ON WIEFERICH PRIMES

DENIS XAVIER CHARLES

ABSTRACT. A non-Wieferich prime is a prime p for which $2^{p-1} \not\equiv 1 \mod p^2$. We show that the problem of showing that there are infinitely many non–Wieferich primes is equivalent to proving lower bounds on the squarefree part of cyclotomic polynomials. This precisely identifies the difficulty in proving that the set of non–Wieferich primes is infinite.

1. Introduction

A theorem of Fermat says that $a^{p-1} \equiv 1 \mod p$ for every prime p and a relatively prime to p. A question that goes back to Abel is to find primes p for which $a^{p-1} \equiv 1 \mod p^2$ for some a relatively prime to p. Given $a \geq 2$ consider the two sets $\{p \mid a^{p-1} \equiv 1 \mod p^2, p \text{ a prime}\}$ and $\{p \mid a^{p-1} \not\equiv 1 \mod p^2, p \text{ a prime}\}$. It is still open whether each of these sets of primes is infinite. This is a frustrating situation given that we know that at least one of these sets must be infinite. Interest in these primes increased after Wieferich [Wie09] showed that if p is a prime for which $2^{p-1} \not\equiv 1 \mod p^2$, then the first case of Fermat's last theorem holds for exponent p. It is now known that up to 5×10^{14} the primes 1093 and 3511 are the only ones for which $2^{p-1} \equiv 1 \mod p^2$. In 1988, Silverman [Sil88] showed assuming the ABC-conjecture that there are infinitely many non-Wieferich primes. Silverman's approach was to use the ABC-conjecture to find cyclotomic polynomials with non-trivial squarefree part. In this article, we show that in some sense this the only way to prove there are infinitely many non-Wieferich primes. In the next section we formally state and prove our result. Our proof relies on a key lemma of Silverman.

2. Cyclotomic polynomials and Non-Wieferich primes

We fix the following notation. If n is a non-zero integer, set

$$\square(n) = \prod_{\mathrm{ord}_p(n)=1} p.$$

So that for any integer n if $p \mid (n/\square(n))$ then $p^2 \mid (n/\square(n))$.
Our main result is the following theorem:

Theorem 2.1. *Let*

$$W = \{p \mid 2^{p-1} \not\equiv 1 \mod p^2\}$$
$$C = \{m \mid \square(\phi_m(2)) > m\},$$

where $\phi_m(x)$ is the m-th cyclotomic polynomial. Then the set W is infinite if and only if the set C is infinite.

We need the following key lemma of Silverman ([Sil88] Lemma 3):

Lemma 2.2. *If p is an odd prime such that $p \not| n$ and suppose $p \mid \phi_n(2)$ and $p^2 \not| \phi_n(2)$. Then the order of 2 in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is exactly n and $2^{p-1} \not\equiv 1 \mod p^2$.*

Proof : Since $\phi_n(2) \equiv 0 \mod p$ and $\phi_n(2)$ divides $2^n - 1$ we have that $2^n - 1 \equiv 0 \mod p$. So the order of $2 \mod p$ is a divisor of n. We argue that the order is exactly n. Let $f(x) = x^n - 1 \in (\mathbb{Z}/p\mathbb{Z})[x]$. Now $f'(x) = nx^{n-1} \neq 0 \mod p$ (as $p \not| n$), and $\gcd(f(x), f'(x)) = 1$. So the polynomial $f(x) = \prod_{d|n} \phi_d(x)$ has

Date: 19 Nov 2002.

no repeated roots in the finite field $\mathbb{Z}/p\mathbb{Z}$. Hence $\phi_d(2) \not\equiv 0 \mod p$ for any proper divisor of n. Thus the order of 2 mod p is exactly n.

Now since p divides $\phi_n(2)$ only to the first power, we have $2^n \not\equiv 1 \mod p^2$. Thus $2^n = 1 + kp$ where k is not divisible by p. By the binomial theorem $2^{p-1} = (1+kp)^{\frac{p-1}{n}} = 1 + \frac{kp(p-1)}{n} \not\equiv 1 \mod p^2$. □

Now we can prove the main theorem.

Proof :(of Theorem 2.1) Suppose that the set W is infinite, we argue that C must be infinite.

Let $q \in W$. By definition we have $2^{q-1} \equiv 1 \mod q$ and $2^{q-1} \not\equiv 1 \mod q^2$. Then by the factorization of the polynomial $x^{q-1} - 1$ we get

$$2^{q-1} - 1 = \prod_{d|q-1} \phi_d(2).$$

Thus we get a d such that $\phi_d(2) \equiv 0 \mod q$ but $\phi_d(2) \not\equiv 0 \mod q^2$. Since d is a divisor of $q-1$ in particular we have $d < q$. Thus $\Box(\phi_d(2)) \geq q > d$. Now since $\phi_m(2) \leq 2^m - 1$ are bounded we get infinitely many integers m which are in C.

Conversely, assume that the set C is infinite. Let $m \in C$, then $\Box(\phi_m(2)) > m$, also $\phi_m(2)$ is odd. Since $\Box(\phi_m(2)) > m$ and squarefree, we can find an odd prime p that divides $\Box(\phi_m(2))$ and not m. Thus by Lemma 2.2 we get that p is a Wieferich prime. Suppose $q \mid \Box(\phi_m(2))$ and $q \mid \Box(\phi_{m'}(2))$ then m is the order of 2 mod q (by Lemma 2.2), but this is the same as m' which means $m = m'$. Thus we get infinitely many non-Wieferich primes and the set W is infinite. □

References

[Sil88] Silverman, J; *Wieferich's Criterion*, J. Number Theory, **30**, 226-237, (1988).

[Wie09] Wieferich, A.; *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math. **136**, 293-302, (1909).