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

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

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

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

It is well known that Wieferich primes and the first case of Fermat’s last theorem are closely related [4]. For any positive integer $a$ with $a \geq 2$, 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...
just called a Wieferich prime. It seems that almost all primes are non-Wieferich primes. However, we cannot prove that non-Wieferich primes are infinite.

For $a \geq 2$ 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 $a \geq 2$ and $k \geq 2$, this result was extended to

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

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 $a \geq 2$ and $k \geq 2$. If one assumes the abc conjecture, then we have

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

**2. Some lemmas**

As usual, let $\Phi_n(x)$ denote the $n$-th cyclotomic polynomial. Let $a$, $k$ be fixed positive integers with $a \geq 2$ and $k \geq 2$. 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:

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

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 $\epsilon$ 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

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

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

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

$$\sum_{n \leq x} \frac{\varphi(nk)}{nk} = \sum_{n \leq x} \sum_{d | nk} \mu(d) \frac{nk}{d} \cdot \frac{1}{nk} = \sum_{n \leq x} \sum_{d | nk} \mu(d) \frac{1}{d}$$

$$= \sum_{d \leq x} \mu(d) \cdot \frac{1}{d} \sum_{n \leq x \text{ d divides n}} \frac{1}{d} = \sum_{d \leq x} \frac{\mu(d)}{d} \left[ \frac{x}{d/(d,k)} \right]$$

$$= x \sum_{d \leq x} \frac{\mu(d)(d,k)}{d^2} + O(\log x) = x \sum_{d=1}^{\infty} \frac{\mu(d)(d,k)}{d^2} + O(\log x)$$
\[ x \prod_p \left( 1 + \frac{\mu(p)(p,k)}{p^2} + \frac{\mu(p^2)(p^2,k)}{p^4} + \cdots \right) + O(\log x) \]

\[ = x \prod_p \left( 1 - \frac{(p,k)}{p^2} \right) + O(\log x). \]

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 \( L = \left\{ n : \varphi(nk) \geq \frac{2c(k)n}{3} nk \right\} \) 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

\[ C_{nk}' \gg a^{\varphi(nk) - \frac{c(k)n}{3}nk} > a^{\frac{c(k)n}{3}nk}. \]

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

\[ S(x) = \sum_{n \leq x} 1 \gg \sum_{n \geq n_0} \sum_{n \in L} 1 = \sum_{n \geq x} \sum_{n \geq n_0} 1. \]

Note that

\[ \sum_{n \leq x} \frac{\varphi(nk)}{nk} \leq \sum_{n \leq x} \frac{2c(k)n}{3} \leq \frac{2c(k)}{3} x. \]

Hence, by Lemma 2.5, we have

\[ S(x) \gg \sum_{n \leq x} \frac{\varphi(nk)}{nk} \leq \sum_{n \geq n_0} \sum_{n \in L} \frac{\varphi(nk)}{nk} \]

\[ = \sum_{n \leq x} \frac{\varphi(nk)}{nk} - \sum_{n \leq x} \frac{\varphi(nk)}{nk} \]

\[ \geq c(k)x + O(\log x) - \frac{2c(k)}{3} x \gg x. \]

**3. Proof of Theorem 1.1**

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

\[ a^{l_n^{-1}} \not\equiv 1 (\mod l_n^2) \]

by Lemma 2.2. Note that \( l_n \mid C_{nk}' \) and \( C_{nk}' \mid \Phi_{nk}(\alpha) \) and \( l_n \mid nk, \) we know that

\[ l_n \equiv 1 (\mod nk) \]

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

\[ a^{l_n^{-1}} \not\equiv 1 (\mod l_n^2), \ l_n \equiv 1 (\mod nk). \]

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

\[ \# \{ p : p \leq x, \ p \in \mathbb{P}, \ a^{p^{-1}} \not\equiv 1 (\mod p^2), \ p \equiv 1 (\mod k) \} \geq \# \{ n \in S, \ C_{nk}' \leq x \}. \]
Since $C'_{nk} \leq C_{nk} \leq a^{nk} - 1$, it is clear that

$$\#\{n : n \in S, C'_{nk} \leq x\} \geq \#\{n : n \in S, a^{nk} - 1 \leq x\}.$$

$$= \#\{n : n \in S, n \leq \frac{\log(x+1)}{k \log a}\}$$

$$= S\left(\frac{\log(x+1)}{k \log a}\right).$$

Hence, by Lemma 2.6, we have

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

Acknowledgement

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

References