THE ABC-CONJECTURE AND THE POWERFUL NUMBERS IN LUCAS SEQUENCES

Minoru Yabuta
Senri High School, 17-1, 2-chome, Takanodai, Suita, Osaka, 565-0861, Japan
e-mail: yabutam@senri.osaka-c.ed.jp

(Submitted August 2007 - Final Revision September 2007)

ABSTRACT

P. Ribenboim and G. Walsh showed that if the ABC-conjecture is true then every Lucas sequence has only finitely many powerful terms in the case of positive discriminant. We extend this result into the case of negative discriminant.

1. INTRODUCTION

We consider two sequences $\{U_n\}_{n\geq 0}$ and $\{V_n\}_{n\geq 0}$ defined by the recursion relations:

$$U_0 = 0,\ U_1 = 1,\ U_{n+2} = PU_{n+1} - QU_n, \tag{1}$$

$$V_0 = 2,\ V_1 = P,\ V_{n+2} = PV_{n+1} - QV_n, \tag{2}$$

where P and Q are non-zero integers such that $D = P^2 - 4Q \neq 0$ and $\gcd(P, Q) = 1$. Each U_n is called the *Lucas number*, which is an integer. A Lucas sequence $\{U_n\}_{n\geq 0}$ is called *degenerate* if the quotient of the roots of the polynomial $X^2 - PX + Q$ is a root of unity and *non-degenerate*, otherwise. Throughout this paper we assume that $\{U_n\}_{n\geq 0}$ and $\{V_n\}_{n\geq 0}$ are non-degenerate. An integer n is *powerful* if p^2 divides n whenever a prime p divides n.

In 1999, Ribenboim and Walsh [6] proved that the following conjecture of Masser and Oesterlé implies that if $P > 0$ and $Q \neq 0$ are integers such that $D = P^2 - 4Q > 0$ and $\gcd(P, Q) = 1$ then U_n and V_n are powerful for only finitely many terms.

ABC-conjecture (Masser and Oesterlé). Let a, b, c be relatively prime integers satisfying $a + b + c = 0$. Then, for every $\epsilon > 0$,

$$\max\{|a|, |b|, |c|\} \ll_\epsilon \left(\prod_{p|abc} p\right)^{1+\epsilon}, \tag{3}$$

where the product is over all primes dividing abc. We use the Vinogradov symbols $\gg_\epsilon$ and $\ll_\epsilon$ with their usual meanings. The constant depends only on ϵ, independent of a, b, c.

In this paper we will extend the result of Ribenboim and Walsh [6] into the case of negative discriminant. In other words, we will show that even if $D = P^2 - 4Q < 0$ the ABC-conjecture implies that U_n and V_n are powerful for only finitely many terms.

The problem of the powerful numbers in Lucas sequences has been studied by several authors. In 1964, Cohn [3] proved that the only squares in the Fibonacci sequence $\{F_n\}_{n\geq 0}$ are $F_0 = 0$, $F_1 = F_2 = 1$ and $F_{12} = 144$. In 1969, London and Finkelstein [4] proved that the only cubes in the Fibonacci sequence are $F_0 = 0$, $F_1 = F_2 = 1$ and $F_6 = 8$. In 1996, Ribenboim and McDaniel [5] proved that if P and Q are odd numbers such that $D = P^2 - 4Q > 0$ and $\gcd(P, Q) = 1$, then U_n is a perfect square only if $n = 0, 1, 2, 3, 6, 12$, and V_n is a perfect square only if $n = 1, 3, 5$. Recently, Bugeaud, Mignotte and Siksek [2] showed that the only perfect powers in the Fibonacci sequence are F_0, F_1, F_2, F_6 and F_{12}.

2. THE POWERFUL NUMBERS IN LUCAS SEQUENCES

Let P and Q be non-zero integers such that $D = P^2 - 4Q \neq 0$ and $\gcd(P, Q) = 1$. Let α and β be the roots of the polynomial $X^2 - PX + Q$. Then, for all integers $n \geq 0$,

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \quad V_n = \alpha^n + \beta^n. \tag{4}$$

We assume that the sequences $\{U_n\}_{n\geq 0}$ and $\{V_n\}_{n\geq 0}$ are non-degenerate. Since $D = (\alpha - \beta)^2$ and $\alpha\beta = Q$, we have that for all $n \geq 0$,

$$V_n^2 - DU_n^2 = 4Q^n. \tag{5}$$

Lemma 2.1: For all integers $n \geq 1$,

(1) $\gcd(U_n, Q) = \gcd(V_n, Q) = 1$ (2) $\gcd(U_n, V_n) = 1$ or 2.

Proof: Let p be an arbitrary prime dividing Q. Then from (1) and (2), we have that $U_n \equiv P^{n-1}$ and $V_n \equiv P^n \pmod{p}$. Since P and Q are relatively prime, $U_n \not\equiv 0$ and $V_n \not\equiv 0 \pmod{p}$. Hence, $\gcd(U_n, Q) = \gcd(V_n, Q) = 1$. Then from (5) we have that $\gcd(U_n, V_n) =$ 1 or 2. □

If N is an integer then we can write $N = uv$ with $\gcd(u, v) = 1$, where u is a squarefree integer and v is a powerful integer. Then u is called the *powerless part* and v the *powerful part.*

Lemma 2.2: Let C be an arbitrary positive number. Then

$$\sharp\{n \in \mathbb{N} : U_n \text{ is powerful and } U_n \leq C\} < \infty.$$

Proof: The proof is by contradiction. In [1] we find that if $n > 30$ then U_n has a primitive divisor, which divides U_n but does not divide U_k for $0 < k < n$. Assume that there are infinitely many powerful terms U_n with $U_n \leq C$. Then $U_l = U_m$ for some integers $30 < l < m$, which contradicts that U_m has a primitive divisor. Thus, we have completed the proof. □

Theorem 2.3: The ABC-conjecture implies that if P and Q are nonzero integers such that $D = P^2 - 4Q \neq 0$ and $\gcd(P, Q) = 1$ then U_n and V_n are powerful for only finitely many terms.

Proof: We will prove this theorem for the sequence $\{U_n\}_{n\geq 0}$. In a similar way, we can prove this theorem for the sequence $\{V_n\}_{n\geq 0}$. We distinguish the proof into two cases, depending on whether $\gcd(U_n, V_n)$ is equal to 1 or 2. We omit the proof for the second case, which is similar to that for the first case.

Now define $N_1 = \{n \geq 1 : \gcd(U_n, V_n) = 1\}$. According to Ribenboim and Walsh [5], for $n \in N_1$ define

$$\begin{cases} Z_n = V_n/2,\ \Delta = D/4,\ E = 1 & \text{for } P \text{ even} \\ Z_n = V_n,\ \Delta = D,\ E = 4 & \text{for } P \text{ odd.} \end{cases}$$

Then

$$Z_n^2 - \Delta U_n^2 = EQ^n, \tag{6}$$

and in both cases $\gcd(Z_n, \Delta U_n, EQ^n) = 1$. We write $U_n = u_n v_n$ with $\gcd(u_n, v_n) = 1$ and $v_n > 0$, where u_n is the powerless part and v_n is the powerful part. Applying the ABC-conjecture to (6), we obtain that there exists a constant κ depending only on ϵ such that

$$\begin{aligned} \max\{|Z_n^2|, |\Delta U_n^2|, |EQ^n|\} &\leq \kappa \left(\prod_{p | Z_n \Delta U_n EQ} p \right)^{1+\epsilon} \\ &\leq \kappa |Z_n \Delta E Q u_n \sqrt{v_n}|^{1+\epsilon}. \end{aligned} \tag{7}$$

Now

$$|Z_n^2| = |\Delta U_n^2 + EQ^n| \leq 2 \max\{|\Delta U_n^2|, |EQ^n|\},$$

so

$$|Z_n| \leq \sqrt{2} \max\{|\Delta U_n^2|, |EQ^n|\}^{1/2}.$$

Substituting this into (7), we have that

$$\max\{|\Delta U_n^2|, |EQ^n|\} \ll_\epsilon \max\{|\Delta U_n^2|^{1/2} |u_n \sqrt{v_n}|,\ |EQ^n|^{1/2} |u_n \sqrt{v_n}|\}^{1+\epsilon},$$

and therefore,

$$\max\{|\Delta U_n^2|, |EQ^n|\}^{(1-\epsilon)/2} \ll_\epsilon |u_n \sqrt{v_n}|^{1+\epsilon}.$$

Hence

$$|\Delta U_n^2|^{(1-\epsilon)/2} \ll_\epsilon |u_n \sqrt{v_n}|^{1+\epsilon}. \tag{8}$$

Now fix $0 < \epsilon < 1/3$. Substituting $U_n = u_n v_n$ into (8), we obtain that for all $n \in N_1$,

$$u_n^{2\epsilon} \gg_\epsilon v_n^{(1-3\epsilon)/2}. \tag{9}$$

This means that there exists a constant $C > 0$ independent of n, so that if $v_n > C$ then $|u_n| > 1$. In other words, the terms U_n with $v_n > C$ is not powerful for any integer $n \in N_1$. From Lemma 2.2 we have further that the term U_n with $v_n \leq C$ is powerful for only finitely many integers $n \in N_1$. It follows that the term U_n is powerful for only finitely many integers $n \in N_1$. We conclude that the term U_n is powerful for only finitely many integers $n \geq 1$. □

Now let $\tilde{E} : y^2 = x^3 + B$ with $B \in \mathbb{Z}$ be an elliptic curve and let $\tilde{P}$ be any rational point of infinite order on the curve $\tilde{E}$. For every integer $n \geq 1$ write $n\tilde{P} = (a_n/d_n^2, b_n/d_n^3)$. Let $\tilde{v}_n$ be the powerful part of d_n. Then Silverman [7] showed that the ABC-conjecture implies $\tilde{v}_n \ll_{\epsilon, \tilde{E}} d_n^\epsilon$. In the proof of Theorem 2.3 we made reference to [7].

ACKNOWLEDGMENTS

The author would like to express his gratitude to the anonymous referee for many useful and valuable suggestions that improved this paper. In particular, the proof of Theorem 2.3 was improved by the referee's suggestion.

REFERENCES

[1] Yu. Bilu, G. Hanrot, P. Voutier (with an appendix by M. Mignotte). "Existence of Primitive Divisors of Lucas and Lehmer Numbers." *J. Reine Angew. Math.* **539** (2001): 75–122.

[2] Y. Bugeaud, M. Mignotte, S. Siksek. "Classical and Modular Approaches to Exponential Diophantine Equations. Fibonacci and Lucas Perfect Powers." *Ann. of Math.* **163.3** (2006): 969–1018.

[3] J. H. E. Cohn. "On Square Fibonacci Numbers." *Proc. London Math. Soc.* **39** (1964): 537–541.

[4] H. London, R. Finkelstein. "On Fibonacci and Lucas Numbers Which are Perfect Powers." *Fibonacci Quart.* **7.5** (1969): 476–481, 487; errata, ibid. **8.3** (1970): 248.

[5] P. Ribenboim and W. L. McDaniel. "The Square Terms in Lucas Sequences." *J. Number Theory* **58** (1996): 104–123.

[6] P. Ribenboim and G. Walsh. "The ABC Conjecture and the Powerful Part of Terms in Binary Recurring Sequences." *J. Number Theory* **74** (1999): 134–147.

[7] J. H. Silverman. "Wieferich's Criterion and the ABC-Conjecture." *J. Number Theory* **30** (1988): 226–237.

AMS Classification Numbers: 11B39, 11D09

✠ ✠ ✠