

AN EXTENSION OF THE FUNDAMENTAL THEOREM ON RIGHT-ANGLED TRIANGLES

DOMINIC VELLA, ALFRED VELLA, AND JULIA WOLF

INTRODUCTION

$\{3, 4, 5\}$ is perhaps the most famous Pythagorean Triple with interest in such triples dating back many thousands of years to the ancient people of Mesopotamia. In this article, we shall consider such triples, with the restriction that the elements of these triples must not have any common factors - they are *Primitive Pythagorean Triples* (PPTs). In particular, we shall consider the question of how many PPTs a given integer can be a member of. The answer to this simple question is, surprisingly, that a given integer n can play the role of a specified side in either 0 or 2^{k-1} different PPTs, where k is the number of distinct prime factors of n . Our result is a generalisation of what Fermat grandly called the Fundamental Theorem on right-angled triangles ([2], chapter 5), which states that:

Every prime of the form $4m + 1$ is the hypotenuse of one, and only one, PPT.

It is well known ([3], p. 190) that any PPT can be written as a triple $\{e, d, h\}$, where $e = 2xy$, $d = x^2 - y^2$, $h = x^2 + y^2$, x and y are natural numbers of opposite parity, with $x > y$ and $(x, y) = 1$. With these restrictions, it is clear that d is always **odd** and e is always **even**. To determine the number of ways a given number can be a member of a PPT, we shall need two preliminary lemmas:

Uniqueness Lemma. *Given positive integers d and e , the real positive solution of $d = x^2 - y^2$ and $e = 2xy$ is unique. In particular, these two equations are satisfied by at most one pair of natural numbers $\{x, y\}$.*

Proof. We have $e = 2xy$ and $d = x^2 - y^2$, so that $x^4 - dx^2 - e^2/4 = 0$. This is a quadratic in x^2 whose solutions are:

$$x^2 = \frac{d \pm \sqrt{d^2 + e^2}}{2}$$

But only one of these is positive and so x is uniquely determined. y is then immediately given by $y = e/2x$, which completes the proof.

Throughout this article, we shall find ourselves counting the number of factorisations of a given number into two integers. To this end, the following lemma will be of great assistance:

Counting Lemma. *Let $n = p_1^{\pi_1} p_2^{\pi_2} \dots p_k^{\pi_k}$, where the p_i are distinct primes and the $\pi_i \geq 1$. There are 2^{k-1} different ways of writing $n = ab$, for positive integers $a > b$ with $(a, b) = 1$.*

Proof. We want to write $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ where the $\alpha_i = 0$ or π_i depending on whether $p_i | a$ or $p_i | b$ (since we are interested in a and b co-prime). Given this a , we immediately have $b = p_1^{\pi_1 - \alpha_1} p_2^{\pi_2 - \alpha_2} \dots p_k^{\pi_k - \alpha_k}$ so to count the number of ways of writing $n = ab$, we need only count the number of ways of writing a in this way, which is 2^k . However, this is an overestimate as each possibility has been counted twice (the factorisations ab and ba are equivalent!) and so the number of factorisations with $a > b$ is just 2^{k-1} , as claimed.

With these preliminary results, we shall now consider each of the sides of the PPT e , d and h in turn.

EVEN e

In this case we want to write $e = 2xy$, where x and y are co-prime and of opposite parity. Now it is clear that different values of x and y will give different PPTs (by the Uniqueness Lemma) and hence we only need calculate the number of ways in which e can be factorised to give x and y that are co-prime and of opposite parity. The condition of opposite parity is guaranteed by the condition that x and y be co-prime, provided that $e \equiv 0 \pmod{4}$ (since otherwise e cannot be a member of a PPT, as shown in [6]), and so we obtain the following result by an application of the Counting Lemma:

Theorem 1. *Let $e = p_1^{\pi_1} p_2^{\pi_2} \dots p_k^{\pi_k}$ with $e \equiv 0 \pmod{4}$, the p_i distinct primes and the $\pi_i \geq 1$. Then there are 2^{k-1} PPTs containing e as the even side.*

ODD d

Here we want to write $d = x^2 - y^2 = p_1^{\pi_1} p_2^{\pi_2} \dots p_k^{\pi_k}$. Observe that $x^2 - y^2$ can be factorised as $(x + y)(x - y)$, so in order to count solutions $\{x, y\}$ to $d = x^2 - y^2$ we can try counting

solutions $\{A, B\}$ to $d = AB$. By the Counting Lemma, we find 2^{k-1} solution pairs $\{A, B\}$ with $(A, B) = 1$ and $A > B$. To see that every co-prime solution pair $\{x, y\}$ of $d = x^2 - y^2$ arises from such a pair $\{A, B\}$, note that, as d is odd, so are $A = x + y$ and $B = x - y$ and because we require that $(x, y) = 1$, we also have that $(A, B) = 1$. We also need to show that each co-prime pair $\{A, B\}$ gives rise to a solution $\{x, y\}$ of the desired form. Writing $x = \frac{1}{2}(A + B)$, $y = \frac{1}{2}(A - B)$, it is clear that both these are integers and further that one is even and one is odd, since each of A and B are either $\pm 1 \pmod{4}$. To show that these factorisations always generate a PPT, we need only show that $(x, y) = 1$. Suppose, on the contrary, that $x = Xq$ and $y = Yq$ for some q , so that $x - y = (X - Y)q$ and $x + y = (X + Y)q$. In this case, we would have $(A, B) \geq q$, which contradicts the fact that $(A, B) = 1$.

Having seen that all of these factorisations do indeed generate PPTs, the question remains of whether the different factorisations lead to different PPTs or whether the same PPT is generated by different factorisations. Because of the Uniqueness Lemma, this is the same as asking whether the values of x and y given above can be achieved using two different factorisations of the same number. Now because $x > y$ (in the notation above) we must then have:

$$A + B = A' + B', \quad A - B = A' - B'$$

which then gives $A = A'$ and $B = B'$. But this is the same as saying that the factorisations $d = AB = A'B'$ were the same in the first place. This in turn shows that each different factorisation of d gives rise to a different PPT with d as one of the shorter sides and so we have proved the following theorem:

Theorem 2. *Let $d = p_1^{\pi_1} p_2^{\pi_2} \dots p_k^{\pi_k}$, where the p_i are distinct odd primes and the $\pi_i \geq 1$. Then there are 2^{k-1} PPTs in which d is one of the shorter sides.*

This result may seem surprising, since the exponents π_i do not appear in the final answer. This is precisely as we saw in the case of even e and is indeed the same as we shall see for the hypotenuse h later; it is a result of the rather strict condition that to generate a PPT, we must have x and y co-prime.

THE HYPOTENUSE h

The reader may wonder whether an integer h is ever the hypotenuse of more than one PPT. In fact, it has been known for many years that those prime numbers that are the hypotenuse of a PPT can only be such for one triangle. Fermat called this result the Fundamental Theorem on right-angled triangles and it is proved in most elementary number theory texts ([5], chapter 8).

We have shown elsewhere [6] that h is the hypotenuse of a PPT *iff* all of its prime factors are of the form $4m + 1$. Thus we need only consider such h . Legendre proved ([3], chapter 16) that these h can be expressed as the sum of two squares in $4d(h)$ different ways, where $d(h)$ is the number of factors of h including 1 and itself. It should be noted, however, that Legendre counts many representations that are for our purposes the same: in particular he counts $(\pm x)^2 + (\pm y)^2$ and the interchanged versions $x \leftrightarrow y$ as all being distinct. To get the number of *distinct* representations where both x and y are positive with $x > y$, we must then divide by 8. Hence, the number of ways of writing $h = x^2 + y^2$ with $x > y \in \mathbb{N}$ is $d(h)/2$.

Proposition 1. *Let $h = p_1 p_2 \dots p_k$ where the p_i are distinct odd primes of the form $4m + 1$. Then h is the hypotenuse of 2^{k-1} PPTs.*

Proof. By the preceding discussion of Legendre's rule and the Counting Lemma, we know that h can be represented as $x^2 + y^2$ with $x > y \in \mathbb{N}$ in 2^{k-1} ways. All that remains to be done is to show that these x and y are co-prime and of opposite parity. Both of these requirements are easily satisfied because of the restrictions that we have placed on h :

- (i) $h \equiv 1 \pmod{4}$. h can only be the sum of one odd and one even number (so that x and y must be of opposite parity).
- (ii) h is square-free. Any common factor of x and y , q say, would have to appear as q^2 in the prime factorisation of h (and so $(x, y) = 1$).

To study more general values of h , we must be careful in the way in which we count the number of representations as the sum of two squares. There are two potential counting problems, which we shall discuss first to make the proof of the next theorem (the generalisation of Proposition 1) more comprehensible.

(A) If $q^2|h$, then there is a representation $(qX)^2 + (qY)^2 = h$ in which $(x = qX, y = qY) \neq 1$. We want to try and exclude such possibilities in our counting.

(B) If $h = z^2$ (i.e. h is a perfect square), then the counting argument of Legendre includes the representations $h = 0 + z^2$ and $h = z^2 + 0$, which are of no interest here.

To counteract the problems in (A) and (B) above we will use the following two lemmas:

Representation Lemma. *Let $n = p_1^{\pi_1} p_2^{\pi_2} \dots p_j^{\pi_j} p_{j+1} \dots p_k$, where the p_i are distinct primes of the form $4m + 1$ and $\pi_i \geq 2$ for $i = 1, 2, \dots, j$. Then the number of representations of n as the sum of two co-prime squares, $\Sigma(n)$, is given by:*

$$\begin{aligned}
 \Sigma(n) &= \frac{1}{2} \left(d(n) + \sum_{l=1}^j \sum_{\substack{I \subseteq \{1, \dots, j\} \\ |I|=l}} (-1)^l d\left(\frac{n}{\prod_{i \in I} p_i^2}\right) \right) \\
 (1) \quad &= \frac{1}{2} \left(d(n) - \sum_{i=1}^j d\left(\frac{n}{p_i^2}\right) + \sum_{\substack{i, i'=1 \\ i \neq i'}}^j d\left(\frac{n}{p_i^2 p_{i'}^2}\right) - \dots \right)
 \end{aligned}$$

Proof. By (A), we know that any common factor of x and y , q say, must appear as a square factor of n . If we let A_i be the set:

$$A_i = \{\{x, y\} \in \mathbb{N}^2 : x > y, x^2 + y^2 = n \text{ and } p_i | (x, y)\}$$

then a moment's thought reveals that the number of *non*-co-prime representations is just $|\bigcup_{i=1}^j A_i|$. We can evaluate this using the Inclusion-Exclusion formula ([1], p. 76)

$$\left| \bigcup_{i=1}^j A_i \right| = \sum_{l=1}^j \sum_{\substack{I \subseteq \{1, \dots, j\} \\ |I|=l}} (-1)^{l+1} \left| \bigcap_{i \in I} A_i \right| = \sum_{i=1}^j |A_i| - \sum_{\substack{i, i'=1 \\ i \neq i'}} |A_i \cap A_{i'}| + \dots$$

along with the modified Legendre count $|A_i| = \frac{1}{2}d(n/p_i^2)$, $|A_i \cap A_{i'}| = \frac{1}{2}d(n/p_i^2 p_{i'}^2)$ etc. from which the lemma follows.

Hypotenuse Descent Lemma. *An integer z^2 is the hypotenuse of a PPT iff z is also the hypotenuse of a PPT.*

Proof. Suppose that z^2 is the hypotenuse of a PPT. Then there exist x and y (co-prime and of opposite parity) such that $x^2 + y^2 = z^2$. The triple $\{x, y, z\}$ is, however, a PPT with z as hypotenuse.

Conversely, if z is the hypotenuse of a PPT, then it must satisfy Pythagoras' Theorem $x^2 + y^2 = z^2$ for some x and y . Clearly, $(x, y) = 1$ (since $\{x, y, z\}$ is a PPT) and since the hypotenuse of a PPT is always odd, x and y must be of opposite parity. Thus z^2 is the hypotenuse of a PPT.

The Generalised Fundamental Theorem on Right-Angled Triangles. *Let $h = p_1^{\pi_1} p_2^{\pi_2} \dots p_k^{\pi_k}$ where the p_i are distinct primes of the form $4m + 1$ and the $\pi_i \geq 1$. Then h is the hypotenuse of 2^{k-1} PPTs.*

Proof. We first suppose that h is not a perfect square, so that the only counting problem we must beware is that considered in (A). We shall first show that the sum for $\Sigma(n)$ in (1) reduces to 2^{k-1} . Note that $d(n) = \prod_{i=1}^k (\pi_i + 1)$, so we can write:

$$\begin{aligned} 2\Sigma(n) &= \prod_{i=1}^k (\pi_i + 1) + \sum_{l=1}^j \sum_{\substack{I \subseteq \{1, \dots, j\} \\ |I|=l}} (-1)^l \prod_{i \in I} (\pi_i - 1) \prod_{i' \notin I} (\pi_{i'} + 1) \\ &= \prod_{i=1}^k (\pi_i + 1) \left(1 + \sum_{l=1}^j \sum_{\substack{I \subseteq \{1, \dots, j\} \\ |I|=l}} (-1)^l \prod_{i \in I} \frac{\pi_i - 1}{\pi_i + 1} \right) \\ &= \left(\prod_{j=1}^k (\pi_j + 1) \right) \prod_{i=1}^k \left(1 - \frac{\pi_i - 1}{\pi_i + 1} \right) = \prod_{j=1}^k (\pi_j + 1) \prod_{i=1}^k \left(\frac{2}{\pi_i + 1} \right) = 2^k \end{aligned}$$

as claimed. Observe that we have included extra terms in (1) corresponding to those i for which $\pi_i = 1$. This is valid since the contribution to the sum over all subsets of size l is 0 for all subsets containing such i .

In the case that h is a perfect square, we know from the Hypotenuse Descent Lemma that we can simply take the square root of h and calculate the number of PPTs for which \sqrt{h} is a hypotenuse. If \sqrt{h} is not a perfect square then we can apply the above analysis to show that it is the hypotenuse of 2^{k-1} PPTs. If \sqrt{h} is a perfect square itself then we continue taking square roots until the result is no longer a perfect square. This proves the theorem.

THE EQUATION $4x^2 + y^2 = n$

Having developed results to tackle the problem of how many PPTs a given integer is a member of, we shall now briefly investigate the applications of such methods to a classical number theoretic problem. In section 5.11 of [4], Niven and Zuckerman prove the following:

Theorem ([4], Theorem 5.15). *Let n be an integer $n > 1$, $n \equiv 1 \pmod{4}$. If n is a prime, then $4x^2 + y^2 = n$ has exactly one non-negative solution and it is a primitive solution i.e. $(x, y) = 1$. If n is not a prime, then $4x^2 + y^2 = n$ has either no primitive solutions, more than one non-negative primitive solution, or it has one non-negative primitive solution and at least one non-negative non-primitive solution.*

Since we can write $n = (2x)^2 + y^2$, and y is necessarily odd (as $n \equiv 1 \pmod{4}$), the results developed in the last section can be applied as they stand to this problem to enumerate the number of solutions to $n = 4x^2 + y^2$ for n not a prime (n a prime has already been enumerated by the above theorem, but is also equivalent to the Fundamental Theorem on right-angled triangles). The following is a strengthened version of Niven and Zuckerman's result:

Theorem 3. *Let $n = p_1^{\pi_1} p_2^{\pi_2} \dots p_k^{\pi_k}$ be an odd integer, $n > 1$.*

(i) *If any prime factor of n is of the form $4m + 3$, then $4x^2 + y^2 = n$ has no primitive solutions.*

(ii) *If n has no prime factors of the form $4m + 3$, then $4x^2 + y^2 = n$ has 2^{k-1} primitive solutions and $\frac{1}{2}(d(n) + \epsilon) - 2^{k-1}$ non-negative solutions where $\epsilon = 1$ or 0 depending on whether n is a perfect square or not.*

Proof. The proof of (i) was given in [6]. The proof of (ii) in the case where n is not a perfect square is a combination of the Generalised Fundamental Theorem and Legendre's rule preceding Proposition 1. For the case in which n is a perfect square, we must return to the original version of Legendre's rule that there are $4d(n)$ solutions of $(2x)^2 + y^2 = n$ in total. For a perfect square, these include the possibilities that $n = 0 + (\pm\sqrt{n})^2$ and its reverse (of which there are 4 variations in total) so that there are $4d(n) - 4$ solutions that do not involve 0. These still include the \pm combinations and reversals so we must now divide this by 8 which leaves $(d(n) - 1)/2$ interesting solutions and 1 trivial solution - i.e.

there are $(d(n) + 1)/2$ non-primitive, non-negative solutions. Of these, we have already established that 2^{k-1} are primitive and so the theorem follows.

CONCLUSIONS

In this article, we have considered each of the three sides of a PPT and shown that any integer that plays the role of e , d or h in one PPT also plays the same role in $2^{k-1} - 1$ other PPTs. Given the very different methods in which Theorems 1 and 2 along with the Generalised Fundamental Theorem were proved, this seems a little surprising at the very least and may perhaps hint at a deeper connection between the various sides of PPTs.

Acknowledgement. We are grateful to a proof reader for pointing out several errors in an earlier version of this note and helping to improve its clarity.

REFERENCES

- [1] P. J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, 1994.
- [2] H. Davenport, *The Higher Arithmetic: An Introduction to the Theory of Numbers*, Seventh Edition, Cambridge University Press, 1999.
- [3] G. H. Hardy and E. M. Wright, *Introduction to the Theory of Numbers*, Fourth Edition, Oxford University Press, 1960.
- [4] I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, Second Edition, Wiley, 1966.
- [5] J. J. Tattersall, *Elementary Number Theory in Nine Chapters*, Cambridge University Press, 1999.
- [6] D. Vella and A. Vella, When is n a member of a Pythagorean Triple?, *Math. Gaz.* (March 2003) **87**, 102-105 (2003).

194, BUCKINGHAM RD., BLETCHLEY, MK3 5JB

KERNERSTRASSE 26, 70182, STUTTGART, GERMANY

E-mail address: pythagoras@thevellas.com