PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 56, April 1976

POLYNOMIAL PELL'S EQUATIONS

MELVYN B. NATHANSON

ABSTRACT. The polynomial Pell's equation is $P^2 - (x^2 + d)Q^2 = 1$, where d is an integer and the solutions P, Q must be polynomials with integer coefficients. It is proved that this equation has nonconstant solutions if and only if $d = \pm 1, \pm 2$, and in these cases all solutions are determined.

Let d be an integer. We consider the polynomial Pell's equation

$$P^2 - (x^2 + d)Q^2 = 1 \tag{1}$$

where P and Q are polynomials with integer coefficients. This equation always has the trivial solutions $P = \pm 1$, $Q = 0$, and these are the only constant solutions. In this note we prove that (1) has nontrivial solutions if and only if $d = \pm 1, \pm 2$, and in these cases we determine all solutions. This answers a question posed by S. Chowla.

Lower case letters ($\neq x$) denote integers, and upper case letters denote polynomials with integer coefficients. The degree of F is denoted deg F.

THEOREM 1. *Let $d \neq \pm 1, \pm 2$. Then the polynomial Pell's equation $P^2 - (x^2 + d)Q^2 = 1$ has no nontrivial solution.*

PROOF. The proof is by Fermat descent on deg P. Let $|d| \geqslant 3$, and suppose that (1) has nontrivial solutions. Choose a solution P, Q of (1) with deg P minimal and deg $P > 0$. There are two cases. If $d \neq -c^2$, then $x^2 + d$ is irreducible, and

$$(P - 1)(P + 1) = P^2 - 1 = (x^2 + d)Q^2.$$

It follows that $x^2 + d$ divides $P - 1$ or $P + 1$, say $P - 1$. Then $P - 1 = (x^2 + D)P_1$ and $P + 1 = (x^2 + d)P_1 + 2$, and so

$$P_1((x^2 + d)P_1 + 2) = Q^2. \tag{2}$$

Since the greatest common divisor of P_1 and $(x^2 + d)P_1 + 2$ is 1 or 2, it follows from (2) that one of the following four cases must hold:

(i) $(x^2 + d)P_1 + 2 = -P_2^2$, $P_1 = -Q_2^2$;

(ii) $(x^2 + d)P_1 + 2 = P_2^2$, $P_1 = Q_2^2$;

(iii) $(x^2 + d)P_1 + 2 = -2P_2^2$, $P_1 = -2Q_2^2$;

(iv) $(x^2 + d)P_1 + 2 = 2P_2^2$, $P_1 = 2Q_2^2$. Setting $x = \sqrt{-d}$ in (i), (ii), (iii), we find that $(a + b\sqrt{-d})^2 = \pm 2$ or $(a + b\sqrt{-d})^2 = -1$ for some integers a,

Received by the editors July 1, 1975.

AMS (MOS) subject classifications (1970). Primary 10B05, 12A20.

Key words and phrases. Pell's equations, polynomial diophantine equations.

b. But for $d \neq -c^2$, $|d| \geqslant 3$, this is impossible. Hence, (iv) must hold. Rewriting (iv), we obtain $P_2^2 - (x^2 + d)Q_2^2 = 1$. But $2 \deg P_2 = 2 + \deg P_1 = \deg P$, and so $0 < \deg P_2 < \deg P$. This contradicts the minimality of $\deg P$. Therefore, (1) has no nontrivial solutions if $|d| \geqslant 3$ and $d \neq -c^2$.

Suppose that $d = -c^2$ and $|c| \geqslant 2$. Then $P(0)^2 + c^2 Q(0)^2 = 1$, and so $Q(0) = 0$ and $P(0) = \pm 1$, say, $P(0) = 1$. Then $P = 1 + xP_1$ and $Q = xQ_1$. Substituting into (1), we obtain

$$P_1(xP_1 + 2) = x(x^2 - c^2)Q_1^2.$$

Clearly, $P_1 = xP_2$, and so

$$P_2(x^2 P_2 + 2) = (x^2 - c^2)Q_1^2. \tag{3}$$

Suppose $x \pm c$ divides $x^2 P_2 + 2$. Setting $x = \mp c$, we obtain $c^2 P_2(\mp c) + 2 = 0$, and so c^2 divides 2. This is impossible, since $c^2 \geqslant 4$. Therefore, both $x + c$ and $x - c$ divide P_2, and $P_2 = (x^2 - c^2)P_3$. Substituting into (3), we obtain

$$P_3(x^2(x^2 - c^2)P_3 + 2) = Q_1^2.$$

Again, the greatest common divisor of P_3 and $x^2(x^2 - c^2)P_3 + 2$ is 1 or 2, and the proof continues exactly as in the case $|d| \geqslant 3$, $d \neq -c^2$.

Finally, let $d = 0$. If $1 = P^2 - x^2 Q^2 = (P - xQ)(P + xQ)$, then $P - xQ = P + xQ = \pm 1$. Adding these equations gives the trivial solutions $P = \pm 1$, $Q = 0$. This proves Theorem 1 in all cases.

THEOREM 2. *Let $d = 1$ or $d = \pm 2$. Define inductively two sequences of polynomials $\{P_n\}_{n=0}^{\infty}$ and $\{Q_n\}_{n=0}^{\infty}$ by $P_0 = 1$, $Q_0 = 0$, and, for $n \geqslant 1$,*

$$P_n = ((2/d)x^2 + 1)P_{n-1} + (2/d)x(x^2 + d)Q_{n-1},$$
$$Q_n = (2/d)xP_{n-1} + ((2/d)x^2 + 1)Q_{n-1}.$$

Then $P^2 - (x^2 + d)Q^2 = 1$ if and only if $P = \pm P_n$ and $Q = \pm Q_n$ for some n.

PROOF. The proof uses a continued fraction recurrence. Let P and Q be polynomials. We define polynomials $\Phi^+(P)$ and $\Phi^+(Q)$ by

$$\Phi^+(P) = \left(\frac{2}{d}x^2 + 1\right)P + \frac{2}{d}x(x^2 + d)Q, \quad \Phi^+(Q) = \frac{2}{d}xP + \left(\frac{2}{d}x^2 + 1\right)Q$$

and we define polynomials $\Phi^-(P)$ and $\Phi^-(Q)$ by

$$\Phi^-(P) = \left(\frac{2}{d}x^2 + 1\right)P - \frac{2}{d}x(x^2 + d)Q, \quad \Phi^-(Q) = -\frac{2}{d}xP + \left(\frac{2}{d}x^2 + 1\right)Q.$$

One checks by direct computation that

$$\Phi^+\Phi^-(P) = \Phi^-\Phi^+(P) = P, \tag{4}$$

$$\Phi^+\Phi^-(Q) = \Phi^-\Phi^+(Q) = Q, \tag{5}$$

$$\begin{aligned}(\Phi^+(P))^2 - (x^2 + d)(\Phi^+ Q)^2 &= (\Phi^-(P))^2 - (x^2 + d)(\Phi^- Q)^2 \\ &= P^2 - (x^2 + d)Q^2.\end{aligned} \tag{6}$$

Since $P_0^2 - (x^2 + d)Q_0^2 = 1$, and $P_n = \Phi^+(P_{n-1})$ and $Q_n = \Phi^+(Q_{n-1})$ for $n \geqslant 1$, it follows from (6) that $P_n^2 - (x^2 + d)Q_n^2 = 1$ for all n.

We show by induction on $m = \deg P$ that if $P^2 - (x^2 + d)Q^2 = 1$, then $P = \pm P_n$ and $Q = \pm Q_n$ for some n.

Clearly, if $m = 0$, then $P = \pm 1 = \pm P_0$ and $Q = 0 = Q_0$.

If $m = 1$, then $P = p_0 x + p_1$ and $Q = q_0$, where $p_0 \neq 0$. Substituting into (1), we obtain

$$\begin{aligned} P^2 - (x^2 + d)Q^2 &= (p_0 x + p_1)^2 - (x^2 + d)q_0^2 \\ &= (p_0^2 - q_0^2)x^2 + 2p_0 p_1 x + (p_1^2 - dq_0^2) = 1. \end{aligned}$$

Since $2p_0 p_1 = 0$ and $p_0 \neq 0$, we have $p_1 = 0$. Then $1 = p_1^2 - dq_0^2 = -dq_0^2$. But this is impossible for $d = 1$ or $d = \pm 2$. Therefore, (1) has no solutions with $m = \deg P = 1$.

Let $m \geqslant 2$. Suppose that $P^2 - (x^2 + d)Q^2 = 1$, where $\deg P = m$. Multiplying P and Q by ± 1 if necessary, we can assume that

$$\begin{aligned} P &= p_0 x^m + p_1 x^{m-1} + p_2 x^{m-2} + \cdots + p_m, \\ Q &= q_0 x^{m-1} + q_1 x^{m-2} + \cdots + q_{m-1}, \end{aligned}$$

where $p_0 \geqslant 1$ and $q_0 \geqslant 1$. Squaring P and Q and collecting terms, we obtain

$$\begin{aligned} 1 &= P^2 - (x^2 + d)Q^2 \\ &= (p_0^2 - q_0^2)x^{2m} + 2(p_0 p_1 - q_0 q_1)x^{2m-1} \\ &\quad + (p_1^2 + 2p_0 p_2 - q_1^2 - 2q_0 q_2 - dq_0^2)x^{2m-2} \\ &\quad + 2(p_0 p_3 + p_1 p_2 - q_0 q_3 - q_1 q_2 - dq_0 q_1)x^{2m-3} + \cdots + (p_m^2 - dq_{m-1}^2). \end{aligned}$$

The constant term equals 1, and the coefficients of all positive powers of x equal 0. Thus,

$$p_0 = q_0, \tag{7}$$

$$p_1 = q_1, \tag{8}$$

$$2p_2 = 2q_2 + dq_0, \tag{9}$$

$$2p_3 = 2q_3 + dq_1, \tag{10}$$

$$p_m^2 - dq_{m-1}^2 = 1. \tag{11}$$

In particular, if $m = 2$, conditions (7)–(11) imply that $P = \pm((2/d)x^2 + 1) = \pm P_1$ and $Q = \pm 2x/d = \pm Q_1$.

We make the induction hypothesis that if $P^2 - (x^2 + d)Q^2 = 1$ and $\deg P < m$, then $P = \pm P_{n-1}$ and $Q = \pm Q_{n-1}$ for some $n \geqslant 1$. Suppose that $\deg P = m$. Then

$$\begin{aligned}\Phi^- P &= ((2/d)x^2 + 1)P - (2/d)x(x^2 + d)Q \\ &= (2/d)(p_0 - q_0)x^{m+2} + (2/d)(p_1 - q_1)x^{m+1} \\ &\quad +((2/d)p_2 + p_0 - (2/d)q_2 - 2q_0)x^m \\ &\quad +((2/d)p_3 + p_1 - (2/d)q_3 - 2q_1)x^{m-1} + \cdots .\end{aligned}$$

It follows from conditions (7)–(10) that $\deg \Phi^- P \leqslant m - 2$. By (6), we have $(\Phi^- P)^2 - (x^2 + d)(\Phi^- Q)^2 = 1$. Then by the induction hypothesis we know that $\Phi^- P = \pm P_{n-1}$ and $\Phi^- Q = \pm Q_{n-1}$ for some $n \geqslant 1$. Then (4) and (5) imply that $P = \Phi^+\Phi^- P = \pm\Phi^+ P_{n-1} = \pm P_n$ and $Q = \Phi^+\Phi^- Q = \pm\Phi^+ Q_{n-1} = \pm Q_n$. This concludes the proof.

THEOREM 3. *Define inductively two sequences of polynomials* $\{P_n\}_{n=0}^{\infty}$ *and* $\{Q_n\}_{n=0}^{\infty}$ *by* $P_0 = 1$, $Q_0 = 0$, *and, for* $n \geqslant 1$,

$$P_n = xP_{n-1} + (x^2 - 1)Q_{n-1}, \qquad Q_n = P_{n-1} + xQ_{n-1}.$$

Then $P^2 - (x^2 - 1)Q^2 = 1$ *if and only if* $P = \pm P_n$ *and* $Q = \pm Q_n$ *for some* n.

PROOF. Let P and Q be polynomials. We define polynomials $\Psi^+ P$ and $\Psi^- P$ by

$$\Psi^+ P = xP + (x^2 - 1)Q, \qquad \Psi^+ Q = P + xQ,$$

and we define polynomials $\Psi^- P$ and $\Psi^- Q$ by

$$\Psi^- P = xP - (x^2 - 1)Q, \qquad \Psi^- Q = -P + xQ.$$

One computes directly that

$$\Psi^+\Psi^- P = \Psi^-\Psi^+ P = P, \tag{12}$$

$$\Psi^+\Psi^- Q = \Psi^+\Psi^- Q = Q, \tag{13}$$

$$\begin{aligned}(\Psi^+ P)^2 - (x^2 + 1)(\Psi^+ Q)^2 &= (\Psi^- P)^2 - (x^2 + 1)(\Psi^- Q)^2 \\ &= P^2 - (x^2 + 1)Q^2.\end{aligned} \tag{14}$$

Since $P_0^2 - (x^2 + 1)Q_0^2 = 1$, and $P_n = \Psi^+ P_{n-1}$ and $Q_n = \Psi^+ Q_{n-1}$, it follows from (14) that $P_n^2 - (x^2 + 1)Q_n^2 = 1$ for all n. The proof that every solution of $P^2 - (x^2 + 1)Q^2 = 1$ is of the form $P = \pm P_n$, $Q = \pm Q_n$ is exactly like the proof of Theorem 2.

It is an open problem to determine the polynomials D for which the polynomial Pell's equation $P^2 - DQ^2 = 1$ has nontrivial solutions.

ADDED IN PROOF. David Zeitlin (personal communication) has observed that the solutions of the polynomial Pell's equations can all be neatly expressed in terms of the Chebyshev polynomials $T_n(x)$ and $U_n(x)$.

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540

DEPARTMENT OF MATHEMATICS, SOUTHERN ILLINOIS UNIVERSITY, CARBONDALE, ILLINOIS 62901

Current address: Department of Mathematics, Brooklyn College (CUNY), Brooklyn, New York 11210