Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Peter Bundschuh, Jau-Shyong Shiue

Solution of a problem on the uniform distribution of integers

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **55** (1973), n.3-4, p. 172–177.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1973_8_55_3-4_172_0>

Teoria dei numeri. — *Solution of a problem on the uniform distribution of integers* (*). Nota (**) di PETER BUNDSCHUH e JAU-SHYONG SHIUE, presentata dal Socio B. SEGRE.

RIASSUNTO. — Si riottiene sotto condizioni più generali un Teorema di Kuipers e Shiue stabilito altrimenti da questi Autori in una precedente Nota lincea [2], e si risolve un problema aperto ivi enunciato.

§ 1. INTRODUCTION

In [3] Niven introduced the notion of uniform distribution of a sequence of integers: Let $\mathcal{G}$ be such an infinite sequence $\{g_n\}_{n=1,2,\cdots}$, let m be a fixed integer ≥ 2, let $0 \leq j < m$ and put

$$A_{\mathcal{G}}(N, j, m) = \sum_{\substack{n \leq N \\ g_n \equiv j \pmod{m}}} 1 .$$

Then $\mathcal{G}$ is said to be uniformly distributed (shortly: u.d.) mod m, if for each $j = 0, \cdots, m-1$

$$\lim_{N \to \infty} \frac{1}{N} A_{\mathcal{G}}(N, j, m)$$

exists and equals $1/m$.

In this Note we study the following sequence $\{G_n\}$. Let A, B, a, b be fixed rational integers, let the equation $x^2 - Ax + B = 0$ have distinct nonzero roots, which means $B \neq 0$ and $D = A^2 - 4B \neq 0$, and moreover let a, b be not both equal to zero. Then let $\{G_n\}$ be defined by

$$G_0 = a \quad , \quad G_1 = b \quad , \quad G_{n+1} = AG_n - BG_{n-1} \qquad (n = 1, 2, \cdots) \tag{1}$$

and let $\{R_n\}$ be the special sequence of $\{G_n\}$ with $a = 0$, $b = 1$. Let P_k and Q_k denote the exact period length of $\{R_n\}$ and $\{G_n\}$ modulo p^k for $k = 1, 2, \cdots$ respectively.

We want to prove the following theorem by a method developed in [1] by one of the present Authors.

THEOREM. *Let p be a prime with $p \mid D$, $p \nmid 2B$, $p \nmid (bA - 2aB)$ and let* d *be the exact order of* B *mod p. If $P_k = 2\,\mathrm{d}p^k$ for $k = 1, 2, \cdots$, then $\{G_n\}$ is u.d. mod p^k for $k = 1, 2, \cdots$.*

(*) This paper was written while the second Author was an Alexander von Humboldt-Stiftung fellow visiting the University of Göttingen.

(**) Pervenuta all'Accademia il 3 settembre 1973.

Note that we can show in Lemma 1 of § 2 that under the same assumptions of our theorem on the prime p we have $Q_k = P_k$ for all k. Note also that the assumptions: P_1 is even and furthermore $P_2 \neq P_1$ in case $p = 3$ imply that $P_k = 2\,d p^k$ for all k under the specified assumptions on p. This will be shown in a later paper on the periods of $\{G_n\}$ modulo a fixed natural number ≥ 2. Here we give two corollaries which are proved at the end of § 3.

COROLLARY 1. *The theorem of Kuipers and Shiue in* [2].

Note that the assumption in [2] that the congruence $2\,Bx \equiv A\,(p)$ is satisfied by a primitive root mod p is superfluous. At the end of [2] there are proposed some unsolved problems which we can answer now.

COROLLARY 2. *Take* $A = 3$, $B = -1$ *and let* (a, b) *be the pair* $(1, 1)$, $(1, 3)$, $(1, 5)$ *respectively. Then the corresponding sequences* $\{G_n\}$ *formed following* (1) *are u.d. mod* 13^k *for* $k = 1, 2, \cdots$.

§ 2. LEMMAS

The first lemma gives the reduction of the periods of the general sequences $\{G_n\}$ to those of the special sequence $\{R_n\}$.

LEMMA 1. *If* $p \mid D$, $p \nmid 2B$, $p \nmid (bA - 2\,aB)$ *then* $Q_k = P_k$ $(k = 1, 2, \cdots)$.

Proof. First we express the G's by the R's:

$$G_n = bR_n - aBR_{n-1}\,. \tag{2}$$

This is correct for $n = 0$ (in virtue of $R_1 = -BR_{-1}$, see for example (7) in Lemma 2) and for $n = 1$. Now

$$-aBR_n = -aB\,(AR_{n-1} - BR_{n-2}) = A\,(G_n - bR_n) -$$
$$- B\,(G_{n-1} - bR_{n-1}) = G_{n+1} - bR_{n+1}$$

gives (2) for $n + 1$. Consider now the system of congruences

$$\begin{aligned} G_q - a &= b \cdot R_q - a\,(1 + BR_{q-1}) \equiv 0 \quad (p^k) \\ G_{q+1} - b &= (bA - aB)\,R_q - b\,(1 + BR_{q-1}) \equiv 0 \quad (p^k) \end{aligned} \tag{3}$$

where $q = Q_k$. For the determinant E of system (3) in R_q and $1 + BR_{q-1}$ we have $-4\,E = 4\,b^2 - 4\,ab\,A + 4\,a^2\,B \equiv (2\,b - aA)^2 \not\equiv 0 \pmod p$, for if $p \mid (2\,b - aA)$, then $p \mid (2\,bA - aA^2)$ and $p \mid 2\,(bA - 2\,aB)$ against an assumption of Lemma 1. Therefore (3) has only the solution $R_q \equiv 0$, $BR_{q-1} \equiv -1 \pmod{p^k}$ or equivalently $R_q \equiv 0$, $R_{q+1} \equiv -BR_{q-1} \equiv 1 \pmod{p^k}$ showing that $P_k \mid q = Q_k$. But $Q_k \mid P_k$ is trivial from (2).

Now let x_1, x_2 be the (different) roots of $x^2 - Ax + B = 0$; then it is well known that

$$R_n = (x_1^n - x_2^n)/(x_1 - x_2) \qquad (n = 0, 1, \cdots) \tag{4}$$

and we can define the R_n by this formula also in case $n < 0$. Let us further define

$$S_n = x_1^n + x_2^n \qquad (n = 0, \pm 1, \cdots)\,. \tag{5}$$

We note here the trivial formulas

$$x_1 = (A + \sqrt{D})/2 \quad , \quad x_2 = (A - \sqrt{D})/2 \, , \tag{6}$$
$$x_1 + x_2 = A \quad , \quad x_1 x_2 = B \quad , \quad x_1 - x_2 = \sqrt{D} \, .$$

LEMMA 2. *For all rational integers n, j one has*

$$R_n = - B^n R_{-n} \quad , \quad S_n = B^n S_{-n} \tag{7}$$

$$S_n^2 = DR_n^2 + 4 B^n \tag{8}$$

$$S_n S_{n+1} = DR_n R_{n+1} + 2 AB^n \tag{9}$$

$$R_j S_n - R_n S_j = 2 R_{j-n} B^n \tag{10}$$

$$R_{j+n} = R_n S_j + B^n R_{j-n} \tag{11}$$

$$R_{jn} = 2^{1-j} R_n (jS_n^{j-1} + KR_n^2) \qquad (\textit{if } n , j \geq 0) \tag{12}$$

with a certain rational integer K.

Proof. Formulas (7) to (11) are easily proved by using (4), (5) and (6). From (4) and (5) one has

$$x_1^n = (S_n + \sqrt{D}\, R_n)/2 \quad , \quad x_2^n = (S_n - \sqrt{D}\, R_n)/2$$

and so

$$\sqrt{D}\, R_{jn} = 2^{-j} ((S_n + \sqrt{D}\, R_n)^j - (S_n - \sqrt{D}\, R_n)^j) = 2^{1-j} \sqrt{D} \sum_{\substack{k=0 \\ k \text{ odd}}}^{j} \binom{j}{k} S_n^{j-k} R_n^k D^{(k-1)/2}$$

showing (12).

REMARK. *If $n \geq 0$ then R_{nk} is a multiple of R_n for each $k = 0 , 1 , \cdots$.* This is trivially true for $k=0, 1$ and for $k \geq 2$ it is seen by induction via (11).

LEMMA 3. *Let p be a prime with $p \mid D$, $p \nmid 2B$ and in case $p = 3$ let further be $P_2 \neq P_1$ and $P_1 \neq 3$. Then $p^k \mid R_{p^k}$, but $p^{k+1} \nmid R_{p^k}$ for each $k = 1 , 2 , \cdots$.*

Proof. By induction on k. In case $k = 1$ we have $p \mid R_p$ from

$$2^{p-1} R_p = pA^{p-1} + \sum_{j=1}^{(p-1)/2} \binom{p}{2j+1} A^{p-2j-1} D^j . \tag{13}$$

If $p > 3$ then $p \left| \binom{p}{3} \right.$ and so $p^2 \nmid R_p$ in virtue of $p \nmid A$. In case $p = 3$ we have from (13) that $R_3 = A^2 - B$. Now $B \equiv 2 \pmod 3$ would imply $A^2 \equiv 2 \pmod 3$ which is impossible; so $B \equiv 1 \pmod 3$ for $3 \nmid B$. If we had $A \equiv 2 \pmod 3$ then

$$R_0 = 0 \quad , \quad R_1 = 1 \quad , \quad R_2 \equiv 2 \quad , \quad R_3 \equiv 0 \quad , \quad R_4 \equiv 1 \qquad \pmod 3$$

such that $P_1 = 3$; so $A \equiv B \equiv 1 \pmod 3$. Therefore we have $R_{n+1} \equiv R_n - R_{n-1} \pmod 3$ and $\{R_n\}$ begins with $0 , 1 , 1 , 0 , 2 , 2 , 0 , 1 , \cdots$, so $P_1 = 6$. Assume $9 \mid R_3$, then from $R_{n+1} = AR_n - BR_{n-1}$ one has

$$\{R_n \pmod 9\} : 0 , 1 , A , 0 , -AB \equiv -A^3 \equiv -1 , -A , 0 , AB \equiv 1 , \cdots ,$$

for $A^2 \equiv B \pmod 9$ by $9 \mid R_3$ and for $A^3 \equiv 1 \pmod 9$ by $A \equiv 1 \pmod 3$. So we have $P_2 = P_1$ against an assumption of Lemma 3. Thus $9 \nmid R_3$ and Lemma 3 is proved for $k = 1$. (It is easily seen that both additional assumptions in case $p = 3$ are also necessary for $9 \nmid R_3$).

Let Lemma 3 be proved for a certain $k \geq 1$, then, from (12) with $n = p^k$ $j = p$, one has

$$2^{p-1} R_{p^{k+1}} = p R_{p^k} S_{p^k}^{p-1} + K R_{p^k}^3 \equiv p R_{p^k} S_{p^k}^{p-1} \quad (p^{k+1})$$

from which Lemma 3 follows for $k+1$ in virtue of $p \nmid S_n$ for $n = 0, 1, \cdots$, since $S_n^2 \equiv 4 B^n \not\equiv 0 \pmod p$ by (8) and the assumptions on p.

LEMMA 4. *Let i, m be integers > 0 and $h \mid (R_i, R_m)$, $(h, 2B) = 1$. Then $h \mid R_{(i,m)}$.*

Proof. If $g = (i, m)$, then there are rational integers r, s such that $g = ir + ms$. Take $j = ir$, $n = -ms$ in (10) then

$$R_{ir} S_{-ms} - R_{-ms} S_{ir} = 2 R_g B^{-ms}. \tag{14}$$

Without loss of generality we may let $ir \geq ms$. If $ms \geq 0$ (so $ir > 0$) we have, from (7) and (14)

$$R_{ir} S_{ms} + R_{ms} S_{ir} = 2 R_g.$$

If $ms < 0$ (so $ir > 0$), then, by (14)

$$R_{ir} S_{m|s|} - R_{m|s|} S_{ir} = 2 R_g B^{m|s|}.$$

Now $h \mid R_i$ and $h \mid R_m$ so $h \mid R_{ir}$ and $h \mid R_{m|s|}$ (by the remark after Lemma 2). Thus $h \mid 2 R_g B^{m|s|}$ by the last two formulas. $(h, 2B) = 1$ shows $h \mid R_g$.

LEMMA 5. *Under the same assumptions of Lemma 3 $p^k \mid R_m$ implies $p^k \mid m$.*

Proof. If $m = p^t m'$ with $0 \leq t < k$ and $p \nmid m'$, then take $i = p^k$ in Lemma 4 such that $(i, m) = p^t$ and by Lemma 3, we have $p^k \mid R_i$. From this result and the assumption $p^k \mid R_m$ of Lemma 5 we get $p^k \mid R_{p^t}$ contradicting Lemma 3.

§ 3. PROOF OF THE THEOREM AND THE COROLLARIES

We show the theorem first for $k = 1$. A simple induction on s via $R_{n+1} = A R_n - B R_{n-1}$ shows that $p \mid D$ (or equivalently $A^2 \equiv 4 B \pmod p$) implies

$$R_{2s} \equiv s A B^{s-1} (p) \quad , \quad R_{2s+1} \equiv (2s+1) B^s \quad (p). \tag{15}$$

Now we assert that each of the numbers $0, \cdots, p-1$ occurs exactly $2d$ times as residue mod p of the G_n with $0 \leq n < 2dp = P_1 = Q_1$ which implies the theorem for $k = 1$. Consider first the even n, $n = 2s$, $0 \leq s < dp$ and among these exactly those p values s leaving the residue t (t fixed and $0 \leq$ $\leq t < d$) mod d; these are exactly the s-values from the set

$$M_t = \{t, t + d, t + 2d, \cdots, t + (p - 1)d\}.$$

From (1) and (15) we get

$$G_{2s} \equiv (s(bA - 2aB) + aB) B^{s-1} \quad (p). \tag{16}$$

Therefore we have: If $s, s' \in M_t$ such that $G_{2s} \equiv G_{2s'}(p)$ then

$$(s - s')(bA - 2aB) \equiv 0 \quad (p)$$

because $B^{s-1} \equiv B^{s'-1}(p)$ (for $s \equiv s'$ (d) and the definition of d). Now $p \nmid (bA - 2aB)$ implies $s \equiv s'$ (mod p) and $s, s' \in M_t$ shows $s = s'$ such that among the p numbers G_{2s} with $s \in M_t$ each residue $0, \cdots, p - 1$ occurs exactly once and among the pd numbers G_{2s}, $0 \leq s < dp$ exactly d times.

The case n odd, $n = 2s + 1$, $0 \leq s < dp$ can be treated in an analogous manner via $G_{2s+1} \equiv (2s(bA - 2aB) + bA) 4^{-1} AB^{s-1}(p)$. Thus the theorem is proved for $k = 1$.

Let $k \geq 1$ and just be proved that each of the numbers $0, \cdots, p^k - 1$ occurs exactly 2d times as residue mod p^k of the G_n with $0 \leq n < 2dp^k =$ $= P_k = Q_k$ (see Lemma 1 for $Q_k = P_k$). We show that this holds also for $k + 1$. Let s be given with $0 \leq s < p^k$ and t with $0 \leq t < P_k$ such that $G_{t+rP_k} =$ $= s + u_r p^k$. Assume that there are r, r' with $0 \leq r' < r < p$ such that $u_r \equiv u_{r'}(p)$ and so

$$p^{k+1} \mid (G_{t+rP_k} - G_{t+r'P_k}). \tag{17}$$

By (1), (11) and $P_k = 2dp^k$ we have

$$\begin{aligned} G_{t+rP_k} - G_{t+r'P_k} = {} & (B^{(r-r')dp^k} - 1)(bR_{t+r'P_k} - aBR_{t+r'P_k-1}) + \\ & + R_{(r-r')dp^k}(bS_{t+(r+r')P_k/2} - aBS_{t+(r+r')P_k/2-1}). \end{aligned} \tag{18}$$

We have $B^{dp^k} \equiv 1 (p^{k+1})$ by $B^d \equiv 1 (p)$ and further $p \nmid (bS_n - aBS_{n-1})$ for $n = 1, 2, \cdots$ since by (8), (9) and $p \mid D$

$$S_{n-1}(bS_n - aBS_{n-1}) \equiv (bA - 2aB) B^{n-1} \not\equiv 0 \quad (p).$$

So we get, from (17) and (18), $p^{k+1} \mid R_{(r-r')dp^k}$. Now from Lemma 5 we have $p \mid (r - r')d$ and so $p \mid (r - r')$ for $d \mid (p - 1)$. But this is impossible for $0 < r - r' < p$ and the contradiction shows the theorem in case $k + 1$.

To Corollary 1. In the theorem of [2] is assumed that $Q_k = (p - 1)p^k$ for $k = 1, 2, \cdots$ and we have to show: $p - 1 = 2d$, where d the order of B mod p. By $p \mid (A^2 - 4B)$, $p \nmid 2A$ and Fermats theorem we have $1 \equiv A^{p-1} \equiv 2^{p-1} B^{(p-1)/2} \equiv B^{(p-1)/2}(p)$ and so $2d \mid (p - 1)$. On the other hand taking $s = dp$ in (15) we see $R_{2dp} \equiv 0 (p)$, $R_{2dp+1} \equiv B^{dp} \equiv 1 (p)$ such that $P_1 \mid 2dp$ so $(p - 1)p = Q_1 = P_1 \mid 2dp$ and then $(p - 1) \mid 2d$.

Note that the last inequality $l < j$ on page 9 of [2] is not correct in the case $j = 1$, $p = 3$.

To Corollary 2. $A = 3$, $B = -1$ gives $D = 13$ and $(1, 1)$, $(1, 3)$, $(1, 5)$ for (a, b) gives that $bA - 2aB$ equals 5, 11, 17 respectively. Now take $p = 13$ and so $d = 2$. By $P_k = 4 \cdot 13^k$ (see the end of [2]) the condition $P_k = 2\,dp^k$ of our theorem is satisfied and the corollary is proved.

REFERENCES

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

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

[3] I. NIVEN, *Uniform distribution of sequences of integers*, «Trans. Amer. Math. Soc.», *98*, 52–61 (1961).