PAIRS OF RECIPROCAL QUADRATIC CONGRUENCES INVOLVING PRIMES

JOHN B. COSGRAVE AND KARL DILCHER

Abstract. Using Pell equations and known solutions that involve Lucas sequences, we find all solutions of the reciprocal pair of quadratic congruences $p^2 \equiv \pm 1 \pmod{q}$, $q^2 \equiv \pm 1 \pmod{p}$ for odd primes p, q. In particular, we show that there is exactly one solution $(p, q) = (3, 5)$ when the right-hand sides are -1 and 1. When the right-hand sides are both -1, there are four known solutions, all of them pairs of Fibonacci primes, and when the the right-hand sides are both 1, there are no solutions. By partly different methods we completely characterize the solutions of $p^2 \equiv \pm N \pmod{q}$, $q^2 \equiv \pm N \pmod{p}$ for $N = 2$ and 4, and give partial results for $N = 3$ and 5. In the process we indicate how the general case can be treated.

1. Introduction

In the process of studying certain congruences for sums of reciprocals of integers and their squares [2], we came across the pair of quadratic congruences

$$p^2 \equiv -1 \pmod{q}, \qquad q^2 \equiv 1 \pmod{p}, \tag{1.1}$$

where p and q are odd primes. In particular, we needed to know whether, apart from the obvious solution $(p, q) = (3, 5)$, there are any other prime solutions to this system of congruences. We consider this question of independent interest, and it is one of the purposes of this paper to solve a more general pair of congruences:

Theorem 1. *For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences*

$$\begin{cases} p^2 \equiv \delta \pmod{q}, \\ q^2 \equiv \varepsilon \pmod{p}, \end{cases} \tag{1.2}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then (1.2) has no solution.*
(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (3, 5)$ is the only solution of (1.2).*
(c) *If $\delta = \varepsilon = -1$, then the only solutions of (1.2) are $(p, q) = (F_n, F_{n+2})$, $n = 1, 2, \ldots$, provided both Fibonacci numbers F_n, F_{n+2} are prime.*

In connection with part (c) we note that computational results on the primality of Fibonacci numbers are known; see [3] or [11, p. 258]. Based on the information in this last reference, the only pairs of Fibonacci primes up to $n = 2\,253\,000$ occur when $n = 5, 11, 431$, and 569. The first two correspond to the solutions $(p, q) = (5, 13)$ and $(p, q) = (89, 233)$, while the third pair has 90 and 91 decimal digits, and the

Key words and phrases. Quadratic congruences, Pell equations, Lucas numbers.
Research supported in part by the Natural Sciences and Engineering Research Council of Canada.

members of the fourth pair both have 119 digits. If there are further solutions, then both primes will have more than 470 849 digits.

The proof of Theorem 1 and all subsequent theorems is based on writing the pair of congruences in question as a special class of Pell equations. This is done in Section 2, where we also quote numerous explicit results on Pell equations, as well as properties of Lucas sequences that will be required. The proof of Theorem 1 is then given in Section 3. In Section 4 we prove the analogous result in the case where the right-hand sides of the congruences (1.2) are $\pm N$ with $N = 4$, and in Section 5 we do the same for $N = 2$, using a different method. Finally, in Section 6, we give partial results for the cases $N = 5$ and $N = 3$. We close the paper with some remarks on further generalizations.

2. Pell Equations and Lucas Sequences

The main idea in the proof of Theorem 1 and of all the subsequent theorems is an easy transformation of the given pairs of quadratic congruences into a single Pell-type equation. We begin with a more general pair than (1.2), namely

$$p^2 \equiv \delta N \pmod{q}, \qquad q^2 \equiv \varepsilon N \pmod{p}, \tag{2.1}$$

with $\delta, \varepsilon \in \{-1, 1\}$ and N a fixed positive integer. The problem now is to find solutions to (2.1) in odd primes p, q with $\gcd(pq, N) = 1$. We multiply the two congruences and obtain

$$(p^2 - \delta N)(q^2 - \varepsilon N) \equiv 0 \pmod{pq}.$$

If we expand the left-hand side and divide by $-\delta N$, we get $q^2 + \delta\varepsilon p^2 - \varepsilon N \equiv 0 \pmod{pq}$, or

$$q^2 + \delta\varepsilon p^2 = \varepsilon N + kpq, \tag{2.2}$$

for some integer k. Since p and q are assumed to be odd, we see that k must have the same parity as N. Multiplying both sides of (2.2) by 4 and completing the square, we get

$$(2q - kp)^2 - (k^2 - 4\delta\varepsilon)p^2 = 4\varepsilon N. \tag{2.3}$$

When N is even then k is even, say $k = 2\tilde{k}$, and (2.3) reduces to

$$(q - \tilde{k}p)^2 - (\tilde{k}^2 - \delta\varepsilon)p^2 = \varepsilon N. \tag{2.4}$$

It is well known that the solutions of such Pell-type equations are closely related to second-order linear recurrences; see, e.g., [9, p. 351 ff.]. In the case of Theorem 1 and of Theorem 2 below, the *Lucas sequences* $\{U_n(P, Q)\}, \{V_n(P, Q)\}$ are particularly important. For integer parameters P and Q, these pairs of sequences are defined by

$$U_0(P, Q) = 0, \quad U_1(P, Q) = 1, \quad V_0(P, Q) = 2, \quad V_1(P, Q) = P, \tag{2.5}$$

and for $n \geq 2$,

$$U_n(P, Q) = P \cdot U_{n-1}(P, Q) - Q \cdot U_{n-2}(P, Q), \tag{2.6}$$

$$V_n(P, Q) = P \cdot V_{n-1}(P, Q) - Q \cdot V_{n-2}(P, Q). \tag{2.7}$$

In particular, we see that for all $n \geq 0$ we have

$$U_n(1, -1) = F_n, \quad V_n(1, -1) = L_n, \tag{2.8}$$

the nth Fibonacci and Lucas numbers, respectively. Among the numerous properties satisfied by these sequences we require the "Binet formulas"

$$U_n(P,Q) = \frac{1}{\sqrt{D}}\left(\left(\frac{P+\sqrt{D}}{2}\right)^n - \left(\frac{P-\sqrt{D}}{2}\right)^n\right), \tag{2.9}$$

$$V_n(P,Q) = \left(\frac{P+\sqrt{D}}{2}\right)^n + \left(\frac{P-\sqrt{D}}{2}\right)^n, \tag{2.10}$$

where $D := P^2 - 4Q$, and the identity

$$U_{n+m}(P,Q) = \frac{1}{2}\big(U_n(P,Q)V_m(P,Q) + U_m(P,Q)V_n(P,Q)\big) \tag{2.11}$$

(see, e.g., [7] or [6]). More specifically, we will need the following three well-known identities which are special cases for $m = 1, 2$, and n, respectively:

$$U_{n+1}(P,Q) = \frac{1}{2}\big(P \cdot U_n(P,Q) + V_n(P,Q)\big), \tag{2.12}$$

$$U_{n+2}(P,Q) = \frac{1}{2}\big((P^2 - 2Q) \cdot U_n(P,Q) + P \cdot V_n(P,Q)\big), \tag{2.13}$$

$$U_{2n}(P,Q) = U_n(P,Q) \cdot V_n(P,Q). \tag{2.14}$$

Here we have used (2.5)–(2.7) to obtain (2.12) and (2.13). We also require the well-known fact that the Lucas sequences $U_n(P,Q)$ are *divisibility sequences*, that is,

$$n \mid m \quad \Rightarrow \quad U_n(P,Q) \mid U_m(P,Q); \tag{2.15}$$

see, e.g., [7] or [6]. Finally, later in this paper we require the following identity for $V_n(P,Q)$:

$$V_{n+m}(P,Q) = V_n(P,Q)V_m(P,Q) - Q^m V_{n-m}(P,Q). \tag{2.16}$$

This last identity and (2.11) follow easily from the Binet-type formulas (2.9) and (2.10).

The point of introducing the Lucas sequences in such detail is that they serve as specific solutions for certain classes of Pell equations, as summarized in Table 1.

	Equation	Restriction	X	Y
(2.17)	$X^2 - (a^2-4)Y^2 = -4$	$a \geq 4$	–	–
(2.18)	$X^2 - (a^2+4)Y^2 = -4$	$a \geq 1$	$V_{2j+1}(a,-1)$	$U_{2j+1}(a,-1)$
(2.19)	$X^2 - (a^2+4)Y^2 = 4$	$a \geq 1$	$V_{2j}(a,-1)$	$U_{2j}(a,-1)$
(2.20)	$X^2 - (a^2-1)Y^2 = -4$	$a \geq 2, a \neq 3$	–	–
(2.21)	$X^2 - (a^2+1)Y^2 = -4$	$a \geq 1, a \neq 2$	$V_{2j+1}(2a,-1)$	$2U_{2j+1}(2a,-1)$
(2.22)	$X^2 - (a^2+1)Y^2 = 4$	$a \geq 1, a \neq 2$	$V_{2j}(2a,-1)$	$2U_{2j}(2a,-1)$
(2.23)	$X^2 - (a^2+1)Y^2 = -1$	$a \geq 1$	$\frac{1}{2}V_{2j+1}(2a,-1)$	$U_{2j+1}(2a,-1)$
(2.24)	$X^2 - (a^2-4)Y^2 = 1$	$a \geq 3$ odd	$\frac{1}{2}V_{3j}(a,1)$	$\frac{1}{2}U_{3j}(a,1)$

Table 1: Solutions (X,Y) of certain Pell equations, $j = 0, 1, 2, \ldots$ [4].

Rows (2.17) and (2.20) in this table indicate that there are no solutions in these cases. The table summarizes Corollaries 2.6, 2.8, 2.9, Theorems 5.4–5.6, Theorem 4.4, and Theorem 3.5 in [4].

3. Proof of Theorem 1

While the proof of part (a) is very easy and elementary, the results quoted in Section 2 will be needed for parts (b) and (c).

(a) The congruence $p^2 \equiv 1 \pmod{q}$ would imply $q \mid (p-1)(p+1)$, and so $q \mid p-1$ or $q \mid p+1$, giving $q < p$ (since p and q are odd). Similarly, the second congruence gives $p < q$, a contradiction.

(b) With $\delta = -1$ and $\varepsilon = 1$, (2.3) becomes

$$(2q - kp)^2 - (k^2+4)p^2 = 4. \tag{3.1}$$

As already noted in the proof of part (a), the congruence $q^2 \equiv 1 \pmod{p}$ implies $p < q$, and from (2.2) it follows that $k \geq 1$. (3.1) is an equation of the form (2.19) with $a = k$, with solutions $p = U_{2j}(k,-1)$ and $2q - kp = V_{2j}(k,-1)$, i.e., by (2.12) we have

$$q = \frac{1}{2}\left(kU_{2j}(k,-1) + V_{2j}(k,-1)\right) = U_{2j+1}(k,-1). \tag{3.2}$$

Hence the solutions of (3.1) are

$$p = U_{2j}(k,-1), \quad q = U_{2j+1}(k,-1), \quad j = 0,1,2,\ldots \tag{3.3}$$

By (2.15), p is composite unless $U_2(k,-1) = 1$. But this happens only when $k = 1$, i.e., in the case of the Fibonacci sequence. And indeed, we have $U_4(1,-1) = F_4 = 3$. By (2.6) it is clear that $U_n(k,-1) > 1$ for all $n \geq 3$ and all $k \geq 1$. Finally, with (2.14) we see that for $j \geq 3$, $U_{2j}(k,-1)$ is composite since both factors on the right of (2.14) are greater than 1 for $P = k \geq 1$ and $Q = -1$.

In summary, $p = U_{2j}(k,-1)$ is prime only when $j = 2$ and $k = 1$. Since then $q = U_{2j+1}(k,-1) = U_5(1,-1) = F_5 = 5$ is also prime, this gives the solution $(p,q) = (3,5)$. To check the cases $j = 0, 1$, we note that $U_0(k,-1) = 0$, $U_1(k,-1) = 1$, $U_2(k,-1) = k$, and $U_3(k,-1) = k^2+1$, which is even since k is odd. Hence these small cases do not give solutions in odd primes. This completes the proof of (b).

(c) If $\delta = \varepsilon = -1$, then once again from (2.2) it follows that $k \geq 1$, and by the theory of quadratic residues the two congruences in (1.2) imply $p \equiv q \equiv 1 \pmod{4}$. This, with (2.2), implies $k \equiv 3 \pmod{4}$. Now (2.3) becomes

$$(2q - kp)^2 - (k^2-4)p^2 = -4. \tag{3.4}$$

For $k \geq 4$ this is Equation (2.17) which has no solutions. This leaves the case $k = 3$, which gives

$$(2q - 3p)^2 - 5p^2 = -4. \tag{3.5}$$

But this is Equation (2.18) with $a = 1$, and Table 1 gives the solutions $2q - 3p = V_{2j+1}(1,-1)$, $p = U_{2j+1}(1,-1)$, $j = 0,1,2,\ldots$. Now we use (2.13) with $P = 1$, $Q = -1$, to get

$$q = \frac{1}{2}\left(3U_{2j+1}(1,-1) + V_{2j+1}(1,-1)\right) = U_{2j+3}(1,-1),$$

and so with (2.8) we see that the solutions of (3.5) are the Fibonacci numbers $p = F_{2j+1}$, $q = F_{2j+3}$, which completes the proof of (c).

4. The case $N = 4$

The case $N = 4$ in the pair of congruences (2.5) can be treated in a similar way as Theorem 1. We begin by stating the corresponding result.

Theorem 2. *For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences*

$$\begin{cases} p^2 \equiv 4\delta \pmod{q}, \\ q^2 \equiv 4\varepsilon \pmod{p}, \end{cases} \tag{4.1}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then (p, q) is a solution of (4.1) if and only if it is a pair of odd twin primes.*
(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (3, 13)$ is the only solution of (4.1).*
(c) *If $\delta = \varepsilon = -1$, then the only solutions of (4.1) are $(p, q) = (P_n, P_{n+2})$, $n = 1, 2, \ldots$, provided both Pell numbers P_n, P_{n+2} are prime.*

The well-known sequence of *Pell numbers* $\{P_n\}$ is defined by $P_0 = 0$, $P_1 = 1$, and

$$P_{n+1} = 2P_n + P_{n-1} \qquad (n \geq 1).$$

This sequence is also a special case of the Lucas sequence (2.6), with $P_n = U_n(2, -1)$, and is therefore a divisibility sequence. This means that, as in the case of Fibonacci numbers, P_n cannot be a prime unless n is also a prime. The only known (probable) prime Pell numbers have index 2, 3, 5, 11, 13, 29, 41, 53, 59, 89, 97, 101, 167, 181, 191, 523, 929, 1217, 1301, 1361, 2087, 2273, 2393, 8093, 13339, 14033, 23747, 28183, 34429, 36749, 90197, with no others less than 188 856 (see [14]). Accordingly, the only known solutions of part (c) in the Theorem are

$$(P_3, P_5) = (5, 29) \quad \text{and} \quad (P_{11}, P_{13}) = (5\,741, 33\,461).$$

For further properties of the Pell numbers, with references, see [12, A000129].

Proof of Theorem 2. **(a)** We proceed as in the proof of Theorem 1(a). The congruence $p^2 \equiv 4 \pmod{q}$ implies $q \mid p - 2$ or $q \mid p + 2$, giving $q \leq p + 2$. By symmetry $p \leq q + 2$, and thus $q - 2 \leq p \leq q + 2$. This means that either $p = q - 2$ or $p = q + 2$, i.e., (p, q) is a pair of twin primes.

For the remaining two cases we consider (2.2) with $N = 4$. Taking both sides modulo 4, we see that

– if $\delta\varepsilon = -1$, then $k \equiv 0 \pmod{4}$, and $\tilde{k}$ is even;
– if $\delta\varepsilon = 1$, then $k \equiv 2 \pmod{4}$, and $\tilde{k}$ is odd.

(b) Considering (2.4) with $\delta\varepsilon = -1$, we see that (2.21) and (2.22) in Table 1 apply, and that for $\tilde{k} \neq 2$, $Y = p$ would be even which has to be excluded since p is an odd prime. This leaves the case $\tilde{k} = 2$, and with (2.4) we get

$$(q - 2p)^2 - 5p^2 = 4\varepsilon. \tag{4.2}$$

When $\varepsilon = 1$, (2.19) in Table 1 gives $p = U_{2j}(1, -1) = F_{2j}$, but we have seen in the proof of Theorem 1(b) that this is prime only when $2j = 4$, with $F_4 = 3$. Then, with $(q - 2p) = V_{2j}(1, -1) = L_{2j}$, we would get $q = L_4 + 2F_4 = 7 + 2 \cdot 3 = 13$. Hence $(p, q) = (3, 13)$ is the only solution in this case.

To conclude the proof of part (b), we note that when $\varepsilon = -1$ in (4.2), we have the situation of (2.18) in Table 1, which gives $p = F_{2j+1}$ and $q - 2p = L_{2j+1}$,

$j = 0, 1, 2, \ldots$ Hence $q = L_{2j+1} + 2F_{2j+1}$, an expression that can be simplified. Indeed, by (2.15) we have $2F_{n+2} = 3F_n + L_n$, and thus, for $n \geq 0$,

$$L_n + 2F_n = 2F_{n+2} - F_n = (F_{n+3} - F_{n+1}) + F_{n+2} - F_n = F_{n+3},$$

and therefore $q = F_{2j+4}$. As we have seen, for $j \geq 1$ this is never prime. For $j = 0$ we have $p = F_1 = 1$, which is not prime. Therefore in this case there is no solution, and part (b) is complete.

(c) When $\delta = \varepsilon = -1$, then (2.4) leads to

$$(q - \tilde{k}p)^2 - (\tilde{k}^2 - 1)p^2 = -4, \tag{4.3}$$

and by row (2.20) in Table 1, recalling that $\tilde{k}$ is odd, we see that (4.3) has no solution unless possibly for $\tilde{k} = 1$ or 3. When $\tilde{k} = 1$, (4.3) clearly has no solution, while $\tilde{k} = 3$ leads to

$$\left(\frac{q - 3p}{2}\right)^2 - 2p^2 = -1.$$

This is covered by (2.23) in Table 1, with $a = 1$, which gives $p = U_{2j+1}(2, -1)$ and $q - 3p = V_{2j+1}(2, -1)$. Then

$$q = 3U_{2j+1}(2, -1) + V_{2j+1}(2, -1) = U_{2j+3}(2, -1),$$

which follows immediately from (2.13). This proves part (c), and the proof of Theorem 2 is complete. □

5. The case $N = 2$

A result similar to Theorems 1 and 2 can be obtained in the case where $N = 2$ in (2.1). It turns out that in this case the explicit results in [4] no longer apply, and therefore we begin by briefly recalling some fundamentals of the well-known connections between Pell equations and continued fractions. For further details, with proofs, see [5] or [10], or see [13] for a summary.

Let D be a non-square positive integer. Then the simple continued fraction expansion of $\sqrt{D}$ becomes periodic after the first term, and has the form

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_r, 2a_0}]. \tag{5.1}$$

In general, given the continued fraction $[b_0, b_1, b_2, \ldots]$, we define the sequences $\{P_n\}$, $\{Q_n\}$ by

$$P_0 = 0, \quad P_1 = b_0, \quad Q_0 = 1, \quad Q_1 = D - b_0^2, \tag{5.2}$$

$$P_n = b_{n-1}Q_{n-1} + P_{n-1}, \quad Q_n = \frac{D - P_n^2}{Q_{n-1}}. \tag{5.3}$$

The main connection to Pell-type equations is now as follows.

Lemma 1. *Let $D > 1$ be a non-square integer. Then the equation*

$$x^2 - Dy^2 = C,$$

with $|C| < \sqrt{D}$, has solutions if and only if C is one of the integers $(-1)^k Q_k$ for some $1 \leq k \leq r$, where r is as in (5.1), and Q_k is as in (5.2), computed with $b_j = a_j$, $j = 0, 1, \ldots, r$.

To state the desired analogue to Theorems 1 and 2, we need to introduce two second-order recurrence sequences: Let

$$R_0 = 1, \quad R_1 = 1, \quad R_n = 2R_{n-1} + R_{n-2} \quad (n \geq 2); \tag{5.4}$$

$$S_0 = 1, \quad S_1 = 1, \quad S_n = 4S_{n-1} - S_{n-2} \quad (n \geq 2). \tag{5.5}$$

These are sequences A001333 and A001835, respectively, in [12]. Although they are of the form (2.6), (2.7), they are not Lucas sequences since (2.5) is not satisfied.

Theorem 3. *For $\delta = \pm 1$ and $\varepsilon = \pm 1$, consider the pair of congruences*

$$\begin{cases} p^2 \equiv 2\delta \pmod{q}, \\ q^2 \equiv 2\varepsilon \pmod{p}, \end{cases} \tag{5.6}$$

in odd primes p and q. We have the following cases.

(a) *If $\delta = \varepsilon = 1$, then (5.6) has no solution.*
(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (R_{2n\pm1}, R_{2n})$, $n = 1, 2, \ldots$, are the only solutions of (5.6), provided that both R_{2n-1}, R_{2n} or R_{2n+1}, R_{2n} are prime.*
(c) *If $\delta = \varepsilon = -1$, then the only solutions of (5.6) are $(p, q) = (S_n, S_{n+1})$, $n = 1, 2, \ldots$, provided both numbers S_n, S_{n+1} are prime.*

Computations show that the only $n \leq 40\,000$ for which the R_n are probable primes (or known primes for smaller n) are $n = 2$, 3, 4, 5, 7, 8, 16, 19, 29, 47, 59, 163, 257, 421, 937, 947, 1493, 1901, 6689, 8087, 9679, and 28753. Accordingly, the only solutions of part (b) known to us occur for the index pairs $(3, 2)$, $(3, 4)$, $(5, 4)$, and $(7, 8)$, namely

$$(p, q) = (7, 3), (7, 17), (41, 17), \text{ and } (239, 577).$$

Similarly, the $n \leq 25\,000$ for which the S_n are probable primes (or known primes for smaller n) are $n = 2$, 3, 4, 6, 7, 10, 12, 19, 23, 75, 114, 139, 156, 159, 246, 324, 360, 474, 520, 597, 750, 934, 967, 2296, 3564, 5637, 6796, 8412, 9271, 13974, and 17176. Since the only consecutive integers $(n, n+1)$ in this list occur for $n = 2$, 3, and 6, the only solutions known to us are

$$(p, q) = (3, 11), (11, 41), \text{and } (571, 2131).$$

To begin the proof of Theorem 3, we use (2.4) with $N = 2$, and for simplicity we write k in place of $\tilde{k}$. Then we have

$$(q - kp)^2 - (k^2 - \delta\varepsilon)p^2 = 2\varepsilon. \tag{5.7}$$

We now deal with the three parts of Theorem 3, and first assume that $\delta = \varepsilon$. We can then apply Lemma 1 with $D = k^2 - 1$ and $C = 2\varepsilon$. The condition $|C| < \sqrt{D}$ is then equivalent to $k^2 > 5$, or $k \geq 3$ (positive by (2.2) since $\delta\varepsilon = 1$).

Next, it is easily obtained that

$$\sqrt{k^2 - 1} = [k - 1, \overline{1, 2k - 2}];$$

see also [10, p. 99]. Hence by (5.2) we have

$$Q_1 = D - a_0^2 = k^2 - 1 - (k - 1)^2 = 2(k - 1).$$

For $k \geq 3$ we can never have $-Q_1 = 2\varepsilon$, so there are no solutions to (5.7) in this case. This leaves $k = 1$ or 2, not covered by Lemma 1.

When $\delta = \varepsilon = 1$ then, since $p^2 \equiv q^2 \equiv 1 \pmod 8$, (2.2) shows that k in that identity is divisible by 8, which forces $4 \mid k$ in (5.7), that is, $k \geq 4$. Hence (5.7) has no solutions in this case, which proves part (a) of the theorem.

In the case $\delta = \varepsilon = -1$ we have no such restriction on k. However, when $k = 1$, then (5.7) reduces to $(q-p)^2 = -2$, which clearly has no solutions. Finally, the case $k = 2$ leads to the Pell-type equation

$$(q-2p)^2 - 3p^2 = -2. \tag{5.8}$$

To deal with this equation we introduce, in addition to the sequence $\{S_n\}$, three related sequences that all satisfy the same recurrence relation, but with different initial values (see Table 2). The characteristic equation associated with this recurrence relation is $x^2 - 4x + 1 = 0$, which has roots $\alpha := 2 + \sqrt{3}$ and $\overline{\alpha} = 2 - \sqrt{3}$. Using standard methods, a Binet-type formula of the form $A\alpha^n + B\overline{\alpha}^n$, for algebraic numbers A, B, can be derived for each of the four sequences. They are shown in the last column of Table 2.

n	0	1	2	3	4	OEIS [12]	Binet
$\overline{S}_n$	1	5	19	71	265	A001834	$\frac{1+\sqrt{3}}{2}\alpha^n + \frac{1-\sqrt{3}}{2}\overline{\alpha}^n$
S_n	1	3	11	41	153	A001835	$\frac{3+\sqrt{3}}{6}\alpha^n + \frac{3-\sqrt{3}}{6}\overline{\alpha}^n$
x_n	2	7	26	97	362	A001075	$\frac{2+\sqrt{3}}{2}\alpha^n + \frac{2-\sqrt{3}}{2}\overline{\alpha}^n$
y_n	1	4	15	56	209	A001353	$\frac{3+2\sqrt{3}}{6}\alpha^n + \frac{3-2\sqrt{3}}{6}\overline{\alpha}^n$

Table 2: Four sequences satisfying $u_n = 4u_{n-1} - u_{n-2}$.

Using the Binet-type formulas, the following identities can be verified by straightforward computations:

$$x_n^2 - 3y_n^2 = 1, \tag{5.9}$$

$$\overline{S}_n^2 - 3S_n^2 = -2, \tag{5.10}$$

$$\overline{S}_n^2 + 1 = x_{2n}, \tag{5.11}$$

$$S_n\overline{S}_n = y_{2n}, \tag{5.12}$$

$$\overline{S}_n = S_{n+1} - 2S_n. \tag{5.13}$$

The fact that (x_n, y_n), $n = 0, 1, 2, \ldots$, are solutions to (5.9) also follows from the continued fraction method (see, e.g., [5], [9], [10]), which furthermore shows that these are all possible solutions of the Pell equation $x^2 - 3y^2 = 1$. While this method does not guarantee that $(\overline{S}_n, S_n)$, $n = 0, 1, 2, \ldots$, are all the solutions of the Pell-type equation $X^2 - 3Y^2 = -2$, this is still the case, as we will now show.

Lemma 2. *The only positive solutions of the equation*

$$X^2 - 3Y^2 = -2 \tag{5.14}$$

are $(X, Y) = (\overline{S}_n, S_n)$, $n = 0, 1, 2, \ldots$, *with* $\overline{S}_n$ *and* S_n *as defined in Table 2.*

For the proof of this lemma we need a result on the terms of the sequence $\{x_n\}$. We use the standard notation $p^a || n$ to mean that p^a, but not p^{a+1}, divides n.

Lemma 3. (*a*) *For any* $n \geq 0$ *we have* $x_{4n+1} \equiv 3 \pmod 4$.
(*b*) *If* $\alpha \geq 2$ *and* $2^\alpha || n$, *then* $2^{2\alpha+1} || x_{n-1} - 1$.

In summary, if n is odd, then the highest power of 2 dividing $x_n - 1$ has an odd exponent.

Proof. (a) The recurrence relation for the x_n, taken modulo 4, reduces to $x_n \equiv -x_{n-2} \pmod 4$, and thus $x_n \equiv x_{n-4} \pmod 4$ for all $n \geq 4$. Since $x_1 = 7 \equiv 3 \pmod 4$, this proves part (a).

(b) It will be convenient to deal with the closely related sequence

$$V_0 = 2, \quad V_n = 2x_{n-1} \quad (n \geq 1). \tag{5.15}$$

Then $V_n = V_n(4,1)$, as defined in (2.5) and (2.7). We first claim that

$$V_{2^n} \equiv 2^{2n+2} + 2 \pmod{2^{2n+3}} \quad (n \geq 2). \tag{5.16}$$

We prove this by induction, based on the quadratic recurrence

$$V_{2^{n+1}} = V_{2^n}^2 - 2, \tag{5.17}$$

which follows immediately from (2.16) with 2^n in place of both n and m. Now

$$V_4 = 2x_3 = 194 = 66 + 128 \equiv 2^6 + 2 \pmod{2^7},$$

so (5.16) holds for $n = 2$. Now suppose that (5.16) holds for some $n \geq 2$, and rewrite it as

$$V_{2^n} = k \cdot 2^{2n+3} + 2^{2n+2} + 2.$$

Using (5.17) we then get

$$\begin{aligned} V_{2^{n+1}} &= \big((2k+1)2^{2n+2} + 2\big)^2 - 2 \\ &= 2^{2(n+1)+2} + 2 + 2k \cdot 2^{2(n+1)+2} + (2k+1)^2 2^{4n+4} \\ &\equiv 2^{2(n+1)+2} + 2 \pmod{2^{2(n+1)+3}}, \end{aligned}$$

which proves (5.16) by induction.

As a next step we show that for all $n \geq 1$,

$$V_{k2^{n+1}} \equiv 2 \pmod{2^{2n+3}}, \quad k = 1, 2, \ldots. \tag{5.18}$$

We prove this by induction on k. We set this up by using (2.16) with $k2^{n+1}$ and 2^{n+1} in place of n and m, respectively, which gives

$$V_{(k+1)2^{n+1}} = V_{k2^{n+1}} V_{2^{n+1}} - V_{(k-1)2^{n+1}}, \tag{5.19}$$

and we also note that by (5.16) we have

$$V_{2^{n+1}} \equiv 2 \pmod{2^{2n+3}}, \qquad V_{2 \cdot 2^{n+1}} = V_{2^{n+2}} \equiv 2 \pmod{2^{2n+3}},$$

which establishes (5.18) for $k = 1$ and 2. Now suppose that (5.18) holds up to some k. Then by (5.19) we have

$$V_{(k+1)2^{n+1}} \equiv 2 \cdot 2 - 2 \equiv 2 \pmod{2^{2n+3}},$$

which proves (5.18). Finally, we use (2.16) once again, with $k \cdot 2^{n+1}$ and 2^n in place of n and m, respectively. This gives, with (5.18),

$$V_{(2k+1)2^n} = V_{k2^{n+1}} V_{2^n} - V_{(2k-1)2^n} \equiv 2V_{2^n} - V_{(2k-1)2^n} \pmod{2^{2n+3}}.$$

This serves as induction step in the proof of the congruence

$$V_{(k+1)2^{n+1}} \equiv 2^{n+2} + 2 \pmod{2^{2n+3}}, \tag{5.20}$$

valid for all integers $n \geq 2$ and $k \geq 0$. To complete the proof of part (b) of Lemma 3, we divide both sides of (5.20) by 2 and use (5.15). □

We remark in passing that the sequence V_{2^n}, $n = 0, 1, \ldots$, which was an important tool in the above proof, also plays an essential role in the Lucas-Lehmer test for primality of Mersenne numbers; see, e.g., [12, A003010] or [1].

Proof of Lemma 2. By (5.10), the pairs $(\overline{S}_n, S_n)$ are indeed solutions, and we show there are no others by proceeding as follows. We have

$$(2X^2 + 2)^2 - 12X^2Y^2 = 4X^4 + 8X^2 + 4 - 4X^2(X^2 + 2) = 4$$

for X and Y satisfying (5.14). That is,

$$(X^2 + 1)^2 - 3(XY)^2 = 1. \tag{5.21}$$

With (5.11) and (5.12) we now see that the solutions in (5.10) lead to all solutions in (5.9) for even n. It remains to show that no solution (X, Y) of (5.14) can lead to an odd-index solution in (5.9). Indeed, any such solution would lead to (5.21). However, by Lemma 3 no odd-index x_n can be of the form $X^2 + 1$; this completes the proof of Lemma 2. □

We have now completed the proof of part (c) of Theorem 3. To prove part (b), we note that with $\delta = 1$ and $\varepsilon = -1$, the equation (5.7) becomes

$$(q - kp)^2 - (k^2 + 1)p^2 = -2. \tag{5.22}$$

It is easily obtained that $\sqrt{k^2 + 1} = [k, \overline{2k}]$ (see also [10, p. 99]). Then with (5.2) and (5.3) we find immediately that $P_0 = 0$, $P_n = k$ for $n \geq 1$, and $Q_n = 1$ for $n \geq 0$. Hence, by Lemma 1, the are no solutions to (5.22) for $|k| \geq 2$. This leaves the cases $k = \pm 1$, that is,

$$(q \pm p)^2 - 2p^2 = -2, \quad \text{i.e.,} \quad 4\left(\tfrac{q \pm p}{2}\right)^2 - 2p^2 = -2.$$

Dividing both sides of this last equation by -2, we arrive at the Pell equation

$$p^2 - 2\left(\tfrac{q \pm p}{2}\right)^2 = 1. \tag{5.23}$$

It is known (and can be derived by way of the continued fraction method) that the equation $X^2 - 2Y^2 = 1$ has as its only solutions $(X, Y) = (R_{2n}, R^*_{2n})$, $n = 0, 1, \ldots$, where R_n is defined by (5.4) and R^*_n satisfies the same recurrence relations but has initial values $R^*_0 = 0$, $R^*_1 = 1$. Using standard methods, we obtain the Binet-type formulas

$$R_n = \frac{1}{2}\left((1 + \sqrt{2})^n + (1 - \sqrt{2})^n\right), \qquad R^*_n = \frac{1}{2\sqrt{2}}\left((1 + \sqrt{2})^n - (1 - \sqrt{2})^n\right).$$

These formulas immediately imply the identities

$$R_{2n+1} - R_{2n} = 2R^*_{2n}, \qquad R_{2n-1} + R_{2n} = 2R^*_{2n}.$$

These, combined with (5.23), complete part (b) of Theorem 3, and we are done.

6. The cases $N = 5$ and $N = 3$

The previous section indicates how the general case (2.1) can be treated by solving the Pell-type equation (2.3) or (2.4). In general it will be difficult to characterize all solutions for a given N. In this section we will first discuss the case $N = 5$ since the Lucas numbers L_n, already mentioned earlier in this paper, are exclusively involved. Following this we state, without proof, the corresponding result for $N = 3$.

By (2.3) with $N = 5$ we have

$$(2q - kp)^2 - (k^2 - 4\delta\varepsilon)p^2 = 20\varepsilon, \tag{6.1}$$

and k, as observed in Section 2, having the same parity as N (here 5), is odd. If we assume that $q > p$, then k is also positive.

We assume that $\delta = \varepsilon$, and leave the opposite case to the reader. For Lemma 1 to be applicable in our case, we need $\sqrt{k^2-4} > 20$, or $k \geq 21$. Now for odd $k \geq 5$ we have

$$\sqrt{k^2-4} = \left[k-1, \overline{1, \tfrac{1}{2}(k-3), 2, \tfrac{1}{2}(k-3), 1, 2k-2}\right],$$

which is not difficult to verify. Lemma 1 can then be used to show that (6.1) with $\delta = \varepsilon$ has no solutions for odd $k \geq 21$.

Now consider (2.2) modulo 5 for $\delta = \varepsilon$, i.e.,

$$p^2 + q^2 - kpq \equiv 0 \pmod 5. \tag{6.2}$$

If p and q are both $\pm 1 \pmod 5$ or both $\pm 2 \pmod 5$, then $p^2 + q^2 \equiv \pm 2 \pmod 5$ and $pq \equiv \pm 1 \pmod 5$, so that $k \equiv \pm 2 \pmod 5$. This means we need only consider $k = 3, 7, 13$, and 17.

On the other hand, if one of p and q is $\pm 1 \pmod 5$ and the other is $\pm 2 \pmod 5$, then $p^2 + q^2 \equiv 0 \pmod 5$ and $pq \equiv \pm 2 \pmod 5$, so that $k \equiv 0 \pmod 5$. This forces $k = 5$ or 15.

(i) We begin with $k = 3$. Then (6.1) becomes $(2q - kp)^2 - 5p^2 = 20\varepsilon$, and upon dividing by -5,

$$p^2 - 5\left(\tfrac{2q-3p}{5}\right)^2 = -4\varepsilon. \tag{6.3}$$

When $\varepsilon = 1$, this is (2.18) with $a = 1$, which gives $p = L_{2j+1}$ and $(2q - 3p)/5 = F_{2j+1}$. Hence

$$q = \frac{1}{2}\left(5F_{2j+1} + 3L_{2j+1}\right) = L_{2j+3},$$

which is easy to verify. Hence $(p, q) = (L_{2j+1}, L_{2j+3})$ is a class of solutions, provided p and q are both prime. When $\varepsilon = -1$ in (6.3), we use (2.19), and just as above we obtain the solutions $(p, q) = (L_{2j}, L_{2j+2})$. While the Lucas numbers $\{L_n\}$ do not form a divisibility sequence, we do have $3 \mid L_{4i+2}$ for all $i \geq 0$, with only $L_2 = 3$ a prime. Since always one of $2j$ and $2j + 2$ is of the form $4i + 2$, the only prime solution is the pair $(p, q) = (3, 7)$ in the case $\delta = \varepsilon = -1$ and $k = 3$.

(ii) When $k = 7$, then in analogy to (6.3) we get

$$(3p)^2 - 5\left(\tfrac{2q-7p}{5}\right)^2 = -4\varepsilon. \tag{6.4}$$

When $\varepsilon = 1$, then (2.18) gives $3p = L_{2j+1}$. However, no odd-index Lucas number is divisible by 3, which can be shown by induction. When $\varepsilon = -1$ then, again similar to the previous case and using (2.19), we get $3p = L_{2j}$ and $3q = L_{2j+4}$. Since we know that $3 \mid L_n$ if and only if $n \equiv 2 \pmod 4$ (this can also be shown by induction), we get the class of solutions $(p, q) = (\frac{1}{3}L_{4j-2}, \frac{1}{3}L_{4j+2})$ for $j \geq 1$, provided both p and q are prime.

(iii) When $k = 13$, respectively 17, then (6.1) leads to

$$33p^2 - 5\left(\tfrac{2q-13p}{5}\right)^2 = -4\varepsilon, \qquad 57p^2 - 5\left(\tfrac{2q-17p}{5}\right)^2 = -4\varepsilon,$$

respectively. Both cases reduce to $\pm 3p^2 \equiv \pm 1 \pmod 5$, i.e., $p^2 \equiv \pm 2 \pmod 5$, which has no solution.

(iv) When $k = 5$, then (6.1) gives

$$X^2 - 21p^2 = 20\varepsilon, \quad (X = 2q - 5p).$$

For $\varepsilon = 1$, this reduces to $X^2 \equiv 2 \pmod 3$, which has no solution. However, $(X, p) = (1, 1)$ is obviously a solution in the case $\varepsilon = -1$. From the theory of Pell equations it follows that infinitely many solutions of $X^2 - 21p^2 = -20$ can be obtained by combining the above specific solution with the solutions of the associated Pell equation $X^2 - 21p^2 = 1$ which are given by (2.24) in Table 1 with $a = 5$. (For details see, e.g., [8, p. 204] or [13]). We conjecture that one of the resulting p, q is always divisible by 2 or by 3, so that this case does not contribute to the set of solutions.

(v) Finally, when $k = 15$, then (6.1) gives

$$X^2 - 221p^2 = 20\varepsilon, \quad (X = 2q - 15p).$$

This reduces to $X^2 \equiv \pm 6 \pmod{13}$, which has no solution.

This completes our discussion of the case $\delta = \varepsilon$; we leave the case $\delta = -\varepsilon$ to the reader. In summary, we have the following result.

Theorem 4. *For $\delta = \pm 1$ and $\varepsilon = \pm 1$, the pair of congruences*

$$\begin{cases} p^2 \equiv 5\delta \pmod q, \\ q^2 \equiv 5\varepsilon \pmod p, \end{cases}$$

has the following solutions in odd primes p and q.

- (a) *If $\delta = \varepsilon = 1$, then $(p, q) = (L_{2n-1}, L_{2n+1})$, $n = 1, 2, \ldots$, provided both these Lucas numbers are prime.*
- (b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (L_n, L_{n+1})$ or (L_{n+1}, L_n), $n = 1, 2, \ldots$, provided both these Lucas numbers are prime.*
- (c) *If $\delta = \varepsilon = -1$, then $(p, q) = (3, 7)$ and $(p, q) = (\frac{1}{3}L_{4j-2}, \frac{1}{3}L_{4j+2})$, $j = 1, 2, \ldots$, provided both numbers are prime.*

In contrast to Theorems 1–3 we are unable to prove that these are all possible solutions; however, we conjecture this to be the case.

Primality of the Lucas numbers, defined in (2.8), has been as well studied as that of the Fibonacci numbers; see [3] or [11, p. 259]. Based on the list of prime and probable prime Lucas numbers in this last reference, which is complete up to index $n = 1\,200\,000$, the only known pairs of Lucas primes (L_{2n-1}, L_{2n+1}) are

(a) (11, 29), (199, 521), and (3571, 9349),

while the only known pairs of consecutive Lucas primes are

(b) (7, 11), (29, 47), and (2207, 3571).

Finally, the only known pair of primes $(\frac{1}{3}L_{4n-2}, \frac{1}{3}L_{4n+2})$ is, according to our own computations,

(c) (41, 281), supplemented by the special solution (3, 7).

Rather than computing the Lucas numbers, we found it easier to compute the numbers $a_n := \frac{1}{3}L_{4n+2}$ by way of the recurrence relation $a_0 = 1$, $a_1 = 6$, and $a_{n+1} = 7a_n - a_{n-1}$. We found that the a_n are primes (or probable primes) for $n =$ 2, 3, 6, 9, 15, 21, 44, 50, 114, 146, 228, 270, 326, 329, 776, 1001, 1353, 1374, 3579, 5144, and 13133; there are no more for $n \le 25\,000$.

For the sake of completeness we conclude this section by stating the corresponding result for $N = 3$, without proof. For this purpose we need to introduce two

further second-order recurrence sequences: Let

$$A_0 = 1, \quad A_1 = 2, \quad A_n = 3A_{n-1} + A_{n-2} \quad (n \geq 2);$$
$$B_0 = 1, \quad B_1 = 4, \quad B_n = 5B_{n-1} - B_{n-2} \quad (n \geq 2).$$

These are sequences A052924 and A004253, respectively, in [12]. They are not Lucas sequences as defined by (2.5)–(2.7).

Theorem 5. *For $\delta = \pm 1$ and $\varepsilon = \pm 1$, the pair of congruences*

$$\begin{cases} p^2 \equiv 3\delta \pmod{q}, \\ q^2 \equiv 3\varepsilon \pmod{p}, \end{cases}$$

has the following solutions in odd primes p and q.

(a) *If $\delta = \varepsilon = 1$, then there are none.*
(b) *If $\delta = -1, \varepsilon = 1$, then $(p, q) = (13, 43)$ and $(p, q) = (A_n, A_{n+1})$ or (A_{n+1}, A_n), $n = 1, 2, \ldots$, provided both A_n, A_{n+1} are prime.*
(c) *If $\delta = \varepsilon = -1$, then $(p, q) = (B_n, B_{n+1})$, $n = 1, 2, \ldots$, provided both numbers are prime.*

The proof is similar to the one we sketched for Theorem 4. Once again we conjecture that there are no other solutions.

Computations show that the terms A_n are primes (or probable primes) for $n =$ 2, 3, 5, 6, 8, 9, 15, 17, 27, 35, 68, 87, 134, 143, 158, 275, 279, 326, 345, 440, 545, 630, 702, 813, 968, 1859, 5913, 8183, 10037, 10353, and 16127. These are all for $n \leq 35\,000$.

Similarly, we found that the B_n are primes (or probable primes) for $n = 2$, 5, 6, 8, 9, 14, 20, 21, 23, 26, 33, 44, 54, 63, 81, 116, 174, 233, 419, 464, 713, 866, 989, 1940, 2459, 2963, 3950, and 4604. These are all for $n \leq 25\,000$.

Accordingly, the only known prime pairs (A_n, A_{n+1}) are

(7, 23), (251, 829), (9 043, 29 867),

while the only known prime pairs (B_n, B_{n+1}) are

(2 089, 10 009), (229 771, 1 100 899), (33 629 651 653 051, 161 129 341 280 179).

7. Some generalizations

1. While the pair of congruences (2.1) already presents a significant generalization of the original pair (1.2), the following more general case can also be treated with our methods. Given the pair

$$p^2 \equiv \delta M \pmod{q}, \qquad q^2 \equiv \varepsilon N \pmod{p}, \tag{7.1}$$

with $\delta, \varepsilon \in \{-1, 1\}$ and M, N fixed positive integers, find solutions to (7.1) in odd primes p, q with $\gcd(pq, MN) = 1$. As we did in Section 2, we first transform (7.1) to

$$Mq^2 + \delta\varepsilon Np^2 = \varepsilon MN + kpq, \tag{7.2}$$

and then, completing the square, we obtain

$$(2Mq - kp)^2 - (k^2 - 4\delta\varepsilon MN)p^2 = 4\varepsilon M^2 N. \tag{7.3}$$

The identity (7.2) shows that k is a multiple of $d := \gcd(M, N)$, so if M and N are not relatively prime, then (7.3) can be reduced by dividing both sides by d^2. In any case, (7.3) is again a Pell-type equation which can be treated in a similar way as outlined in Section 6.

2. A further generalization is possible by removing the requirement that p and q be prime. The corresponding results can be obtained in similar ways as the results in this paper; once again, second order recurrences will usually be involved. However, all this would go beyond the scope of the present paper.

Acknowledgments

We would like to thank Wilfrid Keller for drawing our attention to the Fibonacci prime records in [11].

References

[1] A. V. Aho and N. J. A. Sloane, *Some doubly exponential sequences*, Fibonacci Quart. **11** (1973), 429–437.
[2] J. B. Cosgrave and K. Dilcher, *On a congruence of Emma Lehmer related to Euler numbers*, preprint, 2012.
[3] H. Dubner and W. Keller, *New Fibonacci and Lucas primes*, Math. Comp. **68** (1999), 417–427, S1–S12.
[4] J. P. Jones, *Representation of solutions of Pell equations using Lucas sequences*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **30** (2003), 75–86.
[5] M. Jacobson, Jr., and H. C. Williams, *Solving the Pell Equation*. Springer-Verlag, New York, 2009.
[6] T. Koshy, *Fibonacci and Lucas numbers with applications*. Wiley, New York, 2001.
[7] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math. **1** (1878), 184–240, 289–321. English translation: *The Theory of Simply Periodic Numerical Functions*, The Fibonacci Association, 1969. Available electronically at `http://www.fq.math.ca/simply-periodic.html`.
[8] T. Nagell, *Introduction to Number Theory*. 2nd ed., Chelsea Publishing Company, New York, 1964.
[9] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*. 5th ed., Wiley, 1991.
[10] O. Perron, *Die Lehre von den Kettenbrüchen*. 2nd ed., Chelsea Publishing Co., New York, N.Y., 1950.
[11] P. Ribenboim, *Die Welt der Primzahlen. Geheimnisse und Rekorde*. Zweite, vollständig überarbeitete und aktualisierte Auflage. Aus dem Englischen übersetzt fon Jörg Richstein. Auf den neuesten Stand gebracht von Wilfrid Keller. Springer-Verlag, Heidelberg, 2011.
[12] N. J. A. Sloane, *On-Line Encyclopedia of Integer Sequences*. `http//oeis.org/`.
[13] E. W. Weisstein, *Pell Equation*. From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/PellEquation.html`.
[14] E. W. Weisstein, *Pell Number*. From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/PellNumber.html`.

79 Rowanbyrn, Blackrock, County Dublin, Ireland
E-mail address: `jbcosgrave@gmail.com`

Department of Mathematics and Statistics, Dalhousie University, Halifax, Nova Scotia, B3H 3J5, Canada
E-mail address: `dilcher@mathstat.dal.ca`