THE DIOPHANTINE EQUATION $x^2+y^2+z^2=m^2$

ROBERT SPIRA, University of California, Berkeley

The close connection between the equations $x^2+y^2=z^2$ and $x^4+y^4=z^4$ leads one to suspect a close connection between the title equation and the unsolved equation $x^4+y^4+z^4=m^4$. In this paper, it will be shown that these equations are indeed intimately related. The main portion of the paper, however, is concerned with an exposition and survey of what is known to date about the equation $x^2+y^2+z^2=m^2$. Early references may be found in Dickson [1].

1. Solution. We always take x, y, z and $m>0$, and we are concerned only with rational integral solutions where $(x, y, z)=1$, for the imprimitive solutions where $(x, y, z)>1$ can be obtained from the primitive ones by multiplication. By congruences (mod 8), one sees that x and y can be taken even, with z and m odd. The following theorem has long been known.

THEOREM 1. *Given $x^2+y^2+z^2=m^2$ with z odd and $(x, y, z)=1$, one can find integers u, v, w and t such that*

$$\begin{aligned} x &= 2(uw - vt), \\ y &= 2(ut + vw), \\ z &= u^2 + v^2 - w^2 - t^2, \\ m &= u^2 + v^2 + w^2 + t^2. \end{aligned} \tag{1}$$

Carmichael [2], in 1915, attempted a proof which was incomplete. Dickson [3], in 1920, was the first to give a satisfactory proof. Skolem [4], in 1941, gave a proof which was essentially correct. The following proof is a completion of that given by Skolem. It yields an algorithm to find u, v, w and t from x, y, z and m which is much more direct than the algorithm obtained from Dickson's [3] proof.

Proof. Set $x_1=\frac{1}{2}x$ and $y_1=\frac{1}{2}y$. Then

$$x_1^2 + y_1^2 = \left(\frac{m+z}{2}\right)\left(\frac{m-z}{2}\right).$$

Set $f=(x_1, y_1)$, $f_1=(f, \frac{1}{2}(m+z))$ and $f_2=(f, \frac{1}{2}(m-z))$. By an easy argument one sees that $(f_1, f_2)=1$, and $f=f_1\cdot f_2$. Set $x_2=x_1/f$, $y_2=y_1/f$, $z_1=(m+z)/2f_1^2$ and $z_2=(m-z)/2f_2^2$. Then

$$x_2^2 + y_2^2 = z_1\cdot z_2,$$

where $(x_2, y_2)=1$. Note that z_1 and z_2 are not necessarily relatively prime.

Let

$$x_2 + iy_2 = \prod_{j=1}^{n} \pi_j$$

be a factorization into gaussian primes. Note that x_2+iy_2 cannot be divisible by a rational prime p. For if so, then $(x_2+iy_2)/p=a+ib$, $x_2=pa$, $y_2=pb$, a contradiction, as $(x_2, y_2)=1$. Hence, none of the π_j's is a rational prime $\equiv 3 \pmod 4$.

Now

$$x_2 - iy_2 = \prod_{j=1}^{n} \bar{\pi}_j$$

and

$$z_1 \cdot z_2 = \prod_{j=1}^{n} (\pi_j \bar{\pi}_j), \qquad z_1 = \prod_{j=1}^{m} (\pi_j \bar{\pi}_j), \qquad z_2 = \prod_{j=m+1}^{n} (\pi_j \bar{\pi}_j)$$

if we write the π_j's in a suitable order. Set

$$u_1 + iv_1 = \prod_{j=1}^{m} \pi_j, \qquad w_1 + it_1 = \prod_{j=m+1}^{n} \pi_j.$$

Then

$$z_1 = (u_1 + iv_1)(u_1 - iv_1), \qquad z_2 = (w_1 + it_1)(w_1 - it_1),$$
$$(u_1 + iv_1)(w_1 + it_1) = x_2 + iy_2.$$

Since, given any $\bar{\pi}_j$ dividing u_1-iv_1, we cannot have $\bar{\pi}_j(u_1+iv_1) \mid (x_2+iy_2)$, (for then a rational prime would divide $x_2 + iy_2$), we have $u_1 + iv_1 = \text{G.C.D.}(z_1, x_2+iy_2)$. Similarly, $w_1+it_1=\text{G.C.D.}(z_2, x_2+y_2i)$.

Setting $u=f_1u_1$, $v=f_1v_1$, $w=f_2w_1$ and $t=f_2t_1$, we now easily obtain equations (1). An example in which all the letters introduced occur nontrivially is $12^2+84^2+5^2=85^2$. The algorithm for obtaining u, v, w and t from x, y, z and m is simply Euclid's algorithm applied to $\frac{1}{2}(m+z)$ and x_2+y_2i, and also to $\frac{1}{2}(m-z)$ and x_2+y_2i, along with a few other operations obvious from the proof.

Tables of solutions for $m \leqq 100$ are given in Steiger [5]; and for $m \leqq 207$, in Miksa [6].

In addition to the evenness of x and y, one can also show that if $m \equiv 0 \pmod 3$, then none of x, y and z are $\equiv 0 \pmod 3$; and if $m \not\equiv 0 \pmod 3$, then exactly two of x, y and z are $\equiv 0 \pmod 3$.

Rational parametrizations were given in references [7] through [11]. Sierpinski [12] gives another solution. Dickson's [13] solution is equivalent to (1). Skolem [4] showed that primitive solutions occur as orthogonal triples (see Dickson [14], Buquet [11]). These triples can occur with distinct rows and columns, as shown by

17	16	52	2	34	53
32	−47	4	43	38	−26
46	28	−23	46	−37	22

Parity arguments show that such triples cannot be magic. Reitan [15] discussed chains of solutions.

2. Uniqueness. The following theorem was discovered empirically by Steiger [5] in 1956.

THEOREM 2. *If the parameters u, v, w and t of equations* (1) *are subjected to the conditions*

$$\text{(a)}\ uw > vt, \qquad \text{(b)}\ u^2 + v^2 > w^2 + t^2,$$

$$(c_1)\ u \geqq 1,\ v \geqq 0, \qquad (c_2)\ w \geqq 1,\ t \geqq 0, \qquad (c_3)\ t + v \geqq 1,$$

$$\text{(d)}\ u + v + w + t \equiv 1 \pmod 2,$$

$$\text{(e)}\ (u^2 + v^2,\ w^2 + t^2,\ ut + vw) = 1,$$

$$\text{(f)}\ t = 0 \rightarrow u \leqq v, \qquad \text{(g)}\ v = 0 \rightarrow w \leqq t,$$

then each primitive solution of $x^2+y^2+z^2=m^2$ is obtained once and only once.

Proof. First we show that each solution is obtained at least once under conditions (a) through (g). Since x and z are >0, we have: (a) $uw>vt$, and (b) $u^2+v^2>w^2+t^2$. From the proof of Theorem 1, we can take $u+iv$ in the first quadrant excluding the imaginary axis. Hence, (c_1) $u\geqq 1$ and $v\geqq 0$. It may happen that $\arg(x_2+iy_2)<\arg(u_1+iv_1)$. By our proof, note that we obtain v_1+iu_1 from y_2+ix_2. But then $\arg(y_2+ix_2)>\arg(v_1+iu_1)$, so that by possibly interchanging x and y we can assure that $\arg(x_2+iy_2)\geqq\arg(u_1+iv_1)$. Now from $x=2(uw-vt)$, $w+it$ cannot lie in the second quadrant, and from $y=2(ut+vw)$, $w+it$ cannot lie in the third quadrant. Finally, as $\arg(x_2+iy_2)\geqq\arg(u_1+iv_1)$, we must have $\arg(w+it)\geqq 0$, so that $w+it$ lies in the first quadrant, excluding the imaginary axis. Thus, (c_2) $w\geqq 1$, $t\geqq 0$. If v and t were zero simultaneously, then $y=0$. Hence, (c_3) $t+v\geqq 1$. Modulo 2, $u^2\equiv u$, $v^2\equiv v$, $w^2\equiv w$ and $t^2\equiv t$. Hence, (d) $1\equiv m=u^2+v^2+w^2+t^2\equiv u+v+w+t \pmod 2$. If we let $d \mid (u^2+v^2,\ w^2+t^2,\ ut+vw)$, then $d \mid m$, $d \mid z$, $d \mid y$ and hence $d \mid x$, so $d=1$. Thus we have (e) $(u^2+v^2,\ w^2+t^2,\ ut+vw)=1$. Finally, if $t=0$, by interchanging x and y if necessary, we can have $u\leqq v$. Similarly, if $v=0$, we can have $w\leqq t$. These last are conditions (f) and (g). These seven conditions are similar to those stated by Steiger [5], who used these conditions to construct his table of solutions.

The proof below that these conditions insure that each solution is obtained only once is due to W. H. Mills.

We start from the equations

$$(x + iy)/2 = (u + iv)(w + it),$$

$$(z + m)/2 = u^2 + v^2 = (u + iv)(u - iv).$$

Note that $w+it$ and $u-iv$ are relatively prime; for if a gaussian prime divided both, it would divide w^2+t^2 and u^2+v^2, and would also divide $v(w+it)+t(u-iv)=ut+vw$, which is impossible by condition (e). Hence $u+iv$ is the G.C.D. of

$\frac{1}{2}(x+iy)$ and $\frac{1}{2}(z+m)$, a definite complex number determined up to a unit. But as it lies in the first quadrant, it is determined uniquely. A similar proof holds for $w+it$. Now we use conditions (c), (f) and (g), in an obvious manner, to assure us that we obtain only one of the two possible sets of parameters obtained from the above equations by interchanging x and y. The conditions (a) through (g) are not independent, condition (c_3) being a consequence of (c_1), (c_2) and (f).

3. Application. Since one can go from the variables x, y, z and m to the parameters u, v, w and t, it is easy to see that the equation $x^4+y^4+z^4=m^4$ is equivalent to the four simultaneous quadratic equations:

$$\begin{aligned} x^2 &= 2(uw - vt), \\ y^2 &= 2(ut + vw), \\ z^2 &= u^2 + v^2 - w^2 - t^2, \\ m^2 &= u^2 + v^2 + w^2 + t^2. \end{aligned} \tag{2}$$

One can satisfy any three of these equations, giving x, y, z and m in terms of other parameters. This was done by Escott [16] and Fauquembergue [17]. Incidentally, Werebrusow's [18] identity, as corrected by Padhy [19], which reads

$$(3 + 4t^2)^4 = (-1 + 4t^2)^4 + (2 + 4t)^4 + [8(2t - 1)(2t^2 + t + 1)]^2,$$

is a special case of Escott's identity

$$(m^2 + mn + n^2)^4 = (mn)^4 + (mn + n^2)^4 + [m(m + n)(m^2 + mn + 2n^2)]^2,$$

obtained by taking $n=-1-2t$, $m=-1+2t$. Aside from this, no solution is contained in any other. For instance, Escott's [16] formula does not represent $33^4=31^4+4^4+[8\cdot 64]^2$; and Fauquembergue's formulas,

$$\begin{aligned} (a^4 + 2b^4)^4 &= (a^4 - 2b^4)^4 + (2a^3b)^4 + (8a^2b^6)^2 \\ &= (2a^2b^2)^4 + (2a^3b)^4 + (a^8 - 4a^4b^4 - 4b^8)^2, \end{aligned}$$

cannot represent $7^4=3^4+2^4+48^2$. The derivation of these identities is explained in Xeroudakes [20]. It seems unlikely that one would be able to find a complete solution of three of the above equations (2).

It is an interesting fact, however, that one can indeed find a complete solution of the last two equations. To do this, one subtracts the third from the fourth, and obtains

$$m^2 - z^2 = 2(w^2 + t^2) = (w + t)^2 + (w - t)^2.$$

By a short congruence argument (mod 8) on the third and fourth equations one shows that u and v have opposite parity, while w and t must be even. Thus, setting $r=w+t$ and $s=w-t$ gives a transformation reversible in integers, $w=\frac{1}{2}(r+s)$ and $t=\frac{1}{2}(r-s)$.

Then $r^2+s^2+z^2=m^2$, with r and s even. Moreover, $(r, s, z)=1$, for if p is a prime and $p\mid(r, s, z)$, then $p\mid r+s$ and $p\mid r-s$. So $p\mid 2w$ and $p\mid 2t$. But $p\neq 2$, as

z is odd, so $p \mid w$ and $p \mid t$. Thus $p \mid x^2$, $p \mid y^2$ and $p \mid z^2$, which is impossible. Thus we can apply our parametric solution:

$$\begin{aligned} r &= 2(UW - VT), \\ s &= 2(UT + VW), \\ z &= U^2 + V^2 - W^2 - T^2, \\ m &= U^2 + V^2 + W^2 + T^2. \end{aligned}$$

Solving now for u^2+v^2, we find $u^2+v^2=(U^2+V^2)^2+(W^2+T^2)^2$. Thus, u^2+v^2 is some representation of the sum of two squares $(U^2+V^2)^2+(W^2+T^2)^2$, and if we let u^2+v^2 run over all representations, we clearly obtain all the solutions of the last two of equations (2), namely

$$\begin{aligned} z &= U^2 + V^2 - W^2 - T^2, \\ m &= U^2 + V^2 + W^2 + T^2, \\ w &= UW - VT + UT + VW, \\ t &= UW - VT - UT - VW, \end{aligned} \qquad u^2 + v^2 = (U^2 + V^2)^2 + (W^2 + T^2)^2.$$

I wish to thank the referee for several suggestions.

References

1. L. E. Dickson, History of the Theory of Numbers, vol. 2, Chelsea, New York, 1956, pp. 259–274.

2. R. D. Carmichael, Diophantine Analysis, Wiley, New York, 1915, pp. 38–43.

3. L. E. Dickson, Some relations between the theory of numbers and other branches of mathematics, Comptes rendus du congrès international des mathématiciens, 1920, pp. 41–56.

4. Th. Skolem, Om ortogonalt beliggende gitterpunkter på kuleflater, Norsk Mat. Tidsskr., **23** (1941) 54–61.

5. F. Steiger, Über die Grundlösungen der Gleichung $a^2+b^2+c^2=d^2$, Elem. Math., **11** (1956) 105–108.

6. F. Miksa, A table of integral solutions of $a^2+b^2+c^2=r^2$, Mathematics Teacher, **48** (1955) 251–255.

7. A. Desboves, Applications des formulas générales qui donnent la solution complète, en nombres entiers, de l'équation homogène du second degré contenant un nombre quelconque d'inconnues, Nouv. Ann. Math., ser. 3, **5** (1886) 231–232.

8. D. C. Duncan, Generalized pythagorean numbers, Nat. Math. Mag., **10** (1936) 209–211.

9. N. Ginatempo, Problemi di analisi indeterminata in n variabili, Atti Soc. Peloritana Sci. Fis. Mat. Nat., **1** (1955) 15–25.

10. F. J. Duarte, Sur les équations diophantines $x^2+y^2+z^2=t^2$, $x^3+y^3+z^3=t^3$, Enseignement Math., **33** (1934) 78–87.

11. M. A. Buquet, Comparaison de différentes solutions de l'équation diophantine $x^2+y^2+z^2=t^2$, Mathesis, **58** (1949) 70–73.

12. W. Sierpinski, Teoria Liczb, 1950, pp. 237–240.

13. L. E. Dickson, Modern Elementary Theory of Numbers, The University of Chicago Press, 1939, p. 185.

14. ———, History of the Theory of Numbers, vol. 2, Chelsea, New York, 1956, p. 530.

15. L. Reitan, Nogen betraktninger over et tallteoretisk emne, Norsk Mat. Tidsskr., **22** (1940) 113–115.

16. E. Escott, Question no. 1464, L'intermediaire des Math., **6** (1899) 51.

17. E. Fauquembergue, Question no. 1464, *ibid.*, 7 (1900) 412.
18. A. Werebrusow, Question no. 3935, *ibid.*, 21 (1914) 161.
19. B. Padhy, Note on the expression of a biquadrate as a sum of three biquadrates, Math. Student, 3 (1935) 100–101. See also: *Ibid.*, 3 (1935) 155–156; *ibid.*, 4 (1936) 78.
20. G. Xeroudakes and K. Fasoulakes, Introduction to Diophantine Analysis of Higher Degree, 1947, p. 74.

ON QUASI-ORTHOGONAL NUMBERS

S. TAUBER, Portland State College

1. Introduction. Let m, n, p, and s be positive integers or zero, and let x be a complex variable. We consider polynomials of degree n,

$$P(n, x) = \sum_{m=0}^{n} A_n^m x^m \tag{1}$$

and triangular matrices of their coefficients,

$$A(n) = \begin{bmatrix} A_0^0 & & & & \\ A_1^0 & A_1^1 & & & \\ A_2^0 & A_2^1 & A_2^2 & & \\ \cdot & \cdot & \cdot & \cdot & \\ A_n^0 & A_n^1 & A_n^2 & \cdots & A_n^n \end{bmatrix}. \tag{2}$$

Two sets of numbers A_n^m, and B_n^m, are said to be quasi-orthogonal, according to [1] p. 32, if $A(n)B(n) = I$, i.e. if

$$\sum_{s=m}^{n} A_n^s B_s^m = \delta_n^m, \tag{3}$$

where δ_n^m is the Kronecker-δ. In order to complete the definition of the numbers as given by (1) we assume that $A_n^m = 0$ for $n < 0$, $m < 0$, and $n < m$. Examples of quasi-orthogonal numbers will be given later. The aim of our study is to find recurrence relations for quasi-orthogonal numbers.

2. Q-polynomials and generalized Stirling numbers. Let M and N be two functions of the variable n, such that $M(0) \neq 0$ and for n a positive integer or