Oblong Numbers Representable as Sums of Two Squares and the Primality of $4u^2+1$

KENT SLINKER

Introduction. In this note we will connect three topics commonly encountered in elementary number theory; polygonal numbers (although rarely oblong numbers), numbers representable as sums of two squares, and the primality of $4u^2+1$. In particular we will show that if $4u^2+1$ is composite, then there exist a t and n, below a bound set by the value of u, such that $u^2+t^2=n(n+1)$. In what follows, all variables belong to $\mathbb{N}$.

Primes of the form $4k+1$ make up one of two classes of all primes other than 2, (the other class being those of the form $4k+3$). The fascination associated with the distribution of primes extends naturally to the distribution of k which make up the set of those $4k+1$ which are prime. The following is the complete set of pairs (k, $4k+1$) where $4k+1$ is prime up to $k=100$:

(**1**,5), (3,13), (**4**,17), (7,29), (**9**,37), (10,41), (13,53), (15,61), (18,73), (22,89), (24,97), (**25**,101), (27,109), (28,113), (34,137), (37,149), (39,157), (43,173), (45,181), (48,193), (**49**,197), (57,229), (58,233), (60,241), (**64**,257), (67,269), (69,277), (70,281), (73,293), (78,313), (79,317), (84,337), (87,349), (88,353), (93,373), (97,389), (99,397),(**100**,401)

In boldface type are those k which are also perfect squares. Whether there are an infinite number of such primes is still an open question, and ranks high on the list in Richard Guy's popular *Solved and Unsolved Problems in Number Theory* . Letting $k=u^2$ gives $4u^2+1$ which is the form we will examine.

Polygonal numbers are numbers which can be made to represent a familiar geometric pattern, like the triangular numbers shown in Figure 1.

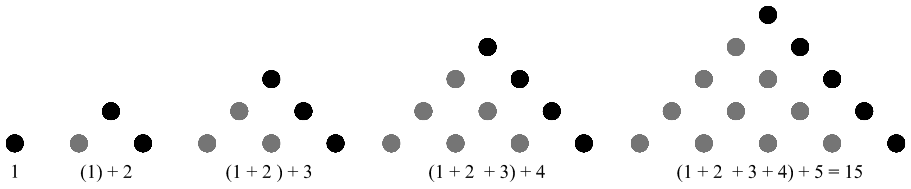

FIGURE 1. Triangular Numbers

Triangular numbers are numbers of the form $1+2+\ldots+n=\frac{n(n+1)}{2}$. The half sisters to triangular numbers are sums of the first n even numbers, $2+4+\ldots+2n=2(1+2+\ldots+n)=n(n+1)$, whose geometric pattern is illustrated in Figure 2.

Numbers of this type are called *oblong* (or sometimes *pronic*) numbers.

Whole numbers which are the sum of two squares have fascinated mathematicians since ancient times, the most familiar being the Pythagorean triples (a,b,c) which satisfy the equation $a^2+b^2=c^2$.

Main Theorem and Examples. We now turn to our main theorem which connects oblong numbers which are sums of two squares to the primality of $4u^2+1$.

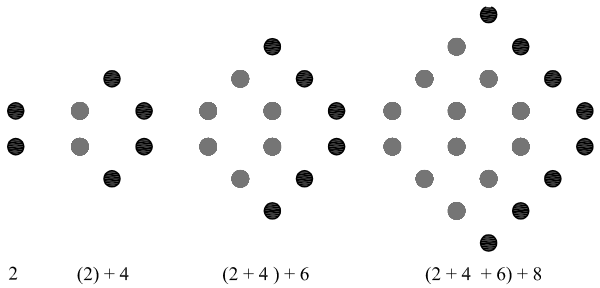

FIGURE 2. Oblong Numbers

Theorem 1. *If $4u^2 + 1$ is composite then there exists natural numbers t and n, such that $t \leq \frac{u^2-6}{5}$ and $u^2 + t^2 = n(n + 1)$.*

To facilitate our proof, let S be the set of u which satisfy this condition:

$$S = \left\{ u \mid u^2 + t^2 = n(n+1), t \leq \frac{u^2 - 6}{5} \right\}$$

Hence if $u \in S$, then $4u^2 + 1$ is composite.

Before we prove our main theorem, let us consider some examples.

Example 1: Consider $11^2 + 23^2 = 25(26)$, since u is an element of S provided that $t \leq \frac{u^2-6}{5}$, and $23 \leq \frac{11^2-6}{5} = 23$, then 11 is an element of S.

Example 2: Since addition is commutative, we also have $23^2 + 11^2 = 25(26)$, so the first condition for membership in S is satisfied, but the second condition requires that $t = 11$ must be lower than the upper bound set by $u = 23$, and indeed $11 \leq \frac{23^2-6}{5}$, so $23 \in S$.

Example 3: Now consider $6^2 + 36^2 = 36(37)$. In this case $36 \nleq \frac{6^2-6}{5} = 6$, so this choice of t does not satisfy the second condition for S. However another choice of t could, and in fact we have $6^2 + 6^2 = 8(9)$ and $6 \leq \frac{6^2-6}{5} = 6$ so $6 \in S$.

From the above three examples we can conclude by our main theorem that $4\,(11)^2 + 1$, $4\,(23)^2 + 1$, and $4\,(6)^2 + 1$ are all composite. Indeed, $4\,(11)^2 + 1 = (5)(97)$, $4\,(23)^2 + 1 = (29)(73)$, and $4\,(6)^2 + 1 = (5)(29)$.

Now let us provide an example of a number which is not in S. First we will note that since $n(n+1)$ is always even, u and t must have the same parity.

Example 4 : Consider $u = 10$. If u is a member of S, then there must be an even number $t \leq \frac{10^2-6}{5} = 18.8$ such that $10^2 + t^2 = n(n + 1)$ for some number n. By checking $t \in \{2, 4, 6, 8, 10, 12, 14, 16, 18\}$, we find no element meets the requirements for membership in S, hence $4(10)^2 + 1$ is prime. (see referee appendix)

We now prove our main theorem by assuming $4u^2 + 1$ is composite and proving the individual requirements for membership in S.

Proof. Suppose that $4u^2+1$ is composite, without loss of generality we can assume $4u^2+1$ is the product of 2 factors, either $4u^2+1=(4m+1)(4k+1)$ or $4u^2+1=(4m+3)(4k+3)$ for some m and k. Before considering each case, we note that $m \neq k$, since if they were equal we would have a perfect square, which is impossible as $4u^2+1$ is one greater than a perfect square. Since $m \neq k$, one must be greater than the other, so we will stipulate that $m<k$ and designate their difference as t which gives $k=t+m$.

Case 1: Substitute $k=t+m$ into $4u^2+1=(4m+1)(4k+1)$ and solve for m using the quadratic formula and taking the positive root to obtain:

$$m=\frac{1}{4}\left(\sqrt{1+4(u^2+t^2)}-(2t+1)\right)$$

Since m is a whole number, and $2t+1$ is odd, then $\sqrt{1+4(u^2+t^2)}$ must necessarily be odd. Let $2n+1=\sqrt{1+4(u^2+t^2)}$. Squaring both sides gives $4n^2+4n+1=1+4(u^2+t^2)$ which simplifies to:

$$u^2+t^2=n(n+1) \tag{0.1}$$

Case 2: Similarly suppose $4u^2+1=(4m+3)(4k+3)$, following the same steps as above we obtain:

$$m=\frac{1}{4}\left(\sqrt{1+4(u^2+t^2)}-(2t+3)\right)$$

By also noting that $2t+3$ is odd we again let $2n+1=\sqrt{1+4(u^2+t^2)}$, squaring and simplifying we obtain once more equation (0.1).

Readers familiar with the law of quadratic reciprocity, which implies $x^2 \equiv -1 \pmod{p}$, p a prime, has a solution only if $p \equiv 1 \pmod 4$, might realize that case 2 is unnecessary, as any prime which divides $4u^2+1$ must be congruent to 1 (mod 4). With a bit more effort, which requires establishing the possible values of n (mod 4) depending on the parity of u and t in equation (0.1), and noting the difference between $2n+1$ and $2t+3$ must be congruent to 0 (mod 4), the same result can be obtained without recourse to quadratic reciprocity (see referee appendix). However, all that is needed to establish the first condition for membership in S is the necessity that $\sqrt{1+4(u^2+t^2)}$ be odd. By focusing on even and odd requirements, which are really just mod (2) requirements, we obtain the simpler result that $u^2+t^2=n(n+1)$, which allows us to connect the primality of $4u^2+1$ to sums of two squares.

We now prove the upper limit for given in the definition of S. Recall by assumption $4u^2+1=(4m+1)(4k+1)$. Without loss of generality, we will assume that the factor $4k+1$ is the greatest possible of the two factors. Since 5 is the first prime congruent to 1 (mod 4), the smallest possible value for m is 1, setting $m=1$ and recalling $k=t+m$, gives $4u^2+1=(4(1)+1)(4(t+1)+1)$. Solving for t in terms of u gives the maximum value for t

as $\frac{u^2-6}{5}$.
This establishes the upper limit for t as given in S and completes our proof of Theorem 1. □

Example 1 illustrates that the upper bound can not be lowered, for it it were, 11 would not be in S. Other examples of this kind can be found by consulting Table 1 below.

Corollaries and a Curiosity. We now establish some easy corollaries, provide some data and discover an interesting curiosity.

Corollary 2. *If $u^2 = \frac{n(n+1)}{2}$ and $u \geqslant 6$, then $4u^2 + 1$ is composite.*

Proof. Suppose $u^2 = \frac{n(n+1)}{2}$, then $2u^2 = u^2 + u^2 = n(n+1)$, so the first condition for membership in S is satisfied. To satisfy the second, we need $u \leq \frac{u^2-6}{5}$, which happens precisely when $u \geqslant 6$. Corollary 2 connects composites of the form $4u^2 + 1$ to triangular numbers which are sums of two squares. □

The following Corollary shows this can be done in general:

Corollary 3. *If $u^2 + t^2 = n(n+1)$, then there exists integers a, b such that $a^2 + b^2 = \frac{n(n+1)}{2}$.*

Proof. Set $a = \left(\frac{t-u}{2}\right)$, and $b = \left(\frac{t+u}{2}\right)$, since t and u have the same parity, both a and b are integers, and $a^2 + b^2 = \left(\frac{t-u}{2}\right)^2 + \left(\frac{t+u}{2}\right)^2 = \frac{(t^2+u^2)}{2} = \frac{n(n+1)}{2}$. □

Fermat numbers are numbers of the form $F_k = 2^{2^k} + 1$ for $k \in \{0, 1, 2, 3 \ldots\}$. Fermat conjectured all were prime, Euler proved him wrong several years later by factoring F_5. Fermat numbers are prime for $k \in \{0, 1, 2, 3, 4\}$, but not for any other known values. It is an open question whether there are an infinite number of such primes. This leads to our next corollary.

Corollary 4. *If $2^{\frac{2^k-2}{2}} \in S$, then F_k is composite.*

Proof. Let $2^{2^k}+1 = 4u^2+1$, solving for u gives $u = 2^{\frac{2^k-2}{2}}$. The remainder of the proof follows immediately from Theorem 1. Indeed, for $k = 5$, we have $u = 2^{\frac{2^5-2}{2}} = 32768$, and $32768^2 + 1674944^2 = 1675264(1675265)$. □

Corollary 5. *If $u = a^2$, and $u \geq 2$ then $u \in S$.*

Proof. Let $t = a$, and $n = a^2$, then $u^2 + t^2 = a^4 + a^2 = a^2(a^2 + 1) = n(n+1)$. We need only check that $t = a \leq \frac{a^4-6}{5} = \frac{u^2-6}{5}$. Observe that $\frac{a^4-6}{4}$ is strictly increasing and for $a = 2$ we have $2 \leq \frac{2^4-6}{5} = 2$. □

Table 1 below gives the ordered pairs (u, t, n) that satisfy requirements for membership in S for $1 \leq u \leq 100$:

$(4,2,4)$	$(34,22,40)$	$(52,86,100)$	$(69,363,369)$	$(86,1478,1480)$	$(6,6,8)$
$(34,40,52)$	$(53,161,169)$	$(69,951,953)$	$(87,21,89)$	$(9,3,9)$	$(34,230,232)$
$(54,582,584)$	$(70,284,292)$	$(87,441,449)$	$(9,15,17)$	$(35,35,49)$	
$(56,32,64)$	$(71,19,73)$	$(87,579,585)$	$(11,23,25)$	$(35,91,97)$	$(56,238,244)$
$(71,127,145)$	$(89,1583,1585)$	$(14,38,40)$	$(36,6,36)$	$(56,626,628)$	$(71,1007,1009)$
$(91,35,97)$	$(15,9,17)$	$(36,72,80)$	$(57,69,89)$	$(72,36,80)$	$(91,143,169)$
$(16,4,16)$	$(36,258,260)$	$(59,133,145)$	$(74,68,100)$	$(91,325,337)$	$(16,50,52)$
$(38,14,40)$	$(59,695,697)$	$(74,418,424)$	$(91,1655,1657)$	$(17,19,25)$	
$(39,303,305)$	$(61,41,73)$	$(74,1094,1096)$	$(93,291,305)$	$(19,17,25)$	$(40,34,52)$
$(61,283,289)$	$(76,1154,1156)$	$(94,1766,1768)$	$(19,71,73)$	$(41,61,73)$	
$(61,743,745)$	$(77,151,169)$	$(95,691,697)$	$(21,87,89)$	$(41,335,337)$	$(64,8,64)$
$(79,1247,1249)$	$(96,66,116)$	$(22,34,40)$	$(43,139,145)$	$(64,134,148)$	$(81,9,81)$
$(96,108,144)$	$(23,11,25)$	$(44,386,388)$	$(64,818,820)$	$(81,219,233)$	$(96,1842,1844)$
$(24,114,116)$	$(46,422,424)$	$(66,30,72)$	$(81,1311,1313)$	$(97,139,169)$	$(25,5,25)$
$(48,174,180)$	$(66,96,116)$	$(82,514,520)$	$(98,224,244)$	$(26,134,136)$	$(49,7,49)$
$(66,168,180)$	$(83,401,409)$	$(99,1959,1961)$	$(29,167,169)$	$(49,137,145)$	$(66,252,260)$
$(84,276,288)$	$(100,10,100)$	$(30,66,72)$	$(49,479,481)$	$(66,870,872)$	
$(84,1410,1412)$	$(100,584,592)$	$(31,191,193)$	$(50,16,52)$	$(68,74,100)$	
$(86,52,100)$	$(100,766,772)$	$(32,56,64)$	$(51,519,521)$	$(69,57,89)$	$(86,106,136)$

By Theorem 1, any $1 \leq u \leq 100$ not in the above table gives a prime value for $4u^2+1$, in other words, if

$$u \in \{1,2,3,5,7,8,10,12,13,18,20,27,28,33,37,42,45,47,$$
$$55,58,60,62,63,65,67,73,75,78,80,85,88,90,92\}$$

then $4u^2+1$ is prime. There are thirty three u in the interval $1 \leq u \leq 100$ which give a prime value for $4u^2+1$. As is to be expected, this large percentage is not typical. Let $p(n)$ be the number of $u \leq n$ such that $4u^2+1$ is prime. Table 2 below shows how $\frac{p(n)}{n}$ decreases as n increases.

n	$p(n)$	$\frac{p(n)}{n}$
100	33	.33
1,000	208	.208
10,000	1558	.1558
100,000	12390	.1239
1,000,000	102204	.102204
10,000,000	872120	.087212

A curiosity arises when we carefully examine Table 1, paying attention to those u which are prime. As it turns out, the corresponding t many times is also prime. In fact, the corresponding t for

$$u \in \{11,17,19,23,29,31,43,61,71,83,89,97\}$$

are all prime, even when u has more than one entry in Table 1. With computational help, the author has verified that the ratio of primes paired with primes in the interval $1 \leq u \leq 1000$ is almost $\frac{1}{2}$. In that interval there are 300 $u \in S$ which are prime, 151 are paired with composite t, 149 are paired with prime t.

Conclusion. Our connection to sums of squares, oblong numbers and composites of the form $4u^2+1$ provides another approach to examining the question concerning the infinitude of primes of the form $4u^2+1$. Corollary 5 establishes the infinitude of primes of the from $4u^2+1$ requires a negative answer to the question, Is there a u_0 such that for all $u > u_0$, $u \in S$? The upper bound on t increases very rapidly as u increases, allowing each u to "look among" an ever increasing number of t in order to gain membership in S. This fact alone seems sufficient to explain the decrease in $\dfrac{p(n)}{n}$ as seen in Table 2. But, by analogy, so too do the number of primes less than n decrease as a ratio of n, but there are still an infinite number of them. A Mathematica notebook for generating elements of S along with other material is available on the author's website at http://kslinker.com/bsquared+1.html

Kent Slinker
San Antonio College
kslinker@alamo.edu

References

1. Albert Beiler, *Recreations in the Theory of Numbers*, Dover, New York, 1964.
2. Underwood Dudley, *Elementary Number Theory*, Dover, New York, 1978.
3. Richard Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1994.
4. G.H. Hardy and E.M. Wright, *Introduction to the Theory of Numbers*, Oxford-Clarendon, Oxford, 1954.
5. M. Křek, F. Luca, and L. Somer, *17 Lectures on Fermat Numbers: From Number Theory to Geometry*, Springer-Verlag, New York, 2001.
6. Stanley Ogilvy and John Anderson, *Excursions in Number Theory*, Dover, New York, 1966.
7. Frederick Stevenson, *Exploring the Real Numbers*, Prentice Hall. New Jersey, 2000.
8. Jeffrey Stopple, *A Primer of Analytic Number Theory*, Cambridge University Press, New York, 2003.