VERSITA

Mathematica Slovaca

DOI: 10.2478/s12175-008-0082-3
Math. Slovaca **58** (2008), No. 3, 387–391

PRIMES OF THE FORM $x^2 + (x + 1)^2$. PROPER DIVISORS OF COMPOSITES OF THE SAME FORM

Andreas Zachariou† — Panayiotis G. Tsangaris

(*Communicated by Stanislav Jakubec*)

ABSTRACT. The aim of the present paper is to characterize prime numbers of the form $n = x^2 + (x + 1)^2$ and to obtain certain proper divisors of composite numbers of the same form, i.e. divisors d of n such that $1 < d < n$.

1. Introduction

The aim of the present paper is to characterize prime numbers of the form $n = x^2 + (x+1)^2$ and to obtain certain proper divisors of composite numbers of the same form, i.e. divisors d of n such that $1 < d < n$. All composite numbers of this form are obtained recursively as in [2]. The paper ends with a table of composite numbers n of the above form together with several of their proper divisors of type d_1 and d_2 as defined in our Theorem 6.

Lemma 1. *Let $n \mid n_1 n_2$, $n \nmid n_1$ and $n \nmid n_2$, where n, n_1 and n_2 are natural numbers. Then the numbers (n, n_1) and (n, n_2) are proper divisors of n.*

Proof. Evidently $(n, n_i) \mid n$ for $i = 1, 2$. Let $(n, n_1) = 1$. Since $n \mid n_1 n_2$ it follows that $n \mid n_2$, which contradicts the assumption $n \nmid n_2$. Let $(n, n_1) = n$. Hence $n \mid n_1$, which contradicts the assumption $n \nmid n_1$. Hence $1 < (n, n_1) < n$. Similarly, it is proved that $1 < (n, n_2) < n$. □

Remark. Lemma 1 simplifies an analogous result of W. Sierpinski. (See [1, p. 16, Exercise 2].)

2000 Mathematics Subject Classification: Primary 11D09, 11A51.
Keywords: prime number, composite number, proper divisor, Diophantine equation.

†Deceased.

Lemma 2. *Let $n = a^2 + b^2 = c^2 + d^2$, where a, b, c, d are non-negative integers such that $a > b$, $c > d$ and $a > c$. Then $n \mid (ac+bd)(ad+bc)$, while $n \nmid (ac+bd)$ and $n \nmid (ad + bc)$. Consequently, the numbers $(n, ac + bd)$ and $(n, ad + bc)$ are proper divisors of n.*

Proof. It is easily seen that $(ac + bd)(ad + bc) = n(ab + cd)$. Thus

$$n \mid (ac + bd)(ad + bc).$$

Also the following hold true:

$$\begin{aligned} n^2 &= (ac - bd)^2 + (ad + bc)^2 &\quad (1)\\ &= (ac + bd)^2 + (ad - bc)^2 &\quad (2) \end{aligned}$$

$$a > c > d > b. \tag{3}$$

From (1) and (3) we obtain: $n > ad + bc$ because $ac - bd > 0$. Hence

$$n \nmid (ad + bc).$$

From (2) and (3) we obtain: $n > ac + bd$ because $ad - bc > 0$. Hence

$$n \nmid (ac + bd).$$

The proof ends by using Lemma 1. □

Remark. Lemma 2 simplifies an analogous result of W. Sierpinski. (See [1, p. 210, Exercise 2].)

Theorem 3. *Consider the Diophantine equation*

$$X^2 - 2Y^2 = 2k^2 - 1, \qquad \textit{where} \quad k = 0, 1, \dots . \tag{F$_k$}$$

Let $X + Y\sqrt{2}$ be a non-negative integral solution of (F_k). Let $x \equiv (X - 1)/2$ and $N(x) \equiv x^2 + (x + 1)^2$. Then $N(x) = Y^2 + k^2$. Moreover, the following are equivalent:

i) *$N(x)$ is composite.*

ii) *$Y > k + 1$.*

Proof. See [2, Theorem 4.9]. □

Theorem 4. *Let x be a natural number. Let $n = x^2 + (x + 1)^2$. Then the following are equivalent:*

i) *n is composite.*

ii) *There exists an integer k with $0 \le k \le x - 1$, such that $n - k^2$ is a square number.*

Proof.

i) $\implies$ ii): Assume that n is composite. Then by Theorem 3 there exist non-negative integers Y, k with $Y > k+1$, such that $n = Y^2 + k^2$. Moreover, we have $k < x$ because:

If $x = k$, then $Y = \pm(k+1)$, which contradicts the inequality $Y > k+1$.

If $x < k$, then $n = x^2 + (x+1)^2 < k^2 + (k+1)^2 < Y^2 + k^2$, which contradicts the fact that $n = Y^2 + k^2$. Thus, there exists an integer k with $0 \le k \le x-1$, such that $n - k^2 = Y^2$, that is $n - k^2$ is a square number.

ii) $\implies$ i): Let $n - k^2 = Y^2$ for some non-negative integers k, Y with $0 \le k \le x-1$. Since $n = x^2 + (x+1)^2$ it follows that

$$Y^2 > (x+1)^2 > (k+1)^2$$

and so $Y > k+1$. Thus, according to Theorem 3, the number n is composite. $\square$

Remark. It can be shown that Theorem 4 is equivalent to an analogous result of A. M. Vaidya. (See [3, p. 105, Lemma].)

Theorem 5. *Let x be a natural number. Let $n = x^2 + (x+1)^2$. Then, the following are equivalent:*

i) *n is prime.*

ii) *$n - k^2$ is not a square-number for every $k = 0, 1, \dots, x-1$.*

Proof. Immediate by Theorem 4. $\square$

Theorem 6. *Let $n = x^2 + (x+1)^2$ be composite. Then there exist non-negative integers Y and k with $0 \le k \le x-1$, such that $n = Y^2 + k^2$. Moreover, the numbers*

$$d_1 = (n, Y(x+1) + kx) \qquad \textit{and} \qquad d_2 = (n, Yx + k(x+1))$$

are proper divisors of n.

Proof. By using Theorem 4 and Lemma 2, where $a = Y$, $b = k$, $c = x+1$ and $d = x$. $\square$

Example. Let $x = T(m) = \frac{m(m+1)}{2}$ = the mth triangular number, where $m > 1$. Let $n = x^2 + (x+1)^2$. Then n is composite. In fact;

$$n = \frac{(m^2+1)(m^2+2m+2)}{2}.$$

For $k = T(m) - (m+1)$ and $Y = T(m) + m$ we have $0 \le k \le x-1$ and $n = Y^2 + k^2$. Let $n_1 = Y(x+1) + kx$ and $n_2 = Yx + k(x+1)$. Then

$$n_1 = \frac{m(m+2)(m^2+1)}{2} \qquad \text{and} \qquad n_2 = \frac{(m^2-1)(m^2+2m+2)}{2}.$$

Let $d_i = (n, n_i)$ for $i = 1, 2$. We distinguish two cases:
Case 1: $m =$ even.
Then

$$d_1 = m^2 + 1 \qquad \text{and} \qquad d_2 = \frac{(m^2 + 2m + 2)}{2}.$$

Case 2: $m =$odd.
Then

$$d_1 = \frac{(m^2 + 1)}{2} \qquad \text{and} \qquad d_2 = m^2 + 2m + 2.$$

Table of composite numbers $n = x^2 + (x+1)^2 = Y^2 + k^2$ together with their proper divisors d_1 and d_2

x	n	k	Y	d_1	d_2	x	n	k	Y	d_1	d_2
3	25	0	5	5	5			31	58	173	25
6	85	2	9	5	17	48	4705	9	68	941	5
8	145	1	12	29	5	49	4901	1	70	169	29
10	221	5	14	17	13			26	65	377	13
11	265	3	16	5	53	51	5305	11	72	5	1061
13	365	2	19	73	5	52	5513	32	67	149	37
15	481	9	20	13	37	53	5725	10	75	1145	5
16	545	4	23	5	109			37	66	25	229
18	685	3	26	137	5	54	5941	30	71	13	457
20	841	0	29	29	29	55	6161	44	65	101	61
21	925	5	30	5	185	56	6385	12	79	5	1277
		14	27	37	25	57	6613	23	78	389	17
23	1105	4	33	221	5	58	6845	11	82	1369	5
		9	32	65	17			37	74	37	185
		12	31	85	13	59	7081	5	84	97	73
26	1405	6	37	5	281	61	7565	13	86	5	1513
27	1513	12	37	17	89			26	83	17	445
28	1625	5	40	325	5			29	82	89	85
		16	37	13	125	62	7813	33	82	601	13
		20	35	25	65	63	8065	12	89	1613	5
31	1985	7	44	5	397	64	8321	20	89	157	53
33	2245	6	47	449	5	66	8845	3	94	29	305
36	2665	8	51	5	533			14	93	5	1769
		19	48	205	13			54	77	61	145
		27	44	65	41	67	9113	37	88	13	701

x	n	k	Y	d_1	d_2	x	n	k	Y	d_1	d_2
37	2813	2	53	29	97	68	9385	13	96	1877	5
38	2965	7	54	593	5	71	10225	15	100	5	2045
40	3281	16	55	193	17			48	89	409	25
41	3445	9	58	5	689	73	10805	14	103	2161	5
		14	57	53	65	74	11101	30	101	653	17
		23	54	13	265	75	11401	40	99	877	13
43	3785	8	61	757	5	76	11705	16	107	5	2341
44	3961	19	60	17	233	77	12013	58	93	293	41
45	4141	35	54	41	101						
46	4325	10	65	5	865						

REFERENCES

[1] SIERPINSKI, W.: *Elementary Theory of Numbers*, P.W.N., Warszawa, 1964.

[2] TSANGARIS, P. G.: *A sieve for all primes of the form* $x^2+(x+1)^2$, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) **25** (1998), 39–53.

[3] VAIDYA, A. M.: *On representing an integer as a sum of two triangular numbers*, Vidya B **15** (1972), 104–105.

Received 19. 7. 2006

Department of Mathematics
University of Athens
Panepistimiopolis
GR–157 84 Athens
GREECE
E-mail: ptsangaris@math.uoa.gr