w}{3} \pmod w$;

$$ad_4 - eb_4 \equiv -wd_4 \equiv \varepsilon_4 \frac{we}{3} \pmod{we},$$

hence $d_4 \equiv -\varepsilon_4 \frac{e}{3} \pmod e$, $b_4 \equiv \frac{a}{3}\frac{3d_4}{e} - \varepsilon_4 \frac{w}{3} \pmod w$.

This gives (5) with

$$\beta = \zeta_w^{a/3}\gamma^{e/3}, \quad r_i = \frac{3d_i}{e} \quad (1 \le i \le 4), \quad e_i \equiv -\varepsilon_i \pmod 3 \quad (2 \le i \le 4).$$

If the case (11) holds, $4 \mid we$ and without loss of generality we may assume that

$$ad_1 - eb_1 \equiv 0, \quad wd_1 \equiv \frac{we}{2} \pmod{we}, \tag{35}$$

$$ad_2 - eb_2 \equiv \varepsilon_2 \frac{we}{2}, \quad wd_2 \equiv 0 \pmod{we}, \tag{36}$$

$$ad_3 - eb_3 \equiv wd_3 \equiv \varepsilon_3 \frac{we}{4} \pmod{we}, \tag{37}$$

$$ad_4 - eb_4 \equiv -wd_4 \equiv \varepsilon_4 \frac{we}{4} \pmod{we}. \tag{38}$$

(35) implies $2 \mid e$ and $d_1 \equiv \frac{e}{2} \pmod e$, $2 \mid a$, $b_1 \equiv \frac{a}{2} \cdot \frac{2d_1}{e} \pmod w$, (36) implies $d_2 \equiv 0 \pmod e$, $b_2 \equiv a\frac{d_2}{e} - \frac{w}{2} \pmod w$, (37) implies $4 \mid e$, $a \equiv w \pmod 4$. Now, we distinguish two subcases

$$w \equiv 2 \pmod 4 \tag{39.1}$$

and

$$w \equiv 0 \pmod 4. \tag{39.2}$$

In the case (39.1) we take

$$\beta = \zeta_w^{\frac{a(w+2)}{8}}\gamma^{e/4}$$

and find

$$\begin{aligned}
\alpha &= \zeta_w^a \gamma^e = \beta^4,\\
\beta_1 = \zeta_w^{b_1}\gamma^{d_1} &= \zeta_w^{\frac{a}{2}\cdot\frac{2d_1}{e}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_1}{e}} \beta^{4d_1}\\
&= \zeta_w^{\frac{2d_1}{e}\left(\frac{a}{2}-\frac{a(w+2)}{4}\right)}\beta^{4d_1/e} = \zeta_w^{-\frac{awd_1}{2e}}\beta^{4d_1/e} = \zeta_w^{\frac{w}{2}}\beta^{4d_1/e} = -\beta^{\frac{4d_1}{e}},\\
\beta_2 = \zeta_w^{b_2}\gamma^{d_2} &= -\zeta_w^{a\frac{d_2}{e}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_2}{e}} \beta^{4d_2}\\
&= -\zeta_w^{\frac{d_2}{e}\left(a-\frac{a(w+2)}{2}\right)}\beta^{4d_2/e} = -\zeta_w^{r-\frac{d_2}{e}\cdot\frac{aw}{2}}\beta^{4d_2/e} = -\beta^{\frac{4d_2}{e}}.
\end{aligned}$$

(37) implies $4 \mid e$, $d_3 \equiv \varepsilon_3\frac{e}{4} \pmod{e}$, $b_3 \equiv \frac{ac_3-\varepsilon_3 w}{4} \pmod{w}$, $c_3 = \frac{4d_3}{e} \equiv \varepsilon_3 \pmod 4$,

$$\begin{aligned}
\beta_3 = \zeta_w^{b_3}\gamma^{d_3} &= \zeta_w^{\frac{ac_3-\varepsilon_3 w}{4}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_3}{e}} \beta^{\frac{4d_3}{e}}\\
&= \zeta_w^{\left(-\frac{a}{2}c_3-\varepsilon_3\right)\frac{w}{4}}\beta^{4d_3/e} = (-1)^{\frac{a+2}{4}}\beta^{\frac{4d_3}{e}}.
\end{aligned}$$

(38) implies $4 \mid e$, $d_4 \equiv -\varepsilon_4\frac{e}{4} \pmod{e}$, $b_4 \equiv \frac{ac_4-\varepsilon_4 w}{4} \pmod{w}$, $c_4 = \frac{4d_4}{e} \equiv -\varepsilon_4 \pmod 2$,

$$\begin{aligned}
\beta_4 = \zeta_w^{b_4}\gamma^{d_4} &= \zeta_w^{\frac{ac_4-\varepsilon_4 w}{4}} \left(\zeta_w^{-\frac{a(w+2)}{8}}\right)^{\frac{4d_4}{e}} \beta^{\frac{4d_4}{e}}\\
&= \zeta_w^{\left(-\frac{a}{2}c_4-\varepsilon_4\right)\frac{w}{4}}\beta^{4d_4/e} = (-1)^{\frac{a-2}{4}}\beta^{\frac{4d_4}{e}}
\end{aligned}$$

and we obtain the case (6).

Consider now the case (39.2). Here (37) implies $4 \mid a$, we take

$$\beta = \zeta_w^{\frac{a-w}{4}}\gamma^{e/4}$$

and find

$$\begin{aligned}
&\alpha = \zeta_w^a\gamma^e = \beta^4,\\
&\beta_1 = \zeta_w^{b_1}\gamma^{d_1} = \zeta_w^{ad_1/e}\gamma^{d_1} = -\beta^{4d_1/e},\\
&\beta_2 = \zeta_w^{b_2}\gamma^{d_2} = -\zeta_w^{ad_2/e}\gamma^{d_2} = -\beta^{4d_2/e}.
\end{aligned}$$

Moreover, (37) gives $d_3 \equiv \varepsilon_3\frac{e}{4} \pmod{e}$, $b_3 \equiv \frac{ad_3}{e} - \varepsilon_3\frac{w}{4} \pmod{w}$, hence

$$\beta_3 = \zeta_4^{-\varepsilon_3}\zeta_w^{ad_3/e}\gamma^{d_3} = \beta^{4d_3/e};$$

(38) gives $d_4 \equiv -\varepsilon_4 \frac{e}{4} \pmod e$, $b_4 \equiv \frac{ad_4}{e} - \varepsilon_4 \frac{w}{4} \pmod w$, hence

$$\beta_4 = \zeta_4^{-\varepsilon_4} \zeta_w^{ad_4/e} \gamma^{d_4} = -\beta^{4d_4/e}$$

and we obtain again the case (6).

Consider now the case (12). Here we have

$$ad_1 - eb_1 \equiv 0 \pmod{we}, \quad wd_1 \equiv \varepsilon_1 \frac{we}{4} \pmod{we},$$

hence $4 \mid e$, $d_1 \equiv \varepsilon_1 \frac{e}{4} \pmod e$, $4 \mid a$, $b_1 \equiv \frac{ad_1}{e} \pmod w$;

$$ad_2 - eb_2 \equiv \frac{we}{2} \pmod{we}, \quad wd_2 \equiv 0 \pmod{we},$$

hence $d_2 \equiv 0 \pmod e$, $b_2 \equiv \frac{ad_2}{e} - \frac{a}{2} \pmod w$;

$$ad_3 - eb_3 \equiv wd_3 \equiv \frac{we}{2} \pmod{we},$$

hence $d_3 \equiv \frac{e}{2} \pmod e$, $b_3 \equiv \frac{ad_3}{e} - \frac{w}{2} \pmod w$;

$$ad_4 - eb_4 \equiv \frac{we}{2} \pmod{we}, \quad wd_4 \equiv \varepsilon_4 \frac{we}{4} \pmod{we},$$

hence $d_4 \equiv \varepsilon_4 \frac{e}{4} \pmod e$, $b_4 \equiv \frac{ad_4}{e} - \frac{w}{2} \pmod w$.

Therefore, setting

$$\beta = \zeta_w^{a/4} \gamma^{e/4}$$

we obtain

$$\alpha = \beta^4, \ \beta_1 = \beta^{4d_1/e}, \ \beta_2 = -\beta^{4d_2/e}, \ \beta_3 = -\beta^{4d_3/e}, \ \beta_4 = -\beta^{4d_4/e},$$

which is again the case (6).

Consider now the case (13). Here we have

$$ad_1 - eb_1 \equiv 0 \pmod{we}, \quad wd_1 \equiv \frac{we}{4} \pmod{we},$$

hence $2 \mid e$, $d_1 \equiv \frac{e}{4} \pmod e$, $2 \mid a$, $b_1 \equiv \frac{ad_1}{e} \pmod w$;

$$ad_2 - eb_2 \equiv \varepsilon_2 \frac{we}{4} \pmod{we}, \quad wd_2 \equiv 0 \pmod{we},$$

hence $d_2 \equiv 0 \pmod e$, $4 \mid w$, $b_2 \equiv ad_2 - \varepsilon_2 \frac{a}{2} \pmod w$;

$$ad_3 - eb_3 \equiv wd_3 \equiv \frac{we}{2} \pmod{we},$$

hence $d_3 \equiv \frac{e}{2} \pmod{e}$, $b_3 \equiv ad_3 - \frac{w}{2} \pmod{w}$;

$$ad_4 - eb_4 \equiv \varepsilon_4 \frac{we}{4} \pmod{we}, \quad wd_4 \equiv \frac{we}{2} \pmod{we},$$

hence $d_4 \equiv \frac{e}{2} \pmod{e}$, $b_4 \equiv \frac{ad_4}{e} - \varepsilon_4 \frac{w}{4} \pmod{w}$.

Therefore, setting

$$\beta = \zeta_w^{a/4} \gamma^{e/4}$$

we obtain

$$\alpha = \beta^2,\ \beta_1 = \beta^{2d_1/e},\ \beta_2 = \zeta_4^{-\varepsilon_2} \beta^{2d_2/e},\ \beta_3 = -\beta^{2d_3/e},\ \beta_4 = \zeta_4^{-\varepsilon_4} \beta^{2d_4/e},$$

which is the case (4).

Sufficiency of the condition follows from Lemma 3 and the covering property of the relevant systems of congruences, which in turn follows from Lemma 1. Indeed, a prime ideal $\mathfrak{p}$ of K is divisible by a prime ideal $\mathfrak{P}$ of $K(\zeta_w, \beta)$, which in turn divides a prime ideal $\mathfrak{q}$ of $\mathbf{Q}(\zeta_w, \beta)$. Solubility of the congruence

$$\prod_{h=1}^{g} \left(\alpha^x - \zeta_w^{A_{h0}} \beta^{A_{h1}/d} \right) \equiv 0 \pmod{\mathfrak{q}}$$

implies solubility of the congruence $f(\alpha^x) \equiv 0 \pmod{\mathfrak{P}}$, and this, since $f \in K[z]$, solubility of $f(\alpha^x) \equiv 0 \pmod{\mathfrak{p}}$.

Lemma 4. *If $u_n = \lambda_1 \alpha^n + \lambda_2 (-\alpha^{-1})^n$ is a recurring sequence in K and α is a root of unity, then solubility of the congruence*

$$u_n \equiv c \pmod{\mathfrak{p}}$$

for infinitely many prime ideals $\mathfrak{p}$ of K implies $c = u_m$, where m is an integer.

Proof. If α is a root unity of order q we have $u_n \in \{u_1, \ldots, u_{2q}\}$, hence if $c \neq u_m$ the congruence in question is soluble for only finitely many prime ideals $\mathfrak{p}$ dividing

$$\prod_{m=1}^{2q} (u_n - c).$$

Proof of Theorem 2. If $b = 0$ we have $u_n = \lambda \alpha^n$ and the assertion follows from Theorem 1 applied to the polynomial $f(z) = \lambda z - c$.

If $b = -1$, we have $u_n = \lambda_1 \alpha^n + \lambda_2 \alpha^{-n}$ and the assertion follows from Theorem 1 applied to the polynomial $f(z) = \lambda_1 z^2 - cz + \lambda_2$.

If $b = 1$, $a = 0$ we have $\alpha = \pm 1$ and the assertion follows by virtue of Lemma 4.

If $b = 1$, $c = 0$ or $\lambda_1 = 0$ or $\lambda_2 = 0$ the assertion follows from Theorem 1 applied to the polynomial $f(z) = \lambda_1 z + \lambda_2$ or $\lambda_2 z - c$ or $\lambda_1 z - c$, respectively. Therefore, assume $b = 1$, $ac\lambda_1\lambda_2 \neq 0$.

Solubility of the congruence $u_n \equiv c \pmod{\mathfrak{p}}$ is equivalent to solubility of the congruence

$$f\left(\alpha^{2n}\right) \equiv 0 \pmod{\mathfrak{p}},$$

where

$$f(z) = \left(\lambda_1 z^2 - cz + \lambda_2\right)\left(\lambda_1\alpha^2 z^2 - c\alpha z - \lambda_2\right).$$

We apply Theorem 1 with α^2 in stead of α, considering successively the cases (2)–(6).

In the case (2) we have $z - \alpha^{2r} \mid f(z)$, hence either $z - \alpha^{2r} \mid \lambda_1 z^2 - cz + \lambda_2$, or $z - \alpha^{2r} \mid \lambda_1\alpha^2 z^2 - c\alpha z - \lambda_2$. In the former case $u_n = c$ has the solution $n = 2r$, in the latter case $n = 2r + 1$.

In the case (3) we have one of the following six cases:

$$\begin{aligned}(40.1)\quad &\lambda_1\alpha^{4r_1+2} - c\alpha^{2r_1+1} + \lambda_2 = 0,\ \lambda_1\alpha^{4r_2} + c\alpha^{2r_2} + \lambda_2 = 0,\\ &\lambda_1\alpha^{4r_3+4} + c\alpha^{2r_3+2} - \lambda_2 = 0;\end{aligned}$$

$$\begin{aligned}(40.2)\quad &\lambda_1\alpha^{4r_1+2} - c\alpha^{2r_1+1} + \lambda_2 = 0,\ \lambda_1\alpha^{4r_2+2} + c\alpha^{2r_2+1} - \lambda_2 = 0,\\ &\lambda_1\alpha^{4r_3+2} + c\alpha^{2r_3+1} + \lambda_2 = 0;\end{aligned}$$

$$\begin{aligned}(40.3)\quad &\lambda_1\alpha^{4r_1+2} - c\alpha^{2r_1+1} + \lambda_2 = 0,\ \lambda_1\alpha^{4r_2+2} + c\alpha^{2r_2+1} - \lambda_2 = 0,\\ &\lambda_1\alpha^{4r_3+4} + c\alpha^{2r_3+2} - \lambda_2 = 0;\end{aligned}$$

$$\begin{aligned}(40.4)\quad &\lambda_1\alpha^{4r_1+4} - c\alpha^{2r_1+2} - \lambda_2 = 0,\ \lambda_1\alpha^{4r_2} + c\alpha^{2r_2} + \lambda_2 = 0,\\ &\lambda_1\alpha^{4r_3+2} + c\alpha^{2r_3+1} + \lambda_2 = 0;\end{aligned}$$

$$\begin{aligned}(40.5)\quad &\lambda_1\alpha^{4r_1+4} - c\alpha^{2r_1+2} - \lambda_2 = 0,\ \lambda_1\alpha^{4r_2} + c\alpha^{2r_2} + \lambda_2 = 0,\\ &\lambda_1\alpha^{4r_3+4} + c\alpha^{2r_3+2} - \lambda_2 = 0;\end{aligned}$$

$$\begin{aligned}(40.6)\quad &\lambda_1\alpha^{4r_1+4} - c\alpha^{2r_1+2} - \lambda_2 = 0,\ \lambda_1\alpha^{4r_2+2} + c\alpha^{2r_2+1} - \lambda_2 = 0,\\ &\lambda_1\alpha^{4r_3+2} + c\alpha^{2r_3+1} + \lambda_2 = 0.\end{aligned}$$

Since $c\lambda_1\lambda_2 \neq 0$ at least one of the determinants $\Delta_1, \ldots, \Delta_6$ is 0, where

$$\Delta_1 = \begin{vmatrix} \alpha^{4r_1+2} & -\alpha^{2r_1+1} & 1 \\ \alpha^{4r_2} & \alpha^{2r_2} & 1 \\ \alpha^{4r_3+4} & \alpha^{2r_3+2} & -1 \end{vmatrix}, \quad \Delta_2 = \begin{vmatrix} \alpha^{4r_1+2} & -\alpha^{2r_1+1} & 1 \\ \alpha^{4r_2+2} & \alpha^{2r_2+1} & -1 \\ \alpha^{4r_3+2} & \alpha^{2r_3+1} & 1 \end{vmatrix},$$

$$\Delta_3 = \begin{vmatrix} \alpha^{4r_1+2} & -\alpha^{2r_1+1} & 1 \\ \alpha^{4r_2+2} & \alpha^{2r_2+1} & -1 \\ \alpha^{4r_3+4} & \alpha^{2r_3+2} & -1 \end{vmatrix}, \quad \Delta_4 = \begin{vmatrix} \alpha^{4r_1+4} & -\alpha^{2r_1+2} & -1 \\ \alpha^{4r_2} & \alpha^{2r_2} & 1 \\ \alpha^{4r_3+2} & \alpha^{2r_3+1} & 1 \end{vmatrix},$$

$$\Delta_5 = \begin{vmatrix} \alpha^{4r_1+4} & -\alpha^{2r_1+2} & -1 \\ \alpha^{4r_2} & \alpha^{2r_2} & 1 \\ \alpha^{4r_3+4} & \alpha^{2r_3+2} & -1 \end{vmatrix}, \quad \Delta_6 = \begin{vmatrix} \alpha^{4r_1+4} & -\alpha^{2r_1+2} & -1 \\ \alpha^{4r_2+2} & \alpha^{2r_2+1} & -1 \\ \alpha^{4r_3+2} & \alpha^{2r_3+1} & 1 \end{vmatrix}.$$

Suppose first that α is not an algebraic integer. Then in the expanded form of the determinant Δ_i the highest power of α must occur at least twice. However, the exponents in the first column of Δ_i are twice the exponents in the second column. Denoting the latter by $\delta_{i1}, \delta_{i2}, \delta_{i3}$ in the decreasing order, we infer that the greatest power of α in Δ_i is $\alpha^{2\delta_{i1}+\delta_{i2}}$ and it is not repeated unless two of the numbers δ_{ij} $(j = 1, 2, 3)$ are equal. This gives the following possibilities:

(41.1) $\quad i = 1, \quad r_2 = r_3 + 1;$

(41.2) $\quad i = 2, \quad r_2 = r_1, \quad \text{or} \quad r_3 = r_1, \quad \text{or} \quad r_3 = r_2;$

(41.3) $\quad i = 3, \quad r_2 = r_1;$

(41.4) $\quad i = 4, \quad r_2 = r_1 + 1;$

(41.5) $\quad i = 5, \quad r_2 = r_1 + 1, \quad \text{or} \quad r_3 = r_1, \quad \text{or} \quad r_2 = r_3 + 1;$

(41.6) $\quad i = 6, \quad r_3 = r_2$

and in each case the equation $\Delta_i = 0$ gives α as 0 or a root of unity, contrary to the assumption, that α is not an algebraic integer.

Assume now that α is an algebraic integer. Since $a^2 + 4 \neq d^2$ (d an integer of K) we have $\alpha \notin K$. Hence α is conjugate over K to $-\alpha^{-1}$ and λ_2 is conjugate to λ_1. By (40.1)–(40.6) we have for an $\varepsilon \in \{1, -1\}$,

$$\lambda_1 \left(\alpha^{2r_1+1+\frac{1-\varepsilon}{2}}\right)^2 - c\left(\alpha^{2r_1+1+\frac{1-\varepsilon}{2}}\right) + \varepsilon\lambda_2 = 0, \tag{42}$$

hence

$$\lambda_1 \alpha^{2r_1+1+\frac{1-\varepsilon}{2}} = \frac{c \mp \sqrt{c^2 - 4\varepsilon\lambda_1\lambda_2}}{2}. \tag{43}$$

If $\lambda_1\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} =: \mu \in K$ then

$$\lambda_1 = \mu\alpha^{-2r_1-1-\frac{1-\varepsilon}{2}}, \quad \lambda_2 = \mu\alpha^{2r_1+1+\frac{1-\varepsilon}{2}}(-1)^{\frac{1+\varepsilon}{2}}$$

and from (42)

$$0 = \mu\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} - c\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} + \varepsilon(-1)^{\frac{1+\varepsilon}{2}}\mu\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} = -c\alpha^{2r_1+1+\frac{1-\varepsilon}{2}},$$

contrary to $c \neq 0$.

If $\lambda_1\alpha^{2r_1+1+\frac{1-\varepsilon}{2}} \notin K$, then from (43) on taking conjugates we obtain

$$\lambda_2(-1)^{\frac{1-\varepsilon}{2}}\alpha^{-2r_1-1-\frac{1-\varepsilon}{2}} = \frac{c \pm \sqrt{c^2 - 4\varepsilon\lambda_1\lambda_2}}{2},$$

hence on multiplication side by side with (43)

$$\lambda_1\lambda_2(-1)^{\frac{1+\varepsilon}{2}} = \varepsilon\lambda_1\lambda_2,$$

contrary to $\lambda_1\lambda_2 \neq 0$.

In the case (4) there exists a permutation $(\zeta_4^{\varepsilon_1}\alpha^{\delta_1}, \dots, \zeta_4^{\varepsilon_4}\alpha^{\delta_4})$ of $(\alpha^{2r_1+1}, !\zeta_4^{e_2}\alpha^{2r_2}, -\alpha^{2r_3+1}, \zeta_4^{e_4}\alpha^{2r_4+1})$ such that

$$\frac{\lambda_2}{\lambda_1} = \zeta_4^{\varepsilon_1+\varepsilon_2}\alpha^{\delta_1+\delta_2} = -\zeta_4^{\varepsilon_3+\varepsilon_4}\alpha^{\delta_3+\delta_4+2}. \tag{44}$$

If $\delta_1+\delta_2 = \delta_3+\delta_4+2$, then $2(\delta_1+\delta_2) = \delta_1+\delta_2+\delta_3+\delta_4+2 = 2r_1+2r_2+2r_3+2r_4+5$, which is impossible mod 2. If $\delta_1+\delta_2 \neq \delta_3+\delta_4+2$, then α is a root of unity and the assertion follows by virtue of Lemma 4.

In the case (5) we have

$$\alpha = \gamma^3, \quad \beta = \gamma^2, \quad \text{where } \gamma = \alpha/\beta$$

and there exists a permutation

$$(\zeta_3^{\varepsilon_1}\gamma^{\delta_1}, \dots, \zeta_3^{\varepsilon_4}\gamma^{\delta_4}) \text{ of } (\gamma^{2r_1}, \zeta_3^{e_2}\gamma^{2r_2}, \zeta_3^{e_3}\gamma^{2r_3}, \zeta_3^{e_4}\gamma^{2r_4})$$

such that

$$\frac{\lambda_2}{\lambda_1} = \zeta_3^{\varepsilon_1+\varepsilon_2}\gamma^{\delta_1+\delta_2} = -\zeta_3^{\varepsilon_3+\varepsilon_4}\gamma^{\delta_3+\delta_4+6}.$$

If $\delta_1+\delta_2 = \delta_3+\delta_4+6$, we obtain $\zeta_3^{\varepsilon_1+\varepsilon_2-\varepsilon_3-\varepsilon_4} = -1$, which is impossible. If $\delta_1+\delta_2 \neq \delta_3+\delta_4+6$, then γ is a root of unity and so is α; the assertion follows by virtue of Lemma 4.

In the case (6) we have

$$\alpha = \varepsilon_0\beta^2, \quad (\varepsilon_0 = \pm 1)$$

and there exists a permutation

$(\varepsilon_1\beta^{\delta_1}, \varepsilon_2\beta^{\delta_2}, \varepsilon_3\beta^{\delta_3}, \varepsilon_4\beta^{\delta_4})$ of $(\beta^{2r_1+1}, -\beta^{4r_2}, -\beta^{2r_3+1}, -\beta^{4r_4+2})$ such that $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) \in \{1, -1\}^4$ and

$$\frac{c}{\lambda_1} = \varepsilon_1\beta^{\delta_1} + \varepsilon_2\beta^{\delta_2} = \varepsilon_0\varepsilon_3\beta^{\delta_3+2} + \varepsilon_0\varepsilon_4\beta^{\delta_4+2}, \tag{45}$$

$$\frac{\lambda_2}{\lambda_1} = \varepsilon_1\varepsilon_2\beta^{\delta_1+\delta_2} = -\varepsilon_3\varepsilon_4\beta^{\delta_3+\delta_4+4}. \tag{46}$$

If β is not an algebraic integer, then it follows from (45) that the greatest term of the sequence $(\delta_1, \delta_2, \delta_3+2, \delta_4+2)$ occurs in this sequence at least twice and from (46) that $\delta_1 + \delta_2 = \delta_3 + \delta_4 + 4$. Hence

$$\delta_1 = \delta_3 + 2, \quad \delta_2 = \delta_4 + 2 \quad \text{or} \quad \delta_1 = \delta_4 + 2, \quad \delta_2 = \delta_3 + 2. \tag{47}$$

This gives the following possibilities:

$$\{\delta_1, \delta_2\} = \{2r_1 + 1, 4r_2\}, \quad \{\delta_3, \delta_4\} = \{2r_3 + 1, 4r_4 + 2\};$$

$$\{\delta_1, \delta_2\} = \{2r_1 + 1, 4r_4 + 2\}, \quad \{\delta_3, \delta_4\} = \{2r_3 + 1, 4r_2\};$$

$$\{\delta_1, \delta_2\} = \{4r_2, 2r_3 + 1\}, \quad \{\delta_3, \delta_4\} = \{2r_1 + 1, 4r_4 + 2\};$$

$$\{\delta_1, \delta_2\} = \{2r_3 + 1, 4r_4 + 2\}, \quad \{\delta_3, \delta_4\} = \{2r_1 + 1, 4r_2\}$$

and we obtain from (45) the following equations

$$\beta^{2r_1+1} - \beta^{4r_2} = -\varepsilon_0\beta^{2r_3+3} - \varepsilon_0\beta^{4r_4+4},$$

$$\beta^{2r_1+1} - \beta^{4r_4+2} = -\varepsilon_0\beta^{2r_3+3} - \varepsilon_0\beta^{4r_2+2},$$

$$-\beta^{4r_2} - \beta^{2r_3+1} = \varepsilon_0\beta^{2r_1+3} - \varepsilon_0\beta^{4r_4+4},$$

$$-\beta^{2r_3+1} - \beta^{4r_4+2} = \varepsilon_0\beta^{2r_1+3} - \varepsilon_0\beta^{4r_4+2}.$$

By (47) the exponents on both sides are equal in pairs, which gives for each value of ε_0 : $\beta = 0$, hence $\alpha = 0$, contrary to $b = 1$.

If β is an algebraic integer so is α. Since $a^2+4 \neq d^2$ (d an integer of K) we have $\alpha \notin K$, hence α is conjugate over K to α^{-1} and λ_1 is conjugate to λ_2. On the other hand, we have

$$\lambda_1 \left(\alpha^{2r_4+1+\frac{1-\varepsilon}{2}}\right)^2 - c\alpha^{2r_4+1+\frac{1-\varepsilon}{2}} + \varepsilon\lambda_2 = 0, \quad \varepsilon \in \{1,-1\}, \tag{48}$$

which differs from (42) only by permutation of r_1 and r_4 and hence leads to contradiction.

Proof of Corollary 1. If $a \in \mathbf{Q}$, then either $a=0$ or $a^2+4 \neq d^2$, $d \in \mathbf{Z}$ hence the assumptions of Theorem 2 are fulfilled.

Proof of Corollary 2. If $a \in K$ and

$$a^2+4 = d^2, \quad d \text{ an integer of } K \tag{49}$$

the zeros of z^2-az-1 are units of K. However, since K is quadratic imaginary, the only units of K are roots of unity and the assertion follows by virtue of Lemma 4.

Example. The following example shows that the assumption $a^2+4 \neq d^2$ (d an integer of K) cannot be altogether omitted. Let $K=\mathbf{Q}(\alpha)$, where $\alpha^3+\alpha^2-\alpha+1=0$ and take

$$u_n = \lambda_1\alpha^n + \lambda_2\left(-\alpha^{-1}\right)^n, \quad \lambda_1 = -\left(1+\alpha^2\right), \quad \lambda_2 = \alpha^2-\alpha^4, \quad c = \alpha^4+1.$$

As observed in the proof of Theorem 2 solubility of the congruence

$$u_n \equiv c \pmod{\mathfrak{p}}, \tag{50}$$

is equivalent to solubility of the congruence

$$f\left(\alpha^{2n}\right) \equiv 0 \pmod{\mathfrak{p}}, \tag{51}$$

where

$$f(z) = \left(\lambda_1 z^2 - cz + \lambda_2\right)\left(\lambda_1\alpha^2 z^2 - c\alpha z - \lambda_2\right).$$

Now

$$f(z) = \lambda_1^2(z-\alpha)(z+1)(z+\alpha)\left(\alpha^2 z+1\right), \tag{52}$$

hence by Theorem 1, case (3), the congruence (51) is soluble for almost all prime ideals $\mathfrak{p}$ of K and so is the congruence (50). On the other hand,op solubility of the equation $u_n=c$ would imply solubility of the equation $f(\alpha^{2n})=0$, hence, by (52), α would be a root of unity, which contradicts $\alpha^3+\alpha^2-\alpha-1=0$.

The author thanks the Department of Mathematics of the University of Colorado at Boulder, where a part of the paper has been written.

References

[1] Schinzel, A., Abelian binomials, power residues and exponential congruences, *Acta Arith.*, **32** (1977), 245–274, Addendum and corrigendum, ibid., **36** (1980), 101–104.

Andrzej Schinzel
Institute of Mathematics PAN
P.O. Box 21, 00-956 Warszawa 10,
e-mail: A.Schinzel@impan.gov.pl