Melbourne High School
Maths Extension Group 2023
Term 1 Week 7 Handout

Section B

1. Substituting $a = st$ and $b = (s^2 - t^2)/2$ into the LHS of $a^2 + b^2 = c^2$ yields

$$\begin{aligned} s^2t^2 + \frac{s^4 - 2s^2t^2 + t^4}{4} &= \frac{4s^2t^2 + s^4 - 2s^2t^2 + t^4}{4} \\ &= \frac{s^4 + 2s^2t^2 + t^4}{4} \\ &= \left(\frac{s^2 + t^2}{2}\right)^2 \end{aligned}$$

The second part of the proof is to show that the three numbers do indeed share no common factors. Note that this proof requires knowledge of the Euclid's lemma, which asserts that if a prime divides a product of two numbers, it must divide at least one of the two numbers. This will be covered in future handouts.

Using Euclid's lemma, We note that if any pair of a, b, and c shared a common prime factor, the third would share that same common factor. This is because if a prime divides $n^2 = n \cdot n$, it divides either n or n; hence it must divide n.

Now suppose that p is a common prime divisor of $a = st$, $b = (s^2 - t^2)/2$, and $c = (s^2 + t^2)/2$. From Euclid's lemma p divides either s or t, but not both, because s and t share no common factors; for now, let's assume that it divides s. Then we can write $s = pu$ for some integer u. Substituting this into b and we get $b = (p^2u^2 - t^2)/2$. Since, by assumption, p divides b, we have $b = pv$ for some integer v. Combining these two statements yields

$$p^2u^2 - t^2 = 2pv.$$

Rearrange for t^2 and we get $t^2 = p^2u^2 - 2pv$. The RHS is clearly divisible by p; hence t^2 must be divisible by p, which implies t is divisible by p. This is a contradiction, because s and t share no common factors.

Now we turn to the case when p divides t instead of s. As before, we can write $t = pu$ for some integer u, and $b = pv$ for some integer v. Again using these statements, we find that

$$s^2 - p^2u^2 = pv.$$

Rearrange for s^2 and deduce that s is divisible by p, once again contradicting the assumption that s and t share no common factors.

Thus a and b cannot share any common factors; this completes the proof that the triple $(st, (s^2 - t^2)/2, (s^2 + t^2)/2)$ for coprime odd integers s and t, where $s > t$, always generates a primitive Pythagorean triple.

2. Since s and t are odd, let $s = 2m + 1$ and $t = 2n + 1$ for integers m and n. We have chosen a

to be odd and b even, and so substituting s and t into $b = (s^2 - t^2)/2$, we get

$$\begin{aligned} b &= \frac{(2m+1)^2 - (2n+1)^2}{2} \\ &= \frac{4m^2 + 4m + 1 - 4n^2 - 4n - 1}{2} \\ &= 2m^2 + 2m - 2n^2 - 2n \\ &= 2m(m+1) - 2n(n+1) \end{aligned}$$

Note that $m(m+1)$ and $n(n+1)$ must be even; hence 4 divides both $2m(m+1)$ and $2n(n+1)$. This completes the proof that b is divisible by 4.

3. We first note that a square can only leave a remainder of 0 or 1 when divided by 3. We can see this just by calculating the squares of the numbers 0, 1, and 2:

$$\begin{aligned} 0^2 &\equiv 0 \pmod 3 \\ 1^2 &\equiv 1 \pmod 3 \\ 2^2 &\equiv 1 \pmod 3 \end{aligned}$$

Assume that neither a or b is divisible by 3. Then both a^2 and b^2 must be congruent to 1 mod 3. Then $c^2 \equiv a^2 + b^2 \equiv 2 \pmod 3$. We have just shown that this is impossible; a square cannot leave a remainder of 2 when divided 3. Hence either a or b must be divisible by 3.

If not familiar with modular arithmetic or its notation, this can also be proven by expanding expression such as $(3m+1)^2$ to determine that the square of a number 1 more than a multiple of 3 is also 1 more than a multiple of 3.

4. We begin, as before, by nothing that the only squares modulo 5 are 0, 1, and 4.

Assume that none of a, b, or c is divisible by 5. Then a^2 and b^2 are both congruent to either 1 or 4. Enumerating all the possibilities we get one of the following possibilities for c^2:

$$\begin{aligned} c^2 &\equiv 1 + 1 \equiv 2 \pmod 5 \\ c^2 &\equiv 1 + 4 \equiv 0 \pmod 5 \end{aligned}$$

We know the first possibility is impossible, so $c^2 \equiv 0 \pmod 5$, which contradicts our initial assumption.

Hence one of a, b, or c must be divisible by 5.

We have shown that each 3, 4, and 5 will always divide one of the numbers in a Pythagorean triple. So every the product of Pythagorean triple must be divisible by $3 \cdot 4 \cdot 5 = 60$. However, the highest common factor of the product of all Pythagorean triples must also be a factor of the product of the Pythagorean triple $(3, 4, 5)$; hence the HCF we are looking for is 60.

5. The equation of the live is $y = m(x+1)$. Substituting this into the equation of the circle, we get

$$\begin{aligned} x^2 + m^2(x^2 + 2x + 1) &= 1 \\ (1 + m^2)x^2 + m^2 2x + m^2 - 1 &= 0 \end{aligned}$$

From here, the quadratic formula could be used, but the better way is to recognise that $x = -1$ is a solution to the above equation; therefore we can use polynomial division to determine the other factor. So dividing the quadratic by $(x+1)$, we get

$$\frac{(1 + m^2)x^2 + m^2 2x + m^2 - 1}{x + 1} = (1 + m^2)x + (m^2 - 1)$$

Solving this equation for x gives $x = (1 - m^2)/(1 + m^2)$. Substitute this value of x into the equation $y = m(x + 1)$ to find

$$\begin{aligned} y &= m\left(\frac{1 - m^2 + 1 + m^2}{1 + m^2}\right) \\ &= m\left(\frac{2}{1 + m^2}\right) \\ &= \frac{2m}{1 + m^2}. \end{aligned}$$

Now we know that the other point of intersection is given by

$$(x, y) = \left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2}\right)$$

Since this point is on the circle given by the equation $x^2 + y^2 = 1$, we have

$$\left(\frac{1 - m^2}{1 + m^2}\right)^2 + \left(\frac{2m}{1 + m^2}\right)^2 = 1.$$

Multiplying both sides by $(1 + m^2)^2$,

$$(1 - m^2)^2 + 4m^2 = (1 + m^2)^2.$$

Since m is a rational number, let $m = v/u$, where u and v are integers. The above equation becomes

$$\begin{aligned} \left(1 - \frac{v^2}{u^2}\right)^2 + \frac{4v^2}{u^2} &= \left(1 + \frac{v^2}{u^2}\right)^2 \\ \left(\frac{u^2 - v^2}{u^2}\right)^2 + \frac{4v^2}{u^2} &= \left(\frac{u^2 + v^2}{u^2}\right)^2. \end{aligned}$$

Finally, multiply both sides by u^4 and we get

$$(u^2 - v^2)^2 + 4v^2u^2 = (u^2 + v^2)^2.$$

This Pythagorean triple generating formula $(a, b, c) = (u^2 - v^2, 2uv, u^2 + v^2)$ doesn't always generate primitive triples. As an extension, come up with conditions on u and v under which the triple generated is primitive.

6. Assume an arithmetic progression of three squares with a common difference that is also a square exists. If we let a^2, b^2, and c^2 be the terms of the sequence and d^2 be the common difference, we have

$$a^2 + d^2 = b^2$$

and

$$b^2 + d^2 = c^2.$$

This implies that

$$\begin{aligned} b^4 &= (a^2 + d^2)(c^2 - d^2) \\ &= a^2c^2 - d^2(a^2 - c^2) - d^4 \end{aligned} \tag{1}$$

Since $a^2 = b^2 - d^2$ and $c^2 = b^2 + d^2$, we have $a^2 - c^2 = b^2 - d^2 - b^2 - d^2 = -2d^2$. Substituting this into (1) yields

$$\begin{aligned} b^4 &= a^2c^2 + 2d^4 - d^4 \\ &= a^2c^2 + d^4 \end{aligned}$$

Let $X = b$, $Y = d$ and $Z = ac$ and rearrange to get the equation

$$X^4 - Y^4 = Z^2.$$

Since this equation has no nonzero integer solutions (and you can try proving this if you are interested), there cannot exist three squares in a arithmetic progression that have a common difference of a square.

7. We could use the formula for primitive triples derived earlier, but it is easier to use Euclid's formula as it was originally written down:

$$(a, b, c) = (2uv, u^2 - v^2, u^2 + v^2)$$

where u and v are coprime integers of different parity. The area of this triangle is $(1/2)ab = uv(u^2 - v^2)$. Assume that this value is a square. The factors of the right-hand side are u, v, $u + v$, and $u - v$; since u and v are coprime, each of those factors are coprime too. Thus we conclude that each of the four factors must be squares themselves, since their product is a square.

Let $u + v = x^2$, $u - v = y^2$, $u = r^2$, and $v = s^2$. Then

$$s^2 + y^2 = r^2$$

and

$$r^2 + s^2 = x^2.$$

Hence y^2, r^2, and x^2 form an arithmetic progression with common difference s^2. From the previous problem we know this is impossible; hence a right-angled triangle with integer length sides cannot have a square area.

You may notice that the question asked for *rational* length sides. Try to determine how the above proof is also (or is not) a proof that a right-angled triangle with rational length sides cannot have a square area.