ON THE SET OF SOLUTIONS OF THE SYSTEM $x_1+x_2+x_3=1,\ x_1x_2x_3=1$

Miloslav Hlaváček†, Praha

(Received April 7, 1995)

Abstract. A proof is given that the system in the title has infinitely many solutions of the form $a_1+\mathrm{i}a_2$, where a_1 and a_2 are rational numbers.

Keywords: Diophantine equations, Weierstrass p-function

MSC 2000: 10B05, 10M05

1. A subset of solutions and derivation of an auxiliary cubic equation

Let R denote the set of rational numbers. Assume that x_1 is real and x_2, x_3 are conjugate complex numbers, $x_2=a+\mathrm{i}b$, $x_3=a-\mathrm{i}b$, a and b rational. The first equation yields $x_1=1-2a$ while the second implies

$$(1-2a)(a^2+b^2)=1.$$

Consequently, we have

$$b^2=(1-a^2+2a^3)/(1-2a). \tag{1}$$

Hence the fraction in (1) has to be a square of a rational number. It is readily seen that the same holds for

$$(1-a^2+2a^3)(1-2a),$$

i.e.,

$$-4a^4+4a^3-a^2-2a+1=M^2, \tag{2}$$

where $M \in R$. Let us set

$$M = 1 - a + na^2, \tag{3}$$

where $n \in R$. Substituting (3) in (2), we obtain

$$-4a^4 + 4a^3 - a^2 = a^2(1 + 2n) - 2na^3 + n^2a^4.$$

The case $a = 0$ can be excluded as it leads to the well-known solution $\{1, \mathrm{i}, -\mathrm{i}\}$. Cancelling by a^2, we arrive at the equation

$$a^2(n^2 + 4) - a(2n + 4) + 2n + 2 = 0,$$

the roots of which are

$$a_{1,2} = (n^2 + 4)^{-1}\bigl(n + 2 \pm ((n + 2)^2 - (n^2 + 4)(2n + 2))^{1/2}\bigr).$$

Its discriminant is

$$-2n^3 - n^2 - 4n - 4 = D^2. \tag{4}$$

Each solution $(n, D) \in R \times R$ of the equation (4) yields $a_1 \in R$, $a_2 \in R$ and hence a couple of solutions of the given problem.

2. Modelling by a Weierstrass p-function

Let us mention that a similar equation is valid for the Weierstrass p-function, namely

$$4p^3(z) - g_2 p(z) - g_3 = (p'(z))^2, \tag{5}$$

where g_2 and g_3 are constants and $p'(z) = \mathrm{d}p(z)/\,\mathrm{d}z$ (see e.g. [1], p. 29). Since p is a doubly periodic function, it can be used in solving the question whether the number of couples $(n, D) \in R \times R$, which satisfy the equation (4), is infinite.

If we substitute

$$n = -\tfrac{1}{2}p - \tfrac{1}{6}$$

in (4) and multiply by 16, we obtain

$$4p^3 + \frac{92}{3}p - \frac{1448}{27} = (4D)^2. \tag{6}$$

If we write $p := p(z)$, $4D := p'(z)$ and set

$$92/3 = -g_2, \quad 1448/27 = g_3, \tag{7}$$

we arrive at the equation (5) for the p-function. Since the coefficients g_2, g_3 are real numbers, one period of this doubly periodic function is real as well. Let us denote it by ω.

The equation

$$4p^3 + \frac{92}{3}p - \frac{1448}{27} = 0$$

has only one real root $e_1 \notin R$ (as can be easily shown), since

$$\begin{aligned} &e_1 = \tfrac{1}{3}(\eta_1 + \eta_2) \\ &\eta_1 = (181 + (44928)^{1/2})^{1/3},\ \eta_2 = (181 - (44928)^{1/2})^{1/3} \end{aligned} \tag{8}$$

by the Cardan formula. It is well-known that

$$p(\omega/2) = e_1,\ p'(\omega/2) = 0.$$

By substitution, we find that (6) is satisfied by numbers $p = \frac{5}{3}$ and $D = \pm 1$, i.e., for $p(z) = \frac{5}{3}$ and $p'(z) = \pm 4$. By means of the graph of the p-function we realize that $p = \frac{5}{3}$ and $p' = -4$ corresponds to an argument $z_1 \in (0, \omega/2)$, whereas the couple $p = \frac{5}{3}$, $p' = +4$ corresponds to $z_2 \in (\omega/2, \omega)$. It is readily seen that $z_1 + z_2 = \omega$.

Let us recall the addition theorem for $p(z)$, which implies that if $p(z_1) \in R$ and $p'(z_1) \in R$, then $p(kz_1) \in R$, $p'(kz_1) \in R$ for any natural number k, since they can be expressed in terms of $p(z_1)$ and $p'(z_1)$ by means of a rational expression.

Let us consider $p(kz_1)$ for $k = 2, 3, 4, \ldots$. The number of different values which can be obtained in this way would be finite if and only if $z_1 = (r/t)\omega$, where r and t are natural, i.e., if and only if z_1 is commensurable with the period ω. Otherwise there exists infinitely many different values of $p(kz_1)$.

It is therefore sufficient to prove that z_1 is not commensurable with the period ω.

1° Assume that

$$z_1 = \frac{\ell}{2n}\,\omega,$$

where ℓ, n are natural, ℓ is odd and $n > 1$. Then we should have

$$p(nz_1) = p(\ell\omega/2) = p(\omega/2).$$

This is, however, impossible, since $p(nz_1)$, when expressed in terms of $\frac{5}{3}$ and (-4) by a rational expression, is rational, whereas $p(\omega/2) = e_1 \notin R$.

2° Assume that

$$z_1 = \frac{s}{2n+1},$$

where s, n are natural, s is even. This is impossible, too. Indeed, then we have

$$z_2 = \omega - z_1 = \frac{\ell}{2n+1}\omega, \text{ with } \ell \text{ odd.}$$

We can calculate $p(z_i)$, $i = 1, 2$, in terms of $p(z_i/2)$ and $p'(z_i/2)$:

$$p(z_i) = (4p^4(z_i/2) + 2g_2p^2(z_i/2) + 8g_3p(z_i/2) + g_2^2/4)(2p'(z_i/2))^{-2} = \tfrac{5}{3}.$$

Using the formula (5) for $p'(z_i/2)$ and the relation (7), in the end we arrive at the equation

$$324p^4(z_i/2) - 2160p^3(z_i/2) - 4968p^2(z_i/2) + 18192p(z_i/2) + 48004 = 0.$$

This equation has two real roots. One of them is equal to $\frac{11}{3}$, the other is irrational. Let us denote it by ϑ. We have

$$\begin{aligned} \vartheta = 1 + \tfrac{1}{3}(\varrho_1 + \varrho_2), \quad \varrho_1 &= (928 + 2(44928)^{1/2})^{1/3}, \\ \varrho_2 &= (928 - 2(44928)^{1/2})^{1/3}, \end{aligned}$$

since ϑ is a root of the equation

$$108p^3 - 324p^2 - 2844p - 4364 = 0.$$

Since $\vartheta > \frac{11}{3}$, the graph of the p-function implies that we may write $p(z_1/2) = \vartheta$, $p(z_2/2) = \frac{11}{3}$. Using (5) and (7), we obtain $p'(z_2/2) = -16$. Multiplying the argument $z_2/2$ by $(2n+1)$, we arrive at

$$p\Big[(2n+1)\frac{\ell\omega}{2(2n+1)}\Big] = p(\ell\omega/2) = p(\omega/2) = e_1 \notin R.$$

This contradicts the fact that $p[(2n+1)z_2/2]$ can be expressed in terms of $\frac{11}{3}$ and (-16) be means of a rational expression.
3° It remains to consider the third possibility

$$z_1 = \ell\omega/(2n+1), \ \ell \text{ odd.}$$

Then we have

$$p(z_1/2) = p\Big[\frac{\ell\omega}{2(n+1)}\Big] = \vartheta$$

and

$$p[(2n+1)z_1/2] = p(\ell\omega/2) = p(\omega/2) = e_1.$$

On the other hand, $p[(2n+1)z_1/2]$ can be expressed in terms of $p(z_1/2)$ and $p'(z_1/2)$ by means of a rational expression, i.e., in terms of ϑ and $(4\vartheta^3 - g_2\vartheta - g_3)^{1/2}$ (cf. (5)). Theory of algebraic numbers (see e.g. [2]) implies that any rational expression in terms of ϑ and $(4\vartheta^3 - g_2\vartheta - g_3)^{1/2}$ can be rewritten in the form

$$c_0 + c_1\vartheta + c_2\vartheta^2 + (d_0 + d_1\vartheta + d_2\vartheta^2)(4\vartheta^3 - g_2\vartheta - g_3)^{1/2},$$

where $c_i \in R$ and $d_i \in R$. Let us denote this expression by $\alpha_0 \equiv A(\vartheta)$. It satisfies an equation of the sixth degree with rational coefficients.

Assume that at least one of the coefficients d_i is not zero. Denote by ϑ', ϑ'' the numbers conjugate with ϑ, i.e., the roots of the minimal equation for ϑ. Then the roots of the above mentioned equation are

$$\begin{aligned} &\alpha_0 = A(\vartheta), \quad \alpha_1 = A(\vartheta'), \quad \alpha_2 = A(\vartheta''), \\ &\alpha_3 = B(\vartheta), \quad \alpha_4 = B(\vartheta'), \quad \alpha_5 = B(\vartheta''), \end{aligned}$$

where

$$B(\vartheta) = c_0 + c_1\vartheta + c_2\vartheta^2 - (d_0 + d_1\vartheta + d_2\vartheta^2)(4\vartheta^3 - g_2\vartheta - g_3)^{1/2}.$$

Among these roots also the roots of the minimal equation for α_0 are contained. If α_i (i $= 0, 1, 2$) is a root of the minimal equation, then α_{i+3} is a root of this equation as well and vice versa. Consequently, the minimal equation for α_0 is an equation of an even degree and its root α_0 cannot equal e_1, since e_1 is a root of an irreducible equation of the third degree.

Next, assume that $p[(2n+1)z_1/2]$ can be expressed by means of a rational expression in terms of $p(z_1/2)$ alone, i.e., let $d_0 = d_1 = d_2 = 0$. Then it is readily seen that

$$e_1 = c_0 + c_1\vartheta + c_2\vartheta^2 = C(\vartheta),\ e_1' = C(\vartheta'),\ e_1'' = C(\vartheta''), \tag{10}$$

where e_1' and e_1'' are the numbers conjugate with e_1.

This is, however, impossible, as we can show by the following approach.

Summing the three equations (10) and making use of the minimal equations for e_1 and ϑ, we are led to the equation

$$3c_0 + 3c_1 + \frac{185}{3}c_2 = 0.$$

Then for instance the second equation (10_2) yields (substituting $c_0 = -c_1 - c_2 185/9$ and arranging) the couple of equations

$$3c_1\varrho_1 + 6c_2\varrho_1 + c_2\varrho_2^2 = 2\eta_1, \tag{11}$$

$$3c_1\varrho_2 + 6c_2\varrho_2 + c_2\varrho_1^2 = 3\eta_2. \tag{12}$$

Multiplying (11) by ϱ_2 and (12) by ϱ_1, we obtain by subtraction that

$$c_2 = 3(\eta_2\varrho_1 - \eta_1\varrho_2)(\varrho_1^3 - \varrho_2^3)^{-1}.$$

Substituting for $\varrho_1, \varrho_2, \eta_1, \eta_2$ and arranging, we find that

$$\begin{aligned}\frac{4}{3}c_2(44928)^{1/2} = {} & (566 \cdot 44928^{1/2} + 78112)^{1/3} \\ & + (566 \cdot 44928^{1/2} - 78112)^{1/3}.\end{aligned}$$

If we multiply this equation by $(44928)^{1/2}$, we obtain on the left-hand side

$$\frac{4}{3}c_2 44928 \in R,$$

whereas the right-hand side equals

$$(566 \cdot 44928^2 + 78112 \cdot 44928^{3/2})^{1/3} + (566 \cdot 44928^2 - 78112 \cdot 44928^{3/2})^{1/3},$$

which is a root of an irreducible cubic equation, as one can show. This number cannot be rational and we thus arrive at a contradiction again.

Altogether, all possibilities have been considered. We have proved that z_1 is not commensurable with the period ω. There exists an infinite number of pairs $[p(kz_1), p'(kz_1)] \in R \times R$. (Of course, there can exist other arguments z for which $p(z) \in R$ and $p'(z) \in R$). As a consequence, the equation (6) has infinitely many solutions $(p, D) \in R \times R$. Obviously, there are infinitely many couples $(n, D) \in R \times R$ satisfying the equation (4), and therefore infinitely many different numbers $a \in R$. For each such a one finds $\pm b \in R$ in accordance with the equation (1). Thus we arrive at an infinite set of triples $\{x_1, x_2, x_3\}$ with the above required properties.

Remark. The author of this contribution died in 1969. He published several short papers on Diophantine equations in Czech journals during his life. As late as in 1995 his son Ivan Hlaváček discovered the above manuscript in his father's inheritance and translated it into English.

References

[1] *K. Chandrasekharan*: Elliptic Functions. Springer-Verlag, Berlin, Heidelberg, 1985.

[2] *S. Schwarz*: Algebraic Numbers. Přírodovědecké nakladatelství, Praha, 1950. (In Slovak.)

Author's son's address: *Ivan Hlaváček*, Matematický ústav AV ČR, Žitná 25, 115 67 Praha 1, Czech Republic.