

ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXIII.

AZ ESZTERHÁZY KÁROLY TANÁRKÉPZŐ FŐISKOLA
TUDOMÁNYOS KÖZLEMÉNYEI

REDIGIT—SZERKESZTI
ORBÁN SÁNDOR, V. RAISZ RÓZSA

SECTIO MATEMATICAE

TANULMÁNYOK
A MATEMATIKAI TUDOMÁNYOK
KÖRÉBŐL

REDIGIT—SZERKESZTI
KISS PÉTER, RIMÁN JÁNOS

EGER, 1995—96

ACTA
ACADEMIAE PAEDAGOGICAE AGRIENSIS
NOVA SERIES TOM. XXIII.

AZ ESZTERHÁZY KÁROLY TANÁRKÉPZŐ FŐISKOLA
TUDOMÁNYOS KÖZLEMÉNYEI

REDIGIT—SZERKESZTI
ORBÁN SÁNDOR, V. RAISZ RÓZSA

SECTIO MATEMATICAE

TANULMÁNYOK
A MATEMATIKAI TUDOMÁNYOK
KÖRÉBŐL

REDIGIT—SZERKESZTI
KISS PÉTER, RIMÁN JÁNOS

EGER, 1995—96

Some identities and congruences for a special family of second order recurrences

JAMES P. JONES* and PÉTER KISS**

Abstract. For a fixed integer a with $|a| > 2$ let $Y(n)$ and $X(n)$ be second order linear recursive sequences defined by

$$Y(n) = aY(n-1) - Y(n-2) \quad \text{and} \quad X(n) = aX(n-1) - X(n-2)$$

respectively, where the initial terms are $Y(0)=0$, $Y(1)=1$, $X(0)=2$ and $X(1)=a$. In this paper we prove identities for these sequences which yield some congruences for the terms $Y(kn)$ and $X(kn)$, where the modulus are a power of the n^{th} terms.

Let $Y(n)$, $n = 0, 1, 2, \dots$, be a second order linear recursive sequence defined by

$$Y(n) = aY(n-1) - Y(n-2),$$

where a is a given integer with $|a| > 2$ and the initial terms are $Y(0) = 0$ and $Y(1) = 1$. Its associated sequence will be denoted by $X(n)$ which is defined by

$$X(n) = aX(n-1) - X(n-2)$$

and by initial terms $X(0) = 2$, $X(1) = a$. It is well known that the terms of these sequences can be expressed as

$$(1) \quad Y(n) = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad X(n) = \alpha^n + \beta^n,$$

where

$$\alpha = \frac{a + \sqrt{a^2 - 4}}{2} \quad \text{and} \quad \beta = \frac{a - \sqrt{a^2 - 4}}{2}$$

are the roots of the polynomial $x^2 - ax + 1$.

* Research supported by National Science and Research Council of Canada, Grant N^o OGP 0004525.

** Research supported by Foundation for Hungarian Higher Education and Research and Hungarian OTKA Foundation, Grant N^o 016975 and 020295.

The sequences $X(n)$ and $Y(n)$ have important applications to Diophantine equations and Hilbert's tenth problem since they give all solutions to the polynomial identity

$$X^2 - (a^2 - 4)y^2 = 4$$

(see [4]). These sequences are special cases $P = a$ and $Q = 1$ of more general linear recurrent sequences V_n and U_n of Lucas which was defined by the recursion $U_n = PU_{n-1} - QU_{n-2}$. Consequently many identities and congruence properties are known for our sequences X, Y and also for more general sequences (see, e.g. [1], [2], [3] and [5]). For example it is well known that

$$Y(kn) \equiv 0 \pmod{Y(n)}$$

for any natural numbers k and n . Lucas [3] also showed many properties of these sequences, e.g. he showed that $Y(2n) = X(n)Y(n)$ and $X(2n) = X(n)^2 - 2$ and so

$$X(2n) \equiv -2 \pmod{X(n)^2}.$$

The purpose of this paper is to prove some congruences involving $Y(kn)$ and $X(kn)$, where the modulus is a power of the n^{th} term. In the proofs we use formulas of (1) but sometimes we give other methods not using the Binet formula. Specifically we prove the following congruences:

Theorem 1. Let k be an even positive integer. Then

$$Y(kn) \equiv \frac{k}{2}Y(2n) \pmod{Y(n)^3}$$

for any integer $n > 0$.

Theorem 2. Let k be an odd positive integer. Then

$$Y(kn) = kY(n) \pmod{Y(n)^3}$$

for any integer $n > 0$.

Theorem 3. Let k be an odd positive integer. Then

$$X(kn) \equiv k(-1)^{\frac{k-1}{2}}X(n) \pmod{X(n)^2}$$

for any integer $n > 0$.

Theorem 4. Let k be an even positive integer. Then

$$X(kn) \equiv 2(-1)^{k/2} \pmod{X(n)^2}$$

for any integer $n > 0$.

We prove some summation identities for the sequences which will be used for the proofs of the above theorems.

Lemma 1. If k is an even positive integer, then

$$Y(kn) - \frac{k}{2}Y(2n) = (a^2 - 4)Y(2n) \sum_{1 \leq i \leq \lfloor \frac{k}{4} \rfloor} Y\left(n \left(\frac{k}{2} - 2i + 1\right)\right)^2$$

for any natural number n .

Proof. Since k is even, we can write $k = 2t$.

Let first t be an odd integer. By (1), using $\alpha - \beta = \sqrt{a^2 - 4}$ and $\alpha\beta = 1$, we have

$$\begin{aligned} Y(kn) &= \frac{\alpha^{2tn} - \beta^{2tn}}{\alpha - \beta} \\ &= \frac{\alpha^{2n} - \beta^{2n}}{\alpha - \beta} \left(\alpha^{2n(t-1)} + \alpha^{2n(t-2)}\beta^{2n} + \dots + \beta^{2n(t-1)} \right) \\ &= Y(2n) \left(1 + \sum_{i=1}^{\frac{t-1}{2}} \left(\alpha^{2n(t-2i+1)} + \beta^{2n(t-2i+1)} \right) \right), \\ &= Y(2n) \left(1 + 2\frac{t-1}{2} + \sum_{i=1}^{\frac{t-1}{2}} \left(\alpha^{n(t-2i+1)} - \beta^{n(t-2i+1)} \right)^2 \right) \\ &= Y(2n) \left(t + \sum_{i=1}^{\frac{t-1}{2}} (a^2 - 4)Y(n(t-2i+1))^2 \right). \end{aligned}$$

From this the lemma follows in the case t is odd.

Now let t be even, i.e. $t = 2j$ for some j . Then

$$\begin{aligned} & \left(\alpha^{2n(t-1)} + \alpha^{2n(t-2)}\beta^{2n} + \dots + \beta^{2n(t-1)} \right) \\ &= \sum_{i=1}^{t/2} \left(\alpha^{2n(t-2i+1)} + \beta^{2n(t-2i+1)} \right) \\ &= 2\frac{t}{2} + \sum_{i=1}^{t/2} \left(\alpha^{n(t-2i+1)} - \beta^{n(t-2i+1)} \right)^2 \\ &= t + \sum_{i=1}^{t/2} (a^2 - 4)Y(n(t-2i+1))^2, \end{aligned}$$

and so, similarly as above

$$Y(kn) = Y(2n) \left(t + (a^2 - 4) \sum_{i=1}^{t/2} Y(n(t - 2i + 1))^2 \right)$$

follows which implies the lemma.

Lemma 2. If k is an even positive integer, then

$$Y(kn) - \frac{k}{2}Y(2n) = (a^2 - 4)Y(n) \sum_{i=1}^{\frac{k-2}{2}} Y(ni)Y(ni + n)$$

for any natural number n .

Proof. The identity will be proved by induction on k . The lemma holds for $k = 2$ since both sides of the identity are 0 in this case. Now let us suppose that the identity holds for an even positive integer k . We prove that then it holds also for $k + 2$. To this and by the induction hypothesis, it is enough to prove that

$$\begin{aligned} & \left(Y'((k+2)n) - \frac{k+2}{2}Y(2n) \right) - \left(Y(kn) - \frac{k}{2}Y(2n) \right) \\ &= (a^2 - 4)Y(n)Y\left(\frac{k}{2}n\right)Y\left(\frac{k}{2}n + n\right), \end{aligned}$$

or equivalently

$$\begin{aligned} & 2Y(kn + 2n) - 2Y(kn) - 2Y(2n) \\ (2) \quad &= 2(a^2 - 4)Y(n)Y\left(\frac{k}{2}n\right)Y\left(\frac{k}{2}n + n\right). \end{aligned}$$

To prove this we need the equations

$$(3) \quad Y(2n) = X(n)Y(n),$$

$$(4) \quad X(2n) = (a^2 - 4)Y(n)^2 + 2 = X(n)^2 - 2,$$

$$(5) \quad 2Y(n + m) = Y(n)X(m) + X(n)Y(m)$$

and

$$(6) \quad 2X(n + m) = X(n)X(m) + (a^2 - 4)Y(n)Y(m).$$

These are old identities known to Lucas [3], which can be proved easily using (1) and the fact that $(\alpha - \beta)^2 = a^2 - 4$.

To verify (2), by (3), (4) and (5) we get

$$\begin{aligned}
 & 2Y(kn + 2n) - 2Y(kn) - 2Y(2n) \\
 &= Y(kn)X(2n) + X(kn)Y(2n) - 2Y(kn) - 2Y(2n) \\
 &= Y(2n)(X(kn) - 2) + Y(kn)(X(2n) - 2) \\
 &= Y(n)X(n)(X(kn) - 2) + Y(kn)(a^2 - 4)Y(n)^2 \\
 &= Y(n)X(n)(a^2 - 4)Y\left(\frac{k}{2}n\right)^2 + Y\left(\frac{k}{2}n\right)X\left(\frac{k}{2}n\right)(a^2 - 4)Y(n)^2 \\
 &= (a^2 - 4)Y(n)Y\left(\frac{k}{2}n\right)\left(Y\left(\frac{k}{2}n\right)X(n) + X\left(\frac{k}{2}n\right)Y(n)\right) \\
 &= 2(a^2 - 4)Y(n)Y\left(\frac{k}{2}n\right)Y\left(\frac{k}{2}n + n\right).
 \end{aligned}$$

So (2) holds and the lemma is proved.

Lemma 3. If k is an even positive integer, then

$$(7) \quad Y(n) \sum_{i=0}^{\frac{k-2}{2}} Y(ni)Y(ni + n) = Y(2n) \sum_{1 \leq i \leq \lfloor \frac{k}{4} \rfloor} Y\left(n\left(\frac{k}{2} - 2i + 1\right)\right)^2$$

and

$$(8) \quad \sum_{i=0}^{k-2} Y(ni)Y(ni + n) = X(n) \sum_{1 \leq i \leq \lfloor \frac{k}{4} \rfloor} Y\left(n\left(\frac{k}{2} - 2i + 1\right)\right)^2$$

for any natural number n .

Proof. (7) follows from Lemma 1 and 2 and (8) follows from (7) using (3).

Lemma 4. If k is an odd positive integer, then

$$Y(kn) - kY(n) = (a^2 - 4)Y(n) \sum_{i=0}^{\frac{k-1}{2}} Y(ni)^2$$

for any natural number n .

Proof. The proof could be carried out by using the Binet formula (1), but we follow another way similar to the proof of Lemma 2.

The lemma holds for $k = 1$, because then both sides are 0. Assume that the identity holds for an odd k . We have to show that then it holds also for $k + 2$. By the induction hypothesis we have to prove that

$$\begin{aligned} & (Y((k+2)n) - (k+2)Y(n)) - (Y(kn) - kY(n)) \\ &= (a^2 - 4)Y(n)Y\left(\frac{n(k+1)}{2}\right)^2 \end{aligned}$$

or equivalently

$$(9) \quad \begin{aligned} & 2Y(kn+2n) - 2Y(kn) - 4Y(n) \\ &= 2(a^2 - 4)Y(n)Y\left(\frac{n(k+1)}{2}\right)^2. \end{aligned}$$

By (3), (4), (5) and (6) we have

$$\begin{aligned} & 2Y(kn+2n) - 2Y(kn) - 4Y(n) \\ &= Y(kn)X(2n) + X(kn)Y(2n) - 2Y(kn) - 4Y(n) \\ &= X(kn)Y(n)X(n) + (X(2n) - 2)Y(kn) - 4Y(n) \\ &= Y(n)X(kn)X(n) + (a^2 - 4)Y(n)^2Y(kn) - 4Y(n) \\ &= Y(n)(X(kn)X(n) + (a^2 - 4)Y(kn)Y(n)) - 4Y(n) \\ &= 2Y(n)X(kn+n) - 4Y(n) = 2Y(n)(X(kn+n) - 2) \\ &= 2Y(n)(a^2 - 4)Y\left(\frac{kn+n}{2}\right)^2 = 2(a^2 - 4)Y(n)Y\left(\frac{n(k+1)}{2}\right)^2. \end{aligned}$$

Thus (9) holds which proves the lemma.

Now we can prove the theorems.

Proof of Theorem 1. The theorem follows from Lemma 1 or Lemma 2 since $Y(tn)$ is divisible by $Y(n)$ for any positive integers t and n .

Proof of Theorem 2. Similarly as above, the theorem follows from Lemma 4 since $Y(n) \mid Y(ni)$.

Proof of Theorem 3. Let $k = 2q + 1$ ($q \geq 0$). We prove the theorem by induction on q . For $q = 0$ and $q = 1$ the theorem can be seen directly. Suppose that $q > 1$ and that the theorem is true for numbers less than q .

Then using $\alpha\beta = 1$ we have

$$\begin{aligned} X(kn) &= X(n(2q+1)) = \alpha^{n(2q+1)} + \beta^{n(2q+1)} \\ &= \left(\alpha^{n(2q-1)} + \beta^{n(2q-1)}\right) (\alpha^{2n} + \beta^{2n}) - \left(\alpha^{n(2q-3)} + \beta^{n(2q-3)}\right) \\ &\equiv (-1)^{q-1} (2q-1) (\alpha^n + \beta^n) (\alpha^{2n} + \beta^{2n}) \\ &\quad - (-1)^{q-2} (2q-3) (\alpha^n + \beta^n) \pmod{(\alpha^n + \beta^n)^2}. \end{aligned}$$

But $\alpha^{2n} + \beta^{2n} = (\alpha^n + \beta^n)^2 - 2 \equiv -2 \pmod{X(n)^2}$ and so

$$\begin{aligned} X(kn) &\equiv (\alpha^n + \beta^n) \left(-2(-1)^{q-1} (2q-1) - (-1)^{q-2} (2q-3)\right) \\ &\equiv (\alpha^n + \beta^n) (-1)^q \left(2(2q-1) - (2q-3)\right) \\ &\equiv (-1)^q (2q+1) (\alpha^n + \beta^n) \pmod{(\alpha^n + \beta^n)^2}. \end{aligned}$$

From this the theorem follows since $k = 2q + 1$.

Proof of Theorem 4. Let $k = 2q$ ($q > 0$). We prove Theorem 4 also by induction on q . By (4) the theorem can be easily verified for $q = 1$ and $q = 2$. Assume that $q > 2$ and that the theorem holds for $q - 1$ and $q - 2$. Then by the hypothesis, using (1) and (4), we have

$$\begin{aligned} X(kn) &= X(2nq) = \alpha^{2nq} + \beta^{2nq} \\ &= \left(\alpha^{2n(q-1)} + \beta^{2n(q-1)}\right) (\alpha^{2n} + \beta^{2n}) - \left(\alpha^{2n(q-2)} + \beta^{2n(q-2)}\right) \\ &\equiv -4(-1)^{q-1} - 2(-1)^{q-2} \equiv 2(-1)^q \pmod{X(n)^2} \end{aligned}$$

which proves the theorem.

References

- [1] D. JARDEN, Recurring sequences. *Riveon Lematematika*, Jerusalem (Israel), 1973.
- [2] J. P. JONES and P. KISS, Generalized Lucas sequences, to appear.
- [3] E. LUCAS, Theorie des fonctions numériques simplement périodiques. *Amer. Jour. of Math.*, **1** (1878), 184–240, 289–321.
- [4] J. ROBINSON and Y. V. MATIJASEVIC, Reduction of an arbitrary diophantine equation to one in 13 unknowns. *Acta Arithmetica*, **27** (1975), 521–553.
- [5] C. R. WALL., Some congruence involving generalized Fibonacci numbers, *Fibonacci Quart.*, **17** (1979), 29–33.

An approximation problem concerning linear recurrences

KÁLMÁN LIPTAI*

Abstract. Let $\{R_n\}_{n=0}^{\infty}$ and $\{V_n\}_{n=0}^{\infty}$ ($n=0,1,2,\dots$) be sequences of integers defined by $R_n = AR_{n-1} - BR_{n-2}$ and $V_n = AV_{n-1} - BV_{n-2}$, where A and B are fixed non-zero integers. We prove that the distance from the points $P_n(R_n, R_{n+1}, V_n)$ to the line L , L is defined by $x=t, y=\alpha t, z=\sqrt{D}t$, tends to zero in some case. Moreover, we show that there is no lattice points (x, y, z) nearer to L than $P_n(R_n, R_{n+1}, V_n)$ if and only if $|B|=1$.

Let $\{R_n\}_{n=0}^{\infty}$ and $\{V_n\}_{n=0}^{\infty}$ be second order linear recurring sequences of integers defined by

$$\begin{aligned}R_n &= AR_{n-1} - BR_{n-2} & (n > 1), \\V_n &= AV_{n-1} - BV_{n-2} & (n > 1),\end{aligned}$$

where $A > 0$ and B are fixed non-zero integers and the initial terms of the sequences are $R_0 = 0, R_1 = 1, V_0 = 2$ and $V_1 = A$. Let α and β be the roots of the characteristic polynomial $x^2 - Ax + B$ of these sequences and denote by D its discriminant. Then we have

$$(1) \quad \sqrt{D} = \sqrt{A^2 - 4B} = \alpha - \beta, \quad A = \alpha + \beta, \quad B = \alpha\beta.$$

Throughout the paper we suppose that $D > 0$ and D is not a perfect square. In this case, α and β are two irrational real numbers and $|\alpha| \neq |\beta|$, so we can suppose that $|\alpha| > |\beta|$.

Furthermore, as it is well known, the terms of the sequences R and V are given by

$$(2) \quad R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad V_n = \alpha^n + \beta^n.$$

Some results are known about points whose coordinate are terms of linear recurrences from a geometric points of view. G. E. Bergum [1] and A. F.

* Research supported by the Hungarian National Scientific Research Foundation, Operating Grant Number OTKA T 016975 and 020295.

Horadam [2] showed that the points $P_n = (R_n, R_{n+1})$ lie on the conic section $Bx^2 - Axy + y^2 + eB^n = 0$, where $e = AR_0R_1 - BR_0^2 - R_1^2$ and the initial terms R_0 and R_1 are not necessarily 0 and 1. For the Fibonacci sequence, when $A = 1$ and $B = -1$, C. Kimberling [6] characterized conics satisfied by infinitely many Fibonacci lattice points $(x, y) = (F_m, F_n)$. J. P. Jones and P. Kiss [4] considered the distance of points $P_n = (R_n, R_{n+1})$ and the line $y = \alpha x$. They proved that this distance tends to zero if and only if $|\beta| < 1$. Moreover, they showed that in the case $|B| = 1$ there is not such a lattice point (x, y) which is nearer to the mentioned line than P_n , if $|x| < |R_n|$. They proved similar arguments in three-dimensional case, too.

In this paper we investigate the geometric properties of the lattice points $P_n = (R_n, R_{n+1}, V_n)$. We shall use the following result of P. Kiss [5]: if $|B| = 1$ and p/q is a rational number such that $(p, q) = 1$, then the inequality

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{D}q^2}$$

implies that $p/q = R_{n+1}/R_n$ for some $n \geq 1$.

It is known, that

$$(3) \quad \lim_{n \rightarrow \infty} \frac{R_{n+1}}{R_n} = \alpha$$

and

$$(4) \quad \lim_{n \rightarrow \infty} \frac{V_n}{R_n} = \sqrt{D}$$

(see. e.g. [3], [7]).

Let us consider the vectors (R_n, R_{n+1}, V_n) . Since by (3) and (4) and using the equality

$$(R_n, R_{n+1}, V_n) = R_n \left(1, \frac{R_{n+1}}{R_n}, \frac{V_n}{R_n} \right)$$

we get that the direction of vectors (R_n, R_{n+1}, V_n) tends to the direction of the vector $(1, \alpha, \sqrt{D})$. However, the sequence of the lattice points $P_n = (R_n, R_{n+1}, V_n)$ does not always tend to the line passing through the origin and parallel to the vector $(1, \alpha, \sqrt{D})$, we give a condition when it is hold.

Theorem 1. Let L be the line defined by $x = t, y = \alpha t, z = \sqrt{D}t$, $t \in \mathbf{R}$. Furthermore, let d_n be the distance from the point (R_n, R_{n+1}, V_n) ($n = 0, 1, 2, \dots$) to the line L . Then $\lim_{n \rightarrow \infty} d_n = 0$ if and only if $|\beta| < 1$.

Proof. It is known that the distance from the point (x_0, y_0, x_0) to the line L is

$$(5) \quad d_{x_0, y_0, z_0} = \sqrt{\frac{(\sqrt{D}x_0 - z_0)^2 + (\alpha x_0 - y_0)^2 (\sqrt{D}y_0 - \alpha z_0)^2}{1 + \alpha^2 + D}}.$$

By (1), (2) and (5), we have

$$(6) \quad \sqrt{\frac{4\beta^{2n} + \left(\frac{-\alpha\beta^n + \beta^{n+1}}{\alpha - \beta}\right)^2 + (-\beta^{n+1} - \alpha\beta^n)^2}{1 + \alpha^2 + D}}$$

$$= \sqrt{\frac{4\beta^{2n} + \beta^{2n} \left(\frac{-\alpha + \beta}{\alpha - \beta}\right)^2 + \beta^{2n} (-\beta - \alpha)^2}{1 + \alpha^2 + D}} = \sqrt{\frac{\beta^{2n}(5 + A^2)}{1 + \alpha^2 + D}} = |\beta|^n \sqrt{\frac{5 + A^2}{1 + \alpha^2 + D}}.$$

From this the theorem follows.

It is easy to see that points P_n are on a plane. We investigate whether there is a lattice point $P = (x, y, z)$ in the plane such that $|x| < |R_n|$ and P is nearer to the line L than P_n . We use the previous denotations.

Theorem 2. The points $P_n = (R_n, R_{n+1}, V_n)$ are in a plane. Furthermore if n is sufficiently large, than there is no lattice pont (x, y, z) in this plane such that $d_{x,y,z} \leq d_n$ and $|x| < |R_n|$ if and only if $|B| = 1$.

Proof. First suppose $|B| = 1$. In this case, obviously, $|\beta| < 1$ and α is irrational, as it was supposed.

Using (2), we have

$$R_{n+1} = \alpha \frac{\alpha^n - \beta^n}{\alpha - \beta} + \frac{\alpha\beta^n - \beta^{n+1}}{\alpha - \beta} = \alpha R_n + \beta^n$$

and similarly

$$R_{n+1} = \beta R_n + \alpha^n.$$

Adding these equation, we get

$$(7) \quad 2R_{n+1} = (\alpha + \beta)R_n + V_n.$$

Consequently, the points P_n are on the plane which is defined by the equation $Ax - 2y + z = 0$. It is easy to prove that L is also on this plane. Assume that for some n there is lattice point (x, y, z) on this plane such that

$$(8) \quad d_{x,y,z} \leq d_n$$

and $|x| < |R_n|$. Using the equation of the plane

$$(9) \quad (\alpha + \beta)x - 2y + z = 0$$

we get the following equalities

$$\begin{aligned} \left| \sqrt{D}x - z \right| &= |(\alpha - \beta)x - z| \\ &= |(\alpha x - (\beta x + z))| = |\alpha x - (2y - \alpha x)| = 2|\alpha x - y| \end{aligned}$$

and

$$(11) \quad \left| \sqrt{D}y - \alpha z \right| = |(\alpha - \beta)y - (2\alpha y - \alpha(\alpha + \beta)x)| = |\alpha + \beta| |\alpha x - y|.$$

Thus, from (1), (5), (6), (8), (10) and (11) we obtain the inequality

$$d_{x,y,z} = \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}} |\alpha x - y| \leq |\beta|^n \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}},$$

and so using $|x| < |R_n|$ and (1), we get

$$\left| \alpha - \frac{y}{x} \right| \leq \frac{|\beta|^n}{|x|} = \frac{1}{|\alpha|^n |x|} = \frac{1 - (\beta/\alpha)^n}{|R_n| \sqrt{D} |x|} < \frac{1 - (\beta/\alpha)^n}{\sqrt{D} |x|^2}.$$

From this, using the mentioned theorem of P. Kiss and its proof, we obtain $x = R_i$, $y = R_{i+1}$ and by (9) $z = 2y - (\alpha + \beta)x = V_n$, for some i , if n is sufficiently large. Thus $d_{x,y,z} \leq d_n$. But by (6), $d_k < d_n$, only if $k > n$, so $i \geq n$. It can be seen that $|R_t|, |R_{t+1}|, \dots$ is an increasing sequence if t is sufficiently large, so $|x| = |R_i| \geq |R_n|$, which contradicts the assumption $|x| < |R_n|$.

To complete the proof, we have to show that in the case $|B| > 1$ there are lattice points (x, y, z) for which $d_{x,y,z} \leq d_n$ and $|x| < |R_n|$ for some n .

Suppose $|B| > 1$. If $|\beta| > 1$, then by (6), $d_n \rightarrow \infty$ as $n \rightarrow \infty$, so there are such lattice points for any sufficiently large n .

If $|\beta| = 1$ the d_n is a constant and there are infinitely many n and points (x, y, z) which fulfill the assumptions.

Suppose $|\beta| < 1$. Let y/x be a convergent of the simple continued fraction expansion of the irrational α . Then, by the elementary properties of continued fraction expansions of irrational numbers and by (10), (11), we have the inequalities

$$\begin{aligned} |\alpha x - y| &< \frac{1}{x}, \\ \left| \sqrt{D}x - z \right| &= 2|\alpha x - y| < \frac{2}{x}, \\ \left| \sqrt{D}y - \alpha z \right| &= |\alpha + \beta| |\alpha x - y| < |\alpha + \beta| \frac{1}{x}. \end{aligned}$$

Using by (5) we obtain

$$(12) \quad d_{x,y,z} < \frac{1}{|x|} \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}}.$$

Let the index n be defined by $|R_{n-1}| \leq |x| < |R_n|$. For this n , by (1), (2), (6) and (12), we have

$$\begin{aligned} d_n &= |\beta|^n \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}} = \frac{|B|^n}{|\alpha|^n} \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}} \\ &= \frac{|B|^n}{|\alpha|^{n-1}} \cdot \frac{1}{|\alpha|} \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}} = \frac{(1 - (\beta/\alpha)^{n-1})}{|\alpha| \sqrt{D} |R_{n-1}|} |B|^n \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}} \\ &> \sqrt{\frac{A^2 + 5}{1 + \alpha^2 + D}} \cdot \frac{1}{x} > d_{x,y,z} \end{aligned}$$

if n is sufficiently large, since $|B| > 1$.

This shows that, for any lattice point (x, y, z) defined as above, there is an n such that $d_{x,y,z} < d_n$ and $|x| < |R_n|$. This completes the proof.

References

- [1] G. E. BERGUM, Addenda to Geometry of a generalized Simson's Formula, *Fibonacci Quart.* **22** N°1 (1984), 22–28.
- [2] A. F. HORADAM, Geometry of a Generalized Simson's Formula, *Fibonacci Quart.* **20** N°2 (1982), 164–68.
- [3] D. JARDEN, Recurring Sequences, *Riveon Lematematika*, Jerusalem (Israel), 1958.
- [4] J. P. Jones and P. Kiss, On points whose coordinates are terms of a linear recurrence, *Fibonacci Quart.* **31**, N°3 (1993), 239–245.
- [5] P. KISS, A Diophantine approximative property of second order linear recurrences, *Period. Math. Hungar.* **11** (1980), 281–287.
- [6] C. KIMBERLING, Fibonacci Hyperbolas, *Fibonacci Quarterly*, **28**, N°1 (1990), 22–27.
- [7] E. LUCAS, Theorie des fonctions numériques simplement periodiques, *American J. Math.*, **1** (1978), 184–240, 289–321.

A note on the prime divisors of Lucas numbers

PÉTER KISS* and BÉLA ZAY*

Abstract. A sequence R_0, R_1, R_2, \dots of rational integers is called sequence of Lucas numbers with parameters A and B if $R_n = AR_{n-1} + BR_{n-2}$ ($n > 1$) and the initial terms are $R_0 = 0, R_1 = 1$. Let $f(n)$ be the reciprocal sum of the distinct prime divisors of R_n . It is known that there is a constant $c > 0$ such that $\sum_{n \leq x} f(n) = cx + o(x)$. We show that the average order of $f(n)$ is also a constant if we consider the function only on a short interval $[x, x+z]$, where $z/\log \log x \rightarrow \infty$ if $x \rightarrow \infty$.

Let R_0, R_1, \dots be a sequence of Lucas numbers with parameters A and B defined by

$$R_n = AR_{n-1} + BR_{n-2} \quad (n > 1),$$

where A, B are fixed nonzero coprime rational integers and the initial terms are $R_0 = 0, R_1 = 1$. Denote by α and β the roots of the equation $x^2 - Ax - B = 0$. In the following we suppose that the sequence is a non degenerate one, i.e. α/β is not a root of unity. It is known that the terms of this sequence can be expressed by

$$(1) \quad R_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$$

for any $n \geq 0$. It is also known that if p is a prime and $p \nmid B$, then there are terms of the sequence divisible by p . We denote the least positive index of these terms by $r(p)$. Thus $p \mid R_{r(p)}$ but $p \nmid R_m$ for $0 < m < r(p)$. If $p \nmid B$, $D = A^2 + 4B$ and (D/p) denote the Legendre symbol with $(D/p) = 0$ in the case $p \mid D$, then we have

$$(2) \quad r(p) \mid (p - (D/p))$$

and

$$(3) \quad p \mid R_n \quad \text{if and only if} \quad r(p) \mid n$$

(see e.g. D. H. Lehmer [4]).

* Research supported by the Hungarian OTKA foundation, N^o T 016975 and 020295.

The purpose of this note is to study the reciprocal sum of the prime divisors of Lucas numbers. Let $f(n)$ be the reciprocal sum of prime divisors of R_n , i.e. let

$$f(n) = \sum_{p|R_n} \frac{1}{p} \quad (n > 0).$$

We write $f(n) = 0$ if $R_n = \pm 1$ ($R_n \neq 0$ for $n > 0$ since α/β is not a root of unity). The value of $f(n)$ can be arbitrarily large (e.g. in the case $n = m!$ $f(n) \gg \log \log \log n$) and arbitrarily small (e.g. if n is a prime then $f(n) \ll (\log \log n)^2/n$). But the average order of $f(n)$ is a constant

$$\sum_{n \leq x} f(n) = c_0 x + O(\log \log x)$$

(see P. Kiss [3]). It is proved in [2] for the special case $(A; B) = (3; -2)$, that if $R_n = 2^n - 1$ is the sequence of Mersenne numbers, then the average order of $f(n)$ is also a constant even if we consider the function in a short interval. For general sequences we show a similar result.

Theorem. Let x and z be positive integers such that

$$\frac{z}{\log \log x} \rightarrow \infty \quad \text{as } x \rightarrow \infty.$$

Then for any sufficiently large x we have

$$\sum_{n=x}^{x+z} f(n) = cz + o(z),$$

where $c > 0$ is a constant depending only on the parameters of the sequence.

For the proof of theorem we need some auxiliary results. In the proofs c_1, c_2, \dots will denote positive constants depending only on the sequence. Furthermore we shall use some elementary results of prime number theory, they can be found e.g. in [1].

Lemma 1. For the reciprocal sum of the primes for which $r(p) \leq y$ we have

$$\sum_{r(p) \leq y} \frac{1}{p} = \log \log y + O(1)$$

for any sufficiently large positive y .

Proof. By (2) $r(p) \leq p + 1$ and so

$$(4) \quad \sum_{r(p) \leq y} \frac{1}{p} \geq \sum_{p \leq y} \frac{1}{p} + O(1) = \log \log y + O(1).$$

On the other hand, by (1),

$$(5) \quad |R_n| < \exp(c_1 n)$$

with some $c_1 > 0$. By (5) R_n has at most $c_2 n$ distinct prime divisors since the product of the first $c_2 n$ primes is greater than $e^{c_1 n}$ for some c_2 . From this it follows that the number of primes for which $r(p) \leq y$ is less than $c_3 y^2$. But each of the first $c_3 y^2$ primes is less than $c_4 y^3$ and so

$$(6) \quad \sum_{r(p) \leq y} \frac{1}{p} < \sum_{p < c_4 y^3} \frac{1}{p} = \log \log y + O(1).$$

From (4) and (6) the lemma follows.

Lemma 2. For the primes with $p \nmid B$ the sum

$$\sum_{\substack{p \\ p \nmid B}} \frac{1}{pr(p)}$$

converges.

Proof. Since $p \mid r_r(p)$, by (5) $p < \exp(c_1 r(p))$ and $\log p < c_1 r(p)$ follows. So

$$\sum_{\substack{p \\ p \nmid B}} \frac{1}{pr(p)} < c_5 \sum_p \frac{1}{p \log p}.$$

It is known that the last sum is convergent which proves the lemma.

Proof of the Theorem. Let x and z be sufficiently large positive integers. We can suppose that $z < x$ since in the case $z \geq x$ the Theorem follows from the case $z < x$. The sum in the Theorem can be written as

$$(7) \quad \sum_{n=x}^{x+z} f(n) = A(x) + B(x),$$

where

$$A(x) = \sum_{n=x}^{x+z} \sum_{\substack{d|n \\ d \leq z}} \sum_{r(p)=d} \frac{1}{p}$$

and

$$B(x) = \sum_{n=x}^{x+z} \sum_{\substack{d|n \\ d \leq z}} \sum_{r(p)=d} \frac{1}{p}.$$

By Lemma 1 and 2, using (3) and the condition of the Theorem, we have

$$(8) \quad \begin{aligned} A(x) &= \sum_{d \leq z} \left(\left(\frac{z}{d} + O(1) \right) \sum_{r(p)=d} \frac{1}{p} \right) = z \sum_{r(p) \leq z} \frac{1}{pr(p)} \\ &+ O \left(\sum_{r(p) \leq z} \frac{1}{p} \right) = cz + o(z), \end{aligned}$$

where c is a constant determined by Lemma 2.

Now we give an estimation for $B(x)$. Since every d with $d > z$ occurs at most once in the sum, by Lemma 1 and $z \leq x$ we get

$$\begin{aligned} B(x) &< \sum_{d \leq x+z} \sum_{r(p)=d} \frac{1}{p} = \sum_{r(p) \leq x+z} \frac{1}{p} = \\ &= \log \log(x+z) + O(1) = \log \log x + O(1). \end{aligned}$$

But $\log \log x = o(z)$ by the condition of the Theorem, so

$$(9) \quad B(x) = o(z).$$

From (7), (8) and (9) the Theorem follows.

Lastly we note that our theorem can be improved. In the proofs we have used only some elementary results of prime number theory. Using some deeper methods and results (e.g. the Brun–Titchmarsh inequality) the condition for z can be replaced by $z/\log \log \log x \rightarrow \infty$.

References

- [1] T. M. APOSTOL, Introduction to analytic number theory, *Springer-Verlag*, New York–Heidelberg–Berlin, 1976.
- [2] P. ERDŐS, P. KISS and C. POMERANCE, On prime divisors of Mersenne numbers, *Acta Arithm.*, **57** (1991), 267–281.
- [3] P. KISS, On prime divisors of the terms of second order linear recurrence sequences, Applications of Fibonacci numbers (ed. by G. E. Bergum), *Kluwer Acad. Publ.*, (1990), 203–207.
- [4] D. H. LEHMER, An extended theory of Lucas function, *Ann. of Math.*, **31** (1990), 419–448.

Two problems related to the Bernoulli numbers

FERENC MÁTYÁS*

Abstract. In this paper we deal with two similar problems. First we look for those polynomials $f_k(n)$ with rational coefficients for which the equality $S_k(n)=1^k+2^k+\dots+n^k=(f_k(n))^m$ holds for every positive integer n with some positive integer k and $m(\geq 2)$. In our first theorem we prove for $m\geq 2$ that $S_k(n)=(f_k(n))^m$ holds for every positive integer n if and only if $m=2$, $k=3$ and $f_3(n)=\frac{1}{2}n^2+\frac{1}{2}n$. In the second part of this paper we look for those polynomials $f(n)$ with complex coefficients for which the equality

$$P_k(n,c)=\sum_{j=k}^{2n-2} n^{\frac{j-c}{2n-j}} \binom{2n-1}{j} B_{2n-j}=(f(n))^m$$

holds for every integer $n\geq k$ with some integer $m\geq 2$, where $k\in\{2,3,4\}$, B_j is the j^{th} Bernoulli number and c is a complex parameter. In our second theorem we prove for $m\geq 2$ that $P_2(n,c)=(f(n))^m$ holds for every integer $n\geq 2$ if and only if $m=2$, $c=1\pm i2\sqrt{2}$ and $f(n)=n+p$ where $p=-1\pm i\frac{\sqrt{2}}{2}$; while in the cases of $k=3$ or 4 and $m\geq 2$ the equality $P_k(n,c)=(f(n))^m$ doesn't hold for any polynomial $f(n)$.

Let us introduce the following notations: $\binom{n}{k}$ is the usual binomial coefficient; B_j is the j^{th} Bernoulli number defined by the recursion

$$(1) \quad \sum_{j=0}^{k-1} \binom{k}{j} B_j = 0 \quad (k \geq 2)$$

with $B_0 = 1$. $S_k(n) = 1^k + 2^k + \dots + n^k$ ($n \geq 1$, $k \geq 1$ are integers); $P_k(n, c) = \sum_{j=k}^{2n-2} n^{\frac{j-c}{2n-j}} \binom{2n-1}{j} B_{2n-j}$, where $n \geq k \geq 2$ are integers and c is a complex parameter; $f_k(n)$ and $f(n)$ are polynomials of n with rational and complex coefficients, respectively.

The problem of looking for those polynomials $f_k(n)$ and integers $m \geq 2$ for which $S_k(n) = (f_k(n))^m$ for every positive integer n was proposed and

* Research supported by the Hungarian OTKA foundation, N^o T 020295.

solved in [1] and the author of this paper also was among the solvers. In our Theorem 1., using the Bernoulli numbers, we give a new proof for this problem.

Theorem 1. If $m \geq 2$ is an integer then there exists a polynomial $f_k(n)$ such that $S_k(n) = \left(f_k(n)\right)^m$ for every positive integer n if and only if $m = 2$, $k = 3$ and $f_3(n) = \frac{1}{2}n^2 + \frac{1}{2}n$.

Proof. It is known that $S_k(n)$ can be expressed by the Bernoulli numbers and the binomial coefficients, that is

$$(2) \quad S_k(n) = \frac{1}{k+1} \left(\binom{k+1}{0} B_0 n^{k+1} + \binom{k+1}{1} B_1 n^k + \cdots + \binom{k+1}{k-1} B_{k-1} n^2 + \binom{k+1}{k} B_k n \right)$$

moreover

$$(3) \quad B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, \dots \quad \text{and} \\ B_j = 0 \quad \text{if and only if } j \geq 3 \text{ and } j \text{ is odd.}$$

Let $f_k(n) = a_j n^j + \cdots + a_1 n + a_0$ be a polynomial of n over the rationals and $a_j \neq 0$. If $S_k(n) = \left(f_k(n)\right)^m$ for some m , then by (2) $a_0 = 0$ follows and since $m \geq 2$ so the degree of the polynomial $\left(f_k(n)\right)^m$ is at least two, that is $B_k = 0$ in (2). But by (3) $B_k = 0$ implies that $k \geq 3$, k is an odd integer and $B_{k-1} \neq 0$.

From the equality $S_k(n) = \left(f_k(n)\right)^m$ it follows that

$$\frac{1}{k+1} \left(\binom{k+1}{0} B_0 n^{k+1} + \cdots + \binom{k+1}{k-1} B_{k-1} n^2 \right) = a_j^m n^{mj} + \cdots + a_1^m n^m$$

and from this we get $m = 2$ and $a_1 \neq 0$.

So we have to investigate the equality

$$(4) \quad \frac{1}{k+1} \left(n^{k+1} + \cdots + \binom{k+1}{k-1} B_{k-1} n^2 \right) = (a_j n^j + \cdots + a_1 n)^2$$

from which we obtain that $k+1 = 2j$ and $\frac{1}{k+1} = a_j^2$. Moreover a_j is a rational number, therefore $k+1 = 4f$ and $j = 2f$. (4) can be written in the following form:

$$(5) \quad \frac{1}{k+1} \left(n^{k+1} + \cdots + \binom{k+1}{k-1} B_{k-1} n^2 \right) \\ = (a_{2f} n^{2f} + \cdots + a_2 n^2 + a_1 n)^2$$

and from (5) by $a_1 \neq 0$ and (3) $a_2 = a_4 = \dots + a_{2f-2} = 0$ follows. But $2a_{2f}a_1 = \frac{1}{k+1} \binom{k+1}{k-2f} B_{k-2f} \neq 0$, that is $B_{k-2f} = B_{4f-1-2f} = B_{2f-1} \neq 0$. It implies that $2f-1 = 1$, and so $f = 1$, $j = 2$ and $k = 3$. Thus we have got the only solution $m = 2$, $k = 3$, $f_3(n) = \frac{1}{2}n^2 + \frac{1}{2}n$ and $S_3(n) = (\frac{1}{2}n^2 + \frac{1}{2}n)^2$

In [2], using the definition $P_k(n, c)$, one can find the proof of the equality $\frac{1}{n}P_2(n, 3) = n - 3 + \frac{3}{2n}$. In our Theorem 2. we generalize this result and the proof will be similar to that proof which was sent for the original problem by the author of this paper.

Theorem 2. a) If $m \geq 2$ is an integer then there exists a polynomial $f(n)$ such that $P_2(n, c) = (f(n))^m$ for every integer $n \geq 2$ if and only if $m = 2$, $c = 1 \pm i2\sqrt{2}$ and $f(n) = n - 1 \pm i\frac{\sqrt{2}}{2}$.

b) If $m \geq 2$ and $k = 3$ or 4 then the equality $P_k(n, c) = (f(n))^m$ can not be solved by any polynomial $f(n)$ and parameter c .

Proof. One can easily verify the following equality:

$$(6) \quad \frac{j-c}{2n-j} \binom{2n-1}{j} = \binom{2n-1}{2n-j} - \frac{c}{2n} \binom{2n}{2n-j}.$$

Using (6), we have

$$(7) \quad P_k(n, c) = n \sum_{j=k}^{2n-2} \binom{2n-1}{2n-j} B_{2n-j} - \frac{c}{2} \sum_{j=k}^{2n-2} \binom{2n}{2n-j} B_{2n-j}.$$

By the recursive definition (1) of the Bernoulli number we can write that

$$(8) \quad \sum_{j=k}^{2n-2} \binom{2n-1}{2n-j} B_{2n-j} = -\binom{2n-1}{k-1} B_{k-1} \\ - \binom{2n-1}{k-2} B_{k-2} - \dots - \binom{2n-1}{1} B_1 - \binom{2n-1}{0} B_0$$

and

$$(9) \quad \sum_{j=k}^{2n-2} \binom{2n}{2n-j} B_{2n-j} = -\binom{2n}{2n-1} B_{2n-1} - \binom{2n}{k-1} B_{k-1} \\ - \binom{2n}{k-2} B_{k-2} - \dots - \binom{2n}{1} B_1 - \binom{2n}{0} B_0.$$

First let us deal with the case a) of the Theorem 2. If $k = 2$ then by (7), (8), (9) and (3)

$$P_2(n, c) = n \left(-\binom{2n-1}{1} B_1 - \binom{2n-1}{0} B_0 \right) - \frac{c}{2} \left(-\binom{2n}{2n-1} B_{2n-1} - \binom{2n}{1} B_1 - \binom{2n}{0} B_0 \right) = n^2 - \frac{3+c}{2}n + \frac{c}{2}$$

follows. From this, investigating the polynomial equality $P_2(n, c) = (f(n))^m$ in the case $m \geq 2$, we can see that $m = 2$ and $f(n) = (n+p)^2$, where $p = -1 \pm i\sqrt{2}$ and $c = 1 \pm i2\sqrt{2}$.

Now let us consider the case b) of the Theorem 2.

If $k = 3$ then by (7), (8), (9), and (3)

$$P_3(n, c) = n \left(-\binom{2n-1}{2} B_2 - \binom{2n-1}{1} B_1 - \binom{2n-1}{0} B_0 \right) - \frac{c}{2} \left(-\binom{2n}{2} B_2 - \binom{2n}{1} B_1 - \binom{2n}{0} B_0 - \binom{2n}{2n-1} B_{2n-1} \right) = \dots = -\frac{n^3}{3} + \frac{9+c}{6}n^2 - \frac{7c+20}{12}n + \frac{c}{2}.$$

If $P_3(k, n) = (f(n))^m$ and $m \geq 2$ then $m = 3$ and $f(n)$ should have the form $f(n) = -\frac{1}{\sqrt[3]{3}}n + \sqrt[3]{\frac{c}{2}}$. But it is easy to verify that such complex numbers c don't exist.

If $k = 4$ then B_3 appears on the right side of (8) and (9). But $B_3 = 0$ and so $P_3(n, c) = P_4(n, c)$. Therefore $P_4(n, c) = (f(n))^m$ ($m \geq 2$) is also unsolvable.

Remark. The statement of the Theorem 2 can also be extended for $k \geq 5$ too, but it seems, that there is no polynomial $f(n)$ such that $P_k(n, c) = (f(n))^m$ where $m \geq 2$.

References

- [1] B. BUGGISH, H. HARBORTH and O. P. LOSSER, Aufgabe 790., *Elemente der Mathematik*, Nr 4. (1978), 97–98.
- [2] P. ADDOR, R. WYSS, Aufgabe 813., *Elemente der Mathematik*, Nr. 6. (1979), 146–147.

Multiplicative functions satisfying the equation $f(m^2 + n^2) = (f(m))^2 + (f(n))^2$

PHAM VAN CHUNG

Abstract. Purpose of the present paper is to characterize multiplicative functions f which satisfy the equation $f(m^2+n^2)=(f(m))^2+(f(n))^2$ for all positive integers m and n .

1. Introduction

A “multiplicative function” is a function f defined on the set of the positive integers such that $f(mn) = f(m)f(n)$ whenever the greatest common divisor of m and n is 1. The function f is called “completely” multiplicative if the condition $f(mn) = f(m)f(n)$ holds for all m and n .

Claudia A. Spiro [2] proved that if a multiplicative function f satisfies the condition $f(p+q) = f(p) + f(q)$ for all primes p, q and $f(p_0) \neq 0$ for at least one prime p_0 , then $f(n) = n$ for each positive integer n .

Replacing the set of primes by the set of squares, in [1], we have investigated the multiplicative functions f satisfying the condition

$$(A) \quad f(m^2 + n^2) = f(m^2) + f(n^2)$$

for all positive integers m, n . We have shown that if $f \neq 0$ is multiplicative, then f fulfills the condition (A) if and only if either

$$(A-1) \quad f(2^k) = 2^k \text{ for all integers } k \geq 0,$$

$$(A-2) \quad f(p^k) = p^k \text{ for all primes } p \equiv 1 \pmod{4} \\ \text{and all integers } k \geq 1, \text{ and}$$

$$(A-3) \quad f(q^{2k}) = q^{2k} \text{ for all primes } q \equiv 3 \pmod{4} \\ \text{and all integers } k \geq 1$$

or

$$(a-1) \quad f(2) = 2 \text{ and } f(2^k) = 0 \text{ for all integers } k \geq 2,$$

$$(a-2) \quad f(p^k) = 1 \text{ for all primes } p \equiv 1 \pmod{4} \\ \text{and all integers } k \geq 1, \text{ and}$$

$$(a-3) \quad f(q^{2k}) = 1 \text{ for all primes } q \equiv 3 \pmod{4} \\ \text{and all integers } k \geq 1.$$

In the present paper we consider a similar question, and we give solutions of multiplicative functions f satisfying the equation

$$(B) \quad f(m^2 + n^2) = (f(n))^2 + (f(n))^2$$

for all positive integers m and n . Investigating this question we have same result by using the method of [1]. Our main result is to prove the following.

Theorem. Let $f \neq 0$ be a multiplicative function. The f fulfills the condition

$$(C) \quad f(m^2 + n^2) = (f(m))^2 + (f(n))^2$$

for all positive integers m and n if and only if

$$(C-1) \quad f(2^k) = 2^k \text{ for all integers } k \geq 0,$$

$$(C-2) \quad f(p^k) = p^k \text{ for all primes } p \equiv 1 \pmod{4} \\ \text{and all integers } k \geq 1, \text{ and}$$

$$(C-3) \quad f(q^{2k}) = q^{2k} \text{ for all primes } q \equiv 3 \pmod{4} \\ \text{and all integers } k \geq 1.$$

We shall prove our theorem in the next two sections. First in Section 2, we verify some auxiliary lemmas. Finally, in Section 3, we give the proof of the theorem.

2. Lemmas

Lemma 1. If f satisfies the hypotheses of the theorem, then we have $f(2) = 2$ and $f(4) = 4$.

Proof. Since $f \neq 0$ multiplicative, we have $f(1) = 1$. Thus, (C) yields $f(2) = f(1^2 + 1^2) = (f(1))^2 + (f(1))^2 = 1 + 1 = 2$. Therefore, by using the equation $5 = 2^2 + 1^2$, (C) implies that $f(5) = (f(2))^2 + (f(1))^2 = 5$. So, we conclude from (C) and the multiplicativity of f that $(f(3))^2 = f(10) - (f(1))^2 = 9$. The fact that $20 = 4^2 + 2^2$, coupled with $f(2) = 2$, $f(5) = 5$ and (C), forces

$$(1) \quad (f(4))^2 = f(20) - (f(2))^2 = 5f(4) - 4.$$

On the other hand, from (C), the multiplicativity of f , and the equation $52 = 4^2 + 6^2$, the equation

$$(2) \quad \begin{aligned} (f(4))^2 &= f(52) - (f(6))^2 = f(13)f(4) - \\ &- (f(2))^2(f(3))^2 = f(13)f(4) - 2^2 3^2 \end{aligned}$$

follows.

But, by using (C) and the fact $13 = 3^2 + 2^2$, we have $f(13) = (f(3))^2 + (f(2))^2 = 9 + 4 = 13$. So, from (2), it follows that

$$(3) \quad (f(4))^2 = 13f(4) - 36.$$

Thus, by (1) and (3), we have $5f(4) - 4 = 13f(4) - 36$. Consequently, $f(4) = 4$. So, the lemma is proved.

Lemma 2. If f fulfills the hypotheses of the theorem, then we have

$$f(2^k) = 2^k \quad \text{for all integers } k \geq 0.$$

Proof. By Lemma 1, we have $f(2^k) = 2^k$ for $k = 1, 2$, and it is clear for cases $k = 0$ and $k = 3$. Assume that n is an integer with $n \geq 3$, and that we have $f(2^k) = 2^k$ for all integers $1 \leq k \leq n$. We will show that $f(2^{n+1}) = 2^{n+1}$. If $n + 1$ is even then $n + 1 = 2k$, where $k + 1 \leq n$. Thus, (C), the multiplicativity of f , $f(5) = 5$, and the hypotheses of the induction yield

$$\begin{aligned} 5f(2^{n+1}) &= f(5 \cdot 2^{n+1}) = f(2^{2k+2} + 2^{2k}) = (f(2^{k+1}))^2 + (f(2^k))^2 \\ &= 2^{2k+2} + 2^{2k} = 5 \cdot 2^{2k} \end{aligned}$$

which gives

$$f(2^{n+1}) = 2^{n+1}.$$

So, it remains to show that $f(2^{n+1}) = 2^{n+1}$, when $n + 1$ is odd. If $n + 1$ is odd, then $n + 1 = 2k + 1$ where $k \leq n$. By using (C) and the hypotheses of induction, we obtain

$$f(2^{n+1}) = f(2^{2k} + 2^{2k}) = 2(f(2^k))^2 = 2 \cdot 2^{2k} = 2^{n+1}.$$

Thus, the lemma is proved.

Lemma 3. If f satisfies the hypotheses of the theorem, then we have

$$f(m^2) = (f(m))^2$$

for all positive integers m .

Proof. From the multiplicativity of f and Lemma 2. we easy reduce that $f(2m) = 2f(m)$ for all positive integers m . Thus, by (C) we have $2f(m^2) = f(2m^2) = f(m^2 + m^2) = 2(f(m))^2$, from which $f(m^2) = (f(m))^2$ follows.

Lemma 4. If f fulfills the hypotheses of the theorem, then we have

$$(f(m))^2 = m^2$$

for all positive integers m .

We note that from (C) and Lemma 3 condition (A) follows. So we have, using Lemma 2, that $(A_1) - (A_3)$ are satisfied. From this we have $f(m^2) = m^2$, which proves the lemma. But here we give another proof.

Proof. We argue by induction on m . In the proof of Lemma 1. we have shown that $(f(m))^2 = m^2$ for $m = 1, 2$ and 3 .

Suppose that n is an integer with $n \geq 3$, and $(f(m))^2 = m^2$ for all positive integers $m \leq n$. We will show that $(f(n+1))^2 = (n+1)^2$. If $n+1$ is even, then $n+1 = 2^k h$ where $h \leq n$ and h is odd. Thus, by the multiplicativity of f , Lemma 2. and the hypotheses of the induction, we obtain

$$(f(n+1))^2 = (f(2^k))^2 (f(h))^2 = 2^{2k} h^2 = (n+1)^2.$$

To show that $(f(n+1))^2 = (n+1)^2$, when $n+1$ is odd, we use the equation $(n-1)^2 + (n+1)^2 = 2(n^2+1)$, where $(2, n^2+1) = 1$. From this and (C) we have $(f(n+1))^2 = f[2(n^2+1)] - (f(n-1))^2 = f(2) [(f(n))^2 + (f(1))^2] - (f(n-1))^2$. Since $f(2) = 2$, and the hypotheses of the induction, we reduce that

$$(f(n+1))^2 = 2(n^2+1) - (n-1)^2 = (n+1)^2,$$

which proves the lemma.

Now we return to prove the theorem.

3. The proof of the theorem

First we verify the necessity of the condition.

Assume that f fulfills the condition of the theorem. Then, by Lemma 2., we have shown that (C—1) is satisfied. Moreover, by using Lemmas 3. and 4., we obtain

$$f(q^{2k}) = (f(q^k))^2 = (q^k)^2 = q^{2k}$$

for all positive integers q and k .

So, the condition (C-3) is fulfilled. If p is prim and $p \equiv 1 \pmod{4}$, then it is well known that there exist positive integers x and y such that

$$p^k = x^2 + y^2.$$

By using (C), Lemma 4., we have

$$f(p^k) = f(x^2 + y^2) = (f(x))^2 + (f(y))^2 = x^2 + y^2 = p^k,$$

which verified the condition (C-2). So, we have completed the proof the necessity of the condition.

Conversely, suppose that the conditions (C-1), (C-2) and (C-3) are satisfied for a multiplicative function f .

It is well known that we can write

$$m^2 + n^2 = 2^k p_1^{\alpha_1} p_2^{\alpha_2} \dots p_h^{\alpha_h} q_1^{2\beta_1} q_2^{2\beta_2} \dots q_s^{2\beta_s},$$

where p_i and q_j are primes, $p_i \equiv 1 \pmod{4}$ and $q_j \equiv 3 \pmod{4}$ for $i = 1, 2, \dots, h$ and $j = 1, 2, \dots, s$, and $k \geq 0$ and α_i, β_i are positive integers. Then by the multiplicativity of f and the conditions (C-1), (C-2) and (C-3),

$$\begin{aligned} f(m^2 + n^2) &= f(2^k) f(p_1^{\alpha_1}) \dots f(p_h^{\alpha_h}) f(q_1^{2\beta_1}) \dots f(q_s^{2\beta_s}) \\ &= 2^k p_1^{\alpha_1} \dots p_h^{\alpha_h} q_1^{2\beta_1} \dots q_s^{2\beta_s} = m^2 + n^2 = (f(m))^2 + (f(n))^2. \end{aligned}$$

So, this completes the proof of the theorem.

References

- [1] P. V. CHUNG, Multiplicative Functions f Satisfying the Equation $f(m^2 + n^2) = f(m^2) + f(n^2)$. *Mathematica Slovaca*, Vol. **44** (1994), (to appear)
- [2] SPIRO, CLAUDIA A., Additive Uniwueness Sets for Arithmetic Functions, *Journal of Number Theory*, **42** (1992), 232—246.



A primality test for Fermat numbers

A. GRZYTCZUK and J. GRZYTCZUK

Abstract. Relying on some properties of Bernoulli numbers we derive a new primality criterion for Fermat numbers $F_n = 2^{2^n} + 1$.

1. Introduction. For a given a sequence of positive integers it is often very hard to decide whether there are infinitely many primes among its terms. Consider for example the sequence $2+1, 2^2+1, 2^3+1, 2^4+1, \dots$. It is an easy observation that $2^m+1, m > 0$ can be a prime only if m is itself a power of 2. So, we obtain in this way the Fermat numbers $F_n = 2^{2^n} + 1, n \geq 0$. The first five of them are $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ and they are all primes. Fermat thought that this pattern persists but Euler found that F_5 is composite: $F_5 = 2^{32} + 1 = (641)(6700417)$. In fact, for $4 < n < 24$ and for many larger values of n Fermat numbers are known to be composite. It is strange that beyond F_5 no further Fermat primes have been found.

The propose of this note is to give a necessary and sufficient condition for the Fermat number F_n to be a prime. Our test is similar to the Lucas—Lehmer test for Mersenne numbers $M_n = 2^n - 1$ (see [2]). Indeed, primality of F_n depends on whether F_n divides an appropriate term of the recurrent sequence $T(m)$ defined by

$$(1a) \quad T(1) = 1,$$

$$(1b) \quad T(m) = (-1)^{m-1} + \sum_{i=1}^{m-1} (-1)^{i+1} \binom{2m-1}{2i} T(m-i), \quad m > 1.$$

This is stated in the following theorem.

Theorem. Let k and n be fixed positive integers such that $0 < k \leq [\log n \log 2]$, $n > 1$ and let $T(m)$ be as above. Then the Fermat number F_k is a prime if and only if F_k does not divide $T(2^{n-1})$.

2. Proof of the Theorem. We derive our assertion from the following lemma.

Lemma. Let B_{2m} denote the $2m$ -th Bernoulli number. Then for every

positive integer m we have

$$(2) \quad B_{2m} = (-1)^{m-1} m T(m) / 2^{2m-1} (2^{2m} - 1)$$

where $T(m)$ is defined by (1a) and (1b).

Proof. It is well known (see e.g. [1]) that

$$B_{2m} = (-1)^{m-1} m T_m / 2^{2m+1} (2^{2m} - 1)$$

where T_m are coefficients in the power series expansion of the function $\operatorname{tg} x$, i. e.

$$\operatorname{tg} x = \sum_{m=1}^{\infty} T_m \frac{x^{2m-1}}{(2m-1)!}.$$

Thus, we are going to prove that $T(m) = T_m$ for all $m > 0$. In fact, we can write

$$(3) \quad \sum_{m=1}^{\infty} T_m \frac{x^{2m-1}}{(2m-1)!} \sum_{m=0}^{\infty} (-1)^m \frac{x^{2m}}{(2m)!} = \sum_{m=1}^{\infty} (-1)^{m-1} \frac{x^{2m-1}}{(2m-1)!}.$$

By comparing coefficients of x^{2m-1} we have $T_1 = 1$ and

$$(4) \quad \begin{aligned} T_m / (2m-1)! - T_{m-1} / 2!(2m-3)! + \\ + T_{m-2} / 4!(2m-5)! - \dots = (-1)^{m-1} / (2m-1)!. \end{aligned}$$

Hence

$$T_m - \binom{2m-1}{2} T_{m-1} + \binom{2m-1}{4} T_{m-2} - \dots = (-1)^{m-1}$$

and the proof of Lemma is complete.

For the proof of the Theorem put $m = 2^{n-1}$. Then we have

$$(5) \quad B_{2^n} = \frac{(-1)2^{n-1}T(2^{n-1})}{2^{2^n-1}(2^{2^n}-1)} = \frac{(-1)2^{n-1}T(2^{n-1})}{2^{2^n-1}F_0F_1\cdots F_{n-1}}.$$

But from the well known theorem of von Staudt and Clausen it follows that if we write $B_{2m} = N_{2m} / D_{2m}$ with $(N_{2m}, D_{2m}) = 1$ then

$$D_{2m} = \prod_{p-1|2m} p, \quad p \text{ prime.}$$

It is now easy to see that D_{2^n} is a product of 2 and Fermat primes F_k with k not greater than $\log n / \log 2$. This finishes the proof of Theorem.

References

- [1] Z. I. BOREVICH and I. R. SHAFAREVICH, *Number Theory*, Moskva, 1964, (in Russian)
- [2] P. RIBENBOIM, *The Book of Prime Number Records*, *Springer-Verlag*, 1988.

On some applications of 2×2 integral matrices

A. GRYTCZUK and N. T. VOROBÈV

Abstract. In this paper we give a matrix representation for the fundamental solution of the Pellian type equation $x^2 - dy^2 = -1$. Using matrices the solutions of linear equations are also represented.

In 1970, in [1] some connections was given between integral 2×2 matrices and the Diophantine equation $ax - by = c$. Namely, we proved that the solution $\langle x_0, y_0 \rangle$ of this equation can be determined by the following equalities:

$$(1) \quad \begin{pmatrix} a & y_0 \\ b & x_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} 0 & -c \\ 1 & 0 \end{pmatrix}$$

if m is even, and

$$(2) \quad \begin{pmatrix} a & y_0 \\ b & x_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} 1 & 0 \\ 0 & c \end{pmatrix}$$

if m is odd, where $\frac{a}{b} = [q_0; q_1, \dots, q_m]$ is a representation of $\frac{a}{b}$ as a simple finite continued fraction.

For example, consider the equation

$$19x - 11y = -2.$$

We have $\frac{19}{11} = [1; 1, 2, 1, 2]$ and consequently $q_0 = 1, q_1 = 1, q_2 = 2, q_3 = 1, q_4 = 2$, thus $m = 4$ and by (1) we obtain

$$(3) \quad \begin{pmatrix} 19 & y_0 \\ 11 & x_0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}.$$

By Cauchy's theorem on product of determinants it follows from (3) that

$$(4) \quad 19x_0 - 11y_0 = -2.$$

So denote that $\langle x_0, y_0 \rangle$ is an integer solution of the equation $19x - 11y = -2$.

On the other hand by an easy calculation, from (3) we obtain

$$(5) \quad \begin{pmatrix} 19 & y_0 \\ 11 & x_0 \end{pmatrix} = \begin{pmatrix} 7 & 19 \\ 4 & 11 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 19 & 14 \\ 11 & 8 \end{pmatrix}.$$

By (5) it follows that $x_0 = 8, y_0 = 14$.

In 1986 A. J. van der Poorten [3] observed that if

$$\begin{pmatrix} c_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} c_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} c_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}, \quad n = 0, 1, \dots$$

then

$$\frac{p_n}{q_n} = [c_0; c_1, \dots, c_n].$$

Based on this observation he gave many interesting applications to the theory of continued fraction and also to the description of the solutions of the well-known Pell's equation $x^2 - dy^2 = 1$. In [2] we gave some connections between fundamental solution $\langle x_0, y_0 \rangle$ of the Pell's equation and representation of 2×2 integral matrix as a product of powers of the prime elements in the unimodular group.

In the present paper we give such connections between the fundamental solution $\langle x_0, y_0 \rangle$ of the non-Pellian equation $x^2 - dy^2 = -1$ and the corresponding matrix representation. We prove the following:

Theorem 1. Let

$$\sqrt{d} = [q_0; \overline{q_1, \dots, q_s}], \quad d > 0 \quad \text{and} \quad s > 1 \quad \text{is odd}$$

is odd, be the representation of \sqrt{d} as a simple periodic continued fraction. Then the fundamental solution $\langle x_0, y_0 \rangle$ of the non-Pellian equation

$$(6) \quad x^2 - dy^2 = -1$$

is contained in the second column of the following matrix:

$$(7) \quad F_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_{s-1}}.$$

Proof. First we prove that if $k = 2n, n = 1, 2, \dots$, then

$$(8) \quad \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & q_k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} P_{k-1} & P_k \\ Q_{k-1} & Q_k \end{pmatrix}$$

where $P_0 = q_0, Q_0 = 1, P_1 = q_0 q_1 + 1, Q_1 = q_1$ and

$$(9) \quad P_k = q_k P_{k-1} + P_{k-2}, \quad Q_k = q_k Q_{k-1} + Q_{k-2}; \quad k = 2n, n = 1, 2, \dots$$

It is easy to see that (8) is true for $k = 2$. Suppose that (8) is true for some $k = 2m$. Then we have

$$(10) \quad \begin{aligned} & \begin{pmatrix} P_{2m-1} & P_{2m} \\ Q_{2m-1} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_{2m+1} & 1 \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} P_{2m-1} + q_{2m+1} P_{2m} & P_{2m} \\ Q_{2m-1} + q_{2m+1} Q_{2m} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

By (9) and (10) it follows that

$$(11) \quad \begin{aligned} & \begin{pmatrix} P_{2m-1} & P_{2m} \\ Q_{2m-1} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_{2m+1} & 1 \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} P_{2m+1} & P_{2m} \\ Q_{2m+1} & Q_{2m} \end{pmatrix} \begin{pmatrix} 1 & q_{2m+2} \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Denoting the left hand side of (11) by F we obtain

$$(12) \quad F = \begin{pmatrix} P_{2m+1} & P_{2m} + q_{2m+2} P_{2m+1} \\ Q_{2m+1} & Q_{2m} + q_{2m+2} Q_{2m+1} \end{pmatrix} = \begin{pmatrix} P_{2m+1} & P_{2m+2} \\ Q_{2m+1} & Q_{2m+2} \end{pmatrix}.$$

By (12), (11) and (10) it follows that (8) is true for $k = 2m + 2$, thus by induction (8) is true for every $k = 2n, n = 1, 2, \dots$

Now, we can consider the following product:

$$(13) \quad F_0 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_{s-1}}, \quad s > 1.$$

Since

$$(14) \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},$$

for every positive integer m , then by (13), (14) and (8) for the case $k = s - 1$ we obtain

$$(15) \quad F_0 = \begin{pmatrix} P_{s-2} & P_{s-1} \\ Q_{s-2} & Q_{s-1} \end{pmatrix}.$$

On the other hand by (13) and (15) we get

$$(16) \quad \det F_0 = 1 = P_{s-2}Q_{s-1} - P_{s-1}Q_{s-2}.$$

Since

$$(17) \quad P_{s-1} = q_0Q_{s-1} + Q_{s-2} \quad \text{and} \quad dQ_{s-2} = q_0P_{s-1} + P_{s-2},$$

by (17) we have

$$(18) \quad P_{s-1}^2 - dQ_{s-1}^2 = P_{s-1}Q_{s-2} - P_{s-2}Q_{s-1}.$$

On the other hand it is well-known that

$$(19) \quad P_{s-1}Q_{s-2} - P_{s-2}Q_{s-1} = (-1)^s.$$

Since $s > 1$ and s is odd then by (18), (19) and (16) we obtain

$$(20) \quad P_{s-1}^2 - dQ_{s-1}^2 = -1,$$

so $\langle x_0, y_0 \rangle = \langle P_{s-1}, Q_{s-1} \rangle$ and the proof is complete.

For example consider the following non-Pellian equation:

$$x^2 - 13y^2 = -1.$$

We have $\sqrt{13} = [3; 1, 1, 1, 1, 6]$ and $q_0 = 3, q_1 = q_2 = q_3 = q_4 = 1, q_5 = 6; s = 5$ is odd. Then by the Theorem 1 we have

$$\begin{aligned} F_0 &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \\ &= \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 4 & 7 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 11 & 18 \\ 3 & 5 \end{pmatrix}, \end{aligned}$$

and consequently $x_0 = 18, y_0 = 5$.

Now, we gave a possibility for an application of 2×2 integral matrices to the examination of the equation:

$$(22) \quad a_1x_1 + a_2x_2 + \cdots + a_nx_n = b.$$

Namely, we prove the following:

Theorem 2. Let $(a_1, a_2, \dots, a_n) = 1$ and $d = (a_i, a_j)$ for some $i, j \in \{1, 2, \dots, n\}$, where (a_1, a_2, \dots, a_n) denote the greatest common divisor of $a_1, a_2, \dots, a_n \in \mathbb{Z}$. Then the integer solutions of (22) are of the form:

$$\langle v_1, v_2, \dots, x_i, \dots, x_j, \dots, v_n \rangle,$$

where x_i, x_j are determined by the following matrix equalities:

$$(23) \quad \begin{pmatrix} a_i & -x_i \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} 0 & -\frac{D}{d} \\ d & 0 \end{pmatrix},$$

if m is even and

$$(24) \quad \begin{pmatrix} a_i & -x_i \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{q_0} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_1} \cdots \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^{q_m} \begin{pmatrix} d & 0 \\ 0 & \frac{D}{d} \end{pmatrix},$$

if m is odd, where $\frac{a_i}{a_j} = [q_0; q_1, \dots, q_m]$, $d \mid D$ and $D = b - \sum_{\substack{k=1 \\ k \neq i, j}}^m a_k v_k$.

Proof. Let $(a_i, a_j) = d$. We can assume without loss of generality that $a_i \geq a_j > 0$. Applying to a_i, a_j the well-known theorem on division with remainder we obtain

$$(25) \quad a_i = a_j q_0 + r_1, \quad a_j = a_i q_1 + r_2, \dots, r_{m-1} = r q_m,$$

$$0 < r_m < r_{m-1} < \dots < r_1 < a_j$$

and

$$r_m = (a_i, a_j) = d.$$

Let $A = \begin{pmatrix} a_i & -x_j \\ a_j & x_i \end{pmatrix}$, then by (25) we obtain

$$A = \begin{pmatrix} a_j q_0 + r_1 & -x_j \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} r_1 & -(x_j + q_0 x_i) \\ a_j & x_i \end{pmatrix}.$$

Denoting by $x_j^{(1)} = -(x_j + q_0 x_i)$ and by $A_1 = \begin{pmatrix} r_1 & x_j^{(1)} \\ a_j & x_i \end{pmatrix}$ in similar way we obtain

$$A_1 = \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \begin{pmatrix} r_1 & x_j^{(1)} \\ r_2 & x_i - q_1 x_j^{(1)} \end{pmatrix}.$$

Denoting by $x_j^{(1)} = x_i - q_1 x_j^{(1)}$ and by $A_2 = \begin{pmatrix} r_1 & x_j^{(1)} \\ r_2 & x_i^{(1)} \end{pmatrix}$ we obtain

$$A_2 = \begin{pmatrix} 1 & q_2 \\ 0 & 1 \end{pmatrix} A_3.$$

Continuing this process we obtain in the last step the following matrices

$$\begin{pmatrix} r_m & 0 \\ 0 & x_i^{(1)} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} 0 & x_j^{(1)} \\ r_m & 0 \end{pmatrix}.$$

Consequently we obtain the following representation:

$$(26) \quad A = \begin{pmatrix} a_i & -x_j \\ a_j & x_i \end{pmatrix} = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & q_m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & x_j^{(1)} \\ d & 0 \end{pmatrix}$$

if m is even, or

$$(27) \quad A = \begin{pmatrix} 1 & q_0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ q_1 & 1 \end{pmatrix} \cdots \begin{pmatrix} 1 & 0 \\ q_m & 1 \end{pmatrix} \begin{pmatrix} d & 0 \\ 0 & x_i^{(1)} \end{pmatrix}$$

if m is odd. From (26) we have

$$\det A = a_i x_i + a_j x_j = D = -d x_j^{(1)}$$

and we obtain $d \mid D$. On the other hand putting $x_k = v_k$ for $k = 1, 2, \dots, n$ and $k \neq i, j$ we have

$$D = a_i x_i + a_j x_j = b - \sum_{\substack{k=1 \\ k \neq i, j}}^n a_k v_k.$$

In similar way by (27) it follows that $\det A = D = d x_j^{(1)}$ and we obtain $d \mid D$. In both cases we have $x_i^{(1)} = -\frac{D}{d}$ if m is even and $x_i^{(1)} = \frac{D}{d}$ if m is odd.

Hence, from (27) and (26) we obtain (23)–(24) and the proof is complete.

Consider the following equation:

$$(28) \quad 12x + 7y + 5z = 24.$$

We have $(12, 7, 5) = 1$. Equation (28) can be represented in the form

$$7y + 5z = 24 - 12x = 12(2 - a); \quad x = a.$$

On the other hand, we have:

$$\frac{7}{5} = [1; 2, 2].$$

By the Theorem 2, we have:

$$A = \begin{pmatrix} 7 & -z \\ 5 & y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}^2 \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 \begin{pmatrix} 0 & -(24 - 12a) \\ 1 & 0 \end{pmatrix},$$

where $D = \det A = 24 - 12a$, $d = (7, 5) = 1$, thus $d \mid D$. So we obtain

$$A = \begin{pmatrix} 7 & -z \\ 5 & y \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 2 & -(24 - 12a) \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 7 & -3(24 - 12a) \\ 5 & -2(24 - 12a) \end{pmatrix}.$$

and we have

$$x = a, \quad y = -2(24 - 12a), \quad z = 3(24 - 12a),$$

where a is an arbitrary integer.

References

- [1] A. GRZYCZUK, Application of integral matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to the determination of integer solutions of the equation $ax - by = \pm 1$, *Biul. WSInz. Mat.-Fiz.* № 4., (1970), Zielona Góra, 149–153, (in Polish).
- [2] A. GRZYCZUK and N. T. VOROB'EV, Application of matrices to the solutions of Diophantine equations, Vitebsk, Bielyorussia, (1990), (pp. 44), (in Russian).
- [3] A. J. VAN DER POORTEN, An introduction to continued fractions, *London Math. Soc. Lect. Note Ser.* № 109., (1986), 99–138.

Az $a^n + b^n = z^3$ diofantoszi egyenletről

MAURICE MIGNOTTE és PETHŐ ATTILA*

Abstract. (On the Diophantine equation $a^2 + b^n = z^3$) Let a, b, n, z be natural numbers for which the equation

$$a^n + b^n = z^3$$

holds. We prove that under the conditions $n > 1, a < b, a + b < 16$ and $(a, b) = 1$ the only solution is $(a, b, n, z) = (2, 11, 2, 5)$. In the proof we use a combination of elementary congruence considerations and an A. Baker's type theory.

1. Bevezetés

Legyenek a és b egész számok. Pethő [9], valamint Shorey and Stewart [12] egy általános tételéből következik, hogy van olyan csak a és b -től függő, effektíven kiszámítható $c > 0$ konstans, hogy az

$$(1) \quad a^n + b^n = z^3$$

diofantoszi egyenlet minden $n, z \in \mathbf{Z}_+$ megoldására $n, z < c$ teljesül. Dolgozatunkban \mathbf{Z}_+ a pozitív egész számok halmazát fogjuk jelölni.

Az effektív megoldhatóság azonban nem jelenti azt, hogy egy konkrét egyenlet összes megoldását ténylegesen meg is tudjuk határozni. A megoldásokat korlátozó konstansok ugyanis általában olyan nagyok, hogy addig a határig a közvetlen behelyettesítés reménytelenül hosszú ideig tartana. A 4. részben látni fogjuk például, hogy ha $a = 2$ és $b = 11$, akkor az (1) egyenletből n -re közvetlenül levezethető felső korlát $4,5 \cdot 10^{10}$.

Bizonyos egyenlettípusokra sikerült az utóbbi időben olyan numerikus technikákat kifejleszteni, amellyel az elméleti felső korlát annyira lecsökkenthető, hogy az alatt már a behelyettesítés is célhoz vezet. Ilyen módszereket dolgoztak ki többek között Thue egyenletekre: Pethő und Schulenberg [10], de Weger [15]; Thue–Mahler egyenletekre: de Weger and Tzanakis [14]; és indexforma egyenletekre: Gaál and Schulte [4] valamint Gaál, Pethő and Pohst [2], [3]. Az (1)-el analóg

$$a^n + b^n = z^2$$

* A szerző ez úton fejezi ki köszönetét az Université Louis Pasteur vendégszerzetéért és olyan alkotó légkör biztosításáért, amelyek többek között ennek a dolgozatnak az elkészítéséhez is hozzájárult.

egyenlet megoldásainak megkeresésével Mignotte [6] foglalkozott. Dolgozatunkban az ő módszerét finomítva és az (1) egyenletre alkalmazva bizonyítjuk az alábbi tételt:

Tétel. Ha az a, b, n, z pozitív egész számokra $n > 1, a < b, a + b \leq 16, (a, b) = 1$ és (1) teljesül, akkor $(a, b, n, z) = (2, 11, 2, 5)$.

Megjegyzés Az $a + b \leq 16$ feltétel csak technikai jellegű, arra szolgál, hogy dolgozatunk ne legyen túl terjedelmes. Mint látni fogjuk módszerünk, amelyik több eljárás kombinációja, alkalmazható tetszőleges rögzített a és b mellett (1) megoldásainak a meghatározására.

Számítógéppel megvizsgáltuk az (1) egyenlet megoldhatóságát modulo 9, 7, 13, 19, 31, 37, 43, 61, 67, 127, 181, 211, 331, 397, 421, 463, 73, 79, 97, 241, 313, 337, 547, 673, 859, 937. Azt tapasztaltuk, hogy az $1 < a < b < 1001$ intervallumban, az $(a, b) = 1$ feltételnek eleget tevő számpárok közül, ha $a + b$ vagy $a^2 + b^2$ nem köbszám, akkor (1) nem megoldható. Amennyiben $a + b$ vagy $a^2 + b^2$ köbszám, akkor pedig néhány esettől eltekintve $n \equiv 1$, illetve $2 \pmod{1441440}$. Ezek a tapasztalati tények azt sejtetik, hogy ha valamely a, b párra (1) teljesül, akkor $n < 3$.

2. Segéd tételek

Segéd tétel 1. Ha $3 \mid n$, akkor (1)-nek nincs triviálistól különböző megoldása.

Ez Euler tétele. Bizonyítását lásd például a Turán—Gyarmati [13, T. 10.9] jegyzetben.

Segéd tétel 2. Ha $a = 1$ és $n > 1$, akkor (1) nem oldható meg.

Ezt a tételt Nagell [8] bizonyította.

Legyen a d -ed fokú α algebrai szám definiáló polinomja $a_0 x^d + \dots + a_d$. Jelöljük α konjugáltjait $\alpha_1, \dots, \alpha_d$ -vel. Ekkor az α abszolút logaritmikus magasságán a

$$h(\alpha) = \frac{1}{d} \log \left(|a_0| \prod_{i=1}^d \max\{1, |\alpha_i|\} \right)$$

számot értjük. Ezzel a jelöléssel meg tudjuk fogalmazni a következő, Mignotte és Waldschmidtől [7] származó tételt.

Segéd tétel 3. Legyenek α és β egy D -ed fokú \mathbf{K} algebrai számtest elemei $a, b \in \mathbf{Z}, |a|, |b| < B$ és

$$\Lambda = a \log \alpha + b \log \beta.$$

Ha $\Lambda \neq 0$, akkor

$$|\Lambda| \geq \exp(-270D^4 h(\alpha)h(\beta)(7,5 + \log B)^2).$$

Az első lemmában nagyon egyszerű kongruenciameggondolásokat használva szűrjük ki a megoldhatatlan egyenletek jelentős hányadát.

Lemma 1. Legyenek a, b, n és z olyan pozitív egész számok, melyekre $b, n > 1$, $3 \nmid n$, $a < b$, $a + b \leq 16$ és $(a, b) = 1$. Ha $(a, b) \neq (2, 11), (3, 8)$ és $(3, 10)$, akkor (1) nem teljesülhet.

Bizonyítás. Az (1) egyenletet először modulo 9 vizsgáljuk. Felhasználjuk, hogy $\varphi(9) = 6$ és modulo 9 a harmadik hatványmaradékok 0, valamint ± 1 .

Mivel $n > 1$, ezért ha $3 \mid a$ akkor

$$b^n \equiv \pm 1 \pmod{9}$$

következik. Felhasználva, hogy $3 \nmid n$ kapjuk a $b \equiv \pm 1 \pmod{9}$ feltételt. Ezeknek és az $a + b \leq 16$, $(a, b) = 1$ követelményeknek csak az $(a, b) = (3, 8)$ és $(3, 10)$ számpárok felelnek meg.

Amikor a nem osztható 3-mal, akkor négy esetet kell megkülönböztetnünk attól függően, hogy $n \equiv 1, 2, 4$ vagy $5 \pmod{6}$.

Ha $n \equiv 1 \pmod{6}$, akkor (1)-ből $a^n + b^n \equiv a + b \equiv 0, \pm 1 \pmod{9}$. Felhasználva az $0 < a + b \leq 16$ és $1 < a < b$ egyenlőtlenségeket ebből következik, hogy $a + b = 8, 9$ vagy 10 , azaz csak a $(2, 7)$ és $(4, 5)$ párok teljesíthetik a feltételeket.

Hasonlóan vizsgálható a másik három alternatíva is, amely után azt találjuk, hogy a fenti négy eseten kívül még a $(2, 11)$ és $(5, 8)$ párok is, de több nem, kielégítik a kongruenciafeltételeket.

Tegyük fel most, hogy van olyan $(n, x) \in \mathbf{N}^2$, hogy

$$(2) \quad 2^n + 7^n = x^3.$$

Ezt az egyenletet modulo 7 vizsgáljuk. Ha $3 \nmid n$, akkor $2^n \equiv 2$ vagy $4 \pmod{7}$. Másrészt $x^3 \equiv 0, 1, 6 \pmod{7}$ teljesül minden $x \in \mathbf{Z}$ -re, így a (2) egyenletnek nincs megoldása.

A $4^n + 5^n = x^3$ egyenletet modulo 31 vizsgálva azt találjuk, hogy a bal oldal 2, 9 illetve 10-el kongruens modulo 31, amikor $n \equiv 0, 1$ illetve $2 \pmod{3}$. Azonban 9 és 10 nem harmadik hatványmaradék, így $3 \mid n$, ami az 1. Segédétel szerint nem lehetséges.

Végezetül, az $5^n + 8^n = x^3$ egyenlőség teljesüléséből, azt modulo 7 vizsgálva, következik $n \equiv 1 \pmod{6}$, ami miatt $5^n + 8^n \equiv 4 \pmod{9}$.

Mivel az $x^3 \equiv 4 \pmod{9}$ kongruencia nem teljesülhet ez az egyenlet sem oldható meg. A bizonyítást befejeztük.

A következő lépésben még mindig elemi kongruenciamegfontolásokkal szűrünk ki megoldhatatlan egyenleteket.

Lemma 2. Az $(a, b) = (3, 8)$ és $(3, 10)$ párokra az (1) egyenlet nem oldható meg.

Bizonyítás. Először az

$$(3) \quad f_1(n) = 3^n + 8^n = x^3$$

egyenletet vizsgáljuk. Az 1. Segédétel szerint elegendő azzal az esettel foglalkozni, amikor n nem osztható 3-mal. Ha (3) megoldható, akkor megoldható modulo 7 is. Ebből egyszerű számolással következik, hogy $n \equiv 5 \pmod{6}$. Következésképpen n páratlan és így $11 \mid 3^n + 8^n$, ami miatt $11^2 = 121 \mid 3^n + 8^n$.

Legyen $n = 6m + 5$ és

$$3^5 (3^6)^m + 8^5 (8^6)^m \equiv 11x_m \pmod{121},$$

ahol $0 \leq x_m < 11$. Az $\{x_m\}_{m=0}^{\infty}$ sorozat periódikus és periódushossza 11. A sorozat első 13 tagját az 1. táblázatban találja az olvasó.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13
x_m	9	0	7	9	2	8	6	9	4	9	7	5	0	7

1. táblázat

A táblázatból látható, hogy $11 \mid x_m$ akkor és csakis akkor, ha $m \equiv 1 \pmod{11}$. Ebből következik, hogy $121 \mid f_1(n)$ pontosan akkor, ha $n \equiv 11 \pmod{66}$. Könnyen ellenőrizhető, hogy ha $n \equiv 11 \pmod{66}$, akkor

$$f_1(n) \equiv 3^{11} + 8^{11} \equiv -2 \pmod{67}.$$

Másrészt szintén egyszerű számolással ellenőrizhető, hogy -2 nem lehet harmadik hatványmaradék modulo 67. Az utóbbi két tényből következik, hogy a (3) egyenletnek nincs megoldása.

Vizsgáljuk most az

$$(4) \quad f_2(n) = 3^n + 10^n = x^3$$

egyenletet. Gondolatmenetünk hasonló az előző esetben alkalmazotthoz. A (4) egyenletet modulo 7 vizsgálva azt találjuk, hogy $n \equiv 1 \pmod{6}$, tehát ha (4) megoldható, úgy $13 \mid x$.

Legyen $n = 6m + 1$ és

$$3(3^6)^m + 10(10^6)^m \equiv 13x_m \pmod{169},$$

ahol $0 \leq x_m < 13$. Az $\{x_m\}_{m=0}^{\infty}$ sorozat első 14 tagját a 2. táblázatban adtuk meg.

m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
x_m	1	7	0	6	12	5	11	4	10	3	9	2	8	1	7

2. táblázat

Ebből látható, hogy $13 \mid x_m$ pontosan akkor, ha $m \equiv 2 \pmod{13}$. Ezért $13^2 \mid f_2(n)$ pontosan akkor, ha $n \equiv 13 \pmod{78}$. Ha $n \equiv 13 \pmod{78}$, akkor

$$f_2(n) \equiv 25 \pmod{79},$$

azonban 25 nem harmadik hatványmaradék modulo 79, így (4) sem oldható meg.

3. A tétel bizonyítása

Az 1. és 2. Lemma valamint az 1. és 2. Segéd-tétel következtében az a feladatunk maradt csak, hogy belássuk: a

$$(5) \quad 2^n + 11^n = x^3$$

egyenletnek egyetlen megoldása van, mégpedig $(n, x) = (2, 5)$. Mielőtt a bizonyításra rátérnénk megjegyezzük, hogy az 1. és 2. lemmában alkalmazott módszerek (5)-re valószínűleg nem vagy legalábbis csak hosszasan kísérletezés, ügyeskedés után alkalmazhatóak. Használhatóságuk korlátairól szinte kizárólag csak numerikus tapasztalataink vannak. Az alábbiakban ismertető eljárással ugyanakkor mindig meg lehet határozni (1) megoldásait. A módszer hátránya az, hogy komoly elméleti és számítástechnikai apparátus szükséges az alkalmazásához. Ezért konkrét esetben, különösen ha azt sejtjük, hogy a feladatnak nincs megoldása, először érdemes moduláris tesztek végrehajtani és csak azok sikertelensége után bevetni a Baker módszert.

Az 1. Segéd-tételből tudjuk, hogy n nem osztható 3-mal, azaz $n = 3m + r$, ahol $r = 1$ vagy 2 . Legyen $\vartheta = \sqrt{2}$ és $\mathbf{K} = \mathbf{Q}(\sqrt{2})$. Akkor \mathbf{K}

egészeinek gyűrűje \mathbf{R} főideálgyűrű, amelyben $1, \vartheta, \vartheta^2$ egészbazist alkot. A ϑ elem konjugáltjai $\vartheta' = \zeta\vartheta$ és $\vartheta'' = \zeta^2\vartheta$, ahol $\zeta = \frac{-1+i\sqrt{3}}{2}$ egy primitív harmadik egységgyök. Hasonlóképpen, α' és α'' fogja jelölni az $\alpha \in \mathbf{K}$ elem α -tól különböző konjugáltjait. \mathbf{R} -ben csak 1 és -1 az egységgyökök és \mathbf{R} egy alapegysége $\eta = 1 + \vartheta + \vartheta^2$. Ezek az adatok megtalálhatók például Delone és Faddeev [1] könyvében. Egyszerűen kiszámítható a (11) (a 11 által generált ideál) felbontása is \mathbf{R} -ben. Ha $\mathcal{P} = 3 + 2\vartheta + \vartheta^2$ és $\mathcal{Q} = 5 - 4\vartheta + \vartheta^2$, akkor $N(\mathcal{P}) = 11$, $N(\mathcal{Q}) = 11^2$ és $(\mathcal{P}\mathcal{Q}) = (11)$.

Az (5) egyenletből következik, hogy

$$(6) \quad (x - \vartheta^r 2^m)(x - \zeta \vartheta^r 2^m)(x - \zeta^2 \vartheta^r 2^m) = (\mathcal{P}\mathcal{Q})^n.$$

Tekintettel arra, hogy x páratlan és (6) teljesül, ezért \mathbf{R} -ben igazak az alábbiak

$$(x - \vartheta^r 2^m, x^2 + x\vartheta^r 2^m + \vartheta^{2r} 2^{2m}) = (x - \vartheta^r 2^m, 3x\vartheta^r 2^m) = (x - \vartheta^r 2^m, 3) = (1).$$

Mivel $(\mathcal{P}, \mathcal{Q}) = 1$, ezért (6)-ból következik, hogy vannak olyan $u, v \in \mathbf{Z}$, amelyekkel

$$(7) \quad x - \vartheta^r 2^m = \eta^u \mathcal{P}^v$$

vagy

$$(8) \quad x - \vartheta^r 2^m = \eta^u \mathcal{Q}^v.$$

Tekintve (7), illetve (8) konjugáltjait és felhasználva a $\mathcal{P}'\mathcal{P}'' = \mathcal{Q}$ valamint a $\mathcal{Q}'\mathcal{Q}'' = 11\mathcal{P}$ azonosságokat arra a következtetésre jutunk, hogy

$$v = \begin{cases} n & (7)\text{-ben} \\ n/2 & (8)\text{-ban.} \end{cases}$$

Elosztva (7)-et illetve (8)-at ugyanezen egyenletek megfelelő konjugáltjával kapjuk az

$$(9) \quad \left(\frac{\eta}{\eta'}\right)^u \left(\frac{\mathcal{P}}{\mathcal{P}'}\right)^v = \frac{x\vartheta^r 2^m}{x - \vartheta^r \zeta^r 2^m} = 1 + \frac{\vartheta^r - 1}{x - \vartheta^r \zeta^r 2^m} \vartheta^r 2^m,$$

illetve

$$(10) \quad \left(\frac{\eta}{\eta'}\right)^u \left(\frac{\mathcal{Q}}{\mathcal{Q}'}\right)^v = \frac{x\vartheta^r 2^m}{x - \vartheta^r \zeta^r 2^m} = 1 + \frac{\vartheta^r - 1}{x - \vartheta^r \zeta^r 2^m} \vartheta^r 2^m$$

egyenleteket.

Mivel (5) miatt $x \geq \sqrt{1111}^m$, hacsak $m \geq 1$ és így $|x - \vartheta^r \zeta^r 2^m| \geq \sqrt{311}^m$, ezért

$$(11) \quad \left| \frac{\vartheta^r - 1}{x - \vartheta^r \zeta^r 2^m} \vartheta^r 2^m \right| \leq \sqrt{4} \left(\frac{2}{11} \right)^m < \frac{1}{9},$$

ha $m \geq 2$. A logaritmusfüggvény tulajdonságaiból következik, hogy ha az x valós szám olyan, hogy $|x| < 1/3$, akkor $|\log(1+x)| < 1,16|x|$. Ezért (11)-et felhasználva (9) illetve (10)-ből következik, hogy

$$(12) \quad |\Lambda_1| = \left| u \log \left| \frac{\eta}{\eta'} \right| + v \log \left| \frac{\mathcal{P}}{\mathcal{P}'} \right| \right| < 5,5 \left(\frac{2}{11} \right)^m$$

illetve

$$(13) \quad |\Lambda_2| = \left| u \log \left| \frac{\eta}{\eta'} \right| + v \log \left| \frac{\mathcal{Q}}{\mathcal{Q}'} \right| \right| < 5,5 \left(\frac{2}{11} \right)^m.$$

Tekintettel arra, hogy sem $\frac{\mathcal{P}}{\mathcal{P}'}$, sem $\frac{\mathcal{Q}}{\mathcal{Q}'}$ nem egység, ezért $\Lambda_1, \Lambda_2 \neq 0$. Alkalmazható tehát rájuk a 3. Segéd-tétel. Az alsó becslés kiszámításához szükséges paraméterek a következők: $D = 6, B = |v|$,

$$h \left(\left| \frac{\eta}{\eta'} \right| \right) < 3,32, \quad h \left(\left| \frac{\mathcal{P}}{\mathcal{P}'} \right| \right) < 2,51, \quad h \left(\left| \frac{\mathcal{Q}}{\mathcal{Q}'} \right| \right) < 0,44.$$

A 3. Segéd-tétel szerint tehát

$$|\Lambda_1|, |\Lambda_2| \geq \exp(-3 \cdot 10^6 (7,5 + \log |v|)^2).$$

Összehasonlítva ezt a becslést (12) illetve (13)-mal kapjuk, hogy $|v| < 5 \cdot 10^9$, azaz így a legrosszabb esetben is $m < 1,5 \cdot 10^{10}$, azaz $n \leq 4,5 \cdot 10^{10}$.

Az (5) egyenlet helyességének közvetlen ellenőrzése a $0 < n \leq 4,5 \cdot 10^{10}$ intervallumban igen nagy teljesítményű számítástechnikai kapacitást igényel. Közvetett utat kell tehát keresnünk, amit a (12) illetve a (13) egyenlőtlenség biztosít. Ehhez a lánc-törtek egy fontos tulajdonságára kell emlékeztetnünk. Legyen a valós, irracionális α szám lánc-törtelőállítás

$$\alpha = [a_0, a_1, a_2, \dots,]$$

és jelölje p_n, q_n az α n -dik ($n \geq 0$) közelítő törtjének számlálóját illetve nevezőjét. Ekkor teljesül az alábbi (lásd pl. Hua [5], Theorem 10.3.1.)

Lemma 3. Ha $0 < q_{n-1} \leq q < q_n$ és $p \in \mathbf{Z}$, akkor

$$|\alpha q - p| > |\alpha q_n - p_n|.$$

A (12) egyenlőtlenségből következik, hogy

$$\left| v \log \left| \frac{\mathcal{P}}{\mathcal{P}'} \right| / \log \left| \frac{\eta}{\eta'} \right| + u \right| < 2,75 \left(\frac{2}{11} \right)^m.$$

Legyen $\alpha = \log \left| \frac{\mathcal{P}}{\mathcal{P}'} \right| / \log \left| \frac{\eta}{\eta'} \right|$ és határozzuk meg az α lánctörtelőállítását olyan pontossággal, hogy az n -dik közelítő tört nevezője nagyobb legyen, mint $|v|$, ami legfeljebb $5 \cdot 10^9$. Ehhez 23 lánctörtjegyet kell kiszámítanunk, amit az alábbiakban közlünk:

$$\alpha = [0; 1, 6, 3, 1, 4, 1, 7, 1, 3, 1, 3, 2, 2, 1, 1, 110, 2, 3, \dots]$$

A számítást a MAPLE V komputer algebrai rendszerrel végeztük, de tehetjük volna más, hasonló programcsomagokkal is, mint például a PAPI-GP. Könnyen ellenőrizhető a MAPLE V-el, hogy $q_{23} > 5 \cdot 10^9$, így a 3. Lemma állítása szerint

$$2,32 \cdot 10^{-9} < |\alpha q_{23} - p_{23}| < |v\alpha + u| < 2,75 \left(\frac{2}{11} \right)^m.$$

Ebből következik, hogy $m \leq 12$, azaz $v \leq 38$.

A legutolsó gondolatmenetet még egyszer megismételhetjük csak most már a $v \leq 38$ nevezőjű törtre és az n -re vonatkozó korlátot leredukálhatjuk 3-ra, ami ebben az esetben a tétel bizonyítását is jelenti.

A (13) egyenlőtlenség lehetetlensége a fentiekből és a

$$\log \left| \frac{\eta}{\eta'} \right| / \log \left| \frac{\mathcal{Q}}{\mathcal{Q}'} \right| = - \log \left| \frac{\eta}{\eta'} \right| / \log \left| \frac{\mathcal{P}}{\mathcal{P}'} \right|$$

egyenlőtlenségből rögtön következik.

Irodalom

- [1] B. N. DELONE and D. K. FADDEEV, The Theory of Irrationalities of the Third Degree. *Translations of Mathematical Monographs*, Vol. 10, AMS, 1964.

- [2] I. GAÁL, A. PETHŐ and M. POHST, On the resolution of index form equations corresponding to biquadratic number fields II., *J. Number Theory*, **38** (1991), 35–51.
- [3] I. GAÁL, A. PETHŐ and M. POHST, On the resolution of index form equations corresponding to biquadratic number fields III., *J. Number Theory*, megjelenés alatt.
- [4] I. GAÁL and N. SCHULTE, Computing all power integral bases of cubic number fields, *Math. Comp.*, **53** (1989), 689–696.
- [5] HUA LOO KENG, Introduction to Number Theory, *Springer-Verlag*, 1982.
- [6] M. MIGNOTTE, Su una classe di equazioni del tipo $a^n + b^n = z^2$, *Rend. del Sem. Univ. Cagliari*, **62** (1992), fasc. 1.
- [7] M. MIGNOTTE and M. WALDSCHMIDT, Linear forms in two logarithms and Schneider's method III., *Annales Fac. Sci. Toulouse*, 1990, 43–75.
- [8] T. NAGELL, Des équations indéterminées $x^2 + x + 1 = y^n$ et $x^2 + x + 1 = 3y^n$, *Norsk. Mat. Forenings Skr.* (1) **2** (1921), 14.
- [9] A. PETHŐ, Perfect powers in second order linear recurrences, *J. Number Theory*, **15** (1983), 117–127.
- [10] A. PETHŐ und R. SCHULENBERG, Effektives Lösen von Thue Gleichungen. *Publ. Math. Debrecen*, **34** (1987), 189–196.
- [11] A. PETHŐ, Über kubische Ausnahmeeinheiten. *Arch. Math.*, **60** (1993), 146–153.
- [12] T. N. SHOREY and C. L. STEWART, On the Diophantine equation $ax^{2t} + bx^t y + cy^2 = d$ and pure powers in recurrences. *Math. Scand.*, **52** (1983), 24–36.
- [13] TURÁN PÁL és GYARMATI EDIT: Számelmélet. (8. utánnomás), *Tankönyvkiadó*, Budapest, 1970.
- [14] N. TZANAKIS and B. M. M. DE WEGER, On the practical solution of the Thue–Mahler equation. In: *Computational Number Theory* Eds.: A. Pethő, M. E. Pohst, H. C. Williams and H. G. Zimmer, *Walter de Gruyter*, 1991, 289–294.
- [15] B. M. M. DE WEGER, Algorithms for Diophantine Equations, *CWI Tract 65, Centre for Math. and Comp. Sci. Amsterdam*, 1989.

A taszító fixpontokról

SZEPESSY BÁLINT

Abstract. (On the repelling fixpoints) If the iterative pointsequence x_0, x_1, x_2, \dots has the limit value c then c , is said to be a fixpoint of first order and the points x_0, x_1, x_2, \dots belong to the point c . A fixpoint c is called to be a repelling point if it has no belonging point except c and its inverse iterated points.

In this paper we prove that repelling fixpoints of first (or higher) order can make a segment in a given closed interval.

1. Bevezetés

Legyen $f(x)$ az $[a, b]$ ($a < b$) zárt intervallumon értelmezett olyan egyértékű valós függvény, amely eleget tesz a következő feltételeknek:

1. $f(x)$ az adott szakasz minden belső pontjában folytonos; a kezdő és végpontban jobbról, illetve balról folytonos;
2. $f(x)$ az $[a, b]$ intervallumot önmagára képezi le;
3. nincs olyan részintervalluma az adott szakasznak, amelyben $f(x) = \text{konstans}$ teljesül.

Az $f(x)$ függvényt iterációs alapfüggvénynek nevezzük az adott intervallumon. Az $f_0(x) = x$, $f_1(x) = f(x)$, $f_2(x) = f(f(x))$, \dots , $f_n(x) = f(f_{n-1}(x))$, \dots függvényeket az $f(x)$ függvény 0-dik, első, második, \dots , n -edik (n -edrendű), \dots iterált függvényeinek (iteráltjainak) nevezzük.

Az $f_n(x)$ ($n = 2, 3 \dots$) függvények is mind rendelkeznek az 1., 2., 3 tulajdonságokkal. (Ezt a közvetett függvény folytonosságára vonatkozó tételekből teljes indukcióval könnyen bizonyíthatjuk.) Teljesülnek az $f_{n+m}(x) = f_n(f_m(x)) = f_m(f_n(x))$ azonosságok is. Ezért bármely $x_0 (\in [a, b])$ pontnak létezik az $x_{n+1} = f(x_n)$ képlettel alkotott $x_0, x_1, x_2, \dots, x_n, \dots$ iterációs pontsorozata és minden n -re $x_n \in [a, b]$ -nek. Az x_n pontot az x_0 pont n -edrendű (n -edik) iteráltjának vagy rákövetkezőjének mondjuk.

Ha $f(c) = c$, akkor a c pontot az $f(x)$ függvény elsőrendű fixpontjának nevezzük. Ha $f_n(c) \neq c$, $n = 1, 2, 3 \dots, r - 1$ esetén, de $f_r(c) = c$, akkor c az $f(x)$ függvény r -edrendű fixpontja. Ekkor a $c_1, c_2, \dots, c_{r-1}, c_r$ pontok is páronként különböző r -edrendű fixpontok [2].

Ha az x_0 pont iterációs pontsorozatának c a határértéke, akkor c elsőrendű fixpont és azt mondjuk, hogy x_0 pont a c ponthoz tartozik.

A c elsőrendű fixpont vonzó, ha létezik olyan pozitív ε valós szám, hogy bármely $x \in (c - \varepsilon, c + \varepsilon)$ esetén x a c ponthoz tartozik. A c elsőrendű fixpont balról-vonzó, ha nem vonzó, de létezik olyan pozitív ε valós szám, hogy minden $x \in (c - \varepsilon, c)$ esetén x a c ponthoz tartozik. Hasonlóképpen értelmezzük a jobbról-vonzó elsőrendű fixpontokat. Ezeket közös néven félig-vonzó fixpontoknak nevezzük.

Taszító egy elsőrendű fixpont, ha saját magán és megelőzőin (inverz-iteráltjain) kívül nincs más hozzátartozó pont. Az olyan elsőrendű fixpontokat, amelyek nem sorolhatók az előbbi csoportok egyikébe sem, vegyes fixpontoknak nevezzük [3].

A magasabb rendű fixpontok értelmezéséből következik, hogy az $f(x)$ függvény r -edrendű fixpontja az $f_r(x)$ függvénynek az elsőrendű fixpontja. Így $f(x)$ függvény r -edrendű fixpontja vonzó, félig vonzó, taszító vagy vegyes aszerint, hogy az $f(x)$ függvény c elsőrendű fixpontja mely típusba tartozik. Ekkor a $c_1, c_2, \dots, c_r = c$ páronként különböző r -edrendű fixpontok mind azonos típusúak.

2. A taszító fixpontokról

A [8] azt a kérdést vizsgálta, hogy milyen iterációs alapfüggvények esetén vannak tetszőleges magasrendű fixpontok. Bebizonyítottuk a következő állítást:

Legyen $f(x)$ az $[a, b]$ zárt intervallumon értelmezett iterációs alapfüggvény, legyen továbbá $[c, d]$ részszakasza az $[a, b]$ szakasznak. Ha van a $[c, d]$ szakaszban két olyan diszjunkt részszakasz, amelyeket a függvény az egész $[c, d]$ szakaszra képezi le, akkor az $f(x)$ függvénynek van tetszőleges magasrendű fixpontja.

A tétel feltételei mellett a $[c, d]$ szakaszban vannak bármilyen (első, másod, ...) rendű fixpontok.

Ugyanilyen tulajdonsággal rendelkező szakaszok lépnek fel $[a, b]$ -ben a [7]-ben bizonyított tétel szerint is.

Felmerült a kérdés, hogy lehetnek-e — és milyen feltételek mellett — csupa azonos rendszámú fixpontokból álló szakaszok.

Azt fogjuk vizsgálni, hogy az első és magasabb rendű taszító fixpontok alkothatnak-e szakaszt az $[a, b]$ intervallumon.

Először bebizonyítjuk a következő állítást.

Tétel. Ha a $[c, d]$ ($c < d, c, d \in [a, b]$) szakaszt a benne monoton növekvő iterációs alapfüggvény önmagára vagy önmagába képezi le, akkor a $[c, d]$ szakaszban csak elsőrendű fixpontok vannak.

Bizonyítás. Tegyük fel állításunkkal ellentétben, hogy van a $[c, d]$ szakaszban n -edrendű fixpont ($n \geq 2$); legyen ez c . Ekkor $c, c_1, c_2, c_3, \dots, c_{n-1}$

pontok is páronként különböző n -edrendű fixpontok; ahol $f(c_{n-1}) = c_n = c$.

Feltehető, hogy c a legkisebb abszcisszájú fixpont ebben a sorozatban, azaz $c < c_1, c_2, \dots, c_{n-1}$ (c_1, c_2, \dots, c_{n-1} fixpontok sorrendje nem feltétlenül nagyság szerinti).

A $c < c_{n-1}$ egyenlőtlenségből $f(x)$ monoton növekedése miatt $f(c) < f(c_{n-1})$ következik. De $f(c) = c_1$ és $f(c_{n-1}) = c$, ezért $c_1 < c$ azzal ellentétben, hogy c a legkisebb abszcisszájú fixpont a sorozatban.

Nem lehet tehát $n \geq 2$.

A $[c, d]$ szakaszban mindig van legalább egy elsőrendű fixpont. Az egész szakaszon ugyanis $f(x) - x > 0$ ($f(x) - x < 0$) nem teljesülhet, mert $f(x) - x > 0$ ($f(x) - x < 0$) esetén $f(x)$ nem képezi le a $[c, d]$ szakaszt önmagára vagy önmagába.

A $[c, d]$ szakaszban akár végtelen sok elsőrendű fixpont is lehet. Ebben az esetben ezek torlódási pontjai is elsőrendű fixpontok.

Ha ugyanis $A_1, A_2, \dots, A_n, \dots$ elsőrendű fixpontok $[c, d]$ -ben és torlódási pontjuk A , akkor

$$\begin{aligned} A &= \lim_{n \rightarrow \infty} A_{n_i} \quad \text{és} \quad f(A_{n_i}) = A_{n_i}, \quad \text{így} \quad A = \lim_{n \rightarrow \infty} A_{n_i} = \\ &= \lim_{n \rightarrow \infty} f(A_{n_i}) = f\left(\lim_{n \rightarrow \infty} A_{n_i}\right) = f(A), \end{aligned}$$

ezért A is elsőrendű fixpont. Az is előfordulhat, hogy a $[c, d]$ szakasz csupa elsőrendű taszító fixpontból áll. Ilyenkor $f(x) = x$ az egész $[c, d]$ intervallumon.

Tehát az $[a, b]$ intervallumon az elsőrendű taszító fixpontok szakaszt alkothatnak.

Tétel. Ha valamely $[c, d]$, ($c < d, c, d \in [a, b]$) szakaszt a benne monoton csökkenő iterációs alapfüggvény önmagára vagy önmagába képezi le, akkor ebben a szakaszban csak első és másodrendű fixpontok vannak.

Bizonyítás. Mivel a $[c, d]$ szakaszban monoton csökkenő függvényre $f(c) \geq f(x) \geq f(d)$ egyenlőtlenségek teljesülnek és így $f(x) - x$ és c helyen pozitív a d helyen negatív értékű, s így $f(x)$ folytonossága által van egy megoldása az $f(x) - x = 0$ egyenletnek a $[c, d]$ szakaszban, ezért a tétel bizonyítása visszavezethető az előbbi tétel bizonyítására.

Monoton csökkenő függvény monoton csökkenő függvénye (iteráltja) ugyanis monoton növekvő, ezért $f_2(x)$ függvény a $[c, d]$ szakaszt önmagára, vagy önmagába leképező monoton növekvő függvény. Erre mint alapfüggvényre alkalmazva az előbbi tételt adódik, hogy az $f_2(x)$ függvénynek csak elsőrendű fixpontjai vannak a $[c, d]$ szakaszban, s ezek az egyetlen elsőrendű fixpont kivételével mind másodrendű fixpontjai az $f(x)$ függvénynek.

Például az $f(x) = -(x-1)^3 + 1$ iterációs alapfüggvényre a $[0, 2]$ szakaszban a tétel feltételei teljesülnek. Az $x_1 = 0$ és $x_2 = 2$ pontok másodrendű fixpontok, ennél magasabb rendű fixpontok ebben a szakaszban nem lépnek fel.

Csupa másodrendű taszító fixpontból álló szakaszok is felléphetnek. Például az $f(x) = 1 - x$ alapfüggvény esetén a $[0, 1]$ intervallumban. Itt $e = \frac{1}{2}$ pont kivételével a szakasz minden pontja másodrendű taszító fixpont.

Az $f(x) = \frac{1}{x}$ függvény az $[a, \frac{1}{a}]$ ($0 < a < 1$) szakaszban szintén kielégíti a tétel feltételeit; a szakasz minden pontja az $e = 1$ elsőrendű fixpont kivételével másodrendű taszító fixpontok.

Általánosabban; ha az $y = f(x)$ görbe az $y = x$ egyenesre vonatkozóan tükörképíveket tartalmaz, akkor ezek mindig másodrendű taszító fixpontból álló szakaszok.

Könnyen belátható a következő:

Tétel. Az $[a, b]$ intervallum tetszőleges n számú páronként diszjunkt zárt szakaszához megadható (akár végtelen sok) olyan iterációs alapfüggvény, amelyre az adott zárt szakaszok pontjai mind n -edrendű taszító fixpontok.

Bizonyítás. Legyen $[a, b]$ szakasznak $\varrho; \varrho_1; \varrho_2; \dots, \varrho_{n-1}$ páronként diszjunkt zárt részintervallumai. Az $f(x)$ iterációs alapfüggvényt az $[a, b]$ szakaszon értelmezzük úgy, hogy a ϱ_{i-1} szakaszt a ϱ_i -re ($i = 1, 2, \dots, n-1; \varrho_0 = \varrho$) bijektív módon képezze le, továbbá ha d a ϱ zárt szakasz egy tetszőleges pontja, akkor $d_{i-1} \in \varrho_{i-1}$ ($i = 1, 2, \dots, n-1; d_i$ a d pont i -edik iteráltja) és $(d_{n-1}, f(d_{n-1}) = d)$ az alapfüggvény pontja (Az $x = d_{n-1}$ és az $y = d$ egyenesek metszéspontja a $(d_{n-1}, f(d_{n-1}) = d)$ pont).

Nyilvánvaló, hogy végtelen sok ilyen iterációs alapfüggvény létezik, s hogy ezekre az adott részintervallumok pontjai mind n -edrendű taszító fixpontok.

Például az $[\frac{1}{4}, \frac{1}{3}]$ szakaszt az $[\frac{5}{6}, \frac{8}{9}]$ szakaszra, az utóbbit az $[\frac{5}{12}, \frac{1}{2}]$ szakaszra, ezt pedig $[\frac{17}{18}, 1]$ zárt szakaszra bijektív módon képezi le a $[0, 1]$ szakaszon értelmezett

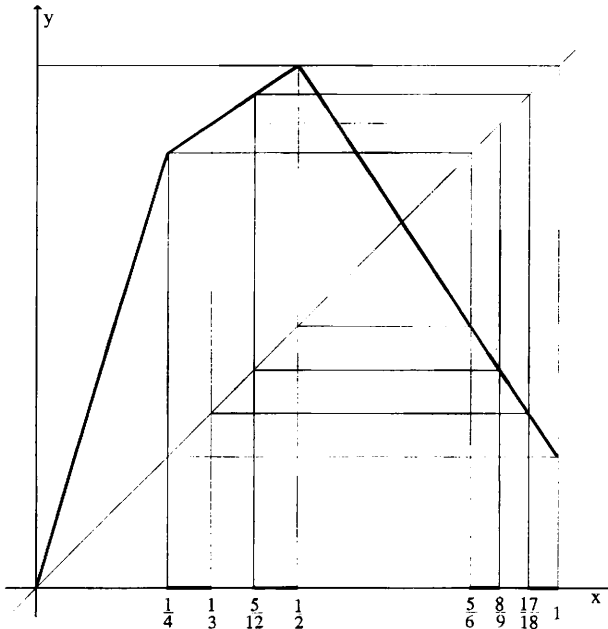
$$f(x) = \begin{cases} \frac{10}{3}x, & \text{ha } 0 \leq x \leq \frac{1}{4}, \\ \frac{2}{3}(x+1), & \text{ha } \frac{1}{4} < x \leq \frac{1}{2}, \\ -\frac{3}{2}x + \frac{7}{4}, & \text{ha } \frac{1}{2} < x \leq 1 \end{cases}$$

iterációs alapfüggvény. Továbbá erre az alapfüggvényre bármely $d \in [\frac{1}{4}; \frac{1}{2}]$ esetén d_3 iterált pontban a függvényérték d . Ezért az $[\frac{1}{4}, \frac{1}{3}]$, $[\frac{5}{6}, \frac{8}{9}]$, $[\frac{5}{12}, \frac{1}{2}]$ és a $[\frac{17}{18}, 1]$ szakaszok pontjai mind negyedrendű taszító fixpontok (lásd az ábrát).

Tehát az első és a magasabb rendű taszító fixpontok zárt intervallumokat alkothatnak az $[a, b]$ szakaszon.

Végül tekintsük az $f(x) = -4(x - \frac{1}{2})^2 + 1$ iterációs alapfüggvényt a $[0, 1]$ intervallumon. Az $x_1 = 0$ és az $x_2 = \frac{3}{4}$ pontok elsőrendű taszító fixpontok. Itt megszámlálható sok magasabb rendű taszító fixpont van a $[0, 1]$ szakaszon, (2 másod, 6 harmad, 8 negyedrendű, ...). Tehát a fixpontok (az n -edrendű fixpontok) halmaza nem alkot szakaszt.

Az $f_n(x) - x = 0$ egyenletnek az $f_n(x)$ iterált függvény két egymásra következő 0-helye által határolt zárt szakaszban két-két gyöke van, ezért a gyökök, vagyis a magasabb rendű taszító fixpontok mindenütt sűrűn helyezkednek el; ezért a $[0, 1]$ szakasz minden pontja taszító fixpontok torlódási pontja.



Irodalom

- [1] A. RALSTON, A first course in numerical analysis. *Mc Graw-Hill, Inc.*, New York, 1969.
- [2] B. BARNA, Über die Iteration reeller Funktionen I., *Publ. Math. Debrecen*, **7** (1960), 16–47.
- [3] B. BARNA, Über die Iteration reeller Funktionen II., *Publ. Math. Debrecen*, **13** (1966), 16–47.
- [4] B. BARNA, Berichtigung zur Arbeit, Über die Iterationen reeller Funktionen II., *Publ. Math. Debrecen*, **20** (1973), 281–282.
- [5] B. BARNA, Über die Iteration reeller Funktionen III., *Publ. Math. Debrecen*, **22** (1979), 267–278.
- [6] L. BERG (Rostock), Über irreguläre Iteratione folgen, *Publ. Math., Debrecen*, **17** (1971), 112–115.
- [7] TIEN—YIEN LI and L. JAMES A. YORKE, Period three implies chaos. *Amer. Math. Monthly* (10) **82** (1975), 985–992.
- [8] SZEPESSY BÁLINT: A magasabb rendű fixpontokról. *Acta Academiae Paedagogicae Agriensis, Sectio mathematicae* XII. (1994), 9–15.

Note on Abel's result about roots of polynomials

DARIUSZ FREJMAN

Abstract. In this Note we give an algebraic proof of the well-know Abel's result about roots of polynomials. Our proof is other than the proof given by M. S. Grosf and G. Taiani in the paper [3].

A theorem of Abel [2] states: if $P(x)$, $Q(x)$ are any polynomials such that $\deg Q = n \geq 3$, $Q(x)$ has no multiple roots and $\deg P = m \leq n - 2$, then

$$(1) \quad \sum_{i=1}^n \frac{P(r_i)}{Q'(r_i)} = 0,$$

where r_i 's are distinct roots of $Q(x)$ and $Q'(x)$ denotes the derivate of $Q(x)$.

We remark that the original proof by Abel uses integrals. The modern proof can be based on residue theory. In the paper [3] given by M. S. Grosf and G. Taiani has been presented an algebraic proof of (1) in spirit of classical theory of equations by using some property of the Vandermonde's determinant. The purpose of this note is to present also algebraic proof of (1) by different method. Nemely, we prove the following:

Theorem. Let $F(x) = \sum_{k=0}^{\infty} a_k x^{m_k}$, where $0 \leq m_k \leq n - 2$ and $Q(x)$ be the polynomial of the degree $n \geq 3$, such that $Q(x)$ has no multiple roots. Then

$$(2) \quad \sum_{i=1}^n \frac{F(r_i)}{Q'(r_i)} = 0,$$

where r_i 's are distinct roots of $Q(x)$ and $Q'(x)$ denotes the derivate of $Q(x)$.

Proof. In the proof of (2) we use of the following result (see [1], p. 87 and solution on p. 220). If $Q(x)$ has no multiple roots and $\deg Q(x) = n \geq 3$, then for every natural fixed s , such that $0 \leq s \leq n - 2$, we have;

$$(3) \quad \sum_{i=1}^n \frac{r_i^s}{Q'(r_i)} = 0,$$

where r_i 's are distinct roots of $Q(x)$.

The proof of (3) easily follows by an algebraic method.

Since $F(x) = \sum_{k=0}^{\infty} a_k x^{m_k}$, and $0 \leq m_k \leq n - 2$, then

$$(4) \quad \sum_{i=1}^n \frac{F(r_i)}{Q'(r_i)} = \sum_{i=1}^n \frac{1}{Q'(r_i)} \sum_{k=0}^{\infty} a_k r_i^{m_k}.$$

From (4) we obtain

$$(5) \quad \sum_{i=1}^n \frac{F(r_i)}{Q'(r_i)} = a_0 \sum_{i=1}^n \frac{r_i^{m_0}}{Q'(r_i)} + a_1 \sum_{i=1}^n \frac{r_i^{m_1}}{Q'(r_i)} + \cdots + a_k \sum_{i=1}^n \frac{r_i^{m_k}}{Q'(r_i)} + \cdots$$

Since $0 \leq m_k \leq n - 2$ then by (3) and (5) we obtain

$$\sum_{i=1}^n \frac{F(r_i)}{Q'(r_i)} = 0,$$

and the proof of the Theorem is complete.

Remark. Putting $m_k = m - k$, $k = 0, 1, \dots, m$; we have

$$F(x) = \sum_{k=0}^m a_k x^{m_k} = \sum_{k=0}^m a_k x^{m-k} = P(x),$$

where $\deg P(x) = m \leq n - 2$, and we obtain (1).

Rereferences

- [1] D. K. FADDIEĬEV and I. S. SOMINSKIĬ, Collection of the problems in higher algebra, Moskov, 1964 (in Russian).
- [2] P. GRIFFITHS, "Variations on a theorem of Abel", *Invent. Math.* **35** (1976), 321–390.
- [3] M. S. GROSOFF and G. TAIANI, "Vandermonde strikes again", *Amer. Math. Monthly*, 1993, 575–577.

The Lie augmentation terminals of groups*

BERTALAN KIRÁLY

Abstract. In this paper we give necessary and sufficient conditions for groups which have finite Lie terminals with respect to commutative ring of characteristic p^s where p is a prime and s is a natural number.

1. Introduction. Let R be a commutative ring with identity, G a group and RG its group ring and let $A(RG)$ denote the *augmentation ideal* of RG , that is the kernel of the ring homomorphism $\phi : RG \rightarrow R$ which maps the group elements to 1. It is easy to see that as R -module $A(RG)$ is a free module with the elements $g - 1$ ($g \in G$) as a basis. It is clear that $A(RG)$ is the ideal generated by all elements of the form $g - 1, g \in G$.

The Lie powers $A^{[\lambda]}(RG)$ of $A(RG)$ are defined inductively: $A(RG) = A^{[1]}(RG)$, $A^{[\lambda+1]}(RG) = [A^{[\lambda]}(RG), A(RG)] \cdot RG$, if λ is not a limit ordinal, and $A^{[\lambda]}(RG) = \bigcap_{\nu < \lambda} A^{[\nu]}(RG)$ otherwise, where $[K, M]$ denote the R -submodule of RG generated by $[k, m] = km - mk, k \in K, m \in M$, and for $K \subseteq RG, K \cdot RG$ denotes the right ideal generated by K in RG (similary $RG \cdot K$ will denote the left ideal generated by K). It is easy to see that the right ideal $A^{[\lambda]}(RG)$ is a two-sided ideal of RG for all ordinals $\lambda \geq 1$.

Evidently there exists a least ordinal $\tau = \tau_R[G]$ such that $A^{[\tau]}(RG) = A^{[\tau+1]}(RG)$ which is called the *Lie augmentation terminal* (or *Lie terminal* for simple when it is obvious from the context what ring R we are working with) of G with respect to R . If $G = \langle 1 \rangle$ we put $\tau_R[G] = 1$.

In general, the question of the classification of groups in regarding to values of the Lie terminals and also of the computation of these terminals, is far from being simple.

We are primarily concerned with finding all groups whose the Lie terminals with respect to commutative ring of characteristic p^s are finite.

In this paper we give necessary and sufficient conditions for groups which have finite Lie terminals with respect to commutative ring of characteristic p^s where p is a prime and s is a natural number (Theorem 3.1).

* Research supported by the Hungarian National Foundation for Scientific Research Grant, N^oT 4265 and N^oT 16432.

2. Notations and some known facts. If H is a normal subgroup of G , then $I(RH)$ (or $I(H)$ for short when it is obvious from the context what ring R we are working with) denotes the ideal of RG generated by all elements of the form $h - 1$, ($h \in H$). It is well known that $I(RH)$ is the kernel of the natural epimorphism $\bar{\phi} : RG \rightarrow RG/H$ induced by the group homomorphism ϕ of G onto G/H . It is clear that $I(RG) = A(RG)$.

Let F be a free group on the free generators x_i ($i \in I$), say, and ZF be its integral group ring (Z denotes the ring of rational integers). Then every homomorphism $\phi : F \rightarrow G$ induces a ring homomorphism $\bar{\phi} : ZF \rightarrow RG$ by letting $\bar{\phi}(\sum n_y y) = \sum n_y \phi(y)$, where $y \in F$ and the sum runs over the finite set of $n_y y \in ZF$. If $f \in ZF$, we denote by $A_f(RG)$ the two-sided ideal of RG generated by the elements $\bar{\phi}(f)$, $\phi \in \text{Hom}(F, G)$, the set of homomorphism from F to G . In other words $A_f(RG)$ is the ideal generated by the values of f in RG as the elements of G are substituted for the free generators x_i -s.

An ideal J of RG is called a *polynomial ideal* if $J = A_f(RG)$ for some $f \in ZF$, F a free group.

It is easy to see that the augmentation ideal $A(RG)$ is a polynomial ideal. Really, $A(RG)$ is generated as an R -module by the elements $g - 1$ ($g \in G$), i.e. by the values of the polynomial $x - 1$.

From [3] (see also [2], Corollary 1.9, page 6) it follows the

Lemma 2.1. ([2]) *The Lie powers $A^{[n]}(RG)$, $n \geq 1$, are polynomial ideals in RG .*

We use also the following

Lemma 2.2. ([2] Proposition 1.4, page 2) *Let $f \in ZF$. Then f defines a polynomial ideal $A_f(RG)$ in every group ring RG . Further, if $\theta : RG \rightarrow KH$ is a ring homomorphism induced by a group homomorphism $\phi : G \rightarrow H$ and a ring homomorphism $\psi : R \rightarrow K$, then*

$$\theta(A_f(RG)) \subseteq A_f(KH).$$

(It is assumed here that $\psi(1_R) = 1_K$, where 1_R and 1_K are identity of the rings R and K respectively.)

Let $\bar{\phi} : RG \rightarrow RG/L$ be a natural epimorphism induced by the group homomorphism ϕ of G onto G/L . By Lemma 2.1 $A^{[n]}(RG)$ ($n \geq 1$) are polynomial ideal and from Lemma 2.2 it follows that

$$\bar{\phi}(A^{[n]}(RG)) = A^{[n]}(RG/L). \quad (1)$$

Consequently

$$A^{[n]}(RG/L) \cong (A^{[n]}(RG) + I(RL))/I(RL) \tag{2}$$

for all $n \geq 1$.

If \mathcal{K} denotes a class of groups (by which we understand that \mathcal{K} contains all groups of order 1 and, with each $H \in \mathcal{K}$, all isomorphic copies of H) we define the class \mathbf{RK} of residually- \mathcal{K} groups by letting $G \in \mathbf{RK}$ if and only if: whenever $1 \neq g \in G$, there exists a normal subgroup H_g of the group G such that $G/H_g \in \mathcal{K}$ and $g \notin H_g$.

We use the following notations for standard group classes: \mathcal{D} : nilpotent groups whose derived groups are torsion-free nilpotent groups and \mathcal{D}_p : nilpotent groups whose derived groups are p -groups of finite exponent.

Let p be a prime and n a natural number. Then we shall denote by G^{p^n} the subgroup generated by all elements of the form $g^{p^n}, g \in G$.

If K, L are two subgroups of G , then we shall denote by (K, L) the subgroup generated by all commutators $(g, h) = g^{-1}h^{-1}gh, g \in K, h \in L$.

The n th term of the lower central series of G is defined inductively: $\gamma_1(G) = G, \gamma_2(G) = G'$ is the commutator subgroup (G, G) of G , and $\gamma_n(G) = (\gamma_{n-1}(G), G)$.

In this paper we shall use also the following theorems:

Theorem 2.1. ([1]) *Let G be a non-Abelian group, R a commutative ring with identity. Then $A^{[n]}(RG) = 0$ for some $n \geq 2$ if and only if G is nilpotent, G' is a finite p -group and p is nilpotent in R .*

The ideal $J_p(R)$ of a ring R is defined by $J_p(R) = \bigcap_{n=1}^{\infty} p^n R$.

Theorem 2.2. ([2], Theorem 2.13, page 85) *Let G be a residually \mathcal{D}_p -group and $J_p(R) = 0$, then $A^{[\omega]}(RG) = 0$.*

We shall use the following lemma, which gives some elementary properties of the Lie powers $A^{[n]}(RG)$ of $A(RG)$.

Lemma 2.3. ([2], Proposition 1.7, page 4) *For an arbitrary natural numbers n and m are true:*

- 1) $I(\gamma_n(G)) \subseteq A^{[n]}(RG)$
- 2) $[A^{[n]}(RG), A^{[m]}(RG)] \subseteq A^{[n+m]}(RG)$
- 3) $A^{[n]}(RG) \cdot A^{[m]}(RG) \subseteq A^{[n+m-1]}(RG)$.

3. The Lie augmentation terminals. *Throughout this section R will denote a commutative ring with identity of characteristic p^s .*

The normal subgroups $G_{p,k}$ is defined by

$$G_{p,k} = \bigcap_{n=1}^{\infty} (G')^{p^n} \gamma_k(G),$$

where $\gamma_k(G)$ is the k th term of the lower central series of G and G' is the commutator subgroup of G . It is clear, that the factor-group $G/G_{p,k}$ is a residually- \mathcal{D}_p group for every k . We have the following sequence

$$G = G_{p,1} \supseteq G_{p,2} \supseteq \dots \supseteq G_p \quad (3)$$

of normal subgroups $G_{p,k}$ of a group G , where $G_p = \bigcap_{k=1}^{\infty} G_{p,k}$.

Lemma 3.1. *Let R be a commutative ring of characteristic p^s . Then $I(G_{p,k}) \subseteq A^{[k]}(RG)$ for all $k \geq 1$.*

Proof. Let the element $h - 1$ be in $I(G_{p,k})$. It will be sufficient to show that $h - 1 \in A^{[k]}(RG)$. For an arbitrary n written the element h as $h = h_1^{p^n} h_2^{p^n} \dots h_m^{p^n} y_k$ ($h_i \in G', y_k \in \gamma_k(G)$) and using the identity

$$ab - 1 = (a - 1)(b - 1) + (a - 1) + (b - 1) \quad (4)$$

we have that

$$h - 1 = (h_1^{p^n} h_2^{p^n} \dots h_m^{p^n} y_k - 1)(y_k - 1) + (h_1^{p^n} h_2^{p^n} \dots h_m^{p^n} - 1) + (y_k - 1).$$

By Lemma 2.3, $I(\gamma_k(G)) \subseteq A^{[k]}(RG)$ and hence $y_k - 1 \in A^{[k]}(RG)$. Therefore

$$h - 1 \equiv (h_1^{p^n} h_2^{p^n} \dots h_m^{p^n} - 1) \pmod{A^{[k]}(RG)}.$$

Applying (4) repeatedly to $(h_1^{p^n} h_2^{p^n} \dots h_m^{p^n} - 1)$ from the previous expression it follows that

$$h - 1 \equiv \sum_{i=1}^m (h_i^{p^n} - 1) b_i \equiv \sum_{i=1}^m \sum_{j=1}^{p^n} \binom{p^n}{j} (h_i - 1)^j b_i \pmod{A^{[k]}(RG)},$$

where $b_i \in RG$. From Lemma 2.3 (cases 1 and 3) we obtain, that the element $(h_i - 1)^j$ lie in $A^{[j+1]}(RG)$ for every i and j . If $n \geq s + k$, then p^s divides $\binom{p^n}{j}$ for $j = 1, 2, \dots, k - 1$. Therefore

$$h - 1 \equiv \sum_{i=1}^m (h_i^{p^n} - 1) b_i \equiv p^s \sum_{i=1}^m \sum_{j=1}^{k-1} d_j (h_i - 1)^j b_i \equiv p^s F_k(h) \pmod{A^{[k]}(RG)},$$

where $F_k(h) = \sum_{i=1}^m \sum_{j=1}^{k-1} d_j (h_i - 1)^j b_i$ and $p^s d_j = \binom{p^n}{j}$. Since p^s is zero in R we have that $h - 1 \in A^{[k]}(RG)$ which implies the inclusion $I(G_{p,k}) \subseteq A^{[k]}(RG)$ and completes the proof of the lemma.

Lemma 3.2. *Let R be a commutative ring of characteristic p^s . Then*

$$A^{[\omega]}(RG) = I(G_p).$$

Proof. From (3) and from Lemma 3.1 the inclusion $I(G_p) \subseteq A^{[\omega]}(RG)$ follows. We can readily verify that G/G_p is the residually- \mathcal{D}_p group and by Theorem 2.2

$$A^{[\omega]}(RG/G_p) = 0. \tag{5}$$

By (1) $\bar{\phi}(A^{[n]}(RG)) = A^{[n]}(RG/G_p)$ for all $n \geq 1$, where $\bar{\phi} : RG \rightarrow RG/G_p$ the natural epimorphism induced by the group homomorphism ϕ of G onto G/G_p . Consequently $\bar{\phi}(A^{[\omega]}(RG)) \subseteq A^{[n]}(RG/G_p)$ for all n and therefore $\bar{\phi}(A^{[\omega]}(RG)) \subseteq A^{[\omega]}(RG/G_p)$. Then from the isomorphism $RG/G_p \cong RG/I(G_p)$ and from (5) we conclude that $A^{[\omega]}(RG) \subseteq I(G_p)$. Therefore $A^{[\omega]}(RG) = I(G_p)$. This completes the proof of the lemma.

If G is a nilpotent group with a finite p -group as the commutator subgroup and R a commutative ring of characteristic p^s then the ideal $A(RG)$ is Lie nilpotent (see Theorem 2.1). Denote $\tau^\circ[A(RG)]$ the Lie nilpotency index of $A(RG)$ i.e. the natural number n for which $A^{[n-1]}(RG) \neq A^{[n]}(RG) = 0$ holds. If $G = \langle 1 \rangle$ we put $\tau^\circ[A(RG)] = 1$.

Let $\tau_p[G]$ denote the smallest natural number k (if it exists) such that $G_{p,k-1} \neq G_{p,k} = \dots = G_p$.

Theorem 3.1. *Let R be a commutative ring of characteristic p^s . Then:*

- 1) $\tau_R[G] = 1$ if and only if $G = G_p$,
- 2) $\tau_R[G] = 2$ if and only if $G \neq G' = G_p$,
- 3) $\tau_R[G] > 2$ if and only if G/G_p is a nilpotent group whose derived group is a finite p -group.

Proof. The statement 1) follows from Lemma 3.2.

2) Let $\tau_R[G] = 2$, i.e.

$$A(RG) \neq A^{[2]}(RG) = A^{[3]}(RG) = \dots = A^{[\omega]}(RG).$$

By statement 1) of our theorem $G_p \neq G$ and consequently $G \neq G'$. Because G/G' is an Abelian group, $A^{[2]}(RG/G') = 0$. From the isomorphism

$$A^{[2]}(RG/G') \cong (A^{[2]}(RG) + I(G'))/I(G'),$$

which follows from (2), we conclude that $A^{[2]}(RG) \subseteq I(G')$. By Lemma 2.3 we obtain the inclusion $A^{[2]}(RG) \supseteq I(G')$. Consequently $A^{[2]}(RG) = I(G')$. Since $\tau_R[G] = 2$, $A^{[2]}(RG) = A^{[\omega]}(RG)$. Then from Lemma 3.2 we have the equality $A^{[2]}(RG) = I(G_p)$. Therefore $I(G_p) = I(G')$ and $G_p = G'$.

Conversely. If $G \neq G' = G_p$, then $A^{[2]}(RG/G_p) = 0$ because G/G_p is an Abelian group. From this equality it follows that $A^{[2]}(RG) \subseteq I(G_p)$ and by Lemma 3.2 $A^{[2]}(RG) = A^{[\omega]}(RG)$. Since $G \neq G_p$, $A(RG) \neq A^{[2]}(RG)$. Consequently $\tau_R[G] = 2$ which prove 2) of our theorem.

3) Suppose that $\tau_R[G] = n > 2$. From the statements 1) and 2) it follows that $G \neq G_p$ and $G' \neq G_p$. It is very simple to see that $G/G_{p,i}$ are residually- \mathcal{D}_p groups and consequently, by Theorem 2.2,

$$A^{[\omega]}(RG/G_{p,i}) = 0$$

for all $i \geq 1$. Because $\tau_R[G]$ is finite then

$$\dots \supseteq A^{[n-1]}(RG) \supseteq A^{[n]}(RG) = A^{[n+1]}(RG) = \dots = A^{[\omega]}(RG)$$

and hence

$$\begin{aligned} \dots \supseteq A^{[n-1]}(RG/G_{p,i}) &\supseteq A^{[n]}(RG/G_{p,i}) = \\ &= A^{[n+1]}(RG/G_{p,i}) = \dots = A^{[\omega]}(RG/G_{p,i}). \end{aligned}$$

It follows that $\tau_R[G/G_{p,i}]$ are finite and not greater than $\tau_R[G]$ for all $i \geq 1$. Then there exists a natural number $k \leq n$ such that

$$A^{[k]}(RG/G_{p,i}) = 0 \tag{6}$$

for all i . Then from (2) we have that $A^{[k]}(RG) \subseteq I(G_{p,i})$ for all i . If $i = k$, by Lemma 3.1 we obtain that $A^{[k]}(RG) = I(G_{p,k})$. Hence $I(G_{p,k}) \subseteq I(G_{p,i})$ and therefore, $G_{p,i} \supseteq G_{p,k}$ for all $i \geq 1$. This implies that

$$\dots \supseteq G_{p,k} = G_{p,k+1} = \dots = G_p \tag{7}$$

and by (6) we have that

$$A^{[k]}(RG/G_p) = 0. \tag{8}$$

By Theorem 2.1 it follows that G/G_p is a nilpotent group whose commutator subgroup is a finite p -group.

We remind that in the proof of this part we obtained the following inequalities: from (7) we have that

$$\tau_R[G] \geq \tau_p[G] \quad (9)$$

and from (8) we obtain that

$$\tau_R[G] \geq \tau^\circ[A(RG/G_p)]. \quad (10)$$

Conversely, let G/G_p is a nilpotent group whose derived group is a finite p -group. Then by Theorem 2.1

$$A^{[k]}(RG/G_p) = 0$$

for the Lie nilpotency index $\tau^\circ[A(RG)] = k$ of $A(RG/G_p)$. It follows that $A^{[k]}(RG) \subseteq I(G_p)$. Hence, by Lemma 3.2, we obtain that $A^{[k]}(RG) \subseteq A^{[\omega]}(RG)$. The inverse inclusion, of course, is trivial. Therefore $A^{[k]}(RG) = A^{[\omega]}(RG)$. Consequently, $\tau_R[G]$ is finite and

$$\tau_R[G] \leq \tau^\circ[A(RG/G_p)]. \quad (11)$$

The proof of the theorem is complete.

Theorem 3.2. *Let R be a commutative ring of characteristic p^s and the Lie augmentation terminal of G is finite. Then*

$$\tau_R[G] = \tau^\circ[A(RG/G_p)] \geq \tau_p[G].$$

The proof of this theorem follows from statements 1) and 2) of Theorem 3.1 and from (9), (10) and (11).

References

- [1] PARMENTER, M. M., PASSI, I. B. S. and SEHGAL, S. K., Polynomial ideals in group rings, *Canad. J. Math.*, **25** (1973), 1174–1182.
- [2] PASSI, I. B., Group ring and their augmentation ideals, Lecture notes in Math., **715**, Springer-Verlag, Berlin-Heidelberg-New York, 1979.
- [3] SANDLING, R., The dimension subgroup problem, *J. Algebra*, **21** (1972), 216–231.

Maradékosztály-gyűrű fölötti polinomgyűrű ideáljairól

VERES ZSUZSANNA

Abstract. (On a ideals of a polynomial ring over a residue class ring) In this paper we describe the system of generators of ideals of the ring $\mathbf{Z}_{p^n}[x]$, where \mathbf{Z}_{p^n} is the residue class modulo p^n , p is a prime and n is a natural number.

Jelöljük $\mathbf{Z}_{p^n}[x]$ -szel a $\mathbf{Z}_{p^n} - p^n$ szerinti ($p \in \mathbf{Z}$ prím, $n \in \mathbf{N}$) maradékosztály-gyűrű — fölötti polinomgyűrűt. Legyen I a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű tetszőleges ideálja. A továbbiakban $g(x) \neq 0$ egy rögzített minimális fokszámú polinom azon I -beli polinomok közül, melyek főegyütthatója osztható p -vel, és $h(x) \neq 0$ egy rögzített minimális fokszámú polinom azon I -beli polinomok közül, melyek főegyütthatója nem osztható p -vel. Jelölje $\deg f(x)$ az $f(x)$ polinom fokát.

1. Lemma. Legyen I a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű tetszőleges ideálja és $g(x)$, $h(x)$ a fent említett polinomok. Ekkor a $g(x)$ polinom minden együtthatója osztható p -vel, és foka nem nagyobb $h(x)$ polinom fokánál, azaz a $g(x)$ fokszáma minimális az I -beli polinomok között.

Bizonyítás. Legyen $g(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. Ekkor p osztja az a_n -t, azaz az a_n együttható $a_n = p \cdot a'_n$ alakban írható fel, ahol a'_n nem osztható p -vel. Mivel $g(x)$ az I ideál eleme, ezért $pg(x)$ is az I ideál eleme és

$$pg(x) = p^2 a'_n x^n + pa_{n-1} x^{n-1} + \dots + pa_1 x + pa_0.$$

A $pg(x)$ polinom minden együtthatója osztható p -vel, és mivel a \mathbf{Z}_{p^2} gyűrűben $p^2 = 0$, foka kisebb a $g(x)$ fokánál. Ez csak abban az esetben lehetséges, ha $pg(x) = 0$. Tehát $pa_i = 0$ ($i = 1, 2, \dots, n$), azaz a $g(x)$ polinom minden együtthatója osztható p -vel, és így, $g(x) = pg_1(x)$ ($g_1(x) \in \mathbf{Z}_{p^2}[x]$) alakban írható fel.

Ha $h(x) = b_k x^k + b_{k-1} x^{k-1} + \dots + b_1 x + b_0$, akkor a feltétel szerint b_k nem osztható p -vel, és ezért a \mathbf{Z}_{p^2} együtthatógyűrű egységcsoportjának eleme. Így $pb_k \neq 0$, és a $ph(x) = pb_k x^k + pb_{k-1} x^{k-1} + \dots + pb_1 x + pb_0$ polinom foka megegyezik a $h(x)$ polinom fokával. A $ph(x)$ polinom főegyütthatója osztható p -vel, ezért foka nem lehet kisebb a $g(x)$ polinom fokánál. Mivel $\deg h(x) = \deg ph(x)$, így a $h(x)$ polinom foka sem kisebb a $g(x)$ polinom

fokánál.

2. Lemma. Ha $t(x) \in \mathbf{Z}_{p^2}[x]$ egy olyan polinom, melynek főegyütthatója nem osztható p -vel, akkor tetszőleges $f(x)$ polinom ($f(x) \in \mathbf{Z}_{p^2}[x]$) felírható a következő alakban:

$$f(x) = t(x)s(x) + r(x),$$

ahol $s(x), r(x) \in \mathbf{Z}_{p^2}[x]$ és $\deg r(x) < \deg t(x)$

Bizonyítás. Legyen

$$\begin{aligned} f(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ t(x) &= b_k x^k + b_{k-1} x^{k-1} + \cdots + b_1 x + b_0. \end{aligned}$$

Ha $k > n$ akkor $f(x) = t(x)0 + f(x)$ és ebben az esetben a lemma be van bizonyítva. Tekintsük a $k \leq n$ esetet. Mivel p nem osztja a b_k együtthatót, ezért $a_n b_k^{-1} \neq 0$, ahol b_k^{-1} a b_k inverze. Így az

$$r_1(x) = f(x) - a_n b_k^{-1} x^{n-k} t(x)$$

polinom foka kisebb $f(x)$ fokánál. Tehát $f(x) = t(x)s_1(x) + r_1(x)$ alakú, ahol $s_1(x) = a_n b_k^{-1} x^{n-k}$. Ha $\deg r_1(x) < \deg t(x)$, akkor a lemma bizonyítást nyert. Ha $\deg r_1(x) \geq \deg t(x)$, akkor megismételve az előző eljárást az $r_1(x)$ polinomra, a következő egyenlőséget kapjuk

$$r_1(x) = t(x)s_2(x) + r_2(x),$$

ahol $\deg r_2(x) < \deg r_1(x)$. Ezt az eljárást addig folytatjuk, míg eljutunk egy olyan $r_i(x)$ polinomig, melynek foka már kisebb a $t(x)$ polinom fokánál. Így

$$f(x) = t(x)s_1(x) + t(x)s_2(x) + \cdots + t(x)s_i(x) + r_i(x),$$

és ezért

$$f(x) = t(x)s(x) + r(x),$$

ahol $s(x) = s_1(x) + s_2(x) + \cdots + s_i(x)$, $r(x) = r_i(x)$ és $\deg r(x) < \deg t(x)$.

3. Lemma. A $\mathbf{Z}_{p^2}[x]$ polinomgyűrű tetszőleges ideálja legfeljebb két polinommal generálódik.

Bizonyítás. Legyen I a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű ideálja és $f(x)$ az I ideál tetszőleges eleme. Elégséges megmutatni, hogy az $f(x)$ polinom felírható

$$f(x) = h(x)s(x) + g(x)q(x)$$

alakban, ahol $h(x)$ és $g(x)$ az 1. Lemmában említett polinomok, $s(x)$ és $q(x)$ pedig a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű megfelelő polinomjai. Két eset lehetséges:

$$\deg f(x) \geq \deg h(x);$$

$$\deg f(x) < \deg h(x).$$

Megjegyezzük, hogy az 1. Lemma miatt igaz a következő egyenlőtlenség:

$$\deg f(x) \geq \deg g(x).$$

Tekintsük az első esetet. A 2. Lemma értelmében

$$(1) \quad f(x) = h(x)s(x) + r(x),$$

ahol

$$(2) \quad \deg r(x) < \deg h(x).$$

Könnyen belátható, hogy $r(x) \in I$, és ezért a (2) egyenlőtlenségből és a $h(x)$ polinom tulajdonságából következik, hogy az $r(x)$ főegyütthatója osztható p -vel.

Ha $\deg r(x) < \deg g(x)$, akkor az 1. Lemma következtében $r(x) = 0$, és így $f(x) = h(x)s(x) + g(x)0$ és ebben az esetben a Lemma állítása igazolást nyert. Tekintsük most azt az esetet, amikor $\deg r(x) \geq \deg g(x)$. Írjuk fel $r(x)$ -et két polinom összegeként

$$r(x) = \varphi_1(x) + \varphi_2(x)$$

úgy, hogy az $\varphi_1(x)$ az $r(x)$ polinom azon tagjaiból áll, melyek együtthatói nem oszthatók p -vel, a $\varphi_2(x)$ pedig az $r(x)$ azon tagjait tartalmazza, melyek együtthatói oszthatók p -vel, azaz

$$\varphi_2(x) = p\varphi_2'(x)$$

alakú, ahol $\varphi_2'(x)$ egyik együtthatója sem osztható p -vel. Mivel az $r(x)$ polinom főegyütthatója osztható p -vel,

$$(3) \quad \deg r(x) = \deg \varphi_2(x) > \deg \varphi_1(x).$$

Figyelembe véve a (2) egyenlőtlenséget a

$$(4) \quad \deg \varphi_1(x) < \deg h(x)$$

egyenlőtlenséghez jutunk.

Az 1. Lemma szerint $g(x) = pg_1(x)$ alakba írható, ahol $g_1(x)$ egyik együtthatója sem osztható p -vel. A 2. Lemma szerint

$$\varphi_2'(x) = g_1(x)q(x) + r_1(x),$$

ahol

$$(5) \quad \deg r_1(x) < \deg g_1(x) = \deg g(x).$$

Ekkor

$$\begin{aligned} r(x) &= \varphi_1(x) + p(g_1(x)q(x) + r_1(x)) = \\ &= \varphi_1(x) + g(x)q(x) + pr_1(x). \end{aligned}$$

Könnyű belátni, hogy a $\varphi_1(x) + pr_1(x)$ polinom az I ideál eleme. Mivel $\deg pr_1(x) = \deg r_1(x)$ az (5) egyenlőtlenségből és az 1. Lemmából a

$$\deg(\varphi_1(x) + pr_1(x)) = \deg \varphi_1(x)$$

egyenlőséghez jutunk. Ez azt jelenti, hogy a $\varphi_1(x) + pr_1(x)$ polinom főegyütthatója nem osztható p -vel. Figyelembe véve a (4) egyenlőtlenséget és azt, hogy az I ideálban azon polinomok fokszáma, melyek főegyütthatója nem osztható p -vel, nem lehet kisebb a $h(x)$ polinom fokszámánál, az utolsó egyenlőségből a $\varphi_1(x) + pr_1(x) = 0$ következik. Így $r(x) = g(x)q(x)$ és az (1) egyenlőség szerint

$$f(x) = h(x)s(x) + g(x)q(x).$$

Tekintsük most a második esetet, azaz amikor

$$\deg f(x) < \deg h(x).$$

Felírjuk az $f(x)$ polinomot két polinom összegeként

$$f(x) = f_1(x) + f_2(x),$$

ahol az $f_1(x)$ polinom az $f(x)$ azon tagjaiból áll, melyek együtthatói nem oszthatók p -vel, az $f_2(x)$ pedig $f(x)$ polinom azon tagjait tartalmazza, melyek együtthatói oszthatók p -vel. Mivel az $f(x)$ polinom fokszáma kisebb a $h(x)$ fokszámánál, ezért $f(x)$ főegyütthatójának osztható p -vel. Ezért

$$\deg f(x) = \deg f_2(x) = \deg pf_2'(x) > \deg f_1(x),$$

ahol $f_2(x) = pf_2'(x)$ és az $f_2'(x)$ polinom egyik együtthatója sem osztható p -vel. A 2. Lemma miatt

$$f_2'(x) = g'(x)q(x) + r_1(x)$$

alakú, ahol $\deg r_1(x) < \deg g'(x) = \deg g(x)$. Ebből nyerjük, hogy

$$\begin{aligned} f(x) &= f_1(x) + p(g'(x)q(x) + r_1(x)) = \\ &= f_1(x) + g(x)q(x) + pr_1(x) \end{aligned}$$

Mint az előző esetben, most is meggyőződhetünk róla, hogy $pr_1(x) + f_1(x) = 0$, ezért

$$f(x) = h(x)0 + g(x)q(x)$$

alakban írható fel. A Lemma be van bizonyítva.

1. Tétel. A $\mathbf{Z}_{p^n}[x]$ polinomgyűrű bármely ideálja legfeljebb n elemmel generálódik.

Bizonyítás. A bizonyítást n -szerinti teljes indukcióval végezzük. A $\mathbf{Z}_p[x]$, a \mathbf{Z}_p test fölötti polinomgyűrű főideálgyűrű, $n = 2$ esetben pedig a 3. Lemma szerint a $\mathbf{Z}_{p^2}[x]$ polinomgyűrű minden ideálja legfeljebb két elemmel generálódik.

Tegyük fel, hogy $\mathbf{Z}_{p^{n-1}}[x]$ minden ideálja legfeljebb $n - 1$ elemmel generálódik. Tekintsük azt a

$$\varphi: \mathbf{Z}_{p^n}[x] \rightarrow \mathbf{Z}_{p^{n-1}}[x]$$

homomorfizmust, amelynek magja $\ker \varphi = p^{n-1}\mathbf{Z}_{p^n}[x]$. Ha I a $\mathbf{Z}_{p^n}[x]$ gyűrű ideálja, akkor a $\varphi(I) = \bar{I}$ ideál az indukciós feltevés alapján legfeljebb $n - 1$,

$$\overline{g_0(x)}, \overline{g_1(x)}, \dots, \overline{g_{n-2}(x)},$$

polinommal generálódik, és ezekre a polinomokra teljesül, hogy $\overline{g_i(x)}$ együtthatói oszthatók p^i -nel, de nem oszthatók p^{i+1} -nel ($i = 0, 1, \dots, n - 2$) és fokszámuk minimális az ezzel a tulajdonsággal bíró \bar{I} ideál polinomjai között. Ha $f(x) \in I$, akkor $\varphi(f(x)) = \overline{f(x)} \in \bar{I}$ és

$$\overline{f(x)} = \overline{g_0(x)} \overline{\psi_0(x)} + \overline{g_1(x)} \overline{\psi_1(x)} + \dots + \overline{g_{n-2}(x)} \overline{\psi_{n-2}(x)}$$

alakban írható fel, ahol $\overline{\varphi_i(x)} \in \mathbf{Z}_{p^{n-1}}[x]$ ($i = 0, 1, \dots, n - 2$). Jelölje $g_i(x)$ és $\psi_i(x)$ ($i = 0, 1, \dots, n - 2$) megfelelően az $\overline{g_i(x)}$ és az $\overline{\psi_i(x)}$ polinomok valamelyik inverz képét. Ekkor

$$f(x) = g_0(x)\psi_0(x) + g_1(x)\psi_1(x) + \dots + g_{n-2}(x)\psi_{n-2}(x) + t(x),$$

ahol $t(x)$ egy megfelelő polinom a φ homomorfizmus magjából. Így a $t(x)$ polinom minden együtthatója osztható p^{n-1} -nel, vagyis $t(x) = p^{n-1}t'(x)$ alakban írható fel. Tehát

$$f(x) = g_0(x)\psi_0(x) + g_1(x)\psi_1(x) + \cdots + g_{n-2}(x)\psi_{n-2}(x) + p^{n-1}t'(x).$$

Ez az egyenlőség azt jelenti, hogy a $\mathbf{Z}_{p^n}[x]$ polinomgyűrű tetszőleges ideálja legfeljebb n elemmel generálódik.

Ha a $t'(x)$ polinomnak nagyobb a foka mint az I ideál azon minimális fokszámú polinomjainak amelyek együtthatói p^{n-1} -nel oszthatók, akkor $t(x) = p^{n-1}t'(x)$ és a 2. Lemma szerint

$$t(x) = p^{n-1}t'(x) = p^{n-1}g'_{n-1}(x)\psi_{n-1}(x) = g_{n-1}(x)\psi_{n-1}(x),$$

ahol $g_{n-1}(x)$ polinom együtthatói oszthatók p^{n-1} -nel, és így,

$$f(x) = g_0(x)\psi_0(x) + g_1(x)\psi_1(x) + \cdots + g_{n-1}(x)\psi_{n-1}(x).$$

Tehát, a $\mathbf{Z}_{p^n}[x]$ gyűrű tetszőleges I ideáljának generátorrendszere olyan

$$g_0(x), g_1(x), \dots, g_{n-1}(x)$$

polinomokból áll, hogy bármelyik $g_i(x)$ -re igaz, hogy $g_i(x)$ együtthatói oszthatók p^i -nel, de nem oszthatók p^{i+1} -nel, és fokszámuk minimális az ezzel a tulajdonsággal bíró polinomok között.

A geometriai szerkeszthetőségről

KISS PÉTER és MÁTYÁS FERENC

Abstract. (On the geometrical constructibility) In this paper we deal with the algebraic theory of geometrical constructibility, especially with the case of the constructibility of regular polygons. We give such a proof of Gauss' famous theorem which can easily be understood by the students of Teachers' Training Colleges.

Dolgozatunkban a geometriai szerkeszthetőség algebrai elmélete tanításának az EKTf matematika szakos hallgatói számára kidolgozott és az elmúlt években tanított változatával foglalkozunk. E témakör tárgyalása természetesen megtalálható több helyen (pl. [1], [2], [3], [4]), de a bizonyítások sokszor csak vázlatosak, főiskolai hallgatók számára nem mindig érthetőek. Cikkünkben igyekszünk a főiskolai hallgatók matematikai ismereteinek megfelelő bizonyításokat adni, így feltételezzük, hogy az olvasó is rendelkezik a harmadéves főiskolai hallgatóktól elvárható algebrai (testbővítési) és számelméleti alapismeretekkel.

Először tisztázzuk, hogy euklideszi szerkesztés során milyen adatokat, milyen eszközöket és milyen eljárásokat engedünk meg. A szerkesztés adatai: adott síkban véges sok pont, egyenes és kör, míg szerkesztési eszközként egyélű vonalzót, ill. körzőt használhatunk. Szerkesztési eljárásként az alábbiakat engedjük meg:

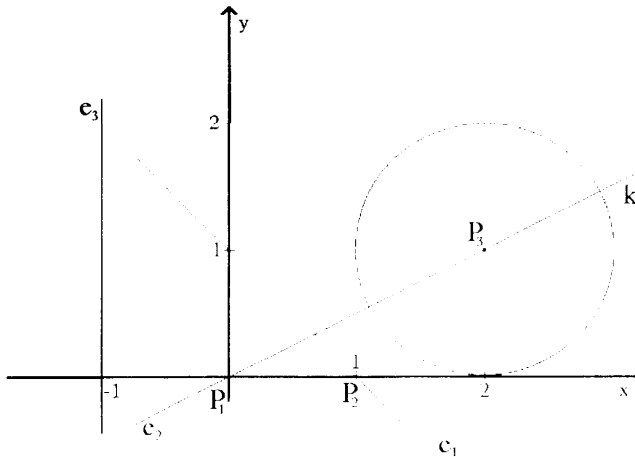
- két adott (vagy már szerkesztett) ponton át egyenes meghúzása;
- adott (vagy szerkesztett) pontok távolságával, mint sugárral adott (vagy szerkesztett) pont, mint középpont köré kör rajzolása;
- két adott egyenes metszéspontjának kijelölése;
- adott egyenes és adott kör metszéspontjainak kijelölése.

A fenti, ún. alapszerkesztések véges sorozatát euklideszi szerkesztésnek nevezzük. Egy szerkesztési feladatot megoldhatónak mondunk, ha a keresett (szerkesztendő) pont vagy ponthalmaz euklideszi szerkesztéssel előállítható.

A geometriai szerkeszthetőség algebrai jellemzése

Mivel az euklideszi szerkesztés minden lépése egy adott síkban történik, ezért mind az adatok, mind az alapszerkesztésekkel kapott újabb pontok,

egyenesek és körök azonosítására vegyünk fel az adott síkban egy derékszögű koordinátarendszert. Az adatok A_0 halmazának legalább két pontot tartalmaznia kell (ellenkező esetben a szerkesztési algoritmus el sem indítható), ezért a koordinátarendszer felvehető úgy, hogy A_0 egyik pontja a koordinátarendszer origója, míg egy másik pontja az egyik koordináta-tengely egységpontja legyen. Ebben a koordinátarendszerben A_0 pontjait koordinátáikkal, A_0 köreit a középpontjaik koordinátaival és sugaraik hosszával, míg A_0 egyeneseit az $a_i x + b_i y = c_i$ normál vektoros egyenletükben szereplő (a_i, b_i, c_i) számhármassokkal jellemezhetjük (ill. azonosíthatjuk). Az A_0 elemeihez így rendelt „koordináták” halmazát jelöljük K_0 -lal. Az adatok A_0 halmazához így előállított K_0 -hoz rendeljük hozzá azt a legszűkebb T_0 számtestet, melyre $K_0 \subset T_0$. Konstruíciónkból adódik, hogy $Q \subseteq T_0 \subset R$. Érdeemes megjegyezni, hogy a T_0 számtest nem függ attól, hogy A_0 mely pontját választottuk a koordinátarendszer kezdő, ill. egységpontjának, mivel az egyik koordinátarendszerből a másikba való áttérés során csak T_0 beli alapműveleteket végzünk, így a transzformációs számítások eredményei is T_0 -ban lesznek. Például, ha $A_0 = \{P_1, P_2, P_3, e_1, e_2, e_3, k\}$, ahol P_1, P_2, P_3 az 1. ábra szerinti pontokat, e_1, e_2, e_3 egyeneseket, míg k kört jelöl, akkor A_0 elemeit az alábbi módon jellemezhetjük.



1. ábra

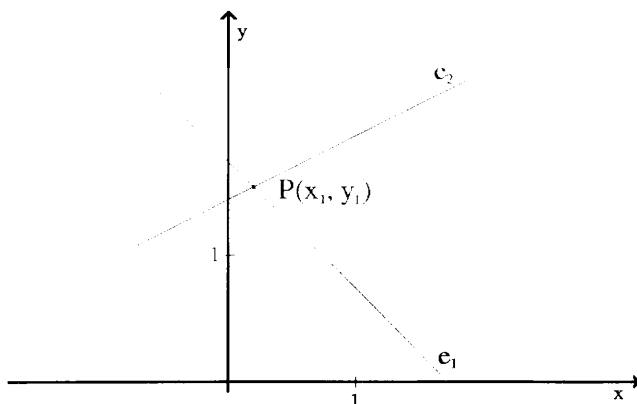
$P_1(0, 0)$; $P_2(1, 0)$; $P_3(2, 1)$, $e_1(1, 1, 1)$, $e_2(1, -2, 0)$, $e_3(1, 0, -1)$ és $k(2, 1, 1)$, mivel e_1 egyenlete: $x + y = 1$, e_2 egyenlete: $x - 2y = 0$, e_3 egyenlete: $x + 0y = -1$ és a k kör egyenlete: $(x - 2)^2 + (y - 1)^2 = 1^2$. Ebben az esetben $K_0 = \{0, 1, 2, -1, -2\}$ és $T_0 = Q$.

A továbbiakban vizsgáljuk meg az A_0 -ból szerkeszthető pontok koordinátáit tartalmazó számtesteket. Erről szól a következő tétel.

1. Tétel. Az adatok A_0 (legalább két pontot tartalmazó) halmazából az A_0 elemeit tartalmazó sík P pontja akkor és csakis akkor szerkeszthető meg euklideszi szerkesztéssel, ha a P pont koordinátái egy olyan \mathbf{T} számtest elemei, mely az A_0 -hoz rendelt \mathbf{T}_0 számtest 2^j -edfokú algebrai bővítése, ahol $j \geq 0$ valamely egész szám.

Bizonyítás. Az A_0 elemeiből euklideszi alapszerkesztésekkel szerkesztett ponthoz juthatunk két egyenes metszéspontjának, egyenes és kör, ill. két kör metszéspontjának meghatározásával. Vizsgáljuk meg az így szerkesztett pont koordinátáit az egyes esetekben.

a) Legyen e_1 és e_2 a két metsző egyenes, melyek egyenlete $e_1: a_1x + b_1y = c_1$ és $e_2: a_2x + b_2y = c_2$, ahol $e_1, e_2 \in A_0$, $a_i, b_i, c_i \in \mathbf{T}_0$ ($i = 1, 2$).



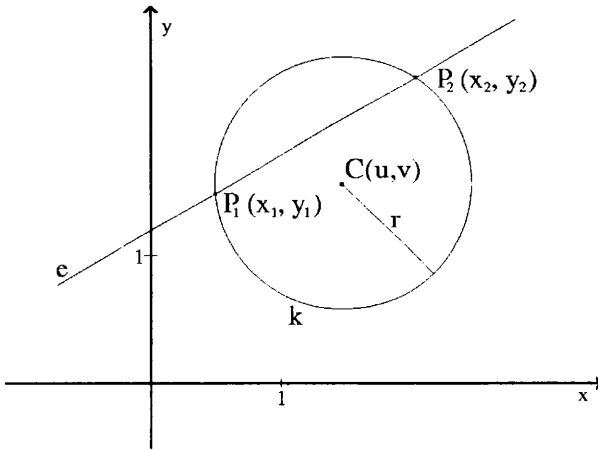
2. ábra

A P metszéspont x_1 és y_1 koordinátáit az

$$x_1 = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}} \quad \text{és} \quad y_1 = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}$$

formulák adják, azaz $x_1, y_1 \in \mathbf{T} = \mathbf{T}_0$.

b) Legyen az egymást metsző e egyenes, ill. k kör egyenlete $e: ax + by = c$, ill. $k: (x - u)^2 + (y - v)^2 = r^2$, ahol $e, k \in A_0$ és $a, b, c, u, v, r \in \mathbf{T}_0$ ($r > 0$).



3. ábra

Az így megszerkeszthető P_1 és P_2 metszéspontok (x_1, y_1) , ill. (x_2, y_2) koordinátáit az

$$\left. \begin{array}{l} ax + by = c \\ (x - u)^2 + (y - v)^2 = r^2 \end{array} \right\}$$

egyenletrendszer megoldásai adják. Az $a^2 + b^2 \neq 0$ miatt feltehetjük, hogy pl. $b \neq 0$ és így x_1, x_2 értékét az

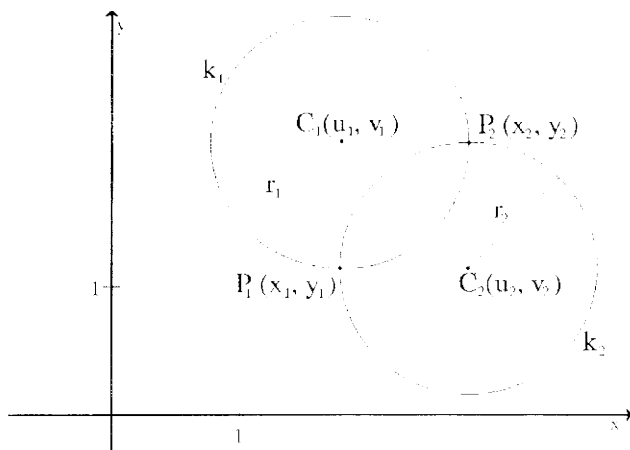
$$(x - u)^2 + \left(\frac{c - ax}{b} - v \right)^2 = r^2,$$

vagy az ebből rövid átalakítással kapható $x^2 + Ax + B = 0$ alakú másodfokú egyenlet

$$x_{1,2} = \frac{-A \pm \sqrt{D}}{2}$$

gyökei adják, ahol A és B az a, b, u, v és r -től lineárisan függő konstans, $D = A^2 - 4B$ és $A, B, D (\geq 0) \in \mathbf{T}_0$, továbbá $y_{1,2} = \frac{1}{b}(c - ax_{1,2})$. Ha $\sqrt{D} \in \mathbf{T}_0$, akkor x_1, x_2, y_1 és y_2 is \mathbf{T}_0 -beli elem, míg $\sqrt{D} \notin \mathbf{T}_0$ esetén az x_1, x_2, y_1 és y_2 koordináták egy olyan \mathbf{T}_1 számtest elemei, melyre $\mathbf{T}_0 \subset \mathbf{T}_1$ és $\mathbf{T}_1 = \mathbf{T}_0(\sqrt{D})$, azaz a \mathbf{T}_1 számtest a \mathbf{T}_0 másodfokú algebrai bővítése.

c) Legyen az egymást metsző k_1 és k_2 körök egyenlete $k_1: (x - u_1)^2 + (y - v_1)^2 = r_1^2$, ill. $k_2: (x - u_2)^2 + (y - v_2)^2 = r_2^2$, ahol $k_1, k_2 \in A_0$, míg $u_i, v_i, r_i \in \mathbf{T}_0$ és $r_i > 0$ ($i = 1, 2$).



4. ábra

A megszerkeszthető P_1 és P_2 pontok (x_1, y_1) , ill. (x_2, y_2) koordinátáit az

$$\left. \begin{aligned} (x - u_1)^2 + (y - v_1)^2 &= r_1^2 \\ (x - u_2)^2 + (y - v_2)^2 &= r_2^2 \end{aligned} \right\}$$

egyenletrendszer megoldásai adják. Látható, hogy pl. az x_1, x_2 megoldások ebben az esetben is egy alkalmas

$$x^2 + Ax + B = 0 \quad (A, B, D(= A^2 - 4B) \geq 0) \in \mathbf{T}_0)$$

egyenlet gyökei. Ezért — hasonlóan a b) esethez — x_1, x_2, y_1 és y_2 elemei \mathbf{T}_0 -nak ha $\sqrt{D} \in \mathbf{T}_0$, míg $\sqrt{D} \notin \mathbf{T}_0$ esetén $x_1, x_2, y_1, y_2 \in \mathbf{T}_1 = \mathbf{T}_0(\sqrt{D})$.

Ha az adatok A_0 és a már megszerkesztett pontok halmazából újabb pontot (vagy pontokat) szerkesztünk, akkor az a), b) vagy c) esetek ismételt alkalmazásával láthatjuk, hogy az új pontok koordinátái \mathbf{T}_0 vagy a \mathbf{T}_1 számtestben, vagy a $\mathbf{T}_2 = \mathbf{T}_1(\sqrt{D_1})$ testben találhatóak, ahol $D_1 \in \mathbf{T}_1$, de $\sqrt{D_1} \notin \mathbf{T}_1$ és $\mathbf{Q} \subseteq \mathbf{T}_0 \subset \mathbf{T}_1 \subset \mathbf{T}_2$. Tovább folytatva a szerkeszthető pontok koordinátáinak meghatározását láthatjuk, hogy minden szerkeszthető pont koordinátája \mathbf{T}_0 -ban, vagy valamely $\mathbf{T}_j = \mathbf{T}_{j-1}(\sqrt{D_{j-1}})$ számtestben található, ahol $D_{j-1} \in \mathbf{T}_{j-1}$, $\sqrt{D_{j-1}} \notin \mathbf{T}_{j-1}$ és

$$\mathbf{Q} \subseteq \mathbf{T}_0 \subset \mathbf{T}_1 \subset \mathbf{T}_2 \subset \cdots \subset \mathbf{T}_j \subset \cdots \subset \mathbf{T}_k \subset \mathbf{R}$$

($1 \leq j \leq k$). Mivel \mathbf{T}_j minden esetben másodfokú algebrai bővítése \mathbf{T}_{j-1} -nek, ezért — tudva, hogy az egymás utáni algebrai bővítések során a bővítések fokszáma szorozódik — \mathbf{T}_j valóban 2^j -edfokú (algebrai) bővítése \mathbf{T}_0 -nak.

Bizonyításunk második részében megmutatjuk, hogy a $\mathbf{T}_j = \mathbf{T}_{j-1}(\sqrt{D_{j-1}})$ ($D_{j-1} \in \mathbf{T}_{j-1}$) test elemeivel, mint koordinátákkal adott minden pont valóban szerkeszthető euklideszi szerkesztéssel.

Ismert, hogy a $\mathbf{T}_j(\sqrt{D_{j-1}})$ test minden eleme $a_{j-1} + b_{j-1}\sqrt{D_{j-1}}$ ($a_{j-1}, b_{j-1}, D_{j-1} \in \mathbf{T}_{j-1}$) alakú, ezért az elemek szerkeszthetősége $a_{j-1}, b_{j-1}, D_{j-1} \in \mathbf{R}^+$ esetén egyenértékű szakaszok összegének, különbségének, szorzatának, hányadosának és négyzetgyökének euklideszi szerkesztéssel való előállításával. Elemi geometriai tanulmányainkból ismert, hogy a fenti szerkesztések mind elvégezhetők a megengedett euklideszi alapszerkesztésekkel. Sőt, ha a komplex számokat vektorként vesszük fel, a műveleteket pedig a komplex számok abszolút értéke és irányszöge segítségével végezzük, akkor $a_{j-1}, b_{j-1}, d_{j-1} \in \mathbf{C}$ esetén is elvégezhető valamennyi fenti szerkesztési lépés. (Néhány szerkesztés menetét lásd. [3]-ban.) Az alaptest minden 2^j -edfokú bővítését másodfokú bővítések sorozata adja, így a tételek állítása bizonyított.

Megjegyzés. Ha az adatok A_0 halmazához rendelt \mathbf{T}_0 számtestre $\mathbf{T}_0 = \mathbf{Q}$, akkor az 1. Tétel szerint pontosan azon P pontok szerkeszthetők meg euklideszi értelemben, melyek koordinátái \mathbf{Q} -nak valamely 2^j -edfokú algebrai bővítésében találhatók, azaz — az algebrai bővítésekről tanultak szerint — a koordináták, mint valós számok zérushelyei egy \mathbf{Q} fölött irreducibilis 2^j -edfokú racionális együtthatós polinomnak. A z komplex számot reprezentáló P pont esetén a szerkeszthetőség kérdése nyilvánvalóan ekvivalens azzal, hogy z gyöke-e egy \mathbf{Q} fölött irreducibilis 2^j -edfokú racionális együtthatós polinomnak.

Klasszikus szerkeszthetőségi problémák

Az 1. Tétel alkalmazásaként könnyen adhatunk választ néhány nevezetes, szerkeszthetőségi problémára.

— **A kockakettőzés** (déloszi probléma) néven ismert szerkesztési feladatban egy adott kocka éléből kell egy kétszer akkora térfogatú kocka élét megszerkeszteni. Tekintsük az adott él, mint szakasz két végpontját egy koordinátarendszer origójának és (egyik tengelye) egységpontjának. Ebben a koordinátarendszerben az adatok jellemezhetők a $K_0 = \{0, 1\}$ halmazzal és így a hozzá tartozó \mathbf{T}_0 testre $\mathbf{T}_0 = \mathbf{Q}$. A feladat megoldásához a kettő térfogatú kocka $\sqrt[3]{2}$ hosszúságú élét kellene megszerkeszteni. De az 1. Tétel után tett megjegyzésünk szerint ez nem lehetséges, mivel $\sqrt[3]{2}$ az $f(x) = x^3 - 2$ racionális együtthatós, \mathbf{Q} fölött irreducibilis de nem 2^j -edfokú polinom zérushelye.

Ha olyan szerkesztési lépéseket is megengedünk, melyek nem euklideszi alapszerkesztések, akkor e probléma szerkesztéssel megoldható lehet, lásd pl. [2], 123. oldal.

— **A szögharmadolás** (triszekció) néven olyan véges szerkesztési eljárás keresése a feladat, mely tetszőleges szög harmadának a szerkesztését adja. Konkrét szög, pl. 90° harmadolására könnyen tudunk euklideszi szerkesztési eljárást adni, ugyanakkor az általános eljárás létezését cáfolhatjuk, ha találunk olyan szöget, melynek harmada nem szerkeszthető euklideszi értelemben. Állítjuk, hogy pl. 60° harmada nem szerkeszthető.

Legyen adott két pont, mely egy koordinátarendszer origója, ill. egységpontja (e két pont ismeretében a 60° -os szög már szerkeszthető). Így $K_0 = \{0, 1\}$ és $\mathbf{T}_0 = \mathbf{Q}$. Mivel 60° harmadának, 20° -nak a szerkeszthetősége nyilvánvalóan ekvivalens $\cos 20^\circ$ (ill. $\sin 20^\circ$) szerkeszthetőségével, ezért elegendő megmutatnunk, hogy $\cos 20^\circ$ nem szerkeszthető. Az $\frac{1}{2} = \cos 60^\circ = 4 \cos^3 20^\circ - 3 \cos 20^\circ$ trigonometrikus egyenlőségből $x = \cos 20^\circ$ helyettesítésével a $8x^3 - 6x - 1 = 0$ egyenlőséghez jutunk, azaz $x = \cos 20^\circ$ zérushelye az $f(x) = 8x^3 - 6x - 1$ polinomnak. Könnyen ellenőrizhetjük, hogy a Rolletétel szerint lehetséges $\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$ racionális számok nem zérushelyei az $f(x)$ polinomnak, ezért $f(x)$ irreducibilis \mathbf{Q} fölött. Mivel $f(x)$ nem 2^j -edfokú polinom, így $\cos 20^\circ$ (és vele együtt 20° nem szerkeszthető euklideszi szerkesztéssel).

Persze, nem-euklideszi szerkesztési lépéseket is megengedve, vagy az adatok A_0 halmazának alkalmas bővítésével e feladat is megoldható, lásd pl. Bolyai János szerkesztési eljárását [2] 129 oldalán.

— **A kör négyszögesítése, ill. kiegyenesítése** néven ismertek azok a szerkesztési feladatok, amikor adott kör területével egyenlő területű négyzet oldalát, ill. adott kör kerületével egyenlő hosszú szakaszt kell szerkeszteni. Legyen ebben az esetben is adott két pont, az egyik a kör középpontja, a másik a kör egy kerületi pontja, melyek a koordinátarendszerünk origója, ill. egységpontjai lesznek. Így $K_0 = \{0, 1\}$ és $\mathbf{T}_0 = \mathbf{Q}$. A feladatok nem megoldhatóságát az $f(x) = x^2 - \pi$, ill. a $g(x) = x - 2\pi$ polinomok zérushelyeinek nem szerkeszthetősége adja. Ugyanis π transzcendens volta miatt $\sqrt{\pi}$ és 2π is transzcendens, holott az 1. Tétel szerint csak (speciális) algebrai számok szerkeszthetők euklideszi szerkesztéssel.

— **A szabályos sokszögek euklideszi szerkeszthetőségére** vonatkozik a következő, Gauss-tól származó híres tétel:

Gauss-tétel: Az n -oldalú szabályos sokszög akkor és csakis akkor szerkeszthető meg euklideszi szerkesztéssel, ha $n = 2^k p_1 p_2 \cdots p_r$ alakú ($n \geq 3, k \geq 0, r \geq 0$), ahol p_1, p_2, \dots, p_r különböző Fermat-féle prímekek. (Egy

p prímszám Fermat-féle, ha $p = 2^{2^t} + 1$ alakú, ahol $t \in \mathbf{N}$).

Megjegyzés. Mivel egy adott szög 2^k -ad része szögfelezéssel mindig szerkeszthető, ezért a bizonyításban feltehetjük, hogy $n(\geq 3)$ páratlan egész, továbbá a tétel bizonyítását az alábbi tételek (részállítások) bizonyítására bontjuk.

2. Tétel. Legyen $n = p \geq 3$ prímszám. A p oldalú szabályos sokszög akkor és csak akkor szerkeszthető euklideszi szerkesztéssel, ha p Fermat-féle prím.

3. Tétel. Legyen $n = p_1 p_2 \cdots p_r$, ahol p_1, p_2, \dots, p_k különböző páratlan prím és $r \geq 2$. Az n -oldalú szabályos sokszög akkor és csak akkor szerkeszthető euklideszi szerkesztéssel, ha p_1, p_2, \dots, p_r Fermat-féle prímek.

4. Tétel. Legyen p páratlan prím. A szabályos p^2 oldalú sokszög nem szerkeszthető euklideszi szerkesztéssel.

5. Tétel. Legyen n páratlan és $p^2 \mid n$, ahol $p \geq 3$ prím. Az n -oldalú szabályos sokszög nem szerkeszthető euklideszi szerkesztéssel.

A tételek bizonyításában felhasználjuk azt az ismert tételt, miszerint a $\binom{p}{k}$ binomiális együttható osztható p -vel, ha p prím és $0 < k < p$. Felhasználjuk továbbá az úgynevezett Schönemann—Eisenstein irreducibilitási kritériumot, mely kimondja: ha $f(x) = a_n x^n + \cdots + a_0$ egy egész együtthatós polinom és p egy prím, mely eleget tesz $p \nmid a_n, p \mid a_i$ ($i = 0, \dots, n-1$), $p^2 \nmid a_0$ feltételeknek, akkor $f(x)$ irreducibilis a racionális számtest felett.

2. tétel bizonyítása. Egy szabályos p oldalú (pl. egységsugarú körbe írt) sokszög szerkeszthetősége nyilvánvalóan ekvivalens olyan véges algoritmus megadásával, mellyel az $\alpha = \frac{2\pi}{p}$ szög szerkeszthető. Mivel $\alpha = \frac{2\pi}{p}$ szög akkor és csak akkor szerkeszthető, ha $\cos \frac{2\pi}{p}$ (ill. $\sin \frac{2\pi}{p}$) szerkeszthető, ezért vizsgálhatjuk az $\varepsilon(p) = \cos \frac{2\pi}{p} + i \sin \frac{2\pi}{p}$ komplex p -edik egységgyök szerkeszthetőségét. Ebben az esetben is indulhatunk a $K_0 = \{0, 1\}$ halmazból, azaz $\mathbf{T}_0 = \mathbf{Q}$. Az 1. tétel után tett megjegyzés szerint $\varepsilon(p)$ akkor és csak akkor szerkeszthető, ha $\varepsilon(p)$ zérushelye egy \mathbf{Q} fölött irreducibilis 2^j -edfokú racionális együtthatós polinomnak. Tudjuk, hogy $\varepsilon(p)$ zérushelye az

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

úgynevezett p -edik körosztási polinomnak, melynek \mathbf{Q} fölötti irreducibilitása az alábbi módon igazolható. Helyettesítsünk x helyére $y + 1$ -et, ekkor

$$f(x) = f(y + 1) = \frac{(y + 1)^p - 1}{y} =$$

$$= y^{p-1} + \binom{p}{1} y^{p-2} + \dots + \binom{p}{p-2} y + \binom{p}{p-1}.$$

Mivel $p \mid \binom{p}{1}, p \mid \binom{p}{2}, \dots, p \mid \binom{p}{p-1}$, de $p^2 \nmid \binom{p}{p-1}$, ezért az említett Schönemann—Eisenstein-tétel szerint $f(y+1)$ (és vele együtt $f(x)$ is) irreducibilis \mathbf{Q} fölött. Így a szerkeszthetőség szükséges és elégséges feltétele ha $p-1 = 2^j$, azaz $p = 2^j + 1$, ahol $j \in \mathbf{N}$. Mivel $p = 2^j + 1$ prím, ezért j csak $j = 2^t$ ($t \in \mathbf{N}$) alakú lehet, mert ellenkező esetben p nem prím (ugyanis $j = 2^t m$, $m \geq 3$ páratlan esetben $2^{2^t} + 1 \mid (2^{2^t})^m + 1$).

3. Tétel bizonyítása. Legyenek p_1, p_2, \dots, p_r különböző Fermat-féle prímekek ($r \geq 2$). A 2. Tétel szerint a p_1, p_2, \dots, p_r oldalú szabályos sokszögek szerkeszthetők, azaz az

$$\alpha_1 = \frac{2\pi}{p_1}, \quad \alpha_2 = \frac{2\pi}{p_2}, \quad \dots, \quad \alpha_r = \frac{2\pi}{p_r}$$

szögek szerkeszthetők. Allítjuk, hogy léteznek olyan k_1, k_2, \dots, k_r egész számok, melyekre

$$k_1 \alpha_1 + k_2 \alpha_2 + \dots + k_r \alpha_r = \alpha,$$

ahol $\alpha = \frac{2\pi}{p_1 p_2 \dots p_r}$, azaz az $n = p_1 p_2 \dots p_r$ oldalú szabályos sokszög szerkeszthetőségével ekvivalens α szög szerkeszthető. Ugyanis a helyettesítéseket

elvégezve és a $q_j = \frac{\prod_{i=1}^r p_i}{p_j}$ jelölést bevezetve a

$$q_1 k_1 + q_2 k_2 + \dots + q_r k_r = 1$$

lineáris diofantoszi egyenletet kapjuk, mely $(q_1, q_2, \dots, q_r) = 1$ miatt mindig megoldható.

A tétel állításának szükséges részét indirekt módon igazoljuk. Tegyük fel, hogy az $n = p_1 p_2 \dots p_r$ oldalú szabályos sokszög szerkeszthető és pl. p_1 nem Fermat-féle prím. Ekkor a megszerkesztett n -oldalú szabályos sokszög minden $p_2 p_3 \dots p_r$ -edik csúcsát összekötve egy p_1 (nem Fermat-féle prím) oldalú szabályos sokszöget kapunk, mely ellentmond a 2. Tételnek.

4. Tétel bizonyítása. Az 1. Tétel szerint elegendő megmutatni, hogy az

$$\varepsilon(p^2) = \cos \frac{2\pi}{p^2} + i \sin \frac{2\pi}{p^2}$$

komplex szám zérushelye egy nem 2^j -edfokú, \mathbf{Q} fölött irreducibilis racionális együtthatós polinomnak. Tudjuk, hogy $\varepsilon(p^2)$ zérushelye az

$$f(x) = \frac{x^{p^2} - 1}{x^p - 1} = x^{p(p-1)} + x^{p(p-2)} + \dots + x^p + 1$$

polinomnak, melynek \mathbf{Q} fölötti irreducibilitása az alábbi módon igazolható. Helyettesítsünk x helyébe $y + 1$ -et, ekkor

$$f(x) = f(y + 1) = \frac{(y + 1)^{p^2} - 1}{(y + 1)^p - 1} = (y + 1)^{p(p-1)} + (y + 1)^{p(p-2)} + \dots + (y + 1)^p + 1 = y^{p(p-1)} + \dots + p,$$

és

$$(y + 1)^p - 1 = y^p + \binom{p}{1}y^{p-1} + \dots + \binom{p}{p-1}y = y^p + ph_1(y),$$

ahol $h_1(y)$ egy egész együtthatós, $p - 1$ -edfokú polinom. Mivel

$$(y + 1)^{p^2} = (y^p + ph_1(y) + 1)^p,$$

így

$$(y + 1)^{p^2} - 1 = ((y^p + 1) + ph_1(y))^p - 1 = (y^p + 1)^p + ph_2(y) - 1 = y^{p^2} + ph_3(y),$$

ahol $h_2(y)$ és $h_3(y)$ egész együtthatós polinomok, melyek fokszáma $p(p - 1)$. Ezért

$$\begin{aligned} f(x) = f(y + 1) &= \frac{(y + 1)^{p^2} - 1}{(y + 1)^p - 1} = \frac{y^{p^2} + ph_3(y)}{y^p + ph_1(y)} = \\ &= y^{p^2-p} + p \frac{h_3(y) - y^{p^2-p}h_1(y)}{y^p + ph_1(y)} = \\ &= y^{p^2-p} + ph_4(y) \end{aligned}$$

ahol $h_4(y)$ alkalmas egész együtthatós, $p^2 - p - 1$ -edfokú polinom. Mivel $f(y + 1) = y^{p(p-1)} + \dots + p$ is igaz, ezért az ismert Schönemann—Eisenstein-tétel szerint $f(y + 1)$ (és vele együtt $f(x)$ is) irreducibilis \mathbf{Q} fölött, de $p^2 - p \neq 2^j$, mert p páratlan prím.

5. Tétel bizonyítása. Indirekt bizonyítást választva, tegyük fel, hogy az $n = p^2m$ oldalú szabályos sokszög szerkeszthető (p páratlan prím és $m \geq 3$). Ekkor a megszerkesztett n oldalú szabályos sokszög minden m -edik csúcsát összekötve egy p^2 oldalú szabályos sokszöget kapunk, mely ellentmond a 4. Tételnek.

A 2—5. Tételekből Gauss tétele már következik.

Végezetül választ adunk arra a kérdésre, hogy mely egész fokos szögek szerkeszthetők euklideszi szerkesztéssel.

6. Tétel. n° ($n \in \mathbf{N}$) akkor és csak akkor szerkeszthető euklideszi szerkesztéssel, ha $3 \mid n$.

Bizonyítás. Gauss tétele szerint a szabályos ötszög szerkeszthető, mert $5 = 2^{2^1} + 1$ alakú Fermat-féle prím, azaz $\frac{360^\circ}{5} = 72^\circ$ szerkeszthető. Mivel 60° könnyen szerkeszthető az ismert módon, ezért a kettő különbsége — $70^\circ - 60^\circ = 10^\circ$ — is szerkeszthető. 10° -ból szögfelezéssel szerkeszthető a 6° , ill. 3° . 3° ismeretében $n = 3k$ esetén $n^\circ = (k3)^\circ$ ($k \in \mathbf{N}$) nyilván szerkeszthető.

Ha $n = 3k \pm 1$ alakú természetes szám és n° szerkeszthető lenne, akkor — $(k3)^\circ$ szerkeszthetősége miatt — 1° is szerkeszthető lenne, amiből a $20 \cdot 1^\circ = 20^\circ$ szerkeszthetősége következne, ami ellentmond a szögharmadolás témában bizonyított állításnak.

Irodalom

- [1] FUCHS LÁSZLÓ: Algebra. Tankönyvkiadó, Bp., 1992.
- [2] SAIN MÁRTON: Nincs királyi út. Gondolat Kiadó, Bp., 1986.
- [3] SZENDREI JÁNOS: Algebra és számelmélet. Tankönyvkiadó, Bp., 1975.
- [4] SZŐKEFALVI NAGY GYULA: Geometriai szerkesztések elmélete. Akadémiai Kiadó, Bp., 1968.

Az általánosítás, mint a problémamegoldás része

OROSZ GYULÁNÉ

Abstract. (The generalization is as part of the problem solving) First part is an introduction. It is about György Polya's method in generally and we give some important definitions, such as problem, problem solving, the steps of the problem solving. Second part consists of a generalization of the mathematics problem. This part consists of examples connect with the generalization.

A problémamegoldás módszertanát, a tanításban és a tanárképzésben betöltött szerepét egy kiváló matematikus, Pólya György könyvei, cikkei részletesen elemzik. Pedagógiai művei a tanárképzésben is jól hasznosítható problémákat, metodikai észrevételeket, útmutatásokat tartalmaznak.

Problémának, nevezzük az olyan szituáció, kérdés, feladat felvetődését, amelyre a választ, a megoldást nem tudjuk azonnal észlelés, emlékezés, tapasztalás alapján közvetlenül megadni, hanem csak közvetet úton, gondolkodási és logikai műveletvégzéseken keresztül.

Problémamegoldáson egy kitűzött cél meghatározott feltételek mellett történő elérésére irányuló tevékenységet értjük.

A problémamegoldás egyes fázisait általánosítható törvényszerűségek jellemzik.

Először a szemlélődés, empírikus tevékenység oldaláról közelítjük meg a kitűzött feladatot, próbáljuk megsejteni az eredményt, találgatunk. Ezt követi a fogalmi szintre történő áttérés. Definíciókat, segédteteleket, részproblémákat fogalmazzunk meg, összefüggéseket keresünk. Az elsődleges megoldást egyre finomítjuk, kiküszöböljük az esetleges hiányokat. Eredményeinket tapasztalati úton ellenőrizzük, majd a megoldást megfelelő logikai rendbe szedve megfogalmazzuk. Ezt a fogalmi szakaszt már átszövi az asszimilálás. A megoldott problémát beépítjük meglévő ismereteink rendszerébe. A megoldásnál alkalmazott módszereket gondolkodásunk egészébe illesztjük, hogy azokat újabb feladatok megoldásánál felhasználhassuk. Felvetődik az alkalmazások lehetősége, esetleg új problémákat, további általánosításokat fogalmazzhatunk meg.

A tanárjelöltek képzésében az „Elemi matematika” című tárgy célja a problémamegoldás metodikájának elsajátítása, a problématervezéshez és megoldáshoz szükséges tanári készség kifejlesztése. A feldolgozásra kerülő problémaanyag tartalmaz általános és középiskolai versenyfeladatokat is. Ezen versenyfeladatok megoldása is alkotó szellemi munka, amely sok örömet okozhat tanárnak, diáknak egyaránt.

A tanulmányi versenyek feladatainak, megoldásuknak az elemzése során felvetődnek azon túlmutató kérdések. Új problémák adódnak az adatok és feltételek variálásakor, az analógiák, átfogalmazások kapcsán, az általánosításra, vagy specializálásra törekvés útján.

Az általánosítások, specializálások fejlesztik a tanárjelöltek problémalátó és problémaalkotó képességét. A tanítás során való alkalmazási lehetőségük jelentős, hiszen a specializálás számos versenyfeladat konstruálását teszi lehetővé. A versenyfeladatok általánosításai, a főiskolai tananyagból ismert mélyebb tételek, módszerek speciális esetei vezethetnek olyan elemi problémákra, amelyek középiskolai, esetenként általános iskolai ismeretek birtokában megközelíthetők.

Úgy véljük, hogy a fenti gondolatokat egy konkrét matematikai példával támaszthatjuk alá leginkább. A következőkben egy középiskolai tanulmányi versenyfeladat általánosítását fogalmazzuk meg és a megoldás gondolatmenetét ismertetjük.

Egy versenyfeladat általánosítása

Egy n ($n > 1$) napig tartó sportversenyen m db érmet osztottak ki. Első nap 1 érmet és a megmaradó érmék $\frac{1}{a}$ -ad része került kiosztásra ($a > 1$), a másodikon 2 érmet, s a még fennmaradók $\frac{1}{a}$ -ad része és így tovább. Végül az n -edik, azaz utolsó napon kiosztották a még visszamaradt pontosan n darab érmét. Hány napig tartott a sportverseny és hány érmét osztottak ki összesen?

Megoldás. Vizsgáljuk meg az egyes napokon megmaradó érméket. Az első nap után:

$$(m - 1) \frac{a - 1}{a}$$

érem maradt. A második nap után:

$$\left((m - 1) \frac{a - 1}{a} - 2 \right) \frac{a - 1}{a}$$

érem maradt. A harmadik nap után:

$$\left(\left((m-1) \frac{a-1}{a} - 2 \right) \frac{a-1}{a} - 3 \right) \frac{a-1}{a}$$

érem maradt.

Az $(n-1)$ -edik nap után n érem maradt. A fentiekből a következő egyenletet kapjuk:

$$(1) \quad \left(\left((m-1) \frac{a-1}{a} - 2 \right) \frac{a-1}{a} \dots - (n-1) \right) \frac{a-1}{a} = n$$

Az egyenletet a következő alakba írhatjuk:

$$(2) \quad m \left(\frac{a-1}{a} \right)^{n-1} - 1 \left(\frac{a-1}{a} \right)^{n-1} - 2 \left(\frac{a-1}{a} \right)^{n-2} - \\ - 3 \left(\frac{a-1}{a} \right)^{n-3} - \dots - (n-1) \left(\frac{a-1}{a} \right) = n$$

A (2) egyenlet mindkét oldalát szorozzuk meg $\left(\frac{a}{a-1} \right)^{n-1}$ -nel

$$(3) \quad m - 1 - 2 \left(\frac{a}{a-1} \right) - 3 \left(\frac{a}{a-1} \right)^2 - \\ - \dots - (n-1) \left(\frac{a}{a-1} \right)^{n-2} = n \left(\frac{a}{a-1} \right)^{n-1}$$

m -re a (3)-ból a következőt kapjuk:

$$(4) \quad m = 1 + 2 \left(\frac{a}{a-1} \right) + 3 \left(\frac{a}{a-1} \right)^2 + \\ + \dots + (n-1) \left(\frac{a}{a-1} \right)^{n-2} + n \left(\frac{a}{a-1} \right)^{n-1}$$

Észrevehetjük, hogy az egyenlet jobb oldalán az

$$1 + 2x + 3x^2 + \dots + nx^{n-1} = f(x)$$

függvény $x = \frac{a}{a-1}$ ($a > 2$) helyen vett értéke áll. Állítsuk elő $f(x)$ -et egyszerűbben.

A mértani sorozat összegképletét alkalmazva:

$$\begin{aligned}
 1 + x + x^2 + \dots + x^{n-1} &= \frac{x^n - 1}{x - 1}, \quad \text{ha } x \neq 1 \\
 x + x^2 + \dots + x^{n-1} &= x \frac{x^{n-1} - 1}{x - 1} = \frac{x^n - x}{x - 1} \\
 x^2 + \dots + x^{n-1} &= x^2 \frac{x^{n-2} - 1}{x - 1} = \frac{x^n - x^2}{x - 1} \\
 &\vdots \\
 &\vdots \\
 x^{n-1} &= x^{n-1} \frac{x - 1}{x - 1} = \frac{x^n - x^{n-1}}{x - 1}
 \end{aligned}$$

Adjuk össze a fenti egyenlőségeket, a jobb oldalon a lehetséges kiemelések után kapjuk:

$$f(x) = 1 + 2x + 3x^2 + \dots + nx^{n-1} = \frac{1}{x-1} \left(nx^n - \frac{x^n - 1}{x-1} \right)$$

A jobb oldalt tovább alakítva:

$$f(x) = \frac{1}{x-1} \left(\frac{nx^{n+1} - nx^n - x^n + 1}{x-1} \right) = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2}$$

Behelyettesítve az $x = \frac{a}{a-1}$ értéket (4)-ből a következő adódik.

$$(5) \quad m = \frac{n \left(\frac{a}{a-1} \right)^{n+1} - (n-1) \left(\frac{a}{a-1} \right)^n + 1}{\left(\frac{a}{a-1} - 1 \right)^2} = \frac{a^n(n-a+1)}{(a-1)^{n-1}} + (a-1)^2$$

Az m egész szám, ezért $\frac{a^n(n-a+1)}{(a-1)^{n-1}}$ -nek is egész számnak kell lennie.

Mivel a és $(a-1)$ relatív prímek, ez csak úgy lehet, ha $\frac{n-(a-1)}{(a-1)^{n-1}}$ is egész szám. Megmutatjuk, hogy $n = a-1$ és $m = (a-1)^2$.

Minden $n > 1$ természetes számra és $a > 1$ rögzített természetes számra:

$$n - a < a^{n-1}$$

Teljes indukcióval bizonyítjuk állításunkat: $n = 1$, esetén $1 - a < a^0 = 1$, mert $a > 1$.

Tegyük fel, hogy $n = k$ -ra $k - a < a^{k-1}$ szorozzuk a -val az egyenlőtlenség mindkét oldalát $ak - a^2 < a^{(k-1)+1} = a^k$.

Mivel $(k + 1)a - a^2 < ak - a^2$, ha $k \geq 1$, ezért méginkább

$$(k + 1) - a < a^{(k+1)-1}.$$

Tehát $\frac{n - (a - 1)}{(a - 1)^{n-1}}$, csak akkor lehet egész szám, ha $n = a - 1$, de ekkor viszont $m = (a - 1)^2$.

Megjegyzések

Specializálással a fenti általánosított feladatra támaszkodva olyan feladatokat készíthetünk, amelyek középiskolai, illetve általános iskolai ismeretek felhasználásával megoldhatók.

1. Ha $a = 7$, akkor egy középiskolai versenyfeladatot kapunk, amelynek megoldása azonnal adódik, $n = 6$ és $m = 36$.
2. Ha $a = 9$, akkor a következő általános iskolai versenyfeladatot fogalmazhatjuk meg:

Egy kis csapat szilvát kapott a táborban uzsonnára. A csapat vezetője úgy osztja szét a tagok között a szilvát, hogy az elsőnek ad egy szilvát és a megmaradt szilvák 9-ed részét, a másodiknak két szilvát és a megmaradt szilvák 9-ed részét, a harmadiknak három szilvát és a megmaradt szilvák 9-ed részét stb. Az utolsó részt a vezető magának tartotta meg. Csodálkozva látták a csapat tagjai, hogy mindenki egyenlően kapott a szilvából.

Hány szilvát kapott a csoport? Hányan voltak? Hány szilvát kapott egy-egy gyerek?

3. Ha $n = 4$ és $a = 5$, akkor konstruálhatunk egy újabb elemi problémát. Egy iskola tanulói 4 napos gyalogtúrán vettek részt. Az első nap megtettek 1 km-t és a hátralévő út $\frac{1}{5}$ részét. A második nap 2 km-t és a még hátralévő út $\frac{1}{5}$ részét. A harmadik nap 3 km-t és az azután megmaradt út $\frac{1}{5}$ részét. A negyedik nap 4 km-t gyalogoltak. Hány km-t gyalogoltak a négy nap folyamán?
4. Függetlenül a jelölésektől számos hasonló feladat adódik még. Például: Egy ékszerész hétfőn eladta drágaköveinek felét és még 4 darabot. Kedden a maradék felét és még 2 darabot. Szerdán 5 darabot. Csütörtökön kettő hóján a maradék felét. Így 8 darab drágakő maradt. Hány darab drágakő volt hétfőn reggel?

Irodalom

- [1] DR. CZEGLÉDY ISTVÁN: Matematika tantárgypedagógia I. *Calibra*, Budapest, 1994.
- [2] KOSZTOLÁNYI—MIKE—VINCZE: Érdekes matematikai feladatok. *Mozaik Oktatási Stúdió*, Szeged, 1992.
- [3] KOSZTOLÁNYI—MIKE—POLÁNKAINÉ—SZEDERKÉNYINÉ—VINCZE: Matematika összefoglaló feladatgyűjtemény 10—14 éveseknek. *Mozaik Oktatási Stúdió*, Szeged, 1994.
- [4] MOLNÁR E.: Matematikai versenyszenyfeladatok gyűjteménye. *Tankönyvkiadó*, Budapest, 1989.
- [5] PÓLYA GYÖRGY: A problémamegoldás iskolája I—II. *Tankönyvkiadó*, Budapest, 1971.
- [6] PÓLYA GÖRGY: A gondolkodás iskolája. *Tankönyvkiadó*, Budapest, 1970.

A geometriai térszemlélet fejlesztése tárgyi modellek alkalmazásával

SZILÁK ALADÁRNÉ

Abstract. La skribleciono demonstracias kelkajn eblecojn evoluigo de vidmanero de la geometria kampo. La modellecioj pretiĝis pro 5—8. klasaj lernantoj. Ĉiu lecionon bazas sur efektivaĵa aktiveco, kaj pretendas uzadon de tiaj instrumentoj, modeloj, kiujn ankaŭ la lernantoj povas pretigi.

A Nemzeti alaptanterv (NAT) matematikára vonatkozó általános fejlesztési követelményei között szerepel a térszemlélet fejlesztése is. Ugyanis a geometria tanításában sok problémát jelent az, hogy a tanulóknak nincs megfelelő térszemléletük. E követelményhez kapcsolódó részletes tananyagot a helyi tantervek tartalmazzák.

A taneszközök (nyomtatott taneszközök, tanulókírási eszközök stb.) megfelelő kiválasztása és használata tekintetében pedig a matematikát tanító tanárnak kell döntenie. Az alábbiakban ehhez az összetett munkához szeretnék segítséget nyújtani.

Mit is értsünk térszemléleten? Válaszként Kárteszi Ferenc **tágabb értelmezését** idéznék: „A matematikai tér nem összevisszaságok szövevénye, hanem **meghatározott rend szerint** épül fel (testek, alakzatok, kölcsönös helyzetük, alak, méret stb.), és ezt a **rendet kell megtanítani**, vagyis fel kell készíteni a tanulókat arra, hogy **elgazodjanak benne**.”

A térszemléletnek igen fontos összetevője a **térlátás képessége**, melynek alapja az az **adottság**, mely az emberrel született tulajdonság. Ezt kialakítani nem lehet, de fejleszteni igen. A tantervi előírások mellett így adódik a tanár számára a térszemlélet fejlesztése, mint cél és feladat.

Hogyan lehet térszemléletet fejleszteni?

Röviden úgy foglalhatnánk össze, hogy **tárgyi tevékenységből kiindulva, tapasztalatszerzés útján** („Amit hallunk, azt elfelejtjük, amit látunk, arra emlékszünk, amit teszünk, azt tudjuk.”). Próbáljuk meg a teret kézzel foghatóan bemutatni, modellekkel ábrázolni! Egy lehetséges megközelítésként a következőket vehetjük figyelembe: Az emberi test, az érzékszervek, az emberi mozgások és a nehézségi erő együttes hatása az, hogy az ember szemléletében három sík állása különös szerepet tölt be. A **vízszintes-sík** (mint a padló), a **homlok-sík** (mint a szemközti fal), az **oldal-sík** (mint

az oldal-fal) állásához viszonyítva szemlélünk mindent. Szemléletünknek ez a természete a térgeometriai ismereteink kialakulásában nagy jelentőségű. Ezért a kocka aprólékos, türelmes tanulmányozása alakíthatja a 8—12 éves korú tanulók térszemléletét a legeredményesebben.

Az alábbi mintafeladatsor 5—6. osztályosok számára készült. Mindegyik feladat a kockához kapcsolódva tárgyi tevékenységre alapoz, olyan eszközök használatát, modellek elkészítését igényli, amelyet a tanulók maguk is elkészíthetnek akár a tanórán, akár otthon.

Gyakorlatok a kockával

1. Három azonos élhosszúságú kockából összeállítottunk egy téglatestet, amelynek felszíne 64 cm^2 -rel lett kisebb, mint a három kocka felszínének összege.

Milyen élhosszúságúak a kockák? Mekkora a téglatest felszíne és térfogata?

2. Egy 96 cm^2 területű téglalap 3 hajtással 6 db egybevágó négyzetre osztható. Rajzlapból vágd ki a kívánt területű téglalapot, majd hajtogatással állítsd elő a 6 db négyzetet!

- Az így kapott alakzat lehet-e kocka testhálója?
- A fenti alakzataból elkészíthető-e a kocka testhálója egyetlen négyzet elmozdításával?
- Két négyzet elmozdításával kaphatjuk a kocka testhálóját? (Keress többféle megoldást!)
- A testhálóból „hajtogass” kockát! Mekkora a keletkezett test felszíne és térfogata?

3. Babylon-készletből készítsétek el egy kocka élváz-modelljét! Ha a kocka A csúcsából a G csúcsába (AG testátló) az éleken vezető különböző és legrövidebb „utak” mindegyikét végigjárjuk, akkor összesen 126 cm -t teszünk meg. (2 utat különbözőnek tekintünk akkor, ha van olyan él az egyikben — mint útszakasz — amelyik a másikban nem szerepel.)

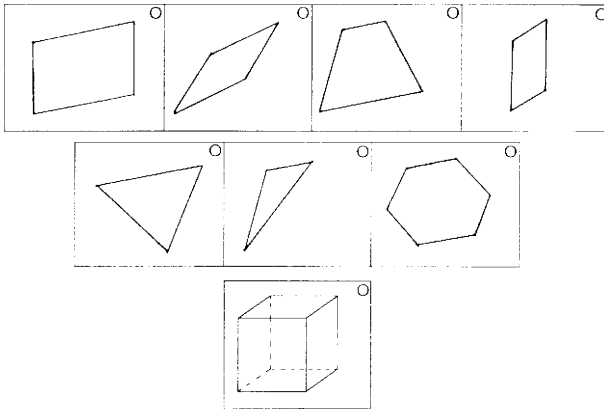
„Írjátok le” az utakat! Mekkora a kocka élei?

4. Babylon-készletből készítsétek kocka élváz-modelljét! Síktükör segítségével keressétek szimmetriasíkot a kockához! Hány szimmetriasíkja lehet?

5. Gyurmából (sajtból, almából, radírgumiból, hungarocellból) készítsétek kockát! A kapott testet vágjátok ketté! A vágások mentén milyen síkidomok keletkeztek?

6. Az átlátszó fóliákon egy-egy sokszöget láttok, melyek a mellékelt kartonra rajzolt kocka síkmetszetei (egy kivételével). Melyik síkmetszet a „kakukktójtás”?

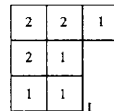
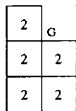
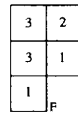
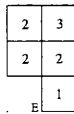
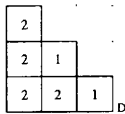
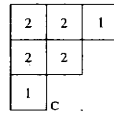
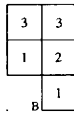
(A feladat megoldásában segítenek a fóliák, ha azokat úgy helyezed a kocka síkbeli rajzára, hogy a kis „köröcskék” — a fólián és a kartonlapon — fedjék egymást.)



7. Egy kocka élleinek felezőpontjait megjelöltük, a szomszédosakat, összekötöttük és az összekötő szakaszok mentén a kocka mindegyik sarkát „levágtuk”. Az így kapott testet milyen lapok határolják? Próbáld meg lerajzolni a testet! Hány lapja, hány csúcsa, hány éle van?

8. Tíz egyenlő nagyságú kockából építettek a gyerekek. Elkészítették az alaprajzokat is. Mindegyik négyzetre ráírták, hogy arra hány kockát tettek.

Némelyik építményről kiderült, hogy ugyanolyan, csak más lapján, más-képpen áll. Keresd és kapcsold össze ezeket! Állapítsd meg, hogy hány különböző építmény alaprajzait látod itt!



7—8. osztályban ösztönözzük a tanulókat arra, hogy a tárgyi tevékenységtől elszakadva — esetleg a modellt elképzelve, rajzzal — próbálják megoldani a hasonló feladatokat!

A geometriai konstrukciók, gyakorlatok című feladatsor — amely nemcsak kockához kapcsolódó feladatokat tartalmaz — még a 7—8. osztályos tanulók érdeklődését is felkelti. A fenti feladatokhoz képest továbblépést jelent az, ha a tapasztalataik alapján megfogalmazott sejtéseiket bizonyítani tudják, válaszaikat indokolják.

Geometriai konstrukciók, gyakorlatok

1. Hosszú papírcsíkot kössünk laza csomóra, óvatosan húzzuk meg és nyomjuk laposra!

Milyen síkidomot alkotnak a fedett részek?

Igazoljuk sejtésünket!

2. a) Téglalap alakú papírlapból hajtogassunk szabályos háromszöget!

b) Hajtsuk meg a háromszög középvonalait, majd ezek mentén hajtsuk fel a háromszög csúcsait! Milyen térbeli alakzatot kaptunk?

c) Ha négy-négy szabályos háromszögből készítünk egy-egy „kosárkát”, és egymásra fordítjuk őket, akkor egy szabályos oktaédert kapunk.

d) Töltsük ki a teret (v. képzeljük el) hézagmentesen az elkészített tetraéderekkel és oktaéderekkel!

3. a) A logikai készlet háromszöglapjaiból készítsünk szabályos tetraédert, majd vonjuk be azt papírral! Egy él mentén felvágva a papírt próbáljuk meg kivenni a testet!

b) Végezzük el a kísérletünket „nem szabályos tetraéderrel” (háromszög alapú gúla) is! Mit tapasztalunk?

4. a) Egy kocka egyik élén ül egy pók. A lehető legrövidebb útvonalat keresi, amely a kocka minden lapján áthaladva visszavezet a kiindulási ponthoz. Milyen útvonalon kell haladnia?

b) Milyen hosszú utat tesz meg a pók, ha egy 5 m élű, kocka alakú szoba egyik élének felezőpontjából indul?

c) Változik-e az útvonal, ha a pók ugyanannak az élnek egy másik pontjából indul?

Irodalom

- [1] KÁRTESZI FERENC: A kocka. Országos Neveléstudományi Intézet, Bp., 1949.

- [2] KÁRTESZI FERENC—ERDŐSI JÓZSEF: A tér megismerése. *Egyetemi Nyomda*, Bp., 1948.
- [3] Matematika 5., 6., 7., 8. (tankönyvek). Szerkesztette: Hajdú Sándor. *Calibra Kiadó*, Bp., 1993, 1994.
- [4] Nemzeti alaptanterv (vitaanyag). *Országos Közoktatási Intézet*, Bp. 1995.

Tartalom

JONES, J. P. and KISS, P., Some identities and congruences for a special family of second order recurrences	3
LIPTAI, K., An approximation problem concerning linear recurrences	11
KISS, P. and ZAY, B., A note on the prime divisors of Lucas numbers	17
MÁTYÁS F., Two problems related to the Bernoulli numbers	23
CHUNG, P. V., Multiplicative functions satisfying the equation $f(m^2 + n^2) = (f(m))^2 + (f(n))^2$	27
GRYTCZUK, A. and GRYTCZUK, J., A primality test for Fermat numbers	33
GRYTCZUK, A. and VOROBÈV, N. T., On some applications of 2×2 integral matrices	37
M. MIGNOTTE és PETHŐ A.: Az $a^n + b^n = z^3$ diofantoszi egyenletről	45
SZEPESSY B.: A taszító fixpontokról	55
FREJMAN, D., Note on Abel's result about roots of polynomials	61
KIRÁLY, B., The Lie augmentation terminals of group	63
VERES ZS.: Polinomgyűrűk	71
KISS P. és MÁTYÁS F.: A geometriai szerkeszthetőségről	77
OROSZ GY.-né: Az általánosítás mint a problémamegoldás része	89
SZILÁK A.-né: A geometriai térszemlélet fejlesztése tárgyi modellek alkalmazásával	95

