Ivan Korec

Palindromic squares for various number system bases

Mathematica Slovaca, Vol. 41 (1991), No. 3, 261--276

Persistent URL: http://dml.cz/dmlcz/131553

Math. Slovaca 41, 1991, No. 3, 261–276

PALINDROMIC SQUARES FOR VARIOUS NUMBER SYSTEM BASES

IVAN KOREC

ABSTRACT. Polynomials generating infinitely many nontrivial b-adic palindromic squares are constructed for every $b > 2$.

1. Introduction

M. Harminc in [1] considered (decadic) palindromic squares and has found several of them by a computer. He has found several nontrivial ones (in the sense explained below) and stated a problem whether there are infinitely many nontrivial palindromic squares (for the base ten). In the present paper a positive answer will be given not only for the base ten but also for all bases $b > 2$. This part, with the exception of the case $b = 5$, is contained also in [2]. Here we prove that the obtained formulae are in some (although rather weak) sense universal: They give all polynomials $g(x)$ with integer coefficients such that for all $b > 9$ and all sufficiently large integers k the values $g(b^k)$ are nontrivial b-adic palindromic squares.

2. Definition and notation

$\mathbb{Z}$ will denote the set of integers and $\mathbb{Z}[x]$ the ring of all polynomials over $\mathbb{Z}$. A polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 , \quad a_n \neq 0 ,$$

will be called reciprocal if $a_{n-i} = a_i$ for all $i = 0, 1, \ldots, n$.

The digits $0, 1, \ldots, 9$ will be used in their usual sense and for an arbitrary number system basis. Since we shall consider arbitrary number bases we shall assume that to any integer $c > 9$ a digit is also associated. (However, we shall not need these digits in explicit numerical examples.) Superscripts in parenthesis will denote repetition of the digits they belong to. When a base b is considered

AMS Subject Classification (1985): Primary 11A63. Secondary 11Y99.
Key words: Palindromic number, Number system

all sequences of digits must be understood as b-adic expansions. The same letter will be used for a (nonnegative) integer and the corresponding digit. The bar is used to distinguish the b-adic expansion $\overline{c_n c_{n-1} \dots c_1 c_0}$ from the product $c_n c_{n-1} \dots c_1 c_0$.

Definition 2.1. (i) *A positive integer will be called a b-adic palindrome ($b > 1$) if its b-adic expansion $\overline{c_n c_{n-1} \dots c_1 c_0}$ (without any leading zeros) satisfies $c_i = c_{n-i}$ for all $i = 0, 1, \dots, n$. Otherwise it will be called nonpalindromic for the base b.*

(ii) *A positive integer will be called a b-adic palindromic square if it is a square (of an integer) and simultaneously a b-adic palindrome.*

(iii) *A b-adic palindromic square $y = \overline{c_n c_{n-1} \dots c_1 c_0}$ will be called trivial if the b-adic expansion $\overline{a_n a_{n-1} \dots a_1 a_0}$ of $\sqrt{y}$ (with leading zeros if necessary) satisfies*

$$\sum_{k=0}^{i} a_k a_{i-k} = c_i \quad \textit{for all} \quad i = 0, 1, \dots, n.$$

Otherwise the b-adic palindromic square y will be called nontrivial.

For example, 121, 10201, 484, 40804, 12321, 102030201, 14641, 104060401, 44944, 404090404 are decadic palindromic squares. It is easy to construct infinitely many similar palindromic squares by inserting zeros, but they will be trivial in the above sense. (Also 1, 4, 9 are trivial palindromic squares.) Nontrivial decadic palindromic squares are e. g. $676 = 26^2$, $69696 = 264^2$, $94249 = 307^2$, $698896 = 836^2$.

The idea of (iii) is that a palindromic square is nontrivial if a carry occurs by the corresponding squaring. In [2] (and implicitly also already in [1]) a little stronger criterion of nontriviality was considered. A palindromic square was called nontrivial if its square root was not palindromic. For example, for $b = 2$ we have $1001 = 11^2$ and for $b = 7$ we have $23300332 = 4114^2$. These palindromic squares are trivial by the original definition but nontrivial by the present one. The new definition seems to be more adequate. However, palindromic squares constructed below will be nontrivial by the original definition, too. (Larger initial numerical examples must be sometimes used to obtain this property; however, $b = 5$ is not the case.)

Definition 2.2. (i) *We shall say that the polynomial $g(x) \in \mathbb{Z}[x]$ produces b-adic palindromic numbers if it is non-constant and for every sufficiently large integer k the value $g(b^k)$ is a b-adic palindromic number.*

(ii) *We shall say that the polynomial $g(x) \in \mathbb{Z}[x]$ produces /nontrivial/ b-adic palindromic squares if it is non-constant and for every sufficiently large integer k the value $g(b^k)$ is a /nontrivial/ b-adic palindromic square.*

The words "for every sufficiently large integer k" ought to be understood here as "for all k such that b^k is greater than the maximum of the absolute values of coefficients of $g(x)$".

For example, the polynomial x^2+2x+1 produces b-adic palindromic squares for every $b > 2$ and the polynomial $x^4+2x^3+3x^2+2x+1$ for every $b > 3$; however, the produced palindromic squares are trivial. The polynomials producing nontrivial palindromic squares will be given later.

3. Existence of nontrivial palindromic squares

Theorem 3.1. *Let S be a nontrivial b-adic palindromic square with all digits less than $\frac{1}{2}b$. Then the polynomial $g(x) = Sx^2+2Sx+S$ produces nontrivial b-adic palindromic squares.*

Proof. Let $C = \sqrt{S}$. Then $g(x) = (Cx+C)^2$ and hence all values of $g(x)$ (for integer x) are squares. Now let $\overline{s_n s_{n-1} \dots s_1 s_0}$ be the b-adic expansion of S and $k > n$. Denote $t_i = 2s_i$ for all $i = 0, \dots, n$; obviously $t_i < b$. Then the b-adic expansion of $g(b^k)$ is

$$\overline{s_n s_{n-1} \dots s_1 s_0 0 \dots 0 t_n t_{n-1} \dots t_1 t_0 0 \dots 0 s_n s_{n-1} \dots s_1 s_0},$$

where both groups of zeros $0 \dots 0$ have the same length $k-n-1$. It is easy to see that this expansion represents a nontrivial palindromic square.

Corollary 3.2. *For every base $b \in \{3,5,6,7,8,9\}$ there are infinitely many nontrivial b-adic palindromic squares.*

Proof. We use the previous theorem. The appropriate palindromic squares (which were found by a computer in most cases) are e. g.

$$\begin{aligned}
&11111 = 102^2 \quad \text{for} \quad b=3,\\
&102201 = 231^2 \quad \text{for} \quad b=6,\\
&10212212221000111212121211100012221221201 =\\
&\qquad = 10103022121232414134 4^2 \quad \text{for} \quad b=5,\\
&202 = 13^2 \quad \text{for} \quad b=7,\\
&112011331102111 = 3025303^2 \quad \text{for} \quad b=8,\\
&430101034 = 20657^2 \quad \text{for} \quad b=9,
\end{aligned}$$

Notice once more that b-adic expansions are used when the base b is considered.

For the case $b = 2$ the above method obviously does not work. The author still does not know whether nontrivial palindromic squares suitable for this method exist for the bases $b = 4$ and $b = 10$ (ten). However, these cases will be solved by another methods, one for $b = 4$ and another for all $b > 7$. (Hence for the cases $b = 8$ and $b = 9$ two constructions of nontrivial palindromic squares are given.)

Theorem 3.3. *For the base $b = 4$ the polynomial*

$$g(x) = 100x^4 + 100x^3 - 10x^2 - 10x + 1$$

produces nontrivial 4-adic palindromic squares. (In the coefficient of $g(x)$ the base 4 is used!)

P r o o f. Since $g(x) = \left(10x^2 + 2x - 1\right)^2$ the values of $g(x)$ for all integers x are squares. Further, it can be easily seen that for every $n > 0$ the 4-adic expansion of $g(4^n)$ is

$$10^{(n)}3^{(n)}23^{(n)}0^{(n)}1 = (10^{(n)}13^{(n)})^2,$$

and it is obviously a nontrivial 4-adic palindrome.

Theorem 3.4. *Let*

$$f_1(x) = x^{2r} + x^{2r-s} + x^{r+s} - x^r + x^{r-s} + x^s + 1\,, \tag{F.1}$$

$$f_2(x) = f_1(x) + x^{2r-2s} + x^{2s}\,, \tag{F.2}$$

$$f_3(x) = f_1(x) + x^{3r/2} + x^{r/2}\,, \tag{F.3}$$

$$f_4(x) = f_1(x) + x^{r+s/2} + x^{r-s/2}\,, \tag{F.4}$$

$$f_5(x) = f_1(x) + x^{3r/2-s/2} + x^{r/2+s/2}\,, \tag{F.5}$$

where the integers r, s satisfy the conditions $r > 2s > 0$ and, moreover,

$r \neq 3s$ for $f_2(x)$,
r is even for $f_3(x)$,
s is even for $f_4(x)$,
$r + s$ is even and $r \neq 3s$ for $f_5(x)$.

Let $g_i(x) = f_i^2(x)$ for $i = 1, \dots, 5$. Then for every $i = 1, \dots, 5$ and every base $b > 9$ the polynomial $g_i(x)$ produces nontrivial b-adic palindromic squares. Further, for $i = 1$ the same holds also for $b = 8$ and $b = 9$.

P r o o f. By an easy computation we obtain

$$\begin{aligned} g_1(x) = {} & x^{4r} + 2x^{4r-s} + x^{4r-2s} + +2x^{3r+s} + \\ & + 2x^{3r-2s} + x^{2r+2s} + 7x^{2r} + x^{2r-2s} + \\ & + 2x^{r+2s} + 2x^{r-s} + x^{2s} + 2x^s + 1\,, \end{aligned} \tag{G.1}$$

$$
\begin{aligned}
g_2(x) = {} & x^{4r} + 2x^{4r-s} + 3x^{4r-2s} + 2x^{4r-3s} + \\
& + x^{4r-4s} + 2x^{3r+s} + 2x^{3r-s} + 2x^{3r-3s} + \\
& + 3x^{2r+2s} + 2x^{2r+s} + 9x^{2r} + 2x^{2r-s} + \\
& + 3x^{2r-2s} + 2x^{r+3s} + 2x^{r+s} + 2x^{r-s} + \\
& + x^{4s} + 2x^{3s} + 3x^{2s} + 2x^{s} + 1 ,
\end{aligned} \tag{G.2}
$$

$$
\begin{aligned}
g_3(x) = {} & x^{4r} + 2x^{4r-s} + x^{4r-2s} + 2x^{7r/2} + \\
& + 2x^{7r/2-s} + 2x^{3r+s} + x^{3r} + 2x^{3r-3s} + \\
& + 2x^{5r/2+s} + 4x^{5r/2-s} + x^{2r+2s} + 9x^{2r} + \\
& + x^{2r-2s} + 4x^{3r/2+s} + 2x^{3r/2-s} + \\
& + 2x^{r+2s} + x^{r} + 2x^{r-s} + 2x^{r/2+s} + \\
& + 2x^{r/2} + x^{2s} + 2x^{s} + 1 ,
\end{aligned} \tag{G.3}
$$

$$
\begin{aligned}
g_4(x) = {} & x^{4r} + 2x^{4r-s} + x^{4r-2s} + 2x^{3r+s} + \\
& + 2x^{3r+s/2} + 4x^{3r-s/2} + 2x^{3r-3s/2} + \\
& + 2x^{3r-2s} + x^{2r+2s} + 2x^{2r+3s/2} + x^{2r+s} + \\
& + 9x^{2r} + x^{2r-s} + 2x^{2r-3s/2} + x^{2r-2s} + \\
& + 2x^{r+2s} + 2x^{r+3s/2} + 4x^{r+s/2} + \\
& + 2x^{r-s/2} + 2x^{r-s} + x^{2s} + 2x^{s} + 1 ,
\end{aligned} \tag{G.4}
$$

$$
\begin{aligned}
g_5(x) = {} & x^{4r} + 2x^{4r-s} + x^{4r-2s} + 2x^{7r/2-s/2} + \\
& + 2x^{7r/2-3s/2} + 2x^{3r+s} + x^{3r-s} + \\
& + 2x^{3r-2s} + 4x^{5r/2+s/2} + 2x^{5r/2-3s/2} + \\
& + x^{2r+2s} + 9x^{2r} + x^{2r-2s} + 2x^{3r/2+3s/2} + \\
& + 4x^{3r/2-s/2} + 2x^{r+2s} + x^{r+s} + 2x^{r-s} + \\
& + 2x^{r/2+3s/2} + 2x^{r/2+s/2} + x^{2s} + 2x^{s} + 1 ,
\end{aligned} \tag{G.5}
$$

Hence $g_i(x) \quad (i = 1, \dots, 5)$ are polynomials with nonnegative coefficients. Since $f_i(x)$ are reciprocal $g_i(x)$ are also reciprocal. Since $f_i(x)$ has only 9 (for $i = 1$ only 7) nonzero coefficients, and they are equal ± 1, the coefficients of $g_i(x)$ do not exceed 9 (or 7 for $i = 1$). Notice that we must not conclude this fact immediately from (G.1)–(G.5) because exponents occurring there need not be pairwise distinct for all admissible values of r, s.

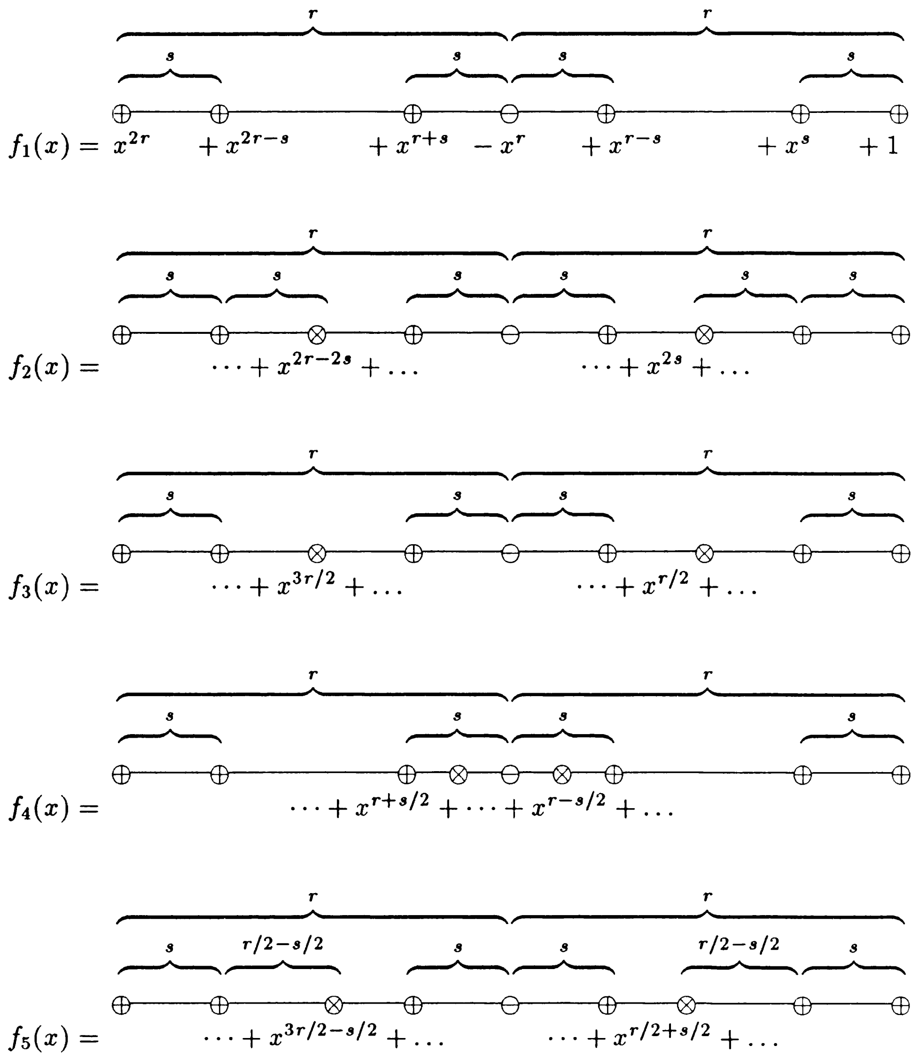

Fig. 1. Scheme of the polynomials $f_i(x)$ from Theorem 3.4.

The polynomials $f_1(x)$–$f_5(x)$ are displayed schematically in Figure 1. The symbols $\oplus$, $\ominus$ are used for the members of $f_1(x)$, the symbol $\otimes$ for the remaining members of $f_2(x)$–$f_5(x)$. If $r = 4s$ then $f_2(x) = f_3(x)$ and several further similar implications hold. However, we can see that the formulae (F.1)–(F.5) are independent in the following sense: For every of them there is a polynomial which can be obtained only from this one (by an admissible choice of r, s).

R e m a r k. Let us forget for a moment the condition $r > 2s > 0$ and assume only $r > s > 0$. Let us substitute $r - s$ by s in (F.2)–(F.5). Then the polynomials $f_2(x)$, $f_3(x)$ remain unchanged and the polynomials $f_4(x)$, $f_5(x)$ are interchanged. In this sense $f_5(x)$ is unnecessary.

4. Auxiliary results

Here several results are given which will be useful in the proof of a converse of Theorem 3.3.

Lemma 4.1. *Let $K > 1$, $n \geq 0$ and let $a_n, a_{n-1}, \dots, a_1, a_0, a_{-1}, \dots$ be reals such that the series $h(x) = \sum_{k=0}^{\infty} a_{n-k}x^{n-k}$ converges for all $x \geq K$. Let for every integer $z \geq b_0$ the value $h(z)$ be an integer. Then $h(x)$ is a polynomial, i. e. $a_{n-k} = 0$ for all $k > n$.*

P r o o f. By induction with respect to n. For $n = 0$ we obviously have $\lim_{z\to\infty} h(z) = a_0$. Hence all but finitely many members of the sequence $h(K)$, $h(K+1)$, $h(K+2), \dots$ are equal to a_0. This gives $h(x) = a_0$.

For $n > 0$ consider the function $h_1(x) = h(x+1) - h(x)$ and the corresponding infinite series $\sum_{k=0}^{\infty} b_{n-k}x^{n-k}$ which also converges for all $x \geq K$; to construct it we use

$$(x+1)^{-1} = x^{-1} - x^{-2} + x^{-3} - x^{-4} + \dots$$

Then obviously $b_n = 0$, and hence the inductive assumption can be used. Hence $h_1(x)$ is a polynomial. However, for $x > K$ we have

$$h(x) = h(K) + \sum_{j=K}^{x-1} \big(h(j+1) - h(j)\big) = h(K) + \sum_{j=K}^{x-1} h_1(x),$$

hence $h(x)$ is a polynomial, too.

R e m a r k. The coefficients of $h(x)$ need not be integers, as we can see on the example $h(x) = \frac{1}{2}x(x+1)$. For more details see [4], VIII, ex. 85 in Chapter 2.

Lemma 4.2. *If $K > 1$ and the values of a polynomial $g(x) \in \mathbb{Z}[x]$ for all integers $x \geq K$ are squares then the polynomial $g(x)$ is also a square, i.e., there is $f(x) \in \mathbb{Z}[x]$ such that $g(x) = f^2(x)$.*

P r o o f. Consider the function $h(x) = \sqrt{g(x^2)}$ and its Laurent series $\sum_{k=0}^{\infty} a_{n-k}x^{n-k}$, where n is the degree of $g(x)$. (The coefficients a_{n-k} are obviously real; only later we shall see that they are integer.) This series satisfies the conditions of Lemma 4.1 (with a suitable K) and therefore $h(x)$ is a polynomial. We can easily check (also before applying Lemma 4.1) that $a_{n-k} = 0$ for all odd k. Therefore there is a polynomial $f(x)$ such that

$$h(x) = f(x^2) \quad \text{if } n \text{ is even} \quad \text{and} \quad h(x) = x \cdot f(x^2) \quad \text{if } n \text{ is odd.}$$

If the second case takes place we have $g(x^2) = x^2 \cdot f^2(x^2)$ and hence $g(x) = x \cdot f^2(x)$. Now choose a nonsquare integer $x > K$ such that $g(x) > 0$. Then $g(x)$ is a square but $x \cdot f^2(x)$ is not a square (of any rational number). This contradiction excludes the second case.

In the first case we have $g(x^2) = f^2(x^2)$, and hence $g(x) = f^2(x)$. Now $f(x) \in \mathbb{Z}[x]$ easily follows from the Gauss lemma about the product of primitive polynomials, see e. g. [3].

R e m a r k. At the 9th Czechoslovak Colloquium on Number Theory (Račkova Dolina, September 1989) A. S c h i n z e l notices that Lemma 4.2 above is known in essential, resp. it is a consequence of a more general result. Therefore its proof was only outlined here. See also [5] in this volume.

Theorem 4.3. *Let* $b_0 \geq 2$ *and let*

$$g(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0 \in \mathbb{Z}[x],$$

where $n > 0$ *and* $c_n > 0$. *Then the polynomial* $g(x)$ *produces* b*-adic palindromes for every* $b \geq b_0$ *if and only if*

either $g(x)$*is reciprocal and all its coefficients are nonnegative and less than* b_0
or $g(0) = -1, \quad -1 \leq c_i = c_{n-i} \leq 1$ *for all* $i = 0, \dots, n$ *and between every two positive coefficients of* $g(x)$ *there is a negative one.*

P r o o f. To prove the direct implication, choose $b = 2.\max(|c_0|, \dots, |c_n|) + 3$ and $k \geq 3$ such that

$$g(b^k) = \overline{a_m a_{m-1} \dots a_1 a_0}\,, \quad a_m \neq 0,$$

is a b-adic palindrome. For every $i = 1, \dots, n$ denote by $\mathrm{nz}(i)$ the greatest $j < i$ such that $c_j \neq 0$; such j exists because $c_0 \neq 0$. Obviously $m = kn - 1$ if and only if $c_n = 1$ and $c_{\mathrm{nz}(n)} < 0$; otherwise $m = kn$. Now distinguish two cases.

Case I. *All coefficients of $g(x)$ are nonnegative.* Then we have $a_{ki} = c_i$ for all $i = 0, \dots, n$, and all remaining a_j are zeros. Since $g(b^k)$ is a b-adic palindrome and $m = kn$ we have

$$c_j = a_{kj} = a_{kn-kj} = c_{n-j} \quad \text{for all} \quad j = 0, \dots, n,$$

and hence $g(x)$ is reciprocal.
Now consider the base $b_1 = \max(c_n, c_{n-1}, \dots, c_0)$ and assume that

$$g(b_1^2) = \overline{d_s d_{s-1} \dots d_0}, \quad d_s \neq 0$$

is a b_1-adic palindrome. There holds $d_0 \neq 0$ and hence $c_0 < b_1$. Then also $c_s < b_1$ and hence $s = 2n$. Consider the greatest j such that $c_j = b_1$. Then also $= c_{n-j-1} = c_{j+1} < b_1$ and hence we have

$$d_{2j+1} = 1, \quad d_{2j} = 0, \quad d_{2n-2j-1} = 0, \quad d_{2n-2j-2} = c_{j-1}.$$

Hence $d_{2j+1} \neq d_{2n-2j+1}$, and $g(b_1^2)$ is not a b_1-adic palindrome. This contradiction shows that $b_1 < b_0$.

Case II. *At least one coefficient of $g(x)$ is negative.* Find the smallest $i \geq 0$ such that $c_i < 0$ and the greatest $j \leq m$ such that $c_j \neq 0$ and $c_{\mathrm{nz}(j)} < 0$. Then a_{kj+k-1}, a_{ki} are the leftmost and the rightmost digits of $g(b^k)$ which are greater than $\frac{1}{2}b$. Therefore

$$a_{kj+k-1} = a_{ki} \qquad \text{and} \qquad m = (kj + k - 1) + ki.$$

It is possible only if $m = kn - 1$. Now we can divide $\overline{a_m a_{m-1} \dots a_1 a_0}$ into n segments of length k; let us number them from the right side to the left. Every segment consists either of digits greater than $\frac{1}{2}b$ or of digits less than $\frac{1}{2}b$. The rightmost digit (and also every inner one) of the jth segment is either 0 or $b-1$; it depends on the sign of $c_{\mathrm{nz}(j)}$. Since $g(b^k)$ is a b-adic palindrome the same holds also for the leftmost digits. Hence every segment is either $0^{(k)}$ or $(b-1)^{(k)}$. This implies that all nonzero coefficients of $g(x)$ are ± 1 and that for every $j = 1, \dots, n$ $c_j \neq 0$ implies $c_{\mathrm{nz}(j)} = -c_j$. It remains to show that $c_{n-i} = -c_i$; it can be done easily using once more that $g(b^k)$ is a b-adic palindrome.

To prove the converse implication assume $b \geq b_0$, $k > 0$ and distinguish the same two cases as above. In the first case the coefficients of $g(x)$ become also the digits of $g(b^k)$; for $k > 0$ the block $0^{(k-1)}$ ought to be inserted between every two neighbour ones. Since $g(x)$ is reciprocal the value $g(b^k)$ is a b-adic palindrome. In the second case we obtain a palindrome consisting of blocks $0^{(k)}$ and $(b-1)^{(k)}$.

Lemma 4.4. *If $f(x) \in \mathbb{Z}[x]$, the polynomial $g(x) = f^2(x)$ is reciprocal and all its coefficients are nonnegative then the polynomial $f(x)$ is also reciprocal.*

Proof. If $f(x)$ is a constant polynomial the statement is trivial; assume that $f(x)$ has degree $n > 0$. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$
$$g(x) = c_{2n}x^n + c_{2n-1}x^{n-1} + \cdots + c_1 x + c_0 .$$

Then we have

$$a_n^2 = c_{2n} = c_0 = a_0^2 ,$$
$$2a_n a_{n-1} = c_{2n-1} = c_1 = 2a_0 a_1 ,$$
$$2a_n a_{n-2} + a_{n-1}^2 = c_{2n-2} = c_2 = 2a_0 a_2 + a_1^2 ,$$
$$\text{etc.}$$

From the first equation we have either $a_n = a_0$ or $a_n = -a_0$. Since $a_n \neq 0$ for $i = 1, \ldots, n$, there can be continually obtained $a_{n-i} = a_i$ in the first case and $a_{n-i} = -a_i$ in the second case However, in the second case we have $f(1) = 0$, and hence also $g(1) = 0$, which is impossible because $g(x)$ has all coefficients nonnegative. Therefore the first case take place, i.e., $f(x)$ is reciprocal.

5. Polynomials producing palindromic squares for almost all bases

Theorem 5.1. *For every $b_0 \geq 2$ and $g(x) \in \mathbb{Z}[x]$ the following conditions are equivalent:*

(i) *for every $b > b_0$ the polynomial $g(x)$ produces /nontrivial/ b-adic palindromic squares;*

(ii) *all coefficients of $g(x)$ are nonnegative and there is a reciprocal polynomial*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] ,$$

$n > 0$ and $a_n > 0$, such that $g(x) = f^2(x)$ and $\sum_{i=0}^{n} a_i^2 \leq b_0$ /and at least one coefficient of $f(x)$ is negative/.

Proof. At first assume that (ii) holds without the text in slashes, $b > b_0$ and $k > 0$. Then $g(x)$ is reciprocal and its coefficients are less than b because for every $k \leq n$ there holds

$$\sum_{i=0}^{k} a_i a_{k-i} \leq \sum_{i=0}^{k} \frac{1}{2}(a_i^2 + a_{k-i}^2) = \sum_{i=0}^{k} a_i^2 \leq \sum_{i=0}^{n} a_i^2 \leq b_0 .$$

Therefore by Theorem 4.3 the value $g(b^k)$ is a b-adic palindrome. It is obviously also a square. Further, assume that $f(x)$ has a negative coefficient. Then $b_0 \geq 4$ (more can be proved) and

$$a_i < \sqrt{b_0 - 2} \leq \frac{1}{2} b_0 \leq \frac{1}{2} b$$

for all $i = 0, \dots, n$. Therefore the sum S of digits of (the b-ary expansion of) $f(b^k)$ is greater than $f(1)$. On the other hand, the sum of digits of $g(b^k)$ is $g(1) = f^2(1) < S^2$, therefore the b-adic palindromic square $g(b^k)$ is nontrivial.

Now assume that (i) holds (at first without "nontrivial"). The values $g(b)$ for all $b > b_0$ are squares and hence by Lemma 4.2 the polynomial $g(x)$ is the square of a polynomial $f(x) \in \mathbb{Z}[x]$. Denote by n the degree of $f(x)$ and by $a_n, \dots, a_0$ its coefficients; we may assume $a_n > 0$. Then $g(0) \geq 0$ and hence by Theorem 4.3 the polynomial $g(x)$ is reciprocal and its coefficients are nonnegative and less or equal to b_0. If we consider the coefficient of x^n, we obtain $\sum_{i=0}^{n} a_i^2 \leq b_0$ and Lemma 4.4 implies that $f(x)$ is reciprocal. Further, if all coefficients of $f(x)$ are nonnegative, then for every $b > b_0$ and $k > 0$ the nonzero digits of $g(b^k)$ coincide with nonzero coefficients of $g(x)$, hence the b-adic palindromic square $g(b^k)$ is trivial. Therefore (i) implies (ii) also with the text in slashes, which completes the proof.

Theorem 5.2. *A polynomial $g(x) \in \mathbb{Z}[x]$ produces nontrivial b-adic palindromic squares for all bases $b > 9$ if and only if $g(x) = f_i^2(x)$ for some $i = 1, \dots, 5$ and some integers r, s, where $f_i(x)$ are polynomials from (F.1)–(F.5) and the parameters satisfy the conditions from Theorem 3.4.*

Proof. The "if" part is contained in Theorem 3.4. To prove the "only if" part, use Theorem 5.1. We know that $g(x) = f^2(x)$ for a reciprocal polynomial

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x], \quad a_n > 0$$

with at least one negative coefficient and such that $\sum_{i=0}^{n} a_i^2 \leq 9$. We shall look for all such polynomials. Let us call the members obtained by formal squaring of $f(x)$ shortly g-members (only in this proof). Further, call a g-member bx^m positive or negative if its coefficient b has this property.

Denote by a_n, a_p, a_q the three highest nonzero coefficients of $f(x)$, i.e., let

$$f(x) = a_n x^n + a_p x^p + a_q x^q + \dots,$$

where $n > p > q$ and the non-written members (if any) have degrees less than q. (The polynomial $f(x)$ has at least three nonzero coefficients because $a_0 = a_n > 0$ and $a_i < 0$ for some i.) By formal squaring of $f(x)$ we obtain

$$g(x) = a_n^2 x^{2n} + 2a_n a_p x^{n+p} + 2a_n a_q x^{n+q} + a_p x^{2p} + \dots,$$

where the non-written g-members have degrees less than $n+q$. The g-member $2a_n a_p^{n+p}$ cannot be added with any other g-member (for any admissible choice of p, q) and therefore the coefficient $2a_n a_p$ must be nonnegative, and hence obviously positive. Therefore $a_p > 0$. Since the polynomial $f(x)$ is reciprocal and has a negative coefficient we have $p > n-p$ and therefore

$$a_n^2 + a_p^2 + a_{n-p}^2 + a_0^2 \le a_0^2 + a_1^2 + \cdots + a_n^2 \le 9 .$$

Hence $a_n^2 + a_p^2 \le 4$, which implies $a_n = a_p = 1$.

Now we prove $a_q > 0$. Let, on the contrary, $a_q < 0$. Consider the coefficients of g-members of degree $n+q$. One of them is $2a_n a_q \le -2$ and the only further one can be $a_p^2 = 1$. Their sum is negative, which contradicts the required properties of $g(x)$. Therefore $a_q > 0$.

We have proved that the three highest nonzero coefficients a_n, a_p, a_q of $f(x)$ (and then also its three lowest nonzero coefficients a_{n-q}, a_{n-p}, a_0) are positive. Further, $f(x)$ has a negative coefficient, i. e. together at least seven nonzero coefficients. Since the sum of their squares does not exceed 9 they all must be equal ± 1, and their number cannot exceed 9.

Now we shall show that $f(x)$ cannot have two or more negative coefficients. Assume the contrary. By the above consideration $f(x)$ has at most 9 nonzero coefficients etc., therefore there holds

$$f(x) = x^n + x^p + x^q - x^s + ax^r - x^{n-s} + x^{n-q} + x^{n-p} + 1$$

for some integers p, q, r, s, a satisfying $n > p > q > s > \frac{1}{2}n$, $-1 \le a \le 1$ and if $a \ne 0$ then $r = \frac{1}{2}n$ (particularly, n is even in this case).

Assume $a \le 0$ at first. Then $f(1) \le 4$, $g(1) \le 16$, and therefore the sum of coefficients of $g(x)$ is at most 16. However,

$$g(x) = x^{2n} + 2x^{n+p} + 2x^{n+q} + \cdots + (8 + a^2) \cdot x^n + \cdots + 2x^{n-q} + 2x^{n-q} + 1 ,$$

the degrees of negative g-members are distinct from the degrees of g-members explicitly written and all coefficients of $g(x)$ are nonnegative. Therefore the sum of coefficient of $g(x)$ is at least 18 which is a contradiction. Hence the case $a \le 0$ is excluded.

Now assume $a = 1$ (and hence $n = 2r$). All mixed g-members (i.e., those of the form $2AB$, where A, B are distinct members of $f(x)$) which have a degree greater than $2r$, are given in Table 1. Its heading column contains all members of $f(x)$ but its heading row contains only those of degree greater than r. In both cases their degrees are in descending order. This induces the descending order of degrees of g-members in every row and in every column of Table 1.

	x^{2r}	x^p	x^q	$-x^s$
x^{2r}				
x^p	$2x^{2r+p}$			
x^q	$2x^{2r+q}$	$2x^{p+q}$		
$-x^s$	$-2x^{2r+s}$	$-2x^{p+s}$	$-2x^{q+s}$	
x^r	$2x^{3r}$	$2x^{p+r}$	$2x^{q+r}$	$-2x^{r+s}$
$-x^{2r-s}$	$-2x^{4r-s}$	$-2x^{2r+p-s}$	$-2x^{2r+q-s}$	
x^{2r-q}	$2x^{4r-q}$	$2x^{2r+p-q}$		
x^{2r-p}	$2x^{4r-p}$			
1				

Table 1. The mixed g-members of degree greater than $2r$ for $f(x)$ with two negative coefficients.

Since all coefficients of $g(x)$ ought to be nonnegative, every negative g-member in Table 1 must be cancelled with a positive one. However, $2x^{2r+p}$ and $2x^{2r+q}$ cannot be used because of their too high degrees. So the cancelling must induce a bijection between seven remaining positive g-members and seven negative ones. In this bijection $2x^{p+q}$ must correspond to $-2x^{2r+s}$ because their degrees are the highest. Then $2x^{3r}$ must correspond to $-2x^{p+s}$ for a similar reason. So we have

$$p + q = 2r + s \qquad \text{and} \qquad p + s = 3r\,.$$

From these equations we can obtain

$$p + r = 4r - s \qquad \text{and} \qquad 4r - q = 2r + p - s\,.$$

We may assume that the g-members with these exponents correspond in the bijection mentioned above. Now let us consider the g-member $2x^{q+r}$. It cannot be cancelled with any of three remaining negative g-members (because of different degrees for any admissible values of p, q, r, s). Therefore the requested bijection cannot exist, and hence the case $a = 1$ is also excluded. Now we know that $f(x)$ has exactly one negative coefficient. This fact together with other proved properties of $f(x)$ implies

$$f(x) = x^{2r} + x^p + x^q - x^r + x^{2r-q} + x^{2r-p} + 1$$

or $$f(x) = x^{2r} + x^p + x^q + x^t - x^r + x^{2r-t} + x^{2r-q} + x^{2r-p} + 1$$

for some integers p, q, r, t satisfying $2r > p > q > r > 0$ and in the second case also $2r > t > r$, $t \neq p$, $t \neq q$. (The relation $<$ or $>$ between t and p, q is not fixed on purpose.)

The negative g-member $-2x^{3r}$ must be cancelled with a positive g-member. In the first case this positive g-member must be $2x^{p+q}$; in the second case we may assume that without loss of generality. Therefore

$$p = 2r - s \qquad \text{and} \qquad q = r + s$$

for a positive integer $s < \frac{1}{2}r$. So we obtain the formula (F.1) in the first case. In the second case we have

$$f(x) = x^{2r} + x^{2r-s} + x^{r+s} + x^{t} - x^{r} + x^{2r-t} + x^{r-s} + x^{s} + 1,$$

and we have to choose t so that all coefficients of $g(x) = f^2(x)$ would be nonnegative. Therefore the negative g-member $-2x^{r+t}$ must be cancelled with a positive g-member. (See Table 2, which is organized in the same way as Table 1.)

	x^{2r}	x^{2r-s}	x^{r+s}	x^{t}
x^{2r}				
x^{2r-s}	$2x^{4r-s}$			
x^{r+s}	$2x^{3r+s}$	$2x^{3r}$		
x^{t}	$2x^{2r+t}$	$2x^{2r+t-s}$	$2x^{r+s+t}$	
$-x^{r}$	$-2x^{3r}$	$-2x^{3r-s}$	$-2x^{2r+s}$	$-2x^{r+t}$
x^{2r-t}	$2x^{4r-t}$	$2x^{4r-t-s}$	$2x^{3r+s-t}$	
x^{r-s}	$2x^{3r-s}$	$2x^{3r-2s}$		
x^{s}	$2x^{2r+s}$			
1				

Table 2. The mixed g-members of degree greater than $2r$ for $f(x)$ with one negative coefficient.

Since the g-members $2x^{3r-s}$, $2x^{2r+s}$ are used to cancel other negative g-members, $-2x^{r+t}$ must be cancelled with one of

$$2x^{3r-2s}, \qquad 2x^{4r-t}, \qquad 2x^{3r+s-t}, \qquad 2x^{4r-t-s}.$$

Therefore $r+t$ must be equal to one of the exponents of the above members, which implies

$$t = 2r - 2s, \qquad t = \frac{3r}{2}, \qquad t = r + \frac{s}{2}, \qquad t = \frac{3r}{2} - \frac{s}{2},$$

and we obtain the formulae (F.2), (F.3), (F.4), (F.5), respectively.

The parity conditions from Theorem 3.4 must be fulfilled because exponents ought to be integer. Finally, $r \neq 3s$ in (F.2) and (F.5) because otherwise we have $2r - 2s = r + s$ or $\frac{3r}{2} - \frac{s}{2} = r + s$, and $f(x)$ would have a coefficient greater than 1.

The case of trivial palindromic squares is less interesting and easier than Theorem 5.2 but we give it for the sake of completeness. Its proof will be written more briefly than that of Theorem 5.2.

Theorem 5.3. *A polynomial $g(x) \in \mathbb{Z}[x]$ produces trivial b-adic palindromic squares for all bases $b > 9$ if and only if $g(x) = f_i^2(x)$ for some $i = 6, \ldots, 9$, where*

$$f_6(x) = x^r + a_p x^{r-p} + a_q x^{r-q} + a_s x^{r-s} + \tag{F.6}$$
$$+ a_{r/2} x^{r/2} + a_s x^s + a_q x^q + a_p x^p + 1\,,$$
$$f_7(x) = 2x^r + a_{r/2} x^r + 2\,, \tag{F.7}$$
$$f_8(x) = x^{2r} + 2x^r + 1\,, \tag{F.8}$$
$$f_9(x) = x^{2r} + x^{2r-t} + 2x^r + x^t + 1\,, \tag{F.9}$$

and the integers p, q, r, s, t, a_p, a_q, $a_{r/2}$, a_s satisfy the conditions

r *is even if* $a_{r/2} \neq 0$,	$0 < p < \frac{r}{2}$ *if* $a_p \neq 0$,
$r > 0$,	$p < q < \frac{r}{2}$ *if* $a_q \neq 0$,
$0 \leq a_{r/2} \leq 1$,	$q < s < \frac{r}{2}$ *if* $a_s \neq 0$,
$0 \leq a_s \leq a_q \leq a_p \leq 1$.	

Proof. By Theorem 5.1 we know that $g(x) = f^2(x)$ for a nonconstant reciprocal polynomial with nonnegative integer coefficients. Moreover, the sum of their squares does not exceed 9. Hence the number of nonzero coefficients of $f(x)$ does not exceed 9. The formula (F.6) covers all possibilities for such $f(x)$ with all nonzero coefficients equal to 1.

Now assume that $f(x)$ has also coefficients greater than 1. Since $f(x)$ has at least two nonzero coefficients it cannot have a coefficient 3 or more. If at least two coefficients are equal 2, then $f(x)$ can have at most one further nonzero coefficient, and it must be equal to 1. This case is covered by the formula (F.7).

Finally, assume that $f(x)$ has exactly one coefficient equal to 2. It must be in the middle of the sequence of coefficients of $f(x)$ and $f(x)$ must have even number of further nonzero coefficients. This number can be either 2 or 4, and we obtain (F.8), (F.9), respectively.

Remark. The simplest polynomial obtained from Theorem 5.3 is $g(x) = (x+1)^2$. It produces b-adic (trivial) palindromic squares for all $b > 2$, while the simplest polynomial from Theorem 5.2,

$$g(x) = (x^6 + x^5 + x^4 - x^3 + x^2 + x + 1)^2$$

produces them only for $b > 7$ (however, nontrivial ones).

6. Open problems

(i) Are there infinitely many palindromic squares for the base $b = 2$?

(ii) Are there nontrivial decadic palindromic squares of all but finitely many lengths? (All nontrivial palindromic squares given by Theorem 5.2 have lengths of the form $4k+1$.)

(iii) Are there further polynomials generating nontrivial decadic palindromic squares ("independent" of those above in a suitable sense) ?

The questions (ii) and (iii) can be stated also for bases $b \neq 10$.

REFERENCES

[1] HARMINC, M.: The existence of palindromic multiples (Slovak). Matematické obzory 32 (1989), 17–24.

[2] KOREC, I.: Palindromic squares of nonpalindromic numbers in various number system bases (Slovak). Matematické obzory 33 (1989), 35–43.

[3] MAC LANE, S.—BIRKHOFF, G.: Algebra. Macmillan, New York, 1968.

[4] POLYA, G.—SZEGÖ, G.: Aufgaben und Lehrsätze aus der Analysis II.

[5] SCHINZEL, A.: A class of polynomials. Math. Slovaca 41 (1991), 295–298.

[6] SCHINZEL, A.: A personal communication at the 9th Czechoslovak Number Theory Conference. September 1989.

Received November 15, 1989

Matematický ústav SAV
Štefánikova 49
814 73 Bratislava
Czecho-Slovakia