On the Solutions of Certain Congruences

Sahar Siavashi

Department of Mathematics and Computer Science
University of Lethbridge

Alberta Number Theory Days IX
March 19, 2017

Wieferich primes

Definition

Let $a > 1$ be an integer. An odd prime p is called a *Wieferich prime* (in base a), if $a^{p-1} \equiv 1 \pmod{p^2}$.

Wieferich primes

Definition

Let $a > 1$ be an integer. An odd prime p is called a *Wieferich prime* (in base a), if $a^{p-1} \equiv 1 \pmod{p^2}$.

Notation

$$W_a(x) = \{p\ ;\ p \leq x \ \text{ and } \ a^{p-1} \equiv 1 \pmod{p^2}\}.$$

Wieferich primes

Definition

Let $a > 1$ be an integer. An odd prime p is called a *Wieferich prime* (in base a), if $a^{p-1} \equiv 1 \pmod{p^2}$.

Notation

$$W_a(x) = \{p \; ; \; p \leq x \text{ and } a^{p-1} \equiv 1 \pmod{p^2}\}.$$

It is conjectured that there are infinitely many Wieferich primes in any base.

Wieferich primes

Definition

Let $a > 1$ be an integer. An odd prime p is called a *Wieferich prime* (in base a), if $a^{p-1} \equiv 1 \pmod{p^2}$.

Notation

$$W_a(x) = \{p \; ; \; p \leq x \quad \text{and} \quad a^{p-1} \equiv 1 \pmod{p^2}\}.$$

It is conjectured that there are infinitely many Wieferich primes in any base.

Size of the set of Wieferich primes

A Heuristic

Assuming that Fermat's quotient $(a^{p-1}-1)/p$ are equally distributed in congruence classes mod p, we have

$$|W_a(x)| \approx \sum_{p \leq x} \frac{1}{p} \sim \log \log x,$$

as $x \to \infty$.

The abc-conjecture

The abc-conjecture

Notation

$\mathrm{rad}(n) = p_1 \cdots p_k$, where $n = p_1^{a_1} \cdots p_k^{a_k}$.

The abc-conjecture

Notation

$\mathrm{rad}(n) = p_1 \cdots p_k$, where $n = p_1^{a_1} \cdots p_k^{a_k}$.

Conjecture (Masser, 1985)

Let a, b, and c be such that $a + b = c$ and $(a, b, c) = 1$. Then, for $\epsilon > 0$, we have

$$\max\{|a|, |b|, |c|\} \ll_\epsilon \mathrm{rad}(abc)^{1+\epsilon}.$$

Non-Wieferich primes

Notation

$$W_a^c(x) = \{p\ ;\ p \leq x \ \text{ and } \ a^{p-1} \not\equiv 1 \pmod{p^2}\}.$$

Non-Wieferich primes

Notation

$$W_a^c(x) = \{p\ ;\ p \leq x \text{ and } a^{p-1} \not\equiv 1 \pmod{p^2}\}.$$

Theorem (Silverman, 1988)

Under the assumption of the *abc*-conjecture, we have

$$|W_a^c(x)| \gg_a \log x,$$

as $x \longrightarrow \infty$.

Non-Wieferich primes

Notation

Let $\lambda(n) = \frac{\log n}{\log(\text{rad } n)}$, for an integer n.

Non-Wieferich primes

Notation

Let $\lambda(n) = \frac{\log n}{\log(\text{rad } n)}$, for an integer n.

Theorem (De Koninck-Doyon, 2007)

Let $0 < \varepsilon < 1$ be a fixed number such the set

$$\{n \in \mathbb{N} \; ; \; \lambda(2^n - 1) < 2 - \varepsilon\}$$

has density 1. Then,

$$|W_2^c(x)| = |\{p \; ; \; p \leq x \text{ and } 2^{p-1} \not\equiv 1 \pmod{p^2}\}| \gg \log x,$$

as $x \to \infty$.

Non-Wieferich primes in arithmetic progressions

Notation

$$W^c_{a,k}(x) = \{p \ \leq x \ ; \ p \equiv 1 \pmod{k} \ \text{ and } \ a^{p-1} \not\equiv 1 \pmod{p^2}\}.$$

Non-Wieferich primes in arithmetic progressions

Notation

$$W^c_{a,k}(x) = \{p \ \leq x \ ; \ p \equiv 1 \pmod{k} \ \text{ and } \ a^{p-1} \not\equiv 1 \pmod{p^2}\}.$$

Theorem (Graves-Murty, 2013)

Let $k, a > 1$ be integers. Under the assumption of the *abc*-conjecture we have

$$|W^c_{a,k}(x)| \gg_{a,k} \frac{\log x}{\log\log x},$$

as $x \to \infty$.

An improvement of Graves-Murty result

Theorem (S., 2017)

Under the assumptions of *abc*-conjecture, we have

$$|W^c_{a,k}(x)| \gg_{a,k} \log x,$$

as $x \longrightarrow \infty$.

Cyclotomic polynomials

Definition

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} (x - e^{\frac{2k\pi i}{n}}).$$

Non-Wieferich primes in an arithmetic progressions

Conjecture

Let $a \geq 1$ be an integer and $\epsilon > 0$. Then, there exists an integer $n_0 = n_0(a, \epsilon)$, such that for $n \geq n_0$ we have

$$\lambda(|\Phi_n(a)|) < 2 - \epsilon.$$

Non-Wieferich primes in an arithmetic progressions

Conjecture

Let $a \geq 1$ be an integer and $\epsilon > 0$. Then, there exists an integer $n_0 = n_0(a, \epsilon)$, such that for $n \geq n_0$ we have

$$\lambda(|\Phi_n(a)|) < 2 - \epsilon.$$

Theorem (S., 2017)

Under the assumption of the above conjecture we have

$$|W^c_{a,k}(x)| \gg_a \log x.$$

Wieferich numbers

$q(a, m) = \frac{a^{\varphi(m)}-1}{m}$. (Euler quotient)

Wieferich numbers

$q(a, m) = \frac{a^{\varphi(m)}-1}{m}$. (Euler quotient)

Definition

An integer $m > 1$ is called a *Wieferich number in base a* if $q(a, m) \equiv 0 \pmod{m^2}$.

Wieferich numbers

Theorem (Banks-Luca-Shparlinski, 2007)

If W_2 is a finite set, then N_2 is also finite. Moreover, let

$$M = \prod_{p \leq w_0} (p-1),$$

where w_0 is the largest Wieferich prime in base 2. Then we have

$$\max N_2 \leq 2^{w_0 |W_2|} M.$$

The set S_a

The set S_a

Definition

- Let $S_a^{(0)} = W_a$.

The set S_a

Definition

- Let $S_a^{(0)} = W_a$.
- $S_a^{(i)} = \{p;\ p|q-1,\ \text{where } q \in S_a^{(i-1)}\}$, for $i \geq 1$.

The set S_a

Definition

- Let $S_a^{(0)} = W_a$.
- $S_a^{(i)} = \{p;\ p|q-1,\ \text{where } q \in S_a^{(i-1)}\}$, for $i \geq 1$.
- $S_a = \bigcup_{i=0}^{\infty} S_a^{(i)}$.

The set S_a

Definition

- Let $S_a^{(0)} = W_a$.
- $S_a^{(i)} = \{p;\ p | q-1,\ \text{where } q \in S_a^{(i-1)}\}$, for $i \geq 1$.
- $S_a = \bigcup_{i=0}^{\infty} S_a^{(i)}$.
- We call S_a *the set of primes generated by the set of primes in* W_a.

Largest known Wieferich number

Largest known Wieferich number

Notation

By $\nu_p(n)$ for an integer n we mean the largest power of p in n.

Largest known Wieferich number

Notation

By $\nu_p(n)$ for an integer n we mean the largest power of p in n.

Theorem (S., 2017)

If W_a is a finite set, then N_a is also finite. Moreover, we have

$$\max N_a = \prod_{p \in W_a} p^{\nu_p(M)+\nu_p(q(a,p))} \prod_{\substack{p \notin W_a \\ p \in S_a \\ p \nmid a}} p^{\nu_p(M)},$$

where $M = \prod_{\substack{p \in S_a \\ p \nmid a}} (p-1)$.

Generalization to number fields

Generalization to number fields

- Let K be a number field with the ring of integer $\mathfrak{O}_K$.

Generalization to number fields

- Let K be a number field with the ring of integer $\mathfrak{O}_K$.
- For an ideal $\mathfrak{a} \in \mathfrak{O}_K$ the norm is defined as

$$N(\mathfrak{a}) = \left|\mathfrak{O}_K/\mathfrak{a}\right|.$$

Generalization to number fields

- Let K be a number field with the ring of integer $\mathfrak{O}_K$.
- For an ideal $\mathfrak{a} \in \mathfrak{O}_K$ the norm is defined as

$$N(\mathfrak{a}) = |\mathfrak{O}_K/\mathfrak{a}|\,.$$

- Generalized Euler totient function is defined as follows.

$$\varphi(\mathfrak{a}) = N(\mathfrak{a}) \prod_{\mathfrak{p}|\mathfrak{a}} \left(1 - \frac{1}{N(\mathfrak{p})}\right),$$

where $\mathfrak{a}$ is an ideal $\in \mathfrak{O}_K$ and $\mathfrak{p}$ is a prime divisor of $\mathfrak{a}$.

Wieferich primes in number fields

Definition

We call $\pi \in \mathfrak{O}_K$ a *K-Wieferich prime in base* $\alpha \in \mathfrak{O}_K^*$ if $\pi \nmid \alpha$ and

$$\alpha^{N(\langle \pi \rangle)-1} \equiv 1 \pmod{\langle \pi^2 \rangle}.$$

Wieferich primes in number fields

Definition

We call $\pi \in \mathfrak{O}_K$ a *K-Wieferich prime in base* $\alpha \in \mathfrak{O}_K^*$ if $\pi \nmid \alpha$ and

$$\alpha^{N(\langle\pi\rangle)-1} \equiv 1 \pmod{\langle\pi^2\rangle}.$$

We write the above congruence for simplicity as

$$\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}.$$

Wieferich primes in number fields

Notation

$W_\alpha(K,x) = \{\pi \in \mathfrak{O}_K \ ; \ N(\pi) \leq x \text{ and } \alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}\}.$

Wieferich primes in number fields

Notation

$W_\alpha(K,x) = \{\pi \in \mathfrak{O}_K \ ; \ N(\pi) \leq x \text{ and } \alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}\}.$

Heuristically, $|W_\alpha(K,x)| \approx \sum_{N(\pi)\leq x} \frac{1}{N(\pi)}$ as $x \to \infty$.

Wieferich primes in number fields

Notation

$W_\alpha(K,x) = \{\pi \in \mathfrak{O}_K \ ; \ N(\pi) \leq x \text{ and } \alpha^{N(\pi)-1} \equiv 1 \pmod{\pi^2}\}$.

Heuristically, $|W_\alpha(K,x)| \approx \sum_{N(\pi)\leq x} \frac{1}{N(\pi)}$ as $x \to \infty$. Thus, if $\mathfrak{O}_K$ is a principal ideal domain, then

$$\sum_{N(\pi)\leq x} \frac{1}{N(\pi)} \sim \log\log x$$

as $x \to \infty$.

Non-Wieferich primes in number fields

Theorem (Kotyada-Muthukrishna,2016)

Let $K = \mathbb{Q}(\sqrt{m})$. Let $\varepsilon \in \mathfrak{O}_K$ be a unit such that $|\varepsilon| > 1$. Then under the assumption of the *abc*-conjecture for K, there are infinitely many non-K-Wieferich primes in base ε.

Wieferich primes and K-Wieferich primes

Theorem (S., 2017)

Let $K = \mathbb{Q}(\sqrt{m})$ with $h_K = 1$. Then the following assertions hold.
(i) Any prime of $\mathfrak{O}_K$ above a Wieferich prime p in an integer base a is a K-Wieferich prime in base a.

Wieferich primes and K-Wieferich primes

Theorem (S., 2017)

Let $K = \mathbb{Q}(\sqrt{m})$ with $h_K = 1$. Then the following assertions hold.
(i) Any prime of $\mathfrak{O}_K$ above a Wieferich prime p in an integer base a is a K-Wieferich prime in base a.
(ii) If π is a K-Wieferich prime in an integer base a above an split prime p, then p is a Wieferich prime in base a.

$\mathbb{Q}(i)$-Wieferich primes

Corollary

Let $K = \mathbb{Q}(i)$, and $a > 1$ be an integer. Assuming the abc-conjecture we have

$$|\{prime\ \pi \in \mathbb{Z}[i]\ ;\ N(\pi) \leq x \quad and \quad a^{N(\pi)-1} \not\equiv 1 \pmod{\pi^2}\}| \gg_a \log x.$$

Theorem

Let $k, a > 1$ be integers. Under the assumption of the *abc*-conjecture we have,

$$|W^c_{a,k}(x)| \gg_{a,k} \log x,$$

as $x \longrightarrow \infty$.

Thank You