MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Pages 000–000
S 0025-5718(XX)0000-0

PERFECT REPDIGITS

Kevin Broughan University of Waikato, Hamilton, New Zealand kab@waikato.ac.nz

Sergio Guzman Sanchez Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México sguzman@matmor.unam.mx

Florian Luca Instituto de Matemáticas, Universidad Nacional Autonoma de México, C.P. 58089, Morelia, Michoacán, México fluca@matmor.unam.mx

Abstract. Here, we give an algorithm to detect all perfect repdigits in any base $g > 1$. As an application, we find all such examples when $g \in [2, \ldots, 333]$, extending a calculation from [2]. In particular, we demonstrate that there are no odd perfect repdigits for this range of bases.

[2010]Primary 11A63, 11A05, 11A25

Key words: Perfect numbers, Repdigits, Pell equations, Lucas sequences.

Contents

1. Introduction

For a positive integer n we write $\sigma(n)$ for the sum of divisors of n. The number n is called *perfect* if $\sigma(n) = 2n$. It is not known if there are infinitely many perfect numbers.

For an integer $g > 1$ a *repdigit* in base g is a positive integer N all of whose base g digits are the same. That is, N has the shape

(1.1)
$$N = d\left(\frac{g^m - 1}{g - 1}\right), \qquad \text{where} \qquad m \geq 1, \quad \text{and} \quad d \in \{1, 2, \ldots, g-1\}.$$

In [9], Pollack proved that given $g > 1$ there are only finitely many repdigits in base g which are perfect. His proof is effective and uses results from Diophantine equations which were proved using lower bounds for linear forms in logarithms. Up until now, no explicit upper bound on the largest solution as a function of g has been computed. In [2], perfect repdigits to bases g have been computed for all $g \in \{2, \ldots, 10\}$. The method of [2] reduces in most cases to using modular constraints or solving several particular exponential type Diophantine equations.

In this paper, we present an algorithm to compute all perfect repdigits in base g. As an illustration, we extend the computations from [2] to all bases $g \in [2, 333]$. As a byproduct of our work we also get some theoretical bounds such as:

Theorem 1.1. (i) *The largest perfect number of the form* (1.1) *satisfies*

$$N < g^{g^{g^{g^3}}}. \tag{1.2}$$

(ii) *The number of perfect repdigits to base g is at most $4g^5$.*

Throughout the paper, we use p, q and r, with or without indices, for prime numbers.

2. Lucas and Lehmer sequences

A *Lucas sequence* is a sequence of integers $\{u_n\}_{n\geq 0}$ satisfying the initial conditions $u_0 = 0$, $u_1 = 1$ and the recurrence

$$u_{n+2} = ru_{n+1} + su_n \qquad \text{for all} \qquad n \geq 0,$$

where r, s are coprime nonzero integers with discriminant $\Delta_u := r^2 + 4s \neq 0$. It is further assumed that if α and β are the two roots of the characteristic equation $x^2 - rx - s = 0$, then α/β is not a root of unity.

The formula for the general term of the Lucas sequence is

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \qquad \text{for} \quad n = 0, 1, \ldots.$$

Given $n > 0$, a *primitive* prime factor of u_n is defined to be a prime divisor p of u_n such that p does not divide Δ_u and p does not divide u_m for any positive integer $m < n$. A result of Carmichael (see [3] and Theorem A in [1]), asserts that if $\Delta_u > 0$ (i.e., the roots α and β are real), then u_n always has a primitive prime factor for all $n \geq 13$. This result has been extended to the instance of the Lucas sequences with complex non–real roots by Bilu, Hanrot and Voutier [1]. For such sequences, u_n has a primitive prime factor for all $n \geq 31$. Moreover, there are only finitely many triples (n, α, β) with $5 \leq n \leq 30$, but $n \neq 6$ such that u_n lacks a primitive prime factor for the corresponding pair of roots (α, β), be they real or complex–conjugated, and all such exceptions are listed in Table 1 in [1]. A primitive prime factor for u_n has the property that $p \equiv \pm 1 \pmod{n}$. When α and β are rational integers, the more precise congruence $p \equiv 1 \pmod{n}$ holds for every primitive prime factor p of u_n. In this particular case, u_n has a primitive divisor for all $n > 6$. In particular, the inequality $p \geq n - 1$ holds for every primitive prime factor p of u_n, and the slightly better inequality $p \geq n + 1$ holds when the roots α and β are rational integers.

Closely related to Lucas sequences are the so-called *Lehmer sequences*. To define a Lehmer sequence, assume again that r and s are coprime nonzero integers with $r > 0$ and $\Delta_v := r + 4s \neq 0$ and let α and β be the two roots of the characteristic equation $x^2 - \sqrt{r}x - s = 0$. Assume again that α/β is not a root of unity. Put

$$v_n = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta}, & \text{if} \quad n \equiv 1 \pmod{2}, \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2}, & \text{if} \quad n \equiv 0 \pmod{2}. \end{cases}$$

The sequence $\{v_n\}_{n \geq 0}$ is called a Lehmer sequence and consists of integers. Like in the case of Lucas sequences, a primitive prime factor of v_n is a prime factor p of v_n dividing neither Δ_v nor any v_m for positive integers $m < n$. Then v_n has a primitive divisor when $\Delta_v > 0$ for all $n \geq 13$ (see [1, Table 2] and [12]).

We conclude this section by presenting three examples of Lucas and Lehmer sequences which are important in the development of the results which follow.

Example 1. If $r = g + 1$ and $s = -g$, then

$$x^2 - rx - s = x^2 - (g + 1)x + g = (x - g)(x - 1).$$

In this case, we can take $\alpha := g$ and $\beta := 1$ and so

$$u_n = \frac{g^n - 1}{g - 1} \qquad \text{for all} \quad n \geq 0.$$

In particular, the sequence of *repunits* in base g (repdigits whose repeating digit is 1) is a Lucas sequence whose roots α and β are rational integers. Hence, u_n is a multiple of a prime $p \geq n + 1$ for all $n \geq 7$. Finally given a prime p, then $p \mid u_n$ for some $n \geq 1$ if and only if $p \nmid g$.

Example 2. Let $D > 1$ be a positive integer which is not a square and let (X_1, Y_1) be the minimal positive integer solution of the Pell equation

$$X^2 - DY^2 = \pm 1. \tag{2.1}$$

By this we mean (X_1, Y_1) is the smallest pair of positive integers such that $X_1^2 - DY_1^2 = \varepsilon$ holds with some $\varepsilon \in \{\pm 1\}$. This always exists since there always exists a solution in positive integers of equation (2.1) for which $\varepsilon = 1$. If a solution with $\varepsilon = -1$ exists, then the minimal one, namely (X_1, Y_1), has corresponding $\varepsilon = -1$ and the smallest solution with $\varepsilon = 1$ in this case is $(2X_1^2 + 1, 2X_1Y_1)$. From the theory of the Pell equations, we know that equation (2.1) always has infinitely many positive integer solutions (X, Y). Moreover, all solutions are of the form (X_n, Y_n), where

$$X_n + \sqrt{D}Y_n = (X_1 + \sqrt{D}Y_1)^n \qquad \text{for all} \qquad n \geq 1.$$

Putting $\alpha := X_1 + \sqrt{D}Y_1$ and $\beta := X_1 - \sqrt{D}Y_1$, conjugating the above relation (i.e., replacing $\sqrt{D}$ by $-\sqrt{D}$) and solving for X_n and Y_n, we get, in particular, that

$$Y_n = \frac{\alpha^n - \beta^n}{2\sqrt{D}} = Y_1 \left(\frac{\alpha^n - \beta^n}{\alpha - \beta} \right).$$

So, if we put $u_n := Y_n/Y_1$ for all $n \geq 1$ and $u_0 := 0$, then $\{u_n\}_{n \geq 0}$ forms a Lucas sequence. Furthermore,

$$X_n = \frac{\alpha^n + \beta^n}{2} = \frac{\alpha^{2n} - \beta^{2n}}{2(\alpha^n - \beta^n)} = \frac{u_{2n}}{2u_n} \qquad \text{for all} \quad n \geq 1.$$

Hence, by Carmichael's result, we get that X_n has a prime factor $p \geq 2n - 1$ for all $n \geq 7$.

Example 3. Let $A > 1$ and $B > 1$ be integers neither of which is a perfect square. Consider the Diophantine equation

$$AX^2 - BY^2 = \pm 1. \tag{2.2}$$

Since the roles of A and B in equation (2.2) are interchangeable, we may assume that the sign on the right is $+1$. It is then known that

if equation (2.2) has a positive integer solution, then it has infinitely many positive integer solutions. Furthermore, letting (X_1, Y_1) be the minimal such positive integer solution, all its positive solutions are of the form (X_m, Y_m) for some odd integer $m \geq 1$, where

$$\sqrt{A}X_m + \sqrt{B}Y_m = (\sqrt{A}X_1 + \sqrt{B}Y_1)^m$$

(see [11]). Putting $\alpha := \sqrt{A}X_1 + \sqrt{B}Y_1$ and $\beta := \sqrt{A}X_1 - \sqrt{B}Y_1$, we have that $r = \alpha + \beta = 2\sqrt{A}X_1 = \sqrt{4AX_1^2}$ and $s = -\alpha\beta = -1$. Furthermore,

$$Y_m = \frac{\alpha^m - \beta^m}{2\sqrt{B}} = Y_1 \left(\frac{\alpha^m - \beta^m}{\alpha - \beta} \right) \qquad \text{for all odd} \quad m \geq 1.$$

Therefore if we put $v_m := Y_m/Y_1$ for odd $m \geq 1$, then $\{v_m\}_{m \geq 1 \text{ odd}}$ is the odd indexed subsequence of the Lehmer sequence of roots α and β. In particular, Y_m is divisible by a prime $p \geq m - 1$ for all odd $m \geq 13$. Furthermore,

$$X_m = \frac{\alpha^m + \beta^m}{2\sqrt{A}} = X_1 \frac{\alpha^m - (-\beta)^m}{\alpha - (-\beta)}.$$

Thus, if we put $w_m := X_m/X_1$ for odd $m \geq 1$, then $\{w_m\}_{m \geq 1 \text{ odd}}$ is also the odd indexed subsequence of the Lehmer sequence with roots α and $-\beta$. (Note that $\alpha + (-\beta) = 2\sqrt{B}Y_1 = \sqrt{4BY_1^2}$, so we may take $r = 4BY_1^2$ and $s = -\alpha(-\beta) = 1$.) Thus, X_m is divisible by a prime $p \geq m - 1$ for all odd $m \geq 13$ as well.

3. The case of the even perfect repdigits

A well-known result of Euclid and Euler says that an even perfect number is necessarily of the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is prime. Thus, to find even perfect repdigits we need to solve the equation

(3.1)
$$N = d\left(\frac{g^m - 1}{g - 1} \right) = 2^{p-1}(2^p - 1), \text{where } d \in \{1, \ldots, g-1\}, \text{and } 2^p - 1 \text{ is prime.}$$

The following proposition is known having appeared as [9, Lemma 7] and extends [2, Lemma 5], but we include it for the convenience of the reader.

Proposition 3.1. *All solutions N of equation* (3.1) *have either $m = 1$ so $g > N$ is arbitrary and $d = N$, or $m = 2$, in which case $d = 2^a$, $g + 1 = 2^b(2^p - 1)$ for some nonnegative integers a and b. Furthermore, in this last case we have $a + b = p - 1$ and $N = 2^a + 2^a g$.*

Proof. Let N be an even perfect repdigit in base g. The case $m = 1$ needs no proof. When $m = 2$, we get $N = d(g + 1) = 2^{p-1}(2^p - 1)$ and $2^p - 1$ is prime. Since $2^p - 1 > 2^{p-1}$ and $g + 1 > d$, it must be the case that $2^p - 1$ divides $g + 1$. So, d is a divisor of 2^{p-1}, therefore $d = 2^a$ for some $a \in \{1, \ldots, p-1\}$, which yields $g+1 = 2^b(2^p - 1)$ with $b = p - 1 - a$.

Let us now show that the case $m \geq 3$ is not possible. It is clear that $2^p - 1$ must divide $(g^m - 1)/(g - 1)$, for otherwise it will divide d, and then

$$g > d \geq 2^p - 1 > \sqrt{N} \geq \left(\frac{g^m - 1}{g - 1}\right)^{1/2} = \sqrt{g^{m-1} + \cdots + 1} > g^{(m-1)/2} \geq g,$$

which is impossible. Thus, $(g^m - 1)/(g - 1) = 2^b(2^p - 1)$ for some nonnegative integer b. If m is odd or m is even but g is even, then $(g^m - 1)/(g - 1)$ is odd, therefore $b = 0$. Hence, $d = 2^{p-1} < g$, and so

$$2^p - 1 = \frac{g^m - 1}{g - 1} = g^{m-1} + \cdots + 1 > g^{m-1} \geq g^2 > 2^{2p-2},$$

which is false for all $p \geq 2$. Thus, g must be odd and m must be even. Put $m = 2m_1$. We then get

$$2^b(2^p - 1) = \frac{g^{2m_1} - 1}{g - 1} = (g^{m_1} + 1)\left(\frac{g^{m_1} - 1}{g - 1}\right).$$

On the right, the first factor is larger then the second factor and on the left, $2^p - 1 > 2^b$ and $2^p - 1$ is prime. Hence, $2^p - 1$ must divide $g^{m_1} + 1$, and we get that $g^{m_1} + 1 = 2^c(2^p - 1)$ and $(g^{m_1} - 1)/(g - 1) = 2^e$ for some positive integers c and e. (Indeed, $c > 0$ because g is odd and $e > 0$ because $m_1 = m/2 > 1$.) Since $(g^{m_1} - 1)/(g - 1)$ is even and g is odd, we get that m_1 is even. Hence, $m_1 = 2m_2$, and so $2^c(2^p - 1) = g^{m_1} + 1 = g^{2m_2} + 1 \equiv 2 \pmod 8$. We next get easily that $c = 1$, then that $2^p - 1 \equiv 1 \pmod 4$, but this is false for any prime $p \geq 2$.

This finishes the proof of the proposition. □

4. The case of the odd perfect numbers with small Eulerian prime p

While it is not known whether odd perfect numbers exist, it is known that every such number is of the form $p\square$, where p is the Eulerian prime and we use $\square$ for a perfect integer square. More is known, for example that $p \equiv 1 \pmod 4$. So, following for example Pollack [9], let

us consider the Diophantine equation

(4.1)
$$d\left(\frac{g^m-1}{g-1}\right)=p\square, \qquad \text{where} \quad d\in\{1,\dots,g-1\}, \quad \text{and} \quad p \text{ is prime.}$$

Equation (4.1) implies that

$$\frac{g^m-1}{g-1}=c_{d,p}\square, \tag{4.2}$$

where $c_{d,p}$ is some squarefree integer which can easily be determined in terms of p and d. To determine it, write $d=d_1d_2^2$ where d_1 is squarefree. Then $c_{d,p}=pd_1$ if $p\nmid d_1$ and $c_{d,p}=d_1/p$ if $p\mid d_1$.

We now distinguish several cases. Here, we say that the Eulerian prime p is *small* if $p\le g$. In the next section, we consider the case $p>g$. First we give a derivation for a bound for the minimal solution to a Pell equation which was stated in [7, Lemma 1], which is sufficient for our purposes.

Lemma 4.1. *Let $d>1$ not be square. Then the minimal positive integer solution (X_0,Y_0) to the Pell equation $X^2-dY^2=1$, satisfies $X_0+\sqrt{d}Y_0<d^{3\sqrt{d}}$.*

Proof. Put $\eta:=X_0+\sqrt{d}Y_0$. Assume first that $d\equiv 0,\ 1 \pmod 4$. By Schur's theorem [4, Theorem 13.5, Page 329], if $(U,V):=(U_0,V_0)$ is the smallest positive integer solution of the equation $U^2-dV^2=4$ (which always exists [5, Theorem 1.3]), then putting

$$\varepsilon:=\frac{U_0+\sqrt{d}V_0}{2},$$

we have $\varepsilon<d^{\sqrt{d}}$. Let's see how we deduce from this our desired conclusion.

We distinguish three cases.

Case 1. V_0 is even. Then so is U_0. So putting $(X,Y):=(U_0/2,V_0/2)$, we have $X^2-dY^2=1$, so $\eta\le X+\sqrt{d}Y=\varepsilon<d^{\sqrt{d}}$, which is better than what we are after.

Case 2. V_0 is odd and U_0 is even. Then $4\mid d$. Further,

$$\varepsilon^2=\left(\frac{U_0^2+dV_0^2}{4}\right)+\sqrt{d}\left(\frac{2U_0V_0}{4}\right)=:X+\sqrt{d}Y.$$

Clearly, $X,\ Y$ are integers and $X^2-dY^2=1$. Thus, $\eta\le\varepsilon^2<d^{2\sqrt{d}}$ in this case.

Case 3. V_0 is odd and U_0 is odd. Then $d \equiv 5 \pmod 8$. Further,

$$\varepsilon^3 = \left(\frac{U_0(U_0^2 + 3dV_0^2)}{8}\right) + \sqrt{d}\left(\frac{V_0(3U_0^2 + dV_0^2)}{8}\right) =: X + \sqrt{d}Y,$$

where X, Y are positive integers with $X^2 - dY^2 = 1$. Thus, $\eta \leq X + \sqrt{d}Y = \varepsilon^3 < d^{3\sqrt{d}}$, which is what we wanted.

Assume next that $d \equiv 2, 3 \pmod 4$, and let again (U_0, V_0) be the minimal positive integer solution to the equation $U^2 - dV^2 = 4$. Then V must be even, for if V is odd, then so is U, and reducing the above equation modulo 4 we would get $d \equiv 1 \pmod 4$, which is not the case we are considering. Thus, $(S, T) := (U_0, V_0/2)$ is a positive integer solution to $S^2 - (4d)T^2 = 4$. Moreover, for every positive integer solution (S, T) to the above equation, the pair $(U, V) := (S, 2T)$ is a positive integer solution to the equation $U^2 - dV^2 = 4$. Thus, by Schur's theorem applied to $4d$, a number which is congruent to 0 modulo 4, we get that

$$\varepsilon = \frac{1}{2}(U_0 + \sqrt{4d}(V_0/2)) < (4d)^{\sqrt{4d}} = (4d)^{2\sqrt{d}}.$$

Note that since $(X, Y) = (U_0/2, V_0/2)$ is a pair of positive integers satisfying $X^2 - dY^2 = 1$, we have that $\eta \leq \varepsilon \leq (4d)^{2\sqrt{d}}$. Since the inequality $(4d)^{2\sqrt{d}} < d^{3\sqrt{d}}$ holds for all $d > 16$, it remains to study the cases when d is in the set $\{2, 3, 6, 7, 10, 11, 14, 15\}$. For each of these instances, a direct check shows that $\eta < d^{3\sqrt{d}}$. □

From now on, we assume that $g > 2$, because if $g = 2$, then $d = 1$ and $N = 2^m - 1$ for some $m \geq 2$, but all such numbers are congruent to 3 modulo 4, so they cannot be odd perfect numbers.

Proposition 4.2. *If the Eulerian prime p satisfies $p \leq g$, then every solution of equation* (4.1) *satisfies $m \leq \max\{144g^2, 12g^3\}$.*

Proof. Note first that the case $p = g$ never occurs since if $p = g$, then p cannot divide d (since $d < g = p$) and p is coprime to $(g^m - 1)/(g - 1) = 1 + g + \cdots + g^{m-1} = 1 + p + \cdots + p^{m-1}$. So, we assume that $p < g$.

Assume now that d and p are fixed and consider equation (4.1) as an equation in the variable m. Rewrite equation (4.2) as

$$g^m - (g - 1)c_{d,p}\square = 1. \tag{4.3}$$

When m is even, the above equation has the form

$$X^2 - DY^2 = 1, \tag{4.4}$$

where $D := (g - 1)c_{d,p}$, and $X := g^{m/2}$. We may assume that D is not a perfect square, otherwise the above equation has no nontrivial solution. Hence, we are in the case of a Pell equation as in Example

2 of Section 2. Using the notations from that example, we have that $X_n = g^{m/2}$. Hence, X_n has no prime factor exceeding g. Thus, by primitive divisors (see the remark at the end of Example 2 in Section 2), we have that $n \leq \max\{6, (g+1)/2\}$. Let

$$\alpha := X_1 + \sqrt{D}Y_1.$$

By Lemma 4.1, $\alpha < D^{3\sqrt{D}}$. Since D divides $(g-1)dp$, we get that $D < g(g-1)^2$. Then

$$g^{m/2} = X_n < \alpha^n < D^{3n\sqrt{D}} < (g^3)^{3n\sqrt{g(g-1)^2}} \leq g^{9n(g-1)g^{1/2}}$$

giving $m \leq 18(g-1)g^{1/2}n$. Since $n \leq \max\{6, (g+1)/2\}$, we get that $m \leq \max\{108g^{3/2}, 9g^{5/2}\}$.

The same holds when m is odd and g is a perfect square. So, assume next that m is odd and g is not a square. Then equation (4.3) can be written as

$$AX^2 - BY^2 = 1, \tag{4.5}$$

where $A := g$, $B := (g-1)c_{d,p}$, and $X := g^{(m-1)/2}$. Now B is not a square, since in that case the equation would read $g^m - 1 = \square$, which is impossible by known results on Catalan's equation. So, we are in the case of Example 3 from Section 2. Thus, if $X_n = g^{(m-1)/2}$, then $n \leq \max\{12, g+1\}$. It is well-known that if

$$\eta := X_1\sqrt{A} + Y_1\sqrt{B}, \tag{4.6}$$

then $\eta^2 = U_1 + \sqrt{AB}V_1$ is such that (U_1, V_1) is the minimal positive integer solution (U, V) of the Pell equation $U^2 - DV^2 = 1$ with $D := AB$ (see [11]). In particular,

$$\eta^2 < D^{3\sqrt{D}}.$$

Note that $D = g(g-1)c_{d,p} < g^2(g-1)^2$. Thus,

$$g^{(m-1)/2} = X_n < \eta^n < D^{(3n/2)\sqrt{D}} < (g^4)^{(3n/2)\sqrt{g^2(g-1)^2}} < g^{6ng(g-1)},$$

leading to $m - 1 < 12ng(g-1)$. Since $n \leq \max\{12, g+1\}$, we get that $m \leq \max\{144g^2, 12g^3\}$, which completes the proof of this proposition. □

Remark 1. While the bound of Proposition 4.2 has the theoretical merit of being explicit in g, it is quite likely not very useful in practice although we shall later invoke it for the proof of Theorem 1.1. However, its method of proof should be quite useful. Namely, for each d and p, compute $c_{d,p}$ and generate the minimal solutions of the two Pell like equations implied by (4.3), namely of equation (4.4) when either m is even or g is a perfect square, or of equation (4.5) when g is not a

square and m is odd (this last one might not have any solutions, but testing for the existence of a solution amounts to computing again the minimal solution of a Pell equation as explained after the definition of η in (4.6)). Then one can evaluate X_n for all $n \le \max\{6, (g+1)/2\}$ (or $n \le \max\{12, g+1\}$, respectively), and test for which of these values of n is X_n a power of g. This algorithm will detect all potential candidates for m such that $N = du_m$ is odd, perfect and the Eulerian prime p is small.

5. The case of odd perfect repdigits with large Eulerian prime p

From now on, the Eulerian prime p is assumed to satisfy $p > g$ and du_m is odd, where $u_m := (g^m - 1)/(g-1)$. Hence, $c_d := c_{d,p}/p$ does not depend on p because d is smaller than g, thus smaller than p, so in particular it is coprime to p. We distinguish and then treat three cases which are in increasing order of complexity.

5.1. **The case when m is even.** Here, we have the following result.

Proposition 5.1. *If the Eulerian prime p satisfies $p > g$ and m is even, then $m \le \max\{216g^{3/2}, 18g^{5/2}\}$.*

Proof. Writing $m = 2m_1$, we get

$$c_d p\Box = \frac{g^m - 1}{g-1} = \left(\frac{g^{m_1}-1}{g-1}\right)(g^{m_1}+1).$$

The two factors on the right are coprime because their greatest common divisor divides $(g^{m_1}+1) - (g^{m_1}-1) = 2$ and they are both odd. Thus, there exists some divisor λ_d of c_d such either

$$\frac{g^{m_1}-1}{g-1} = \lambda_d\Box, \qquad \text{or} \qquad g^{m_1}+1 = \lambda_d\Box. \tag{5.1}$$

If the first instance occurs, then we are in case similar to the one treated when p was small. Namely, the equation on the left is

$$g^{m_1} - (g-1)\lambda_d\Box = 1,$$

which is of the form $X^2 - DY^2 = 1$ with $X := g^{m_1/2}$ and $D = (g-1)\lambda_d \le (g-1)^2$ if m_1 is even or $g = \Box$, or of the form $AX^2 - BY^2 = 1$ with $A := g$, $X := g^{(m_1-1)/2}$ and $B := (g-1)\lambda_d$, so $D = AB = g(g-1)\lambda_d \le g(g-1)^2$ provided that m_1 is odd and $g \ne \Box$. Using the same methods as in the proof of Proposition 4.2 yields that $m \le \max\{144g, 12g^2\}$ in case m_1 is even or $g = \Box$, and $m \le \max\{216g^{3/2}, 18g^{5/2}\}$ in case m_1 is odd and $g \ne \Box$, which leads easily to the desired conclusion.

The case of the second equation in (5.1) is similar. Namely, rewriting it as $g^{m_1} - \lambda_d \square = -1$, we recognize that it is either of the form $X^2 - DY^2 = -1$, with $X := g^{m_1/2},\ D = \lambda_d \leq g-1$, provided that m_1 is even or $g = \square$, or of the form $AX^2 - BY^2 = -1$ with $A := g,\ X := g^{(m_1-1)/2}$ and $B := \lambda_d$, so $D = AB = g\lambda_d \leq g(g-1)$ provided that m_1 is odd and $g \neq \square$. Note that in this last case we may assume that $B = \lambda_d$ is not a square, for if it were, then we would be in the situation when $g^{m_1} - \square = -1$, which gives either $m_1 = 1$ (so, $m = 2$, which satisfies the conclusion of the proposition), or leads to a nontrivial solution of the Catalan equation, and the only possibility is $2^3 - 3^2 = -1$, so $m_1 = 3$ and $g = 2$, which for us it is not convenient because $g > 2$. Again using the method of Proposition 4.2 yields that $m \leq \max\{72g^{1/2}, 12g^{3/2}\}$ in case m_1 is even or $g = \square$, and $m \leq \max\{144g, 24g^2\}$ in case m_1 is odd and $g \neq \square$. The proposition now follows. □

Remark 2. Similar considerations as in Remark 1 regarding computing all possible values for m apply to this case also. For precise details consult the code described in Section 7, "The Computations" below.

5.2. **The case when $d = \square$.** From now on, m is odd. Since $d = \square$, we have that $c_d = 1$. Here, we prove the following result.

Proposition 5.2. *If $d = \square$, then either $m = q$ is a prime, or $m = q^2$, where q is a prime dividing $g - 1$.*

Proof. Assume that m is not a prime and let q be its minimal prime factor. Observe that q is odd. Then

$$p\square = \frac{g^m - 1}{g - 1} = \left(\frac{g^m - 1}{g^{m/q} - 1}\right)\left(\frac{g^{m/q} - 1}{g - 1}\right), \tag{5.2}$$

where as before p is the Eulerian prime. A classical argument shows that the two factors on the right are either coprime, or their greatest common divisor is exactly q, and this holds only when $q \mid g - 1$. Furthermore, in this case q exactly divides the first factor. Let us go through this argument. Say P is a common prime factor of the two factors appearing in the right–hand side of (5.2). Put $a := g^{m/q}$. Then P divides $a - 1 = g^{m/q} - 1$ and also $(a^q - 1)/(a - 1) = (g^m - 1)/(g^{m/q} - 1)$. Since

$$\frac{a^q - 1}{a - 1} = 1 + a + \cdots + a^{q-1} \equiv q \pmod{a - 1},$$

we get that P divides q; hence, $P = q$. Next, q divides $g^{m/q} - 1$ and by Fermat's Little Theorem, q also divides $g^{q-1} - 1$. By a well-known

property of the Lucas sequences, q divides

$$\gcd(g^{m/q}-1, g^{q-1}-1) = g^{\gcd(m/q,q-1)}-1,$$

and, since q is the smallest prime factor of m, we have $\gcd(m/q, q-1) = 1$. Hence, q divides $g-1$. Finally, to see that in this last case q appears with exponent 1 in the factorization of the first factor, write $a-1 = qv$. Then

$$\frac{g^m-1}{g^{m/q}-1} = \frac{a^q-1}{a-1} = 1+a+\cdots+a^{q-1} = 1+(1+qv)+\cdots+(1+qv)^{q-1}.$$

In the right–hand side above, we use the Newton binomial formula for each of the summands and reduce the result modulo q^2 getting

$$\begin{aligned}\frac{g^m-1}{g^{m/q}-1} &\equiv q+qv(0+1+\cdots+q-1) \pmod{q^2}\\ &\equiv q+q^2v(q-1)/2 \pmod{q^2} \equiv q \pmod{q^2},\end{aligned}$$

where the last congruence above follows because q is odd, as a factor of the odd number m, so $(q-1)/2$ is an integer. The above congruence shows that q exactly divides the first factor, as claimed above.

Returning to (5.2), if the two factors on the right are coprime, it then follows that either the first factor or the second factor is a square. By a classical result of Ljunggren [6], the only positive integer solutions of the equation

$$\frac{x^n-1}{x-1} = y^2, \qquad \text{with} \quad x>1 \quad \text{and} \quad n\geq 3$$

are $(x,n,y) = (7,4,20)$ and $(3,5,11)$. Since our exponent m is odd, it follows that either $m/q = 1$, which is what we want to prove, or $g=3$ and $m/q = 5$. The second possibility leads to $m = 5q$, so $m \in \{15, 25\}$. However, neither of the numbers $(3^{15}-1)/2$ or $(3^{25}-1)/2$ is of the form $p\square$. Thus, this possibility cannot occur, and so $m = q$ is a prime.

Let us now look at the case when the greatest common divisor of the two factors on the right–hand side of (5.2) is precisely q. Since $q < g < p$, q must appear with even exponent in $(g^m-1)/(g-1)$, and since it appears with exponent 1 in the first factor in the right–hand side of (5.2), it follows that q must also divide the second factor. It then follows easily that $q \mid m/q$. Hence, $q^2 \mid m$. Now rewrite equation (5.2) as

$$p\square = \frac{g^m-1}{g-1} = \left(\frac{g^m-1}{g^{m/q^2}-1}\right)\left(\frac{g^{m/q^2}-1}{g-1}\right). \tag{5.3}$$

By an argument similar to the one used at the beginning of the proof of this proposition, the greatest common divisor of the two factors

appearing on the right–hand side of (5.3) above is a power of q. It is easy to see that the exponent of q in $(g^m-1)/(g^{m/q^2}-1)$ is exactly 2. Since the exponent of q in $(g^m-1)/(g-1)$ is even, it follows that the exponent of q in $(g^{m/q^2}-1)/(g-1)$ is also even. These arguments show that either $(g^m-1)/(g^{m/q^2}-1)$ is a square, or $(g^{m/q^2}-1)/(g-1)$ is a square. Assuming that $m > q^2$, the only possibility, via Ljunggren's result, is $g = 3$ and $m/q^2 = 5$, therefore $m = 5q^2$. However, q must divide $g-1 = 2$, and this is false since m must be odd. The conclusion is that $m = q^2$ must hold in this case and of course q divides $g-1$, which is what we wanted to prove. □

We next give a bound on m.

Proposition 5.3. *If $d = \square$, then $m < \max\{g^2, 8g\log(4g)\}$.*

Proof. We apply Proposition 5.2. If $m = q^2$ for some prime $q \mid g-1$, then obviously $m < g^2$. Assume next that $m = q$ is prime. We may also assume that $q > g$.

In particular, q does not divide $g-1$. Let

$$N = d\left(\frac{g^q-1}{g-1}\right) = d\prod_{i=1}^{k} Q_i^{\alpha_i} =: dM,$$

where $Q_1 < \cdots < Q_k$ are primes. It is clear that if Q is a prime dividing M, then $g^q \equiv 1 \pmod{Q}$, therefore either $q \mid Q-1$, or $Q \mid g-1$. The second possibility implies that $q = Q$, so q divides $g-1$, which is not allowed. Hence, $Q_i \equiv 1 \pmod{q}$ for all $i = 1, \ldots, k$. Therefore

$$g^q > \frac{g^q-1}{g-1} = M \geq (2q+1)^k,$$

so

$$k < \frac{q\log g}{\log(2q+1)}. \tag{5.4}$$

Observe next that d and M are coprime. Indeed, for if not, then d will be divisible with some prime Q so $d \geq Q \geq 2q+1 > 2d$, which is impossible.

Hence,

$$\sigma(N) = \sigma(d)\sigma(M).$$

Since d is a proper divisor of the perfect number N, we have that $\sigma(d) < 2d$, so therefore $\sigma(d) \leq 2d-1$. We get that

$$2 = \frac{\sigma(N)}{N} = \left(\frac{\sigma(d)}{d}\right)\left(\frac{\sigma(M)}{M}\right) \leq \left(\frac{2d-1}{d}\right)\left(\frac{\sigma(M)}{M}\right),$$

so

$$\frac{\sigma(M)}{M} \geq \frac{2d}{2d-1} = 1 + \frac{1}{2d-1} > 1 + \frac{1}{2g}.$$

Since $\sigma(M)/M < M/\phi(M)$, we get that

$$1 + \frac{1}{2g} < \frac{M}{\phi(M)} = \prod_{i=1}^{k} \left(1 + \frac{1}{Q_i - 1}\right).$$

Taking logarithms and using the fact that the inequality

$$x/2 < \log(1+x) < x \qquad \text{is valid for all} \quad x \in (0,1),$$

together with (5.4) and the fact that $q > g$, we get that

$$\begin{aligned} \frac{1}{4g} &< \log\left(1 + \frac{1}{2g}\right) < \sum_{i=1}^{k} \log\left(1 + \frac{1}{Q_i - 1}\right) < \sum_{i=1}^{k} \frac{1}{Q_i - 1} \\ &< \frac{1}{2q} \sum_{i=1}^{k} \frac{1}{i} < \frac{1}{2q}\left(1 + \int_1^k \frac{dt}{t}\right) = \frac{1}{2q}(1 + \log k) \\ &< \frac{1}{2q}\left(1 + \log\left(\frac{q \log g}{\log(2q+1)}\right)\right) < \frac{1}{2q}\log(eq) \end{aligned}$$

(here, we used the fact that since $q > g$, we have $\log(2q+1) > \log g$), which implies

$$q < 2g \log(eq) < 4g \log q, \tag{5.5}$$

where the last inequality on the right above follows because $q \geq 3 > e$. Since the function $x \mapsto x/\log x$ is increasing for $x > e$, one proves easily that

$$\text{if} \qquad \frac{x}{\log x} < A, \qquad \text{then} \qquad x < 2A \log A \qquad \text{whenever} \qquad A \geq 3.$$

Applying this to our inequality (5.5), which can be rewritten as $q/\log q < 4g$ with $x := q$ and $A := 4g$, we get that $q < 8g \log(4g)$, which is what we wanted to prove. □

5.3. **The case when m is odd and $d \neq \square$.**

5.3.1. *Preliminary results.* Throughout this section, instead of c_d we write c and we study the equation

$$u_m = cp\square, \tag{5.6}$$

where $\{u_n\}_{n \geq 0}$ is the Lucas sequence of general term $u_n = (g^n - 1)/(g-1)$ for all $n \geq 0$ of Example 1 of Section 2, $c \in \{2, \ldots, g-1\}$ is squarefree and $p > g$ is a prime. Later on, we shall also use the fact that du_m is perfect for some $d \leq g-1$ such that $dc = \square$. Observe that we can

assume $g \geq 4$, since if $g = 3$, then we are either in the $d = 1$ case which is treated in Section 5.2, or in the $d = 2$ case in which N is even, and this is treated in Section 3.

For a positive integer k let $z(k)$ be the minimal positive integer ℓ such that $k \mid u_\ell$. It is known that if q is a prime dividing $g - 1$, then $z(q^a) = q^a$.

If q is a prime not dividing $g - 1$, then $z(q) \mid q - 1$. (We exclude the case $q \mid g$ since then $z(q) = \infty$.) Moreover, if

$$u_{z(q)} = q^{e_q} \prod_{\substack{r \mid u_{z(q)} \\ r \neq q}} r^{e_r},$$

then for all $a \geq 1$, $z(q^a) = q^{\max\{0, a-e_q\}} z(q)$, so $q^{\max\{0,a-e_q\}} || z(q^a)$.

Then for all k, if $k = \prod_{q \mid k} q^{a_q}$, then $z(k) = \mathrm{lcm}[z(q^{a_q}) : q \mid k]$.

The above conditions can be reformulated as follows. For any prime p and any nonzero integer m let $v_p(m)$ be the exact exponent at which p appears in the factorization of m. If p is a prime not dividing $g - 1$ and $z(p) \nmid m$ then $v_p(u_m) = 0$. If $z(p) \mid m$ then

$$v_p(u_m) = v_p\left(u_{z(p)}\right) + v_p\left(\frac{m}{z(p)}\right).$$

If p is any odd prime with $p \mid g - 1$, then $v_p(u_m) = v_p(m)$.

We next define for a squarefree number $k > 1$ another parameter $Z(k)$ which closely related to $z(k)$ as follows. Write

$$u_{z(k)} = \prod_{p \mid k} p^{e_p} \prod_{\substack{q \nmid k \\ q \mid g-1}} q^{f_q} \prod_{\substack{r \mid u_{z(k)} \\ r \nmid k(g-1)}} r^{g_r}.$$

Then put

$$Z(k) := z(k) \prod_{\substack{p \mid k \\ e_p \equiv 0 \pmod 2}} p \prod_{\substack{q \nmid k \\ q \mid g-1 \\ f_q \equiv 1 \pmod 2}} q.$$

The following result now follows from the preceding remarks.

Proposition 5.4. *Suppose that k is squarefree and that for some $m \geq 1$ we have*

$$u_m = \prod_{p \mid k} p^{a_p} \prod_{\substack{q \nmid k \\ q \mid g-1}} q^{b_q} \prod_{\substack{r \mid u_m \\ r \nmid k(g-1)}} r^{c_r},$$

where a_p is odd for all $p \mid k$ and b_q is even for all $q \nmid k$ with $q \mid (g-1)$. Then

(i) *$Z(k) \mid m$;*

(ii) *if* $m = Z(k)\prod_{p|k(g-1)} p^{\alpha_p}\prod_{\substack{q|m\\ q\nmid k(g-1)}} q^{\beta_q}$, *then* α_p *is even for all primes* $p \mid k(g-1)$.

Proof. Since a_p is odd, it follows that $a_p \geq 1$, therefore k divides u_m. Thus, $z(k)$ divides m. Therefore, since $u_{z(k)} \mid u_m$, we have $a_p \geq e_p$. If e_p is even, then since a_p is odd, it follows that $a_p \geq e_p + 1$, and $e_p \geq 1$ since $k \mid u_{z(k)}$. Thus, for such p, we must have $z(p^{e_p+1}) = pz(p) \mid m$.

Next, again because $z(k) \mid m$, we also have $b_q \geq f_q$. But $q \mid g-1$ so $z(q^{f_q}) = q^{f_q} \| u_{z(k)}$, and it follows that $q^{f_q} \| z(k)$. Similarly, $q^{b_q} \| m$. Consequently, if f_q is odd, then $b_q \geq f_q + 1$, because b_q is even, so, in fact, $q^{f_q+1} \mid m$. Hence, m is a multiple of

$$A := \mathrm{lcm}[a : a \in \mathcal{A}],$$

where $\mathcal{A}$ is the following set of numbers

$$\begin{aligned} \mathcal{A} \;&:=\; \{z(k)\} \cup \{pz(p) : p \mid k \text{ and } e_p \equiv 0 \pmod 2\} \\ &\cup\; \{q^{f_q+1} : q \nmid k,\ q \mid (g-1) \text{ and } f_q \equiv 1 \pmod 2\}. \end{aligned}$$

However, it is easy to see that the above least common multiple is precisely $Z(k)$. This proves (i). Part (ii) is also immediate. □

We have the following corollary.

Corollary 5.5. *If* m *gives a solution to equation* $u_m = cp\square$ *with a prime* $p > g$ *and a squarefree integer* c *with* $1 \leq c \leq g-1$, *then* m *is a multiple of* $Z(c)$. *Furthermore, the exponents of the primes dividing* $c(g-1)$ *appear in the factorization of* $m/Z(c)$ *at an even exponent.*

This suggests to do the following. Given an odd squarefree $k > 1$, let $\mathcal{M}_k$ denote the set of odd positive integers m such that the relation

(5.7)
$$u_m = k\delta_m\square \qquad \text{holds with some } \mu^2(k\delta_m) = 1 \quad \text{and} \quad \gcd(\delta_m, g-1) = 1.$$

Here, we use the Möbius function $\mu(n)$ with its standard meaning, namely that it is 0 if n is not squarefree, and that it is $(-1)^{\omega(n)}$, where $\omega(n)$ is the number of distinct prime factors of n, in case n is squarefree. From what we have said above, we have that $Z(k)$ divides m for all $m \in \mathcal{M}_k$. Furthermore, if m_1 divides m_2 and are both in $\mathcal{M}_k$, then all prime factors dividing $k(g-1)$ appear at even exponents in m_2/m_1. So, it makes sense to study what happens with δ_{m_1} and δ_{m_2} in the extremal case when m_2/m_1 is either a prime not dividing $g-1$, or a square of prime dividing $k(g-1)$.

We have the following proposition, which can be thought of as a generalization of Proposition 5.2.

Proposition 5.6. *Let $k > 1$ be odd and squarefree and let $m_1,\ m_2$ be odd positive integers. Assume that*

$$u_{m_1} = k\delta_{m_1}\square, \qquad \text{and} \qquad u_{m_2} = k\delta_{m_2}\square,$$

where

$$\mu^2(k\delta_{m_1}) = \mu^2(k\delta_{m_2}) = \gcd(\delta_{m_1}, g-1) = \gcd(\delta_{m_2}, g-1) = 1,$$

and $m_2 = m_1 t$, with t being either a prime not dividing $k(g-1)$, or the square of a prime dividing $k(g-1)$. Then $\omega(\delta_{m_2}) \geq \omega(\delta_{m_1})$. The above inequality is always strict except possibly when t is a prime factor of δ_{m_1}.

Proof. To begin write $m = p_1 p_2 \cdots p_s$, with $3 \leq p_1 \leq p_2 \leq \cdots \leq p_s$ and

$$u_m = \left(\frac{u_m}{u_{m/p_1}}\right)\left(\frac{u_{m/p_1}}{u_{m/(p_1p_2)}}\right)\cdots\left(\frac{u_{m/(p_1\cdots p_{s-1})}}{u_{m/(p_1\cdots p_s)}}\right) =: N_{m,1}\cdots N_{m,s}.$$

The main observation here is that $\gcd(N_{m,i}, N_{m,j}) = 1$ for all $1 \leq i < j \leq s$ except when $p_i = \cdots = p_j := q$ is a prime factor of $g-1$. In this last case, $q \| N_{m,\ell}$ for all $\ell = i, i+1, \ldots, j$. Indeed, assume that $q \mid \gcd(N_{m,i}, N_{m,j})$. Then $q \mid u_{m/(p_1\cdots p_{j-1})} \mid u_{m/(p_1\cdots p_i)}$ (because $i < j$) and also $q \mid N_{m,i} = u_{m/(p_1\cdots p_{i-1})}/u_{m/(p_1\cdots p_i)}$ (here, $p_0 := 1$). Hence,

$$q \mid \gcd\left(u_{m/(p_1\cdots p_i)}, \frac{u_{m/(p_1\cdots p_{i-1})}}{u_{m/(p_1\cdots p_i)}}\right).$$

It is well-known and easy to see that this is possible only when $q = p_i$. Now $q \mid g^{m/(p_1\cdots p_{j-1})} - 1 = g^{p_j\cdots p_s} - 1$, and $q \mid g^{p_i - 1} - 1$, so $q \mid g^{\gcd(p_i-1, p_j\cdots p_s)} - 1$. Since $p_i - 1$ and $p_j \cdots p_s$ are coprime, we get that $q \mid g - 1$. Since $q \mid u_{m/p_1\cdots p_{j-1}}/u_{m/(p_1\cdots p_j)}$ and $q \mid g-1$, it follows that $q = p_j$. Hence, $q = p_i = \cdots = p_j$, which is what we claimed. The remaining assertion that $q \| N_{\ell,m}$ for $\ell = i, i+1, \ldots, j$ is also clear. (This argument has appeared before in many places such as in the proof of Lemma 3 in [8], for example.)

Now write

$$N_{m,i} = A_{m,i}B_{m,i}\square, \qquad \text{for} \qquad i = 1, \ldots, s,$$

where $\mu^2(A_{m,i}B_{m,i}) = 1$, all prime factors of $B_{m,i}$ divide $g-1$, and $A_{m,i}$ is coprime to $g-1$. Since for any odd prime p and any positive integer l, $p \mid g-1$ implies that the exponents of p in the factorizations of l and u_l are the same, it follows easily that $B_{m,i} = p_i$ or 1 according to whether p_i divides $g-1$ or not. Furthermore, by the observation made above, any two of the positive integers $A_{m,1}, \ldots, A_{m,s}$ are coprime.

Assume now that $m \in \mathcal{M}_k$; i.e., $u_m = k\delta_m\square$ with $\mu^2(k\delta_m) = \gcd(\delta_m, g-1) = 1$. Then, since $k = \gcd(k, g-1) \cdot (k/\gcd(k, g-1))$, we have

$$\prod_{i=1}^{s} B_{m,i} = \gcd(k, g-1)\square, \qquad \text{and} \qquad \prod_{i=1}^{s} A_{m,i} = \left(\frac{k}{\gcd(k, g-1)}\right)\delta_m\square$$

(the right–most $\square$ above is in fact equal to 1). Assume next that $m := m_1$ and that $m_2 := m_1 t$ is also in $\mathcal{M}_k$. Assume also that $t = q$ is a prime with $q \nmid g-1$.

We look at

$$u_{m_2} = N_{m_2,1} \cdots N_{m_2,s+1}$$

and compare this factorization with the corresponding one

$$u_{m_1} = N_{m_1,1} \cdots N_{m_1,s}$$

for u_{m_1}. We let i_0 be the minimal index in $\{0, 1, \ldots, s\}$ for which the inequality $p_i \le q < p_{i+1}$ holds, where $p_0 := 1$ and $p_{s+1} := \infty$. Observe that i_0 is the only index i such that the inequality $p_i < q < p_{i+1}$ holds in case $q \nmid m_1$, whereas i_0 is the minimal index i for which $p_i = q$ in case $q \mid m_1$. Here, in the extreme cases $i_0 = 0$ and $i_0 = s$ we read that $q < p_1$ and $q \ge p_s$, respectively. We have $N_{m_2,\ell+1} = N_{m_1,\ell}$ for all $\ell \ge i_0 + 1$. If $1 \le \ell \le i_0$, then

$$N_{m_2,\ell} = \frac{u_{drq}}{u_{dq}} \qquad \text{and} \qquad N_{m_1,\ell} = \frac{u_{dr}}{u_d},$$

where $d := p_{\ell+1} \cdots p_s$ and $r := p_\ell$. Let us see that $N_{m_1,\ell} \mid N_{m_2,\ell}$ for all $\ell = 1, \ldots, i_0 - 1$. Indeed, if $q \ne r$ this is true even with $\ell := i_0$ because then

$$\frac{N_{m_2,\ell}}{N_{m_1,\ell}} = \frac{u_{dqr}u_d}{u_{dq}u_{dr}} = \frac{(g^{dqr}-1)(g^d-1)}{(g^{dq}-1)(g^{dr}-1)} = \Phi_{qr}(g^d) \in \mathbb{Z}, \tag{5.8}$$

where $\Phi_{qr}(X)$ is the cyclotomic polynomial whose roots are the primitive roots of unity of order qr. Thus, $N_{m_1,\ell} \mid N_{m_2,\ell}$ for all $\ell = 1, \ldots, i_0$, if $q \ne r$. On the other hand, the case $q = r$ leads to $p_{i_0} \le q = r = p_\ell$, so $\ell \ge i_0$ and this is possible when $\ell \le i_0$ only when $\ell = i_0$. Thus, the divisibility relation $N_{m_1,\ell} \mid N_{m_2,\ell}$ still holds for all $\ell = 1, \ldots, i_0 - 1$, and one checks that $N_{m_2,i_0+1} = N_{m_1,i_0}$ in case $q = p_{i_0} \mid m_1$.

So, to summarize, we showed that

$$N_{m_2,\ell} = N_{m_1,\ell-1} \qquad \text{for all} \qquad \begin{cases} i_0 + 2 \le \ell \le s+1, & \text{if } q \nmid m_1, \\ i_0 + 1 \le \ell \le s+1, & \text{if } q \mid m_1, \end{cases}$$

and that

$$N_{m_1,\ell} \mid N_{m_2,\ell} \qquad \text{for all} \qquad \begin{cases} 1 \le \ell \le i_0, & \text{if } q \nmid m_1, \\ 1 \le \ell \le i_0 - 1, & \text{if } q \mid m_1. \end{cases}$$

Put $j_0 := i_0$ if q does not divide m_1 and $j_0 := i_0 - 1$ if q divides m_1. Recall that we are assuming here that q does not divide $g-1$.

Let us treat first the case that q does not divide δ_{m_1}. Then the exponents of all primes dividing δ_{m_1} in u_{m_1} and u_{m_2} are the same.

This shows that

$$\begin{aligned} A_{m_2,\ell} &= A_{m_1,\ell-1}, \quad \text{and} \quad B_{m_2,\ell} = B_{m_1,\ell-1}, \text{ for all } j_0+2 \le \ell \le s+1, \\ A_{m_1,\ell} &= A_{m_2,\ell}, \quad \text{and} \quad B_{m_2,\ell} = B_{m_1,\ell}, \text{ for all } 1 \le \ell \le j_0. \end{aligned} \tag{5.9}$$

However, we still have the number

$$N_{m_2,j_0+1} = A_{m_2,j_0+1} B_{m_2,j_0+1} \square$$

to consider. By what was shown above, and since we are assuming that q does not divide $g-1$, we have $B_{m_2,j_0+1} = 1$. Furthermore, the number N_{m_2,j_0+1} is not a perfect square by Ljunggren's result mentioned in the proof of Proposition 5.2 (observe that the two exceptional solutions of the equation $(x^n-1)/(x-1) = y^2$ with $x > 1$ and $n > 2$ which have $(x,n) = (3,5)$ and $(7,4)$ do not apply to our instance since for us $g \ge 4$ and the exponents are odd). Hence, $A_{m_2,j_0+1} > 1$, and since

$$\prod_{\ell=1}^{s+1} B_{m_2,\ell} = \prod_{\ell=1}^{s} B_{m_1,\ell} = \gcd(k, g-1)\square,$$

we therefore get that

$$\frac{\delta_{m_2} k}{\gcd(k,g-1)} = \prod_{\ell=1}^{s+1} A_{m_2,\ell} \text{ is a proper multiple of } \prod_{\ell=1}^{s} A_{m_1,\ell} = \frac{\delta_{m_1} k}{\gcd(k,g-1)}.$$

(Note that we have used the fact that the $A_{m_i,\ell}$ are coprime and squarefree, so the square $\square$ in the equations for their products with $i = 1, 2$ derived above in each case is 1, so such squares do not interfere.) So, we see that if $t = q$ and $q \nmid \delta_{m_1}$, then $\delta_{m_2}/\delta_{m_1} > 1$ is an integer, so $\omega(\delta_{m_2}) > \omega(\delta_{m_1})$.

Minor variations of this argument apply in the remaining cases. For example, suppose that we still have $t = q$ but $q \mid \delta_{m_1}$. Suppose first that q does not divide m_1, so $j_0 = i_0$. With the above notations, let i_1 be the unique index $i \in \{1, \ldots, s\}$ such that $q \mid A_{m_1,i_1}$. Then $q \mid N_{m_1,i_1}$. A minute of reflection convinces us that p_{i_1} is the minimal prime factor of the index of appearance $z(q)$ of q in $\{u_n\}_{n \ge 0}$. Note that $z(q) \le q - 1 < q$, therefore $q > p_{i_1}$. In particular, $i_1 \le i_0$. Thus, since N_{m_1,i_1} is divisible by q at an odd exponent and $m_2 = m_1 q$, it follows that N_{m_2,i_1} is divisible by q at an even exponent. Everything else stays the same as before so relations (5.9) still hold for all $\ell \in \{1, 2, \ldots, s+1\}$ except for $\ell = j_0 + 1$ and $\ell = i_1$, while when $\ell = i_1$, we have that

$A_{m_1,i_1}/q \mid A_{m_2,i_1}$ (and $B_{m_2,i_1} = B_{m_1,i_1}$). Thus, here we loose one prime out of δ_{m_1} (namely the prime q), but we gain at least one other prime from A_{m_2,j_0+1}. This shows that $\omega(\delta_{m_2}) \geq \omega(\delta_{m_1})$, but it is no longer true that δ_{m_1} divides δ_{m_2} in this case (although δ_{m_1}/q divides δ_{m_2}).

Assume now that it is still the case that $t = q$ divides δ_{m_1}, but that $q \mid m_1$. Then $j_0 = i_0 - 1$ and $i_1 < i_0$. With the same notations as above, we have again that $q \mid N_{m_1,i_1}$. However, recalling that $q^{e_q} \| u_{z(q)}$, it then follows that $q^a \| m_1$, where $a \geq 1$ is some integer such that $a + e_q \equiv 1 \pmod 2$. Since $p_{i_1} < q$, it follows that $m_1/(p_1 \cdots p_{i_1-1})$ is a multiple of $z(q)q^a$, while $m_2/(p_1 \cdots p_{i_1-1})$ is a multiple of $z(q)q^{a+1}$. So, again relations (5.9) hold for all $\ell \in \{1, \ldots, s+1\}$ except for $\ell = j_0 + 1$ and $\ell = i_1$, while for $\ell = i_1$, we get, as in the previous case, that $A_{m_1,i_1}/q \mid A_{m_2,i_1}$ (and $B_{m_2,i_1} = B_{m_1,i_1}$). So, again here we loose one prime out of δ_{m_1} (namely the prime q), but we gain at least one other prime from $A_{m_2,j_0+1} > 1$. So, again we have that $\omega(\delta_{m_2}) \geq \omega(\delta_{m_1})$.

Let us outline the case when $t = q^2$ and q divides $k(g-1)$. We keep the notation i_0 as the minimal index i in $\{0, \ldots, s\}$ such that $p_i \leq q < p_{i+1}$. Then as in the preceding case one argues that there exists $j_0 \in \{0, \ldots, s+2\}$ such that

$$N_{m_2,\ell} = N_{m_1,\ell-2} \qquad \text{for all} \qquad \ell \in \{j_0 + 3, \ldots, s+2\}, \tag{5.10}$$

and

$$N_{m_1,\ell} \mid N_{m_2,\ell} \qquad \text{for all} \qquad \ell \in \{1, \ldots, j_0\}. \tag{5.11}$$

Here, again $j_0 := i_0$ if q is coprime to m_1 and $j_0 := i_0 - 1$ if $q \mid m_1$. For the divisibility relation (5.11), one uses the fact that the polynomial

$$\frac{(X^{q^2 r} - 1)(X - 1)}{(X^{q^2} - 1)(X^r - 1)} = \Phi_{q^2 r}(X)\Phi_{qr}(X) \qquad \text{has integer coefficients,}$$

instead of the argument from relation (5.8). Hence, $A_{m_2,\ell} = A_{m_1,\ell-2}$ and $B_{m_2,\ell} = B_{m_1,\ell-2}$ for all $\ell \in \{j_0+3, \ldots, s+2\}$. By arguments similar to the previous ones, we get easily when q divides $g-1$, that since q does not divide δ_{m_1}, we also have that $A_{m_1,\ell} \mid A_{m_2,\ell}$ and $B_{m_1,\ell} = B_{m_2,\ell}$ for all $\ell \in \{1, \ldots, j_0\}$.

When q divides $k/\gcd(k, g-1)$, a similar conclusion can be deduced in the following way. Observe first that $q \mid k \mid g^{m_1} - 1$ and $q \mid g^{q-1} - 1$ by Fermat's Little Theorem. Hence, $q \mid g^{\gcd(m_1, q-1)} - 1$ and since $q \nmid g - 1$, it follows that $q \mid u_{\gcd(m_1,q-1)}$. In other words, $i_0 > 0$ and $q \mid u_{p_1 \ldots p_{j_0}}$. Now each one of the expressions $N_{m_1,\ell}$ for $\ell \in \{1, \ldots, j_0\}$ is of the form $(g^{dr} - 1)/(g^d - 1)$ for some prime $r < q$ and its corresponding $N_{m_2,\ell}$ is of the form $(g^{drq^2} - 1)/(g^{dq^2} - 1)$. It is now easy to check that the exponent of the prime q has the same residue class modulo 2 in the

factorization of $N_{m_1,\ell}$ and $N_{m_2,\ell}$, respectively, which does imply that $A_{m_1,\ell} \mid A_{m_2,\ell}$ for $\ell \in \{1, \ldots, j_0\}$. We still have N_{m_2,j_0+1} and N_{m_2,j_0+2} to look at. Since $q \mid k(g-1)$, we get that $B_{m_2,j_0+2} = B_{m_2,j_0+1}$ and their common value is q or 1 according to whether q divides $(g-1)$ or $k/\gcd(k, g-1)$, respectively.

Recall that A_{m_2,j_0+1} and A_{m_2,j_0+2} are coprime. If it were true that both A_{m_2,j_0+1} and A_{m_2,j_0+2} were 1, we would then get that with some divisor d of m_1 (here, $d := p_{i_0+1} \cdots p_s$ if $q \nmid m_1$ and $d := p_{i_0} \cdots p_s$ when $q \mid m_1$), we would have

$$\frac{g^{dq}-1}{g^d-1} = B_{m_2,j_0+2}\square, \qquad \text{and} \qquad \frac{g^{dq^2}-1}{g^{dq}-1} = B_{m_2,j_0+1}\square.$$

By Ljunggren's result, neither of B_{m_2,j_0+2} or B_{m_2,j_0+1} can be 1 so both must be q. By multiplying the above two relations, we would get $(g^{dq^2}-1)/(g^d-1) = \square$, which again is impossible. Thus, $e := A_{m_2,j_0+1}A_{m_2,j_0+2} > 1$. Because, as we have seen, $A_{m_1,\ell} | A_{m_2,\ell}$ for $1 \le \ell \le j_0$ and $A_{m_1,\ell} = A_{m_2,\ell+2}$ for $j_0+1 \le \ell \le s$, the product of the $A_{m_1,\ell}$ divides the product of the $A_{m_2,\ell}$ divided by e. And since $e > 1$, one gets that the corresponding ratio of the product of the $A_{m_1,\ell}$ to the product of the $A_{m_2,\ell}$ is greater than 1. But this ratio is also the ratio $\delta_{m_2}/\delta_{m_1}$. Since both δ_{m_1} and δ_{m_2} are squarefree, it follows that $\omega(\delta_{m_2}) > \omega(\delta_{m_1})$. The proposition is therefore proved. □

Remark 3. The referee sketched a somewhat shorter proof of Proposition 5.6 using, in addition to Ljunggren's result, Lemma 2.4 from [10]. We thank the referee for the alternative proof of this statement.

The following corollary is of interest:

Corollary 5.7. (i) *If $m_1 \mid m_2$ are in $\mathcal{M}_k$, $m_2/m_1 > 1$ and $\delta_{m_1} = 1$, then $\delta_{m_2} > 1$.*

(ii) *If $m_1 \mid m_2$ are in $\mathcal{M}_k$, $m_2/m_1 > 1$ and $\delta_{m_1} > g$ is prime, then $\delta_{m_2} > 1$ and, in addition, if it is prime, then $m_2 = m_1\delta_{m_1}$.*

Proof. Part (i) is immediate. Indeed, let $r \mid m_2/m_1$ and assume for a contradiction that $u_{m_2} = k\square$. Then $r^2 \mid m_2/m_1$ if r divides $k(g-1)$. Let $t := r^2$ if r divides $k(g-1)$ and $t := r$ otherwise. Then $m_1 t \mid m_2$, and $\delta_{m_1} = 1$, so by Proposition 5.6, we have $\delta_{m_1 t} > 1$. Hence, $\omega(\delta_{m_1 t}) \ge 1$. By induction over the number of prime factors of $m_2/(m_1 t)$ using Proposition 5.6, we get that $\omega(\delta_{m_2}) \ge 1$, a contradiction.

As for (ii), denote $p := \delta_{m_1}$. Let r be some prime factor of m_2/m_1. Let again $t := r^2$ if r divides $k(g-1)$ and $t := r$ otherwise. Then $m_1 t$ divides m_2.

Furthermore, by Proposition 5.6, if $r \ne p$ then $\omega(\delta_{m_1 t}) \ge 2$.

Now by induction over the number of prime factors of $m_2/(m_1 t)$, we get, by Proposition 5.6 again, that $\omega(\delta_{m_2}) \geq 2$, a contradiction. Therefore we must have $r = p$.

But this is then true for every prime factor of m_2/m_1, so $m_2 = m_1 p^a$ for some $a \geq 1$.

Let us now show that $a = 1$. Assume otherwise. Proposition 5.6 shows that $u_{m_1} = kp\square$ and $u_{pm_1} = kq\square$, where $q = \delta_{m_1 p}$ is a prime. Then q is not the same as p (in fact, $q \equiv 1 \pmod{p}$ since $p > g$). Therefore, by Proposition 5.6 applied to $m_1 p$ and $m_1 p^2$, we get $\omega(\delta_{m_1 p^2}) > \omega(\delta_{m_1 p}) = 1$.

Now again by induction over a using Proposition 5.6, we get that $\omega(\delta_{m_2}) = \omega(\delta_{m_1 p^a}) \geq \omega(\delta_{m_1 p^2}) \geq 2$, which is the final contradiction.

This establishes the desired corollary. □

5.3.2. *An algorithm to compute all solutions.* We are now ready to explain an algorithm which detects all possible candidates for m such that $N = du_m$ is perfect in this case, namely N is odd, $p > g$, $d \neq \square$, m is odd and $g \geq 4$.

We return to equation (5.6); i.e., $u_m = cp\square$ with $c = c_d$. First eliminate three cases where modular constraints imply no solution: d even, $g \equiv 2 \pmod{4}$ with $d \equiv 1 \pmod{4}$, and $4 \mid g$ with $d \equiv 3 \pmod{4}$.

Observe that, since here $\delta_m = p > g$, we have $(\delta_m, g-1) = 1$, so $m \in \mathcal{M}_c$. By Proposition 5.4, $m_d := Z(c) \mid m$. Thus, $u_{m_d} = c\delta_d\square$ with δ_d squarefree. Clearly, $m_d \in \mathcal{M}_c$. Put $m =: m_d n$. Then, by Corollary 5.5, all prime factors of n dividing $c(g-1)$ appear at even exponents in n. The goal is to give a short list containing all the candidates for n.

Recall that

$$u_{m_d} = c\delta_d\square, \qquad \text{where} \qquad \mu^2(c\delta_d) = \gcd(\delta_d, g-1) = 1.$$

If $\omega(\delta_d) \geq 2$, then Proposition 5.6 plus an induction on the number of prime factors of m/m_d, shows that

$\omega(\delta_m) \geq 2$ for all $m \in \mathcal{M}_c$, so we don't get any convenient solutions n.

If δ_d is a prime, then Corollary 5.7 (ii) shows that $n \in \{1, \delta_d\}$.

Assume next that $\delta_d = 1$. Write

$$N = \left(d\frac{g^{m_d}-1}{g-1}\right)\left(\frac{g^{m_d n}-1}{g^{m_d}-1}\right). \tag{5.12}$$

Assume first that the two factors on the right in relation (5.12) above are not coprime. Let q be a prime dividing both these two factors. If $q \mid u_{m_d}$, then since $q \mid (g^{m_d n}-1)/(g^{m_d}-1) = u_{m_d n}/u_{m_d}$, we then get

that $r \mid n$, where $r = q$. If not, then $q \mid d$ and $q \nmid u_{m_d}$, so $z(q) \mid m_d n$ and $z(q) \nmid m_d$. Hence, there exists a prime r such that $r \mid n$, and this prime is either q if $q \mid u_{m_d}$, or it is a prime factor of $z(q)/\gcd(z(q), m_d)$, where $q \mid d$, otherwise. At any rate, we can say that n is a multiple of t, where $t := r$, if r does not divide $c(g-1)$, and $t := r^2$, if r divides $c(g-1)$, and r is one of the previous primes. Now

$$u_{m_d t} = c\delta_{d,t}\square,$$

where by Corollary 5.7 (i), we have that $\delta_{d,t} > 1$. If $\omega(\delta_{d,t}) \geq 2$, then there are no convenient solutions n, while if $\delta_{d,t}$ is a prime then $n \in \{t, t\delta_{d,t}\}$, by Corollary 5.7 (ii).

Assume next that the two factors appearing on the right in equation (5.12) are coprime. Then

$$2N = \sigma(N) = \sigma(du_{m_d})\sigma\left(\frac{g^{m_d n}-1}{g^{m_d}-1}\right).$$

Now $du_{m_d} < \sigma(du_{m_d}) < 2du_{m_d}$. We know that if $q^a \| du_{m_d}$, then $q^a \| 2N$. Hence, there must exist a prime number q dividing $\sigma(du_{m_d})$ which does not divide du_{m_d}. If this prime is 2, then $\sigma(u_{m_d n}/u_{m_d})$ is odd, therefore $u_{m_d n}/u_{m_d} = \square$, which is not allowed if $n > 1$ by Ljunggren's result. Hence, q is odd. We thus get that $q \mid (g^{m_d n}-1)/(g^{m_d}-1)$, therefore $z(q) \mid m_d n$, but $z(q) \nmid m_d$. Let r be some prime factor of $z(q)/\gcd(z(q), m_d)$. Then n is divisible by t, where again as before we put $t := r$, if r does not divide $c(g-1)$, and $t := r^2$, otherwise. Now write

$$u_{m_d t} = c\delta_{d,t}\square.$$

Then $\delta_{d,t} > 1$ by Corollary 5.7 (i). If $\omega(\delta_{d,t}) \geq 2$, then there are no such solutions n. Finally, if $\delta_{d,t}$ is a prime, then $n \in \{t, t\delta_{d,t}\}$, by Corollary 5.7 (ii).

This exhausts all the possibilities, and so all the potential candidates m such that du_m is perfect are obtained in one of the ways described above.

6. The proof of Theorem 1

We start with (i). If N is even, then Proposition 3.1 shows that $N < g^2$. In case N is odd, then $N < g^m$, so it suffices to bound m. When N is odd and the Eulerian prime p is small, then Proposition 4.2 shows that $m < 144g^3 < g^{11}$, while if $p > g$ is large but m is even, then $m \leq 216g^{5/2} < g^{11}$ because $g \geq 2$. When p is large and $d = \square$, then Proposition 5.3 shows that either $m < g^2$, or $m < 8g\log(4g) \leq 8g\log(g^3) = 24g\log g < g^{11}$. Summarizing, in all cases except the last one when N is odd, p is large and $d \neq \square$, we have that $m < g^{11} <$

$g^{g^4} < g^{g^{g^2}}$. So, let us look at the last case which can occur only when $g \geq 4$.

It is clear that $z(c_d) \leq c_d \leq g-1$, therefore $m_d = Z(c_d) \leq z(c_d)d(g-1) \leq (g-1)^3$. Hence, prime factors q of either du_{m_d}, or of $\sigma(du_{m_d})$, do not exceed $2g^{(g-1)^3}$ because du_{m_d} divides a perfect number, so any prime factor r of their index of appearance in u_{m_d} is at most as large as the same bound $2g^{(g-1)^3}$. Hence, with the notations from Section 5.3.2, we have that either $t \leq r \leq 2g^{(g-1)^3}$, or $t = r^2 \leq (g-1)^2$, with this case appearing only provided that $r \mid (g-1)$. Observe that $(g-1)^2 < 2g^{(g-1)^3}$ since $g \geq 4$. Thus, $m_d t < 2(g-1)^3 g^{(g-1)^3}$, and so any prime factor of $u_{m_d t}$ is at most

$$g^{2(g-1)^3 g^{(g-1)^3}} < g^{g^{(g-1)^3+4}}. \tag{6.1}$$

Since $g \geq 4$, we have that $g^3 > (g-1)^3 + 4$, therefore the expression appearing on the right hand side in inequality (6.1) above is less than $g^{g^{g^3}}$, which completes the proof of part (i) of the theorem.

We next address (ii). If N is even, then Proposition 3.1 shows that either $m = 1$ and $N < g$, or $m = 2$ and $d = 2^a$ and $g + 1 = 2^b(2^p - 1)$ for some nonnegative integers a and b. We can see that when $m = 2$, the number N is (at best) uniquely determined. Thus, the number of even perfect repdigits in base g is less than g.

Assume now that N is odd and that the Eulerian prime p is small, so $p < g$. Then the number of choices for the pair (d, p) is less than g^2. For each such choice, every m arises as $X_n = g^{\lfloor m/2 \rfloor}$, where $X = X_n$ arises as the first coordinate of a positive integer solution (X, Y) of either equation (4.4), or of equation (4.5), depending on the parity of m. If $n \geq 7$ in the first case, or $n \geq 13$ in the second case, then X_n has a primitive divisor, so $X_n = g^{\lfloor m/2 \rfloor}$ can happen for at most one such n. Hence, the number of solutions m when (p, d) is given is $\leq (6+1) + (13+1) = 20$. So, we get a totality of at most $20g^2$ such solutions.

We next consider the case when N is odd, p is large and m is even. Given d, the number λ_d used in the proof of Proposition 5.1 is a divisor of c_d, so it can have at most c_d values.

Given λ_d, the number $m = 2m_1$ arises from a relation as $X_n = g^{\lfloor m_1/2 \rfloor}$, where $X = X_n$ is the first coordinate of a positive integer solution (X, Y) to one of the two equations arising from (5.1). The previous argument shows that each one of them has at most 20 solutions. Thus, we get at most $2 \times 20 c_d < 40g$ solutions m for each fixed value of d, therefore a totality of at most $40g^2$ solutions all together in this case.

We next consider the case when N is odd, p is large and $d = \square$. Then, by Propositions 5.2 and 5.3, we get that either $m = q^2$, where q is a prime factor of $g-1$, or $m = p < 8g\log(4g) \leq 8g\log(g^3) = 24g\log g < 24g^2$. The number $g-1$ has less than g prime factors. Hence, the number of solutions in this case is less than $24g^2 + g$.

We now consider the last case when N is odd, p is large and $d \neq \square$. Here, $g \geq 4$. Given d, we compute δ_d. If $\omega(\delta_d) \geq 2$, we are through and there are no such solutions. If δ_d is a prime, then we have two possibilities for n. Suppose now that $\delta_d = 1$. We have $m_d = Z(c_d) < g^3$ as we saw in the proof of part (i). Therefore $du_{m_d} < \sigma(du_{m_d}) < 2du_{m_d} < 2g^{m_d} < g^{g^3}$, again because du_{m_d} divides a perfect number. Thus, the totality of the number of prime factors of $du_{m_d}\sigma(du_{m_d})$ is less than

$$\frac{g^3\log g}{\log 2} + \frac{g^3\log g}{\log 2} < g^4.$$

Here, we used the inequality $g^2 \leq 2^g$ valid for all $g \geq 4$ in the form $(2\log g)/(\log 2) \leq g$. Each one of the prime factors of $du_{m_d}\sigma(du_{m_d})$ determines, using Proposition 5.6, at most one value for t. For each of these numbers t, we compute $u_{m_d t} = c_d\delta_{d,t}\square$, and if $\delta_{d,t}$ is a prime, then $m \in \{m_d t, m_d t\delta_{d,t}\}$; otherwise, there is no solution for such t. Thus, we get at most $2(g^4+1)$ possibilities once d is fixed, so a totality of at most $2g^5 + 2g$ possibilities altogether in this case.

To summarize, the number of solutions is

$$< g + 20g^2 + 40g^2 + (24g^2 + g) + (2g^5 + 2g) = 2g^5 + 84g^2 + 4g. \tag{6.2}$$

The above bound is less than $4g^5$ for all $g \geq 4$. When $g = 3$, the last term $(2g^5 + 2g)$ does not appear in the sum from (6.2), so the bound is in fact $84g^2 + 2g < 4g^5$. This completes the proof of (ii) and of the theorem.

7. The computations

The algorithms described in Remark 1 at the end of Section 4 (the "small Eulerian prime p case"), Remark 2 at the end of Section 5.1 (the "even m, large p case") and in Section 5.3.2 (the "odd m large p case") were implemented in Mathematica. No odd perfect repdigits were found for any digit d up to $g = 333$ and there is no particular reason, other than computational resources, why this could not be carried through to higher values of g.

There was a need to solve Pell equations $x^2 - Dy^2 = \pm 1$ with large D, and this posed no particular obstacle using Mathematica's function "Reduce". As expected, at times we obtained very large fundamental

solutions. When solving the generalized Pell equation $Ax^2 - By^2 = \pm 1$, using the method based on the standard equation, sometimes there was a need to find the square root of a very large integer when it was a square. We simply tested for squareness using up to 1000 quadratic residues. With success we then used indefinite precision floating point arithmetic to give a complete test and found the square root when it existed.

In computing the function Z we avoided factoring integers of the order of 100 or more digits, which was slow in Mathematica.

Finally, given values of d and very large values of m, in the odd m large p case, we needed to test whether repdigits

$$N := d\left(\frac{g^m - 1}{g - 1}\right)$$

were perfect or not. We adopted a strategy similar to the following example, and this worked in each case considered.

Let $d = 23,\ g = 54,\ m = 102735452373554407$ so

$$N = 23\left(\frac{54^m - 1}{53}\right).$$

Now $23 \mid 54^{m \pmod{\varphi(23)}} - 1$ and $23^2 \nmid 54^{m \pmod{\varphi(23^2)}} - 1$ where $\varphi(n)$ is Euler's phi function. Hence $23^2 \| N$. But $\sigma(23^2) = 7 \cdot 79$ and $7 \nmid 54^{m \pmod{\varphi(7)}} - 1$, so N is not perfect.

Copies of the Mathematica code are available on request from the first author.

Acknowledgements. We thank the referees for numerous helpful comments and for pointing out several small computational flaws throughout several preliminary versions of this manuscript. During the preparation of this paper, F. L. was supported in part by Grants SEP-CONACyT 79685 and PAPIIT 100508.

References

1. Y. Bilu, G. Hanrot and P. M. Voutier with an appendix by M. Mignotte, 'Existence of primitive divisors of Lucas and Lehmer numbers', *J. reine angew. Math.* **539** (2001), 75–122.
2. K. A. Broughan and Q. Zhou, 'Odd repdigits to small bases are not perfect', *INTEGERS*, to appear.
3. R. D. Carmichael, 'On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$', *Ann. Math. (2)* **15** (1913), 30–70.
4. L. K. Hua, *Introduction to number theory*, Springer-Verlag, 1982.
5. M. J. Jacobson, Jr. and H. C. Williams, *Solving the Pell equation*, Springer, 2009.

6. W. Ljunggren, 'Some theorems on indeterminate equations of the form $\frac{x^n-1}{x-1} = y^q$', *Norsk Mat. Tidsskr.* **25** (1943), 17–20.
7. F. Luca and M. Křížek, 'On the solutions of the congruence $n^2 \equiv 1 \pmod{\phi^2(n)}$', *Proc. Amer. Math. Soc.* **129** (2001), 2191–2196.
8. F. Luca and P. Pollack, 'Multiperfect numbers with identical digits', *J. Number Theory* **131** (2011), 260–284.
9. P. Pollack, 'Perfect numbers with identical digits', *INTEGERS* **11A** (2011), A18.
10. J. Voight, 'On the nonexistence of odd perfect numbers', *MASS selecta*, 293–300, Amer. Math. Soc., Providence, RI, 2003.
11. D. T. Walker, 'On the diophantine equation $mX^2 - nY^2 = \pm 1$', *Amer. Math. Monthly* **74** (1967), 504–513.
12. M. Ward, 'The intrinsic divisors of Lehmer numbers', *Ann. Math. (2)* **62** (1955), 230–236.