ON PELL NUMBERS OF THE FORM PX^2, WHERE P IS PRIME

NEVILLE ROBBINS
San Francisco State University, San Francisco, CA 94132
(Submitted February 1983)

INTRODUCTION

Let n be a natural number, p a prime. Following Lucas [4], let A and B be integers such that

(i) $(A, B) = 1$ and $D = A^2 + 4B \neq 0$.

Let the roots of (ii) $x^2 = Ax + B$ be

(iii) $a = \frac{1}{2}(A + D^{1/2})$, $b = \frac{1}{2}(A - D^{1/2})$.

Consider the sequences

(iv) $u_n = (a^n - b^n)/(a - b)$, $v_n = a^n + b^n$.

If $A = B = 1$, then u_n, v_n are the Fibonacci and Lucas sequences, respectively. If $A = 3$ and $B = -2$, then u_n, v_n are the Mersenne and Fermat sequences, respectively. If $A = 2$ and $B = 1$ (so that $D = 8$), then u_n is called the Pell sequence (see [4, p. 187]), and is denoted P_n; v_n may be called the secondary Pell sequence, and denoted R_n, following [7]. For the sake of convenience, we occasionally write $u(n)$ instead of u_n and $P(n)$ instead of P_n. Table 1, below, lists P_n and R_n for $1 \leq n \leq 50$.

TABLE 1

n	P_n	R_n
1	1	2
2	2	6
3	5	14
4	12	34
5	29	82
6	70	198
7	169	478
8	408	1154
9	985	2786
10	2378	6726
11	5741	16238
12	13860	39202
13	33461	94642
14	80782	228486
15	195025	551614
16	470832	1331714
17	1136689	3215042
18	2744210	7761798
19	6625109	18738638
20	15994428	45239074
21	38613965	109216786

TABLE 1 (continued)

n	P_n	R_n
22	93222358	263672646
23	225058681	636562078
24	543339720	1536796802
25	1311738121	3710155682
26	3166815962	8957108166
27	7645370045	21624372014
28	18457556052	52205852194
29	44560482149	126036076402
30	107578520350	304278004998
31	259717522849	734592086398
32	627013566048	1773462177794
33	1513744654945	4281516441986
34	3654502875938	10336495061766
35	8822750406821	24954506565518
36	21300003689580	60245508192802
37	51422757785981	145445522951122
38	124145519261542	351136554095046
39	299713796309065	847718631141214
40	723573111879672	2046573816377474
41	1746860020068409	4940866263896162
42	4217293152016490	11928306344169798
43	10181446324101389	28797478952235758
44	24580185800219268	69523264248641314
45	59341817924539925	167844007449518386
46	143263821649299118	405211279147678086
47	345869461223138161	978266565744874558
48	835002744095575440	2361744410637427202
49	2015874949414289041	5701755387019728962
50	4866752642924153522	13765255184676885126

All solutions of the Pell equations $x^2 - 2y^2 = \pm 1$ such that $x \geqslant y \geqslant 0$ are given, respectively, by

$$(x_n, y_n) = \left(\frac{1}{2}R_{2n}, P_{2n}\right), \left(\frac{1}{2}R_{2n-1}, P_{2n-1}\right).$$

Furthermore, if $(x, x+1, z)$ is a Pythagorean triple, then there exists n such that $z = P_{2n+1}$, while

$$\{x, x+1\} = \{P_{n+1}^2 - P_n^2, 2P_nP_{n+1}\}.$$

These results follow from [8, pp. 44-48 and 94-98].

In [3], W. Ljunggren proved that if $x \geqslant y \geqslant 0$ and $x^2 - 2y^4 = -1$, then

$$(x, y) = (1, 1) \text{ or } (239, 13).$$

From this result, it follows that if $P_n = x^2$ with $x > 0$, then

$$(n, x) = (1, 1) \text{ or } (7, 13).$$

In this article, we consider the equation:

$$P_n = px^2. \qquad (*)$$

ON PELL NUMBERS OF THE FORM PX^2, WHERE P IS PRIME

We obtain all solutions such that $p \equiv 3 \pmod 4$ or $p < 1000$. The method used here is similar to the method used in [6] to find Fibonacci numbers of the same form. (m/p) is the Legendre symbol.

Definition 1: $z(n) = \min\{k : n \mid u_k\}$; $z^*(n) = \min\{k : n \mid P_k\}$.

Definition 2: $y(p)$ is the least prime divisor of $z(p)$.

PRELIMINARY RESULTS

(1) $z^*(2) = 2$

(2) $z^*(3) = 4$

(3) $z^*(5) = 3$

(4) $z^*(7) = 6$

(5) $z^*(13) = z^*(13^2) = 7$

(6) $z^*(29) = 5$

(7) If $D \neq s^2$, then $z(p) \mid (p - e)$, where $e = \begin{cases} (D/p) & \text{if } p \nmid D \\ 0 & \text{if } p \mid D \end{cases}$

(8) $p \mid u_n$ iff $z(p) \mid n$; $p \mid P_n$ iff $z^*(p) \mid n$

(9) $P_{2n+1} = P_n^2 + P_{n+1}^2$

(10) $(P_m, P_n) = P_{(m, n)}$

(11) $P_{2n} = P_n R_n$

(12) $(P_n, R_n) = \begin{cases} 1 & \text{if } n \text{ is odd} \\ 2 & \text{if } n \text{ is even} \end{cases}$

(13) $R_n \equiv 2 \pmod 4$ for all n

(14) $\left(\frac{1}{2}R_n\right)^2 - 2P_n^2 = (-1)^n$

(15) $u_n \mid u_{kn}$; $P_n \mid P_{kn}$

(16) If m is odd, then $R_n \neq ms^2$

(17) If $p \equiv 3 \pmod 4$, then $z^*(p)$ is even

(18) $(u_n, u_{kn}/u_n) \mid k$; $(P_n, P_{kn}/P_n) \mid k$

(19) If $x^4 - 2y^2 = (-1)^n$, then n is odd and $x^2 = y^2 = 1$

(20) $R_n = 2x^2$ implies $n = 1$

(21) $P_n = x^2$ implies $n = 1$ or 7

(22) If p is odd and $p^k \| u_n$, then $p^{k+1} \| u_{pn}$

Remarks: Results (1) through (6) may be verified by examining the first seven entries in Table 1. (7) through (15) are elementary and/or well known. (16) follows from (13). (17) follows from (9), (10), Definition 1, and [2, Theorem 367, p. 299]. (18) is Theorem 2 in [5]. (19) is proved in [8, p. 98]. (20) follows from (14) and (19). (21) follows from (14) and the result of Ljunggren mentioned above. (22) follows from [1, Theorem X, p. 42].

THE MAIN THEOREMS

Theorem 1

$P_n = 2x^2$ implies $n = 2$.

Proof: Hypothesis, (1), and (8) imply $n = 2m$, so that (11) implies

$$P_m R_m = 2x^2.$$

If m is even, then (12) implies

$$\left(\frac{1}{2}P_m, \frac{1}{2}R_m\right) = 1.$$

But

$$\left(\frac{1}{2}P_m\right)\left(\frac{1}{2}R_m\right) = 2\left(\frac{1}{2}x\right)^2.$$

Now (13) implies $\frac{1}{2}R_m = s^2$, so that (20) implies $m = 1$, a contradiction. If m is odd, then (12) and (16) imply $P_m = r^2$, $R_m = 2s^2$. Now (20) implies $m = 1$, so $n = 2$.

Theorem 2

If p is odd and $P_{2m} = px^2$, then $p = 3$ and $2m = x^2 = 4$.

Proof: Hypothesis and (11) imply $P_m R_m = px^2$. If m is odd, then (12) implies $R_m = s^2$ or ps^2, contradicting (16). If m is even, then (12) implies

$$\left(\frac{1}{2}P_m, \frac{1}{2}R_m\right) = 1.$$

But

$$\left(\frac{1}{2}P_m\right)\left(\frac{1}{2}R_m\right) = p\left(\frac{1}{2}x\right)^2.$$

Therefore, P_m or $R_m = 2s^2$. Now (20) and Theorem 1 imply $m = 2$, so that

$$P_{2m} = P_4 = 12 = 3(2)^2.$$

Corollary 1

If p is odd, $z^*(p)$ is even, and $P_n = px^2$, then $p = 3$ and $n = x^2 = 4$.

Proof: Hypothesis and (8) imply n is even, so that the conclusion follows from Theorem 2.

Corollary 2

If $p \equiv 3 \pmod 4$ and $P_n = px^2$, then $p = 3$ and $n = x^2 = 4$.

Proof: Follows from hypothesis, (17), and Corollary 1.

If $p \geq 5$, then the investigation of (*) is facilitated by Lemmas 1 and 2 below, which hold for general sequences u_n, v_n which satisfy (i) through (iv) above, where $D \neq s^2$.

Lemma 1

Suppose p is odd, $p\nmid m$, and $c_i = u(mp^i)/u(mp^{i-1})$ for $i \geq 1$. If $i < j$, then

$$(c_i, c_j) = \begin{cases} p & \text{if } p \mid D \\ 1 & \text{if } p \nmid D. \end{cases}$$

Proof: Let $d = (c_i, c_j)$, where $i < j$. Therefore, $d \mid c_i$, $d \mid c_j$, and $d \mid u(mp^i)$. Now hypothesis and (15) imply $d \mid u(mp^{j-1})$, so

$$d \mid (u(mp^{j-1}), u(mp^j)/u(mp^{j-1})).$$

Therefore, (18) implies $d \mid p$. If $p \nmid D$, then (7) and (8) imply $p \nmid u(p)$, so that (15) implies $p \nmid u(mp^i)$. Therefore, $p \nmid d$, so $d = 1$. If $p \mid D$, then (7) and (8) imply $p \mid u(p)$. Now (22) implies $p \mid c_i$ and $p \mid c_j$, so $p \mid d$, and $d = p$.

Lemma 2

If $u_n = px^r$, $y(p) = q$, a prime, and $(pq, D) = 1$, then $n = q^k m$, where $k \geq 1$ and $(s, m) = 1$ for all primes, s, such that $s \leq q$, and, furthermore, $p \nmid u_m$. If also $q \nmid u_m$, then $u_m = c^r$ and there is an integer, t, such that $1 \leq t \leq k$, and for all j such that $1 \leq j \leq k$, we have

$$u(mq^j)/u(mq^{j-1}) = \begin{cases} px_j^r & \text{if } j = t \\ x_j^r & \text{if } j \neq t. \end{cases}$$

Proof: Hypothesis, (8), and Definitions 1 and 2 imply $n = q^k m$, $k \geq 1$, and $(s, m) = 1$ for all primes, s, such that $s \leq q$. (8) implies $p \nmid u_m$. Let

$$d = (u_m, u_n/u_m).$$

If $q \nmid u_m$, then (18) implies $d = 1$. Since $(u_m)(u_n/u_m) = px^r$, we have $u_m = c^r$ and $u_n/u_m = pw^r$. For each j such that $1 \leq j \leq k$, let $a_j = u(mq^j)/u(mq^{j-1})$. Now

$$u_n/u_m = \prod_{j=1}^{k} a_j,$$

so that

$$(1/p) \prod_{j=1}^{k} a_j = w^r.$$

Lemma 1 implies the factors on the left side of this last equation are pairwise coprime; the conclusion now follows.

Theorem 3

If $P_n = 5x^2$, then $n = 3$.

Proof: Hypothesis, (3), (8), and Lemma 2 imply $n = 3^k m$ and $(6, m) = 1$. Therefore, (2) and (8) imply $3 \nmid P_m$. Now Lemma 2 implies $P_m = s^2$, so (21) implies $m = 1$ or 7. Lemma 2 implies $P_{3m}/P_m = s^2$ or $5s^2$. Since $P_{21}/P_7 = 5*45697 \neq s^2, 5s^2$, we must have $m = 1$. If $k \geq 2$, then Lemma 2 implies $197 = P_9/P_3 = s^2$, an impossibility. Therefore, $k = 1$, so $n = 3$.

Theorem 4

If $P_n = 29x^2$, then $n = 5$.

Proof: Hypothesis, (6), (8), and Lemma 2 imply $n = 5^k m$ and $(30, m) = 1$. Therefore, (3) and (8) imply $5 \nmid P_m$. Now Lemma 2 implies $P_m = s^2$, so (21) implies $m = 1$ or 7. Lemma 2 implies $P_{5m}/P_m = s^2$ or $29s^2$. Since

$$P_{35}/P_7 = 29*1800193921 \neq s^2, 29s^2,$$

we must have $m = 1$. If $k \geq 2$, then Lemma 2 implies $45232349 = P_{25}/P_5 = s^2$, an impossibility. Therefore, $k = 1$, so $n = 5$.

Lemma 3

If $P_n = px^2$, where $n = 7^k m$, $k \geq 1$, and $(14, m) = 1$, then $P_m = px_1^2$.

Proof: Let $d = (P_m, P_n/P_m)$. Hypothesis, (4), and (8) imply $7 \nmid P_m$, so $7 \nmid d$. Now (18) implies $d = 1$, so $P_m = x_1^2$ or px_1^2. If $P_m = x_1^2$, then hypothesis and (21) imply $m = 1$, so $n = 7^k$. Since

$$P_7 = 13^2 \neq px_1^2,$$

we must have $k \geq 2$. But then Lemma 2 implies

$$293*40710764977973 = P_{49}/P_7 = x_2^2 \text{ or } px_2^2,$$

an impossibility. Therefore, we must have $P_m = px_1^2$.

Corollary 3

$P_n \neq 13x^2$.

Proof: If $P_n = 13x^2$, then (5) and (8) imply $n = 7^k m$, $7 \nmid m$. Theorem 2 implies m is odd, so Lemma 3 implies $P_m = 13x_1^2$, contradicting (5) and (8).

Theorem 5

Let $P_n = px^2$, where p and $z^*(p)$ are odd. Then there exists a prime, t, such that $P_t = py^2$. In fact, $t = z^*(p)$.

Proof: If n is prime, then $t = n$ and $x^2 = y^2$. Therefore, assume n is composite. Hypothesis and Theorem 2 imply n is odd. (1) and (8) imply P_n is odd, so x is odd. If $n = 7^k m$, $7 \nmid m$, then Hypothesis and Lemma 3 imply $P_m = px_1^2$. So without loss of generality assume $7 \nmid n$, so that if $d|n$, then $d \neq 7$.

Case 1 Suppose there exists d such that $d|n$, $1 < d < n$, and $z^*(p) \nmid d$. Then (8) implies $p \nmid P_d$. Since $d \neq 7$, (21) implies $P_d \neq s^2$. Therefore, there exists a prime, q_1, such that $q_1 \neq p$ and $q_1^{2j_1-1} \| P_d$. Now, (15) implies $q_1^{2j_1-1} | P_n$, so that $q_1^{2j_1-1} | x^2$. This implies that $q_1^{2j_1} | x^2$, so that $q_1^{2j_1} | P_n$. But (22) implies $q_1^{j_1} \| P_{dq_1}$. Therefore, $q_1^{2j_1} | (P_n, P_{dq_1})$. Now, (10) implies $q_1^{2j_1} | P_{(n, dq_1)}$. Since $q_1^{2j_1-1} \| P_d$, we must have $(n, dq_1) > d$, so that $(n/d, q_1) > 1$. Therefore, $q_1 | n/d$ and $q_1 | n$. Since $q_1 \neq 7$, (21) implies $P(q_1) \neq s^2$. Thus, there exists a prime, q_2, such that $q_2^{2j_2-1} \| P(q_1)$. If the only such prime is p, then

$$P(q_1) = p^{2j_2-1}s^2 = p(p^{j_2-1}s)^2,$$

so that $t = q_1$. If $q_2 \neq p$, then $q_2^{2j_2-1} \mid x^2$, so that by reasoning as above we obtain $q_2 \mid n$. Continuing in like fashion, we obtain a sequence of primes: q_1, q_2, q_3, etc., such that $q_i \mid P(q_{i-1})$ and either $q_i \mid n$ or $q_i = p$ for $i \geqslant 2$. Since the q_i are all odd, (7) and (8) imply $q_i \neq q_{i-1}$. Now (10) implies that the q_i are all distinct. Since n has only finitely many divisors, there must exist r such that $q_r = p$, and thus $q_{r-1} = t$.

Case 2 Suppose that $z^*(p) \mid d$ for all d such that $d \mid n$ and $1 < d < n$. Then $z^*(p) = q$ is a prime and $n = q^k$. Now Lemma 2 implies $P_q = x_1^2$ or px_1^2. (21) implies $P_q \neq x_1^2$, so $P_q = px_1^2$ and $t = q$. In either case, since $p \mid P_t$, (8) implies $z^*(p) \mid t$. Since t is prime, we must have $z^*(p) = t$.

Lemma 4

Suppose $z^*(p) = q$, a prime, and $q > 3$. If $p \equiv \pm 2 \pmod 5$, then

$$\left(\frac{p^{-1}P_q}{5}\right) = -1;$$

if $p \equiv 3, 5, \text{ or } 6 \pmod 7$, then

$$\left(\frac{p^{-1}P_q}{7}\right) = -1.$$

Proof: Hypothesis implies $q \equiv \pm 1 \pmod 6$, so that $P_q \equiv \pm 1 \pmod 5$ and $P_q \equiv 1 \pmod 7$. If $p \equiv \pm 2 \pmod 5$, then

$$\left(\frac{p^{-1}P_q}{5}\right) = \left(\frac{p^{-1}}{5}\right)\left(\frac{P_q}{5}\right) = \left(\frac{p}{5}\right)\left(\frac{P_q}{5}\right) = (-1)1 = -1.$$

If $p \equiv 3, 5, \text{ or } 6 \pmod 7$, then

$$\left(\frac{p^{-1}P_q}{7}\right) = \left(\frac{p^{-1}}{7}\right)\left(\frac{P_q}{7}\right) = \left(\frac{p}{7}\right)\left(\frac{P_q}{7}\right) = (-1)1 = -1.$$

Lemma 5

Suppose $z^*(p) = q$, a prime, and $q > 3$. If either

(i) $\left(\frac{p}{11}\right) = -1$ and $q \equiv \pm 1 \text{ or } \pm 7 \pmod{24}$, or

(ii) $\left(\frac{p}{11}\right) = 1$ and $q \equiv \pm 5 \text{ or } \pm 11 \pmod{24}$,

then $\left(\frac{p^{-1}P_q}{11}\right) = -1$.

Proof: If (i) holds, then $P_q \equiv 1 \text{ or } 4 \pmod{11}$, so $\left(\frac{P_q}{11}\right) = 1$; if (ii) holds,

then $P_q \equiv 7$ or $10 \pmod{11}$, so $\left(\frac{P_q}{11}\right) = -1$. Therefore,

$$\left(\frac{p^{-1}P_q}{11}\right) = \left(\frac{p^{-1}}{11}\right)\left(\frac{P_q}{11}\right) = \left(\frac{p}{11}\right)\left(\frac{P_q}{11}\right) = (-1)1 \text{ or } 1(-1) = -1.$$

Theorem 6

If $P_n = px^2$ and $p < 1000$, then $(n, p) = (2, 2), (4, 3), (3, 5)$, or $(5, 29)$.

Proof: By Theorems 1, 3, 4, and 5, and Corollaries 2 and 3, we need only consider those primes p, such that $37 \leqslant p < 1000$, $p \equiv 1 \pmod 4$, and $z^*(p) = q$ is prime. Examining Table 2 below, we see that these primes are:

37, 61, 137, 157, 229, 277, 397, 421, 541, 569, 593,
613, 661, 677, 733, 757, 821, 853, 857, 877, 997.

Lemma 4 implies that $p^{-1}P_q$ is a quadratic nonresidue (mod 5) or (mod 7) except for $p = 421$, 541, 569, and 821. In each of these four latter cases, Lemma 5 implies that $p^{-1}P_q$ is a quadratic nonresidue (mod 11). Therefore, in no case does $P_q = px^2$.

TABLE 2

PELL ENTRY POINTS OF PRIMES, p, SUCH THAT $p \equiv 1 \pmod 4$, $p < 1000$

p	$z^*(p)$	p	$z^*(p)$	p	$z^*(p)$	p	$z^*(p)$
5	3	197	9	433	216	709	355
13	7	229	23	449	224	733	367
17	8	233	116	457	114	757	379
29	5	241	40	461	231	761	190
37	19	257	64	509	255	769	384
41	10	269	15	521	65	773	129
53	27	277	139	541	271	797	399
61	31	281	140	557	279	809	202
73	36	293	49	569	71	821	137
89	44	313	78	577	16	829	415
97	48	317	159	593	37	853	61
101	51	337	28	601	60	857	107
109	55	349	175	613	307	877	439
113	28	353	22	617	308	881	220
137	17	373	187	641	320	929	464
149	75	389	39	653	327	937	468
157	79	397	199	661	331	941	471
173	87	401	200	673	336	953	119
181	91	409	102	677	113	977	488
193	96	421	211	701	351	997	499

REFERENCES

1. R. D. Carmichael. "On the Numerical Factors of the Forms $\alpha^n \pm \beta^n$." *Ann. Math.* 15 (1913):30-70.
2. G. H. Hardy & E. M. Wright. *The Theory of Numbers*. 4th ed. Oxford: Oxford University Press, 1960.

3. W. Ljunggren. "Zur Theorie der Gleichung $x^2 + 1 = Dy^4$." *Avh. Norsk. Vid. Akad. Oslo* (1942), pp. 1-27.
4. E. Lucas. "Theorie des Fonctions Numeriques Simplement Periodiques." *Am. J. Math.* 1 (1877):184-240; 289-321.
5. N. Robbins. "Some Identities and Divisibility Properties of Linear Second-Order Recursion Sequences." *The Fibonacci Quarterly* 20 (1982):21-24.
6. N. Robbins. "On Fibonacci Numbers of the form px^2, Where p is Prime." *The Fibonacci Quarterly* 21 (1983):266-71.
7. C. E. Serkland. "The Pell Sequence and Some Generalizations." Master's Thesis, San Jose State University, 1973.
8. W. Sierpinski. *Elementary Theory of Numbers*. Warsaw: Panstwowe Wydawnictwo Naukowe, 1964.

◆◇◆◇◆