Journal of Number Theory 133 (2013) 1809–1813

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The abc conjecture and non-Wieferich primes in arithmetic progressions

Hester Graves [a,*], M. Ram Murty [b]

[a] 518 Jeffrey Hall, Queen's University, Kingston, Ontario K7L 3N6, Canada
[b] 312 Jeffrey Hall, Queen's University, Kingston, Ontario K7L 3N6, Canada

ARTICLE INFO

Article history:
Received 18 June 2012
Revised 12 September 2012
Accepted 6 October 2012
Available online xxxx
Communicated by Greg Martin

MSC:
11A41
11B25

Keywords:
Wieferich primes
Arithmetic progressions
abc conjecture

ABSTRACT

Silverman proved that, if one assumes the abc conjecture, then there are $\gg \log x$ non-Wieferich primes for base a for all $a \geqslant 2$. We show that for any $a \geqslant 2$ and any fixed $k \geqslant 2$, there are $\gg \log x/\log\log x$ primes $p \leqslant x$ such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$, under the assumption of the abc conjecture.

1. Wieferich primes

In 1909, Arthur Wieferich showed that if there existed some odd prime p and some integers x, y, z such that $xyz \neq 0$ and

$$x^p + y^p + z^p = 0,$$

p coprime to xyz, then

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{1}$$

* Corresponding author.
E-mail addresses: gravesh@mast.queensu.ca (H. Graves), murty@mast.queensu.ca (M. Ram Murty).

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.10.012

Since then, primes satisfying (1) have been called Wieferich primes. If

$$a^{p-1} \equiv 1 \pmod{p^2} \tag{2}$$

for some integer a, then we say p is a Wieferich prime for base a.

The only known Wieferich primes for base two are 1093 and 3511, found respectively by Meissner in 1913 and Beegner in 1922. According to the PrimeGrid project, as of May 2012, these are the only Wieferich primes for base two less than 17×10^{15}. Even though only two Wieferich primes for base two are known, it is unknown whether there are finitely many or infinitely many Wieferich primes. It is not even known if there are infinitely many non-Wieferich primes.

The only non-computational results on Wieferich primes are conditional. Silverman showed that if the abc conjecture (see the next section) holds, then there are $\gg \log x$ non-Wieferich primes. De Koninck and Doyon proved the same result under the weaker assumption that there exists some $\epsilon > 0$ such that the set $\{n \in \mathbb{N}: \frac{\log(2^n-1)}{\log \operatorname{rad}(2^n-1)} < 2-\epsilon\}$ is of density one [1].

In this paper, we will show that if the abc conjecture is true, then for any integer $k > 1$, there are infinitely many non-Wieferich primes p with $p \equiv 1 \pmod{k}$. In fact, the number of such primes is $\gg \frac{\log x}{\log\log x}$.

2. Background

Let us recall that the **abc conjecture** of Oesterlé and Masser (1985) states that if a, b and c are positive integers such that $a + b = c$ and $(a, b) = 1$, then for all $\epsilon > 0$,

$$c \ll_\epsilon \left(\operatorname{rad}(abc)\right)^{1+\epsilon}.$$

Let us also remind ourselves that Rosser found a lower bound for the nth prime, stated below.

Proposition 2.1 *(Rosser's theorem). (See [3].) The nth prime is strictly greater than $n \log n$.*

One can prove, assuming the conjecture, the infinitude of non-Wieferich primes $p \equiv 1 \pmod{k}$ using elementary methods, but we use the following recent result of Thangadurai and Vatwani [5] in order to cleanly prove our growth result. Before we state their result, we define ϕ to be the Euler totient function and $\Phi_n(x)$ to be the nth cyclotomic polynomial.

Proposition 2.2. *For all integers $a \geqslant 2$ and $n > 2$,*

$$\left|\Phi_n(a)\right| \geqslant \frac{1}{2} a^{\phi(n)}.$$

Our proof also requires the following, proved on page 233 of [2].

Lemma 2.3. *If $p \mid \Phi_n(a)$, then either $p \mid n$ or $p \equiv 1 \pmod{n}$.*

Lastly, we need the concept of the powerful part of a number.

Definition 1. Given an integer n, $n = \prod_p p^\alpha$, where the product is over the distinct primes $p \mid n$, we define its **powerful part** to be the product of the prime powers $p^\alpha \mid n$ such that $p^{\alpha+1} \nmid n$, and $\alpha \geqslant 2$.

Lemma 2.4. *Suppose $a^n - 1$ is factored into $C_n D_n$, where D_n is the powerful part of $a^n - 1$. If $p \mid C_n$, then $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

Proof. This proof follows Silverman [4]. Suppose that $p \mid C_n$. Let e be the order of a modulo p, so $e \mid (p-1)$ and $a^e = 1 + pt$. We know that $a^n \equiv 1 \pmod{p}$, so $e \mid n$. Therefore,

$$a^n = \left(a^e\right)^{\frac{n}{e}} = (1+pt)^{\frac{n}{e}} \equiv 1 + \frac{n}{e}pt \pmod{p^2}.$$

Since $p \mid C_n$ and C_n is square-free, $p^2 \nmid (a^n - 1)$ and $p \nmid t$.

Similarly,

$$a^{p-1} = \left(a^e\right)^{\frac{p-1}{e}} = (1+pt)^{\frac{p-1}{e}} \equiv 1 + \frac{p-1}{e}pt \pmod{p^2}$$

and, as $p \nmid t$, $p^2 \nmid (\frac{p-1}{e}pt)$ and thus $a^{p-1} \not\equiv 1 \pmod{p^2}$. □

3. Results

Theorem 3.1. *If a and k are integers greater than one and one assumes the abc conjecture, then there are infinitely many primes p such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$.*

Proof. Let $\epsilon < \frac{\phi(k)}{3k}$. We denote by p_n the nth prime number that is relatively prime to k and we factor $a^{p_n k} - 1 = C_{p_n k} D_{p_n k}$, where $D_{p_n k}$ is the powerful part of $a^{p_n k} - 1$. Since

$$a^{p_n k} = \left(a^{p_n k} - 1\right) + 1,$$

the abc conjecture implies that

$$a^{p_n k} \ll_\epsilon \left(\operatorname{rad}\left(a^{p_n k}\left(a^{p_n k} - 1\right)\right)\right)^{1+\epsilon/2},$$

so

$$a^{p_n k} - 1 \ll_\epsilon \left(\operatorname{rad}(a C_{p_n k} D_{p_n k})\right)^{1+\epsilon/2}$$

and thus

$$C_{p_n k} D_{p_n k} \ll_\epsilon \left(a C_{p_n k} D_{p_n k}^{1/2}\right)^{1+\epsilon/2},$$

since $\operatorname{rad}(D_{p_n k}) \leqslant D_{p_n k}^{1/2}$. This implies that

$$D_{p_n k}^{1/2} \ll_{\epsilon,a} (a C_{p_n k} D_{p_n k})^{\epsilon/2},$$

so $D_{p_n k} \ll_{\epsilon,a} (a(a^{p_n k} - 1))^{\epsilon}$ and we conclude that

$$D_{p_n k} \ll_{\epsilon,a} a^{p_n k \epsilon}.$$

As

$$a^{p_n k} - 1 \ll_{\epsilon,a} C_{p_n k} a^{p_n k \epsilon},$$

$$C_{p_n k} \gg_{\epsilon,a} a^{p_n k (1-\epsilon)}.$$

Let $C'_{p_nk} = (C_{p_nk}, \Phi_{p_nk}(a))$ and $D'_{p_nk} = (D_{p_nk}, \Phi_{p_nk}(a))$, so that $C'_{p_n} D'_{p_nk} = \Phi_{p_nk}(a)$. By Proposition 2.2,

$$a^{p_nk\epsilon} C'_{p_nk} \gg \Phi_{p_nk}(a) \geqslant \frac{1}{2} a^{\phi(p_nk)},$$

so by our choice of ϵ and Rosser's theorem (Proposition 2.1, [3]),

$$C'_{p_nk} \gg a^{\phi(p_nk) - p_nk\epsilon} \gg a^{\frac{\phi(p_nk)}{2}} \gg a^{n \log n}.$$

Thus as C'_{p_nk} is a product of distinct primes,

$$\lim_{n\to\infty} \left| \{\text{primes } p\colon\ p \mid C'_{p_jk},\ j \leqslant n\} \right| = \infty.$$

Every prime p that divides C'_{p_nk} also divides $\Phi_{p_nk}(a)$ and is therefore congruent to 1 modulo p_nk by Lemma 2.3. We also know that if p divides C'_{p_nk}, then $a^{p-1} \not\equiv 1 \pmod{p^2}$ by Lemma 2.4. Thus there are infinitely many primes p such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$. □

Lemma 3.2. *For large n, there exists some prime p such that $p \mid C'_{p_nk}$ but $p \nmid C'_{p_jk}$ for $j < n$.*

Proof. Proof by contradiction. Suppose not. Then

$$C'_{p_nk} \leqslant \prod_{i=1}^{n-1} (C'_{p_ik}, C'_{p_nk}).$$

As $C'_{p_ik} \mid (a^{p_ik} - 1)$ and $C'_{p_nk} \mid (a^{p_nk} - 1)$, $(C'_{p_ik}, C'_{p_nk}) \mid (a^{p_ik} - 1, a^{p_nk} - 1)$. It is well-known that $(a^b - 1, a^c - 1) = (a^{(b,c)} - 1)$. Therefore, $C'_{p_nk} \leqslant (a^k - 1)^{n-1} \ll a^{kn}$. From the proof of Theorem 3.1, we know that $C'_{p_nk} \gg a^{n \log n}$, so

$$a^{kn} \gg C'_{p_nk} \gg a^{n \log n},$$

which is clearly a contradiction for large n. □

Theorem 3.3. *If a, k, and n are positive integers and one assumes the abc conjecture, then*

$$\left| \left\{ \text{primes } p \leqslant x\colon\ \begin{matrix} p \equiv 1 \pmod{k} \\ a^{p-1} \not\equiv 1 \pmod{p^2} \end{matrix} \right\} \right| \gg \frac{\log x}{\log\log x}.$$

Proof. The largest n such that

$$x \geqslant a^{p_nk}$$

is $\ll \frac{\log x}{\log\log x}$, and as $a^{p_nk} > C'_n$ and

$$\left| \left\{ \text{primes } p \leqslant C'_n\colon\ \begin{matrix} p \equiv 1 \pmod{k} \\ a^{p-1} \not\equiv 1 \pmod{p^2} \end{matrix} \right\} \right| \gg n,$$

we obtain that

$$\left|\left\{\text{primes } p \leqslant x\colon \begin{array}{l} p \equiv 1 \pmod{k} \\ a^{p-1} \not\equiv 1 \pmod{p^2} \end{array}\right\}\right| \gg \frac{\log x}{\log\log x}. \qquad \square$$

Acknowledgments

We thank the referee for several helpful remarks on an earlier version of this paper.

References

[1] J.M. De Koninck, N. Doyon, On the set of Wieferich primes and of its complement, Ann. Univ. Sci. Budapest. Sect. Comput. 27 (2007) 3–13.
[2] M. Ram Murty, Problems in Analytic Number Theory, second edition, Grad. Texts in Math., vol. 206, Springer, 2008.
[3] J.B. Rosser, The nth prime is greater than $n\log(n)$, Proc. London Math. Soc. 45 (1938) 21–44.
[4] J. Silverman, Wieferich's criterion and the abc-conjecture, J. Number Theory 30 (2) (1988) 226–237.
[5] R. Thangadurai, A. Vatwani, The least prime congruent to one modulo n, Amer. Math. Monthly 118 (2011) 737–742.