involve

a journal of mathematics

An unresolved analogue of the Littlewood Conjecture

Clarice Ferolito

mathematical sciences publishers

2010 vol. 3, no. 2

INVOLVE 3:2(2010)

An unresolved analogue of the Littlewood Conjecture

Clarice Ferolito

(Communicated by Nigel Boston)

This article begins with an introduction to a conjecture made around 1930 in the area of Diophantine approximation: the Littlewood Conjecture. The conjecture asks whether any two real numbers can be simultaneously well approximated by rational numbers with the same denominator. The introduction also focuses briefly on an analogue of this conjecture, regarding power series and polynomials with coefficients in an infinite field. Harold Davenport and Donald Lewis disproved this analogue of the Littlewood Conjecture in 1963. Following the introduction we focus on a claim relating to another analogue of this conjecture. In 1970, John Armitage believed that he had disproved an analogue of the Littlewood Conjecture, regarding power series and polynomials with coefficients in a finite field. The remainder of this article shows that Armitage's claim was false.

1. Introduction

Through studying the results of John Littlewood and Godfrey Hardy on topics of Diophantine approximation, Littlewood's student Donald Spencer questioned whether any two real numbers can be approximated simultaneously by rational numbers with the same denominator. For some reason this conjecture was attributed to Littlewood and is known as *Littlewood's problem of Diophantine approximation* [Burkill 1979], or simply the *Littlewood Conjecture*.

To state it more formally, we fix some notation. As usual, $|n|$ denotes the absolute value of a number n. For x a real number, let $\|x\|$ denote the Euclidean distance of x to the nearest integer: $\|x\| = \inf_{a\in\mathbb{Z}} |x - a|$.

Conjecture 1.1 (Littlewood Conjecture). *For every θ, $\phi \in \mathbb{R}$ and for all $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that*

$$n \,\|n\theta\|\, \|n\phi\| < \varepsilon.$$

MSC2000: 11K60.

Keywords: Littlewood Conjecture, John Vernon Armitage.

No one has been able to prove this, in part because the method of continued fractions commonly used with approximations cannot be used for simultaneous approximations. The following definitions will aid in describing the analogue of the Littlewood Conjecture for power series and polynomials, which is easier to study than the original conjecture.

For any field K, let $K[t]$ denote the set of polynomials with coefficients in K. Define the norm of $N \in K[t]$ as $|N|_K = e^h$, where h is the degree of N. Series with coefficients in K, possibly infinitely many negative exponents, and finitely many positive exponents form the field $K((t^{-1}))$. For every $\Psi \in K((t^{-1}))$, define the norm of Ψ to be $\|\Psi\|_K = e^l$, where l is the greatest negative exponent of t. For example, if $K = \mathbb{R}$ and $\Psi(t) = 12t^{50} + 3t^9 + 2 + 5t^{-11} + 20t^{-99} + \cdots \in K((t^{-1}))$, then $\|\Psi(t)\|_K = e^{-11}$.

Conjecture 1.2 (Polynomial analogue of the Littlewood Conjecture). *Let K be a field and consider $\Theta, \Phi \in K((t^{-1}))$. For every $\varepsilon > 0$, there exists $N \in K[t]$ such that*

$$|N|_K \|N\Theta\|_K \|N\Phi\|_K < \varepsilon.$$

Davenport and Lewis [1963] proved that this analogue fails when K is an infinite field. Baker [1964] furthered this result by showing that $e^{1/t}$ and $e^{2/t} \in K((t^{-1}))$ serve as counterexamples to the analogue of the Littlewood Conjecture when K is the set of real numbers. With the analogue of the Littlewood Conjecture settled when K is an infinite field, the next problem to solve is the analogue with K a finite field.

2. Armitage's claim

Armitage [1970] published a corrigendum and addendum to his article from the previous year, entitled *An analogue of a problem of Littlewood* [Armitage 1969]. At first, it appeared that Armitage had disproved the analogue of the Littlewood Conjecture when K is a finite field of characteristic greater than or equal to 5. For many years, mathematicians accepted this claim. Armitage's proof appeared to imitate Baker's proof for his counterexample to the analogue of the Littlewood Conjecture with $K = \mathbb{R}$.

However, we found a parenthetical comment in [Adamczewski and Bugeaud 2007] that Armitage's counterexample does not hold, an observation these authors attribute to Bernard de Mathan. We also found a reference in [Larcher and Niederreiter 1993] that Yves Taussat, a student of Mathan, disproved Armitage's claim in his Ph.D. thesis [Taussat 1986]. However, in this paper, Taussat did not show why Armitage's counterexample fails. Below we provide a simplified wording of

Armitage's claim and in the next section we will show that his claim fails to disprove the analogue of the Littlewood Conjecture for K a finite field of characteristic $p \geq 5$.

Claim 2.1 [Armitage 1970]. *Let K be a field of characteristic $p > 3$. Define the norm of $N \in K[t]$ as $|N|_K = p^{\deg N}$, and the norm of $\Psi \in K((t^{-1}))$ as $\|\Psi\|_K = p^l$, where l is the greatest negative exponent of t in Ψ. Define $\Theta, \Phi \in K((t^{-1}))$ by*

$$\Theta(t) = (1+t^{-1})^{1/3}, \quad \Phi(t) = (1+t^{-1})^{2/3}.$$

Then for all nonzero $N \in K[t]$,

$$|N|_K \, \|N\Theta\|_K \, \|N\Phi\|_K \geq p^{-17}.$$

Note that Armitage uses p for the base of the norms rather than e, so his "lower bound", p^{-17}, for $|N|_K \, \|N\Theta\|_K \, \|N\Phi\|_K$ specifies the characteristic of K.

To show that Armitage's claim fails, we prove the following theorem.

Theorem 2.2. *Let K be a field of characteristic $p > 3$. Define $\Theta, \Phi \in K((t^{-1}))$ by*

$$\Theta = (1+t^{-1})^{1/3}, \quad \Phi = (1+t^{-1})^{2/3}.$$

Given any $\varepsilon > 0$, there exists a polynomial $N \in K[t]$ such that

$$|N|_K \, \|N\Theta\|_K \, \|N\Phi\|_K < \varepsilon.$$

The proof is divided into two cases, depending on the residue of p modulo 3.

3. Preliminary lemmas

Lemma 3.1. *For any prime p congruent to 2 modulo 3 and not equal to 2, the coefficient of t^{-n} in the expansion of $(1+t^{-1})^{1/3}$ is congruent to 0 modulo p if $(p^3+1)/3 < n < p^3$.*

Proof of Lemma 3.1. Consider the number of factors of p in the numerator of the coefficient of t^{-n} in $\Theta = (1+t^{-1})^{1/3}$. By the binomial theorem, this coefficient is

$$\binom{\frac{1}{3}}{n} = \frac{(-1)^{n-1}\big(1(3\cdot 1-1)(3\cdot 2-1)\cdots(3(n-1)-1)\big)}{3^n\, n!}.$$

Thus, the last term in the numerator of the coefficient of t^{-n} is $3n-4$. Since 3 always has a multiplicative inverse modulo p, we have

$$3l-1 \equiv 3m-1 \pmod{p} \iff l \equiv m \pmod{p}.$$

Moreover, the greatest common divisor of 3 and p^2 is 1 for any $p \neq 3$, so

$$3l-1 \equiv 3m-1 \pmod{p^2} \iff l \equiv m \pmod{p^2}.$$

Since $3l-1 \equiv 3m-1 \pmod{p} \Longleftrightarrow l \equiv m \pmod{p}$, p divides at least $\lfloor n/p \rfloor$ terms in the numerator of the coefficient of t^{-n}. Similarly, because

$$3l-1 \equiv 3m-1 \pmod{p^2} \iff l \equiv m \pmod{p^2},$$

p^2 divides at least $\lfloor n/p^2 \rfloor$ terms.

Since $p \equiv 2 \pmod{3}$, p^3 will divide a term in the numerator of a coefficient if and only if for some $r \in \mathbb{Z}^+$ $(0 \le r \le n-1)$ there exists $s \in \mathbb{Z}$ such that $3r-1 = sp^3$. In other words, $r = (sp^3+1)/3$ must be a positive integer. Thus, such an s must satisfy $s \equiv 1 \pmod{3}$. We are only considering $n \le p^3-1$ and $r = (sp^3+1)/3 \le n-1$, so $(sp^3+1)/3 \le p^3-2$. Thus, sp^3 will divide a numerator in the coefficient of t^{-n} for $n \le p^3-1$ if and only if $s \le (3p^3-7)/p^3 < 3$ and $s \equiv 1 \pmod{3}$. In other words, the only term that could be divisible by p^3 in the numerator of the coefficient of t^{-n} for $n \le p^3-1$ is p^3 itself. The final term in the numerator of the coefficient of $t^{-(p^3+4)/3}$ is $3((p^3+4)/3-1)-1 = p^3$. Thus, the first time that p^3 appears in the numerator of a coefficient of t^{-n} is actually when $n = (p^3+4)/3$. So, for each $(p^3+4)/3 \le n \le p^3-1$, the numerator of the coefficient of t^{-n} has exactly one term that is divisible by p^3. This and the preceding paragraph show that for each $(p^3+4)/3 \le n \le p^3-1$, the numerator of the coefficient of t^{-n} has at least $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + 1$ factors of p.

Now looking at the denominator of the coefficient of t^{-n} for $(p^3+4)/3 \le n \le p^3-1$, the only powers of p that divide $n!$ are p and p^2. So there are only $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor$ factors of p in the denominator of t^{-n} for $(p^3+4)/3 \le n \le p^3-1$.

Therefore, for any $(p^3+4)/3 \le n \le p^3-1$, the numerator of the coefficient of t^{-n} will have at least one more factor of p than the denominator and the coefficient will be congruent to zero modulo p. □

The proof of the next lemma is similar to that of Lemma 3.1.

Lemma 3.2. *For any prime p congruent to* 1 *modulo* 3, *the coefficient of t^{-n} in the expansion of $(1+t^{-1})^{2/3}$ is congruent to zero modulo p if $(p^2+2)/3 < n < p^2$.*

Lemma 3.3. *For any prime $p > 3$ and any even positive integer b, there exists an integer $a < 0$ such that $\frac{1}{3} = a + p^b \cdot \frac{1}{3}$.*

Proof of Lemma 3.3. We have

$$\tfrac{1}{3} = a + p^b \cdot \tfrac{1}{3} \iff a = (1-p^b)/3 \in \mathbb{Z} \iff p^b \equiv 1 \pmod{3}.$$

For any $p > 3$, $p \equiv 1 \pmod{3}$ or $p \equiv 2 \pmod{3}$. Obviously, $1^2 \equiv 1 \pmod{3}$, but also $2^2 \equiv 1 \pmod{3}$. Thus, for any prime $p > 3$, $p^2 \equiv 1 \pmod{3}$. This further implies that $p^{2k} = (p^2)^k \equiv 1^k \equiv 1 \pmod{3}$ for any $k \in \mathbb{N}$. Therefore, we have shown that for any even integer b, $p^b \equiv 1 \pmod{3}$. □

The proof of the following lemma is analogous to that of Lemma 3.3.

Lemma 3.4. *For any prime $p > 3$ and any even positive integer b, there exists an integer $a < 0$ such that $\frac{2}{3} = a + p^b \cdot \frac{2}{3}$.*

4. Proof of Theorem 2.2

By assumption, the characteristic of K is $p > 3$.

First case: $p \equiv 2 \pmod 3$. By Lemma 3.3, for b an even positive integer, there exists a negative integer a such that $(1+t^{-1})^{1/3} = (1+t^{-1})^{a+p^b/3}$. Multiplying both sides by $(1+t^{-1})^{-a}$, yields $(1+t^{-1})^{-a}\,(1+t^{-1})^{1/3} = (1+t^{-1})^{p^b/3}$. Since we are working in a field with characteristic p, $(1+t^{-1})^{p^b/3} = (1+t^{-p^b})^{1/3}$, and therefore

$$(1+t^{-1})^{-a}\,(1+t^{-1})^{1/3} = (1+t^{-p^b})^{1/3}.$$

Multiplying both sides by t^{-a} results in

$$(1+t)^{-a}\,(1+t^{-1})^{1/3} = t^{-a}(1+t^{-p^b})^{1/3}.$$

Now applying Lemma 3.1, we know that the coefficient of t^{-i} in $t^{-a}(1+t^{-p^b})^{1/3}$ is congruent to zero modulo p for each i with $a+((p^3+1)/3)p^b < i < a+(p^3)p^b$. Multiplying

$$(1+t)^{-a}\,(1+t^{-1})^{1/3} = t^{-a}(1+t^{-p^b})^{1/3}$$

by $t^{a+((p^3+1)/3)p^b}$, we have

$$t^{a+((p^3+1)/3)p^b}(1+t)^{-a}\,(1+t^{-1})^{1/3} = q(t) + c\,t^{p^b((-2p^3+1)/3)} + \cdots,$$

where $q(t) \in K[t]$ and $c \not\equiv 0 \pmod p$.

Let N be the polynomial

$$N(t) = t^{a+((p^3+1)/3)p^b}(1+t)^{-a}.$$

Then by the definitions for the norm of a polynomial and the norm of a power series,

$$|N| = p^{((p^3+1)/3)p^b} \quad \text{and} \quad \|N\Theta\| = p^{\,p^b((-2p^3+1)/3)}.$$

Therefore

$$|N|\,\|N\Theta\| = p^{\,p^b((2-p^3)/3)}.$$

For any $\varepsilon > 0$, choosing an even positive integer b such that

$$b > \log_p\left|\frac{\log_p(\varepsilon)}{((2-p^3)/3)}\right|$$

implies that $|N|\,\|N\Theta\| < \varepsilon$.

Second case: $p \equiv 1 \pmod 3$. A similar method of proof works in this case, if we choose as the approximating polynomial

$$N = t^{a+((p^2+2)/3)p^b}(1+t)^{-a},$$

with b an even positive integer such that

$$b > \log_p \left| \frac{\log_p(\varepsilon)}{((4-p^2)/3)} \right|.$$

Since $\|N\Psi\| \le p^0$ for any $\Psi \in K((t^{-1}))$, together these cases show that Theorem 2.2 holds with the approximating polynomial N chosen as above depending on the characteristic of the finite field. □

Thus, Armitage's counterexample does not settle the analogue of the Littlewood Conjecture when K is a finite field of characteristic $p \ge 5$.

References

[Adamczewski and Bugeaud 2007] B. Adamczewski and Y. Bugeaud, "On the Littlewood conjecture in fields of power series", pp. 1–20 in *Probability and Number Theory* (Kanazawa, 2005), edited by S. Akiyama et al., Adv. Stud. Pure Math. **49**, Math. Soc. Japan, Tokyo, 2007. MR 2009e:11130 Zbl 05286791

[Armitage 1969] J. V. Armitage, "An analogue of a problem of Littlewood", *Mathematika* **16** (1969), 101–105. MR 42 #1768a Zbl 0188.35002

[Armitage 1970] J. V. Armitage, "Corrigendum and addendum: "An analogue of a problem of Littlewood".", *Mathematika* **17** (1970), 173–178. MR 42 #1768b

[Baker 1964] A. Baker, "On an analogue of Littlewood's Diophantine approximation problem", *Michigan Math. J.* **11** (1964), 247–250. MR 29 #2218 Zbl 0218.10052

[Burkill 1979] J. C. Burkill, "John Edensor Littlewood", *Bull. London Math. Soc.* **11**:1 (1979), 59–103. MR 80h:01027 Zbl 0409.01010

[Davenport and Lewis 1963] H. Davenport and D. J. Lewis, "An analogue of a problem of Littlewood", *Michigan Math. J.* **10** (1963), 157–160. MR 27 #4794 Zbl 0107.04202

[Larcher and Niederreiter 1993] G. Larcher and H. Niederreiter, "Kronecker-type sequences and non-Archimedean Diophantine approximations", *Acta Arith.* **63**:4 (1993), 379–396. MR 94c:11063

[Taussat 1986] Y. Taussat, *Approximation diophantienne dans un corps de séries formelles*, Ph.D. thesis, Université de Bordeaux, 1986.

Received: 2009-09-02 Revised: 2010-04-05 Accepted: 2010-06-02

cefero09@gmail.com *College of the Holy Cross, 355 California Street, Newton, MA 02548, United States*

involve

pjm.math.berkeley.edu/involve

See inside back cover or http://pjm.math.berkeley.edu/involve for submission instructions.

The subscription price for 2010 is US $100/year for the electronic version, and $120/year (+$20 shipping outside the US) for print and electronic. Subscriptions, requests for back issues from the last three years and changes of subscribers address should be sent to Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94704-3840, USA.

Involve (ISSN 1944-4184 electronic, 1944-4176 printed) at Mathematical Sciences Publishers, Department of Mathematics, University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

Involve peer review and production are managed by EditFLOW™ from Mathematical Sciences Publishers.

PUBLISHED BY

mathematical sciences publishers

http://www.mathscipub.org

A NON-PROFIT CORPORATION

Typeset in LaTeX

involve

2010 vol. 3 no. 2

Recursive sequences and polynomial congruences 129
J. Larry Lehman and Christopher Triola

The Gram determinant for plane curves 149
Józef H. Przytycki and Xiaoqi Zhu

The cardinality of the value sets modulo n of $x^2 + x^{-2}$ and $x^2 + y^2$ 171
Sara Hanrahan and Mizan Khan

Minimal k-rankings for prism graphs 183
Juan Ortiz, Andrew Zemke, Hala King, Darren Narayan and Mirko Horňák

An unresolved analogue of the Littlewood Conjecture 191
Clarice Ferolito

Mapping the discrete logarithm 197
Daniel Cloutier and Joshua Holden

Linear dependency for the difference in exponential regression 215
Indika Sathish and Diawara Norou

The probability of relatively prime polynomials in $\mathbb{Z}_{p^k}[x]$ 223
Thomas R. Hagedorn and Jeffrey Hatley

$\mathbb{G}$-planar abelian groups 233
Andrea DeWitt, Jillian Hamilton, Alys Rodriguez and Jennifer Daniel

1944-4176(2010)3:2;1-F