C. R. Acad. Sci. Paris, Ser. I 357 (2019) 483–486

Contents lists available at ScienceDirect

C. R. Acad. Sci. Paris, Ser. I

www.sciencedirect.com

Number theory

Non-Wieferich primes under the abc conjecture

La conjecture abc et les nombres premiers qui ne satisfont pas la condition de Wieferich

Yuchen Ding

Department of Mathematics, Nanjing University, Nanjing 210093, People's Republic of China

ARTICLE INFO

Article history:
Received 10 April 2019
Accepted after revision 17 May 2019
Available online 6 June 2019

Presented by the Editorial Board

ABSTRACT

Assuming the abc conjecture, Silverman proved that, for any given positive integer $a \geqslant 2$, there are $\gg \log x$ primes $p \leqslant x$ such that $a^{p-1} \not\equiv 1 \pmod{p^2}$. In this paper, we show that, for any given integers $a \geqslant 2$ and $k \geqslant 2$, there still are $\gg \log x$ primes $p \leqslant x$ satisfying $a^{p-1} \not\equiv 1 \pmod{p^2}$ and $p \equiv 1 \pmod{k}$, under the assumption of the abc conjecture. This improves a recent result of Chen and Ding.

RÉSUMÉ

Admettant la conjecture abc, Silverman a montré que, pour tout entier $a \geqslant 2$, il existe au moins $\gg \log x$ nombres premiers $p \leqslant x$ tels que $a^{p-1} \not\equiv 1 \pmod{p^2}$. Admettant toujours la conjecture abc, nous montrons ici que, pour tous entiers $a \geqslant 2$ et $k \geqslant 2$ donnés, il y a encore au moins $\gg \log x$ nombres premiers $p \leqslant x$ tels que $a^{p-1} \not\equiv 1 \pmod{p^2}$ et $p \equiv 1 \pmod{k}$. Ceci améliore un résultat récent de Chen et Ding.

1. Introduction

The famous abc conjecture asserts that, for every $\epsilon > 0$, there exists a constant $\kappa(\epsilon)$ such that, for any nonzero coprime integers a, b and c with $a + b = c$, we have

$$\max\{|a|, |b|, |c|\} \leqslant \kappa(\epsilon) \cdot (\mathrm{rad}(abc))^{1+\epsilon},$$

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

It is well known that Wiefereich primes and the first case of Fermat's last theorem are closely related [4]. For any positive integer a with $a \geqslant 2$, we say that p is a Wieferich prime for base a if $a^{p-1} \equiv 1 \pmod{p^2}$. A Wieferich prime for base 2 is

E-mail address: 840172236@qq.com.

https://doi.org/10.1016/j.crma.2019.05.007
1631-073X/

just called a Wieferich prime. It seems that almost all primes are non-Wieferich primes. However, we cannot even prove that non-Wieferich primes are infinite.

For $a \geqslant 2$ a positive integer, Silverman [3] proved that there are $\gg \log x$ non-Wieferich primes for base a, if the abc conjecture holds. For any integers $a \geqslant 2$ and $k \geqslant 2$, this result was extended to

$$\#\{p: \ p \leqslant x, \ a^{p-1} \not\equiv 1 \pmod{p^2}, \ p \equiv 1 \pmod{k}\} \gg \frac{\log x}{\log\log x}$$

by Graves and Murty [2], assuming the abc conjecture. Recently, Chen and Ding [1] improved this bound to obtain

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

for any fixed number M. The bound is improved further in this paper. Let $\mathbb{P}$ be the set of all primes. Our result is stated in the following.

Theorem 1.1. *Let a and k be given integers with $a \geqslant 2$ and $k \geqslant 2$. If one assumes the abc conjecture, then we have*

$$\#\{p: \ p \leqslant x, \ p \in \mathbb{P}, \ a^{p-1} \not\equiv 1 \pmod{p^2}, \ p \equiv 1 \pmod{k}\} \gg \log x.$$

2. Some lemmas

As usual, let $\Phi_n(x)$ denote the n-th cyclotomic polynomial. Let a, k be fixed positive integers with $a \geqslant 2$ and $k \geqslant 2$. We follow the notation of Chen and Ding [1] for convenience. Let C_n and D_n be the square-free and powerful part of $a^n - 1$ respectively. This means that we factor $a^n - 1$ as follows:

$$a^n - 1 = \prod_i p_i^{k_i}, \ C_n = \prod_{k_i=1} p_i, \ D_n = \prod_{k_i>1} p_i^{k_i}, \ a^n - 1 = C_n D_n.$$

Let $C'_n = (C_n, \Phi_n(a)), \ D'_n = (D_n, \Phi_n(a))$.

We give some lemmas in the following.

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

Lemma 2.2. *([2, Lemma 2.4]). If p is a prime with $p|C_n$, then $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

Lemma 2.3. *([1, Lemma 2.4]). Let ϵ be a positive number. Suppose that the abc conjecture is true. Then $C'_n \gg a^{\phi(n)-\epsilon n}$.*

Lemma 2.4. *([1, Lemma 2.5]). If $m < n$, then $(C'_m, C'_n) = 1$.*

Lemma 2.5. *Let $\varphi(n)$ be the Euler totient function. For any given positive integer k, we have*

$$\sum_{n \leqslant x} \frac{\varphi(nk)}{nk} = c(k)x + O(\log x),$$

where $c(k) = \prod_p \left(1 - \frac{(p,k)}{p^2}\right) > 0$ and the implied constant depends on k.

Proof. Noting that $\varphi(nk) = \sum_{d|nk} \mu(d) \frac{nk}{d}$, we have

$$\begin{aligned}\sum_{n \leqslant x} \frac{\varphi(nk)}{nk} &= \sum_{n \leqslant x} \sum_{d|nk} \mu(d) \frac{nk}{d} \cdot \frac{1}{nk} = \sum_{n \leqslant x} \sum_{d|nk} \frac{\mu(d)}{d} \\ &= \sum_{d \leqslant xk} \frac{\mu(d)}{d} \sum_{\substack{n \leqslant x \\ d|nk}} 1 = \sum_{d \leqslant xk} \frac{\mu(d)}{d} \sum_{\substack{n \leqslant x \\ \frac{d}{(d,k)}|n}} 1 = \sum_{d \leqslant xk} \frac{\mu(d)}{d} \left[\frac{x}{d/(d,k)}\right] \\ &= x \sum_{d \leqslant xk} \frac{\mu(d)(d,k)}{d^2} + O(\log x) = x \sum_{d=1}^{\infty} \frac{\mu(d)(d,k)}{d^2} + O(\log x)\end{aligned}$$

$$= x\prod_p\left(1+\frac{\mu(p)(p,k)}{p^2}+\frac{\mu(p^2)(p^2,k)}{p^4}+\cdots\right)+O(\log x)$$
$$= x\prod_p\left(1-\frac{(p,k)}{p^2}\right)+O(\log x).$$

It is clear that $c(k)=\prod_p\left(1-\frac{(p,k)}{p^2}\right)>0.$ □

Let $S=\{n: C'_{nk}>nk\}$ and $S(x)=|S\cap[1,x]|$.

Lemma 2.6. *We have $S(x)\gg x$, where the implied constant depends only on a, k.*

Proof. Let $L=\left\{n:\varphi(nk)>\frac{2c(k)}{3}nk\right\}$ and $L(x)=|L\cap[1,x]|$. Take $\epsilon=\frac{c(k)}{3}$ in Lemma 2.3, then for any $n\in L$, we have

$$C'_{nk}\gg a^{\varphi(nk)-\frac{c(k)}{3}nk}>a^{\frac{c(k)}{3}nk}.$$

So, there exists a number n_0 depending only on a, k such that, if $n>n_0$ and $n\in L$, then $C'_{nk}>nk$. Thus, we obtain that

$$S(x)=\sum_{\substack{n\leqslant x\\ C'_{nk}>nk}}1\geqslant\sum_{\substack{n\leqslant x\\ n\geqslant n_0,n\in L}}1=\sum_{\substack{n\leqslant x\\ n\geqslant n_0\\ \varphi(nk)>\frac{2c(k)}{3}nk}}1.$$

Note that

$$\sum_{\substack{n\leqslant x\\ \varphi(nk)\leqslant\frac{2c(k)}{3}nk}}\frac{\varphi(nk)}{nk}\leqslant\sum_{\substack{n\leqslant x\\ \varphi(nk)\leqslant\frac{2c(k)}{3}nk}}\frac{2c(k)}{3}\leqslant\frac{2c(k)}{3}x.$$

Hence, by Lemma 2.5, we have

$$S(x)\geqslant\sum_{\substack{n\leqslant x\\ n\geqslant n_0\\ \varphi(nk)>\frac{2c(k)}{3}nk}}1\gg\sum_{\substack{n\leqslant x\\ \varphi(nk)>\frac{2c(k)}{3}nk}}1\geqslant\sum_{\substack{n\leqslant x\\ \varphi(nk)>\frac{2c(k)}{3}nk}}\frac{\varphi(nk)}{nk}$$
$$=\sum_{n\leqslant x}\frac{\varphi(nk)}{nk}-\sum_{\substack{n\leqslant x\\ \varphi(nk)\leqslant\frac{2c(k)}{3}nk}}\frac{\varphi(nk)}{nk}$$
$$\geqslant c(k)x+O(\log x)-\frac{2c(k)}{3}x\gg x.\quad\square$$

3. Proof of Theorem 1.1

Proof. For any $n\in S$, since C_{nk} is square-free, so is $C'_{nk}=(C_{nk},\Phi_{nk}(a))$. It follows from $C'_{nk}>nk$ that there exists a prime l_n such that $l_n|C'_{nk}$ and $l_n\nmid nk$. From $C'_{nk}|C_{nk}$ and $l_n|C'_{nk}$, we get

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

by Lemma 2.2. Note that $l_n|C'_{nk}$, $C'_{nk}|\Phi_{nk}(a)$ and $l_n\nmid nk$, we know that

$$l_n\equiv 1\pmod{nk}$$

by Lemma 2.1. That is to say, for any $n\in S$, there is a prime l_n satisfying

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

Moreover, these l_n $(n\in S)$ are distinct primes because of Lemma 2.4. Therefore, we find that

$$\#\{p:\ p\leqslant x,\ p\in\mathbb{P},\ a^{p-1}\not\equiv 1\pmod{p^2},\ p\equiv 1\pmod{k}\}\geqslant\#\{n:\ n\in S,\ C'_{nk}\leqslant x\}.$$

Since $C'_{nk} \leqslant C_{nk} \leqslant a^{nk} - 1$, it is clear that

$$\begin{aligned}\#\{n : n \in S, C'_{nk} \leqslant x\} &\geqslant \#\{n : n \in S, a^{nk} - 1 \leqslant x\} \\ &= \#\left\{n : n \in S, n \leqslant \frac{\log(x+1)}{k \log a}\right\} \\ &= S\left(\frac{\log(x+1)}{k \log a}\right).\end{aligned}$$

Hence, by Lemma 2.6, we have

$$\#\{p : p \leqslant x, p \in \mathbb{P}, a^{p-1} \not\equiv 1 \pmod{p^2}, p \equiv 1 \pmod{k}\} \geqslant S\left(\frac{\log(x+1)}{k \log a}\right) \gg \log x. \quad \square$$

Acknowledgement

The author would like to thank Prof. C.X. Chen and Prof. Y.G. Chen for their generous help.

References

[1] Y.-G. Chen, Y. Ding, Non-Wieferich primes in arithmetic progressions, Proc. Amer. Math. Soc. 145 (2017) 1833–1836.
[2] H. Graves, M.R. Murty, The abc conjecture and non-Wieferich primes in arithmetic progressions, J. Number Theory 133 (2013) 1809–1813.
[3] J.H. Silverman, Wieferich's criterion and the abc-conjecture, J. Number Theory 30 (1988) 226–237.
[4] A. Wieferich, Zum letzten Fermatschen Theorem, J. Reine Angew. Math. 136 (1909) 293–302 (in German).