Andrzej Schinzel

Second order strong divisibility sequences in an algebraic number field

Archivum Mathematicum, Vol. 23 (1987), No. 3, 181--186

Persistent URL: http://dml.cz/dmlcz/107294

ARCHIVUM MATHEMATICUM (BRNO)
Vol. 23, No. 3 (1987), 181–186

SECOND ORDER STRONG DIVISIBILITY SEQUENCES IN AN ALGEBRAIC NUMBER FIELD

A. SCHINZEL

(Received March 21, 1986)

Abstract. There are determined all second order linear recurrences u_n, consisting of integers of an algebraic number field and satisfying the condition $(u_n, u_m) = (u_{(u,m)})$ for all positive integers m, n. This answers a question of L. Skula.

Key words. Linear recurrence of the second order, strong divisibility sequence.

MS Classification. 12 A 05, 10 A 35

Let K be an algebraic number field, O its ring of integers, O^* the group of units. Let us consider a linear recurrence of the second order defined over O, i.e. a sequence u_n satisfying the conditions

$$(1) \qquad u_1, u_2 \in O, \qquad u_{n+2} = cu_{n+1} + du_n \qquad (n = 1, 2, \dots)$$

for suitable $c, d \in O$, $d \neq 0$. The sequence u_n is called a strong divisibility sequence if the equality of ideals

$$(u_n, u_m) = (u_{(n,m)})$$

holds for all pairs of positive integers m, n. P. Horak and L. Skula [1] have determined all strong divisibility sequences u_n for $K = Q$ and L. Skula has asked [3] for their determination in the general case. A nearly final answer to this problem is given by the following theorem. In this theorem ζ_k denotes a primitive root of unity of order k.

Theorem. *The sequence u_n defined by the conditions* (1) *with $u_1 \neq 0$ is a strong divisibility sequence if and only if at least one of the following five conditions holds*

$$\text{(i)} \qquad \frac{u_2}{u_1} = c, \qquad (c, d) = 1;$$

$$\text{(ii)} \qquad \frac{u_2}{u_1} \in O^*, \qquad \left(\frac{u_2}{u_1}\right)^2 = c\left(\frac{u_2}{u_1}\right) + d;$$

$$\text{(iii)} \qquad c = 0, \qquad d \in O^*, \qquad \frac{u_2}{u_1} \in O,$$

(iv) $$d = -c^2 \in O^*, \qquad \frac{u_2}{u_1} \in O^*,$$

(v) $$d = -c^2 \frac{\zeta_k}{(1+\zeta_k)^2} \in O^* \qquad (3 < k, \varphi(k) \leqq 2[K:Q]),$$

$$\frac{u_n}{u_1\left(\dfrac{-d(1+\zeta_k)}{c\zeta_k}\right)^n} \in F_k,$$

where F_k is a finite set of strong divisibility sequences in the ring of integers of $K(\zeta_k)$ periodic with period of length k. F_k can be effectively computed for each K and k.

P. Horak and L. Skula have not assumed that $d \neq 0$. It is easy to see that all strong divisibility sequences corresponding to $d = 0$, $u_1 \neq 0$ are given by conditions

$$c \in O^*, \qquad \frac{u_2}{u_1} \in O^*.$$

The proof of the theorem is based on three lemmata.

Lemma 1. *Let $\alpha, \beta, \gamma, \delta$ be non-zero algebraic numbers. There exists an effectively computable constant c, depending only on the height and the degree of α/β and γ/δ such that for every positive integer n either $\gamma\alpha^n - \delta\beta^n = 0$ or*

$$|\gamma\alpha^n - \delta\beta^n| \geqq \min\{|\gamma|, |\delta|\}(\max\{|\alpha|, |\beta|\})^n n^{-c}.$$

Proof. We assume without loss of generality that $|\alpha| \geqq |\beta|$ and apply Baker's estimate for $|\alpha_1^{b_1}\alpha_2^{b_2} \ldots \alpha_n^{b_n} - 1|$ in the form given to it in [2] (p. 66, Theorem A) taking there

$$\alpha_1 = \frac{\delta}{\gamma}, \qquad \alpha_2 = \frac{\beta}{\alpha}, \qquad b_1 = 1, \qquad b_2 = n.$$

We get either

$$\frac{\delta}{\gamma}\left(\frac{\beta}{\alpha}\right)^n - 1 = 0$$

or

$$\left|\frac{\delta}{\gamma}\left(\frac{\beta}{\alpha}\right)^n - 1\right| \geqq n^{-c},$$

which implies the lemma.

Lemma 2. *Let L be an algebraic number field, $\alpha, \beta, \gamma, \delta \in L^*$, α, β algebraic integers. Then either $N_{L/Q}(\gamma\alpha^n - \delta\beta^n)$ is unbounded or α, β are units and β/α is a root of unity or $\alpha = \beta$, $\gamma = \delta$.*

Proof. If for all sufficiently large n

$$\gamma\alpha^n - \delta\beta^n = 0$$

then clearly $\gamma = \delta$, $\alpha = \beta$. Otherwise we have for arbitrarily large n:

$$\gamma^{(\sigma)}\alpha^{(\sigma)n} - \delta^{(\sigma)}\beta^{(\sigma)n} \neq 0$$

for all isomorphic injections σ of L into C. Applying Lemma 1 we get

$$| \gamma^{(\sigma)}\alpha^{(\sigma)n} - \delta^{(\sigma)}\beta^{(\sigma)n} | \geqq \min \{| \gamma^{(\sigma)} |, | \delta^{(\sigma)} |\} \max \{| \alpha^{(\sigma)} |, | \beta^{(\sigma)} |\}^n n^{-c}$$

and on multiplication

$$| N_{L/Q}(\gamma\alpha^n - \delta\beta^n) | \geqq C_1 C_2^n n^{-c[L:Q]} \tag{2}$$

where

$$C_1 = \prod_\sigma \min \{| \gamma^{(\sigma)} |, | \delta^{(\sigma)} |\},$$
$$C_2 = \prod_\sigma \max \{| \alpha^{(\sigma)} |, | \beta^{(\sigma)} |\}. \tag{3}$$

If α is not a unit, we have

$$\prod_\sigma | \alpha^{(\sigma)} | \geqq 2$$

and the right hand side of (2) tends to ∞. If α is a unit we have

$$\prod_\sigma \max \{| \alpha^{(\sigma)} |, | \beta^{(\sigma)} |\} = \prod_\sigma \max \left\{1, \left| \frac{\beta^{(\sigma)}}{\alpha^{(\sigma)}} \right|\right\} > 1, \tag{4}$$

unless, by a theorem of Kronecker, β/α is a root of 1. The formulae (2), (3) and (4) imply that $N_{L/Q}(\gamma\alpha^n - \delta\beta^n)$ is unbounded and the lemma is proved.

Lemma 3. *If γ, δ, n are non-zero elements of an algebraic number field L and S is a finite set of prime ideals of L then the equation*

$$\gamma\varepsilon - \delta\varepsilon' = \eta$$

has only finitely many solutions in S-units ε, ε' of L, which can be effectively determined.

Proof, see Sprindžuk [1], Chapter VI, lemma 6.2.

Proof of the theorem. Let $x^2 - cx - d = (x - \alpha)(x - \beta)$, $\alpha\beta \neq 0$. If $\alpha = \beta$ we have from the general theory of linear recurrences

$$u_n = (\gamma n - \delta)\,\alpha^n, \qquad \alpha, \gamma, \delta \in K.$$

From $(u_n, u_{n+1}) = (u_1)$ we get that $(\gamma, \delta)\,\alpha^n \mid (\gamma - \delta)\,\alpha \neq 0$, hence $\alpha \in O^*$. From $u_n \mid u_{2n}$ we get

$$\gamma n - \delta \mid 2\gamma n - \delta$$

and since

$$\gamma n - \delta \mid 2\gamma n - 2\delta$$

we obtain

$$\gamma n - \delta \mid \delta, \qquad N_{K/Q}(\gamma n - \delta) \mid N_{K/Q}\delta.$$

If $\gamma \neq 0$ then $N_{K/Q}(\gamma n - \delta)$ is a non-constant polynomial in n, it is unbounded, hence $N_{K/Q}\delta = 0$, $\delta = 0$, $u_n = \gamma n\alpha^n$,

$$\frac{u_2}{u_1} = 2\alpha = c \qquad \text{and} \qquad (c, d) = (2\alpha, \alpha^2) = 1$$

thus (i) holds. If $\gamma = 0$, then $\frac{u_2}{u_1} = \alpha$ and (ii) holds. Suppose now, that $\alpha \neq \beta$. Then, as is well known

$$u_n = \gamma\alpha^n - \delta\beta^n$$

for suitable $\gamma, \delta \in K(\alpha, \beta)$ such that $\gamma - \delta \in K, \gamma\delta \in K$. Let us choose a positive integer D so that $\gamma D, \delta D$ are algebraic integers. Assume first that $\gamma\delta = 0$; without loss of generality $\delta = 0$,

$$u_n = \gamma\alpha^n.$$

From $(u_n, u_{n+1}) = (u_1)$ we get that $\alpha \in O^*$, hence $\frac{u_2}{u_1} \in O^*$. Moreover

$$\left(\frac{u_2}{u_1}\right)^2 - c\left(\frac{u_2}{u_1}\right) - d = 0$$

hence (ii) holds.

Assume now that $\gamma\delta \neq 0$. From $(u_n, u_{n+1}) = (u_1)$ we get that $(\alpha, \beta) = 1$ hence $(c, d) = 1$. From $u_n \mid u_{2n}$ we get

$$\gamma\alpha^n - \delta\beta^n \mid \gamma\alpha^{2n} - \delta\beta^{2n},$$

but

$$\gamma\alpha^n - \delta\beta^n \mid (\gamma^2\alpha^{2n} - \delta^2\beta^{2n})\, D,$$

hence

$$\gamma\alpha^n - \delta\beta^n \mid (\alpha^{2n}, \beta^{2n})\, D\gamma\delta(\gamma - \delta) \mid D\gamma\delta(\gamma - \delta)$$

and either $\gamma = \delta$ or

$$0 < | N_{K/Q}(\gamma\alpha^n - \delta\beta^n) | \leqq | N_{K/Q}D\gamma\delta(\gamma - \delta) |. \tag{5}$$

In the former case we have

$$\frac{u_2}{u_1} = \frac{\gamma\alpha^2 - \gamma\beta^2}{\gamma\alpha - \gamma\beta} = \alpha + \beta = c$$

and (i) holds. In the latter case we apply lemma 2 with $L = K(\alpha, \beta)$ and infer from (5) that $\alpha, \beta \in O^*$ and $\beta/\alpha = \zeta_k$ for a suitable k. The case $k = 1$ is impossible, since $\alpha \neq \beta$. In the case $k = 2$ we get $c = 0$ and since $(c, d) = 1$ we get $d \in O^*$, case (iii). In the case $k = 3$ we get $c = \alpha + \beta = \alpha(1 + \zeta_3) = -\alpha\zeta_3^2$, $d = -\alpha\beta = -\zeta_3\alpha^2 =$

$= -c^2$. Since $(c, d) = 1$ we get $d \in O^*$. Since $u_2 \mid u_4$ we get $u_2 \mid cu_3 + du_2$; $u_2 \mid u_3$; $u_2 \mid cu_2 + du_1$; $u_2 \mid u_1$, hence $\frac{u_2}{u_1} \in O^*$, the case (iv).

In the case $k > 3$ we infer from $c = \alpha + \beta = \alpha(1 + \zeta_k)$, $d = -\alpha\beta = -\zeta_k\alpha^2$ that

$$d = \frac{-c^2\zeta_k}{(1 + \zeta_k)^2}$$

and since $(\alpha, \beta) = 1$ that $d \in O^*$. Since ζ_k satisfies an equation of degree 2 over K its absolute degree $\varphi(k)$ is at most $2[K : Q]$. It remains to show the last assertion of (v). We notice first that $\alpha = \frac{-d(1 + \zeta_k)}{c\zeta_k}$ and put

$$\varepsilon_n = \frac{u_n}{u_1\alpha^{n-1}} = \frac{\alpha}{u_1}(\gamma - \delta\zeta_k^n) = \frac{\gamma - \delta\zeta_k^n}{\gamma - \delta\zeta_k}.$$

The sequence ε_n is a strong divisibility sequence in the ring of integers of $K(\zeta_k)$ (note that $\alpha, \beta, \gamma, \delta \in K(\zeta_k)$). It is periodic with period k and satisfies the recurrence relation

$$\varepsilon_{n+2} = (1 + \zeta_k)\,\varepsilon_{n+1} - \zeta_k\varepsilon_n. \tag{6}$$

From $\varepsilon_2 \mid \varepsilon_4$ we infer that $\varepsilon_2 \mid (1 + \zeta_k)\,\varepsilon_3$, hence $\varepsilon_2 \mid (1 + \zeta_k)\,\varepsilon_1 = 1 + \zeta_k$. From $\varepsilon_3 \mid \varepsilon_6$ we infer that $\varepsilon_3 \mid (1 + \zeta_k)\,\varepsilon_5 - \zeta_k\varepsilon_4$, hence

$$\varepsilon_3 \mid (1 + \zeta_k)^2\,\varepsilon_4 - \zeta_k\varepsilon_4 = (1 - \zeta_k + \zeta_k^2)\,\varepsilon_4,$$

hence further

$$\varepsilon_3 \mid (1 + \zeta_k + \zeta_k^2)\,\varepsilon_2 \mid (1 + \zeta_k)(1 + \zeta_k + \zeta_k^2).$$

Thus ε_2 and ε_3 are S-units, where S is the set of all prime divisors of $(1 + \zeta_k) \cdot (1 + \zeta_k + \zeta_k^2)$. On the other hand

$$\varepsilon_3 - \varepsilon_2(1 + \zeta_k) = -\zeta_k.$$

By Lemma 3 with $L = K(\zeta_k)$ there are only finitely many choices for $\varepsilon_2, \varepsilon_3$, hence by (6) for the sequence ε_n, which proves that F_k is finite.

Thus we have proved that every second order strong divisibility sequence satisfies the alternative (i)–(v). The converse is true, since in case (i)

$$u_n = u_1\frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad (\alpha, \beta) = 1,\ \alpha \neq \beta \text{ or } u_n = u_1 n\alpha^{n-1},\ \alpha \in O^*.$$

in case (ii)

$$u_n = u_2\left(\frac{u_2}{u_1}\right)^{n-2}, \qquad \frac{u_2}{u_1} \in O^*,$$

in case (iii)

$$u_n = d^{(n-r)/2}u_r \qquad \text{for } n \equiv r \pmod 2,\ r = 1 \text{ or } 2$$

in case (iv)

$$u_n = (-c)^{(n-r)/3} u_r \qquad \text{for } n \equiv r (\bmod 3),\ r = 1 \text{ or } 2 \text{ or } 3$$

(note that in this case u_2/u_1 is a unit).
in case (v)

$$u_n = u_1 \left(\frac{-c\zeta_k}{d(1+\zeta_k)} \right)^{1-n} \varepsilon_n,$$

where $\{\varepsilon_n\} \in F_k$ and $\dfrac{c\zeta_k}{d(1+\zeta_k)}$ is a unit.

Remark. In the case $K = Q$, $d = \dfrac{c^2\zeta_k}{(1+\zeta_k)^2} \in Q^*$ is impossible for $k > 3$, hence the case (v) does not occur. In the proof of (i)–(iv) only the conditions $(u_n, u_{n+1}) = (u_1)$ and $u_n \mid u_{2n}$ have been used. Hence these two conditions imply for $K = Q$ that $\{u_n\}$ is a strong divisibility sequence.

REFERENCES

[1] P. Horák and L. Skula, *A characterization of the second-order strong divisibility sequences*, The Fibonacci Quarterly, 23 no 2 (1985), pp. 126–132.
[2] T. N. Shorey, A. J. van der Poorten, R. Tijdeman and A. Schinzel, *Applications of the Gelfond–Baker method to Diophantine equations*. Transcendence theory: advances and applications, pp. 59–77, London 1977.
[3] L. Skula, *Problem 5*, Summer School on Number Theory held at Chlebske September 1983, p. 98, Brno 1985.
[4] V. G. Sprindzuk, *Klassiceskiye diofantovy uravneniya ot dvuh neizvestnyh*, Moskva 1982.

Andrzej Schinzel
PAN Warszawa
ul. Sniadeckich 8
00 950 Warszawa
Poland