ON THE SET OF WIEFERICH PRIMES AND OF ITS COMPLEMENT

J.-M. DeKoninck and N. Doyon
(Québec, Canada)

Dedicated to the memory of Professor M.V. Subbarao

Abstract. A prime number p is called a *Wieferich prime* if $2^{p-1} \equiv 1 \pmod{p^2}$. More generally, given an integer $r \geq 2$, let W_r stand for the set of all primes p such that $2^{p-1} \equiv 1 \pmod{p^r}$ and W_r^c for its complement in the set of all primes. For each integer $r \geq 2$, let

$$W_r(x) := \sharp\{p \leq x : p \in W_r\} \quad \text{and} \quad W_r^c(x) := \sharp\{p \leq x : p \in W_r^c\}.$$

Silverman has shown that it follows from the *abc* conjecture that

$$(*) \qquad W_2^c(x) \gg \log x.$$

Here, we show that this lower bound is a consequence of a weaker hypothesis. In fact, we show that if the index of composition of $2^n - 1$ remains "small" as n increases, then (*) holds and that if it is not "too small" for infinitely many n's, then $|W_2| = +\infty$. Also, we improve the estimate $W_{16}^c(x) \gg \frac{\log x}{\log\log x}$ obtained by Mohit and Murty under a conjecture of Hall, by removing the denominator $\log\log x$.

1. Introduction

A prime number p is called a *Wieferich prime* if $2^{p-1} \equiv 1 \pmod{p^2}$. The only known such numbers are 1093 and 3511; any other Wierferich prime, if any, must be larger than 1.25×10^{15} (see Crandall, Dilcher & Pomerance [2] and the WEB site [9]). More generally, given an integer $r \geq 2$, let W_r stand for the set of all primes p such that $2^{p-1} \equiv 1 \pmod{p^r}$ and W_r^c for its complement in the set of all primes. Neither of the sets $W = W_2$ and $W^c = W_2^c$ has been shown to be infinite, although it is believed that they both are and moreover that the later one is of density 1 in the set of all primes.

For each integer $r \geq 2$, let

$$W_r(x) := \sharp\{p \leq x : p \in W_r\} \quad \text{and} \quad W_r^c(x) := \sharp\{p \leq x : p \in W_r^c\},$$

and for short $W(x) = W_2(x)$ and $W^c(x) = W_2^c(x)$. In 1988, using cyclotomic polynomials, Silverman [8] showed that it follows from the *abc* conjecture that

$$W^c(x) \gg \log x. \tag{1}$$

Here, we show that (1) holds, assuming a weaker hypothesis.

In [3], we studied the *index of composition* $\lambda(n)$ of an integer $n \geq 2$, defined by Jerzy Browkin [1] as the quotient $\frac{\log n}{\log \gamma(n)}$, where $\gamma(n) = \prod_{p|n} p$. This index measures essentially the mean multiplicity of the prime factors of an integer. Further let $\nu(n) := \prod_{p\|n} p$, and for convenience, set $\lambda(1) = \gamma(1) = \nu(1) = 1$.

We will show that if the index of composition of $2^n - 1$ remains "small" as n increases, then (1) holds, and on the other hand that if it is not "too small" for infinitely many n's, then $|W| = +\infty$. Finally, we improve the estimate $W_{16}^c(x) \gg \frac{\log x}{\log\log x}$ obtained by Mohit and Murty [6] under a conjecture of Hall, by removing the denominator $\log\log x$.

2. Main results

Theorem 1. $|W| = +\infty$ *if and only if* $\limsup_{n\to\infty} \dfrac{2^n - 1}{n \cdot \gamma(2^n - 1)} = +\infty.$

Theorem 2. $|W^c| = +\infty$ *if and only if there exist infinitely many integers* n *such that* $\nu(2^n - 1) \geq n$.

Theorem 3. *If there exists a real number* $\xi > 0$ *such that the set* $\{n \in \in \mathbf{N} : \lambda(2^n - 1) < 2 - \xi\}$ *is of density one, then (1) holds.*

Observe that the *abc* conjecture implies that $\lambda(2^n - 1) < 1 + \varepsilon$ for any $\varepsilon > 0$ provided n is large enough.

Before stating the next theorem, we mention the following conjecture of Hall [5]:

Hall's Conjecture. *Given any $\varepsilon > 0$, there exists a positive integer D_0 such that if $|D| > D_0$, any solution (x, y, D) to the diophantine equation $x^3 - D = y^2$ must satisfy $|x| < |D|^{2+\varepsilon}$.*

Theorem 4. *Hall's conjecture implies that $W_{16}^c(x) \gg \log x$.*

3. Preliminary results

Given a prime p, let α_p be the unique positive integer such that $p^{\alpha_p} \| 2^{p-1} - -1$. Also, given an integer $m \geq 2$, we denote by $\rho(m)$ the order of 2 mod m.

Lemma 1. *If some positive integer n, a prime p satisfies $p \| 2^n - 1$, then $p \in W^c$.*

This result is well known, but for the sake of completeness, we give a proof.

Proof. Let $r = \rho(p)$ and $k = (2^r - 1)/p$. Since, by hypothesis, $2^r \not\equiv 1 \pmod{p^2}$, we have that $gcd(k, p) = 1$. Since $r | p - 1$, there exists a positive integer $s \leq p - 1$ such that $p - 1 = rs$. Hence $gcd(ks, p = 1)$, so that

$$2^{p-1} = (2^r)^s = (1 + kp)^s \equiv 1 + skp \not\equiv 1 \pmod{p^2},$$

which proves that $p \in W^c$, as claimed.

Remark. Note that it follows from Lemma 1 (the known fact) that if there exists a prime q such q^2 divides a Mersenne number $2^p - 1$, then $q \in W$.

Lemma 2. *For each positive integer k,*

$$\rho(p^{\alpha_p + k}) = \rho(p) \cdot p^k.$$

Proof. We use introduction on k. We will show that if for some positive integer $i, p^{i+1} \not| 2^{\rho(p^i)} - 1$, then $\rho(p^{i+1}) = p \cdot \rho(p^i)$ and $p^{i+2} \not| 2^{\rho(p^{i+1})} - 1$, thereby establishing our claim.

First observe that $\rho(p^{i+1}) = d \cdot \rho(p^i)$ for some integer $d > 1$. Hence, arguing modulo p^{i+2}, there exist non negative integers m and n such that

$$\begin{aligned} 2^{\rho(p^{i+1})} &= \left(2^{\rho(p^i)}\right)^d \equiv \\ &\equiv (mp^{i+1} + np^i + 1)^d \equiv \\ &\equiv dmp^{i+1} + \frac{d(d-1)}{2} n^2 p^{2i} + dnp^i + 1 \pmod{p^{i+2}}. \end{aligned} \tag{2}$$

Since $2^{\rho(p^{i+1})} \equiv 1 \pmod{p^{i+1}}$, it follows that $dnp^i + 1 \equiv 1 \pmod{p^{i+1}}$. On the other hand, it is clear that $p \not| n$, since otherwise $2^{\rho(p^i)} \equiv 1 \pmod{p^{i+1}}$ which would contradict our induction hypothesis. Therefore, in order not to contradict the minimal choice of d, we must have that $p|d$, and in fact $p = d$.

It then follows from (2) that

$$2^{\rho(p^{i+1})} \equiv pmp^{i+1} + pnp^i + \frac{p(p-1)}{2} n^2 p^{2i} + 1 \equiv np^{i+1} + 1 \pmod{p^{i+2}},$$

and therefore that $p^{i+2} \not| 2^{\rho(p^{i+1})} - 1$, thus completing the proof of Lemma 2.

Denote by $2 = p_1 < p_2 < \ldots$ the sequence of all Wieferich primes, and given an integer $m \geq 2$, let

$$A_m := LCM\{\rho(p_i) : 1 \leq i \leq m\} \quad \text{and} \quad B_m := \prod_{i=1}^{m} p_i.$$

Lemma 3. *For all integers $m \geq 2$, we have*

$$\frac{B_m}{A_m} > 2^{m-1}.$$

Proof. First observe that

$$\begin{aligned} A_m =& LCM\{\rho(p_i) :\ 1 \leq i \leq m,\ \rho(p_i) = p_i - 1\} \cdot \\ & \cdot LCM\{\rho(p_i) :\ 1 \leq i \leq m,\ \rho(p_i) < p_i - 1\} = \\ =& L_1 \cdot L_2, \end{aligned} \tag{3}$$

say, and set $c_1 = |\{p_i : 1 \leq i \leq m,\ \rho(p_i) = p_i - 1\}|$ and $c_2 = |\{p_i : 1 \leq i \leq m,\ \rho(p_i) < p_i - 1\}|$.

Since $p_i - 1$ is even for each i, it follows that

$$L_1 \leq \frac{1}{2^{c_1 - 1}} \prod_{\substack{1 \leq i \leq m \\ \rho(p_i) = p_i - 1}} (p_i - 1). \tag{4}$$

On the other hand, since $\rho(p) | p-1$ and $\rho(p) < p - 1$ for those $p \in L_2$, we have that $\rho(p) \leq \dfrac{p-1}{2} < \dfrac{p}{2}$ and therefore

$$L_2 \leq \prod_{\substack{1 \leq i \leq m \\ \rho(p_i) < p_i - 1}} \rho(p_i) < \frac{1}{2^{c_2}} \prod_{\substack{1 \leq i \leq m \\ \rho(p_i) = p_i - 1}} p_i. \tag{5}$$

Using (4) and (5) in (3) we get

$$A_m < \frac{1}{2^{c_2+c_1-1}} \prod_{1\le i\le m} p_i = \frac{1}{2^{m-1}} B_m,$$

thus completing the proof of Lemma 3.

Lemma 4. *For all integers $m \ge 2$, B_m divides* $\dfrac{2^{A_m}-1}{\gamma(2^{A_m}-1)}$

Proof. We only need to show that for each positive integer

$$i \le m, \quad p_i \,\Big|\, \frac{2^{A_m}-1}{\gamma(2^{A_m}-1)},$$

or equivalently that $p_i^2 | 2^{A_m} - 1$. But since $\rho(p_i)|A_m$, we have that $p_i | 2^{A_m} - 1$. Moreover, since $p_i \in W$, we have $\alpha_{p_i} \ge 2$, which implies that $p_i^2 | 2^{A_m} - 1$, as requested, thus completing the proof of Lemma 4.

Lemma 5. *Let n be a positive integer for which there exists a positive real number $\xi < 1$ such that $\lambda(2^n - 1) < 2 - \xi$. Then $\log \nu(2^n - 1) > \xi_0 \log(2^n - 1)$, where $\xi_0 = \dfrac{\xi}{2-\xi}$.*

Proof. Let n and $\xi > 0$ be such that $\lambda(2^n - 1) < 2 - \xi$, and write

$$2^n - 1 = uv, \quad \text{with} \quad v = \nu(2^n - 1) \quad \text{and} \quad u = \frac{2^n - 1}{v}.$$

Then

$$2 - \xi > \lambda(2^n - 1) = \lambda(uv) = \frac{\log(uv)}{\log \gamma(uv)} > \frac{\log u + \log v}{\log v + \frac{1}{2}\log u},$$

which implies that $(1-\xi)\log v > \dfrac{\xi}{2} \log u$ and therefore that

$$\log(2^n - 1) = \log u + \log v < \log v + \frac{2(1-\xi)}{\xi} \log v = \frac{2-\xi}{\xi} \log v.$$

This allows us to write

$$\log v > \frac{\xi}{2-\xi} \log(2^n - 1),$$

thus completing the proof of Lemma 5.

Lemma 6. *Let $\xi, 0 < \xi < 1$ be a fixed number such that the set $A = A_\xi = \{n \in \mathbf{N} : \lambda(2^n - 1) < 2 - \xi\}$ has density 1. Then, if x is sufficiently large,*

$$\sum_{n \le \log_2 x} \sum_{p \| 2^n - 1} \log_2 p > \frac{3}{8}\xi_0 (\log_2 x)^2,$$

where ξ_0 is the constant appearing in Lemma 5.

(From here on, $\log_2 x$ stands for the logarithm of x in base 2.)

Proof. Since $\sum\limits_{p \| 2^n - 1} \log_2 p = \log_2(\nu(2^n - 1))$, then using Lemma 5,

$$\sum_{n \le \log_2 x} \sum_{p \| 2^n - 1} \log p > \sum_{\substack{n \le \log_2 x \\ n \in A}} \sum_{p \| 2^n - 1} \log p > \xi_0 \sum_{\substack{n \le \log_2 x \\ n \in A}} n + O\left(\sum_{n \le \log_2 x} \frac{1}{2^n} \right) >$$
$$> \xi_0 \frac{1}{2} (\log_2 x)^2 + O(1) > \frac{3}{8}\xi_0 (\log_2 x)^2,$$

provided x is sufficiently large, thus completing the proof of Lemma 6.

4. Proof of the main results

Proof of Theorem 1. First assume that $|W| = +\infty$ and let k be an arbitrary positive integer. Then choose m_0 such that $2^{m_0 - 1} > k$. Then using Lemma 3 and Lemma 4, we get that for all $m \ge m_0$,

$$\frac{2^{A_m} - 1}{\gamma(2^{A_m} - 1)} \ge B_m \ge 2^{m-1} A_m > k A_m,$$

which proves the first part of Theorem 1.

To prove the second part, we will show that assuming that

$$\limsup_{n \to \infty} \frac{2^n - 1}{n \cdot \gamma(2^n - 1)} = +\infty$$

and that $|W| < +\infty$ leads to a contradiction. Let $W = \{p_1, p_2, \ldots, p_r\}$ and $R := \prod\limits_{i \le r} p_i^{\alpha_{p_i}}$. We will prove that for all integers $a \ge 2$, we have $\frac{2^a - 1}{\gamma(2^a - 1)} \le Ra$. Fix a and denote by $q_1, q_2, \ldots, q_s$ the prime divisors of $2^a - 1$. Then, for each

$1 \le i \le s$, let $\alpha_{q_i} + k_i$ be the unique positive integer satisfying $q_i^{\alpha_{q_i}+k_i} \| 2^a - 1$. It follows that

$$\frac{2^a-1}{\gamma(2^a-1)} = \prod_{i\le s} q_i^{\alpha_{q_i}+k_i-1} = \prod_{i\le s} q_i^{\alpha_{q_i}-1} \cdot \prod_{i\le s} q_i^{k_i} \le \prod_{i\le s} q_i^{\alpha_{q_i}-1} \cdot a$$

by Lemma 2. Indeed, since $\rho(q^{\alpha_{q_i}+k_i})|a$ and since by Lemma 2 $\rho(q_i^{\alpha_{q_i}+k_i}) = = \rho(q_i) q_i^{k_i}$ we get $\prod_{i\le s} q_i^{k_i} | a$. It follows from this that

$$\frac{2^a-1}{\gamma(2^a-1)} \le Ra,$$

thus providing the desired contradiction and concluding the proof of Theorem 1.

Proof of Theorem 2. First assume that the set $W^c = \{q_1, q_2, \ldots\}$ is infinite. Then, for each i, we have

$$\nu(2^{\rho(q_i)} - 1) \ge q_i > \rho(q_i),$$

which implies that $\nu(2^n - 1) > n$ for infinitely many n's.

Assume now that W^c is finite, and let $R := \prod_{p \in W^c} p$. Then for all $a > R$, we have

$$\nu(2^a - 1) \le R < a,$$

which completes the proof of Theorem 2.

Proof of Theorem 3. Let ξ, $0 < \xi < 1$ be a real number such that the set A_ξ has a density of 1. In view of Lemma 6, we have

$$\begin{aligned} \frac{3\xi_0 \log_2^2 x}{8} &< \sum_{n=1}^{[\log_2 x]} \sum_{p \| 2^n - 1} \log_2 p \le \sum_{n=1}^{[\log_2 x]} \sum_{\substack{p | 2^n - 1 \\ p \le x,\ p \in W^c}} \log_2 p = \\ &= \sum_{n=1}^{[\log_2 x]} \sum_{a | n} \sum_{\substack{\rho(p) = a \\ p \le x,\ p \in W^c}} \log_2 p = \sum_{a=1}^{[\log_2 x]} \left[\frac{\log_2 x}{a}\right] \sum_{\substack{\rho(p) = a \\ p \le x,\ p \in W^c}} \log_2 p. \end{aligned} \tag{6}$$

Letting E be this last expression, we now split the first sum in E in two parts, namely as a varies from 1 to $[\xi_1 \log_2 x]$ and then from $[\xi_1 \log_2 x] + 1$ to $[\log_2 x]$, where $\xi_1 := 3\xi_0/16$. We then have

$$\begin{aligned} E = &\sum_{a=1}^{[\xi_1 \log_2 x]} \left[\frac{\log_2 x}{a}\right] \sum_{\substack{\rho(p)=a \\ p\le x,\ p\in W^c}} \log_2 p + \\ &+ \sum_{a=[\xi_1 \log_2 x]+1}^{[\log_2 x]} \left[\frac{\log_2 x}{a}\right] \sum_{\substack{\rho(p)=a \\ p\le x,\ p\in W^c}} \log_2 p = \\ &= S_1 + S_2, \end{aligned} \tag{7}$$

say. We first find an upper bound for S_1. Since

$$\sum_{\substack{\rho(p)=a \\ p\le x,\ p\in W^c}} \log p < \sum_{p|2^a-1} \log p < a \log 2,$$

we have that

$$S_1 < \sum_{a=1}^{[\xi_1 \log_2 x]} \left[\frac{\log_2 x}{a}\right] a \log 2 < \xi_1 \log_2^2 x \log 2. \tag{8}$$

It then follows from (6), (7) and (8) that

$$S_2 \ge \frac{3\xi_0 \log_2^2 x}{8} - S_1 \ge \left(\frac{3\xi_0}{8} - \xi_1 \log 2\right) \log_2^2 x. \tag{9}$$

On the other hand,

$$\begin{aligned} S_2 &\le \frac{1}{\xi_1} \sum_{a=[\xi_1 \log_2 x]+1}^{[\log_2 x]} \sum_{\substack{\rho(p)=a \\ p\le x,\ p\in W^c}} \log_2 p < \\ &< \frac{1}{\xi_1} \sum_{\substack{\rho(p)\in[\xi_1 \log_2 x, \log_2 x] \\ p\le x,\ p\in W^c}} \log_2 p < \\ &< \frac{1}{\xi_1} \sum_{p\le x,\ p\in W^c} \log_2 p < \frac{1}{\xi_1} \log_2 x |W^c(x)|. \end{aligned} \tag{10}$$

Putting together (9) and (11), it follows that

$$W^c(x) \ge \xi_1 \left(\frac{3\xi_0}{8} - \xi_1 \log 2\right) \log_2 x,$$

which completes the proof of Theorem 3.

Proof of Theorem 4. Before proving Theorem 4, we will show that the *abc* conjecture implies Hall's conjecture. Indeed, applying the *abc* conjecture to the equation $y^2+D=x^3$, we have that for all $\delta>0$,

$$\gamma(x^3y^2D)^{1+\delta}=\gamma(xyD)^{1+\delta}\gg x^3. \tag{11}$$

It follows from $y^2+D=x^3$ that $y\le x^{3/2}$. Hence using this in (11) and observing that $\gamma(xyD)\le xyD$, we get that

$$x^3\ll\gamma(xyD)^{1+\delta}\le(xyD)^{1+\delta}\le(x^{5/2}D)^{1+\delta},$$

which implies that $D^{1+\delta}\gg x^{1/2-5\delta/2}$, that is

$$D^{\frac{1+\delta}{1/2-5\delta/3}}\gg x.$$

Since the exponent of D tends to 2 when $\delta\to 0$, we have that for each $\varepsilon>$ >0, $D^{2+\varepsilon}\gg x$. We may therefore conclude that the *abc* conjecture implies Hall's conjecture.

Let us now prove that Hall's conjecture implies that $W_{16}^c(x)\gg\log x$. First consider the equation $2^{3k+1}-1=n$ and write $n=uv$, where

$$v:=\prod_{p^b\| n,\ b\ge 16}p^b,$$

and where $u=n/v$. Furthermore, let a be the smallest positive integer such that an is a perfect square, so that

$$a=\prod_{p^b\| n,\ b\ \text{odd}}p.$$

Hence, multiplying both sides of $2^{3k+1}-1=uv$ by $4a^3$, we obtain that

$$a^32^{3k+3}-4a^3=4a^3uv,$$

that is,

$$(a2^{k+1})^3-4a^3=(\sqrt{4a^3uv})^2.$$

Since $4a^2$ and auv are perfect squares, it follows that $\sqrt{4a^3uv}$ is an integer. Therefore, using Hall's conjecture, we have that

$$a2^{k+1}<(4a^3)^{2+\varepsilon},$$

or equivalently

$$a^{15+9\varepsilon} > 2^{3k-3} > \frac{uv}{16}. \tag{12}$$

On the other hand, from the definitions of a and v, we also have that $a \leq uv^{1/16}$. Using this in (12), we successively obtain that

$$\begin{aligned} (uv^{1/16})^{15+\varepsilon} &> uv, \\ 16u^{14+\varepsilon} &> v^{\frac{1}{16}-\frac{9\varepsilon}{16}}, \\ v &< Cu^{224+\varepsilon_1}, \end{aligned}$$

where C is an absolute constant and $\varepsilon_1 = \varepsilon_1(\varepsilon)$ tends to 0. Hence,

$$2^{3k+1} - 1 = uv < Cu^{225+\varepsilon_1},$$

and therefore

$$\log u \gg \frac{\log(2^{3k+1})}{225+\varepsilon}.$$

Thereafter, using essentially the same technique as in the proof of Theorem 3, the result follows.

5. Final remarks

It is surprising that though we only know the existence of two Wieferich primes, we are unable to prove the deceptively obvious $W^c(x) = \infty$. Even worse, we cannot prove that $|W_r^c| = +\infty$ for any integer $r \geq 2$ even a large one. As a first step of an eventual proof, one could consider the 1986 result of Granville [4] who proved that if there exists no three consecutive powerful numbers, then $|W^c| = +\infty$.

One might consider that the quantity 2^p belongs to one of the classes of congruence $1, p+1, 2p+1, (p-1)p+1$ modulo p^2 with equal likelihood. Furthermore, if one assumes that the probability that a given prime p is a Wieferich prime is equal to $\frac{1}{p}$, one should expect the order of magnitude of $W_2^c(x)$ to be about $\sum_{p<x} \frac{1}{p} \approx \log\log x$; a quantity growing so slowly that numerical evidence neither infirms or confirms this conjecture.

Seemingly, there is nothing special with basis 2 except that it is the simplest occurrence of the question: for which prime p does p^2 divides $2^{p-1}-1$?

References

[1] **Browkin J.,** The abc-conjecture, *Number Theory,* Trends Math., Birkhäuser, Basel, 2000, 75-105.

[2] **Crandall R., Dilcher K. and Pomerance C.,** A search for Wieferich and Wilson primes, *Math. Comp.,* **66** (1997), 433-449.

[3] **DeKoninck J.-M. and Doyon N.,** À propos de l'indice de composition des nombres, *Monatshefte für Mathematik,* **139** (2003), 151-167.

[4] **Granville A.,** Powerful numbers and Fermat's last theorem, *C.R. Math. Rep. Acad. Sci. Canada,* **8** (3) (1986), 215-218.

[5] **Hall Jr. M.,** The diophantine equation $x^3-y^2=k$, *Computers in number theory. Proc. Sci. Res. Council Atlas Sympos. 2, Oxford, 1969,* Academic Press, London, 1971, 173-198.

[6] **Mohit S. and Murty M.R.,** Wieferich primes and Hall's conjecture, *C.R. Math. Acad. Sci. Soc. R. Can.,* **20** (1) (1998), 29-32.

[7] **Ribenboim P.,** *My numbers, my friends,* Springer Verlag, 2000.

[8] **Silverman J.H.,** Wieferich's criterion and the *abc*-conjecture, *J. Number Theory,* **30** (1988), 226-237.

[9] `www.utm.edu/research/primes/references/refs.cgi`

(Received July 18, 2006)

J.-M. DeKoninck
Département de mathématiques
et de statistique
Université Laval, Québec
Québec G1K 7P4, Canada
jmdk@mat.ulaval.ca

N. Doyon
Département de mathématiques
et de statistique
Université Laval, Québec
Québec G1K 7P4, Canada
ndoyon@mat.ulaval.ca