<table>
<thead>
<tr>
<th>Title</th>
<th>On Integers Defined by a Linear Recurrence Relation of Order Two</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>UCHIYAMA, Saburo</td>
</tr>
<tr>
<td>Citation</td>
<td>数理解析研究所講究録 (1984), 537: 35-41</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1984-10</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/2433/98697">http://hdl.handle.net/2433/98697</a></td>
</tr>
<tr>
<td>Type</td>
<td>Departmental Bulletin Paper</td>
</tr>
<tr>
<td>Textversion</td>
<td>publisher</td>
</tr>
</tbody>
</table>

Kyoto University
2次の一線型回帰数列について

— On Integers Defined by a Linear Recurrence Relation of Order Two —

筑波大 数学 内山三郎 (Saburō UCHIYAMA)

In the course of studying various Diophantine problems the writer had several occasions to encounter the sequence of so-called Pell numbers, that is, a sequence of integers $P_n$ $(n = 0, 1, 2, \ldots)$ defined by

$$P_0 = 0, \quad P_1 = 1, \quad \text{and} \quad P_{n+1} = 2P_n + P_{n-1} \quad \text{for} \quad n \geq 1.$$ 

It will be convenient to consider, together with the Pell numbers $P_n$, the associated numbers $Q_n$ $(n = 0, 1, 2, \ldots)$ defined by

$$Q_0 = 1, \quad Q_1 = 1, \quad \text{and} \quad Q_{n+1} = 2Q_n + Q_{n-1} \quad \text{for} \quad n \geq 1.$$ 

Explicit formulae for the $P_n$ and $Q_n$ are

$$P_n = \frac{1}{2\sqrt{2}} \left( (1 + \sqrt{2})^n - (1 - \sqrt{2})^n \right),$$

$$Q_n = \frac{1}{2} \left( (1 + \sqrt{2})^n + (1 - \sqrt{2})^n \right),$$

and, to collect some simple identities involving $P_n$ and $Q_n$ we note

$$(P_m, P_n) = P_{(m, n)}, \quad P_{m+n} = P_mQ_n + P_nQ_m,$$

$$Q_{m+n} = Q_mQ_n + 2P_mP_n, \quad P_n^2 - P_{n-1}P_{n+1} = (-1)^{n-1}.$$
\[ P_{2n-1} = P_n^2 + P_{n-1}^2, \quad P_{2n} = 2P_n(P_n + P_{n-1}), \]
\[ Q_n^2 - 2P_n^2 = (-1)^n. \]

Here we discuss some arithmetical properties of the (sequences of) Pell numbers \( P_n \).

1) The sequence \((P_n)_{n=1,2,...}\) is uniformly distributed modulo an integer \( m > 1 \) (in the sense of I. Niven) for \( m = 2 \) and for no other values of \( m \).

The discriminant of the characteristic polynomial of the defining relation for the \( P_n \) is \( 8 = 2^3 \). The sequence \((P_n)\) is uniformly distributed modulo 2 since
\[ P_n \equiv n \pmod{2}, \]
and is not uniformly distributed modulo \( 2^h \) for any \( h > 1 \), since
\[ P_n \equiv 0, 1, 2, \text{ or } 1 \pmod{4} \]
according as
\[ n \equiv 0, 1, 2, \text{ or } 3 \pmod{4}. \]

2) The sequence \((\log P_n)_{n=1,2,...}\) is uniformly distributed modulo 1.

This follows from the fact that we have for \( n \to \infty \)
\[ \log P_{n+1} - \log P_n \to \log (1 + \sqrt{2}) \not\in \mathbb{Q}. \]

3) The sequence \((\lfloor \log P_n \rfloor)_{n=1,2,...}\) is uniformly distributed modulo \( m \) for every integral \( m \geq 2 \).

These results can be obtained just as in L. Kuipers, J.-Sh. Shiue, and H. Niederreiter, who proved the corresponding results for the sequence of Fibonacci numbers \( F_n \).
4) By a general result of K. Nagasaka, 'Benford's Law of
Anomalous Numbers' is obeyed by the sequence \((P_n)_{n=1,2,...}\).
Thus, in particular, the frequency of appearance of a \((1 \leq a
\leq 9)\) as the left-most digit in the \(P_n\) equals \(\log_{10}(1+(1/a))\),
the \(P_n\) being expressed in the ordinary decimal system.

Here is a small numerical observation.

<table>
<thead>
<tr>
<th>digit</th>
<th>number of count ((1 \leq n \leq 100))</th>
<th>number of count ((101 \leq n \leq 200))</th>
<th>expected number (100 \log_{10}(1+\frac{1}{a}))</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30</td>
<td>31</td>
<td>30.1</td>
</tr>
<tr>
<td>2</td>
<td>19</td>
<td>17</td>
<td>17.6</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>13</td>
<td>12.5</td>
</tr>
<tr>
<td>4</td>
<td>9</td>
<td>9</td>
<td>9.7</td>
</tr>
<tr>
<td>5</td>
<td>9</td>
<td>8</td>
<td>7.9</td>
</tr>
<tr>
<td>6</td>
<td>6</td>
<td>7</td>
<td>6.7</td>
</tr>
<tr>
<td>7</td>
<td>6</td>
<td>6</td>
<td>5.8</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
<td>4</td>
<td>5.1</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
<td>5</td>
<td>4.6</td>
</tr>
</tbody>
</table>

5) It is known that \(P_1 = 1\) and \(P_7 = 169\) are the only
square Pell numbers (apart from \(P_0 = 0\)). One can hardly prove
this fact without appealing to W. Ljunggren's theorem which
states that the only solutions in positive integers \(x, y\) of
the Diophantine equation

\[x^2 - 2y^4 = -1\]

are \(x = y = 1\) and \(x = 239, y = 13\).

By the way, Ljunggren's proof for his above mentioned
result being highly complicated and difficult, there are some
authors who express their wish to have a simple and/or elemen-
tary proof of the result. We find that the problem is eventually to prove that \( X = 3, \ Y = 2 \) is the only solution in positive integers \( X, \ Y \) of the equation
\[
X^4 + 4X^3Y - 6X^2Y^2 - 4XY^3 + Y^4 = 1
\]
and that the equation
\[
X^4 - 4X^3Y - 6X^2Y^2 + 4XY^3 + Y^4 = 1
\]
has no solutions in positive integers \( X, \ Y \).

It will be of some interest to note that an application of A. Baker's argument of effectiveness yields the following upper bound for \(|X|, |Y|\), where \( X, Y \) are any possible integer solutions of these Diophantine equations:
\[
\max \ (|X|, |Y|) < \exp(3^2 \cdot 2^{3522617}) = 10^{10^{10^{10^{6.02548}}}}
\]

It is not hard to prove that \( P_0 = 0 \) is the only square value of \( P_{2n} \), that is, the equation
\[
x^2 - 2y^4 = 1
\]
adopts only trivial solutions with \( y = 0 \). In fact, we have
\[
P_{n+8} \equiv P_n \quad (\text{mod} \ 8); \text{ also } P_{n+20} \equiv P_n \quad (\text{mod} \ 29),
\]
since
\[
P_{n+20} = Q_n P_{20} + Q_{20} P_n
\]
and
\[
29 = P_5 | P_{20}, \quad Q_{20} = 22619537 \equiv 1 \quad (\text{mod} \ 29).
\]
We have, therefore,
\[
\begin{align*}
P_n & \equiv 2 \quad (\text{mod} \ 29) \quad \text{if } n \equiv 2, 8, 22, \text{ or } 28 \quad (\text{mod} \ 40), \\
P_n & \equiv 12 \quad (\text{mod} \ 29) \quad \text{if } n \equiv 4, 6, 24, \text{ or } 26 \quad (\text{mod} \ 40), \\
P_n & \equiv 27 \quad (\text{mod} \ 29) \quad \text{if } n \equiv 12, 18, 32, \text{ or } 38 \quad (\text{mod} \ 40),
\end{align*}
\]
\[ P_n \equiv 17 \pmod{29} \quad \text{if} \quad n \equiv 14, 16, 34, \text{or} \quad 36 \pmod{40}, \]
\[ P_n \equiv 2 \pmod{8} \quad \text{if} \quad n \equiv 10 \pmod{40}, \text{and} \]
\[ P_n \equiv 6 \pmod{8} \quad \text{if} \quad n \equiv 30 \pmod{40}. \]

(Note that 2, 12, 27, 17 are quadratic non-residues \( \pmod{29} \).) It remains, therefore, only to consider the values of \( P_n \) for 
\[ n \equiv 0, \text{or} \quad 20 \pmod{40}. \]

We have
\[ P_{n+10} = Q_n P_{10} + Q_{10} P_n, \]
where
\[ Q_{10} = 3363 \equiv 1 \pmod{41}, \quad P_{10} = 2378 \equiv 0 \pmod{41}. \]

Now, let \( m \) be the least positive integer such that \( P_{10m} \) is either a square or twice a square. If \( m \) is odd then
\[ P_{10m} = 2Q_{5m}P_{5m}, \]
where
\[ P_{5m} \equiv P_5 = 29 \pmod{41}, \]
29 being a quadratic non-residue \( \pmod{41} \). So \( m \) must be even, and \( P_{5m} = P_{10(m/2)} \) must be a square or twice a square, and we have a contradiction. It follows that \( m = 0, P_0 = 0 \).

6) It follows from the result of 4) above that there are no Pell numbers \( P_n \) which are twice a square, other than \( P_2 = 2 \) (and \( P_0 = 0 \)).

7) Finally, we should like to give a proof for the fact that \( Q_0 = Q_1 = 1 \) are the only numbers \( Q_n \) which are a square.

Note that \( Q_n \equiv 1 \pmod{2} \) for all \( n \). We distinguish two cases according as \( n \) is even or odd.
Case of \( n \) even: Consider the Diophantine equation

\[
x^4 - 2y^2 = 1,
\]

which can be rewritten as \((x^2 - 1)(x^2 + 1) = 2y^2\). Since \((x^2 - 1, x^2 + 1) = 2\) and \(2 \parallel x^2 + 1\), we must have \(x^2 + 1 = 2z^2\) and \(x^2 - 1 = w^2\) for some integral \(z, w\). Therefore, the only possibility is \(w = 0, x = 1, z = 1, y = 0\) (here, and in what follows also, we have only to consider non-negative values of the unknowns involved), thus giving \(Q_0 = 1\).

Case of \( n \) odd: Consider the equation

\[
x^4 - 2y^2 = -1,
\]

which we rewrite as

\[
\left(\frac{x^2 - 1}{2}\right)^2 + \left(\frac{x^2 + 1}{2}\right)^2 = y^2.
\]

Since \((x^2 - 1)/2\) and \((x^2 + 1)/2\) are coprime and \((x^2 + 1)/2\) is odd, we have for some integers \(a, b\) with \((a, b) = 1\),

\[
a + b \equiv 1 \pmod{2},
\]

\[
\frac{x^2 - 1}{2} = 2ab, \quad \frac{x^2 + 1}{2} = a^2 - b^2;
\]

this implies

\[
x^2 = a^2 - b^2 + 2ab, \quad 1 = a^2 - b^2 - 2ab
\]

and so

\[
x^2 = (a^2 - b^2)^2 - (2ab)^2.
\]

Hence we must have for some integral \(c, d\) \(2ab = 2cd\), \(x = c^2 - d^2\), \(a^2 - b^2 = c^2 + d^2\), which gives us \(l = c - d, \ x = c + d, \) where \(a \equiv c \equiv l \pmod{2}, \ b \equiv d \equiv 0 \pmod{2}\). How-
ever, it is known and in fact is not quite difficult to prove that the only integer solutions of the equation

\[ x^2 = a^4 - 6a^2b^2 + b^4, \quad (a, b) = 1, \]

are given by \( a = 0 \) or \( b = 0 \). Thus we have \( b = d = 0 \), giving \( x = c = 1 \) and so \( Q_1 = 1 \).

This completes the proof of our assertion.

References


H. Niederreiter: Distribution of Fibonacci numbers \( \mod 5^k \). Fibonacci Quart., 10, No. 4(1972), 373–374.

L. Kuipers: Remark on a paper by R. L. Duncan concerning the uniform distribution \( \mod 1 \) of the sequence of the logarithms of the Fibonacci numbers. Fibonacci Quart., 7, No. 7(1969), 465–466, 473.


