数理解析研究所講究録
第537巻 1984年 35-41

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　(Saburô 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

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

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

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

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

$$(P_m, P_n) = P_{(m,n)}, \quad P_{m+n} = P_m Q_n + P_n Q_m,$$

$$Q_{m+n} = Q_m Q_n + 2P_m P_n, \quad P_n^2 - P_{n-1}P_{n+1} = (-1)^{n-1},$$

$$P_{2n-1} = P_n^2 + P_{n-1}^2 \ , \quad P_{2n} = 2P_n(P_n + P_{n-1}) \ ,$$

$$Q_n^2 - 2P_n^2 = (-1)^n \ .$$

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

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

This follows from the fact that we have for $n \to \infty$

$$\log P_{n+1} - \log P_n \to \log(1 + \sqrt{2}) \notin Q .$$

3) The sequence $([\log P_n])_{n=1,2,\ldots}$ is uniformly distributed modulo m for every integral $m \geqq 2$.

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 $(1 \leqq a \leqq 9)$ 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.

digit a	number of count $(1 \leqq n \leqq 100)$	number of count $(101 \leqq n \leqq 200)$	expected number $100 \log_{10}(1+\frac{1}{a})$
1	30	31	30.1
2	19	17	17.6
3	11	13	12.5
4	9	9	9.7
5	9	8	7.9
6	6	7	6.7
7	6	6	5.8
8	5	4	5.1
9	5	5	4.6

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 elementary 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

$$X^4 + 4X^3Y - 6X^2X^2 - 4XY^3 + Y^4 = 1$$

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:

$$\max(|X|, |Y|) < \exp(3^2 \cdot 2^{3522617}) = 10^{10^{10^{6.02548}}}$$

It is not hard to prove that $P_0 = 0$ is the only square value of P_{2n}, that is, the equation

$$x^2 - 2y^4 = 1$$

admits only trivial solutions with $y = 0$. In fact, we have $P_{n+8} \equiv P_n \pmod 8$; also $P_{n+20} \equiv P_n \pmod{29}$, since

$$P_{n+20} = Q_n P_{20} + Q_{20} P_n$$

and

$$29 = P_5 | P_{20}, \qquad Q_{20} = 22619537 \equiv 1 \pmod{29}.$$

We have, therefore,

$$P_n \equiv 2 \pmod{29} \quad \text{if} \quad n \equiv 2, 8, 22, \text{ or } 28 \pmod{40},$$

$$P_n \equiv 12 \pmod{29} \quad \text{if} \quad n \equiv 4, 6, 24, \text{ or } 26 \pmod{40},$$

$$P_n \equiv 27 \pmod{29} \quad \text{if} \quad n \equiv 12, 18, 32, \text{ or } 38 \pmod{40},$$

$P_n \equiv 17 \pmod{29}$ if $n \equiv 14, 16, 34,$ or $36 \pmod{40}$,
$P_n \equiv 2 \pmod{8}$ if $n \equiv 10 \pmod{40}$, and
$P_n \equiv 6 \pmod{8}$ if $n \equiv 30 \pmod{40}$.

(Note that 2, 12, 27, 17 are quadratic non-residues (mod 29).) It remains, therefore, only to consider the values of P_n for

$$n \equiv 0, \text{ or } 20 \pmod{40}.$$

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

$$P_{10m} = 2\,Q_{5m}\,P_{5m} ,$$

where

$$P_{5m} \equiv P_5 = 29 \pmod{41},$$

29 being a quadratic non-residue (mod 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 $2 \| x^2 + 1$, 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 $1 = c - d$, $x = c + d$, where $a \equiv c \equiv 1 \pmod 2$, $b \equiv d \equiv 0 \pmod 2$. However, 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

I. Niven: Uniform distribution of sequences of integers. Trans. Amer. Math. Soc., 98(1961), 52 - 61.

L. Kuipers and J.-Sh. Shiue: A distribution property of the sequence of Fibonacci numbers. Fibonacci Quart., 10, No. 4(1972), 375 - 376, 392.

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.

K. Nagasaka: On Benford's law. Ann. Inst. Stat. Math., to appear.

W. Ljunggren: Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. Avh. det Norske Vid.-Akad. Oslo. I. Mat.-Naturvid. Klasse, nr. 5(1942). Especially, § 2.

A. Baker: Contributions to the theory of Diophantine equations.
I. On the representation of integers by binary forms.
II. The Diophantine equation $y^2 = x^3 + k$.
Phil. Trans. Roy. Soc. London, Ser. A., 263(1968), 173 - 191, 193 - 208.

L. J. Mordell: Diophantine Equations. Pure and Appl. Math. Vol. 30. Academic Press, London and New York 1969. Cf. Chap. 4, Theorem 3 (pp. 18 - 19).