NNTDM 3 (1997) 4, 185 - 187

A NOTE ON SUMS OF SQUARES OF INTEGERS

J.H. Clarke and A.G. Shannon

University of Technology, Sydney,
NSW 2007, Australia

The purpose of this note is to prove that if an integer can be expressed as the sum of two squares, then any power of that integer can also be expressed as the sum of two squares. This result complements Lagrange's result that the product of two sums of squares is the sum of two squares [3]. More general still is Waring's problem [3].

For integers, n, x and y, if

$$n = x^2 + y^2,$$

then a well-known theorem in number theory states that $n = N^2 m$, where $N \in \mathbb{Z}$ (and may be unity) and m is square-free with no factors of the form $4k + 3$ in which k is a non-negative integer [1]. We aim to prove that for a positive integer r and integers a and b :

$$n^r = a^2 + b^2.$$

Let $$z = x + iy, \quad i^2 = -1.$$

Then $$z^r = (x + iy)^r$$

(1) $$z^r = \sum_{j=0} (-1)^j \binom{r}{2j} x^{r-2j} y^{2j} + i \sum_{j=0} (-1)^j \binom{r}{2j+1} x^{r-2j-1} y^{2j+1}$$

$$= a + ib, \text{ say,}$$

and $$(\overline{z})^r = a - ib$$

Thus $$(z\overline{z})^r = a^2 + b^2;$$

that is, $(x^2 + y^2)^r = a^2 + b^2$, as required.
For example, for $n = 13$ and $r = 5$,

$$13 = N^2 m = 1^2(4.3 + 1)$$

$$= 3^2 + 2^2$$

$$(3^2 + 2^2)^5 = 597^2 + 122^2 \text{ using } x = 3 \text{ and } y = 2 \text{ in (1)}$$

$$= 371293.$$

Sometimes of course n may be expressed as the sum of two squares in more than one way; for example,

$$145 = 1^2(4.36 + 1) = 8^2 + 9^2 = 12^2 + 1^2.$$

This may be avoided by letting $n = (m + 1)^2 + m^2$, where m is an integer ≥ 1. Suitable large values for n (or m) and r give extremely large values for a and b [cf.8]. The method used here can also be utilised to establish more neatly than the usual proof that, more generally, the sums of two squares form a closed set under multiplication [5]:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad - bc)^2.$$

Using the fact that Gaussian integers (complex numbers with integral coefficients) form a Euclidean ring, where the metric of $a + i + b, a, b \in \mathbb{Z}$, is taken to be

$$d(a + ib) = a^2 + b^2,$$

one can further prove that the prime factors of a number which is the sum of two squares are each the sum of two squares [7]. Fermat took this further and showed that an odd prime number is the sum of two primes if, and only if, it is 1 (mod 4) [4]. This means that numbers expressible as the sum of two squares can be characterised as having no prime factors which are 3 (mod 4) [1]. Our expansion of the product of two sums of two squares can be extended to sums of four or eight squares. The four squares case is the Lagrange identity:

$$(a^2+b^2+c^2+d^2)(u^2+v^2+w^2+x^2)$$

$$= (au-bv-cw-dx)^2 + (av+bu+cx-dw)^2$$

$$+ (aw-bx+cu+dv)^2(ax+bw-cv+du)^2$$

This eventually leads to Lagrange's famous theorem by also showing that every prime is the sum of 4 squares [6]. Finally, Ewell [2] has an historical account of the major results on representations of integers by sums of four or fewer squares, and Stewart [9] discusses Minkowski's proof of the two-squares theorem.

References

1. D.M. Burton, Elementary Number Theory, Allyn and Bacon, Boston, 1980.

2. J.A. Ewell, On sums of triangular numbers and sums of squares *American Mathematical Monthly,* 99 (1992): 752-757.

3. H. Griffin, *Elementary Theory of Numbers*, McGraw-Hill, New York, 1954.

4. G.H. Hardy and J E Littlewood, Some problems of partitio numerorum, *Proceedings of the London Mathematical Society* (2), 28 (1928): 518-542.

5. G.H. Hardy and E M Wright, *An Introduction to the Theory of Numbers,* 4th edition, Clarendon Press, Oxford, 1960.

6. K. Ireland and M.I. Rosen, *Elements of Number Theory,* Bogden and Quigley, Tarrytown-on-Hudson, 1972.

7. L.J. Mordell, *Diophantine Equations,* Academic Press, London, 1969.

8. I. Niven and H.S. Zuckerman, *An Introduction to the Theory of Numbers,* John Wiley, New York, 1972.

9. I. Stewart, Fermat's Christmas Theorem is described in one dickens of a tale, *Scientific American,* 263(6) (1990): 94-97.