Publ. Math. Debrecen
59 / 3-4 (2001), 459–469

On square factors of terms of binary recurring sequences and the *ABC* Conjecture

By PAULO RIBENBOIM (Kingston)

Abstract. Assuming that the (ABC) Conjecture is true, we prove that for each binary recurring sequence with terms U_n, there exist infinitely many primes p such that p^2 does not divide $U_{p-\left(\frac{D}{p}\right)}$. This generalizes the result of Silverman about the incongruence of Wieferich $a^{p-1} \not\equiv 1 \pmod{p^2}$.

§ 1. Introduction

By Fermat's little theorem, if $a > 1$ and p is a prime number not dividing a, then $a^{p-1} \equiv 1 \pmod{p}$. If $a^{p-1} \equiv 1 \pmod{p^2}$ we say that *p satisfies the congruence of Wieferich* for the basis a. This congruence has first appeared in a theorem of Wieferich concerning Fermat's last theorem (see Ribenboim [9]). Due to the work of Inkeri [5], Aaltonen and Inkeri [1], and more recently of Mihăilescu [6], [7] the study of this congruence has become relevant in connection with Catalan's conjecture. Very few examples of primes satisfying the congruence of Wieferich are known, despite extensive calculations. For base 2, the only known primes p satisfying the congruence are 1093 and 3511 (the search was done for $p < 4 \times 10^{12}$ in [2] and continued to $p < 42 \times 10^{12}$ by R. Brown and R. McIntosh, unpublished). Therefore in most computed cases the incongruence of Wieferich $a^{p-1} \not\equiv 1 \pmod{p^2}$ holds. Nevertheless the following statement has never been proved:

Mathematics Subject Classification: 11B37, 11D61, 11A07.
Key words and phrases: *ABC* conjecture, wieferich congruence, binary recurring sequence, powerful numbers.

1.1. For each basis $a \geq 2$ there exist infinitely many primes p such that $a^{p-1} \not\equiv 1 \pmod{p^2}$.

In [17] Silverman proved:

1.2. If the (ABC) Conjecture is true then the statement 1.1 is also true.

In [14] we gave a different and simpler proof of 1.2.

For more information about Wieferich's congruence the reader may consult [10], [11].

For each integer $a \geq 2$ the numbers $a^n - 1$ (for $n \geq 0$) are the terms of a binary recurring sequence. Our purpose in this paper is to extend the concept of Wieferich congruence and incongruence to binary recurring sequences, to formulate the analogue of 1.1 and to prove the result corresponding to 1.2.

§2. Preliminaries and requisite results

A. Binary recurring sequences

Let $P > 0$, $Q \neq 0$ be integers such that $\gcd(P, Q) = 1$ and $D = P^2 - 4Q \neq 0$. Let $U_0 = 0$, $U_1 = 1$, $V_0 = 2$, $V_1 = P$ and for all $n \geq 2$ let

$$U_n = PU_{n-1} - QU_{n-2}$$
$$V_n = PV_{n-1} - QV_{n-2}.$$

$\mathcal{U} = \mathcal{U}(P, Q) = (U_n)_{n\geq 0}$ and $\mathcal{V} = \mathcal{V}(P, Q) = (V_n)_{n\geq 0}$ are the *binary recurring sequences of first kind* (respectively *of second kind*) *with parameters* (P, Q). If $\alpha = \frac{P+\sqrt{D}}{2}$, $\beta \frac{P-\sqrt{D}}{2}$ then α, β are the roots of $X^2 - PX + Q = 0$. Below we list well-known facts about these sequences which will be required in this paper. For details, see [11] or [15].

2.1. For all $n \geq 0$:

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

2.2. For all $n \geq 0$:

$$V_n^2 - DU_n^2 = 4Q^n.$$

2.3. If $1 \leq m < n$ then $U_m \mid U_n$ if and only if $m \mid n$.

2.4. If $1 < m < n$ then $V_m \mid V_n$ if and only if $m \mid n$ and $\frac{n}{m}$ is odd.

Let $d = \gcd(m, n)$. Then we have:

2.5. $$\gcd(U_m, U_n) = U_d.$$

2.6. $$\gcd(V_m, V_n) = \begin{cases} V_d \text{ when } \dfrac{m}{d}, \dfrac{n}{d} \text{ are odd,} \\ 1 \text{ or } 2 \text{ otherwise.} \end{cases}$$

2.7. $$\gcd(U_m, V_n) = \begin{cases} V_d \text{ when } \dfrac{m}{d} \text{ is even so } \dfrac{n}{d} \text{ is odd,} \\ 1 \text{ or } 2 \text{ otherwise} \end{cases}$$

2.8. $$\gcd(U_m, Q) = \gcd(V_m, Q) = 1$$

for all $m \geq 1$, $\gcd(D, Q) = 1$.

2.9. $$\begin{aligned} U_{2m} &= U_m V_m, \\ V_{2m} &= V_m^2 - 2Q^m \end{aligned} \qquad \text{for all } m \geq 0.$$

2.10. If $r \geq 1$, $m \geq 1$ and m is odd then $U_{rm} = U_r Z$ where

$$\begin{aligned} Z = {} & D^{\frac{m-1}{2}} U_r^{m-1} + \frac{m}{1} Q^r D^{\frac{n-3}{2}} U_r^{m-3} + \frac{m}{2} \binom{m-3}{1} Q^{2r} D^{\frac{m-5}{2}} U_r^{m-5} \\ & + \cdots + \frac{m}{i} \binom{m-i-1}{i-1} Q^{ir} D^{\frac{m-2i-1}{2}} U_r^{m-2i-1} + \cdots + m Q^{\frac{m-1}{2} r}. \end{aligned}$$

2.11. If $r \geq 1$, $m \geq 1$ and m is odd, then $V_{mr} = V_r T$ where

$$\begin{aligned} T = {} & V_r^{m-1} - \frac{m}{1} Q^r V_r^{m-3} + \frac{m}{2} \binom{m-3}{1} Q^{2r} V_r^{m-5} - \cdots \\ & \cdots + (-1)^i \frac{m}{i} \binom{m-i-1}{i-1} Q^{ir} V_r^{m-2i-1} \pm \cdots + (-1)^{\frac{m-1}{2}} m Q^{\frac{m-1}{2} r}. \end{aligned}$$

We write $p \mid \mathcal{U}$, respectely $p \mid \mathcal{V}$ and we say that the prime p divides the sequence $\mathcal{U}$, respectively $\mathcal{V}$, if there exists $n \geq 1$ such that $p \mid U_n$, respectively $p \mid V_n$. In this situation there exists the smallest such index, which is denoted by $r = r(p)$ for the sequence $\mathcal{U}$, and denoted by $s = s(p)$

for the sequence $\mathcal{V}$. The index $r(p)$, respectively $s(p)$ is called the *rank of appearance of* p in $\mathcal{U}$, respectively in $\mathcal{V}$. Then $p \mid U_n$ if and only if $r(p) \mid n$, while $p \mid V_n$ if and only if $s(p) \mid n$ and $\frac{n}{s(p)}$ is odd.

For the sequences $\mathcal{U}$ and $\mathcal{V}$ we have the following results about the rank of appearance:

2.12. If P is even and Q is odd then $r(2) = 2$ and $s(2) = 1$. If P is odd and Q is even then 2 does not divide $\mathcal{U}$, nor $\mathcal{V}$. If P and Q are both odd, then $r(2) = 3$ and $s(2) = 3$.

2.13. Let p be an odd prime. If $p \mid P$ but $p \nmid Q$ then $r(p) = 2$. If $p \nmid P$ but $p \mid Q$ then p does not divide $\mathcal{U}$. If $p \nmid PQ$ but $p \mid D$ then $r(p) = p$. Finally, if $p \nmid PQD$ then $r(p) \mid \left(p - \left(\frac{D}{p}\right)\right)$, where $\left(\frac{D}{p}\right)$ is the Legendre symbol.

For $p > 2$, no analogous fully satisfactory result is valid for the sequence $\mathcal{V}$ (see [11] or [15]).

The following lemma, proved in [12] will be needed; the proof below is simpler and it is included for the convenience of the reader.

Lemma 2.14. *For $r \geq 1$ and $m \geq 1$, $U_{rm} = U_r Z$, where* $\gcd(U_r, Z)$ *divides m.*

Proof. If m is odd, by 2.10 $U_{rm} = U_r Z$ and $\gcd(U_r, Z)$ divides m. Now let $m = 2^e n$, where $e \geq 1$ and n is odd. Then

$$U_{rm} = U_{nr} V_{nr} V_{2nr} \dots V_{2^{e-1}nr}.$$

Since n is odd we have $U_{nr} = U_r Z_0$ with $\gcd(U_r, Z_0)$ dividing n. Let $Z = Z_0 V_{nr} V_{2nr} \dots V_{2^{e-1}nr}$. Then $U_{rm} = U_r Z$. Since $\gcd(U_r, V_{2^i nr}) = 1$ or 2 (for $i = 0, 1, \dots, e-1$). Then $\gcd(U_r, Z)$ divides $2^e n = m$. □

For the sequence $\mathcal{V}$ we also have:

Lemma 2.15. *If $r \geq 1$, $m \geq 1$ and m is odd, then $V_{rm} = V_r T$ where* $\gcd(V_r, T)$ *divides m.*

Proof. This follows at once from 2.11. □

Note 2.16. The condition that $D \neq 0$ implies that the terms of $\mathcal{U}$, as well as the terms of $\mathcal{V}$ are all distinct.

B. Powerful numbers

Let p be any prime number; we denote by v_p the p-adic valuation.

Let $k \geq 2$. The non-zero integer n is said to be *k-powerful* when $v_p(n) = 0$ or $v_p(n) \geq k$ for every prime number p. A 2-powerful number is simply called a powerful number. If $k \leq h$ every h-powerful number is also a k-powerful number.

The reader may wish to consult Ribenboim [10] or [15] to learn about the interesting properties of powerful numbers.

It is immediate that every powerful number n may be written (but not in a unique way) in the form $n = a^2b^3$. For any number n, the factor $n^* = \prod p^{v_p(n)}$ (for all p such that $v_p(n) \geq k$) is called the *k-powerful part* of n. Then $n = n^*n'$ with $\gcd(n^*, n') = 1$.

If n is any non-zero integer, its *radical* is defined to be

$$\operatorname{rad}(n) = \prod_{p|n} p.$$

We note:

2.17. If $m, n \neq 0$ then $\operatorname{rad}(mn) \leq \operatorname{rad}(m) \cdot \operatorname{rad}(n)$. If $m \mid n$ then $\operatorname{rad}(m) \mid \operatorname{rad}(n)$. If $\gcd(m, n) = 1$ then $\operatorname{rad}(mn) = \operatorname{rad}(m) \cdot \operatorname{rad}(n)$.

2.18. If n is k-powerful then

$$\big(\operatorname{rad}(n)\big)^k \leq |n|.$$

C. Consequences of the (ABC) Conjecture

First we recall the statement of the (ABC) Conjecture.

2.19. (ABC) Conjecture. For every $\varepsilon > 0$ there exists $K > 0$ (depending on ε) such that if A, B, C are non-zero coprime integers such that $A + B + C = 0$. Then

$$\max\big\{|A|, |B|, |C|\big\} < K\big[\operatorname{rad}(ABC)\big]^{1+\varepsilon}.$$

There are many consequences of the (ABC) Conjecture for solutions of diophantine equations.

The following statement is not very different from some results in [13] and in [14]. For the convenience of the reader we give the proof below.

2.20. Let A, B, C, R be positive square-free integers. Let S be the set of all triples (x, y, z) of non-zero integers such that:

1) There exist integers $\ell, m \geq 2$ such that $\frac{1}{\ell} + \frac{1}{m} < 1$ and x is ℓ-poweful and y is m-powerful;
2) $\operatorname{rad}(z) \mid R$;
3) there exist non-zero integers a, b, c (which depend on the triple (x, y, z)) such that $\operatorname{rad}(a) \mid A$, $\operatorname{rad}(b) \mid B$, $\operatorname{rad}(c) \mid C$, $\gcd(ax, by, cz) = 1$ and $ax + by + cz = 0$.

If the (ABC) Conjecture is assumed to be true then S is a finite set.

Proof. Let $S_1 = \{(x, y, z) \in S \bigm| |y| \leq |x|\}$, and $S_2 = \{(x, y, z) \in S \bigm| |x| \leq |y|\}$. We show that S_1 is a finite set. By symmetry, we deduce that S is also finite.

Let $\varepsilon = \frac{1}{6}$. By the (ABC) Conjecture there exists $K > 0$ such that if $(x, y, z) \in S_1$ then

$$|x| \leq |ax| < K r^{\frac{7}{6}}$$

where

$$r = \operatorname{rad}(ax \cdot by \cdot cz) \leq \operatorname{rad}(abc) \cdot |x|^{\frac{1}{\ell}} |y|^{\frac{1}{m}} \operatorname{rad}(z) \leq ABCR\, |x|^{\frac{1}{\ell} + \frac{1}{m}}.$$

So $|x| < K' |x|^{\left(\frac{1}{\ell} + \frac{1}{m}\right)\frac{7}{6}}$ where $K' = K(ABCR)^{\frac{7}{6}}$. Since $\frac{1}{\ell} + \frac{1}{m} \leq \frac{5}{6}$ then $|x| < K' |x|^{\frac{35}{36}}$ hence $|x| < (K')^{36}$. So $|x|$ is bounded, hence also $|y|$ is bounded. Since $ax + by + cz = 0$ then $|z|$ is also bounded, showing that S_1 is a finite set. □

We shall now indicate a consequence of the (ABC) Conjecture concerning powerful terms in binary recurring sequences. A proof that there are only finitely many powerful Fibonacci numbers (under the assumption of the (ABC) Conjecture may be found in the paper of Mollin [8]. It should be noted that the proofs constants flaws (it considers only Fibonacci numbers with odd indices and does not take into account that if $3 \mid n$ then the Fibonacci number U_n and the Lucas number V_n are both even); these flaws are, of converse very easy to repair.

In the paper of Ribenboim and Walsh [16] there are results about the powerful part of terms U_n and V_n. As a special case, it was shown for any binary recurring sequences:

2.21. If the (ABC) Conjecture is assumed to be true then the sets $\{n \geq 1 \mid U_n \text{ is powerful}\}$ and $\{n \geq 1 \mid V_n \text{ is powerful}\}$ are finite.

A direct proof of this result is very simple. But we shall actually prove a stronger statement which will be needed in the main Theorem 3.1.

For the sequence $\mathcal{V}(P, Q)$ we write each terms as a product $V_n = V_n^\sharp V_n'$ where $V_n^\sharp = \prod_{p|2P} p^{v_p(V_n)}$, $V_n' = \prod_{p\nmid 2P} p^{v_p(V_n)}$. So $\gcd(V_n^\sharp, V_n') = 1$; moreover V_n is powerful if and only if both V_n' and $V_n^\sharp$ are powerful. Thus $\{n \geq 1 \mid V_n \text{ is powerful}\} \subseteq \{n \geq 1 \mid V_n' \text{ is powerful}\}$. These sets may be different: $V_2(4, -1) = 18 = 2 \times 9$ is not powerful but $V_2'(4, -1) = 9$ is.

Our purpose now is to prove:

2.22. If the (ABC) Conjecture is assumed to be true then the sets $\{n \geq 1 \mid U_n \text{ is powerful}\}$ and $\{n \geq 1 \mid V_n' \text{ is powerful}\}$ are finite.

Proof. Let $N = \{n \geq 1 \mid U_n \text{ is powerful or } V_n' \text{ is powerful}\}$. The proof hinges on the identity $V_n^2 - DU_n^2 = 4Q^n$ and we shall use the facts that $\gcd(V_n, Q) = \gcd(U_n, Q) = 1$ for every $n \geq 1$ and $\gcd(D, Q) = 1$. We distinguish several cases, according to the parity of P, Q.

Let $A = \text{rad}(2P)$, $B = \text{rad}(2D)$, $C = 2$, $R = \text{rad}(Q)$ and let S be the set of triples associated to A, B, C, R, introduced in 2.20. We shall define an injective mapping $n \mapsto (W_n^2, T_n^2, Q^n)$ from N to S. By 2.20 S is a finite set, so N is also a finite set. Now we come to the actual proof.

Case 1. P is even, hence Q is odd. $4 \mid D$ and V_n is even for every $n \geq 1$. Let $a_n = \left(\frac{V_n^\sharp}{2}\right)^2$, $b_n = -\frac{D}{4}$, $c_n = -1$, $W_n = V_n'$, $T_n = U_n$. So $a_n W_n^2 + b_n T_n^2 + c_n Q^n = 0$, $\gcd(a_n W_n^2, b_n T_n^2, c_n Q^n) = 1$. Also if U_n is powerful, then T_n^2 is 4-powerful, W_n^2 is 2-powerful. If V_n' is powerful, then W_n^2 is 4-powerful and T_n^2 is 2-powerful. Therefore $(W_n^2, T_n^2, Q^n) \in S$ for every $n \in N$. Clearly the mapping $n \mapsto (W_n^2, T_n^2, Q^n)$ is injective, hence in Case 1 the set N is finite.

Case 2. P is odd and Q is even, so D is odd and V_n is odd for every $n \geq 1$. Now let $a_n = (V_n^\sharp)^2$, $b_n = -D$, $c_n = -4$, $W_n = V_n'$, $T_n = U_n$. We verify in the same way that $(W_n^2, T_n^2, Q^n) \in S$ and so N is also finite in Case 2.

Case 3. P and Q are odd, hence D is odd. If $3 \nmid n$ then U_n and V_n are odd; if $3 \mid n$ then U_n and V_n are even.

(a) $3 \nmid n$. We put $a_n = (V_n^\sharp)^2$, $b_n = -D$, $c_n = -4$, $W_n = V_n'$, $T_n = U_n$. As before if $n \in N$ then $(W_n^2, T_n^2, Q^n) \in S$.

(b) $3 \mid n$. We consider two possibilities

(b1) U_n is powerful. Since U_n is even, then $v_2(U_n) \geq 2$.

- If $v_2(U_n) = 2$ let $a_n = \left(\frac{V_n^\sharp}{2}\right)^2$, $b_n = -4D$, $c_n = -1$, $W_n = V_n'$ and $T_n = \frac{U_n}{4}$, hence T_n is powerful. As before $(W_n^2, T_n^2, Q^n) \in S$.
- If $v_2(U_n) \geq 3$ let $a_n = \left(\frac{V_n^\sharp}{2}\right)^2$, $b_n = -D$, $c_n = -1$, $W_n = V_n'$ and $T_n = \frac{U_n}{2}$ so T_n is powerful and again $(W_n^2, T_n^2, Q^n) \in S$.

(b2) V_n' is powerful. Let $a_n = \left(\frac{V_n^\sharp}{2}\right)^2$, $b_n = -D$, $c_n = -1$, $W_n = V_n'$, $T_n = \frac{U_n}{2}$; then $(W_n^2, T_n^2, Q^n) \in S$.

This completes the discussion of all the cases. □

Now let $a > b \geq 1$ with $\gcd(a, b) = 1$. Let $P = a + b$, $Q = ab$, so $D = (a - b)^2$. The integers $U_n \in \mathcal{U}$, $V_n \in \mathcal{V}$ are given by $U_n = \frac{a^n - b^n}{a - b}$, $V_n = a^n + b^n$.

In particular, if $a = 2$, $b = 1$ then $U_n = 2^n - 1$, $V_n = 2^n + 1$. Thus, we obtain, in particular the well-known consequences of the (ABC) Conjecture:

2.23. The (ABC) Conjecture implies that there are only finitely numbers $2^n - 1$ or $2^n + 1$ which are powerful.

In particular these are only finitely many Mersenne numbers $M_q = 2^q - 1$ (with q prime) or Fermat numbers $F_m = 2^{2^m} + 1$ (with $m \geq 0$) which are powerful.

No proof of these statements is known without assuming the truth of the (ABC) Conjecture. This matter has been more fully discussed in [15].

§3. The new theorem

We keep the same notations. In particular, $r(p)$ denotes the rank of appearance of p in $\mathcal{U}$, when $p \mid \mathcal{U}$, and $s(p)$ denotes the rank of appearance of p in $\mathcal{V}$ when $p \mid \mathcal{V}$.

Theorem 3.1. *We assume that the (ABC) Conjecture is true. Then:*

1) *The set $\left\{p \text{ prime}, p \nmid 2PQD \mid \text{for every } n, \text{ either } p^2 \nmid U_n \text{ or } p \mid \frac{n}{r(p)}\right\}$ is infinite.*
2) *The set $\left\{p \text{ prime}, \ p \nmid 2PQD \mid p \text{ divides } \mathcal{V} \text{ and for every } n \text{ either } p^2 \nmid V_n \text{ or } p \mid \frac{n}{s(p)}\right\}$ is infinite.*

Proof. 1) By 2.22 there exists n_0 such that U_n is not powerful for every $n > n_0$. Let $n_0 < q_1 < q_2 < \dots$ where each q_i is a prime number. Then $\gcd(U_{q_i}, U_{q_j}) = 1$ for $i \neq j$. For each $i \geq 1$ there exists a prime p_i such that $p_i \mid U_{q_i}$ but $p_i^2 \nmid U_{q_i}$. Since $\gcd(U_{q_i}, U_{q_j}) = 1$ for $i \neq j$ then $p_i \neq p_j$. Hence there exists $i_0 \geq 1$ such that $p_i \nmid 2PQD$ for all $i \geq i_0$.

Let $r_i = r(p_i)$ so $r_i \neq 1$ and $r_i \mid q_i$ hence $r_i = q_i$.

Let n be such that $p_i^2 \mid U_n$, so $r_i = q_i$ divides n and by Lemma 2.14 $U_n = U_{q_i} Z$ where $\gcd(U_{q_i}, Z)$ divides $\frac{n}{q_i}$. By hypothesis $p_i \mid U_{q_i}$ but $p_i^2 \nmid U_{q_i}$; hence $p_i \mid Z$ and so $p_i \mid \frac{n}{q_i} = \frac{n}{r_i}$.

This shows that the set of all primes $p \nmid 2PQD$, such that if $p^2 \mid U_n$ then $p \mid \frac{n}{r(p)}$, is an infinite set.

2) By 2.22 there exists n_0 such that if $n > n_0$ then V'_n is not powerful. Let $n_0 < q_1 < q_2 < \dots$ where each q_i is an odd prime. We have $\gcd(V'_{q_i}, V'_{q_j}) \mid \gcd(V_{q_i}, V_{q_j}) = P$, but $\gcd(V'_{q_i}, P) = 1$, so $\gcd(V'_{q_i}, V'_{q_j}) = 1$ for all $i \neq j$. For each $i \geq 1$ there exists a prime p_i such that $p_i \mid V'_{q_i}$ but $p_i^2 \nmid V'_{q_i}$. Then $p_i \neq p_j$ for all $i \neq j$. Hence there exists i_0 such that $p_i \nmid 2PQD$ for all $i \geq i_0$. Each $p_i \mid V'_{q_i}$, so $p_i \mid V_{q_i}$. Let n be such that $p_i^2 \mid V_n$; we denote by $s_i = s(p_i)$. Since $p_i \mid V'_{q_i}$ then $p_i \mid V_{q_i}$ hence $s_i \mid q_i$. But $p_i \nmid P$ so $s_i \neq 1$ therefore $s_i = q_i$. We also have: $s_i = q_i$ divides n with $\frac{n}{q_i}$ odd and by Lemma 2.14. $V_n = V_{q_i} T$ where $\gcd(V_i, T)$ divides $\frac{n}{q_i}$. Since $p_i \mid V'_{q_i}$ then $p_i \mid V_{q_i}$; if $p_i^2 \mid V_{q_i}$, since $p_i \nmid 2P$ then $p_i^2 \mid V'_{q_i}$ which is absurd. So $p_i^2 \nmid V_{q_i}$, hence $p_i \mid T$ and $p_i \mid \frac{n}{q_i}$. This shows that the set of all primes p, $p \nmid 2PQD$ such that if $p^2 \mid V_n$ then $p \mid \frac{n}{s(p)}$ is an infinite set. □

We obtain the immediate corollary:

Corollary 3.2. *There exist infinitely many primes p such that $p^2 \nmid U_{p-(\frac{D}{p})}$.*

Proof. Consider the set S of all primes p such that $p \nmid 2PQD$ and if $p^2 \mid U_n$ then $p \mid \frac{n}{r(p)}$. Let $p \in S$. Since $p \mid U_{p-(\frac{D}{p})}$ but $p \nmid \frac{p-(\frac{D}{p})}{r(p)}$ because $(\frac{D}{p}) = \pm 1$, then $p^2 \nmid U_{p-(\frac{D}{p})}$, by Theorem 3.1, we deduce that there are infinitely many primes p such that $p^2 \nmid U_{p-(\frac{D}{p})}$. □

We obtain the following corollary, which includes Silverman's result mentioned in the Introduction. Let $a > 1$, $P = a+1$, $Q = a$ and consider the sequences $\mathcal{U}(P,Q)$, $\mathcal{V}(P,Q)$. Then $U_n = \frac{a^n-1}{a-1}$, $V_n = a^n + 1$. We have $D = P^2 - 4Q = (a-1)^2$, so $U_{p-(\frac{D}{p})} = \frac{a^{p-1}-1}{a-1}$. We also note that p divides $\mathcal{V}$ if and only if $p \nmid a$ and there exists the smallest s such that $a^s \equiv -1 \pmod{p}$ so the order of a modulo p is even, namely $2s$. Now we indicate the corollary.

Corollary 3.3. *We assume that the (ABC) Conjecture is true. Let $a > 1$, then:*

1) *There exist infinitely many primes p such that $a^{p-1} \not\equiv 1 \pmod{p^2}$.*

2) *There exist infinitely many primes p such that $p \nmid a$, the order of a modulo p is $2s$ and $a^s \not\equiv -1 \pmod{p^2}$.*

Proof. 1) We consider the sequence $\mathcal{U}(a+1,a)$, with $D = (a-1)^2$. By Corollary 3.2 there exist infinitely many primes $p \nmid a(a+1)(a-1)$ such that $p^2 \nmid U_{p-(\frac{D}{p})} = \frac{a^{p-1}-1}{a-1}$, hence $a^{p-1} \not\equiv 1 \pmod{p^2}$.

2) By Theorem 3.1 there are infinitely many primes p such that $p \mid \mathcal{V}(a+1,a)$ and $p^2 \nmid V_s$ where $2s$ is the order of a modulo p. This translates into the statement (2). □

References

[1] M. Aaltonen and K. Inkeri, Catalan's equation $x^p - y^q = 1$ and related congruences, *Math. Comp.* **56** (1991), 359–370.

[2] R. Crandall, K. Dilcher and C. Pomerance, A search for Wieferich and Wilson primes, *Math. Comp.* **66** (1997), 433–449.

[3] A. Granville, Powerful numbers and Fermat's last theorem, *C. R. Math. Rep. Acad. Sci. Canada* **8** (1986), 215–218.

[4] A. Granville, Some conjectures related to Fermat's last theorem, in: Number Theory, *W. de Gruyter*, *Berlin*, 1990, 177–192.

[5] K. Inkeri, On Catalan's conjecture, *J. Nb. Th.* **34** (1990), 142–152.

[6] P. Mihăilescu, A theorem on Catalan's conjecture, (*preprint*).

[7] P. Mihăilescu, A class-number-free criterion for Catalan's equation, (*to appear in* J. Nb. Th.).

[8] R. A. Mollin, Masser's conjecture used to prove results about powerful numbers, *J. Math. Sci.* **7** (1996), 29–32.

[9] P. Ribenboim, 13 Lectures on Fermat's Last Theorem, *Springer-Verlag*, *New York*, 1979.

[10] P. Ribenboim, Catalan's Conjecture, *Academic Press*, *Boston*, 1994.

[11] P. Ribenboim, The New Book of Prime Number Records, *Springer-Verlag*, *New York*, 1996.

[12] P. Ribenboim, An algorithm to determine the points with integral coordinates in certain elliptic curves, *J. Nb. Th.* **74** (1999), 19–38.

[13] P. Ribenboim, *ABC* candies, *J. Nb. Th.* **81** (2000), 48–60.

[14] P. Ribenboim, Consequences of the (*ABC*) Conjecture for almost powerful numbers, (submitted for publication).

[15] P. Ribenboim, My Numbers, My Friends, *Springer-Verlag*, *New York*, 2000.

[16] P. Ribenboim and P. G. Walsh, The *ABC* Conjecture and the powerful part of terms in binary recurring sequences, *J. Nb. Th.* **74** (1999), 134–147.

[17] J. H. Silverman, Wieferich's criterion and the *abc*-conjecture, *J. Nb. Th.* **30** (1988), 226–237.

PAULO RIBENBOIM
DEPARTMENT OF MATHEMATICS
KINGSTON, ONTARO K7L3N6
CANADA

(Received February 19, 2001)