COLLOQUIUM MATHEMATICUM

VOL. 96 2003 NO. 1

MULTIPLICATIVE DEPENDENCE OF SHIFTED ALGEBRAIC NUMBERS

BY

PAULIUS DRUNGILAS and ARTŪRAS DUBICKAS (Vilnius)

Abstract. We show that the set obtained by adding all sufficiently large integers to a fixed quadratic algebraic number is multiplicatively dependent. So also is the set obtained by adding rational numbers to a fixed cubic algebraic number. Similar questions for algebraic numbers of higher degrees are also raised. These are related to the Prouhet–Tarry–Escott type problems and can be applied to the zero-distribution and universality of some zeta-functions.

1. Introduction. Throughout we denote by $\mathbb{Z}$ and $\mathbb{Q}$ the sets of integers and of rational numbers respectively. Given a set $M \subset \mathbb{Q}$, we say that a complex number α is *M-dependent* if there are two distinct collections $x_1, \ldots, x_n \in M$ and $y_1, \ldots, y_m \in M$ such that

$$(\alpha + x_1) \ldots (\alpha + x_n) = (\alpha + y_1) \ldots (\alpha + y_m). \tag{1}$$

Here, for $m = 0$, the right-hand side is assumed to be equal to 1. Assume that α is M-dependent. We define the *length of multiplicative dependence* of α (and denote it by $\ell(\alpha, M)$) to be the smallest $n + m$ for which there are $x_1, \ldots, x_n, y_1, \ldots, y_m \in M$ satisfying (1).

Of course, if α is transcendental, then it is M-independent for any $M \subset \mathbb{Q}$. We denote by $\mathbb{Z}_t$ the set of integers greater than or equal to t. The question whether or not an algebraic α is $\mathbb{Z}_0$-dependent is of importance in the theory of the Hurwitz zeta-function $\zeta(\alpha, s) = \sum_{j=0}^{\infty} (j + \alpha)^{-s}$. (See, e.g., the paper of Cassels [2], where he proves that at least half of the numbers $\alpha + x$, $x \in \mathbb{Z}_0$, do not belong to the multiplicative group generated by $\alpha, \alpha + 1, \ldots, \alpha + x - 1$.) The zero-distribution and the universality property of the Lerch zeta-function

$$L(\lambda, \alpha, s) = \sum_{j=0}^{\infty} \frac{\exp\{2\pi\lambda j\sqrt{-1}\}}{(j + \alpha)^s}$$

2000 *Mathematics Subject Classification*: 11D57, 11D72, 11R04.

Key words and phrases: algebraic numbers, Prouhet–Tarry–Escott problem, multiplicative dependence.

also rely on $\mathbb{Z}_0$-independence of α. (See, e.g., [6], [7] for more references concerning limit theorems and universality of Lerch and other zeta-functions which rely on $\mathbb{Z}_0$-independence of α.) The following question is therefore of importance in the theory of zeta-functions.

QUESTION. *Is every algebraic number $\mathbb{Z}_0$-dependent?*

Not only this, but also similar questions, like: is every algebraic (over $\mathbb{Q}$) number $\mathbb{Z}$-dependent or is it $\mathbb{Q}$-dependent, apparently cannot be answered by using the methods of this note. However in some particular cases the above question can be easily answered. For instance, if α is a root of unity, then $\alpha^n = 1$ for some positive integer n, so that α is $\mathbb{Z}_0$-dependent and $\ell(\alpha, \mathbb{Z}_0) \le n$. Similarly, the equality $\alpha(\alpha + x) = \alpha + y$ shows that every quadratic algebraic integer is $\mathbb{Z}$-dependent and $\ell(\alpha, \mathbb{Z}) \le 3$. The second named author [3] showed that all rational numbers and quadratic algebraic integers are $\mathbb{Z}_t$-dependent for every $t \in \mathbb{Z}$. Furthermore, we have $\ell(\alpha, \mathbb{Z}_t) \le 4$ for every rational α and $\ell(\alpha, \mathbb{Z}_t) \le 5$ for every quadratic algebraic integer α. Note that, for α being an algebraic number but not an algebraic integer, $\ell(\alpha, \mathbb{Z})$ must be even, because (1) can hold only if $n = m$.

In this note we prove the following.

THEOREM 1. *Let α be a quadratic algebraic number*, *and $t \in \mathbb{Z}$. Then α is $\mathbb{Z}_t$-dependent and $\ell(\alpha, \mathbb{Z}_t) \le 8$.*

THEOREM 2. *Let α be a cubic algebraic number. Then α is $\mathbb{Q}$-dependent and $\ell(\alpha, \mathbb{Q}) \le 8$.*

The proofs, given in Section 3, are based on Dirichlet's theorem about prime numbers lying in an arithmetic progression and on certain elementary identities. These are simple to check, but not easy to find! The last section of the paper contains some identities for quartic algebraic numbers. In Section 2 we show that some particular cases of this problem involving length of multiplicative dependence are related to the Prouhet–Tarry–Escott and Erdős–Straus problems.

2. Connection with other problems. The Prouhet–Tarry–Escott problem is equivalent to the question whether there are two distinct vectors $\mathbf{x} = (x_1, \dots, x_d) \in \mathbb{Z}^d$ and $\mathbf{y} = (y_1, \dots, y_d) \in \mathbb{Z}^d$ such that

$$(\sigma_1(\mathbf{x}) - \sigma_1(\mathbf{y}) : \sigma_2(\mathbf{x}) - \sigma_2(\mathbf{y}) : \dots : \sigma_d(\mathbf{x}) - \sigma_d(\mathbf{y})) = (0 : 0 : \dots : 0 : 1)$$

in the projective space $\mathbb{P}^{d-1}$. Here, $\sigma_1(\mathbf{x}) = x_1 + \dots + x_d$, $\sigma_2(\mathbf{x}) = x_1x_2 + x_1x_3 + \dots + x_{d-1}x_d, \dots, \sigma_d(\mathbf{x}) = x_1x_2 \dots x_d$ and the respective $\sigma_j(\mathbf{y})$, $j = 1, \dots, d$, are the elementary symmetric functions. This question was answered in the affirmative for all $d \le 10$, but remains unsettled for every $d > 10$. See, for instance, the review of Borwein and Ingalls [1] for more equivalent formulations and the references on this problem.

Assume that α is an algebraic number of degree $d-1$ which is not an algebraic integer, i.e. $a\alpha^{d-1} + b\alpha^{d-2} + \ldots + e\alpha + f = 0$ with integer $a \geq 2$, $f \neq 0, b, \ldots, e$. Then (1) with integer $x_1, \ldots, x_n$, $y_1, \ldots, y_m$ can only be true if $n = m \geq d$. Thus $\ell(\alpha, \mathbb{Z}) \geq 2d$ with equality if and only if there exist two distinct vectors $\mathbf{x} \in \mathbb{Z}^d$ and $\mathbf{y} \in \mathbb{Z}^d$ such that

$$(\sigma_1(\mathbf{x}) - \sigma_1(\mathbf{y}) : \sigma_2(\mathbf{x}) - \sigma_2(\mathbf{y}) : \ldots : \sigma_d(\mathbf{x}) - \sigma_d(\mathbf{y})) = (a : b : \ldots : e : f).$$

One can easily see that this question is more general than that of Prouhet–Tarry–Escott. For instance, by taking $d=3$, $\mathbf{x}=(1,1,16)$ and $\mathbf{y}=(0,-3,-11)$, we see that

$$(\sigma_1(\mathbf{x}) - \sigma_1(\mathbf{y}) : \sigma_2(\mathbf{x}) - \sigma_2(\mathbf{y}) : \sigma_3(\mathbf{x}) - \sigma_3(\mathbf{y})) = (32 : 0 : 16) = (2 : 0 : 1).$$

So, for both roots of the equation $2\alpha^2 + 1 = 0$, we have the identity

$$(\alpha+1)^2(\alpha+16) = \alpha(\alpha-3)(\alpha-11).$$

This implies that $\ell(\alpha, \mathbb{Z}) = 6$ for $\alpha = \sqrt{-1/2}$. Similarly, for α satisfying $a\alpha^2 + c = 0$ with integer $a \geq 2$, $c \neq 0$, its $\mathbb{Z}$-dependence follows from the identity

$$(\alpha+2c)(\alpha+1-2c)(\alpha+2c(2c-1)) \\ = \alpha^2(\alpha + 4ac(2c-1)^2 + 2c(2c-1) + 1),$$

giving $\ell(\alpha, \mathbb{Z}) = 6$ for $\alpha = \sqrt{-c/a}$.

A little computation with Maple shows however that

$$(\sigma_1(\mathbf{x}) - \sigma_1(\mathbf{y}) : \sigma_2(\mathbf{x}) - \sigma_2(\mathbf{y}) : \sigma_3(\mathbf{x}) - \sigma_3(\mathbf{y})) \neq (2 : 0 : 3)$$

for all $\mathbf{x}, \mathbf{y} \in \{1, \ldots, 1000\}^3$. This suggests that the inequality $\ell(\alpha, \mathbb{Z}_1) \leq 8$ of Theorem 1 is sharp in general.

Recall that the Erdős–Straus conjecture is equivalent to the following statement: for every prime number p there are three positive integers x_1, x_2, x_3 such that

$$1/x_1 + 1/x_2 + 1/x_3 = 4/p.$$

(See [5, Problem D11] for many references on this and related problems about Egyptian fractions.) Let α be a root of $\alpha^2 + 4\alpha + p = 0$. One can easily see that the question whether there are positive integers x_1, x_2, x_3 and $y_1 \in \mathbb{Z}$ such that

$$(\alpha+x_1)(\alpha+x_2)(\alpha+x_3) = \alpha^2(\alpha+y_1)$$

is equivalent to that of Erdős–Straus.

As already noticed in [3], by taking the norm of both sides of (1) over $\mathbb{Q}$, we can ask similar questions about multiplicative dependence of $Q(z)$, where Q is the minimal polynomial of $-\alpha$ and where z runs over the values of M. For quadratic polynomials such questions were considered in [3]. Elliott [4, Chapter 17] considered a similar, but apparently unrelated question about representation of integers by products of polynomials $Q(z)$ at integer points for Q having all roots at negative integers. Note that Theorem 2 implies that the values of a cubic (irreducible in $\mathbb{Q}[z]$) polynomial $Q(z) = z^3 + bz^2 + cz + e \in \mathbb{Q}[z]$ at rational numbers are multiplicatively dependent. More precisely, there are at most eight rational numbers $r_1, \dots, r_8$ giving the non-trivial equality $Q(r_1)^{\pm 1} \dots Q(r_8)^{\pm 1} = 1$. (We do not claim that these eight are distinct nor that eight is the minimal possible number! It was shown in [3] that for quadratic polynomials the minimal possible number is four.)

3. Proofs

Proof of Theorem 1. Write $a\alpha^2 + b\alpha + c = 0$, where a, b, c are integers satisfying $a > 0$, $c \neq 0$ and $D = b^2 - 4ac \neq 0$. We will show first that there is a positive integer k such that $b^2k^2 + 2ck$ is a quadratic residue modulo $2ak + 1$.

For $h \in \mathbb{Z}$ and an odd integer $P > 1$, let $\left(\frac{h}{P}\right)$ be the Jacobi symbol. The identity

$$4a^2(b^2k^2 + 2ck) = b^2(2ak+1)^2 - 2(b^2 - 2ac)(2ak+1) + D$$

implies that

$$\left(\frac{b^2k^2 + 2ck}{2ak+1}\right) = \left(\frac{D}{2ak+1}\right).$$

Set $k = 2Dk'$ with $k' \in \mathbb{Z}$ such that $Dk' > 0$ and, by Dirichlet's theorem, the number $p = 2ak + 1 = 4aDk' + 1$ being prime. It suffices to show that

$$\left(\frac{D}{p}\right) = 1, \tag{2}$$

where the Jacobi symbol becomes the Legendre symbol. Write $D = 2^s D' \varepsilon$, where $s \in \mathbb{Z}_0$, $D' > 0$ is odd, and $\varepsilon = \pm 1$. Then

$$\left(\frac{D}{p}\right) = \left(\frac{2^s}{p}\right)\left(\frac{D'}{p}\right)\left(\frac{\varepsilon}{p}\right). \tag{3}$$

Since $p \equiv 1 \pmod 4$ and $p \equiv 1 \pmod{D'}$, we get

$$\left(\frac{D'}{p}\right) = \left(\frac{p}{D'}\right) = 1$$

and $\left(\frac{\varepsilon}{p}\right) = 1$. Moreover,

$$\left(\frac{2^s}{p}\right) = 1,$$

which is clear for even s, whereas for odd s it follows from $\left(\frac{2}{p}\right) = 1$, because then $p \equiv 1 \pmod 8$. Hence the Legendre symbols on the right-hand side of (3) are all three equal to 1. This implies (2), thus $b^2k^2 + 2ck$ is a quadratic residue modulo $2ak + 1$ provided that $k = 2Dk'$ with k' as above.

Our next step is to show that the equation

$$(4) \qquad (2ak+1)(\alpha+x_1)(\alpha+x_2) = (\alpha+y_1)(\alpha+y_2)$$

has infinitely many integer solutions $x_1, x_2, y_1, y_2 > t$. Since $a\alpha^2 = -b\alpha - c$, (4) is true provided that $y_1 + y_2 = (2ak+1)(x_1+x_2) - 2bk$ and $y_1y_2 = (2ak+1)x_1x_2 - 2ck$. Set $y_2 = x_2 - 1$, $y_1 = (2ak+1)x_1 + 2akx_2 - 2bk + 1$. Then the sum of y_1 and y_2 is as required. As for the product, it suffices to show that the equation

$$((2ak+1)x_1 + 2akx_2 - 2bk + 1)(x_2 - 1) = (2ak+1)x_1x_2 - 2ck$$

has solutions in sufficiently large $x_1, x_2 \in \mathbb{Z}$. Let us write the last equation in the form

$$(5) \qquad x_1(2ak+1) = (2ak+1)x_2(x_2-1) - (x_2 - 1 + bk)^2 + b^2k^2 + 2ck.$$

By the above, there is an $x_0 \in \mathbb{Z}$ such that $x_0^2 - b^2k^2 - 2ck$ is divisible by $2ak+1$. Accordingly, there is a sufficiently large $x_2 \in \mathbb{Z}$ such that $(x_2 - 1 + bk)^2 - b^2k^2 - 2ck$ is divisible by $2ak+1$. It is clear that with this x_2 and with

$$x_1 = x_2(x_2-1) - ((x_2 - 1 + bk)^2 - b^2k^2 - 2ck)/(2ak+1) \in \mathbb{Z},$$

(5) holds. Evidently, x_1 is sufficiently large if x_2 is.

Let us take two integer solutions of (4), say $x_1, x_2, y_1, y_2 > t$ and $y_3, y_4, x_3, x_4 > \max\{x_1, x_2, y_1, y_2\}$. Consider a quotient of

$$(2ak+1)(\alpha+x_1)(\alpha+x_2) = (\alpha+y_1)(\alpha+y_2)$$

and

$$(2ak+1)(\alpha+y_3)(\alpha+y_4) = (\alpha+x_3)(\alpha+x_4).$$

It follows that

$$(\alpha+x_1)(\alpha+x_2)(\alpha+x_3)(\alpha+x_4) = (\alpha+y_1)(\alpha+y_2)(\alpha+y_3)(\alpha+y_4),$$

where $y_3 \neq x_1, x_2$. Furthermore, $y_3 \neq x_3$, for otherwise we obtain the equality $(2ak+1)(\alpha+y_4) = \alpha + x_4$, which is impossible as $\alpha \notin \mathbb{Q}$. Similarly, $y_3 \neq x_4$. Therefore x_1, x_2, x_3, x_4 is not a permutation of y_1, y_2, y_3, y_4, which is the desired conclusion.

Proof of Theorem 2. By adding to α a rational number, we can, without loss of generality, assume that α is a root of the equation $z^3 + pz + q = 0$, where $p, q \in \mathbb{Q}$, $q \neq 0$. If $p = 0$, then $\alpha^3 = -q$, and the identity

$$(\alpha+1)^2(\alpha-1)^2\alpha^2 = (\alpha+q)^2$$

shows that $\ell(\alpha, \mathbb{Q}) \leq 6 + 2 = 8$. If $p \neq 0$, then, by employing $\alpha^3 = -p\alpha - q$, we have the identity

$$(\alpha + 2q/p)^3(\alpha - 2q/p) = \alpha^3(\alpha + 4q(4q^2 + p^3)/p^4),$$

which completes the proof.

4. Identities for quartic algebraic numbers. The direct method used in the proof of Theorem 2 suggests that perhaps there are some more complicated identities which imply that every quartic algebraic number is $\mathbb{Q}$-dependent. For this, one needs to find a solution of (1) in rational numbers using the equation $\alpha^4 + p\alpha^2 + q\alpha + r = 0$, where $p, q, r \in \mathbb{Q}$, $r \neq 0$. We now give such identities in some particular cases.

Let throughout $\varepsilon = \pm 1$. The simplest case of quartics for which (1) has a non-trivial solution is $p = 0$, $q = \varepsilon$. Then $\alpha^8 = (\alpha + \varepsilon r)^2$. We were unable to find such an identity for $p = q = 0$, but for $p = -3/2$, $q = 0$ we have

$$(\alpha - 1/2)^3(\alpha + 3/2) = \alpha - r - 3/16.$$

More generally, for $p = -6t^2$, $q = \varepsilon - 8t^3$, where $t \in \mathbb{Q}$, we found

$$(\alpha + t)^6(\alpha - 3t)^2 = (\alpha + \varepsilon(3t^4 + r))^2.$$

Similarly, for $p = -(1 + u + u^2)t^2$, $q = \varepsilon - (u + u^2)t^3$, where $u, t \in \mathbb{Q}$, we have

$$\alpha^2(\alpha + t)^2(\alpha + ut)^2(\alpha - (1 + u)t)^2 = (\alpha + \varepsilon r)^2.$$

Finally, for $p = -t^2$, $q = 0$, $r = \varepsilon + 4t^4(u^3 - u)^2/(u^2 + 1)^4$ $(u, t \in \mathbb{Q})$, the required identity is

$$(\alpha + vt)^2(\alpha - vt)^2(\alpha + wt)^2(\alpha - wt)^2 = 1,$$

where $v = (u^2 - 1)/(u^2 + 1)$, $w = 2u/(u^2 + 1)$. Note that for all quartic α as above we have $\ell(\alpha, \mathbb{Q}) \leq 10$.

The research of the second named author was partially supported by the Lithuanian State Science and Studies Foundation.

REFERENCES

[1] P. Borwein and C. Ingalls, *The Prouhet–Tarry–Escott problem revisited*, Enseign. Math. (2) 40 (1994), 177–184.

[2] J. W. S. Cassels, *Footnote to a note of Davenport and Heilbronn*, J. London Math. Soc. 36 (1961), 177–184.

[3] A. Dubickas, *Multiplicative dependence of quadratic polynomials*, Lithuanian Math. J. 38 (1998), 225–231.

[4] P. D. T. A. Elliott, *Arithmetic Functions and Integer Products*, Springer, New York, 1985.

[5] R. K. Guy, *Unsolved Problems in Number Theory*, Springer, New York, 1994.

[6] A. Laurinčikas, *Limit Theorems for the Riemann Zeta-Function*, Kluwer, Dordrecht, 1996.

[7] A. Laurinčikas and K. Matsumoto, *The joint universality and the functional independence for Lerch zeta-functions*, Nagoya Math. J. 157 (2000), 211–227.

Department of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius 2600, Lithuania
E-mail: padr0254@uosis.mif.vu.lt
arturas.dubickas@maf.vu.lt

Received 19 June 2002;
revised 9 September 2002 (4239)