A generalized Ramanujan-Nagell equation related to certain strongly regular graphs

Benne de Weger
Eindhoven University of Technology
b.m.m.d.weger@tue.nl

version 0.5, October 24, 2013

Abstract

A quadratic-exponential Diophantine equation in 4 variables, describing certain strongly regular graphs, is completely solved. Along the way we encounter different types of generalized Ramanujan-Nagell equations whose complete solution can be found in the literature, and we come across a problem on the order of the prime ideal above 2 in the class group of an imaginary quadratic number field, which is related to the size of the squarefree part of $2^n - 1$ and to Wieferich primes, and the solution of which can be based on the abc-conjecture.

1 Introduction

The question to determine the strongly regular graphs with parameters $(v,k,\lambda,\mu)$ with $v = 2^n$ and $\lambda = \mu$, was recently posed by Natalia Tokareva. Somewhat later Tokareva noted that the problem had already been solved by Bernasconi, Codenotti and Vanderkam [BCV], but nevertheless we found it, from a Diophantine point of view, of some interest to study a ramification of this problem.

We note the following facts about strongly regular graphs, see [vLW]. They satisfy $(v-k-1)\mu = k(k-\lambda-1)$. With $v = 2^n$ and $\lambda = \mu$ this becomes $2^n = 1 + k(k-1)/\mu$. In this case their eigenvalues are $k$ and $\pm t$ with $t^2 = k - \mu$, with $t$ an integer. From these data Bernasconi and Codenotti [BC] derived the diophantine equation $k^2 - 2^n k + t^2(2^n - 1) = 0$, which was subsequently solved in [BCV]. The only solutions turned out to be $(k,t) = (0,0), (1,1), (2^n - 1,1), (2^n,0)$ for all $n$, and additionally $(k,t) = (2^{n-1} - 2^{\frac{1}{2}n-1}, 2^{\frac{1}{2}n-1}), (2^{n-1} + 2^{\frac{1}{2}n-1}, 2^{\frac{1}{2}n-1})$ for even $n$. As a result, the only nontrivial strongly regular graphs of the desired type $(2^n, k, \mu, \mu)$ are those with even $n$ and $(k,\mu) = (2^{n-1} \pm 2^{\frac{1}{2}n-1}, 2^{n-2} \pm 2^{\frac{1}{2}n-1})$. These are precisely the graphs associated to so-called bent functions, see [BC].

In studying this diophantine problem we take a somewhat deviating path. Without loss of generality we may assume that there are three distinct eigenvalues, i.e. $t \geq 1$ and $k > 1$. The

---

1 See [vLW] for the definition of strongly regular graphs with these parameters.
2 Personal communication to Andries Brouwer, March 2013.
3 Personal communication to BdW, April 2013.
4 I owe this idea to Andries Brouwer.
multiplicity of $t$ then is $(2^n - 1 - k/t)/2$, so $t | k$. It follows that also $t | \mu$. We write $k = at$ and $\mu = bt$. Then we find $t = a - b$ and $2^n = (a^2 - 1)t/b$. Let $g = \gcd(a, b) = \gcd(b, t)$, and write $a = cg, b = dg$. It then follows that $2^n$ is the product of the integers $(a^2 - 1)/d$ and $t/g$, which therefore both are powers of 2. Let $(a^2 - 1)/d = 2^m$. Then we have $m \leq n$.

Since $2^n - 1 = a(2^n - 1)/b = a(2^m - ab - 1)/b$, the question now has become to determine the solutions in positive integers $n, m, c, g$ of the diophantine equation

$$2^n - 1 = c \left(2^m - cg^2\right).$$

(1)

For the application at hand only $n \geq m$ is relevant, but we will study $n < m$ as well. With $n \geq m$ there obviously are the four families of Table 1. Our first, completely elementary, result is that there are no others.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$m$</th>
<th>$c$</th>
<th>$g$</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>any</td>
<td>$n$</td>
<td>1</td>
</tr>
<tr>
<td>II</td>
<td>$n$</td>
<td>$2^n - 1$</td>
<td>1</td>
</tr>
<tr>
<td>III</td>
<td>even $\frac{1}{2}n + 1$</td>
<td>$2^\frac{1}{2}n - 1$</td>
<td>1</td>
</tr>
<tr>
<td>IV</td>
<td>even $\frac{1}{2}n + 1$</td>
<td>$2^\frac{1}{2}n + 1$</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 1: Four families of solutions of (1) with $n \geq m$.

**Theorem 1** All the solutions of (1) with $n \geq m$ are given in Table 1.

**Proof.** Note that $c$ and $g$ are odd, and that $cg^2 < 2^m$.

For $m \leq 2$ the only possibilities for $cg^2 < 2^m$ are $c = g = 1$, leading to $m = n$, fitting in [I], and for $m = 2$ also $c = 3, g = 1$, leading to $n = 2$, fitting in [II].

For $m \geq 3$ we look at [I] modulo $2^m$. Using $n \geq m$ we get $(cg)^2 \equiv 1 \pmod{2^m}$, and by $m \geq 3$ this implies $cg \equiv \pm 1 \pmod{2^{m-1}}$. So either $c = g = 1$, immediately leading to $m = n$ and thus to [I], or $cg \geq 2^{m-1} - 1$. Since also $cg^2 \leq 2^m - 1$ we get $g \leq \frac{2^m - 1}{2^{m-1} - 1} < 3$, hence $g = 1$.

We now have $c \equiv \pm 1 \pmod{2^{m-1}}$ and $1 < c < 2^m$, implying $c = 2^{m-1} - 1$ or $c = 2^{m-1} + 1$ or $c = 2^m - 1$, leading to exactly [III], [IV], [II] respectively.

Note that this result implies the result of [BCV].

When $m > n$, a fifth family and seven isolated solutions are easily found, see Table 2. For $n = 3$ and $c = 1$ equation [I] is precisely the well known Ramanujan-Nagell equation [N].

We will prove the following result, which is not elementary anymore.

**Theorem 2** All the solutions of (1) with $m > n$ are given in Table 3.

Our proof works for both cases $n \geq m$ and $m > n$ at once.
2 Small \( n \)

The cases \( n \leq 2 \) are elementary.

**Proof of Theorems 1 and 2 when \( n \leq 2 \).** Clearly \( n = 1 \) leads to \( c = 1 \) and \( 2^m - g^2 = 1 \), which for \( m \geq 2 \) is impossible modulo 4. So there is only the trivial solution \( m = g = 1 \). And for \( n = 2 \) we find \( 3 = c (2^m - cg^2) \), so \( c = 1 \) or \( c = 3 \). With \( c = 1 \) we have \( 2^m - g^2 = 3 \), which for \( m \geq 3 \) is impossible modulo 8. So we are left with the trivial \( m = 2, g = 1 \) only. And with \( c = 3 \) we have \( 2^m - 3g^2 = 1 \), which also for \( m \geq 3 \) is impossible modulo 8. So we are left with the trivial \( m = 2, g = 1 \) only. \( \square \)

3 Recurrence sequences

From now on we assume \( n \geq 3 \). Let us write \( D = 2^n - 1 \).

**Lemma 3** If \((n, m, c, g)\) is a solution of (1) then there exists an integer \( h \) such that

\[
\begin{align*}
    h^2 + Dg^2 &= 2^\ell \\
    c &= \frac{2^{m-1} \pm h}{g^2}.
\end{align*}
\]

**Proof.** We view equation (1) as a quadratic equation in \( c \). Its discriminant is \( 2^{2m} - 4Dg^2 \), which must be an even square, say \( 4h^2 \). This immediately gives the result. \( \square \)

So \( \ell \) is even, but when studying (2) we will also allow odd \( \ell \) for the moment. Note the ‘basic’ solution \((h, g, \ell) = (1, 1, n)\) of (2). In the quadratic field \( \mathbb{K} = \mathbb{Q}(\sqrt{-D}) \) we therefore look at

\[
\alpha = \frac{1}{2} \left( 1 + \sqrt{-D} \right),
\]

which is an integer of norm \( 2^{n-2} \). Note that \( D \) is not necessarily squarefree (e.g. \( n = 6 \) has \( D = 63 = 3^2 \cdot 7 \)), so the order \( \mathcal{O} \) generated by the basis \( \{1, \alpha\} \), being a subring of the ring

\[
\begin{array}{|c|c|c|c|}
\hline
n & m & c & g \\
\hline
[V] & \text{any} & 2n - 2 & 1 & 2^{n-1} - 1 \\
\hline
[VI] & 3 & 5 & 1 & 5 \\
& 6 & 7 & 3 \\
& 7 & 1 & 11 \\
& 15 & 1 & 181 \\
\hline
[VII] & 4 & 5 & 3 & 3 \\
& 7 & 5 & 5 \\
& 9 & 3 & 13 \\
\hline
\end{array}
\]

Table 2: One family and seven isolated solutions of (1) with \( m > n \).
of integers (the maximal order of $\mathbb{K}$), may be a proper subring. The discriminant of $\mathbb{K}$ is the squarefree part of $-D$, which, just like $-D$ itself, is $\equiv 1 \pmod{8}$. So in the ring of integers the prime 2 splits, say $2 = \wp \bar{\wp}$, and w.l.o.g. we can say $(\alpha) = \wp^{n-2}$. Note that it may happen that a smaller power of $\wp$ already is principal. Indeed, for $n = 6$ we have $\wp = \left(\frac{1}{2} \left(1 - \sqrt{-7}\right)\right)$ itself already being principal, where $(\alpha) = \left(\frac{1}{2} \left(1 + \sqrt{-63}\right)\right) = \wp^4$. But note that $\wp, \wp^2, \wp^3$ are not in the order $O$, and it is this order which interests us. We have the following result.

**Lemma 4** The smallest positive $s$ such that $\wp^s$ is a principal ideal in $O$ is $s = n - 2$.

In a later section we further comment on the order of $\wp$ in the full class group for general $n$. In particular we gather some evidence for the following conjecture, showing a.o. that it follows from (an effective version of) the abc-conjecture (at least for large enough $n$).

**Conjecture 5** For $n \neq 6$ the smallest positive $s$ such that $\wp^s$ is a principal ideal in the maximal order of $\mathbb{K}$ is $s = n - 2$.

**Proof of Lemma 4**. There exists a minimal $s > 0$ such that $\wp^s$ is principal and is in the order $O$. Let $\frac{1}{2} (a + b\sqrt{-D})$ be a generator of $\wp^s$, then $a, b$ are coprime and both odd, and

$$a^2 + Db^2 = 2^{s+2}. \quad (4)$$

Since $\wp^{n-2} = (\alpha)$ is principal and in $O$, we now find that $s | n - 2$, and

$$\left(a + b\sqrt{-D}\right)^k = \pm 2^{k-1} \left(1 + \sqrt{-D}\right), \text{ with } k = \frac{n-2}{s}. \quad (5)$$

Comparing imaginary parts in (5) gives that $b | 2^{k-1}$, and from the fact that $b$ is odd it follows that $b = \pm 1$. Equation (4) then becomes $a^2 + D = 2^{s+2}$, which is $a^2 = 2^{s+2} - 2^n + 1$. This equation, which is a generalization of the Ramanujan-Nagell equation that occurs for $n = 3$, has, according to Szalay [S], only the solutions given in Table 3. Only in case [ii] we have $k = \frac{n-2}{s}$ integral, and this proves $k = 1, s = n - 2$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$s$</th>
<th>$a$</th>
</tr>
</thead>
<tbody>
<tr>
<td>[i]</td>
<td>any $\geq 2$</td>
<td>$2^{n-4}$</td>
</tr>
<tr>
<td>[ii]</td>
<td>$2n - 4$</td>
<td>$n - 2$</td>
</tr>
<tr>
<td>[iii]</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>181</td>
</tr>
</tbody>
</table>

Table 3: The solutions of $a^2 = 2^{s+2} - 2^n + 1$ with $a > 0$.

We next show that the solutions $h, g$ of (2) are elements of certain binary recurrence sequences. We define for $k \geq 0$

$$h_k = \alpha^k + \overline{\alpha}^k, \text{ with } h_0 = 2, h_1 = 1, \text{ and } h_{k+1} = h_k - 2^{n-2}h_{k-1} \text{ for } k \geq 1,$$

$$g_k = \frac{1}{\sqrt{-D}} \left(\alpha^k - \overline{\alpha}^k\right), \text{ with } g_0 = 0, g_1 = 1, \text{ and } g_{k+1} = g_k - 2^{n-2}g_{k-1} \text{ for } k \geq 1.$$
For even $n$, say $n = 2r$, we can factor $D$ as $(2^r - 1)(2^r + 1)$. Now we define

$$\lambda = \frac{1}{2} \left( 2^r + 1 + \sqrt{-D} \right), \quad \mu = \frac{1}{2} \left( 2^r - 1 + \sqrt{-D} \right),$$

satisfying $N\lambda = 2^{2r-1} + 2^{r-1}$ and $N\mu = 2^{2r-1} - 2^{r-1}$, $\lambda\mu = -\alpha\sqrt{-D}$, $\lambda\mu = 2^{r-1}\sqrt{-D}$, $\lambda^2 = (2^r + 1)\alpha$, and $\mu^2 = -(2^r - 1)\alpha$. Next, for $n = 2r$ and $\kappa \geq 0$ we define

$$u_\kappa = \frac{1}{2^r + 1} \left( \lambda\alpha^\kappa + \lambda\alpha^{\kappa+1} \right), \quad v_\kappa = \frac{-1}{2^{r-1}(2^r - 1)} \left( \mu\alpha^\kappa + \mu\alpha^{\kappa+1} \right),$$

with $u_0 = 1, u_1 = -(2^{r-1} - 1)$, and $u_{\kappa+1} = u_\kappa - 2^{n-2}u_{\kappa-1}$ for $\kappa \geq 1$, and $v_0 = 1, v_1 = 2^{r-1} + 1$, and $v_{\kappa+1} = v_\kappa - 2^{n-2}v_{\kappa-1}$ for $\kappa \geq 1$.

We present a few useful properties of these recurrence sequences.

**Lemma 6**

(a) For any $n \geq 3$ we have for all $\kappa \geq 0$

$$g_{2\kappa} = g_\kappa h_\kappa.$$

(b) For even $n = 2r$ we have for all $\kappa \geq 0$

$$g_{2\kappa+1} = u_\kappa v_\kappa.$$

(c) For any $n$ and even $k = 2\kappa$, we have

$$2^{(n-2)\kappa+1} + h_{2\kappa} = h_\kappa^2, \quad 2^{(n-2)\kappa+1} - h_{2\kappa} = (2^n - 1)g_\kappa^2.$$

(d) For any even $n = 2r$ and odd $k = 2\kappa + 1$, we have

$$2^{(r-1)(2\kappa+1)+1} + h_{2\kappa+1} = (2^r + 1)u_\kappa^2, \quad 2^{(r-1)(2\kappa+1)+1} - h_{2\kappa+1} = (2^r - 1)v_\kappa^2.$$

**Proof.** Trivial by writing out all equations and using the mentioned properties of $\lambda, \mu$. □

For curiosity only, note that $(2^r + 1)u_\kappa^2 + (2^r - 1)v_\kappa^2 = 2^{(r-1)(2\kappa+1)+2}$.

Now that we have introduced the necessary binary recurrence sequences, we can state the relation to the solutions of (2).

**Lemma 7** Let $(h, g, \ell)$ be a solution of (2).

(a) There exists a $k \geq 0$ such that $h = \pm h_k$, $g = \pm g_k$ and $(n-2)k = \ell - 2$.

(b) If $\ell$ is even and equation (3) holds with $m = \frac{1}{2}(n-2)k + 2$ and integral $c$, then one of the four cases [A], [B], [C], [D] as shown in Table 4 applies, according to $k$ being even or odd, and the $\pm$ in (3) being $+$ or $-$.

5
Table 4: The four cases.

<table>
<thead>
<tr>
<th>n</th>
<th>k</th>
<th>±</th>
<th>condition</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>[A]</td>
<td>any</td>
<td>2κ</td>
<td>+</td>
<td>g_κ = ±1</td>
</tr>
<tr>
<td>[B]</td>
<td></td>
<td>2κ + 1</td>
<td>-</td>
<td>h_κ</td>
</tr>
</tbody>
</table>

Proof.

(a) Equation (2) implies that g, h are coprime, and then it implies that \((\frac{1}{2} (h \pm g\sqrt{-D})) = \sqrt{\ell - 2}\). Lemma 4 then implies that \(n - 2 \mid \ell - 2\). We take \(k = \frac{\ell - 2}{n - 2}\) and thus have \(\frac{1}{2} (h \pm g\sqrt{-D}) = \pm \alpha k\), and the result follows.

(b) Note that \(\ell\) being even implies that at least one of \(n, k\) is even.

For even \(k = 2\kappa\), (a) and Lemma 6(a) say that \(g = \pm g_k = \pm u_\kappa v_\kappa\).

If \(\pm = +\) then equation (3) and Lemma 6(a,c) say that \(c = 2^{(n-2)\kappa+1} h_\kappa = \frac{2n-1}{h_\kappa^2}\). Then \(c\) being integral implies \(g_\kappa = \pm 1\) and \(c = 1\).

If \(\pm = -\) then equation (3) and Lemma 6(a,c) say that \(c = 2^{(n-2)\kappa+1} h_\kappa = \frac{2n-1}{h_\kappa^2}\). Then \(c\) being integral implies \(h_\kappa \mid 2^n - 1\).

For even \(n = 2r\) and odd \(k = 2\kappa + 1\), (a) and Lemma 6(b) say that \(g = \pm g_k = \pm u_\kappa v_\kappa\).

If \(\pm = +\) then equation (3) and Lemma 6(b,d) say that \(c = 2^{(r-1)(2\kappa+1)+1} h_{2\kappa+1} = \frac{2^r + 1}{v_\kappa^2}\). Then \(c\) being integral implies \(v_\kappa^2 \mid 2^r + 1\).

If \(\pm = -\) then equation (3) and Lemma 6(b,d) say that \(c = 2^{(r-1)(2\kappa+1)+1} h_{2\kappa+1} = \frac{2^r - 1}{u_\kappa^2}\). Then \(c\) being integral implies \(u_\kappa^2 \mid 2^r - 1\).

Let’s trace the known solutions.

Families [I] and [II] have \(k = 2\), so \(\kappa = 1\), and \(c = 1\) or \(c = 2^n - 1\), so they are in cases [A] and [B] with \(h_1 = 1\) and \(g_1 = 1\), respectively.

Families [III] and [IV] have \(k = 1\), so \(\kappa = 0\), and \(c = 2^r - 1\) or \(c = 2^r + 1\), so they are in cases [D] and [C] with \(u_0 = 1\) and \(v_0 = 1\), respectively.

Family [V] has \(k = 4\), so \(\kappa = 2\), and \(c = \frac{2(n-2)\kappa+1 + h_4}{g_4^2} = \frac{h_4^2}{g_4^2 h_4^2} = \frac{1}{g_4^2} = 1\), so it is in case [A].

The known solutions with \(n = 3\) and even \(k = 2\kappa\) are presented Table 5, and the known solutions with \(n = 4\) and even \(k = 2\kappa\) resp. odd \(k = 2\kappa + 1\) are presented in Table 6.
Lemma 10 Cases [C] and [D] lead to only the solutions from families [III] and [IV], and the isolated solutions [VII].
Proof. It is easy to see that \( u_\kappa \equiv 1 - 2^{r-1} \pmod{2^{2^{r-2}}} \), \( v_\kappa \equiv 1 + 2^{r-1} \pmod{2^{2^{r-2}}} \) for all \( \kappa \geq 1 \). If \( r \geq 3 \) then it follows that \( |v_\kappa| \geq 2^{r-1} + 1 \) and \( |u_\kappa| \geq 2^{r-1} - 1 \), so the condition in Table 4 shows that in case \([C]\) \((2^{r-1} + 1)^2 \leq 2^r + 1\) and in case \([D]\) \((2^{r-1} - 1)^2 \leq 2^r - 1\), which both are impossible. Thus \( r = 2 \) or \( \kappa = 0 \).

The case \( \kappa = 0 \) gives \( k = 1 \), so \( m = \frac{1}{2}n + 1 \), and this gives exactly families \([III]\) and \([IV]\). So we are left with \( r = 2 \) and \( \kappa \geq 1 \), so \( n = 4 \).

In case \([C]\) the condition in Table 4 shows that \( v_2^2 \leq 5 \), but also always \( v_\kappa \equiv 3 \pmod{4} \), leaving only room for \( v_\kappa = -1, c = 5 \). This leaves us with solving \( 3 = 2^m - 5g^2 \). This equation is a special case of the generalized Ramanujan-Nagell equation treated in [dW, Chapter 7], from which it can easily be deduced that the only solutions are \((m, g) = (3, 1), (7, 5)\). It might occur elsewhere in the literature as well.

In case \([D]\) the condition in Table 4 shows that \( u_2^2 \leq 3 \), but also always \( u_\kappa \equiv 3 \pmod{4} \), leaving only room for \( u_\kappa = -1, c = 3 \). This leaves us with solving \( 5 = 2^m - 3g^2 \). Again this equation is a special case of the generalized Ramanujan-Nagell equation treated in [dW, Chapter 7], and it can easily be deduced that the only solutions are \((m, g) = (3, 1), (5, 3), (9, 13)\). It might also occur elsewhere in the literature as well. \( \square \)

Proof of Theorems 1 and 2 when \( n \geq 3 \). This is done in Lemmas 3, 7, 8, 9 and 10. \( \square \)

5 The order of the prime ideal above 2 in the ideal class group of \( \mathbb{Q}(\sqrt{-D}) \), and Wieferich primes

We cannot fully prove Conjecture 5, but we will indicate why we think it’s true. We will deduce it from the \( abc\)-conjecture, and we have a partial result.

Recall that a Wieferich prime is a prime \( p \) for which \( 2^{p-1} \equiv 1 \pmod{p^2} \). For any odd prime \( p \) we introduce \( w_{p,k} \) as the order of 2 in the multiplicative group \( \mathbb{Z}_{p^k}^* \), and \( \ell_p \) as the number of factors \( p \) in \( 2^{p-1} - 1 \). Fermat’s theorem shows that \( \ell_p \geq 1 \), and Wieferich primes are those with \( \ell_p \geq 2 \).

**Theorem 11** Let \( n \geq 3 \), \( 2^n - 1 = D = e^2D' \) with \( D' \) squarefree and \( e \geq 1 \). Let \( \wp \) be a prime ideal above 2 in \( \mathbb{K} = \mathbb{Q}(\sqrt{-D}) \).

(a) If \( e < 2^{n/4-3/5} \) then the smallest positive \( s \) such that \( \wp^s \) is a principal ideal in the maximal order of \( \mathbb{K} \) is \( s = n - 2 \).

(b) The condition \( e < 2^{n/4-3/5} \) holds at least in the following cases:

(1) \( n \neq 6 \) and \( n \leq 200 \),

(2) \( n \) is not a multiple of \( w_{p,k} \) for some Wieferich prime \( p \).

In particular Conjecture 5 is true for all \( n \neq 6 \) with \( 3 \leq n \leq 200 \).
Proof of Theorem 11.

(a) We start as in the proof of Lemma 4. There exists a minimal \( s > 0 \) such that \( \varphi^s \) is principal in the ring of integers of \( \mathbb{K} = \mathbb{Q}(\sqrt{-D'}) \). Let \( \frac{1}{2} (a + b\sqrt{-D'}) \) be a generator of this principal ideal, then \( a, b \) are both odd and coprime, and \( a^2 + D' b^2 = 2^{k+2} \). Since \( \varphi^{n-2} = (\alpha) \) (with \( \alpha = \frac{1}{2} (1 + \sqrt{-D'}) \)) is principal with norm \( 2^{n-2} \), we now find that \( s \mid n - 2 \). Let us write \( k = \frac{n - 2}{s} \).

The condition \( e < 2^{n/4 - 3/5} \) implies \( D' > \frac{2^n - 1}{2^{n/2 - 6/5}} \). As \( ks = n - 2 \) and we don’t know much about \( s \) we estimate \( k \leq n - 2 \). We may however assume \( k \geq 2 \), as \( k = 1 \) is what we want to prove. This means that we get \( s \leq \frac{1}{2} n - 1 \), and from \( a^2 + D' b^2 = 2^{k+2} \) we get \( 1 \leq |b| \leq \frac{2^{k+1/2}}{\sqrt{D'}} < 2^{n/2 - 1/10} \). And this contradicts \( n \geq 3 \).

(b) We would like to get more information on how big \( e \) can become. To get an idea of what happens we computed \( e \) for all \( n \leq 200 \). Table 7 shows the cases with \( e > 1 \). Note that in all these cases \( e \mid n \), and that in all of these cases except \( n = 6 \) we have \( e < 2^{n/4 - 3/5} \), with for larger \( n \) an ample margin. This proves that condition (1) is sufficient.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( e )</th>
<th>( n )</th>
<th>( e )</th>
<th>( n )</th>
<th>( e )</th>
<th>( n )</th>
<th>( e )</th>
<th>( n )</th>
<th>( e )</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>3</td>
<td>30</td>
<td>3</td>
<td>60</td>
<td>15</td>
<td>84</td>
<td>21</td>
<td>108</td>
<td>17</td>
</tr>
<tr>
<td>12</td>
<td>3</td>
<td>36</td>
<td>3</td>
<td>63</td>
<td>7</td>
<td>90</td>
<td>3</td>
<td>110</td>
<td>11</td>
</tr>
<tr>
<td>18</td>
<td>3</td>
<td>40</td>
<td>5</td>
<td>66</td>
<td>3</td>
<td>96</td>
<td>3</td>
<td>114</td>
<td>3</td>
</tr>
<tr>
<td>20</td>
<td>5</td>
<td>42</td>
<td>21</td>
<td>72</td>
<td>3</td>
<td>100</td>
<td>5</td>
<td>120</td>
<td>15</td>
</tr>
<tr>
<td>21</td>
<td>7</td>
<td>48</td>
<td>3</td>
<td>78</td>
<td>3</td>
<td>102</td>
<td>3</td>
<td>126</td>
<td>21</td>
</tr>
<tr>
<td>24</td>
<td>3</td>
<td>54</td>
<td>9</td>
<td>80</td>
<td>5</td>
<td>105</td>
<td>7</td>
<td>132</td>
<td>3</td>
</tr>
<tr>
<td>30</td>
<td>3</td>
<td>60</td>
<td>15</td>
<td>84</td>
<td>21</td>
<td>108</td>
<td>17</td>
<td>136</td>
<td>17</td>
</tr>
<tr>
<td>36</td>
<td>3</td>
<td>63</td>
<td>7</td>
<td>90</td>
<td>3</td>
<td>110</td>
<td>11</td>
<td>138</td>
<td>3</td>
</tr>
<tr>
<td>40</td>
<td>5</td>
<td>66</td>
<td>3</td>
<td>96</td>
<td>3</td>
<td>114</td>
<td>3</td>
<td>140</td>
<td>5</td>
</tr>
<tr>
<td>42</td>
<td>21</td>
<td>72</td>
<td>3</td>
<td>100</td>
<td>5</td>
<td>120</td>
<td>15</td>
<td>144</td>
<td>3</td>
</tr>
<tr>
<td>48</td>
<td>3</td>
<td>78</td>
<td>3</td>
<td>102</td>
<td>3</td>
<td>126</td>
<td>21</td>
<td>147</td>
<td>7</td>
</tr>
<tr>
<td>54</td>
<td>9</td>
<td>80</td>
<td>5</td>
<td>105</td>
<td>7</td>
<td>132</td>
<td>3</td>
<td>150</td>
<td>3</td>
</tr>
</tbody>
</table>

Table 7: The values of \( e > 1 \) for all \( n \leq 200 \).

Next let condition (2) hold, i.e. \( n \) is not a multiple of \( w_{p,2} \) for some Wieferich prime \( p \). We will prove that in this case \( e \mid n \), as was already observed in Table 7. This then is sufficient, as \( e \mid n \) implies \( e \leq n \), and \( n < 2^{n/4 - 3/5} \) is true for \( n \geq 20 \), and for \( 3 \leq n \leq 19 \) with the exception of \( n = 6 \) we already saw that \( e < 2^{n/4 - 3/5} \).

The following result is easy to prove: if \( p \) is an odd prime and \( a \equiv 1 \pmod{p^t} \) for some \( t \geq 1 \) but \( a \not\equiv 1 \pmod{p^{t+1}} \), then \( a^2 \equiv 1 \pmod{p^{t+1}} \) but \( a^p \not\equiv 1 \pmod{p^{t+2}} \). By the obvious \( w_{p,\ell_p} \mid p - 1 \) it now follows that \( p \nmid w_{p,\ell_p} \), and the above result used with induction now gives \( w_{p,k} = w_{p,\ell_p} p^{k-\ell_p} \) for \( k \geq \ell_p \).

Now assume that \( p \) is a prime factor of \( e \), and \( p^k \mid e \) but \( p^{k+1} \nmid e \). Then \( 2^n \equiv 1 \pmod{p^{2k}} \), \( 2^{p-1} \not\equiv 1 \pmod{p^{n+1}} \), and \( w_{p,2k} = w_{p,\ell_p} p^{2k-\ell_p} \) has \( w_{p,2k} \mid n \). Hence \( p^{2k-\ell_p} \mid n \). When \( k \geq \ell_p \) for all \( p \) we find that \( e \mid n \). But condition (2) implies that \( \ell_p = 1 \) for all \( p \mid e \), and we’re done. \( \square \)

Extending Table 7 soon becomes computationally challenging, as \( 2^n - 1 \) has to be factored. However, we can easily compute a divisor of \( e \), and thus a lower bound, for many more values of \( n \), by simply trying only small prime factors. We computed for all primes up to \( 10^9 \) to which power they appear in \( 2^n - 1 \) for all \( n \) up to 12000. We conjecture that the resulting lower bounds for \( e \) are the actual values. In most cases we found them to be divisors of \( n \) indeed. But interestingly we found a few exceptions.
The only cases for $n$ where we are not yet sure that the conditions of Theorem 11(b) are fulfilled are related to Wieferich primes. Only two such primes are known: 1093 and 3511, with $w_{1093,2} = 364$, $w_{3511,2} = 1755$. So the multiples of 364 and 1755 are interesting cases for $n$. Indeed, we found that the value for $e$ in those cases definitely does not divide $n$. See Table 8 for those values for $n \leq 12000$.

Most probably 364 is the smallest $n$ for which the conditions of Theorem 11(b) do not hold, but we are not entirely sure, as there might exist a Wieferich prime $p$ with exceptionally small $w_{p,2}$.

If $n$ is divisible by $w_{p,2}$ for a Wieferich prime $p$, then the above proof actually shows that when $n$ is multiplied by at most $p^{\ell_p - 1}$ (for each such $p$) it will become a multiple of $e$. It seems quite safe to conjecture the following.

**Conjecture 12** For all $n \geq 7$ we have $e < 2^{n/4 - 3/5}$.

Most probably a much sharper bound is true, probably a polynomial bound, maybe even $e < n^2$.

According to the Wieferich prime search\(^5\), there are no other Wieferich primes up to $10^{17}$. A heuristic estimate for the number of Wieferich primes up to $x$ is $\log \log x$, see [CDP]. This heuristic is based on the simple expectation estimate $\sum_{p \leq x} p^{-1}$ for the number of $p$ such that the second $p$-ary digit from the right in $2^{p-1} - 1$ is zero. A similar argument for higher powers of $p$ indicates that the number of primes $p$ such that $2^{p-1} \equiv 1 \pmod{p^3}$ (i.e. $\ell_p \geq 3$) is finite, probably at most 1, because $\sum_{p} p^{-2} \approx 0.4522$. This gives some indication that $e$ probably always divides $n$ times a not too large factor. However, $w_{p,\ell_p}$ might be much smaller than $p$, and thus a multiplication factor of $p$ might already be large compared to $n$. We do not know how to find a better lower bound for $w_{p,2}$ than the trivial $w_{p,2} > 2 \log_2 p$.

---

\(^5\)See [http://www.primegrid.com](http://www.primegrid.com)
6 Connection to the abc-conjecture

Miller\footnote{Message of April 8, 2013 to the NMBRTHRY mailing list.} gives an argument that an upper bound for $e$ in terms of $n$ follows from the abc-conjecture. The abc-conjecture states that if $a + b = c$ for coprime positive integers, and $N$ is the product of the prime numbers dividing $a$, $b$ or $c$, then for every $\epsilon > 0$ there are only finitely many exceptions to $c < N^{1+\epsilon}$. Indeed, assuming $e \geq 2^{n/4-3/5}$ for infinitely many $n$ contradicts the abc-conjecture, namely $2^n = 1 + e^2 D'$ has $c = 2^n$ and $N \leq 2eD' = 2(2^n - 1)/e < 2^{3n/4+8/5}$, so that $\frac{\log c}{\log N} < \frac{4/3}{1 + 32/(15n)}$, which contradicts the conjecture. Indeed, assuming that the abc-conjecture is true, there is for every $\epsilon > 0$ a constant $K = K(\epsilon)$ such that $c < KN^{1+\epsilon}$, and we get $e < K^{1/(1+\epsilon)}2^{1+2\epsilon/(1+\epsilon)}$. This shows that any $\epsilon < 1/3$ will for sufficiently large $n$ give the truth of Conjecture 5 via Theorem 11(a).

Stewart and Tenenbaum\footnote{Unpublished, for a reference to this result see \url{http://www.math.leidenuniv.nl/~desmit/abc/}} formulate a strong form of the abc-conjecture, implying that $\log c < \log N + C \sqrt{\frac{\log N}{\log \log N}}$ for a constant $C$ (probably essentially $4\sqrt{3}$). Using $c = 2^n$ and $N \leq 2^n e^2$ we then obtain $n \log 2 < (n + 1) \log 2 - \log e + C \sqrt{\frac{(n + 1) \log 2}{\log(n + 1) + \log \log 2}}$, hence $e < \exp \left( C' \sqrt{\frac{n}{\log n}} \right)$ for a constant $C'$ slightly larger than $C$, probably $C' < 7.5$. Not exactly polynomial, but this is a general form of the abc-conjecture, not using the special form of our abc-example.

Even though Conjecture 5 follows from an effective version of the abc-conjecture, it might be possible to prove it in some other way.

Acknowledgements

The author is grateful to Aart Blokhuis, Andries Brouwer, Victor Miller and Natalia Tokareva for fruitful discussions.

References

\begin{itemize}
\end{itemize}


[S] László Szalay, “The equations \(2^N \pm 2^M \pm 2^L = z^2\)”, *Indagationes Mathematicae* **13** [2002], 131-142.