Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

William A. Webb, Calvin T. Long

Distribution modulo p^h of the general linear second order recurrence

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **58** (1975), n.2, p. 92–100.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1975_8_58_2_92_0>

Teoria dei numeri. — *Distribution modulo p^h of the general linear second order recurrence.* Nota di WILLIAM A. WEBB e CALVIN T. LONG, presentata [(*)] dal Socio B. SEGRE.

RIASSUNTO. — Interessanti risultati di altri Autori, sull'argomento specificato nel titolo, vengono completati in modo esauriente.

1. INTRODUCTION

Let $\{u_n\}_{n\geq 0}$ be the linear second order recurrence defined by

$$u_0 = c \quad , \quad u_1 = d \quad , \quad u_{n+1} = au_n + b_{n-1} \qquad (\forall n \geq 1) \tag{1}$$

where a, b, c, and d are integers. Let

$$\rho = \frac{a+\sqrt{a^2+4b}}{2} \quad \text{and} \quad \sigma = \frac{a-\sqrt{a^2+4b}}{2} . \tag{2}$$

Then it is easily shown that

$$u_n = \frac{(d-c\sigma)\,\rho^n - (d-c\rho)\,\sigma^n}{\rho-\sigma} \tag{3}$$

for all $n \geq 0$. Also, it is easily shown that $\{u_n\}$ is periodic modulo m for any positive integer m. Let $k(m)$ be the (least) period of $\{u_n\}$ modulo m.

In [3], Kuipers and Shiue show that the Fibonacci sequence is uniformly distributed modulo 5, is not uniformly distributed modulo p for any prime $p \neq 5$, is not uniformly distributed modulo m for any composite $m \neq 5^k$ for $k > 1$, and conjecture that the sequence is uniformly distributed modulo 5^k for all $k \geq 1$. In [5], Niederreiter proves that the conjecture of Kuipers and Shiue is correct. In [1], Bundschuh obtains the result of Niederreiter utilizing some well-known relationships between the Fibonacci and Lucas sequences. In [4], Kuipers and Shiue consider the general second order recurrence defined above and give sufficient conditions that $\{u_n\}$ be uniformly distributed modulo p^h for all integers $h \geq 1$ where p is an odd prime. However, the conditions of the Kuipers-Shiue result are unusually cumbersome; nothing is said about necessary conditions, and the case $p = 2$ is not discussed. In [2], Bundschuh and Shiue improve on the result of Kuipers and Shiue, but again give only sufficient conditions. In [6], Shiue and Hu show that if a and b have the same parity, then $\{u_n\}$ is not uniformly distributed modulo 2^h for any integer $h \geq 1$. Again, however, the result is incomplete in that the cases when a and b have opposite parity are not considered and no attempt is made to find necessary conditions. In the present

(*) Nella seduta dell'8 febbraio 1975.

paper, we settle the issue for prime power moduli by giving necessary and sufficient conditions that $\{u_n\}$ be uniformly distributed modulo p^h for any prime p and for all integers $h \geq 1$.

2. PRELIMINARY RESULTS

At the outset we observe that if $p \mid ab$, then it is easily seen that $\{u_n\}$ is uniformly distributed modulo p if and only if $p = 2$, a is even, b is odd, and c and d are of opposite parity. Thus, except for Theorem 4, for the remainder of the paper we restrict our attention to the case $(p, ab) = 1$.

If $p \mid c$ and $p \mid d$, then $u_n \equiv 0 \pmod{p}$ for all n and $\{u_n\}$ is not uniformly distributed modulo p, thus we may exclude this case from consideration. If $p \nmid d$, then $(p, u_1) = 1$ since $u_1 = d$. If $p \mid d$, then $(p, ad + bc) = 1$. Hence, by renumbering so that $u_0 = d$ and $u_1 = ad + bc$, we again have $(p, u_1) = 1$. Thus, we may henceforth assume that $(p, abd) = 1$ since all other cases are essentially trivial or easily reduce to this case.

From (3) it is easy to derive the following

LEMMA 1. *If p is an odd prime, $(p, a^2 + 4b) = 1$, and $p \mid c$, then $p \mid u_{p-1} u_{p+1}$.*

THEOREM 1. *If p is an odd prime and $p \nmid (a^2 + 4b)$, then $\{u_n\}$ is not uniformly distributed modulo p.*

Proof. Recall that we are assuming that $(p, ab) = 1$ and assume that $\{u_n\}$ is uniformly distributed modulo p. Since $p \nmid b$, it is easy to see that $\{u_n\}$ is purely periodic. Thus, $u_k = 0$ for some k and, without loss in generality, we may assume that $u_0 = 0 = c$. But then $u_n = du_n^*$ where u_n^* is defined by

$$u_0^* = 0 \quad , \quad u_1^* = 1 \quad , \quad u_{n+1}^* = au_n^* + bu_{n-1}^* \qquad (\forall n \geq 1) \tag{4}$$

and $\{u_n\}$ is uniformly distributed modulo p if and only if $\{u_n^*\}$ is uniformly distributed modulo p. Hence, again without loss in generality, we may assume that $u_1 = 1 = d$.

Let j be the least positive integer such that $p \mid u_j$. Let $t \equiv bu_{j-1} \pmod{p}$ and let t belong to s modulo p. Then the sequence modulo p becomes

$$0, 1, \cdots, u_{j-1}, 0, t, \cdots, tu_{j-1}, 0, t^2, \cdots, t^2 u_{j-1}, 0, \cdots, 0, t^{s-1}, \cdots, t^{s-1} u_{j-1}, \cdots$$

with the sequence repeating after the element $t^{s-1} u_{j-1}$. It follows that js is the length of the period of $\{u_n\}$ modulo p and hence that every residue modulo p appears s times in the period since zero does. But since there are just p residues modulo p, this implies that $ps = js$ and hence that $p = j$. Therefore $u_p \equiv u_j = 0 \pmod{p}$ by definition of j. But, by Lemma 1, $p \mid u_{p-1} u_{p+1}$ and so p divides two consecutive terms in $\{u_n\}$ and hence all terms from at least u_p on. Since this is a clear contradiction of the assumption that $\{u_n\}$ is uniformly distributed modulo p, the proof is complete.

LEMMA 2. *Let* $p \mid (a^2 + 4b)$. *Then* $p \mid u_n$ *for some* n *if and only if* $(p, ad + 2bc) = 1$.

Proof. Since we are assuming throughout that $(p, ab) = 1$, the hypothesis $p \mid (a^2 + 4b)$ clearly implies that p is odd. Observing that $\rho\sigma = -b$ and $\rho - \sigma = \sqrt{a^2 + 4b}$, we have from (3) that

$$u_n = \frac{(d - c\sigma)\rho^n - (d - c\rho)\sigma^n}{\rho - \sigma} = \frac{d(\rho^n - \sigma^n)}{\rho - \sigma} + \frac{cb(\rho^{n-1} - \sigma^{n-1})}{\rho - \sigma} = \tag{5}$$

$$= \frac{d}{2^{n-1}} \sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} a^{n-2k-1}(a^2 + 4b)^k + \frac{cb}{2^{n-2}} \sum_{k=0}^{[(n-2)/2]} \binom{n-1}{2k+1} a^{n-2k-2}(a^2 + 4b)^k .$$

Since $a^2 + 4b \equiv 0 \pmod p$, this implies that

$$2^{n-1} u_n \equiv dna^{n-1} + 2bc(n-1)a^{n-2} \equiv a^{n-2}[(n-1)(ad + 2bc) + ad] \equiv 0 \pmod p$$

for some n, if and only if the congruence

$$(ad + 2bc)x \equiv -ad \pmod p$$

is solvable; i.e., if and only if $(p, ad + 2bc) = 1$ since we also have that $(p, d) = 1$. Since p is odd, this yields the desired conclusion.

LEMMA 3. *Let* p *be odd and* $p \mid (a^2 + 4b)$, *then* $\{u_n\}$ *is periodic modulo* p^h *and* $k(p^h) \mid p^h(p-1)$ *for* $h \geq 1$.

Proof. Let m and n be integers with $0 \leq m < n$ and

$$n \equiv m \pmod{p^h(p-1)} . \tag{6}$$

Then

$$2^{n-m} a^{m-2k-1} \equiv a^{n-2k-1} \pmod{p^h} \tag{7}$$

since $\varphi(p^h) \mid (n - m)$. Therefore,

$$\begin{aligned} 2^{n-1}(u_n - u_m) &= d \sum_{k \geq 0} \binom{n}{2k+1} a^{n-2k-1}(a^2 + 4b)^k - \\ &- d\, 2^{n-m} \sum_{k \geq 0} \binom{m}{2k+1} a^{m-2k-1}(a^2 + 4b)^k + \\ &+ 2cb \sum_{k \geq 0} \binom{n-1}{2k+1} a^{n-2k-2}(a^2 + 4b)^k - \\ &- 2^{n-m}\, 2cb \sum_{k \geq 0} \binom{m-1}{2k+1} a^{m-2k-2}(a^2 + 4b)^k \equiv \\ &\equiv d \sum_{k \geq 0} a^{n-2k-1}(a^2 + 4b)^k \left[\binom{n}{2k+1} - \binom{m}{2k+1}\right] + \\ &+ 2cb \sum_{k \geq 0} a^{n-2k-2}(a^2 + 4b)^k \left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] \pmod{p^h}. \end{aligned} \tag{8}$$

At this point, let $\text{ord}_p(n)$ denote the exponent to which p appears in the canonical representation of n. Then

$$(9) \qquad \text{ord}_p \left\{ \left[\binom{n}{2k+1} - \binom{m}{2k+1} \right] a^{n-2k-1} (a^2+4b)^k \right\} \geq$$
$$\geq \text{ord}_p \left[n(n-1)\cdots(n-2k) - m(m-1)\cdots(m-2k) \right] -$$
$$- \text{ord}_p (2k+1)! + k \geq$$
$$\geq h - \sum_{j \geq 1} \left[\frac{2k+1}{p^j} \right] + k \geq h - k + k = h$$

and, similarly,

$$(10) \qquad \text{ord}_p \left\{ \left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1} \right] a^{n-2k-2} (a^2+4b)^k \right\} \geq h .$$

In view of (9) and (10) and since p is odd, it follows from (8) that

$$u_n \equiv u_m \pmod{p^h} .$$

Thus, $\{u_n\}$ is periodic modulo p^h and $k(p^h) \mid p^h(p-1)$ by (6) as claimed.

3. THE PRINCIPAL RESULTS

The following theorems give necessary and sufficient conditions that $\{u_n\}$ be uniformly distributed modulo p^h for any prime p and for all integers $h \geq 1$.

THEOREM 2. *Let $p > 3$ be an odd prime and let $h \geq 1$ be an integer. Then the sequence $\{u_n\}$ is uniformly distributed modulo p^h if and only if $p \mid (a^2 + 4b)$ and $(p, ad + 2bc) = 1$.*

Proof. Suppose first that $\{u_n\}$ is uniformly distributed modulo p^h. Then $\{u_n\}$ is uniformly distributed modulo p and we have from Theorem 1 that $p \mid (a^2 + 4b)$. Also, it is immediate from Lemma 2 that $(p, ad + 2bc) = 1$ since, otherwise, there does not exist n such that $u_n \equiv 0 \pmod{p}$ as must be the case if $\{u_n\}$ is uniformly distributed modulo p.

Now suppose that $p \mid (a^2 + 4b)$ and $(p, ad + 2bc) = 1$. By Lemma 2, there exists n such that $u_n \equiv 0 \pmod{p}$. Hence, without loss in generality, we may take $u_0 = 0$. Now $u_1 = d$ and $(d, p) = 1$ so that we may also take $d = 1$ without loss in generality. With these simplifications $u_n = u_u^*$ as defined in (4) and, by essentially the same argument as in the proof of Lemma 2,

$$(11) \qquad u_n \equiv s^{n-1} \sum_{k=0}^{[(n-1)/2]} \binom{n}{2k+1} a^{n-2k-1} (a^2+4b)^k \equiv n(sa)^{n-1} \equiv nt^{n-1} \pmod{p}$$

where $2s \equiv 1 \pmod{p}$, and t is defined by $2t \equiv a \pmod{p}$. Thus, it is clear that $\{u_n\}$ is periodic modulo p with period pe where t belongs to e modulo p

and $e \mid (p - 1)$. Therefore, $(p, e) = 1$ so that for each h, $0 \le h \le e - 1$, the elements

$$(h + re + 1)\, t^{h+re}, \qquad r = 0, 1, \cdots, p - 1$$

constitute a complete residue system modulo p since $t^{h+re} \equiv t^h \pmod{p}$ and $(p, t) = 1$. Thus, $\{nt^{n-1}\}_{n=1}^{pe}$ runs over each residue modulo p precisely e times and the same is true for $\{u_n\}_{n=1}^{pe}$. Thus, $\{u_n\}$ is uniformly distributed modulo p.

Now assume that $\{u_n\}$ is uniformly distributed modulo p^{h-1} for some $h \ge 2$ and note that we no longer assume $c = 0$, $d = 1$ since these simplifying assumptions were only valid for p and not for p^h with $h > 1$. By Lemma 3, $\{u_n\}$ has period $k(p^{h-1})$ where $k(p^{h-1}) \mid p^{h-1}(p - 1)$ and it follows that the sequence runs over each residue modulo p^{h-1} precisely $p - 1$ times for $1 \le n \le p^{h-1}(p - 1)$. That is to say, for a given g, the congruence

$$u_n \equiv g \pmod{p^{h-1}}$$

is satisfied for precisely $p - 1$ elements in the set

$$C = \{1, 2, \cdots, p^{h-1}(p - 1)\}.$$

The desired result will follow if we can show that the congruence

$$u_n \equiv g \pmod{p^h} \tag{12}$$

is also satisfied for precisely $p - 1$ elements in the set

$$D = \{1, 2, \cdots, p^h(h - 1)\}.$$

Let $c_1, c_2, \cdots, c_{p-1}$ be those elements of C such that

$$u_n \equiv g \pmod{p^{h-1}} \quad \text{iff} \quad n \equiv c_i \pmod{p^{h-1}(p - 1)}.$$

Let m and n be in D with $m \le n$ and assume that

$$u_n \equiv g \equiv u_m \pmod{p^h}, \qquad n \equiv c_i \equiv m \pmod{p^{h-1}(p - 1)}. \tag{13}$$

If we can show that $n = m$, then the number of n in D satisfying (12) must be at most $p - 1$ since there are only $p - 1$ elements c_i and a unique n for each c_i. Since there are p^h different values of g modulo p^h and $p^h(p - 1)$ elements in D, it then follows that the number of n in D satisfying (12) is precisely $p - 1$ as desired.

From (13) and (5), we obtain

$$\begin{aligned} d \sum_{k \ge 0} \binom{n}{2k+1} a^{n-2k-1} (a^2 + 4b)^k - d\, 2^{n-m} \sum_{k \ge 0} \binom{m}{2k+1} a^{m-2k-1} (a^2 + 4b)^k + \\ + 2cb \sum_{k \ge 0} \binom{n-1}{2k+1} a^{n-k-2} (a^2 + 4b)^k - \\ - 2cb\, 2^{n-m} \sum_{k \ge 0} \binom{m-1}{2k+1} a^{m-k-2} (a^2 + 4b)^k \equiv 0 \pmod{p}. \end{aligned} \tag{14}$$

Again,

$$2^{n-m}\, a^{m-2k-1} \equiv a^{n-2k-1} \pmod{p^h}$$

since $\varphi(p^h) \mid (n-m)$ by (13). Therefore, from (14) we have

$$(15)\qquad d \sum_{k\geq 0} a^{n-2k-1}(a^2+4b)^k \left[\binom{n}{2k+1} - \binom{m}{2k+1}\right] +$$

$$+ 2cb \sum_{k\geq 0} a^{n-2k-2}(a^2+4b)^k \left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] \equiv 0 \pmod{p^h}.$$

Then, for $k \geq 1$, it follows from (13) that

$$\operatorname{ord}_p \left\{\left[\binom{n}{2k+1} - \binom{m}{2k+1}\right] a^{n-2k-1}(a^2+4b)^k\right\} \geq$$

$$\geq \operatorname{ord}_p [n(n-1)\cdots(n-2k) - m(m-1)\cdots(m-2k)] -$$

$$- \operatorname{ord}_p (2k+1)! + k \geq$$

$$\geq h - 1 \sum_{j\geq 1} \left[\frac{2k+1}{p^j}\right] + k \geq h - 1 - (k-1) + k = h$$

and the same thing would be true of

$$\operatorname{ord}_p \left\{\left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] a^{n-2k-1}(a^2+4b)^k\right\}.$$

Therefore, p^h divides all terms in (15) with $k \geq 1$ and this implies that

$$0 \equiv da^{n-1}\left[\binom{n}{1} - \binom{m}{1}\right] + 2cba^{n-2}\left[\binom{n-1}{1} - \binom{m-1}{1}\right] \equiv$$

$$\equiv da^{n-1}(n-m) + 2cba^{n-2}(n-m) \equiv a^{n-2}(n-m)(ad+2cb) \pmod{p^h}$$

and hence that

$$n \equiv m \pmod{p^h}$$

since $(a, p) = (ad + 2cb, p) = 1$. But (13) also gives

$$n \equiv m \pmod{p-1}$$

and so

$$n \equiv m \pmod{p^h(p-1)}.$$

But since m and n are both in D, this implies that $n = m$ and the proof is complete.

THEOREM 3. *The sequence $\{u_n\}$ is uniformly distributed modulo 3^h for all $h \geq 1$ if and only if $3 \mid (a^2 + 4b)$, $(3, ad + 2bc) = 1$ and (a, b) modulo 9 is not one of the pairs* (1,8), (8,8), (4,2), (5,2), (2,5), or (7,5).

Proof. It is easily seen that each of the pairs (1,8), (8,8), (4,2), (5,2), (2,5), and (7,5) modulo 9 leads to a sequence $\{u_n\}$ that is uniformly distributed modulo 3 but not uniformly distributed modulo 9 and hence, *a fortiori*, not uniformly distributed modulo 3^h for any $h \geq 2$. Now the remainder of the proof exactly follows that of Theorem 2 up to (15). Modulo 3^h, (15) becomes

$$(16)\qquad d \sum_{k \geq 0} a^{n-2k-1} (a^2 + 4b)^k \left[\binom{n}{2k+1} - \binom{m}{2k+1}\right] + $$
$$+ 2cb \sum_{k \geq 0} a^{n-2k-2} (a^2 + 4b)^k \left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] \equiv 0 \pmod{3^h}.$$

Now if $x \equiv y \pmod{3^{h-1}}$ and $k \geq 1$,

$$\operatorname{ord}_3 \left\{\left[\binom{x}{2k} - \binom{y}{2k}\right] (a^2 + 4b)^k\right\} \geq$$
$$\geq \operatorname{ord}_3 [x(x-1)\cdots(x-2k+1) - y(y-1)\cdots(y-2k+1)] -$$
$$- \operatorname{ord}_3 (2k)! + k \geq$$
$$\geq h - 1 - (k-1) + k = h.$$

Thus, it follows that

$$(17)\qquad \left[\binom{x}{2k} - \binom{y}{2k}\right] (a^2 + 4b)^k \equiv 0 \pmod{3^h}$$

for $k \geq 1$ and the result is trivially true for $k = 0$. Therefore, for any term in (16) we have

$$\left[\binom{n}{2k+1} - \binom{m}{2k+1}\right) (a^2 + 4b)^k =$$
$$= \left\{\left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] + \left[\binom{n-1}{2k} - \binom{m-1}{2k}\right]\right\} (a^2 + 4b)^k \equiv$$
$$\equiv \left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] (a^2 + 4b)^k \equiv \cdots$$
$$\equiv \left[\binom{n-m+2k+1}{2k+1} - \binom{2k+1}{2k+1}\right] (a^2 + 4b)^k =$$
$$= \left[\binom{n-m+2k}{2k+1} + \binom{n-m+2k}{2k} - \binom{2k}{2k}\right] (a^2 + 4b)^k \equiv$$
$$\equiv \binom{n-m+2k}{2k+1} (a^2 + 2t)^k \pmod{3)^h}.$$

Hence, equation (16) reduces to

$$(18)\qquad d \sum_{k=0}^{1} a^{n-2k-1} (a^2 + 4b)^k \binom{n-m+2k}{2k+1} +$$
$$+ 2cb \sum_{k=0}^{1} a^{n-2k-2} (a^2 + 4b)^k \binom{n-m+2k}{2k+1} +$$
$$\equiv a^{n-2} (ad + 2bc) (n-m) + a^{n-4} (ad + 2cb) \binom{n-m+2}{3} (a^2 + 4b) \equiv$$
$$\equiv a^{n-4} (ad + 2bc) (n-m) [a^2 + (a^2 + 4b) (n-m+2) (n-m+1)/6] \equiv$$
$$\equiv 0 \pmod{3^h}.$$

Since $3 \mid (a^2 + 4b)$, we may define t by

$$a^2 + 4b \equiv 6t \pmod{3^h}.$$

Also, $(n - m + 2)(n - m + 1) \equiv 2 \pmod{3^h}$ since $n \equiv m \pmod{3^{h-1}}$ and $h \geq 2$. Using this in (18) and observing that $(a, 3) = (ad + 2bc, 3) = 1$, we obtain

$$(n - m)(a^2 + 4b) \equiv 0 \pmod{3^h}.$$

This implies either $n - m \equiv 0 \pmod{3^h}$ or

$$2t \equiv -a^2 \equiv 2 \pmod{3}$$

so that $t \equiv 1 \pmod{3}$. But $t \equiv 1 \pmod{3}$, implies

$$a^2 + 4b \equiv 6 \pmod{9}$$

and this is so if and only if (a, b) modulo 9 is one of the pairs (1,8), (8,8), (4,2), (5,2), (2,5), or (7,5) since $(a, b) = 1$. Thus

$$n \equiv m \pmod{3^h}$$

and the remainder of the proof is the same as for Theorem 2.

THEOREM 4. *The sequence $\{u_n\}$ is uniformly distributed modulo 2 if and only if a is even, b is odd and c and d have opposite parity. The sequence $\{u_n\}$ is uniformly distributed modulo 2^h for $h \geq 2$ if and only if $a \equiv 2$ (mod 4), $b \equiv 3$ (mod 4), and c and d have opposite parity.*

Proof. The truth of the assertion modulo 2 is easily checked simply by considering the various cases. In a similar way, it is easy to see that $\{u_n\}$ is uniformly distributed modulo 4 if and only if $a \equiv 2 \pmod{4}$, $b \equiv 3 \pmod{4}$ and c and d have opposite parity. Since $\{u_n\}$ is uniformly distributed modulo 4 if is uniformly distributed modulo 2^h for any $h \geq 2$, it remains only to show that the given conditions are sufficient. The proof again proceeds as in Theorem 2 except that we cannot use Lemma 3 which presumes that p is odd. Using induction, we assume that $\{u_n\}$ is uniformly distributed modulo 2^{h-1} for some $h \geq 3$ and is periodic of period 2^{h-1} modulo 2^h. As in the proof of Theorem 2, it will suffice to show that

$$(19) \qquad u_n \equiv u_m \pmod{2^h} \quad \text{and} \quad n \equiv m \pmod{2^{h-1}}$$

together imply $n \equiv m \pmod{2^h}$.

Since $a = 2t$ with t odd, $\rho = t + \sqrt{t^2 + b}$, $\sigma = t - \sqrt{t^2 + b}$, and equation (5) becomes

$$(20) \qquad u_n = d \sum_{k \geq 0} \binom{n}{2k+1} t^{n-2k-1} (t^2 + b)^k + cb \sum_{k \geq 0} \binom{n-1}{2k+1} t^{n-2k-2} (t^2 + b)^k.$$

Thus, it follows from (19) that $t^m \equiv t^n \pmod{2^h}$ and hence that

$$(21) \qquad d \sum_{k\geq 0} \left[\binom{n}{2k+1} - \binom{m}{2k+1}\right] t^{n-2k-2} (t^2+b) + \\ + cb \sum_{k\geq 0} \left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] t^{n-2k-2} (t^2+b) \equiv 0 \pmod{2^h}.$$

Since $t^2 \equiv 1 \pmod 4$ and $b \equiv 3 \pmod 4$, $4 \mid (t^2+b)$. Thus, for $k \geq 1$,

$$(22) \qquad \mathrm{ord}_2 \left[\binom{n}{2k+1} - \binom{m}{2k+1}\right] t^{n-2k-1} (t^2+b)^k \geq \\ \geq \mathrm{ord}_2 \left[n(n-1)\cdots(n-2k) - m(m-1)\cdots(m-2k)\right] - \\ - \mathrm{ord}_2 (2k+1)! + 2k > (h-1) - 2k + 2k = h-1$$

and, similarly,

$$(23) \qquad \mathrm{ord}_2 \left[\binom{n-1}{2k+1} - \binom{m-1}{2k+1}\right] t^{n-2k-2} (t^2+b) > h-1.$$

With (21), these results imply that

$$(n-m)(dt+cb) = 0 \pmod{2^h}$$

and hence that

$$n \equiv m \pmod{2^h}$$

since $(tb, 2) = 1$ and c and d are of opposite parity. This completes the induction and the proof.

References

[1] P. Bundschuh (1974) – *On the distribution of Fibonacci numbers*, «Tamkang J.», *5*, 75–79.

[2] P. Bundschuh and J. Shiue (1973) – *Solution of a problem on the uniform distribution of integers*, «Atti Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. nat.», *55*, 172–177.

[3] L. Kuipers and J. Shiue (1972) – *A distribution property of the sequence of Fibonacci numbers*, «Fibonacci Quart. J.», *10*, 375–392.

[4] L. Kuipers and J. Shiue (1972) – *A distribution property of a linear recurrence of the second order*, «Atti Accad. Naz. Lincei, Rend. Cl. Sci. fis. mat. nat.», *52*, 6–10.

[5] H. Niederreiter (1972) – *Distribution of Fibonacci numbers mod* 5^k, «Fibonacci Quarterly», *10*, 373–374.

[6] J. Shiue and M. Hu (1973) – *Some remarks on the uniform distribution of a linear recurrence of the second order*, «Tamkang J. Math.», *4*, 101–103.