A GENERALIZED RAMANUJAN-NAGELL EQUATION RELATED TO CERTAIN STRONGLY REGULAR GRAPHS

Benne de Weger
Faculty of Mathematics and Computer Science, Eindhoven University of Technology, Eindhoven, The Netherlands
b.m.m.d.weger@tue.nl

Received: 10/24/13, Accepted: 4/29/14, Published: 8/5/14

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 groups of certain imaginary quadratic number fields, 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[1] (v, k, λ, μ) with $v = 2^n$ and $\lambda = \mu$, was recently posed by Natalia Tokareva[2]. Somewhat later Tokareva noted[3] that the problem had already been solved by Bernasconi, Codenotti and Vanderkam [2], 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 [5]. 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 [1] derived the diophantine equation $k^2 - 2^n k + t^2(2^n - 1) = 0$, which was subsequently solved in [2]. 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

[1]See [5] 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.

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 [1].

In studying this diophantine problem we take a somewhat deviating path[4]. Without loss of generality we may assume that there are three distinct eigenvalues, i.e., $t \geq 1$ and $k > 1$. The multiplicity of t then is $(2^n - 1 - k/t)/2$, so $t \mid k$. It follows that also $t \mid \mu$. 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 are both powers of 2. Let $(a^2 - 1)/d = 2^m$. Then we have $m \leq n$.

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

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

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.

	n	m	c	g
[I]	any	n	1	1
[II]		n	$2^n - 1$	1
[III]	even	$\frac{1}{2}n + 1$	$2^{\frac{1}{2}n} - 1$	1
[IV]		$\frac{1}{2}n + 1$	$2^{\frac{1}{2}n} + 1$	1

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 (1) 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 $g \leq \dfrac{2^m - 1}{2^{m-1} - 1} < 3$, 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 [2].

[4] I owe this idea to Andries Brouwer.

When $m > n$, a fifth family and seven isolated solutions are easily found, see Table 2. For $n = 3$ and $c = 1$ equation (1) is precisely the well known Ramanujan-Nagell equation [6].

	n	m	c	g
[V]	any ≥ 3	$2n-2$	1	$2^{n-1}-1$
[VI]	3	5	1	5
		6	7	3
		7	1	11
		15	1	181
[VII]	4	5	3	3
		7	5	5
		9	3	13

Table 2: One family and seven isolated solutions of (1) with $m > n$.

In Sections 2, 3 and 4 we will prove the following result, which is not elementary anymore, and works for both cases $n \geq m$ and $m > n$ at once.

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

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 $3 = c\left(2^m - cg^2\right)$, 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. *For any solution* (n, m, c, g) *of* (1) *there exists an integer* h *such that*

$$h^2 + Dg^2 = 2^\ell \quad \text{with} \quad \ell = 2m-2, \tag{2}$$

$$c = \frac{2^{m-1} \pm h}{g^2}. \tag{3}$$

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 ℓ is even, but when studying (2) we will also allow odd ℓ for the moment. Note the 'basic' solution $(h, g, \ell) = (1, 1, n)$ of (2). In the quadratic field $\mathbb{K} = \mathbb{Q}\left(\sqrt{-D}\right)$ 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 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 congruent to $1 \pmod 8$. So in the ring of integers the prime 2 splits, say $(2) = \wp\overline{\wp}$, and without loss of generality 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 $\mathcal{O}$, and it is the order which interests us. We have the following result.

Lemma 4. *The smallest positive s such that $\wp^s$ is a principal ideal in $\mathcal{O}$ 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 (among other things) 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 $\mathcal{O}$. Let $\frac{1}{2}\left(a + b\sqrt{-D}\right)$ be a generator of $\wp^s$, then a, b are coprime and both odd, and

$$a^2 + Db^2 = 2^{s+2}. \tag{4}$$

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

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

Comparing imaginary parts in (5) gives that $b \mid 2^{k-1}$, 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 [8], only the solutions given in Table 3. Only in case [ii] we have $k = \dfrac{n-2}{s}$ integral, and this proves $k = 1$, $s = n - 2$. $\square$

	n	s	a
[i]	any ≥ 2	$2n-4$	$2^{n-1}-1$
[ii]		$n-2$	1
[iii]	3	3	5
		5	11
		13	181

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 $k \geq 0$

$$h_k = \alpha^k + \overline{\alpha}^k, \quad \text{with } h_0 = 2, h_1 = 1, \text{ and } h_{k+1} = h_k - 2^{n-2}h_{k-1} \text{ for } k \geq 1,$$
$$g_k = \frac{\alpha^k - \overline{\alpha}^k}{\sqrt{-D}}, \quad \text{with } g_0 = 0, g_1 = 1, \text{ and } g_{k+1} = g_k - 2^{n-2}g_{k-1} \text{ for } k \geq 1.$$

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

$$u_\kappa = \frac{1}{2^r+1}\left(\lambda\alpha^\kappa + \overline{\lambda}\overline{\alpha}^\kappa\right), \quad \text{with } u_0 = 1, u_1 = -(2^{r-1} - 1), \text{ and } u_{\kappa+1} = u_\kappa - 2^{n-2}u_{\kappa-1} \text{ for } \kappa \geq 1,$$
$$v_\kappa = \frac{-1}{2^{r-1}(2^r-1)}\left(\mu\alpha^{\kappa+1} + \overline{\mu}\overline{\alpha}^{\kappa+1}\right), \quad \text{with } v_0 = 1, v_1 = 2^{r-1} + 1, \text{ and } v_{\kappa+1} = v_\kappa - 2^{n-2}v_{\kappa-1} \text{ for } \kappa \geq 1.$$

We present a few useful properties of these recurrence sequences.

Lemma 6.

(a) *For any $n \geq 3$ we have $g_{2\kappa} = g_\kappa h_\kappa$ for all $\kappa \geq 0$.*

(b) *For even $n = 2r$ we have $g_{2\kappa+1} = u_\kappa v_\kappa$ for all $\kappa \geq 0$.*

(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 λ, μ. $\square$

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, ℓ) 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 ℓ 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 $-$.*

	n	k	$\pm$	condition	c
[A]	any	2κ	$+$	$g_\kappa = \pm 1$	1
[B]			$-$	$h_\kappa^2 \mid 2^n - 1$	$\dfrac{2^n-1}{h_\kappa^2}$
[C]	$2r$	$2\kappa+1$	$+$	$v_\kappa^2 \mid 2^r + 1$	$\dfrac{2^r+1}{v_\kappa^2}$
[D]			$-$	$u_\kappa^2 \mid 2^r - 1$	$\dfrac{2^r-1}{u_\kappa^2}$

Table 4: The four cases.

Proof.

(a) Equation (2) implies that g, h are coprime, so that $\left(\frac{1}{2}\left(h \pm g\sqrt{-D}\right)\right) = \wp^{\ell-2}$. Lemma 4 then implies that $n-2 \mid \ell-2$. We take $k = \dfrac{\ell-2}{n-2}$ and thus have $\frac{1}{2}\left(h \pm g\sqrt{-D}\right) = \alpha^k$ or $\overline{\alpha}^k$, and the result follows.

(b) Note that ℓ being even implies that at least one of n, k is even.
For even $k = 2\kappa$, (a) and Lemma 6(a) say that $g = \pm g_k = \pm g_\kappa h_\kappa$.
If $\pm = +$ then equation (3) and Lemma 6(a,c) say that $c = \dfrac{2^{(n-2)\kappa+1} + h_{2\kappa}}{g_{2\kappa}^2} = \dfrac{1}{g_\kappa^2}$. Then c being integral implies $g_\kappa = \pm 1$ and $c = 1$.
If $\pm = -$ then equation (3) and Lemma 6(a,c) say that $c = \dfrac{2^{(n-2)\kappa+1} - h_{2\kappa}}{g_{2\kappa}^2} = \dfrac{2^n-1}{h_\kappa^2}$. Then c being integral implies $h_\kappa^2 \mid 2^n - 1$.

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 $c = \dfrac{2^{(r-1)(2\kappa+1)+1} + h_{2\kappa+1}}{g_{2\kappa+1}^2} = \dfrac{2^r+1}{v_\kappa^2}$. Then c being integral implies $v_\kappa^2 \mid 2^r+1$.
If $\pm = -$ then equation (3) and Lemma 6(b,d) say that $c = \dfrac{2^{(r-1)(2\kappa+1)+1} - h_{2\kappa+1}}{g_{2\kappa+1}^2} = \dfrac{2^r-1}{u_\kappa^2}$. 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 $g_1 = 1$ and $h_1 = 1$, 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 $c = \dfrac{2^{(n-2)2+1} + h_4}{g_4^2} = \dfrac{h_2^2}{g_2^2 h_2^2} = \dfrac{1}{g_2^2} = 1$, 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.

	κ	0	1	2	3	4	5	6	7	...	11	12	13
	h_κ	2	1	−3	−5	1	11	9	−13	...	67	−47	−181
	g_κ	0	1	1	−1	−3	−1	5	7	...	23	45	−1
	m	2	3	4	5	6	7	8	9	...	13	14	15
[A]	c		1	1	1		1						1
[B]	c		7			7							

Table 5: Tracing the solutions with $n = 3$ and even $k = 2\kappa$ to elements in recurrence sequences.

4. Solving the Four Cases

All four cases [A], [B], [C] and [D] can be reduced to diophantine equations known from the literature.

Lemma 8. *Case* [A] *leads to only the solutions from families* [I] *and* [V], *and the three isolated solutions from* [VI] *with odd* m.

	κ	0	1	2	3
	h_κ	2	1	-7	-11
	g_κ	0	1	1	-3
	m	2	4	6	8
[A]	c		1	1	
[B]	c		15		

$k = 2\kappa$

	κ	0	1	2	3	4
	u_κ	1	-1	-5	-1	19
	v_κ	1	3	-1	-13	-9
	m	3	5	7	9	11
[C]	c	5		5		
[D]	c	3	3		3	

$k = 2\kappa + 1$

Table 6: Tracing the solutions with $n = 4$ and even $k = 2\kappa$, resp. odd $k = 2\kappa + 1$, to elements in recurrence sequences.

Proof. Table 4 gives $g_k = \pm 1$ and $c = 1$. Then Equation (1) becomes the generalized Ramanujan-Nagell equation $g^2 = 2^m - 2^n + 1$, which was completely solved by Szalay [8]. $\square$

Lemma 9. *Case* [B] *leads to only the solutions from family* [II]*, and the isolated solution from* [VI] *with m even.*

Proof. Note that we have $\kappa \geq 1$, and then $h_\kappa \equiv 1 \pmod{2^{n-2}}$, so we have either $h_\kappa = 1$ or $|h_\kappa| \geq 2^{n-2} - 1$. In the latter case the condition in Table 4 implies $(2^{n-2} - 1)^2 \leq h_\kappa^2 \leq 2^n - 1$, leading to $n \leq 4$. If $n = 3$ we must have $h_\kappa = \pm 1$. But h_κ is never congruent to $-1 \pmod 8$, so $h_\kappa = 1$. If $n = 4$ then we must have $|h_\kappa| = 1$. Note that (when $\kappa \geq 1$) we always have $h_\kappa \equiv 1 \pmod 4$. So we find that $h_\kappa = 1$ always, and it follows from Table 4 that $c = 2^n - 1$, and Equation (1) now becomes $g^2 = \dfrac{2^m - 1}{2^n - 1}$. Hence $n \mid m$. The equation $g^2 = \dfrac{x^t - 1}{x - 1}$ has been treated by Ljunggren [4], proving (among other results) that for even x always $t \leq 2$. Hence either $m = n$, $g = 1$ leading to family [II], or $m = 2n$, in which case $2^n + 1$ must be a square. This happens only for $n = 3$, leading to $m = 6$, thus to the only solution from [VI] with even m. $\square$

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 $u_\kappa \equiv 1 - 2^{r-1} \pmod{2^{2r-2}}$, $v_\kappa \equiv 1 + 2^{r-1} \pmod{2^{2r-2}}$ 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 $g = 1$, and $m = \frac{1}{2}n + 1$, 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 $v_\kappa^2 \leq 5$, but also we alway have $v_\kappa \equiv 3 \pmod 4$, 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 [9, Chapter 7], from which it can easily be deduced that the only solutions are $(m, g) = (3, 1), (7, 5)$ (solutions nrs. 72 and 223 in [9, Chapter 7, Table I]). It might occur elsewhere in the literature as well.

In case [D] the condition in Table 4 shows that $u_\kappa^2 \le 3$, 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 [9, Chapter 7], and it can easily be deduced that the only solutions are $(m, g) = (3, 1), (5, 3), (9, 13)$ (solutions nrs. 43, 123 and 257 in [9, Chapter 7, Table I]). It might also occur elsewhere in the literature as well. □

Proof of Theorems 1 and 2 when $n \ge 3$. This is done in Lemmas 3, 7, 8, 9 and 10. □

5. The Order of the Prime Ideal Above 2 in the Ideal Class Group of $\mathbb{Q}\left(\sqrt{-(2^n-1)}\right)$, and Wieferich Primes

We cannot fully prove Conjecture 5, but we will indicate why we think it is 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 ℓ_p as the number of factors p in $2^{p-1} - 1$. Fermat's theorem shows that $\ell_p \ge 1$, and Wieferich primes are those with $\ell_p \ge 2$.

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

(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) *$n \ne 6$ and $n \le 200$,*

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

In particular Conjecture 5 is true for all $n \ne 6$ with $3 \le n \le 200$.

Proof of Theorem 11.

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

The condition $e < 2^{n/4-3/5}$ implies $D' > \dfrac{2^n-1}{2^{n/2-6/5}}$. 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 $a^2 + D'b^2 = 2^{s+2}$ we get $1 \leq |b| \leq \dfrac{2^{n/4+1/2}}{\sqrt{D'}} < \dfrac{2^{n/2-1/10}}{\sqrt{2^n-1}}$. 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.

n	e	n	e	n	e	n	e	n	e	n	e	n	e
6	3	36	3	66	3	100	5	126	21	150	3	180	15
12	3	40	5	72	3	102	3	132	3	155	31	186	3
18	3	42	21	78	3	105	7	136	17	156	39	189	7
20	5	48	3	80	5	108	9	138	3	160	5	192	3
21	7	54	9	84	21	110	11	140	5	162	9	198	3
24	3	60	15	90	3	114	3	144	3	168	21	200	5
30	3	63	7	96	3	120	15	147	7	174	3		

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 $a^p \equiv 1 \pmod{p^{t+1}}$ 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 $2^n \equiv 1 \pmod{p^{2k}}$, $2^{p-1} \not\equiv 1 \pmod{p^{\ell_p+1}}$, 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 $p|e$, and we're done. □

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 10^5 to which power they appear in $2^n - 1$ for all n up to 12000.

$\frac{n}{364}$	$\frac{e}{1093}$	$\frac{1093n}{e}$
1	1	364
2	1	728
3	273	4
4	1	1456
5	5	364
6	273	8
7	1	2548
8	1	2912
9	273	12
10	5	728
11	1	4004

$\frac{n}{364}$	$\frac{e}{1093}$	$\frac{1093n}{e}$
12	273	16
13	1	4732
14	1	5096
15	1365	4
16	1	5824
17	1	6188
18	273	24
19	1	6916
20	5	1456
21	273	28
22	1	8008

$\frac{n}{364}$	$\frac{e}{1093}$	$\frac{1093n}{e}$
23	1	8372
24	273	32
25	5	1820
26	1	9464
27	819	12
28	1	10192
29	29	364
30	1365	8
31	1	11284
32	1	11648

$\frac{n}{1755}$	$\frac{e}{3511}$	$\frac{3511n}{e}$
1	1	1755
2	9	390

$\frac{n}{1755}$	$\frac{e}{3511}$	$\frac{3511n}{e}$
3	1	5265
4	585	12

$\frac{n}{1755}$	$\frac{e}{3511}$	$\frac{3511n}{e}$
5	1	8775
6	9	1170

Table 8: Lower bounds / conjectured values of e for all $n \leq 12000$ for which $e \nmid n$.

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,ℓ_p}.

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

[5] See `http://www.primegrid.com`.

$\log\log x$, see [3]. This heuristic is based on the simple expectation estimate $\sum_{p \le x} p^{-1}$ 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., $\ell_p \ge 3$) 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,ℓ_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 $w_{p,2} > 2\log_2 p$.

6. Connection to the *abc*-Conjecture

Miller[6] 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 $e \ge 2^{n/4-3/5}$ for infinitely many n contradicts the *abc*-conjecture, namely $2^n = 1 + e^2 D'$ has $c = 2^n$ and $N \le 2eD' = 2(2^n - 1)/e < 2^{3n/4+8/5}$, so that $\dfrac{\log c}{\log N} > \dfrac{4/3}{1 + 32/(15n)}$, 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 $e < K^{1/(1+\epsilon)} 2^{1+n\epsilon/(1+\epsilon)}$. This shows that any $\epsilon < 1/3$ will for sufficiently large n give the truth of Conjecture 5 via Theorem 11(a).

Robert, Stewart and Tenenbaum [7] formulate a strong form of the *abc*-conjecture, implying that $\log c < \log N + C\sqrt{\dfrac{\log N}{\log\log N}}$ for a constant C (asymptotically $4\sqrt{3}$). Using $c = 2^n$ and $N \le 2^{n+1}/e \le 2^{n+1}$ we then obtain $n \log 2 < (n+1)\log 2 - \log e + C\sqrt{\dfrac{(n+1)\log 2}{\log(n+1) + \log\log 2}}$, hence $e < \exp\left(C'\sqrt{\dfrac{n}{\log n}}\right)$ 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, and it does of course imply Conjecture 5.

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.

[6] "Re: Order of an ideal in a class group", message to the NMBRTHRY mailing list, April 7, 2013, `https://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind1304&L=NMBRTHRY&F=&S=&P=5692`.

References

[1] Anna Bernasconi and Bruno Codenotti, Spectral analysis of Boolean functions as a graph eigenvalue problem, *IEEE Trans. Computers* **48** (1999), 345-351.

[2] Anna Bernasconi, Bruno Codenotti, and Jeffrey M. Vanderkam, A Characterization of bent functions in terms of strongly regular graphs, *IEEE Trans. Computers* **50** (2001), 984-985.

[3] Richard E. Crandall, Karl Dilcher, and Carl Pomerance, A search for Wieferich and Wilson primes, *Math. Comp* **66** (1997), 433-449.

[4] W. Ljunggren, Noen Setninger om ubestemte likninger av formen $(x^n - 1)/(x - 1) = y^q$, *Norsk Mat. Tidsskr.* **25** (1943), 17-20.

[5] Jacobus H. van Lint and Richard M. Wilson, A Course in Combinatorics, Cambridge University Press, Cambridge, 1992.

[6] T. Nagell, Løsning Oppg. 2, 1943, s.29, *Norsk Mat. Tidsskr.* **30** (1948), 62-64.

[7] O. Robert, C.L. Stewart, and G. Tenenbaum, A refinement of the *abc* conjecture, preprint, available at `http://iecl.univ-lorraine.fr/~Gerald.Tenenbaum/PUBLIC/Prepublications_et_publications/abc.pdf`.

[8] László Szalay, The equations $2^N \pm 2^M \pm 2^L = z^2$, *Indag. Math. (N.S.)* **13** (2002), 131-142.

[9] Benne de Weger, Algorithms for Diophantine Equations, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.