PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 5, May 2017, Pages 1833–1836
http://dx.doi.org/10.1090/proc/13201
Article electronically published on January 23, 2017

NON-WIEFERICH PRIMES IN ARITHMETIC PROGRESSIONS

YONG-GAO CHEN AND YU DING

(Communicated by Matthew A. Papanikolas)

Abstract. Graves and Murty proved that for any integer $a \geq 2$ and any fixed integer $k \geq 2$, there are $\gg \log x / \log\log x$ primes $p \leq x$ such that $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$, under the assumption of the abc conjecture. In this paper, for any fixed M, the bound $\log x / \log\log x$ is improved to $(\log x/\log\log x)(\log\log\log x)^M$.

1. Introduction

In 1909, A. Wieferich [5] found that Fermat's last theorem is related to the primes p with

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{1.1}$$

That is, for any odd prime p, if the equation $x^p + y^p + z^p = 0$ has a solution in integers x, y, z with $p \nmid xyz$, then (1.1) holds. Since then, such primes have been called Wieferich primes. For any integer $a \geq 2$ and any prime p, if

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

then p is said to be a Wieferich prime for base a. Otherwise, p is said to be a non-Wieferich prime for base a. Currently, the only known Wieferich primes are 1093 and 3511. It is unknown whether there are infinitely many Wieferich primes and also unknown whether there are infinitely many non-Wieferich primes.

The abc conjecture says that, if a, b and c are positive integers with $a + b = c$ and $(a, b) = 1$, then, for any $\varepsilon > 0$,

$$c \ll_\varepsilon (\mathrm{rad}(abc))^{1+\varepsilon},$$

where $\mathrm{rad}(abc)$ is the product of all distinct prime factors of abc.

Silverman [4] proved that there are $\gg \log x$ non-Wieferich primes under the assumption of the abc conjecture. DeKoninck and Doyon [1] proved the same result under the weaker assumption. In 2013, Graves and Murty [2] proved that for any integer $a \geq 2$ and any fixed integer $k \geq 2$, there are

$$\gg \frac{\log x}{\log\log x}$$

Received by the editors November 4, 2015 and, in revised form, February 25, 2016.
2010 *Mathematics Subject Classification.* Primary 11A41, 11B25.
Key words and phrases. Wieferich primes, arithmetic progressions, abc conjecture.
This work was supported by the National Natural Science Foundation of China (No. 11371195) and PAPD.

primes $p \le x$ such that

$$a^{p-1} \not\equiv 1 \pmod{p^2}, \quad p \equiv 1 \pmod{k},$$

under the assumption of the abc conjecture.

In this paper, the bound is improved.

Theorem 1.1. *Let a and k be fixed integers with $a \ge 2$ and $k \ge 2$ and let $\mathcal{P}$ be the set of all primes. Suppose that the abc conjecture is true. Then, for any positive integer M, we have*

$$\left|\{p : p \le x, p \in \mathcal{P}, p \equiv 1 \,(\mathrm{mod}\ k), a^{p-1} \not\equiv 1 \,(\mathrm{mod}\ p^2)\}\right| \gg \frac{(\log x)(\log\log\log x)^M}{\log\log x}.$$

2. Proof of Theorem 1.1

In the following, we fix integers a, k and M with $a \ge 2$, $k \ge 2$ and $M \ge 1$.

Let p_i be the ith prime. Let

$$\delta_M = \prod_{i=1}^{M+1} \left(1 - \frac{1}{p_i}\right)$$

and let $\mathcal{T}_M$ be the set of all square-free integers with exactly $M+1$ prime factors. We follow the proof of Graves and Murty [2]. For any positive integer n, let $a^n - 1 = q_1^{\alpha_1} \cdots q_r^{\alpha_r}$ be the standard factorization of $a^n - 1$. Define

$$C_n = \prod_{\alpha_i = 1} q_i, \quad D_n = \prod_{\alpha_i > 1} q_i^{\alpha_i}.$$

Let ϕ be the Euler totient function and $\Phi_n(x)$ be the nth cyclotomic polynomial. Let

$$C_n' = (C_n, \Phi_n(a)), \quad D_n' = (D_n, \Phi_n(a)).$$

Since $a^n - 1 = C_n D_n$, $(C_n, D_n) = 1$ and $\Phi_n(a) \mid a^n - 1$, it follows that

$$\Phi_n(a) = (a^n - 1, \Phi_n(a)) = (C_n D_n, \Phi_n(a)) = C_n' D_n'.$$

We need the following lemmas.

Lemma 2.1 ([2, Lemma 2.3])**.** *If p is a prime with $p \mid \Phi_n(a)$, then either $p \mid n$ or $p \equiv 1 \pmod{n}$.*

Lemma 2.2 ([2, Lemma 2.4])**.** *If p is a prime with $p \mid C_n$, then*

$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

Lemma 2.3 ([3, Theorem 437])**.** *Let $\pi_m(x)$ denote the number of square-free integers which do not exceed x and have exactly m prime factors. Then*

$$\pi_m(x) \sim \frac{x(\log\log x)^{m-1}}{(m-1)!\log x}.$$

Lemma 2.4. *Let ε be a (small) positive number. Suppose that the abc conjecture is true. Then*

$$C_n' \gg a^{\phi(n) - \varepsilon n}.$$

Proof. A proof is similar to that of [2, Theorem 3.1]. We omit the details here. ☐

The following lemma is one of the key lemmas in this paper.

Lemma 2.5. *If $m < n$, then $(C_m', C_n') = 1$.*

Proof. Suppose that $(C'_m, C'_n) > 1$. Let p be a prime such that $p \mid C'_m$ and $p \mid C'_n$. By the definitions of C'_m and C'_n, we have $p \mid \Phi_m(a)$ and $p \mid \Phi_n(a)$. So

$$p \mid a^m - 1, \quad p \mid a^n - 1.$$

Thus $p \mid a^{(m,n)} - 1$. By $m < n$, we have $(m,n) < n$. Since

$$a^n - 1 = \frac{a^n - 1}{a^{(m,n)} - 1}\left(a^{(m,n)} - 1\right), \quad \Phi_n(a) \Big| \frac{a^n - 1}{a^{(m,n)} - 1},$$

it follows that $p^2 \mid a^n - 1$, a contradiction with $p \mid C'_n$. Therefore,

$$(C'_m, C'_n) = 1.$$

□

Lemma 2.6. *Suppose that the abc conjecture is true. Then there exists an integer n_0 depending only on a, k, M such that, if $n \in \mathcal{T}_M$ with $n \ge n_0$, then $C'_{nk} > nk$.*

Proof. Let

$$\varepsilon = \frac{\delta_M \phi(k)}{3k}.$$

By Lemma 2.4, we have

$$C'_{nk} \gg a^{\phi(nk) - \varepsilon nk}. \tag{2.1}$$

Since

$$\phi(m) = m \prod_{p \mid m}\left(1 - \frac{1}{p}\right) \tag{2.2}$$

and

$$\prod_{p \mid nk}\left(1 - \frac{1}{p}\right) \ge \prod_{p \mid n}\left(1 - \frac{1}{p}\right)\prod_{p \mid k}\left(1 - \frac{1}{p}\right),$$

it follows that $\phi(nk) \ge \phi(n)\phi(k)$. If $n \in \mathcal{T}_M$, then, by (2.2), we have

$$\phi(nk) - \varepsilon nk \ge \phi(n)\phi(k) - \varepsilon nk \ge \delta_M n \phi(k) - \varepsilon nk = 2\varepsilon nk.$$

It follows from (2.1) that if $n \in \mathcal{T}_M$, then

$$C'_{nk} \gg a^{2\varepsilon nk} \gg a^{2\varepsilon nk - \log(nk)/\log a} nk.$$

Therefore, there exists an integer n_0 depending only on a, k, M such that, if $n \in \mathcal{T}_M$ with $n \ge n_0$, then $C'_{nk} > nk$. □

Lemma 2.7. *Let n_0 be as in Lemma 2.6. If $n \in \mathcal{T}_M$ with $n \ge n_0$, then there exists a prime q_n such that*

$$q_n \mid C'_{nk}, \quad q_n \equiv 1 \pmod{nk}, \quad a^{q_n - 1} \not\equiv 1 \pmod{q_n^2}.$$

Proof. Let $n \in \mathcal{T}_M$ with $n \ge n_0$. By Lemma 2.6 and C'_{nk} being square-free, there is a prime q_n such that $q_n \mid C'_{nk}$ and $q_n \nmid nk$. Since $C'_{nk} \mid \Phi_{nk}(a)$ and $q_n \nmid nk$, it follows from Lemma 2.1 that $q_n \equiv 1 \pmod{nk}$. By $q_n \mid C'_{nk}$, $C'_{nk} \mid C_{nk}$ and Lemma 2.2, we have $a^{q_n - 1} \not\equiv 1 \pmod{q_n^2}$. □

Proof of Theorem 1.1. Let n_0 and q_n be as in Lemma 2.7. By Lemma 2.5, the primes $q_n(n \in \mathcal{T}_M, n \geq n_0)$ are distinct. It is clear that $a^{nk} - 1 \leq x$ if and only if

$$n \leq \frac{\log(x+1)}{k \log a}.$$

Thus, $a^{nk} - 1 \leq x$ with $n \in \mathcal{T}_M$ if and only if

$$n \leq \frac{\log(x+1)}{k \log a}, \quad n \in \mathcal{T}_M.$$

It follows from Lemma 2.3 that the number of integers n with $a^{nk} - 1 \leq x$, $n \in \mathcal{T}_M$ and $n \geq n_0$ is

$$\gg \frac{(\log x)(\log\log\log x)^M}{\log\log x}.$$

Since $q_n \leq C'_{nk} \leq a^{nk} - 1$, it follows that the number of q_n with $q_n \leq x$, $n \in \mathcal{T}_M$ and $n \geq n_0$ is

$$\gg \frac{(\log x)(\log\log\log x)^M}{\log\log x}.$$

By Lemma 2.7, we have

$$q_n \equiv 1 \pmod{nk}, \quad a^{q_n - 1} \not\equiv 1 \pmod{q_n^2}.$$

Therefore,

$$\left|\{p : p \leq x, p \in \mathcal{P}, p \equiv 1 \,(\mathrm{mod}\ k), a^{p-1} \not\equiv 1 \,(\mathrm{mod}\ p^2)\}\right| \gg \frac{(\log x)(\log\log\log x)^M}{\log\log x}.$$

This completes the proof of Theorem 1.1. □

Acknowledgment

The authors are grateful to the referee for helpful comments.

References

[1] J.-M. DeKoninck and N. Doyon, *On the set of Wieferich primes and of its complement*, Ann. Univ. Sci. Budapest. Sect. Comput. **27** (2007), 3–13. MR2388537

[2] Hester Graves and M. Ram Murty, *The abc conjecture and non-Wieferich primes in arithmetic progressions*, J. Number Theory **133** (2013), no. 6, 1809–1813, DOI 10.1016/j.jnt.2012.10.012. MR3027939

[3] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th ed., The Clarendon Press, Oxford University Press, New York, 1979. MR568909

[4] Joseph H. Silverman, *Wieferich's criterion and the abc-conjecture*, J. Number Theory **30** (1988), no. 2, 226–237, DOI 10.1016/0022-314X(88)90019-4. MR961918

[5] Arthur Wieferich, *Zum letzten Fermatschen Theorem* (German), J. Reine Angew. Math. **136** (1909), 293–302, DOI 10.1515/crll.1909.136.293. MR1580782

School of Mathematical Sciences and Institute of Mathematics, Nanjing Normal University, Nanjing 210023, People's Republic of China

E-mail address: ygchen@njnu.edu.cn

School of Mathematical Sciences and Institute of Mathematics, Nanjing Normal University, Nanjing 210023, People's Repubilc of China

E-mail address: 840172236@qq.com