Revista Colombiana de Matemáticas
Volumen 40 (2006), páginas 81–86

Palindromic powers

Santos Hernández Hernández*
Pontificia Universidad Católica de Chile, Santigo

Florian Luca
Universidad Nacional Autónoma de México, México D. F.

Abstract. In this paper, given an integer $a > 1$, we look at the smallest exponent n such that a^n is not a palindrome.

Keywords and phrases. Palindromes, Applications of Baker's method, Discrepancy.

2000 Mathematics Subject Classification. Primary: 11D75. Secondary: 11J25, 11J71, 11J86.

Resumen. En este artículo, dado un entero $a > 1$, nosotros estudiamos el menor exponente n tal que a^n no sea *palindromo*.

1. Introduction

A *palindrome* is a positive integer whose sequence of base 10 digits reads the same from left to right and from right to left. More generally, given any integer $b > 1$ a *base b palindrome* is a positive integer a such that if its base b representation is

$$a = a_0 + a_1 b + \ldots + a_t b^t, \qquad a_i \in \{0, \ldots, b-1\}, \qquad a_t > 0,$$

then $a_i = a_{t-i}$ holds for all $i = 0, \ldots, t$. For example, 12345678987654321 is a palindrome and $b^t + 1$ is a base b palindrome for $b > 1$ and $t \geq 1$.

Several authors have investigated the occurrence of palindromes in special sequences. For example, Korec [3] looked at palindromic squares, Harminic and Soták [2] looked at the occurrence of palindromes in arithmetical progressions and Luca [5] looked at palindromic Fibonacci numbers. In [1], it is shown that almost all palindromes are composite.

*Present address: Unidad Académica de Matemáticas, Universidad Autónoma de Zacatecas, Camino a la Bufa intersección Calzada Solidaridad, Apdo. Postal 612, C. P. 98000 Zacatecas, Zacatecas, Mexico. E-mail: shh@mate.reduaz.mx.

The Theorem on page 222 in [5] shows that if $a > 1$ is any fixed integer, then the set of n such that a^n is a base b palindrome is of asymptotic density zero. Hence, there certainly exists an n such that a^n is not a base b palindrome. It is the smallest positive integer $n := n(a, b)$ with this property that we investigate in this paper.

Note that if $a = b + 1$ and m is such that $\binom{m}{j} < b$ for all $j = 0, \ldots, m$, then all the numbers

$$a^k = (b+1)^k = \sum_{j=0}^{k} \binom{k}{j} b^j, \qquad k = 1, \ldots, m.$$

are base b palindromes. Since the inequality

$$\binom{m}{\lfloor m/2 \rfloor} \gg \frac{2^m}{\sqrt{m}},$$

holds for all positive integers m, it follows that for $a = b + 1$ we have that $n(a, b) \geq (\log b)/\log 2 + O(\log\log b)$. Here, we use log for the natural logarithm. In particular, $n(a, b)$ can be large. Further, note that $n(1, b) = \infty$, which is why we assume that $a > 1$.

In this note, we prove the following upper bound on the size of $n(a, b)$ when $a > 1$.

Theorem 1. *There exists an absolute constant C_0 such that if $a > 1$ and $b > 1$, then*

$$n(a, b) < \exp\left(C_0(\log A)^3 \log\log A\right),$$

where $A = \max\{a, b\}$.

2. Proof of Theorem 1

Proof. Let a, b and A be as in Theorem 1. We assume that $\log A > 1$ (otherwise, $a = b = 2$, and so $n(a, b) = 0$). We assume that $b > 2$ and we shall indicate at the end how to modify the proof in such a way as to deal with the case $b = 2$ also.

Given a and b we write $b = b_1 b_2$, where every prime factor of b_1 divides a and b_2 is coprime to a. It is clear that b_1 and b_2 are uniquely determined by a and b, and in particular they are coprime. Let $c \in \{0, \ldots, b-1\}$ be the number such that $c \equiv 0 \pmod{b_1}$ and $c \equiv 1 \pmod{b_2}$. The number c exists and is uniquely determined by the Chinese Remainder Theorem.

For a positive integer m let $\phi(m)$ be its Euler function. We note that the congruence

$$a^{m\phi(b)} \equiv c \pmod{b},$$

holds for all positive integers m. Indeed, note that since b_2 and a are coprime, Euler's Theorem tells us that $a^{\phi(b)} \equiv 1 \pmod{b_2}$. Hence, $a^{m\phi(b)} \equiv 1 \pmod{b_2}$ for all $m \geq 1$. We now prove that $a^{\phi(b)}$ is divisible by b_1. For this, let p be a prime factor of b_1 and assume that $p^\alpha \mid b_1$. Since $2^{n-1} \geq n$ holds for all positive integers n, we get that

$$p^{\phi(b)} \geq p^{\phi(p^\alpha)} = p^{p^{\alpha-1}(p-1)} \geq p^{p^{\alpha-1}} \geq p^{2^{\alpha-1}} \geq p^\alpha,$$

and since $p \mid a$, we get that $a^{\phi(b)}$ is a multiple of p^α. Since this is true for all prime powers p^α dividing b_1, we get that $a^{\phi(b)}$ is a multiple of b_1. Hence, $a^{m\phi(b)} \equiv 0 \pmod{b_1}$ for all $m \geq 1$. Recalling the definition of c, we conclude that

$$a^{m\phi(b)} \equiv c \pmod{b} \qquad \text{for all } m \geq 1.$$

Thus, the last base b digit of $a^{m\phi(b)}$ is c for all $m \geq 1$. In particular, if every prime factor of a divides b, then $c = 0$ and so $a^{m\phi(b)}$ cannot be a palindrome. Thus, $n(a,b) < \phi(b)$ in this case. In fact, it is easy to show that the better inequality

$$n(a,b) \leq \max\{\alpha : p^\alpha \mid b \text{ for some prime } p\},$$

is satisfied in this case.

From now on, we will assume that there exists a prime factor p of a not dividing b. In particular, $c > 0$ and $(\log a/\log b) \notin \mathbb{Q}$.

Suppose now that $a^{m\phi(b)}$ is a palindrome for $m = 1, \ldots, N$ where N is some positive integer. Then the first digit of $a^{m\phi(b)}$ is also c. Thus, for each $m = 1, \ldots, N$, there exists $n := n(m)$ such that

$$cb^n \leq a^{m\phi(b)} < (c+1)b^n.$$

Taking logarithms and dividing both sides of the resulting inequality by $\log b$ we get

$$\frac{\log c}{\log b} + n \leq m\left(\frac{\phi(b)\log a}{\log b}\right) < \frac{\log(c+1)}{\log b} + n. \tag{2.1}$$

Let $\theta = \phi(b)\log a/\log b$. Note that $\theta \notin \mathbb{Q}$. Since $1 \leq c < c+1 \leq b$, we get that $0 \leq \log c/\log b < \log(c+1)/\log b \leq 1$, therefore $n = \lfloor m\theta \rfloor$ and inequality (2.1) leads to the conclusion that

$$\{m\theta\} \in \mathcal{I} = \left[\frac{\log c}{\log b}, \frac{\log(c+1)}{\log b}\right], \qquad m = 1, \ldots, N, \tag{2.2}$$

where $N = \lfloor n(a,b)/\phi(b) \rfloor$. In the above, we used $\lfloor x \rfloor$ and $\{x\}$ for the integer part and the fractional part of x, respectively.

Recall now that the discrepancy D_N of a sequence $(a_m)_{m=1}^N$ of real numbers (not necessarily distinct) is defined as

$$D_N = \sup_{0 \leq \gamma \leq 1} \left| \frac{\#\{m \leq N \;:\; \{a_m\} < \gamma\}}{N} - \gamma \right|.$$

From the above definition we see that the inequality

$$\#\{m \leq N \;:\; \alpha \leq \{a_m\} < \beta\} \leq (\beta - \alpha)N + 2D_N N$$

holds for all $0 \leq \alpha \leq \beta \leq 1$.

Thus, setting $a_m = m\theta$ for all $m = 1, \dots, N$, containment (2.2) for $m = 1, \dots, N$ leads to the conclusion that

$$\begin{aligned} N &= \#\{m \le N : \{a_m\} \in \mathcal{I}\} \le \left(\frac{\log(c+1)}{\log b} - \frac{\log c}{\log b}\right) N + 2D_N N \\ &\le \frac{\log 2}{\log b} N + 2D_N N. \end{aligned} \tag{2.3}$$

We now bound D_N. The Koksma-Erdős-Turán inequality (see Lemma 3.2 in [4]) bounds the discrepancy D_N as

$$D_N \le \frac{3}{H} + \frac{3}{N} \sum_{m=1}^{H} \frac{1}{m\|a_m\|}, \tag{2.4}$$

where $\|x\|$ is the distance from x to the nearest integer and $H \le N$ is an arbitrary positive integer (see [7] for an even better inequality).

To bound $\|a_m\|$, note that

$$\|a_m\| = \left| m \frac{\phi(b) \log a}{\log b} - t \right| = \frac{1}{\log b} |m\phi(b) \log a - t \log b| ,$$

where t is an integer such that $t \le m\phi(b)\log a + \log b$. Note that $\|a_m\|$ is nonzero since $\theta \notin \mathbb{Q}$. Thus, $|m\phi(b)\log a - t\log b| \ne 0$ and a lower bound to it can be obtained by using the theory of linear forms in logarithms. Indeed, the main result of Matveev [6] shows that there exists an effectively computable constant $C_1 > 1$ such that

$$\begin{aligned} |m\phi(b)\log a - t\log b| &> \exp\left(-C_1 \log(2m\phi(b)\log a)\log a \log b\right) \\ &\ge \exp\left(-C_1 \log(2m)\left(1 + \frac{2\log A}{\log 2}\right)(\log A)^2\right). \end{aligned} \tag{2.5}$$

We thus get that if $H \ge 2$ and $m \le H$ then $\log(2m) \le 2\log H$ and so the inequality (2.5) leads to

$$\frac{1}{\|a_m\|} \le (\log b) H^{C_2(\log A)^3} \le (\log A) H^{C_2(\log A)^3},$$

where we can take $C_2 = 2(1 + 2/\log 2)C_1$. Thus,

$$D_N \le 3\left(\frac{1}{H} + \frac{\log A}{N} H^{C_2(\log A)^3} \sum_{m=1}^{H} \frac{1}{m}\right) \le 3\left(\frac{1}{H} + \frac{\log A}{N} H^{C_2(\log A)^3+1}\right).$$

Choosing $H = \lfloor N^{1/(C_2(\log A)^3+2)} \rfloor$ we get, assuming still that $H \ge 2$ and therefore that

$$(N^{-1/(C_2(\log A)^3+2)} - 1)^{-1} \le 2N^{1/(C_2(\log A)^3+2)},$$

that

$$D_N \le 9(\log A) N^{-1/(C_2(\log A)^3+2)},$$

which together with inequality (2.3) leads to

$$0 < \left(1 - \frac{\log 2}{\log b}\right) \leq 18(\log A)N^{-1/(C_2(\log A)^3+2)},$$

or

$$\begin{aligned} N &\leq \left(\frac{18 \log A}{1-(\log 2)/\log 3}\right)^{C_2(\log A)^3+2} \\ &\leq (54 \log A)^{C_2(\log A)^3+2} \\ &= \exp(C_3(\log A)^3(\log\log A + 2\log(54))), \end{aligned}$$

where we can take $C_3 = C_2 + 2(\log A)^{-3}$. Since $n(a,b) \leq \phi(b)N < AN$, we get the conclusion of Theorem 1 with a suitable constant C_0.

When $b = 2$, an argument similar to the one from the beginning of this proof shows that there exists $c \in \{0, 1, 2, 3\}$ such that $a^2 \equiv c \pmod 4$. We may assume of course that c is odd since if not then the last binary digit of a is zero so no power of a of positive exponent can be a binary palindrome. Thus, the last two digits of a^2 in base 2 are determined and they are either 11 or 01. Since a^{2m} is a binary palindrome for $m = 1, \ldots, \lfloor n(a,2)/2 \rfloor$, it follows that the first two binary digits of a^m are the same for all such m. Now one may apply the same argument as before based on the Koksma-Erdős-Turán inequality (2.4) and the lower bounds for the linear forms in logarithms (2.5) to get a similar upper bound for $n(a,b)$. We do not give further details here. ☑

Acknowledgments. We thank the anonymous referees for comments which improved the quality of this paper. This work was done in April of 2006, while the second author was in residence at the Centre de Recherches Mathemátiques of the Université de Montréal for the thematic year *Analysis and Number Theory.* This author thanks the organizers for the opportunity of participating in this program. The first author was supported by the Postdoctoral Fellowship MECESUP PUC-0103. The second author was also supported in part by Grants SEP-CONACyT 46755, PAPIIT IN104505 and a Guggenheim Fellowship.

References

[1] W. D. Banks, D. N. Hart & M. Sakata, Almost all palindromes are composite, *Math. Res. Lett.* **11** (2004), 853–868.

[2] M. Harminic & R. Soták, Palindromic numbers in arithmetic progressions, *Fibonacci Quart.* **36** (1998), 259–261.

[3] I. Korec, Palindromic squares for various number system bases, *Math. Slovaca* **41** (1991), 261–276.

[4] L. Kuipers & H. Niederreiter, *Uniform Distribution of Sequences*, Wiley-Interscience, New-York, 1974.

[5] F. Luca, Palindromes in Lucas sequences, *Monatsh. Math.* **138** (2003), 209–223.

[6] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers II, *Izv. Ross. Akad. Nauk. Ser. Math.* **64** (2000), 125–180; English translation *Izv. Math.* **64** (2000), 1217–1269.

[7] J. Rivat & G. Tenenbaum, Constantes d'Erdős-Turán, *Ramanujan J.* **9** (2005), 111–121.

(Recibido en mayo de 2006. Aceptado en julio de 2006)

Facultad de Matemáticas
Vicuña Mackenna 4860
Santiago, Chile
e-mail: shernand@mat.puc.cl

Instituto de Matemáticas
C.P. 58089, Morelia
Michoacán, México
e-mail: fluca@matmor.unam.mx