On the equation $x^2 + ry^2 = z^2$

EMRYS READ

In this Article, we derive a method for classifying all *positive integer* solutions of the equation $x^2 + ry^2 = z^2$, where r is a given *positive rational*. In order to simplify notation, such a solution with $x = a$, $y = b$ and $z = c$ will be denoted by the ordered triple (a, b, c) and, in all that follows, the term *solution* will be taken to mean a positive integer solution of the above equation. The method employed will be similar to that used in [1] to find all integer triangles containing an angle whose cosine is known.

We start by considering a simple example. It may easily be verified that (5, 6, 7), (5, 12, 11) and (10, 12, 14) are all solutions of $x^2 + ry^2 = z^2$ when $r = \frac{2}{3}$. The first and third solutions are clearly related to one another whereas the second is a fundamentally different solution. In order to be able to avoid any unnecessary repetitions, we formally define two solutions as being equivalent as follows.

Definition 1: Two solutions (a, b, c) and (e, f, g) of the equation $x^2 + ry^2 = z^2$ are said to be *equivalent* if there exists a rational s such that $e = sa, f = sb$ and $g = sc$.

Before proceeding further, we introduce the concept of an r-pair which will play a central role in our discussions below.

Definition 2: The ordered pair (α, β) is called an r-pair if α, β are both rational with $\alpha > \beta > 0$ and $\alpha\beta = r$.

Lemma 1: Let (a, b, c) be a solution of the equation $x^2 + ry^2 = z^2$. Then

(i) (a, b, c) is associated in a canonical way with an r-pair (α, β),

(ii) any solution equivalent to (a, b, c) will be associated with the same r-pair (α, β).

Proof:

(i) Rearranging the equation $a^2 + rb^2 = c^2$, we have

$$r = \frac{(c + a)(c - a)}{b^2}. \tag{1}$$

Putting

$$\frac{(c + a)}{b} = \alpha \text{ and } \frac{(c - a)}{b} = \beta, \tag{2}$$

we see that α, β are both rational, $\alpha > \beta > 0$ and from (1), $\alpha\beta = r$.

https://doi.org/10.1017/mag.2019.10 Published online by Cambridge University Press

(ii) Any solution equivalent to (a, b, c) will be of the form (sa, sb, sc) for some positive rational s and

$$\frac{(sc + sa)}{sb} = \frac{(c + a)}{b} = \alpha \text{ and } \frac{(sc - sa)}{sb} = \frac{(c - a)}{b} = \beta.$$

Before proceeding to Lemma 2, we note that (2) implies that $\alpha + \beta = \frac{2c}{b}$ and $\alpha - \beta = \frac{2a}{b}$.

We now write $\alpha = \frac{\alpha_1}{\alpha_2}$, $\beta = \frac{\beta_1}{\beta_2}$, where $\alpha_1, \alpha_2, \beta_1, \beta_2$ are positive integers with $\gcd(\alpha_1, \alpha_2) = \gcd(\beta_1, \beta_2) = 1$. Substituting for α, β gives

$$\frac{\alpha_1\beta_2 + \alpha_2\beta_1}{\alpha_2\beta_2} = \frac{2c}{b} \text{ and } \frac{\alpha_1\beta_2 - \alpha_2\beta_1}{\alpha_2\beta_2} = \frac{2a}{b}$$

and thus

$$\frac{\alpha_1\beta_2 - \alpha_2\beta_1}{a} = \frac{2\alpha_2\beta_2}{b} = \frac{\alpha_1\beta_2 + \alpha_2\beta_1}{c}. \tag{3}$$

In the light of (3), we proceed as follows.

Definition 3: Given any r-pair (α, β), define $T_{(\alpha,\beta)}$ to be the ordered triple

$$(\alpha_1\beta_2 - \alpha_2\beta_1,\ 2\alpha_2\beta_2,\ \alpha_1\beta_2 + \alpha_2\beta_1),$$

where $\alpha_1, \alpha_2, \beta_1, \beta_2$ are as above.

Lemma 2:

(i) $T_{(\alpha,\beta)}$ is a solution of the equation $x^2 + ry^2 = z^2$.

(ii) The r-pair associated with $T_{(\alpha,\beta)}$ in the sense of Lemma 1 is (α, β).

(iii) $T_{(\alpha,\beta)}$ and $T_{(\gamma,\delta)}$ are equivalent solutions if, and only if, $(\alpha, \beta) = (\gamma, \delta)$.

Proof:

(i) All three components of the triple are clearly integers and $\alpha_1\beta_2 - \alpha_2\beta_1$ is positive since $\alpha > \beta$.

It may also easily be verified that

$$(\alpha_1\beta_2 - \alpha_2\beta_1)^2 + \frac{\alpha_1\beta_1}{\alpha_2\beta_2}(2\alpha_2\beta_2)^2 = (\alpha_1\beta_2 + \alpha_2\beta_1)^2.$$

(ii) $$\frac{(\alpha_1\beta_2 + \alpha_2\beta_1) + (\alpha_1\beta_2 - \alpha_2\beta_1)}{2\alpha_2\beta_2} = \frac{2\alpha_1\beta_2}{2\alpha_2\beta_2} = \alpha$$

and $$\frac{(\alpha_1\beta_2 + \alpha_2\beta_1) - (\alpha_1\beta_2 - \alpha_2\beta_1)}{2\alpha_2\beta_2} = \frac{2\alpha_2\beta_1}{2\alpha_2\beta_2} = \beta.$$

(iii) This now follows from part (ii) above and part (ii) of Lemma 1.

https://doi.org/10.1017/mag.2019.10 Published online by Cambridge University Press

It will be convenient to use the following notation to bring together the results of Lemma 1 and Lemma 2.

Let S be the set of all solutions of the equation $x^2 + ry^2 = z^2$. Then S may be partitioned into a disjoint union of subsets S_i where two solutions belong to the same S_i if, and only if, they are equivalent.

Let $Q = \{S_i\}$ and $P = \{r\text{-pairs}\}$.

Theorem 1: Let τ be the function from P to Q which maps the r-pair (α, β) to S_i, where S_i is the set containing the solution $T_{(\alpha,\beta)}$ defined above. Then the results of Lemma 1 and Lemma 2 imply that the function τ is 1-1 and onto.

Let us now consider the examples given in the two tables below.

(a) $r = \frac{3}{4}$

α	β	$a = \alpha_1\beta_2 - \alpha_2\beta_1$	$b = 2\alpha_2\beta_2$	$c = \alpha_1\beta_2 + \alpha_2\beta_1$	$\gcd(a, b, c)$
$\frac{1}{1}$	$\frac{3}{4}$	1	8	7	1
$\frac{3}{2}$	$\frac{1}{2}$	4	8	8	4
$\frac{5}{2}$	$\frac{3}{10}$	44	40	56	4
$\frac{6}{5}$	$\frac{5}{8}$	23	80	73	1

(b) $r = \frac{8}{9}$

α	β	$a = \alpha_1\beta_2 - \alpha_2\beta_1$	$b = 2\alpha_2\beta_2$	$c = \alpha_1\beta_2 + \alpha_2\beta_1$	$\gcd(a, b, c)$
$\frac{4}{3}$	$\frac{2}{3}$	6	18	18	6
$\frac{16}{3}$	$\frac{1}{6}$	93	36	99	3
$\frac{2}{1}$	$\frac{4}{9}$	14	18	22	2
$\frac{8}{5}$	$\frac{5}{9}$	47	90	97	1

Clearly the solutions produced by our method do not always appear in their simplest form. For example, the solution (4, 8, 8) in the first table is equivalent to the solution (1, 2, 2) and in the same way, (93, 36, 99) in the second table is equivalent to (31, 12, 33). Consequently, we make the following definition.

Definition 4: A solution (a, b, c) is called *primitive* if $\gcd(a, b, c) = 1$. We note that given any solution (a, b, c), we can find an equivalent primitive solution simply by dividing each component of the triple by $\gcd(a, b, c)$.

https://doi.org/10.1017/mag.2019.10 Published online by Cambridge University Press

We shall therefore look more closely at the possible values which can be taken by $\gcd(a, b, c)$. In particular, in Theorem 2 below, we establish a relationship between $\gcd(a, b, c)$ and $\gcd(\alpha_2, \beta_2)$.

Definition 5: Using the notation of Definition 3 above, we let $h = \gcd(a, b, c)$ and $d = \gcd(\alpha_2, \beta_2)$. We also write $\alpha_2 = 2^u k$, $\beta_2 = 2^v q$, $d = 2^w m$ and $h = 2^t n$, where u, v, w, t are integers greater than or equal to 0 and k, q, m, n are odd integers.

Lemma 3

(i) $w = \min(u, v)$ and $m = \gcd(k, q)$.

(ii) $d \mid h$ and consequently, $m \mid n$ and $w \leqslant t$.

(iii) $\gcd(n, \alpha_1) = \gcd(n, \beta_1) = 1$.

(iv) $n = m$.

Proof:

(i) This follows as a direct consequence of the definitions of the expressions for α_2, β_2, d and h in terms of u, v, w, t, k, q, m and n given above.

(ii) We note that since $d \mid \alpha_2$ and $d \mid \beta_2$ then it must also be true that $d \mid a$, $d \mid b$ and $d \mid c$. Thus $d \mid h$ and it now follows immediately that $m \mid n$ and $w \leqslant t$.

(iii) Let p be a prime such that $p \mid \gcd(n, \alpha_1)$. Since $p \mid n$, p must be odd and $p \mid a$, $p \mid b$, $p \mid c$. It follows that $p \mid (c - a + b) = 2\alpha_2(\beta_1 + \beta_2)$ and, as $p \mid \alpha_1$ and $\gcd(\alpha_1, \alpha_2) = 1$, we must have $p \mid (\beta_1 + \beta_2)$. In the same way, by considering $(c - a - b)$, we see that $p \mid (\beta_1 - \beta_2)$. These two facts imply that $p \mid \beta_1$ and $p \mid \beta_2$, which contradicts the fact that $\gcd(\beta_1, \beta_2) = 1$. Thus no such p can exist and $\gcd(n, \alpha_1) = 1$.

The fact that $\gcd(n, \beta_1) = 1$ can be proved in a similar way and is left as an exercise for the reader.

(iv) We note that $n \mid (c + a) = 2\alpha_1\beta_2$. By part (iii), $\gcd(n, \alpha_1) = 1$ and since n is odd we must have $n \mid \beta_2$. In the same way, by considering $(c - a)$, we see that $n \mid \alpha_2$. Thus $n \mid d$ and since n is odd, $n \mid m$. This, taken together with the result of part (ii), implies that $n = m$.

Let us now consider what happens when h is even. This can occur if, and only if, $\alpha_1\beta_2$ and $\alpha_2\beta_1$ are either both even or both odd. We consider three separate cases.

- α_2, β_2 both odd and α_1, β_1 either both even or both odd.
  In this case, using the notation of Definition 5, we see that $w = 0$ and $t = 1$.
- $\alpha_2 = 2^u k$, $\beta_2 = 2^v q$ both even with $u \neq v$, α_1, β_1 both odd.
  By Lemma 3 part (i), $w = \min(u, v)$ and it follows that the

https://doi.org/10.1017/mag.2019.10 Published online by Cambridge University Press

highest powers of 2 dividing a, b and c are w, $u + v + 1$ and w respectively. Thus $t = w$.

- $\alpha_2 = 2^u k$, $\beta_2 = 2^v q$ both even with $u = v$, α_1, β_1 both odd. We note that $w = u = v$ and thus the highest power of 2 dividing b is $2w + 1$. On the other hand, $a = 2^w(\alpha_1 q - k\beta_1)$ and $c = 2^w(\alpha_1 q + k\beta_1)$. Both $\alpha_1 q - k\beta_1$ and $\alpha_1 q + k\beta_1$ are even but only one is divisible by 4. Thus we can conclude that $t = w + 1$.

We can now express the outcomes of the three cases considered above together with the result of part (iv) of Lemma 3 in the form given below in Theorem 2. As this just comprises a gathering together of previous results, the details are omitted.

Theorem 2: Let $h = \gcd(a, b, c)$ and $d = \gcd(\alpha_2, \beta_2)$. Then $h = 2d$ if *either*

α_2, β_2 are both odd and α_1, β_1 are either both even or both odd

or

α_2, β_2 are both even and the highest power of 2 dividing α_2 is equal to the highest power of 2 dividing β_2.

Otherwise $h = d$.

Before proceeding further, the reader should revisit the two tables above and in the light of the results of Theorem 2 check the values of $\gcd(a, b, c)$ given.

The situation is somewhat simplified when r is a positive *integer*. In this case we have the following result.

Lemma 4: If r is a positive integer, then using the same notation as above, $d = \gcd(\alpha_2, \beta_2) = 1$.

Proof: First of all we rewrite $r = \dfrac{\alpha_1\beta_1}{\alpha_2\beta_2}$ as $r\alpha_2\beta_2 = \alpha_1\beta_1$. Now let p be any prime such that $p \mid \alpha_2$ and $p \mid \beta_2$. Since r is an integer, the above equation implies that $p \mid \alpha_1$ or $p \mid \beta_1$. This, however, contradicts the fact that $\gcd(\alpha_1, \alpha_2) = \gcd(\beta_1, \beta_2) = 1$. Thus no such p can exist and we must have $\gcd(\alpha_2, \beta_2) = 1$.

We can combine the results of Theorem 2 and Lemma 4 as follows.

Theorem 3: Let r be a positive integer. All solutions are primitive except when α_2, β_2 are both odd and α_1, β_1 are either both even or both odd. In this case, $h = 2$.

https://doi.org/10.1017/mag.2019.10 Published online by Cambridge University Press

We now apply this result to different values of r.

r an odd integer greater than 1

All solutions are primitive except when $a_2, \beta_2, \alpha_1, \beta_1$ are all odd. In this case, $h = 2$.

r an even integer divisible by 4

All solutions are primitive except when α_2, β_2 are both odd and α_1, β_1 are both even. In this case, $h = 2$.

r an even integer not divisible by 4

All solutions are primitive.

$r = 1$

The problem now reduces to that of finding positive integer solutions to the equation $x^2 + y^2 = z^2$. The classification of *pythagorean triples* is a classical problem, the solution of which is well documented [2, pp 219-224]. Using our approach, we see, for example, that the solutions corresponding to $\alpha = \frac{2}{1}$, $\beta = \frac{1}{2}$ and $\gamma = \frac{3}{1}$, $\delta = \frac{1}{3}$ are (3, 4, 5) and (8, 6, 10) respectively. Whereas these are not equivalent in the sense of Definition 1, they clearly belong to the same family of solutions. In general, we have the following result, the proof of which is left as a simple exercise to the reader.

Lemma 5: Let $\alpha_1 > \alpha_2 > 0$ be positive integers, one of which is even and one of which is odd, with $\gcd(\alpha_1, \alpha_2) = 1$. Putting $\alpha = \dfrac{\alpha_1}{\alpha_2}$ and $\gamma = \dfrac{\alpha_1 + \alpha_2}{\alpha_1 - \alpha_2}$ and using the notation of Definition 3, we have

(i) $T_{(\alpha,1/\alpha)} = \left(\alpha_1^2 - \alpha_2^2,\ 2\alpha_1\alpha_2, \alpha_1^2 + \alpha_2^2\right)$ and is always a primitive solution.

(ii) $T_{(\gamma.1/\gamma)} = \left(4\alpha_1\alpha_2,\ 2\left(\alpha_1^2 - \alpha_2^2\right),\ 2\left(\alpha_1^2 + \alpha_2^2\right)\right)$ and is always such that $h = 2$.

Thus to avoid repetitions when $r = 1$, all we need do is to choose α_1, α_2 as in Lemma 5 and confine ourselves to solutions of the form $T_{(\alpha,1/\alpha)}$.

The tables below each contain four simple examples of solutions which illustrate the above results for $r = 2$, $r = 3$ and $r = 4$. The reader is encouraged to carry out further verification by considering other integer values of r with appropriate choice of α and β.

https://doi.org/10.1017/mag.2019.10 Published online by Cambridge University Press

(a) $r = 2$

α	β	$a = \alpha_1\beta_2 - \alpha_2\beta_1$	$b = 2\alpha_2\beta_2$	$c = \alpha_1\beta_2 + \alpha_2\beta_1$	h	Equivalent primitive solution
$\frac{3}{1}$	$\frac{2}{3}$	7	6	11	1	(7, 6, 11)
$\frac{5}{3}$	$\frac{6}{5}$	7	30	43	1	(7, 30, 43)
$\frac{7}{4}$	$\frac{8}{7}$	17	56	81	1	(17, 56, 81)
$\frac{30}{19}$	$\frac{19}{15}$	89	570	811	1	(89, 570, 811)

(b) $r = 3$

α	β	$a = \alpha_1\beta_2 - \alpha_2\beta_1$	$b = 2\alpha_2\beta_2$	$c = \alpha_1\beta_2 + \alpha_2\beta_1$	h	Equivalent primitive solution
$\frac{4}{1}$	$\frac{3}{4}$	13	8	19	1	(13, 8,19)
$\frac{5}{2}$	$\frac{6}{5}$	13	20	37	1	(13, 20, 37)
$\frac{7}{1}$	$\frac{3}{7}$	46	14	52	2	(23, 7, 26)
$\frac{17}{7}$	$\frac{21}{17}$	142	238	436	2	(71, 119, 218)

(c) $r = 4$

α	β	$a = \alpha_1\beta_2 - \alpha_2\beta_1$	$b = 2\alpha_2\beta_2$	$c = \alpha_1\beta_2 + \alpha_2\beta_1$	h	Equivalent primitive solution
$\frac{8}{3}$	$\frac{3}{2}$	7	12	25	1	(7, 12, 25)
$\frac{20}{9}$	$\frac{9}{5}$	19	90	181	1	(19, 90, 181)
$\frac{14}{3}$	$\frac{6}{7}$	80	42	116	2	(40, 21, 58)
$\frac{38}{17}$	$\frac{34}{19}$	144	646	1300	2	(72, 323, 650)

References

1. Emrys Read, On integer triangles, *Math. Gaz.*, **98** (March 2014) pp. 107-112.
2. Gareth A. Jones and J. Mary Jones, *Elementary number theory*, Springer (2002).

10.1017/mag.2019.10

EMRYS READ
5 Cefn Cynrig, Bethel, Caernarfon, Gwynedd LL55 1UW
e-mail: *mairacemrys@btinternet.com*

https://doi.org/10.1017/mag.2019.10 Published online by Cambridge University Press