SOME COUNTEREXAMPLES AND PROBLEMS ON LINEAR RECURRENCE RELATIONS

DAVID SINGMASTER
American University of Beirut, Beirut, Lebanon

In [1, pp. 48-50], several false assertions are made concerning linear recurrence relations (mod m). I will give counterexamples to these and will establish one result on a stronger hypothesis. Theorems 3.6 and 3.7 of [1] are false as stated, and it is an open question what additional hypotheses are required for their validity.

Let

\[ u_{n+1} = \sum_{i=0}^{j} a_i u_{n-i} + b. \]

For a given modulus m, let \( x_n \) be the least non-negative residue of \( u_n \) (mod m). In [1], it is assumed that \( a_i \geq 0, b \geq 0 \), and

\[ (a_0, a_1, \cdots, a_j, m) = (x_0, x_1, \cdots, x_j, b, m) = 1, \]

although these hypotheses do not appear to be essential. Of course, all quantities are integers. Let \( H(m) \) be the period of \( x_n \) (mod m). The following false assertions are made in [1; (3.12), 3.6, 3.7 are his numbers]:

\( x_n \) is a purely periodic sequence, i.e.,

\[ \exists H: \forall n, k \geq 0 \quad x_{n+kH} \equiv x_n \pmod{m}. \]

Theorem 3.6 \( H(p^{e+1}) = H(p^e) \) or \( p \cdot H(p^e) \).

In the supposed proof, \( c_{ik} \) is defined by

\[ u_{i+kH} = u_i + c_{ik}p^e \]

for \( m = p^e, H = H(p^e) \). Then \( c_{ik} \geq 0 \). It is asserted that
and the proof is completely dependent on this:

**Theorem 3.7.** If

\[ H(p) = H(p^2) = \cdots = H(p^e) \neq H(p^{e+1}) , \]

then \( H(p^{e+f}) = p^f H(p^e) \).

**Example 1.** \( u_{n+1} = u_n + 2u_{n-1} \), \( u_0 = u_1 = 1 \). All hypotheses are satisfied for \( m = 2^e \). The sequence \( u_n \) is given below, together with the \( x_n \) sequences (mod 2, 4, 8, and 16).

<table>
<thead>
<tr>
<th>( n )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u_n ) (mod 2)</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>11</td>
<td>21</td>
<td>43</td>
<td>85</td>
<td>171</td>
<td>341</td>
<td>683</td>
</tr>
<tr>
<td>( x_n ) (mod 2)</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x_n ) (mod 4)</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>( x_n ) (mod 8)</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>3</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>( x_n ) (mod 16)</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>11</td>
<td>5</td>
<td>11</td>
<td>5</td>
<td>11</td>
<td>5</td>
<td>11</td>
</tr>
</tbody>
</table>

We have

\[ u_{n+1} = (2^{n+1} + (-1)^n)/3 \]

For \( e = 1 \), \( x_n \) is purely periodic with period \( H(2) = 1 \). For \( e > 1 \), we have

\[ u_0 = u_1 < u_2 < \cdots < u_e < 2^e \]

and

\[ u_{e-1} \equiv u_{e-1+2k} \pmod{2^e} , \]

and

\[ u_e \equiv u_{e+2k} \pmod{2^e} . \]

Clearly \( H(p^e) = 2 \) for \( e > 1 \), but \( x_n \) is not purely periodic. Further, for (mod 4), we have \( c_{12} = 5, c_{11} = 1, 2 \not| c_{11} \) but \( c_{12} \not\equiv 2 \cdot c_{11} \pmod{2} \).
(Of course, \( x_n \pmod{4} \)) is not purely periodic as assumed in the proof of Theorem 3.6, but we can drop the first term by shifting indices.) Equation (2) does not even hold for \( p \mid c_{11} \) since for \( x_n \pmod{2} \), we have \( c_{02} = 1, \) \( c_{01} = 0 \) but \( c_{02} \neq 2 \cdot c_{01} \pmod{2} \). Finally, we have \( H(2) \neq H(4) \), but \( H(8) \neq 4 \cdot H(2) \). So we have shown that equations (3.12) and (2) and Theorem 3.7 are false as stated.

The proper assertion for (3.12) is that \( x_n \) is \((\text{eventually})\) periodic, i.e.,

\[
\exists n_0, \exists H : \forall n \geq n_0, \forall k \geq 0 \quad x_{n+kH} \equiv x_n \pmod{m}.
\]

However, we can obtain pure periodicity under a different assumption.

**Theorem.** \( x_n \) is purely periodic \((\pmod{m})\) if \((a_j,m) = 1\).

**Proof.** Let \( n_0 \) be the least integer \( \geq 0 \) such that (3) holds. From (1) we have

\[
a_j x_{n-j} \equiv x_{n+1} - \sum_{i=0}^{j-1} a_i x_{n-i} \pmod{m}.
\]

Since \((a_j,m) = 1\), there is an \( a_j^{-1} \) such that \( a_j a_j^{-1} \equiv 1 \pmod{m} \), so we have

\[
(4) \quad x_{n-j} \equiv a_j^{-1} \left[ x_{n+1} - \sum_{i=0}^{j-1} a_i x_{n-i} - b \right] \pmod{m},
\]

That is, we can reverse the recurrence relation to get terms of smaller index from terms of larger index. If \( n_0 > 0 \), set \( n = n_0 + j - 1 \) and \( n = n_0 + kH + j - 1 \) in (4) to get

\[
(5) \quad x_{n_0-1} \equiv a_j^{-1} \left[ x_{n_0+j} - \left( \sum_{i=0}^{j-1} a_i x_{n_0+j-i-1} - b \right) \right] \pmod{m}.
\]
\( (6) \quad x_{n_0-1+kH} \equiv a_j^{-1} \left[ x_{n_0+j+kH} - \left( \sum_{i=0}^{j-1} a_i x_{n_0+j-1-i+kH} \right) - b \right] \pmod{m} \).

Now (3) shows that the right-hand sides of (5) and (6) are congruent \( \pmod{m} \), so \( x_{n_0-1} \equiv x_{n_0-1+kH} \pmod{m} \). Hence \( n_0 \) is not the least integer such that (3) holds, hence \( n_0 = 0 \), that is \( x_n \) is purely periodic \( \pmod{m} \).

In view of this result, one might ask if Theorems 3.6 and 3.7 and Eq. (2) might be valid if \( (a_j, m) = 1 \).

**Example 2.**

\[
 u_{n+1} = u_{n-2} \cdot u_0 = u_1 = 1, \quad u_2 = 3. 
\]

Again, all hypotheses are satisfied for \( m = 2^e \) and \( a_j = 1 \), so \( (a_j, m) = 1 \). The resulting sequence is \( x_n \equiv 1 \pmod{2} \) and \( x_n = u_n \pmod{2^e} \) for \( e > 1 \). \( u_n \) is given by:

<table>
<thead>
<tr>
<th>n</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u_n )</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

Clearly \( H(2) = 1, H(2^e) = 3 \) for \( e > 1 \), but \( H(2^2) \neq 2 \cdot H(2) \), so that Theorems 3.6 and 3.7 both fail. For \( p^e = 2, c_{20} = 1 \neq 2 \cdot c_{01} = 0 \pmod{2} \) and \( c_{30} = 0 \neq 3 \cdot c_{11} = 3 \pmod{2} \), so (3.12) fails here also.

Further, it is clear that this example can be modified to work for any modulus \( p^e \).

Finally, we remark that we can construct a less artificial example with similar properties from

\[
 u_{n+1} = u_n + u_{n-1} + 1, \quad u_0 = u_1 = 1. 
\]

<table>
<thead>
<tr>
<th>n</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>( u_n )</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>9</td>
<td>15</td>
<td>25</td>
<td>41</td>
<td>67</td>
<td>109</td>
<td>117</td>
</tr>
<tr>
<td>( x_n \pmod{2} )</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x_n \pmod{4} )</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>3</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>( x_n \pmod{8} )</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>1</td>
<td>7</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>1</td>
</tr>
</tbody>
</table>

[Continued on page 279.]