Prime Divisors of Palindromes

William D. Banks
Department of Mathematics, University of Missouri
Columbia, MO 65211 USA
bbanks@math.missouri.edu

Igor E. Shparlinski
Department of Computing, Macquarie University
Sydney, NSW 2109, Australia
igor@ics.mq.edu.au

Abstract

In this paper, we study some divisibility properties of palindromic numbers in a fixed base $g \ge 2$. In particular, if $\mathcal{P}_L$ denotes the set of palindromes with precisely L digits, we show that for any sufficiently large value of L there exists a palindrome $n \in \mathcal{P}_L$ with at least $(\log\log n)^{1+o(1)}$ distinct prime divisors, and there exists a palindrome $n \in \mathcal{P}_L$ with a prime factor of size at least $(\log n)^{2+o(1)}$.

1 Introduction

For a fixed integer base $g \ge 2$, consider the *base g representation* of an arbitrary natural number $n \in \mathbb{N}$:

$$n = \sum_{k=0}^{L-1} a_k(n) g^k, \qquad (1)$$

where $a_k(n) \in \{0, 1, \ldots, g-1\}$ for each $k = 0, 1, \ldots, L-1$, and the leading digit $a_{L-1}(n)$ is *nonzero*. The integer n is said to be a *palindrome* if its digits satisfy the symmetry condition:

$$a_k(n) = a_{L-1-k}(n), \qquad k = 0, 1, \ldots, L-1.$$

It has recently been shown in [1] that almost all palindromes are composite.

For any $n \in \mathbb{N}$, the number L in (1) is called the *length* of n; let $\mathcal{P}_L \subset \mathbb{N}$ denote the set of all palindromes of length L. In this paper, as in [1], we estimate exponential sums of the form

$$S_q(L;c) = \sum_{n \in \mathcal{P}_L} \mathbf{e}_q(cn),$$

where as usual $\mathbf{e}_q(x) = \exp(2\pi i x/q)$ for all $x \in \mathbb{R}$. Using these estimates, we show that for all sufficiently large values of L, there exists a palindrome $n \in \mathcal{P}_L$ with at least $(\log\log n)^{1+o(1)}$ distinct prime divisors, and there exists a palindrome $n \in \mathcal{P}_L$ with a prime factor of size at least $(\log n)^{2+o(1)}$.

Throughout the paper, all constants defined either explicitly or implicitly via the symbols O, Ω, $\ll$ and $\gg$ *may depend on* g but are absolute otherwise. We recall that, as usual, the following statements are equivalent: $A = O(B)$, $B = \Omega(A)$, $A \ll B$, and $B \gg A$. We also write $A \asymp B$ to indicate that $B \ll A \ll B$.

Acknowledgements. The authors wish to thank Florian Luca for some useful conversations. Most of this work was done during a visit by the authors to the Universidad de Cantabria; the hospitality and support of this institution is gratefully acknowledged. W. B. was supported in part by NSF grant DMS-0070628, and I. S. was supported in part by ARC grant DP0211459.

2 Preliminary Results

For every natural number q with $\gcd(q, g) = 1$, we denote by t_q the order of g in the multiplicative group modulo q. For arbitrary integers a, b, K with $K \ge 1$ we consider the exponential sums

$$T_q(a,b) = \sum_{k=1}^{t_q} \mathbf{e}_q\left(ag^k + bg^{-k}\right) \quad \text{and} \quad T_q(K;a,b) = \sum_{k=1}^{K} \mathbf{e}_q\left(ag^k + bg^{-k}\right),$$

where the inversion g^{-k} is taken in the residue ring $\mathbb{Z}_q$.

Lemma 1. *Let $\mathcal{S}$ be a set of primes coprime to g, with $\gcd(t_{p_1}, t_{p_2}) = 1$ for all distinct $p_1, p_2 \in \mathcal{S}$. Then for the integer $q = \prod_{p \in \mathcal{S}} p$ one has*

$$T_q(a,b) = \prod_{p \in \mathcal{S}} T_p(a,b).$$

Proof. Consider the Kloosterman sums

$$K_\chi(a,b;q) = \sum_{\substack{1\le c\le q\\ \gcd(c,q)=1}} \chi(c)\ \mathbf{e}_q(ac+b\overline{c})$$

as χ varies over the multiplicative characters of $\mathbb{Z}_q^*$. Denoting by X_q the group of all such characters for which $\chi(g)=1$, as in the proof of Lemma 2.1 of [1] one has

$$T_q(a,b) = \frac{t_q}{\varphi(q)} \sum_{\chi\in X_q} K_\chi(a,b;q).$$

Because of the assumed property of the set $\mathcal{S}$, we see that $t_q = \prod_{p\in\mathcal{S}} t_p$, and therefore

$$\#X_q = \frac{\varphi(q)}{t_q} = \prod_{p\in\mathcal{S}} \frac{\varphi(p)}{t_p} = \prod_{p\in\mathcal{S}} \#X_p.$$

By duality theory, it follows that X_q is the direct product of the groups $\{X_p : p\in\mathcal{S}\}$, hence every character $\chi\in X_q$ has a unique decomposition

$$\chi = \prod_{p\in\mathcal{S}} \chi_p$$

where $\chi_p\in X_p$ for each $p\in\mathcal{S}$. By the well known multiplicative property of Kloosterman sums,

$$K_\chi(a,b;q) = \prod_{p\in\mathcal{S}} K_{\chi_p}(a,b;p),$$

and therefore

$$T_q(a,b) = \frac{t_q}{\varphi(q)} \sum_{\chi\in X_q} \prod_{p\in\mathcal{S}} K_{\chi_p}(a,b;p) = \prod_{p\in\mathcal{S}} \frac{t_p}{\varphi(p)} \sum_{\chi_p\in X_p} K_{\chi_p}(a,b;q).$$

The result follows. □

Lemma 2. *Let $\mathcal{S}$ be a set of primes p such that $p\ge z$, $p\equiv 3 \pmod 4$, $\gcd(p,g(g-1))=1$, and $t_p=\Omega(\log^2 p)$ for every $p\in\mathcal{S}$. Suppose that $\gcd(t_{p_1},t_{p_2})\le 2$ for all distinct $p_1,p_2\in\mathcal{S}$. If z is sufficiently large, then for some absolute constant $A>0$ and all $a,b\in\mathbb{Z}$ one has*

$$\bigl|T_q(a,b)\bigr| \le t_q \prod_{\substack{p\in\mathcal{S}\\ \gcd(a,b,p)=1}} \left(1-\frac{A}{\log p(\log\log p)^5}\right),$$

where $q=\prod_{p\in\mathcal{S}} p$.

Proof. If t_q is odd, then $\gcd(t_{p_1}, t_{p_2}) = 1$ for all distinct $p_1, p_2 \in \mathcal{S}$, thus

$$t_q = \prod_{p \in \mathcal{S}} t_p.$$

By Lemma 1, we also have

$$T_q(a, b) = \prod_{p \in \mathcal{S}} T_p(a, b).$$

Moreover,

$$T_p(a, b) = \frac{t_p}{p-1} \sum_{x \in \mathbb{Z}_p^*} \mathbf{e}_p \left(a x^{(p-1)/t_p} + b x^{-(p-1)/t_p} \right)$$

for all $p \in \mathcal{S}$. If $\gcd(a, b, p) = 1$, then since $t_p = \Omega(\log^2 p)$, Theorem 1.1 of [2] implies that the estimate

$$\left| \sum_{x \in \mathbb{Z}_p^*} \mathbf{e}_p \left(a x^{(p-1)/t_p} + b x^{-(p-1)/t_p} \right) \right| \le (p-1) \left(1 - \frac{A}{\log p (\log \log p)^5} \right)$$

holds for some absolute constant $A > 0$ provided that z is large enough. On the other hand, $T_p(a, b) = t_p$ if $\gcd(a, b, p) = p$. This completes the proof in the case that t_q is odd.

If t_q is even, then the multiplicative order of g^2 modulo q is $\tau_q = t_q/2$, and for each $p \in \mathcal{S}$ the multiplicative order of g^2 modulo p is $\tau_p = t_p/2$ or $\tau_p = t_p$ according to whether t_p is even or odd, respectively. Since each prime $p \in \mathcal{S}$ is congruent to $3 \pmod 4$, it follows that τ_p is odd, and we have

$$\tau_q = \prod_{p \in \mathcal{S}} \tau_p.$$

We now write

$$T_q(a, b) = \sum_{k=1}^{\tau_q} \mathbf{e}_q \left(a f^k + b f^{-k} \right) + \sum_{k=1}^{\tau_q} \mathbf{e}_q \left(a g f^k + b g^{-1} f^{-k} \right)$$

where $f = g^2$. Noting that $\tau_p = \Omega(\log^2 p)$ for all $p \in \S$, we can apply the preceding argument to both of these sums (with g replaced by g^2), and we derive the stated result in the case that t_q is even. $\square$

Lemma 3. *If y is sufficiently large, there is a set $\mathcal{S} \in [y(\log y)^{-2}, y]$ of primes p with $p \equiv 3 \pmod 4$ and $\gcd(p, g(g^2-1)) = 1$, of cardinality at least $\#\mathcal{S} = \Omega(y^{1/4}(\log y)^{-2})$, such that $\gcd(t_{p_1}, t_{p_2}) \le 2$ for any distinct $p_1, p_2 \in \mathcal{S}$, and $t_p \ge p^{1/4}$ for all $p \in \mathcal{S}$.*

Proof. According to Lemma 1 of [3] (taking $k = 1$, $u = 3$ and $v = 16$ in that lemma), for every sufficiently large value of y there are at least $\Omega(y/\log^2 y)$ primes $p \le y$ with $p \equiv 3 \pmod{16}$ such that either $p = 2r_1r_2 + 1$ where $r_1, r_2 \ge y^{1/4}$ are primes, or $p = 2r_0 + 1$ where r_0 is a prime. Clearly, the interval $[y(\log y)^{-2}, y]$ also contains a set $\mathcal{L}$ of $\Omega(y/\log^2 y)$ such primes. Note that for y large enough, we have that $p \nmid g(g^2 - 1)$ for each $p \in \mathcal{L}$.

Take the smallest such prime $p_1 \in \mathcal{L}$ and put it into the set $\mathcal{S}$. Next, remove all primes $p \in \mathcal{L}$ for which $\gcd(p-1, p_1-1) > 2$; since this condition implies that $\gcd(p-1, p_1-1) \ge y^{1/4}$, we remove at most $O(y^{3/4})$ such primes at this step. Now take the smallest remaining prime $p_2 \in \mathcal{L}$ and add it to $\mathcal{S}$, then remove the $O(y^{3/4})$ primes $p \in \mathcal{L}$ for which $\gcd(p - 1, p_2 - 1) > 2$. Continuing in this manner, we eventually put $\Omega(\#\mathcal{L}y^{-3/4}) = \Omega(y^{1/4}(\log y)^{-2})$ primes into the set $\mathcal{S}$. Noting that each $t_p > 2$ and $t_p \mid p - 1$, it follows that $t_p \ge y^{1/4} \ge p^{1/4}$ for every $p \in \mathcal{S}$. □

We also need the following bound for incomplete sums:

Lemma 4. *For any prime p with $\gcd(p, g) = 1$ and any natural number $K \le t_p$, the following bound holds:*

$$\max_{\gcd(a,b,p)=1} \left| T_p(K; a, b) \right| \ll p^{1/2} \log p.$$

Proof. It is easy to see that for any $h = 0, \ldots, t_p$,

$$\sum_{k=1}^{t_p} \mathbf{e}_p\left(ag^k + bg^{-k}\right) \mathbf{e}_{t_p}(hk) = \frac{t_p}{p-1} \sum_{x \in \mathbb{F}_p^*} \mathbf{e}_p\left(ax^{(p-1)/t_p} + bx^{-(p-1)/t_p}\right) \chi(x)$$

where $\chi(x)$ is a certain multiplicative character on $\mathbb{F}_p^*$. Applying the Weil bound to the last sum (see Example 12 in Appendix 5 of [6]; also Theorem 3 of Chapter 6 in [4], and Theorem 5.41 and the comments to Chapter 5 in [5]), we derive that

$$\sum_{k=1}^{t_p} \mathbf{e}_p\left(ag^k + bg^{-k}\right) \mathbf{e}_{t_p}(hk) \ll p^{1/2}.$$

Now using the standard reduction from complete sums to incomplete ones, we obtain the desired result. □

A relation between the sums $S_q(L;c)$ and $T_q(K;a,b)$ has been found in [1] which we now present in a slightly modified form.

Lemma 5. *Let $K = \lfloor L/2 \rfloor$. Then*

$$\left|S_q(L;c)\right| \le g^2 \left(g^2 - 1 + \frac{1}{K}\left|T_q(K;c,cg^{L-1})\right|\right)^{K/2}.$$

Proof. As in the proof of Lemma 3.1 of [1] we have

$$\left|S_q(L;c)\right| \le g^2 \prod_{k=1}^{K} \left|\sum_{a=0}^{g-1} \mathbf{e}_q\left(ac\left(g^k + g^{L-1-k}\right)\right)\right|.$$

Then, using the arithmetic-geometric mean inequality, we derive that

$$\begin{aligned}\left|S_q(L;c)\right| &\le g^2 \left(\frac{1}{K}\sum_{k=1}^{K} \left|\sum_{a,b=0}^{g-1} \mathbf{e}_q\left(ac\left(g^k + g^{L-1-k}\right)\right)\right|^2\right)^{K/2} \\ &= g^2 \left(\frac{1}{K}\sum_{a,b=0}^{g-1}\sum_{k=1}^{K} \mathbf{e}_q\left(c(a-b)\left(g^k + g^{L-1-k}\right)\right)\right)^{K/2}.\end{aligned}$$

Estimating each inner sum trivially as K for all a and b except for $a = 1$, $b = 0$, we obtain the desired statement. $\square$

3 Exponential Sums with Palindromes

Theorem 6. *There exists a constant $B > 0$ such that for all sufficiently large values of L and any prime $p \le L^2/\log^4 L$ such that $\gcd(p, g(g-1)) = 1$, the following bound holds:*

$$\max_{\gcd(c,p)=1} \left|S_p(L;c)\right| \le \#\mathcal{P}_L \exp\left(-L/\log p(\log\log p)^B\right).$$

Proof. Taking $K = \lfloor L/2 \rfloor$, we have by Lemma 5:

$$\left|S_p(L;c)\right| \le g^2 \left(g^2 - 1 + \frac{1}{K}\left|T_p(K;c,cg^{L-1})\right|\right)^{K/2}. \qquad (2)$$

Suppose that $\gcd(c,p)=1$. Let us write $K = Qt_p + R$ where $Q \ge 0$ and $0 \le R < t_p$.

Let us first consider the case $K \ge t_p$. Since $p \mid (g^{t_p}-1)$, it is clear that $t_p = \Omega(\log p)$; using Theorem 1.1 of [2] as in the proof of Lemma 2, it follows that for all sufficiently large primes p,

$$\left|T_p(c, cg^{L-1})\right| \le t_p\left(1 - \frac{1}{\log p(\log\log p)^{C_0}}\right) \tag{3}$$

for some constant $C_0 > 0$. Moreover, for any prime p coprime to $g(g-1)$, it is clear that $t_p \ne 1$ and that

$$\left|T_p(c, cg^{L-1})\right| < t_p.$$

Therefore, adjusting the value of C_0 if necessary, we see that the bound (3) holds for every prime p such that $\gcd(p, g(g-1)) = 1$. Thus, in the case that $K \ge t_p$ we have

$$\begin{aligned}
\left|T_p(K; c, cg^{L-1})\right| &= Q\left|T_p(c, cg^{L-1})\right| + \left|T_p(R; c, cg^{L-1})\right| \\
&\le Qt_p\left(1 - \frac{1}{\log p(\log\log p)^{C_0}}\right) + R \\
&= K - \frac{Qt_p}{\log p(\log\log p)^{C_0}} \le K\left(1 - \frac{1}{2\log p(\log\log p)^{C_0}}\right).
\end{aligned}$$

When $K < t_p$ we apply Lemma 4 to deduce that

$$\left|T_p(K; c, cg^{L-1})\right| \ll p^{1/2}\log p \ll K(\log p)^{-1},$$

since $K \gg L \ge p^{1/2}(\log p)^2$. Thus, in this case, we have a much stronger bound.

Therefore, for sufficiently large p,

$$\begin{aligned}
g^2 - 1 + \frac{1}{K}\left|T_p(K; c, cg^{L-1})\right| &\le g^2 - \frac{1}{2\log p(\log\log p)^{C_0}} \\
&\le g^2 \exp\left(-\frac{1}{2g^2\log p(\log\log p)^{C_0}}\right).
\end{aligned}$$

Using this estimate in (2) together with the obvious relation $\#\mathcal{P}_L \asymp g^{L/2}$, we derive the stated result. $\square$

4 Congruences with Palindromes

Let us denote

$$\mathcal{P}_L(q) = \left\{n \in \mathcal{P}_L : n \equiv 0 \pmod q\right\}.$$

Proposition 4.2 of [1] asserts that if $\gcd(q, g(g^2-1)) = 1$, then for $L \geq 10 + 2q^2 \log q$ the following asymptotic formula holds:

$$\#\mathcal{P}_L(q) = \frac{\#\mathcal{P}_L}{q} + O\left(\frac{\#\mathcal{P}_L}{q} \exp\left(-\frac{L}{2q^2}\right)\right).$$

Here we obtain a nontrivial bound on $\#\mathcal{P}_L(q)$ without any restrictions on the size or the arithmetic structure of q.

Theorem 7. *For all positive integers L and q, the following bound holds:*

$$\#\mathcal{P}_L(q) \ll \frac{\#\mathcal{P}_L}{q^{1/2}}.$$

Proof. Let r be the largest integer for which $r \equiv L \pmod 2$ and $g^r \leq q$. Clearly, $g^r \gg q$. We observe that every palindrome $n \in \mathcal{P}_L$ can be expressed in the form

$$n = g^{(L+r)/2} k_1 + g^{(L-r)/2} m + k_2$$

where $k_1, k_2 < g^{(L-r)/2}$, $g^{(L-r)/2} k_1 + k_2$ is a palindrome of length $L - r$, and $m < g^r$. Note that for each choice of k_2, the value of k_1 is uniquely determined by the palindromy condition.

Let $d = \gcd(q, g)$. If $n \in \mathcal{P}_L$ is divisible by q, then $d \,|\, k_2$; since $k_2 \neq 0$ there are at most $g^{(L-r)/2}/d$ choices for k_2. Since $g^r \leq q$, it follows that for each choice of k_2 there are at most d values of $m < g^r$ such that the congruence $g^{(L+r)/2} k_1 + g^{(L-r)/2} m + k_2 \equiv 0 \pmod q$ holds. Therefore, $\#\mathcal{P}_L(q) \leq g^{(L-r)/2} \ll \#\mathcal{P}_L\, q^{-1/2}$. □

5 Prime Divisors of Palindromes

Let $\omega(n)$ denote the number of distinct prime divisors of an integer $n \geq 2$.

Theorem 8. *For all sufficiently large L, there is a palindrome n whose length is L and for which*

$$\omega(n) = \Omega\left(\frac{\log\log n}{\log\log\log n}\right).$$

Proof. Define y by the equation

$$2C_1 y^{1/4}(\log y)^{-1} = \log L,$$

where C_1 is the constant implied by the Ω-symbol in Lemma 3, and let $\mathcal{S}$ be a set of primes of cardinality $\#\mathcal{S} = \lfloor C_1 y^{1/4}(\log y)^{-2} \rfloor$ with the properties stated in that lemma. Putting

$$q = \prod_{p\in\mathcal{S}} p,$$

by Lemma 2 we see that

$$\max_{\gcd(a,b,q)<q} \left|T_q(a,b)\right| \le t_q\left(1 - \frac{C_2}{\log y(\log\log y)^5}\right)$$

for some constant $C_2 > 0$ provided that L is large enough. In particular, supposing that $\gcd(c,q) = 1$, we obtain the estimate

$$\left|T_q(c, cg^{L-1})\right| \le t_q\left(1 - \frac{C_2}{\log y(\log\log y)^5}\right) \tag{4}$$

since $\gcd(g,q) = 1$ for sufficiently large L. Taking $K = \lfloor L/2 \rfloor$, we have by Lemma 5:

$$\left|S_q(L;c)\right| \le g^2\left(g^2 - 1 + \frac{1}{K}\left|T_q(K;c,cg^{L-1})\right|\right)^{K/2}. \tag{5}$$

As in the proof of Theorem 6, we now write $K = Qt_q + R$ with integers $Q \ge 0$ and $0 \le R < t_q$. Because $K = \lfloor L/2 \rfloor \ge (t_q^2 - 1)/2 \ge t_q$ we have $Q \ge 1$. Thus, provided that L is large enough, using (4) we derive

$$\begin{aligned}
|T_q(K;c,c)| &= Q|T_q(c,c)| + |T_q(R;c,c)| \\
&\le Qt_q\left(1 - \frac{C_2}{\log y(\log\log y)^5}\right) + R \\
&= K - \frac{C_2 Q t_q}{\log y(\log\log y)^5} \le K\left(-\frac{C_2}{2\log y(\log\log y)^5}\right),
\end{aligned}$$

since $Qt_q \ge Q > R$.

Applying this to (5), it follows that

$$\left|S_q(L;c)\right| \le \#\mathcal{P}_L \exp\left(-C_4 L/\log y(\log\log y)^5\right)$$

for some constant $C_4 > 0$, provided that $\gcd(c, q) < q$ and L is sufficiently large.

Now let us denote

$$\mathcal{P}_L(q, a) = \{n \in \mathcal{P}_L : n \equiv a \pmod q\}. \tag{6}$$

By the same arguments given in the proof of Proposition 4.2 of [1], it is easily shown that the preceding estimate implies

$$\#\mathcal{P}_L(q, a) = \frac{\#\mathcal{P}_L}{q} + O\left(\#\mathcal{P}_L \exp\left(-C_4 L / \log y (\log\log y)^5\right)\right).$$

In particular $\mathcal{P}_L(q, 0) > 0$ for sufficiently large L. Taking any $n \in \mathcal{P}_L(q, 0)$ we obtain $\omega(n) \geq \omega(q) \geq \#\mathcal{S} = \Omega(y^{1/4}(\log y)^{-2})$, and since $L \asymp \log n$ the result follows. ∎

Theorem 9. *There is a constant $C > 0$ such that for all sufficiently large L*

$$\prod_{\substack{p \leq L^2(\log L)^{-C} \\ \gcd(p, g(g-1))=1}} p \;\Bigg|\; \prod_{n \in \mathcal{P}_L} n$$

Proof. Repeating the same arguments as in the proof of Proposition 4.1 of [1], we derive from Theorem 6 that

$$\#\mathcal{P}_L(p, a) = \frac{\#\mathcal{P}_L}{p} + O\left(\#\mathcal{P}_L \exp\left(-L/2 \log p (\log\log p)^B\right)\right)$$

where, B is defined in Theorem 6 and as before, $\mathcal{P}_L(p, a)$ is defined by (6). In particular, $\#\mathcal{P}_L(p, 0) > 0$ provided that L is large enough. ∎

Theorem 9 immediately implies that

$$\omega\left(\prod_{n \in \mathcal{P}_L} n\right) = \Omega\left(\frac{L^2}{(\log L)^C}\right).$$

We now use Theorem 7 to derive a more precise result.

Theorem 10. *For all sufficiently large L,*

$$\omega\left(\prod_{n \in \mathcal{P}_L} n\right) = \Omega\left(\frac{L^2}{(\log L)^2}\right).$$

Proof. Let

$$W = \prod_{n \in \mathcal{P}_L} n, \qquad s = \omega(W).$$

For each prime p, we denote by r_p the exact power of p dividing W; then

$$\prod_{n \in \mathcal{P}_L} n = \prod_{p \,|\, W} p^{r_p},$$

and this implies that

$$r_p = \sum_{\alpha=1}^{\infty} \#\mathcal{P}_L(p^\alpha).$$

By Theorem 7 we have the estimate

$$r_p \ll \#\mathcal{P}_L \sum_{\alpha=1}^{\infty} p^{-\alpha/2} \ll \frac{\#\mathcal{P}_L}{p^{1/2}};$$

thus,

$$\#\mathcal{P}_L \sum_{p \,|\, W} \frac{\log p}{p^{1/2}} \gg \sum_{p \,|\, W} r_p \log p = \log W \gg L g^L.$$

Denoting by p_j the j-th prime number, we obtain

$$L \ll \sum_{p \,|\, W} \frac{\log p}{p^{1/2}} \le \sum_{j=1}^{s} \frac{\log p_j}{p_j^{1/2}} \ll (s \log s)^{1/2}$$

which finishes the proof. □

6 Remarks

It is an open question (posed in [1]) as to whether there exist infinitely many prime palindromes in a given base $g \ge 2$, and the solution appears to be quite difficult. Indeed, since the collection of palindromes in any base forms a set as thin as that of the square numbers, this question is likely to be as difficult as that of showing the existence of infinitely many primes of the form $p = n^2 + 1$. At the present time, however, even the question as to whether there exist infinitely squarefree palindromes remains open.

References

[1] W. Banks, D. Hart and M. Sakata, 'Almost all palindromes are composite', to appear in *Math. Res. Lett.*

[2] T. Cochrane, C. Pinner and J. Rosenhouse, 'Bounds on exponential sums and the polynomial Waring problem mod p', *J. London Math. Soc. (2)* **67** (2003) no. 2, 319–336.

[3] D. R. Heath-Brown, 'Artin's conjecture for primitive roots', *Quart. J. Math.*, **37** (1986), 27–38.

[4] W.-C. W. Li, *Number theory with applications*, World Scientific, Singapore, 1996.

[5] R. Lidl and H. Niederreiter, *Finite fields*, Cambridge University Press, Cambridge, 1997.

[6] A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.