Additivity of 2nd degree polynomials

Logan Gaastra

February 2017

1 Introduction

A Pythagorean triple is a triplet of integers (x,y,z) such that $x^2 + y^2 = z^2$. The idea of a Pythagorean triple was created by Pythagoras through his study of right triangles and fascination with integers, with a Pythagorean triple representing a right triangle with sides of integer lengths.

This paper attempts to purport not only the existence of triplets for the polynomial x^2 but also for all 2nd degree polynomials.

2 Additive Triplets

Definition. *Additive Triplets: Let $AP(a_0, a_1, ..., a_n)$ denote the set of integer triplets (x,y,z) such that for nth degree polynomial $P(x) = a_0 + a_1 x + ... + a_n x^n$,*

$$P(x) + P(y) = P(z)$$

We will call this the set of additive triplets for a polynomial.

We note that if $(x, y, z) \in AP(a_0, .., a_n)$, then $(y, x, z) \in AP(a_0, .., a_n)$, which fairly obviously follows from the additivity of integers. We will be focusing specifically on the case for 2nd degree polynomials, which we will denote as AP(a,b,c).

Let $(x, y, z) \in AP(a, b, c)$, then

$$ax^2 + bx^2 + c + ay^2 + by + c = az^2 + bz + c$$

Further,

$$a(z^2 - x^2 - y^2) + b(z - x - y) = c$$

So if we can show that there exist integers x,y,z that satisfy the previous equation, then we can show that AP(a,b,c) is not empty.

Lemma 1. *if and only if $i \equiv j(mod 2)$, there exists integers x,y,z such that $x^2 + y^2 - z^2 = i$, $x + y - z = j$*

Pf: We begin by noting that $x^2+y^2-z^2 \equiv x+y-z(2)$ so then for $i \equiv j+1(2)$ there will not exist x,y,z to satisfy the equalities.

Let i and j be odd, then i = 2i' + 1, j = 2j' + 1 for some i', j'. Then

$$(2j')^2 + (i' - 2j'^2 + 1)^2 - (i' - 2j'^2)^2 = 2i' + 1 = i$$

$$(2j') + (i' - 2j'^2 + 1) - (i' - 2j'^2) = 2j' + 1 = j$$

So then $(x, y, z) = (2j', i' - 2j'^2 + 1, i' - 2j'^2)$ solves the equalities.

Now let i and j be even, then i = 2i', j = 2j' for some i', j'. Then

$$(2j' - 1)^2 + (2j'^2 + 3j' - i')^2 - (2j'^2 - 3j' - i' - 1)^2 = 2i' = i$$

$$(2j' - 1) + (2j'^2 + 3j' - i') - (2j'^2 - 3j' - i' - 1) = 2j' = j$$

So then $(x, y, z) = (2j', 2j'^2 - 3j' - i', 2j'^2 - 3j' - i' - 1)^2$ solves the inequalities. So then for both even and odd i, j there exists integer x,y,z that solves the equalities $x^2 + y^2 - z^2 = i$, $x + y - z = j$

Lemma 2. Bezouts Identity: *For the equation ai+bj=c, if gcd(a,b) does not divide c, then the equation has no solutions.*

Lemma 3. *If ai+bj=1 has solutions, exclusively either there exist integers i', j' such that $i' \equiv j'$(mod 2) or $a \equiv b$(mod 2)*

If ai+bj=1 has solutions, then gcd(a,b)=gcd(i,j)=1, so then $i \not\equiv j$(mod 2) or $a \not\equiv b$(mod 2).

If only $a \not\equiv b$(mod 2) then we need not prove any further.

If $a \not\equiv b$(mod 2) and $i \not\equiv j$(mod 2) then $i \equiv a$(mod 2) and $j \equiv b$(mod 2). Further, $i \not\equiv j \equiv b$(mod 2) and also $j \not\equiv i \equiv a$(mod 2). Then a(i+b)+b(j-a)=1 is also true, and $i + b \equiv j - a$(mod 2).

Finally, if $a \equiv b$(mod 2), then i, j must not both be odd or even, or else ai+bj would be even.

Theorem 2.1. *For $P(x) = ax^2+bx+c$ there exist x,y,z such that P(x)+P(y)=P(z) if and only if $gcd(a,b) \mid c$ and either $2 * gcd(a,b) \mid c$ or $\frac{ab}{gcd(a,b)^2}$ is even. This is equivalent to saying that P(x) +P(y)+P(z) if and only if $\frac{abc}{2gcd(a,b)^3} \in \mathbb{Z}$*

P(x)+P(y)=P(z) for $P(x) = ax^2 + bx + c$ is equivalent to $a(z^2 - x^2 - y^2) + b(z - x - y) = c$. Using Lemma 2, we know that gcd(a,b)—c must be true for the equation to have solutions, so we need not prove that any further.

Continuing, let $a' = \frac{a}{gcd(a,b)}$ and $b' = \frac{b}{gcd(a,b)}$, $c' = \frac{c}{gcd(a,b)}$ then gcd(a',b')=1, so then there exists i,j such that a'i+b'j=1, further a'(ic')+b'(jc')=c'. So now, we just need to show that there exists x,y,z such that $ic' = z^2 - x^2 - y^2$ and $jc' = z - x - y$.

Let c' be divisible by 2, then ic' and jc' are equivalent modulo 2, so then using Lemma 1, there must exist solutions to $ic' = z^2 - x^2 - y^2$ and $jc' = z - x - y$.

Now let $2|\frac{ab}{gcd(a,b)^2}$, then 2—a'b', so then $a' \equiv b' + 1(mod 2)$. By Lemma 3, since $a \equiv b + 1(mod 2)$, there must exist i',j' such that $i' \equiv j'(mod 2)$. As such, $i'c' \equiv j'c'(mod2)$ so then by Lemma 1 there must exist solutions such that $ic' = z^2 - x^2 - y^2$ and $jc' = z - x - y$.

For the case in which neither c' nor $\frac{ab}{gcd(a,b)^2}$ is divisible by 2, a corollary of $\frac{ab}{gcd(a,b)^2}$ not being divisible by 2 is that $a \equiv b(mod2)$ and by Lemma 3, since $a \equiv b(mod2)$, there does not exist i',j' such that $i' \equiv j'(mod2)$. Also, c' is odd, so then $ic' \equiv i(mod2)$ and $jc' \equiv j(mod2)$ so then $ic' \equiv i \equiv j+1 \equiv jc'+1(mod2)$ and by Lemma 1, since ic' is not equivalent to jc' modulus 2, there do not exist solutions to $x^2 + y^2 - z^2 = ic'$, $x + y - z = jc'$.

$$QED$$

2.1 Additional Theorem

Theorem 2.2. *If (x,y,z) is contained in AP(a,b,c) for any a,b,c, then* $(z-x) \mid P(y)$ *and* $(z-y) \mid P(x)$

We know that if P(x)+P(y)=P(z) then $a(z^2 - x^2 - y^2) + b(z - x - y) = c$. so then

$$a(z^2 - x^2 - y^2) + b(z - x - y) = c$$

$$a(z^2 - y^2) + b(z - y) = P(x)$$

$$P(x) = a(z-y)(z+y) + b(z-y)$$

$$P(x) = (z-y)a((y+z) + b)$$

$$(z-y) \mid P(x)$$

You can use the same technique to arrive at the other result.

$$QED$$