MATHEMATICS OF COMPUTATION
VOLUME 45, NUMBER 172
OCTOBER 1985, PAGES 613-620

Sets in Which $xy + k$ is Always a Square

By Ezra Brown

Abstract. A P_k-set of size n is a set $\{x_1, \ldots, x_n\}$ of distinct positive integers such that $x_i x_j + k$ is a perfect square, whenever $i \neq j$; a P_k-set X can be extended if there exists $y \notin X$ such that $X \cup \{y\}$ is still a P_k-set. The most famous result on P_k-sets is due to Baker and Davenport, who proved that the P_1-set $\{1, 3, 8, 120\}$ cannot be extended. In this paper, we show, among other things, that if $k \equiv 2 \pmod 4$, then there does not exist a P_k-set of size 4, and that the P_{-1}-set $\{1, 2, 5\}$ cannot be extended.

1. Introduction and Background. Let k be an integer. A P_k-*set* (*of size* n) is a set $\{x_1, \ldots, x_n\}$ of distinct positive integers for which $x_i x_j + k$ is the square of an integer, whenever $i \neq j$. Thus, $\{1, 2, 5\}$ is a P_{-1}-set of size 3, $\{1, 79, 98\}$ is a P_2-set of size 3 and $\{51, 208, 465, 19732328\}$ is a P_1-set of size 4. A P_k-set X can be *extended* if there exists a positive integer $y \notin X$ such that $X \cup \{y\}$ is still a P_k-set.

The problem of extending P_k-sets is an old one, dating from the time of Diophantus (see Dickson [2, Vol. II, p. 513]). The most spectacular recent advance in this area was made by Baker and Davenport (see [1]) who proved that the P_1-set $\{1, 3, 8, 120\}$ cannot be extended. Their proof used results from Diophantine approximation and involved calculating four real numbers to 600 decimal digits. This problem was intriguing enough for three more distinct methods of proof to appear over the next ten years, by Kanagasabapathy and Ponnudurai [5], Sansone [8] and Grinstead [3]. Recently, Mohanty and Ramasamy [6] have shown that the P_{-1}-set $\{1, 5, 10\}$ cannot be extended, and Thamotherampillai [9] proved that the P_2-set $\{1, 2, 7\}$ cannot be extended. (For more details on the history of this problem, see [4, especially the references] and [2, Vol. II, pp. 513–520].)

The aim of this paper is to prove the following theorems about the nonextendability of P_k-sets:

THEOREM 1. *If* $k \equiv 2 \pmod 4$, *then there does not exist a* P_k-*set of size* 4. {*This greatly generalizes the theorem of* [9].}

THEOREM 2. *If* $k \equiv 5 \pmod 8$, *then there does not exist a* P_k-*set of size* 4 *with an odd* x_j *or with some* $x_j \equiv 0 \pmod 4$.

THEOREM 3. *The following* P_{-1}-*sets cannot be extended*:
(a) $\{n^2 + 1, (n+1)^2 + 1, (2n+1)^2 + 4\}$ *if* $n \not\equiv 0 \pmod 4$;
(b) $\{17, 26, 85\}$;
(c) $\{2, 2n^2 + 2n + 1, 2n^2 + 6n + 5\}$, *if* $n \equiv 1 \pmod 4$.

Received November 7, 1984; revised February 19, 1985.
1980 *Mathematics Subject Classification*. Primary 10B05, 10A10, 10A35.

THEOREM 4. *The P_{-1}-set $\{1, 2, 5\}$ cannot be extended.*

We note that the proofs of Theorems 1, 2 and 3 are straightforward and elementary, relying on nothing stronger than the Quadratic Reciprocity Law and theorems on the group of units of a quadratic field. Theorem 4, however, is more subtle, using the results of Baker [1] and the techniques of Grinstead [3].

2. Nonexistence of P_k-Sets of Size 4, for $k \equiv 2 \pmod 4$.

THEOREM 1. *If $k \equiv 2 \pmod 4$, then there does not exist a P_k-set of size 4.*

Proof. Suppose that $\{x_1, x_2, x_3, x_4\}$ is a P_k-set, with $k \equiv 2 \pmod 4$. Then

$$x_i x_j + k = y_{ij},$$

say. Looking at the equation (mod 4), we see that

$$x_i x_j + k \equiv 0 \text{ or } 1 \pmod 4$$

so that

$$x_i x_j \equiv 2 \text{ or } 3 \pmod 4.$$

Hence, at most one of the x_i can be even; without loss of generality, we may assume that x_1, x_2 and x_3 are odd. This implies that

$$x_i x_j \equiv 3 \pmod 4 \quad \text{for } 1 \leqslant i \neq j \leqslant 3.$$

Hence, no two of x_1, x_2, x_3 have the same residue (mod 4). As all three are odd, this is a contradiction. Thus, no P_k-set of size 4 can exist, if $k \equiv 2 \pmod 4$.

Comment. This is a considerable generalization of the result in [9], and the proof is much more elementary.

3. Nonexistence of Certain P_k-Sets, for $k \equiv 5 \pmod 8$.

THEOREM 2. *If $k \equiv 5 \pmod 8$, then there does not exist a P_k-set of size 4 with an odd x_j or with some $x_j \equiv 0 \pmod 4$.*

Proof. Suppose that $\{x_1, x_2, x_3, x_4\}$ is a P_k-set of size 4, with $k \equiv 5 \pmod 8$. Then $x_i x_j + k = a^2$ implies that

$$x_i x_j \equiv 3, 4 \text{ or } 7 \pmod 8.$$

If x_1 is odd and x_2 is even, then we must have $x_1 x_2 \equiv 0 \pmod 4$. In that case, x_3 and x_4 must be odd, else $x_2 x_3 \equiv 0 \pmod 8$. Thus,

$$x_1 x_3 \equiv x_1 x_4 \equiv 3 \pmod 4,$$

$$x_3 \equiv x_4 \pmod 4, \quad \text{and so}$$

$$x_3 x_4 \equiv 1 \pmod 4,$$

which is a contradiction. By the above reasoning, we see that a P_k-set can contain at most two odd x_j and one $x_j \equiv 0 \pmod 4$. We conclude that if $k \equiv 5 \pmod 8$, then a P_k-set of size 4 contains no odd x_j and no $x_j \equiv 0 \pmod 4$. Thus, if $\{x_1, x_2, x_3, x_4\}$ is a P_k-set, with $k \equiv 5 \pmod 8$, then $x_i \equiv 2 \pmod 4$ for all i.

4. Nonextendability of Certain P_{-1}-Sets. Suppose that $X = \{a, b, c\}$ is a P_k-set; if X can be extended, then there exist d, x, y and z such that

$$ad + k = x^2, \quad bd + k = y^2, \quad \text{and} \quad cd + k = z^2.$$

These lead to the equations

$$(*)\qquad \begin{cases} ay^2 - bx^2 = (a-b)k, \\ az^2 - cx^2 = (a-c)k, \quad \text{and} \\ bz^2 - cy^2 = (b-c)k. \end{cases}$$

The degree of difficulty of showing that X cannot be extended depends upon whether the system $(*)$ already has solutions that can be found by inspection. For example, if $k = 1$, then there are the obvious solutions $x = y = z = 1$. If $k = -1$ and $a = 1$, then $\{1, b, c\}$ is a P_{-1}-set, so that

$$b = n^2 + 1, \qquad c = m^2 + 1,$$

and so the system $(*)$ has the solution $x = 0$, $y = n$, $z = m$. If such solutions exist, then one must show that they are the only solutions. This is why Theorem 4 is a bit involved.

It is often easier if the aim is to show that the system $(*)$ has no solutions at all; Theorem 1 is a good example of that, as is Theorem 3.

THEOREM 3. *The following P_{-1}-sets cannot be extended*:
(a) $\{n^2 + 1, (n+1)^2 + 1, (2n+1)^2 + 4\}$, *if* $n \not\equiv 0 \pmod 4$;
(b) $\{17, 26, 85\}$;
(c) $\{2, 2n^2 + 2n + 1, 2n^2 + 6n + 5\}$, *if* $n \equiv 1 \pmod 4$.

Proof. (a) Suppose that $\{n^2 + 1, (n+1)^2 + 1, (2n+1)^2 + 4, d\}$ is a P_{-1}-set. Then the equations $(*)$ become

$$(1)\qquad (n^2+1)y^2 - \left((n+1)^2 + 1\right)x^2 = 2n + 1,$$

$$(2)\qquad (n^2+1)z^2 - \left((2n+1)^2 + 4\right)x^2 = 3n^2 + 4n + 4, \quad \text{and}$$

$$(3)\qquad \left((n+1)^2 + 1\right)z^2 - \left((2n+1)^2 + 4\right)y^2 = 3n^2 + 2n + 3.$$

First, suppose that n is odd; write $n = 4k + \varepsilon$, with $\varepsilon = \pm 1$. Then (1) becomes

$$2y^2 - x^2 \equiv \pm 1 \pmod 4,$$

so that x is odd.

If $\varepsilon = 1$, then

$$n^2 + 1 \equiv 8k + 2 \pmod{16},$$
$$(n+1)^2 + 1 \equiv 5 \pmod{16}, \quad \text{and}$$
$$(2n+1)^2 + 4 \equiv 13 \pmod{16}.$$

Hence, (3) becomes

$$5z^2 - 13y^2 \equiv 8 \pmod{16},$$

so that y and z are both odd. Then, (2) yields

$$(8k+2)z^2 - 13x^2 \equiv 8k + 11 \pmod{16},$$
$$2 + 3x^2 \equiv 11 \pmod{16},$$
$$x^2 \equiv 3 \pmod{16},$$

which is a contradiction.

If $\varepsilon = -1$, then

$$n^2 + 1 \equiv 8k + 2 \pmod{16},$$
$$(n+1)^2 + 1 \equiv 1 \pmod{16}, \quad \text{and}$$
$$(2n+1)^2 + 4 \equiv 5 \pmod{16}.$$

Thus, (1) and (3) become

$$2y^2 - x^2 \equiv -1 \pmod 8,$$
$$z^2 - 5y^2 \equiv 4 \pmod{16}.$$

Thus, y is even and z is even, but neither is divisible by 4. Putting $y = 2v$, $z = 2u$ with u and v odd yields

$$u^2 - 5v^2 \equiv 1 \pmod 4,$$

which is impossible with u and v odd.

Next, suppose that $n = 2k$ is even. Then (1) becomes

$$y^2 - 2x^2 \equiv 1 \pmod 4,$$

so that y is odd and x is even. Now (3) becomes

$$2z^2 - 5y^2 \equiv 4k + 3 \pmod 8,$$

so that z is even. Putting $z = 2u$ and $x = 2v$ in (2) leads to the equation

$$(4k^2+1)u^2 - (16k^2 + 8k + 5)v^2 = 3k^2 + 2k + 1.$$

If k is odd, this leads to the congruence

$$u^2 - 5v^2 \equiv \pm 2 \pmod 8,$$

which is impossible.

Thus, if $n \equiv 1$, 2 or 3 (mod 4), then the P_{-1}-set $\{n^2+1, (n+1)^2+1, (2n+1)^2 + 4\}$ cannot be extended.

(b) The situation for $n \equiv 0 \pmod 4$ is more complicated, and most likely will have to be studied on a case-by-case basis. One such case is $n = 4$, which corresponds to the P_{-1}-set $\{17, 26, 85\}$. Equations (1) and (2) become

$$17y^2 - 26x^2 = 9, \tag{4}$$
$$z^2 - 5x^2 = 4. \tag{5}$$

Modulo 16, (4) implies that $y^2 + 6x^2 \equiv 9 \pmod{16}$, which implies that x is even. Hence, z is also even; putting $z = 2u$ and $x = 2v$ yields

$$u^2 - 5v^2 = 1, \tag{6}$$
$$17y^2 - 104v^2 = 9. \tag{7}$$

Now all solutions to (6) are given by $u_n + v_n\sqrt5 = (9 + 4\sqrt5)^n$ for $n = 0, \pm1, \pm2, \ldots$ (see Nagell [7, p. 197]). It is easy to show that

$$v_0 = 0, \quad v_1 = 4, \quad v_{n+1} = 18v_n - v_{n-1} \quad \text{for } n \geqslant 1, \quad \text{and}$$
$$v_{-n} = -v_n \qquad \text{for } n \geqslant 1;$$

so it follows that $v \equiv 0$, 4 or 13 (mod 17).

If we look at Eq. (7) mod 17, we see that

$$-2v^2 \equiv 9 \pmod{17},$$
$$v^2 \equiv 4 \pmod{17},$$
$$v \equiv \pm 2 \pmod{17}.$$

Hence (6) and (7) have no common solution; we conclude that $\{17, 26, 85\}$ cannot be extended.

(c) Suppose that $\{2, 2n^2 + 2n + 1, 2n^2 + 6n + 5\}$ can be extended. Then, the equations $(*)$ become

$$2y^2 - (2n^2 + 2n + 1)x^2 = 2n^2 + 2n - 1, \tag{8}$$

$$2z^2 - (2n^2 + 6n + 5)x^2 = 2n^2 + 6n + 3, \quad \text{and} \tag{9}$$

$$(2n^2 + 2n + 1)z^2 - (2n^2 + 6n + 5)y^2 = 4n + 4. \tag{10}$$

Examining these equations mod 4 shows that

$$2y^2 - x^2 \equiv -1 \pmod 4,$$

$$2z^2 - x^2 \equiv 3 \pmod 4,$$

so that x is odd, y is even and z is even. Putting $y = 2v$, $z = 2u$ into (10) yields

$$u^2 - v^2 \equiv n + 1 \pmod 4,$$

which is impossible if $n \equiv 1 \pmod 4$.

5. Nonextendability of the P_1-Set $\{1, 2, 5\}$. We follow the procedure outlined by Grinstead in [3]. If $\{1, 2, 5\}$ is extendable, then the equations $(*)$ become

$$y^2 - 2x^2 = 1, \quad z^2 - 5x^2 = 4, \quad 2z^2 - 5y^2 = 3,$$

so that the two equations

$$y^2 - 8t^2 = 1, \tag{11}$$

$$u^2 - 5t^2 = 1 \tag{12}$$

(where $z = 2u$, $x = 2t$) have a common solution other than $t = 0$, $y = u = 1$. (The solution $t = 0$, $y = u = 1$ corresponds to the fact that $\{1, 2, 5\}$ is a P_{-1}-set.) We will now show that the equations (11) and (12) have no other common solution.

It is well-known (see Nagell [7, p. 197]) that the solutions to the equations

$$y^2 - 8v^2 = 1, \tag{13}$$

$$u^2 - 5w^2 = 1, \tag{14}$$

are given by

$$y_n + v_n\sqrt{8} = (3 + \sqrt{8})^{n-1}, \quad n \text{ an integer}, \quad \text{and}$$

$$z_k + w_k\sqrt{5} = (9 + 4\sqrt{5})^{k-1}, \quad k \text{ an integer}.$$

Without loss of generality, we may assume $v_n \geqslant 0$, $w_k \geqslant 0$; hence $n, k \geqslant 1$. We see that

$$v_n = \frac{(3 + \sqrt{8})^{n-1} - (3 - \sqrt{8})^{n-1}}{2\sqrt{8}} \quad \text{and} \quad w_k = \frac{(9 + 4\sqrt{5})^{k-1} - (9 - 4\sqrt{5})^{k-1}}{2\sqrt{5}}.$$

Put

$$P = (3 + \sqrt{8})^{n-1}/\sqrt{8}, \qquad Q = (9 + 4\sqrt{5})^{k-1}/\sqrt{5}.$$

If there is a common solution to (11) and (12) other than $t = 0$, then there exist $n \geqslant 2$ and $k \geqslant 2$ such that $v_n = t = w_k$, in which case

$$P - \tfrac{1}{8}P^{-1} = 2v_n = 2w_k = Q - \tfrac{1}{5}Q^{-1}.$$

Hence,

$$P - Q = \tfrac{1}{8}P^{-1} - \tfrac{1}{5}Q^{-1} < \tfrac{1}{5}\left(P^{-1} - Q^{-1}\right) = \tfrac{1}{5}P^{-1}Q^{-1}(Q - P).$$

Also, $P^{-1} < 1$ and $Q^{-1} < 1$ (because $n, k \geqslant 2$), so that

$$P - Q < \tfrac{1}{5}(Q - P).$$

It follows that $P - Q < 0$, so that $P < Q$ and $Q^{-1} < P^{-1}$. Hence

$$0 < Q - P = \tfrac{1}{5}Q^{-1} - \tfrac{1}{8}P^{-1} < \left(\tfrac{1}{5} - \tfrac{1}{8}\right)P^{-1} = \tfrac{3}{40}P^{-1},$$

so that

$$0 < \frac{Q - P}{Q} < \frac{3}{40}P^{-1}Q^{-1} < \frac{3}{40}P^{-2} < 1. \tag{15}$$

Hence,

$$\log\left(1 - \frac{Q - P}{Q}\right) = \log\frac{P}{Q} < 0.$$

Thus,

$$0 < \log\frac{Q}{P} = -\log\frac{P}{Q} = -\log\left(1 - \frac{Q - P}{Q}\right).$$

Now if $0 < r < 1$, then

$$\begin{aligned}-\log(1 - r) &= r + \frac{r^2}{2} + \frac{r^3}{3} + \frac{r^4}{4} + \cdots < r + \frac{r^2}{2}(1 + r + r^2 + \cdots)\\ &= r + \frac{r^2}{2}\cdot\frac{1}{1 - r}.\end{aligned}$$

Setting $r = (Q - P)/Q$, we have, from (15), that

$$0 < r < \tfrac{3}{40}P^{-2} < \tfrac{1}{10},$$

so that

$$\frac{1}{1 - r} < \frac{10}{9}.$$

Furthermore, $P > 1$, so that $P^{-4} < P^{-2}$, and so finally

$$\begin{aligned}0 < \log\frac{Q}{P} &= -\log\left(1 - \frac{Q - P}{Q}\right) < \frac{Q - P}{Q} + \frac{5}{9}\left(\frac{Q - P}{Q}\right)^2\\ &< \frac{3}{40}P^{-2} + \frac{5}{9}\cdot\frac{9}{1600}P^{-4} < \frac{3}{40}P^{-2} + \frac{1}{320}P^{-2}\\ &= \frac{5}{64}P^{-2} = \frac{5}{8}\cdot\frac{1}{(3 + \sqrt{8})^{2n-2}}.\end{aligned}$$

It is clear that $3 + \sqrt{8} > e$, so that we obtain

$$\begin{aligned}0 < \log\frac{Q}{P} &= \log\frac{\sqrt{8}\,(9 + 4\sqrt{5})^{k-1}}{\sqrt{5}\,(3 + \sqrt{8})^{n-1}}\\ &= (k - 1)\log(9 + 4\sqrt{5}) - (n - 1)\log(3 + \sqrt{8}) + \log\frac{\sqrt{8}}{\sqrt{5}} \qquad (16)\\ &< \frac{5}{8}e^{-(n-1)} < e^{-(n-1)}.\end{aligned}$$

We now appeal to a deep theorem of Baker (see [1]), which says that if $m \geqslant 2$, and $\alpha_1, \ldots, \alpha_m$ are nonzero algebraic numbers of degrees $\leqslant d$ and heights $\leqslant A$, where $d \geqslant 4$, $A \geqslant 4$, and if the rational integers $b_1, \ldots, b_m$ satisfy

$$0 < |b_1 \log \alpha_1 + \cdots + b_m \log \alpha_m| < e^{-\delta H},$$

where $0 < \delta \leqslant 1$ and $H = \max(|b_1|, \ldots, |b_m|)$, then

$$H < \left(4^{m^2}\delta^{-1}d^{2m}\log A\right)^{(2m+1)^2}. \tag{17}$$

Here, $H = n - 1$ (plainly $n \geqslant k$), $m = 3$ and we can choose $\delta = 1$ in (16). The equations for $\alpha_1 = 9 + 4\sqrt{5}$, $\alpha_2 = 3 + \sqrt{8}$ and $\alpha_3 = \sqrt{1.6}$ are

$$\alpha_1^2 - 18\alpha_1 + 1 = 0, \quad \alpha_2^2 - 6\alpha_2 + 1 = 0, \quad \text{and} \quad 5\alpha_3^2 - 8 = 0.$$

This yields a maximum height of $A = 18$, and we can choose $d = 4$. Thus, (17) becomes

$$n - 1 = H < \left(4^9 \cdot 4^6 \cdot \log 18\right)^{49} = 4^{735}(\log 18)^{49} < 4^{735} \cdot 3^{49} < 10^{466}.$$

Hence, any n such that $v_n = w_k = t$ is a common solution to (11) and (12) satisfies $1 \leqslant n \leqslant 10^{466}$. To show that $n = 1$ is the only solution in this range, it suffices to show $n \equiv 1 \pmod{M}$, where M is any integer $\geqslant 10^{466}$. It happens that

$$M = \prod_{p \leqslant 1103} p,$$

the product of all primes $\leqslant 1103$, is such an integer. The reason for choosing the M is clear: if, for all primes $p \leqslant 1103$, we can show that $n \equiv 1 \pmod{p}$, then $n \equiv 1 \pmod{M}$ by the Chinese Remainder Theorem.

We adopt Grinstead's strategy [3] to fit our problem; let us outline the procedure here.

Let p be a prime $\leqslant 1103$, such that for all primes $r < p$, it has been shown that if $v_n = w_k$, then $n \equiv 1 \pmod{r}$; also, we assume $n \equiv 1 \pmod{2^2 \cdot 3^3}$, which takes 5 minutes with a pocket calculator to show (just examine $\{v_n\}$ and $\{w_k\}$ mod 8 and 53).

It is easier to work with v_n and w_k when we realize that they are defined by the following recurrences:

$$v_1 = 0, \quad v_2 = 1; \quad v_{n+1} = 6v_n - v_{n-1} \quad \text{for } n \geqslant 2;$$
$$w_1 = 0, \quad w_2 = 4; \quad w_{k+1} = 18w_k - w_{k-1} \quad \text{for } k \geqslant 2.$$

If we define $L(q)$ to be the length of the period of the sequence $\{v_n\} \pmod{q}$, let us generate a sequence of primes q such that $L(q)$ is divisible only by primes not exceeding p, is power-free (except possibly for 2^2, 3^2 and 3^3) and is divisible by p. By our previous assumption, $v_n = w_k$ implies that $n \equiv 1 \pmod{L(q)/p}$, for each such q.

Choose the least such q, and consider $\{v_n\}$ and $\{w_k\}$ mod q. By previous remarks, there are only p possible indices for which $v_n \equiv w_k \pmod{q}$: just those indices $\equiv 1 \pmod{L(q)/p}$. If a number v_n in one of those positions does not appear in the listing of $w_k \pmod{q}$, that position is deleted. If all such positions are deleted, except $n \equiv 1 \pmod{L(q)}$, then we have shown that $n \equiv 1 \pmod{p}$, and we go on to the next p. If any positions are not eliminated, we note them and go on to the next q: at the next q, we only need to check those positions not previously eliminated. Eventually, all positions except $n \equiv 1 \pmod{p}$ will be eliminated; in the actual running of this algorithm, no prime p required more than 10 values of q to be eliminated.

Let us demonstrate how this works with $p = 11$. First, let $q = 23$, because $L(23) = 11$. The sequence $\{v_n\} \pmod{23}$ is as follows:

$$\{0, 1, 6, 12, 20, 16, 7, 3, 11, 17, 22\}.$$

Now the sequence $\{w_k\} \pmod{23}$ looks like this:

$$\{0, 4, 3, 4, 0, 19, 20, 19\}.$$

Hence, all positions are eliminated except those corresponding to $v_n \equiv 0$, 3 or 20 $\pmod{23}$; thus, if $v_n = w_k$, then $n \equiv 1$, 5, or 8 $\pmod{11}$.

Next, let $q = 43$, as $L(43) = 44$. Then $\{v_n\} \pmod{43}$ is as below:

$$\{0, 1, 6, 35, 32, 28, 7, 14, 34, 18, 31, 39, 31, 18, 34, 14,$$
$$7, 28, 32, 35, 6, 1, 0, 42, 37, 8, 11, 15, 36, 29, 9, 25, 12,$$
$$4, 12, 25, 9, 29, 36, 15, 11, 8, 37, 42\}.$$

But we know that $n \equiv 1 \pmod{4\ (= 44/11)}$, so that we only need look at the positions corresponding to $n \equiv 1, 5, 9, \ldots, 37, 41 \pmod{44}$. Furthermore, we saw from our work $\pmod{23}$ that $n \equiv 1$, 5 or 8 $\pmod{11}$, so that we need only consider $n \equiv 1$, 5 or 41 $\pmod{44}$. This leaves the values

$$v_n \equiv 0, 32, 11 \pmod{43}.$$

But $\{w_k\} \pmod{43}$ looks like this:

$$\{0, 4, 29, 41, 21, 36, 25, 27, 31, 15, 24, 30, 0, 13, 19, 28,$$
$$12, 16, 18, 7, 22, 2, 14, 39\}.$$

Neither 32 nor 11 appears on this last list, so we have shown that $n \equiv 1 \pmod{11}$.

Curiously, $p = 7$ needs three values of q to eliminate all but $n \equiv 1 \pmod 7$, namely $q = 13$ (which eliminates $n \equiv 0, 2 \pmod 7$), $q = 83$ (which deletes $n \equiv 4, 6 \pmod 7$) and $q = 113$ (which disposes of $n \equiv 3, 5 \pmod 7$). On the other hand, $p = 31$ needs only $q = 61$ to eliminate all but $n \equiv 1 \pmod{31}$.

It is not possible to predict $L(q)$ in advance, except that it can be shown that $L(q)$ is a factor of $q^2 - 1$. Moreover, if 2 is a quadratic residue of q, then $L(q) | q - 1$.

Department of Mathematics
Virginia Polytechnic Institute
and State University
Blacksburg, Virginia 24061-4097

1. A. Baker & H. Davenport, "The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$," *Quart. J. Math. Oxford Ser.* (3), v. 20, 1969, pp. 129–137.

2. L. E. Dickson, *History of the Theory of Numbers*, vol. II, Carnegie Institute, Washington, 1920; reprinted, Chelsea, New York, 1966.

3. C. M. Grinstead, "On a method of solving a class of Diophantine equations," *Math. Comp.*, v. 32, 1978, pp. 936–940.

4. P. Heichelheim, "The study of positive integers (a, b) such that $ab + 1$ is a square," *Fibonacci Quart.*, v. 17, 1979, pp. 269–274.

5. P. Kanagasabapathy & T. Ponnudurai, "The simultaneous Diophantine equations $y^2 - 3x^2 = -2$ and $z^2 - 8x^2 = -7$," *Quart. J. Math. Oxford Ser.* (3), v. 26, 1975, pp. 275–278.

6. S. P. Mohanty & A. M. S. Ramasamy, "The simultaneous Diophantine equations $5Y^2 - 20 = X^2$ and $2Y^2 + 1 = Z^2$," *J. Number Theory*, v. 18, 1984, pp. 356–359.

7. T. Nagell, *Introduction to Number Theory*, Wiley, New York, 1951.

8. G. Sansone, "Il sistema diofanteo $N + 1 = x^2$, $3N + 1 = y^2$, $8N + 1 = z^2$," *Ann. Mat. Pura Appl.* (4), v. 111, 1976, pp. 125–151.

9. N. Thamotherampillai, "The set of numbers $\{1, 2, 7\}$," *Bull. Calcutta Math. Soc.*, v. 72, 1980, pp. 195–197.