Canad. Math. Bull. Vol. **28** (3), 1985

NUMBERS DIFFERING FROM CONSECUTIVE SQUARES BY SQUARES

BY

E. J. BARBEAU

Dedicated to the memory of R. A. Smith

ABSTRACT. It is shown that there are infinitely many natural numbers which differ from the next four greater perfect squares by a perfect square. This follows from the determination of certain families of solutions to the diophantine equation $2(b^2 + 1) = a^2 + c^2$. However, it is essentially known that any natural number with this property cannot be 1 less than a perfect square. The question whether there exists a number differing from the next five greater squares by squares is open.

1. **Introduction**. The numbers 720 and 5040 have the interesting property that each differs from the next three greater perfect squares by a perfect square. Thus,

$$720 = 27^2 - 3^2 = 28^2 - 8^2 = 29^2 - 11^2$$

$$5040 = 71^2 - 1^2 = 72^2 - 12^2 = 73^2 - 17^2.$$

We will show that, not only do such numbers occur frequently, there are infinitely many which differ from each of the next *four* greater perfect squares by a perfect square. Any number N which differs from the next four greater squares by a square must satisfy, for suitable z, a, b, c:

$$(z - 1)^2 \leqslant N = z^2 - a^2 = (z + 1)^2 - b^2$$
$$= (z + 2)^2 - c^2 = (z + 3)^2 - d^2.$$

This reduces to determining non-consecutive integers a, b, c, d to satisfy

$$2(b^2 + 1) = a^2 + c^2 \tag{1}$$

$$2(c^2 + 1) = b^2 + d^2 \tag{2}$$

$$b^2 \geqslant 2(a^2 + 1). \tag{3}$$

Inequality (3) arises from $2z - 1 \geqslant a^2$ and $2z + 1 = b^2 - a^2$. Since both a and c must be of opposite parity to both b and d, any solution of (1), (2), (3) will yield the requisite integers z and N.

Numerical evidence reveals one class of solutions for (1) and (2) with

Received by the editors June 4, 1984 and, in revised form, September 4, 1984.
AMS Subject Classification (1980): 10B05.

$$a = 2k^3 - 5k = 2(k + \tfrac{1}{2})^3 - 3(k + \tfrac{1}{2})^2 - \tfrac{7}{2}(k + \tfrac{1}{2}) + \tfrac{9}{4}$$
$$b = 2k^3 + 2k^2 - k + 1 = 2(k + \tfrac{1}{2})^3 - (k + \tfrac{1}{2})^2 - \tfrac{3}{2}(k + \tfrac{1}{2}) + \tfrac{7}{4}$$
$$c = 2k^3 + 4k^2 + k - 2 = 2(k + \tfrac{1}{2})^3 + (k + \tfrac{1}{2})^2 - \tfrac{3}{2}(k + \tfrac{1}{2}) - \tfrac{7}{4}$$
$$d = 2k^3 + 6k^2 + k - 3 = 2(k + \tfrac{1}{2})^3 + 3(k + \tfrac{1}{2})^2 - \tfrac{7}{2}(k + \tfrac{1}{2}) - \tfrac{9}{4}.$$

The reader will note that $d(k) = a(k + 1)$, and also that $a(k) = -d(-1 - k)$ and $b(k) = -c(-1 - k)$, so that the solutions for negative integers k are the negatives of the solutions for $k \geqslant 2$. For $k = 0, 1$, the absolute values of a, b, c, d are consecutive. Since the limit of b/a as $k \to +\infty$ is 1, (3) will be satisfied only for a finite number of k. However, there are some solutions of (1) and (2) other than these, such as (16, 87, 122, 149), so there is still hope for (1), (2), (3) to have infinitely many solutions.

2. **A different class of solutions**. The first step is to produce solutions to (1), some of which may lead to solutions of (2) as well. The form of (1) reminds us of the Euler identity

$$(4) \qquad (p^2 + q^2)(r^2 + s^2) = (pr + qs)^2 + (ps - qr)^2 = (ps + qr)^2 + (pr - qs)^2.$$

The substitution $p = q = r = 1$, $s = b$ yields solutions to (1) with a, b, c consecutive. For non-consecutive integer solutions, we express the left side of (1) in a different way as a product of two-square sums. To do this, find an integer which is the sum of two squares and divides $b^2 + 1$. For example, if $b^2 + 1$ is divisible by $13 = 2^2 + 3^2$, write $b = 13k + 5$ and note that

$$\begin{aligned} 2(b^2 + 1) &= 26(13k^2 + 10k + 2) \\ &= (5^2 + 1^2)((2k + 1)^2 + (3k + 1)^2) \\ &= (17k + 6)^2 + (7k + 4)^2. \end{aligned}$$

This gives us the solution $(a, b, c) = (7k + 4, 13k + 5, 17k + 6)$, which, for each k satisfies (3) as well. Equation (2) leads to $d^2 = 409k^2 + 278k + 49$, which can be transformed into a Pell equation.

To put this into a general framework, we present a generalization of Theorem 5.9 of ([4], p. 149).

THEOREM. *Let n be a positive integer exceeding 1, and let t be a positive integer for which $1 \leqslant t \leqslant n$ and $t^2 \equiv -1 \pmod{n}$. Then there exist positive integers x, y, u and a nonnegative integer v such that*

(a) $x^2 + y^2 = n$;
(b) $ty \equiv x \pmod{n}$;
(c) $t^2 + 1 = n(u^2 + v^2)$;
(d) $xu + yv = t$;
(e) $xv - yu = -1$.

https://doi.org/10.4153/CMB-1985-040-9 Published online by Cambridge University Press

PROOF. For the special case $t^2 + 1 = n$, we can take $x = t$, $y = u = 1$, $v = 0$. This covers the case $n = 2$ and we can use induction. Suppose $n \geqslant 3$ and the result holds for all integers up to $n - 1$ and relevant t.

Let $t^2 + 1 = mn$. Since $1 \leqslant t \leqslant n - 1$, $mn \leqslant (n - 1)^2 + 1 = n^2 - 2n + 2 < n^2$. Hence $m < n$. The case $m = 1$ is already covered, so we may suppose $m \geqslant 2$.

Choose h and w so that $t = mh + w$ and $1 \leqslant w < m$. Then $w^2 \equiv -1 \pmod{m}$, and we can find positive integers u, v, q and a nonnegative integer p with

(i) $u^2 + v^2 = m$;
(ii) $tu \equiv wu \equiv v \pmod{m}$;
(iii) $w^2 + 1 = m(p^2 + q^2)$;
(iv) $pu + qv = w$;
(v) $pv - qu = -1$.

With $x = uh + p$ and $y = vh + q$, it is straightforward to check (a), (d), (e) and $ty - x = vmh^2 + (2v(vq + pu) + u(qu - pv - 1))h + p(qu - pv - 1) + v(p^2 + q^2) = vn \equiv 0 \pmod{n}$. From (b) and (e), neither x nor y can vanish, so x, y and u are positive, as required. Also, v can vanish only if $y = u = 1$, whereupon $x = t$ and $n = t^2 + 1$. □

To apply this result to the equation $2(b^2 + 1) = a^2 + c^2$, let n and t satisfy the conditions of the theorem and choose x, y, u, v accordingly. Let $b = nk + t$. Then

$$2(b^2 + 1) = 2n((xk + u)^2 + (yk + v)^2).$$

If $2n = i^2 + j^2$, then (1) is satisfied with

$$a = i(yk + v) - j(xk + u) = (iy - jx)k + (iv - ju)$$
$$b = nk + t$$
$$c = i(xk + u) + j(yk + v) = (ix + jy)k + (iu + jv).$$

For each n and t, there are at least four possibilities for (i, j), namely $(x + y, y - x)$, $(x - y, x + y)$, $(y - x, x + y)$, $(x + y, x - y)$. The first leads to consecutive a, b, c, and the second to essentially the same solution. The third yields $a = (y^2 - x^2 - 2xy)k + (y - x)v - (x + y)u$ and $c = (y^2 - x^2 + 2xy)k + (y - x)u + (x + y)v$. The fourth essentially gives this solution with a and c interchanged and one change of sign.

Having found a family of solutions for (1), it remains to choose k to secure (2) and (3). For (3), we see that $b^2 - 2(a^2 + 1)$ is a quadratic in k whose leading coefficient is $n^2 - 2(iy - jx)^2 = \frac{1}{2}((ix + jy)^2 - 3(iy - jx)^2)$. If this can be made positive, then a sufficiently high value of the parameter k will ensure (3). Turn now to (2). We need

$$d^2 = 2(c^2 + 1) - b^2 = Ak^2 + 2Bk + C$$

where $A = 2(ix + jy)^2 - n^2$, $B = 2(ix + jy)(iu + jv) - nt$ and $C = 2(iu + jv)^2 + 2 - t^2$. This leads to the problem of solving the Diophantine equation

$$D = w^2 - Ad^2 \tag{5}$$

https://doi.org/10.4153/CMB-1985-040-9 Published online by Cambridge University Press

for (w, d) where $w = Ak + B$ and $D = B^2 - AC = 2((t(ix + jy) - n(iu + jv))^2 + (n^2 - 2(ix + jy)^2)) = 2((jx - iy)^2 - A)$. If, as is possible, C turns out to be a perfect square, then there is an obvious solution $w = B$ and $d^2 = C$. However, w must also be such as to make k itself an integer. Let us look at some examples.

EXAMPLE 1. *Let t be arbitrary and $n = t^2 + 1$. Then the theorem is satisfied with $x = t$, $y = 1$, $u = 1$ and $v = 0$. We can take $i = t + 1$ and $j = t - 1$ from which*

$$a = (1 + 2t - t^2)k + (1 - t)$$
$$b = (t^2 + 1)k + t$$
$$c = (t^2 + 2t - 1)k + (t + 1)$$
$$A = t^4 + 8t^3 + 2t^2 - 8t + 1$$
$$B = t^3 + 6t^2 + t - 2$$
$$C = (t + 2)^2$$
$$D = -24(t - 1)t(t + 1) \text{ (a multiple of 144).}$$

The equation $D = w^2 - Ad^2$ has the obvious solution $(w, d) = (t^3 + 6t^2 + t - 2, t + 2)$. This leads to $k = 0$ and $(a, b, c, d) = (1 - t, t, t + 1, t + 2)$, an essentially consecutive quartuple. However, if A happens to be square free, then we can generate an infinite family of solutions to (5) from the solutions of $1 = w^2 - Ad^2$ and the particular solution of (5).

Condition (3) imposes another restriction on the possible values of t. Since $b^2 - 2(a^2 + 1) = (-t^4 + 8t^3 - 2t^2 - 8t - 1)k^2 + (-2t^3 + 12t^2 - 2t - 4)k + 4(t - 1)$, we must have $1 \leqslant t \leqslant 7$. Let us examine these cases in turn. $t = 1$ makes a, b, c consecutive, so we reject this. $t = 2$ leads to $A = 73$, a prime; the equation $1 = w^2 - 73d^2$ has infinitely many solutions (w'_r, d'_r) given by

$$w'_r + d'_r\sqrt{73} = (2\,281\,249 + 267\,000\,\sqrt{73})^r.$$

The values of B and D are 32 and -144 respectively, and the solutions of $-144 = w^2 - 73d^2$ derived from the obvious solution are $(w, d) = (32w'_r + 292d'_r, 4w'_r + 32d'_r)$ $(r = 0, 1, 2, \ldots)$. Not all these solutions are suitable, since $w = 73k + 32$ and k must be an integer. Thus, we should have $w \equiv 32 \pmod{73}$, which can be arranged by $w'_r \equiv 1 \pmod{73}$. Since $2\,281\,249 \equiv -1$, it is straightforward to show that any even r will do. (As it happens, $-144 = w^2 - 73d^2$ is also satisfied by $(w, d) = (-41, 5)$ which yields another set of solutions to the system.) Thus, (1), (2), (3) has infinitely many solutions.

$t = 3$ leads to $A = 292 = 4 \cdot 73$, $B = 82$ and $D = -576$. The equation $-576 = w^2 - 292d^2$ is satisfied by $(w, d) = (82w'_r + 730d'_r, 5w'_r + 41d'_r)$ with w'_r, d'_r as above. If r is even, the k determined by $w = 292k + 82$ is an integer.

$t = 4$ and $t = 6$ lead to $A = 769$ and $A = 3049$, respectively, both of which are primes, and we can solve (1), (2), (3) as in the earlier cases. $t = 5$ and $t = 7$ lead to $A = 1636 = 4 \cdot 409$ and $A = 5188 = 4 \cdot 1297$, respectively, and we can proceed as in the case $t = 3$.

EXAMPLE 2. *Let* $n = 13$. *One choice of* t *is* 8. *With* $x = 3$, $y = 2$, $u = 2$, $v = 1$, $i = 5$, $j = 1$, *we have* $(a, b, c) = (7k + 3, 13k + 8, 17k + 11)$, $A = 409$, $B = 270$, $C = 180$ *and* $D = -720$. *We have to solve* $-720 = w^2 - 409d^2$ *in a way that makes* k *an integer for which* $w = 409k + 270$. *The Pell equation* $1 = w^2 - 409d^2$ *can certainly be solved with* $w \equiv 1 \pmod{409}$, *but, with* C *not a perfect square, it is not easy to see what a solution of* $-720 = w^2 - 409d^2$ *might be.*

However, we can shed light on this by looking at a related situation. With $n = 13$, let $t = 5$, $x = 2$, $y = 3$, $u = 1$, $v = 1$, $i = 1$, $j = 5$ to make $(a, b, c) = (-7k - 4, 13k + 5, 17k + 6)$, $A = 409$, $B = 139$, $C = 49$ and $D = -720$. This time we have to solve $-720 = w^2 - 409d^2$ with $w = 409k + 139$. But now we can start with the solution (139, 7) for (w, d) and obtain an infinite family. As a bonus, we can handle the $t = 8$ case by starting with $(w, d) = (-139, 7)$, since $-139 \equiv 270 \pmod{409}$.

To generalize, let $(n, t, x, y, u, v, i, j, A, B, C, D)$ be a system which satisfies the theorem. Then we can form another system $(n, t', x', y', u', v', i', j', A', B', C', D')$ with $t' = n - t$, $x' = y$, $y' = x$, $i' = j$, $j' = i$, $u' = y - v$, $v' = x - u$, which also satisfies the theorem. It is straightforward to check that $A' = A$, $B' = A - B$, $C' = A + C - 2B$ and $D' = D$. It might be hoped that either C or C' is a perfect square, as in the $n = 13$ case, since both systems lead to the same equation $-D = w^2 - Ad^2$, but this is not true in general.

EXAMPLE 3. *Other individual solutions are not hard to find. When* $n = 5$, $t = 2$, *the system* (a, b, c) *is equal to* $(k - 1, 5k + 2, 7k + 3)$, *so that* $d^2 = 73k^2 + 64k + 16 = (3k)^2 + (4(2k + 1))^2$. *The right side is square for* $k = 17$ *and* 1767, *yielding the respective solutions* $(a, b, c, d) = (16, 87, 122, 149)$ *and* $(1766, 8837, 12372, 15101)$ *to* (1), (2), (3). *When* $n = 5$, $t = 3$, *the system* $(a, b, c) = (k + 2, 5k + 3, 7k + 4)$ *leads to* $d^2 = 73k^2 + 82k + 25$, *a square for* $k = 4$, 175 *and* 6754. *This yields* $(a, b, c, d) = (6, 23, 32, 39)$, $(177, 878, 1229, 1500)$ *and* $(6756, 33773, 47282, 57711)$.

3. **Conclusion**. It is clear from the last section that the system (1), (2), (3) is amply supplied with solutions. But are there any for which the number N is less by only 1 than a perfect square? In this case, we ask that $a = 1$ and, since b must be even, $b = 2k$. Then $c^2 = 8k^2 + 1$ and $d^2 = 12k^2 + 4 = 4(3k^2 + 1)$. (At this point, we oberve that trivially, a nonzero N less by 1 than a perfect square cannot differ from the next *five* perfect squares by a perfect square, since the fifth difference would be $16k^2 + 9$, which is square only when $k = 0$ or $k = 1$.) Thus, it must be investigated when $8k^2 + 1$ and $3k^2 + 1$ can be made squares simultaneously. There is a variety of ways of showing that there are at most finitely many k making both expressions square, all of which use deep results on diophantine approximation. For example, $8k^2 + 1$ is a perfect square only when k is a member of the recursion sequence $\{u_n\}$ where $u_0 = 0$, $u_1 = 1$, $u_n = 6u_{n-1} - u_{n-2}$; $3k^2 + 1$ is square only when k is a member of the recursion sequence $\{v_n\}$ where $v_0 = 0$, $v_1 = 1$, $v_n = 4v_{n-1} - v_{n-2}$. M. Mignotte [2], using a result of Baker, showed that the two recurrences have at most finitely many numbers in common. Another approach begins with the factorizations $8k^2 = (c - 1)(c + 1)$ and $3k^2 = (e - 1)(e + 1)$, where $d = 2e$, uses the fact that the two factors on the right have

greatest common divisor 1 or 2, and ultimately reduces the problem to solving the diophantine equation $3y^4 - 2z^4 = s$, where s is either -2 or 1. A theorem of Ljunggren ([3], p. 274) can be applied to establish that there are at most finitely many possibilities. However, remarkably, the problem is essentially solved for us in a paper of A. Baker and H. Davenport in 1969 [1]. They were seeking values of k for which $3k^2 - 2$ and $8k^2 - 7$ are simultaneously square. In both our and their situations, for some integers m and n, k must have the form

$$c_1(2 + \sqrt{3})^m + c_2(2 - \sqrt{3})^m = c_3(3 + \sqrt{8})^n + c_4(3 - \sqrt{8})^r$$

for suitable nonrational constants c_i. With a few modifications, their analysis can be carried over to show that $3k^2 + 1$ and $8k^2 + 1$ are square only for $k = 0$ and $k = 1$. It would be nice to have a more elementary proof of this fact.

It is natural to ask whether there are numbers which differ from the next five greater squares by a square. In the notation of the introduction, we ask for numbers N, z, a, b, c, d, h which satisfy all the relations there along with $N = (z + 4)^2 - h^2$, so that $2(d^2 + 1) = c^2 + h^2$. So far, no such N has been found, and attempts to build on solutions already found for (1), (2), (3) have all failed. For example, if $(a, b, c) = (k - 1, 5k + 2, 7k + 3)$, then d and h must satisfy

$$d^2 = 73k^2 + 64k + 16 = (3k)^2 + (4(2k + 1))^2$$

$$h^2 = 97k^2 + 86k + 25 = (3(3k + 1))^2 + (4(k + 1))^2.$$

Since $(3k, 4(2k + 1), d)$ and $(3(3k + 1), 4(k + 1), h)$ are pythagorean triples, there are integers p, q, r, s for which

$$2(2k + 1) = pq \qquad 3k = p^2 - q^2 \tag{6}$$

$$2(k + 1) = rs \qquad 3(3k + 1) = r^2 - s^2, \text{ whence} \tag{7}$$

$$3(p^2 - q^2 + 1) = r^2 - s^2. \tag{8}$$

By (6), p and q have opposite parity. Since $r^2 - s^2$ is never congruent to 2 modulo 4, p must be even and q odd, from (8). Also from (8), r and s have the same parity, and so, by (7), are both even. From $k \equiv 1 \pmod 4$ follows $rs \equiv 4 \pmod 8$, and so $r \equiv s \equiv 2 \pmod 4$. By (6), $p \equiv 2 \pmod 4$, so the left side of (8) is congruent to 4 modulo 8 while the right side is congruent to 0. This contradiction demonstrates that the required d and h cannot be found.

References

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

2. M. Mignotte, *Intersection des images de certaines suites récurrentes linéaires*, Theor. Comp. Sci. **7** (1978), pp. 117–122.

3. L. J. Mordell, *Diophantine Equations*, (Academic, 1969).

4. I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, (4th ed.) Wiley, 1960, 1966, 1972, 1980.

University of Toronto, Toronto, M5S 1A1