PACIFIC JOURNAL OF MATHEMATICS
Vol. 139, No. 2, 1989

THE DIOPHANTINE EQUATION $x^2 = 4q^n - 4q + 1$

CHRIS SKINNER

In this paper all integral solutions to the equation $x^2 = 4q^n - 4q + 1$ when q is an odd prime are determined. This is done by working in a quadratic field, using the unique factorization of ideals to reduce the problem to one about certain binary linear recurrences. One of the results is that the equation has no solutions with $n > 2$ if $q > 5$.

0. Introduction. In 1913 the Indian mathematician S. Ramanujan conjectured that the equation $x^2 = 2^n - 7$ had only five solutions in positive integers. The solutions he gave were:

$$\begin{array}{cccccc} n = 3 & 4 & 5 & 7 & 15 \\ x = 1 & 3 & 5 & 11 & 181 \end{array}$$

This conjecture was first proved by T. Nagell in 1948. There followed during the period 1950–70 a number of proofs based on a variety of methods (see for example [2], [5]). The purpose of this paper is to solve a generalized form of the Ramanujan equation: $x^2 = 4q^n - 4q + 1$ where q is any odd prime.

In Nagell's paper unique factorization of integers was used to reduce the problem to one about a binary linear recurrence which was then solved using p-adic methods. To solve the title equation for all odd primes q, we will use unique factorization of ideals along with linear recurrences and congruences. Most importantly, we show that for $q > 5$ there exist no solutions with $n > 2$.

1. The diophantine equation $x^2 = 4q^n - 4q + 1$. We will determine the values of n which provide solutions to the title equation: $x^2 = 4q^n - 4q + 1$, which we prefer to view as

$$x^2 + 4q - 1 = 4q^n \tag{1}$$

where q is any prime. The two obvious solutions that exist for all q are $x = 1, 2q - 1$ with $n = 1, 2$, respectively. We now prove the following theorems which provide a characterization of solutions to (1).

THEOREM 1. *The only even n for which $x^2 + 4q - 1 = 4q^n$ has a solution is $n = 2$.*

Proof. Let $m = n/2$. Then $4q - 1 = (2q^m + x)(2q^m - x)$. If $m > 1$, then $2q^m > 4q - 1$.

THEOREM 2. *$x^2 + 4q - 1 = 4q^n$ has a solution if and only if $b_n = \pm 1$ where $\{b_k\}$ is defined recursively by $b_k = b_{k-1} - qb_{k-2}$, $k > 2$, $b_1 = b_2 = 1$.*

Proof. Clearly any solution x is odd. Let $\gamma = (x-1)/2$, $d = 4q - 1$, $\zeta = (1 + \sqrt{-d})/2$, $\zeta' = (1 - \sqrt{-d})/2$, and $\mathbf{R}$ the ring of integers of $\mathbf{Q}(\zeta)$. Equation (1) can now be written as

$$(\gamma + \zeta)(\gamma + \zeta') = \zeta^n \zeta'^n \tag{2}$$

and so

$$\langle \gamma + \zeta \rangle \langle \gamma + \zeta' \rangle = \langle \zeta \rangle^n \langle \zeta' \rangle^n \tag{3}$$

where $\langle \alpha \rangle$ means the ideal generated by α. By algebraic number theory the ideals on the right in (3) are seen to be the decomposition of $\langle q^n \rangle$ into prime ideals. We now show that the ideals on the left in (3) are relatively prime. The factors $(\gamma + \zeta)$ and $(\gamma + \zeta')$ are easily seen to be relatively prime. Assume there is some prime ideal π which divides both of these. Then π divides their sum x and their difference $\sqrt{-d}$. Upon taking norms we find that $\mathrm{Norm}(\pi)$ must divide x^2 and d. However, this implies $\mathrm{Norm}(\pi) = 2$ or q, both of which are prime to d. It follows that $(\gamma + \zeta)$ and $(\gamma + \zeta')$ are relatively prime. Note that ζ and ζ' are not units in $\mathbf{R}$. Now if $\langle \zeta \rangle | \langle \gamma + \zeta \rangle$ and $\langle \zeta \rangle | \langle \gamma + \zeta' \rangle$ then there exist $\alpha, \beta \in \mathbf{R}$ such that $\alpha\zeta = (\gamma + \zeta)$ and $\beta\zeta = (\gamma + \zeta')$. However, this is impossible since $(\gamma + \zeta)$ and $(\gamma + \zeta')$ are relatively prime. The same argument holds if we assume that $\langle \zeta' \rangle | \langle \gamma + \zeta \rangle$ and $\langle \zeta' \rangle | \langle \gamma + \zeta' \rangle$. It follows that $\langle \gamma + \zeta \rangle$ and $\langle \gamma + \zeta' \rangle$ are relatively prime. Thus we must have

$$\langle \zeta \rangle^n = \langle \gamma + \zeta \rangle \quad \text{or} \quad \langle \zeta \rangle^n = \langle \gamma + \zeta' \rangle$$

and so

$$\zeta^n = \pm(\gamma + \zeta) \quad \text{or} \quad \zeta^n = \pm(\gamma + \zeta').$$

We know that $\zeta + \zeta' = 1$ and $\zeta\zeta' = q$ so $\zeta^2 = \zeta - q$. From this we find $\zeta^n = \pm(\gamma + \zeta)$ or $\zeta^n = \pm(\gamma + 1 - \zeta)$. We now write ζ^n in the form $a + b\zeta$, $a, b \in \mathbf{Z}$. Thus if n is a solution to (1), $b = \pm 1$. Letting $\zeta^k = a_k + b_k\zeta$, we have $\zeta^{k+1} = -qb_k + (a_k + b_k)\zeta$. It follows that $b_k = b_{k-1} - qb_{k-2}$, $b_1 = b_2 = 1$. Thus we have the linear recurrence found in the statement of the theorem.

If $b_n = \pm 1$ for some n, then $4\zeta^n\zeta'^n = (2a_n \pm 1)^2 + 4q - 1$ and we have a solution to (1).

THEOREM 3. *If n is an integer, $n > 2$ such that $b_n = \pm 1$, then n is of the form $n = qk + 2$ and $q \neq 3$, $n \equiv 1$ or $2 \pmod 6$.*

Proof. It is easily seen that $b_n = qc_n + 1$ where $\{c_n\}$ is defined recursively by $c_n = c_{n-1} - qc_{n-2} - 1$ and $c_1 = c_2 = 0$. Since $q > 2$, -1 never appears in $\{b_n\}$ and so we concern ourselves only with the case $b_n = 1$. Now $b_n = 1$ iff $c_n = 0$, so we consider $\{c_n\}$ modulo q. The first few terms of this series are

$$0, 0, q-1, \ldots, 2, 1, 0, q-1, \ldots.$$

This series has period q, and for $n > 2$, c_n can equal 0 only if n is of the form $qk + 2$. Since $b_n = 1$ only when $c_n = 0$, $b_n = 1$ only if n is of the form $n = qk + 2$.

Now consider the series $\{b_n\}$ modulo $q - 1$. The first eight terms of this series are

$$1, 1, 0, -1, -1, 0, 1, 1, \ldots.$$

This series has period 6 and so if n is a solution to (1) then $n \equiv 1$ or $2 \pmod 6$. The case $q = 3$ is an exception since $-1 \equiv 1 \pmod 2$.

In the following theorems we find all solutions to (1). In the first we show that for $q > 5$ there are no solutions with $n > 2$. In the second we find all solutions for $q = 3$ and 5.

THEOREM 4. *If q is an odd prime > 5 then the only solutions to $x^2 + 4q - 1 = 4q^n$ occur when $n = 1$ and 2.*

Proof. In Theorem 3 we have shown that if n is a solution to (1) then $n = qk + 2$ and $n \equiv 1$ or $2 \pmod 6$. However, if $n \equiv 2 \pmod 6$ and $(6, q) = 1$ then $k \equiv 0 \pmod 6$ and so n is even. But in Theorem 1 we have shown that the only even n for which a solution exists is $n = 2$. The case when $n \equiv 1 \pmod 6$ is a little more complicated. It is well known that the binary linear recurrence of Theorem 2 can be written as

$$b_k = \varepsilon\alpha^k + \delta\beta^k$$

where α, β are the roots of $x^2 = x - q$ and

$$\varepsilon = (b_1 - b_0\beta)/(\alpha - \beta) \quad \text{and} \quad \delta = (b_0\alpha - b_1)/(\alpha - \beta).$$

In this case $\alpha = \zeta$, $\beta = \zeta'$ and $\varepsilon = -\delta = (\zeta - \zeta')^{-1}$ so

$$b_k = (\zeta^k - \zeta'^k)/(\zeta - \zeta').$$

Suppose $n \equiv 1 \pmod 6$; then we wish to solve

$$\zeta^{m+1} - \zeta'^{m+1} = \zeta - \zeta' \quad \text{where } m = n - 1. \tag{4}$$

Now $\zeta^3 + 1 = (\zeta + 1)(\zeta^2 - \zeta + 1) = -(\zeta + 1)(q - 1)$. If $m = 3r$, then (4) implies

$$\zeta(1 + (q-1)(\zeta+1))^r - \zeta'(1 + (q-1)(\zeta'+1))^r = \zeta - \zeta'. \tag{5}$$

Now $q - 1 \neq 1, 2, 4$, so $(q-1)/2$ does not divide

$$(\zeta(\zeta + 1) - \zeta'(\zeta' + 1))/(\zeta - \zeta') = 2.$$

Equation (5) can be written as

$$\zeta - \zeta' + \sum_{k=1}^{r} \binom{r}{k} (q-1)^k (\zeta(\zeta+1)^k - \zeta'(\zeta'+1)^k) = \zeta - \zeta',$$

and we obtain

$$r \sum_{k=1}^{r} (q-1)^{k-1}/k \binom{r-1}{k-1} (\zeta(\zeta+1)^k - \zeta'(\zeta'+1)^k)/(\zeta - \zeta') = 0.$$

If $r > 0$, the sum must vanish. It is easily seen that $(q-1)^{k-1}/k \equiv 0 \pmod{(q-1)/2}$ if $k = 2$ and $(q-1)^{k-1}/k \equiv 0 \pmod{q-1}$ if $k > 2$. This implies that $(q-1)/2$ divides the first term of the sum

$$(\zeta(\zeta + 1) - \zeta'(\zeta' + 1))/(\zeta - \zeta'),$$

which we have already seen to be impossible. Thus r must equal 0, and $n = 1$ gives the only solution to (1) with $n \equiv 1 \pmod 6$ and $q > 5$.

THEOREM 5. *The solutions to* $x^2 + 4q - 1 = 4q^n$ *when* $q = 3$ *and* 5 *are as follows*:

(i) $q = 3$

$n =$	1	2	5
$x =$	1	5	31

(ii) $q = 5$

$n =$	1	2	7
$x =$	1	9	559

In the proof of this theorem we will make use of the following two lemmas.

LEMMA 1. *If n is a solution to $x^2 + 4q - 1 = 4q^n$, then n satisfies $2^{n-1} \equiv n \pmod{d}$ where $d = 4q - 1$.*

Proof. We have seen that if n is a solution to (1), then $\zeta^n - \zeta'^n = \zeta - \zeta'$. Expanding the left side and reading it modulo d we find

$$2^{n-1} \equiv n \pmod{d}.$$

LEMMA 2. *If n and m give solutions to (1) then n cannot be congruent to m modulo $d\phi(d)$, d a prime.*

Proof. The proof of this theorem follows the same reasoning as one that appeared in [**6**] for the case $d = 7$. Assume that m and n are two such solutions. Let d^e be the highest power of d dividing $m - n$. Then

$$\zeta^n = \zeta^m \zeta^{n-m} = \zeta^m (1/2)^{n-m} (1 + \sqrt{-d})^{n-m}. \tag{6}$$

Now

$$(1/2)^{n-m} = [(1/2)^{\phi(d)}]^{(n-m)/\phi(d)} \equiv 1 \pmod{d^{e+1}}$$

and

$$(1 + \sqrt{-d})^{n-m} \equiv 1 + (n - m)\sqrt{-d} \pmod{d^{e+1}}.$$

(First raise to the powers $d, d^2, \ldots, d^e$, then to the power $(n - m)/d^e$.) Since

$$\zeta^m \equiv (1 + m\sqrt{-d})/2^m \pmod{d^{e+1}}$$

substituting in (6) gives

$$\zeta^n \equiv \zeta^m + [(n - m)\sqrt{-d}]/2^m \pmod{d^{e+1}}$$

and

$$\zeta'^n \equiv \zeta'^m - [(n - m)\sqrt{-d}]/2^m \pmod{d^{e+1}}.$$

But

$$\zeta^m - \zeta'^m = \zeta^n - \zeta'^n,$$

so

$$(m - n)\sqrt{-d} \equiv 0 \pmod{d^{e+1}}.$$

Since m and n are integers,

$$m \equiv n \pmod{d^{e+1}}$$

which contradicts the definition of e. It follows that there are no solutions to (1) congruent modulo $d\phi(d)$.

It is now relatively easy to find the solutions to (1) for the cases $q = 3, 5$. By Lemma 2 all possible n are uniquely congruent to numbers

less than $qd\phi(d)$. Thus we search for numbers of the form $qk+2$ less than $qd(d-1)$ which satisfy the restriction of Lemma 1.

Carrying these computations out on a computer we find the following solutions to $2^{n-1} \equiv n \pmod{d}$:

$$\begin{aligned} q &= 3 \\ &\qquad n \equiv 2, 5 \pmod{330} \\ q &= 5 \\ &\qquad n \equiv 2, 7 \pmod{1710} \end{aligned}$$

All of these provide solutions to (1) and it follows from Lemma 2 that they are the only solutions. Thus we have proved Theorem 5.

2. Summary of results. In the preceding section we have solved the title equation for all odd primes. In particular we have shown:

(i) The diophantine equation $x^2+11 = 4\cdot 3^n$ has only the solutions given by

$$\begin{array}{cccc} n = & 1 & 2 & 5 \\ x = & 1 & 5 & 31 \end{array}$$

(ii) The diophantine equation $x^2+19 = 4\cdot 5^n$ has only the solutions given by

$$\begin{array}{cccc} n = & 1 & 2 & 7 \\ x = & 1 & 9 & 559 \end{array}$$

(iii) The diophantine equation $x^2 + 4q - 1 = 4q^n$ $(q > 5)$ has only the solutions given by

$$\begin{array}{cccc} n = & 1 & & 2 \\ x = & 1 & & 2q-1 \end{array}$$

3. Discussion. We have thus solved the diophantine equation $x^2 = 4q^n - 4q + 1$ for all odd primes q. As already noted, the case when $q = 2$ has been discussed elsewhere (see for example [5]). The methods used in this paper are mostly elementary. By elementary we mean we have not used analytic number theory. In fact, the only place where knowledge of even algebraic number theory is necessary is in the proof of Theorem 2. There are other more advanced methods which could be used to solve similar types of problems. The most prominent of these is Skolem's p-adic method. In [5] this has been used to solve the case $q = 2$. Petho and de Weger in [3] give a method for solving a similar type equation based on the powerful methods of p-adic and complex Gelfond-Baker theory. However, this method is purely algorithmic and insufficient when trying to determine all solutions for a class of equations as in this paper.

A number of equations similar to the one discussed in this paper have been solved. Tzanakis in [7] discusses the equation $y^2 - D = 2^k$. In [8] Tzanakis and Wolfskill discuss the Calderbank equation $y^2 = 4q^n + 4q + 1$ where q is a prime power.

Though Ramanujan introduced his problem as essentially one in number theory, it has turned out to have applications to such diverse areas as coding theory [4] and differential algebra [1]. It is possible that the equations discussed in this paper may have similar applications in these areas. The Calderbank equation, which is very similar in form, arose from a study of a certain class of codes.

References

[1] D. G. Mead, *The equation of Ramanujan-Nagell and* $[y^2]$, Proc. Amer. Math. Soc., **4** (1973), 333–341.

[2] L. J. Mordell, *Diophantine Equations*, Academic Press, New York (1969), 205–206.

[3] A. Petho and B. M. M. de Weger, *Products of prime powers in binary recurrence sequences* I, Math. Comp., **47** (1986), 713–727.

[4] H. S. Shapiro and D. L. Slotnik, *On the mathematical theory of error correcting codes*, IBM J. Res. Develop., **3** (1959), 25–34.

[5] Th. Skolem, S. Chowla, and D. J. Lewis, *The diophantine equation* $2^{n+2} - 7 = x^2$ *and related problems*, Proc. Amer. Math. Soc., **10** (1959), 663–669.

[6] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*, Chapman and Hall, London (1979).

[7] N. Tzanakis, *On the diophantine equation* $y^2 - D = 2^k$, J. Number Theory, **17** (1983), 144–164.

[8] N. Tzanakis and J. Wolfskill, *On the diophantine equation* $y^2 = 4q^n + 4q + 1$, J. Number Theory, **23** (1986), 219–237.

Received April 22, 1988 and in revised form June 27, 1988.

3724 Sierra Forest Drive
Little Rock, AR 72212