MAU22103/33101 - Introduction to Number Theory

Exercise Sheet 4

Trinity College Dublin

Course homepage

Answers are due for Friday November 8th, 2pm.
The use of electronic calculators and computer algebra software is allowed.

Exercise 1 *Infinite descent with infinite equations*

Consider the Diophantine equation

$$x^2 + y^2 + z^2 = 2xyz.$$

We want to show that it has no non-negative integer solutions other than $(0, 0, 0)$.

1. (10pts) Show that if (x, y, z) is a solution where at least one of x, y, or z is 0, then they are all 0.

   Knowing this, it suffices to show that we have no positive integer solutions.

2. (10pts) Show that there are no solutions (x, y, z) where exactly 1 or 3 of x,y, and z are odd.

   Hint: Parity

3. (15pts) Show that there are no solutions (x, y, z) where exactly 2 of x, y, and z are odd.

   Hint: Parity^2*: if one is even, what is* $2xyz \pmod 4$*?*

4. (25pts) Show that, given a positive integer solution (x_1, y_1, z_1) to the Diophantine equation given, there exists a positive integer solution to the Diophantine equation

$$x^2 + y^2 + z^2 = 4xyz.$$

5. (25pts) Show that, given a positive integer solution (x_k, y_k, z_k) to the Diophantine equation

$$x^2 + y^2 + z^2 = 2^k xyz$$

   there exists a positive integer solution to the Diophantine equation

$$x^2 + y^2 + z^2 = 2^{k+1} xyz.$$

6. (15pts) Hence conclude that there are no positive integer solutions to

$$x^2 + y^2 + z^2 = 2xyz$$

   Hint: How important is the equation to infinite descent?

Solution 1

1. If one of x, y, or z is 0, then $2xyz = 0$. As

$$x^2 + y^2 + z^2 \geq 0$$

   and each square individually is non-negative, the only way to have

$$x^2 + y^2 + z^2 = 0$$

   is if $x = y = z = 0$.

2. Note that the right hand side $2xyz$ is always even. If all of x, y, z are odd, then $x^2 + y^2 + z^2$ is the sum of three odd numbers, which is odd, so there can be no solutions. Similarly, if exactly one of x, y, or z is odd, then $x^2 + y^2 + z^2$ is odd, so there can be no such solutions.

3. Suppose exactly two of x, y, z are odd and the third is even. Then $2xyz$ is 2 times an even number, and so is divisible by 4. Hence, we must have

$$x^2 + y^2 + z^2 \equiv 0 \pmod 4.$$

But if exactly two of them are odd, then

$$x^2 + y^2 + z^2 \equiv 2 \pmod 4.$$

Thus, there can be no such solutions.

4. Given a positive integer solution (x_1, y_1, z_1) to

$$x^2 + y^2 + z^2 = 2xyz$$

we have seen that x_1, y_1, z_1 must all be even. Hence, there exist $a, b, c \in \mathbb{N}$ such that

$$x_1 = 2a, \quad y_1 = 2b, \quad z_1 = 2c$$

which satisfy

$$4a^2 + 4b^2 + 2c^2 = 16abc$$

and hence

$$a^2 + b^2 + c^2 = 4abc.$$

Therefore $(x, y, z) = (\frac{x_1}{2}, \frac{y_1}{2}, \frac{z_1}{2})$ is a positive integer solution to

$$x^2 + y^2 + z^2 = 4xyz.$$

5. Suppose we have a positive integer solution (x_k, y_k, z_k) to

$$x^2 + y^2 + z^2 = 2^k xyz$$

By the same arguments as above, we must have that x_k, y_k, and z_k are all even. Hence, there exist $x_{k+1}, y_{k+1}, z_{k+1} \in \mathbb{N}$ such that

$$x_k = 2x_{k+1}, \quad y_k = 2y_{k+1}, \quad z_k = z_{k+1}.$$

As (x_k, y_k, z_k) satisfies

$$x^2 + y^2 + z^2 = 2^k xyz$$

we have that

$$4x_{k+1}^2 + 4y_{k+1}^2 + 4z_{k+1}^2 = 2^{k+3}x_{k+1}y_{k+1}z_{k+1}$$

and therefore

$$x_{k+1}^2 + y_{k+1}^2 + z_{k+1}^2 = 2^{k+1}x_{k+1}y_{k+1}z_{k+1}.$$

Thus $(x, y, z) = (x_{k+1}, y_{k+1}, z_{k+1}) = (\frac{x_k}{2}, \frac{y_k}{2}, \frac{z_k}{2})$ is a positive integer solution to

$$x^2 + y^2 + z^2 = 2^{k+1}xyz.$$

6. The equation is mostly irrelevant to infinite descent. What matters is that we cannot have infinite strictly decreasing sequences of integers.

   Suppose we have a positive integer solution (x_1, y_1, z_1) to

   $$x^2 + y^2 + z^2 = 2xyz.$$

   Then, from the previous parts of the question, we have that there exists a positive integer solution (x_k, y_k, z_k) to

   $$x^2 + y^2 + z^2 = 2^k xyz$$

   such that $z_k = 2z_{k+1}$ for each $k \geq 1$. In particular, as $z_1 > 0$, we must have that

   $$z_1 > z_2 > z_3 > \cdots > z_k > \cdots > 0$$

   is an infinite decreasing sequence of positive integers. This is impossible, therefore no such (x_1, y_1, z_1) can exist. Hence, we have no positive integer solutions.

This was the only exercise that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them

However, I strongly encourage you to give them a try, as the best way to learn number theory is through practice.

The exercises marked with a star are the exercises I will try to talk about in the tutorial lecture. If there are any exercises would would particularly like to discuss, please let me know

The exercises are arranged by theme, and roughly in order of difficulty within each theme, with the first few working as good warm-ups, and the remainder being of similar difficulty to the main exercise. You are welcome to email me if you have any questions about them. The solutions will be made available with the solution to the main exercise.

Exercise 2 *General Pythagorean triples*

Show that every Pythagorean triple (a, b, c) is of the form

$$a = d(u^2 - v^2), \quad b = 2duv, \quad c = d(u^2 + v^2)$$

up to swapping a and b, where $u, v, d \in \mathbb{N}$ satisfy $u > v$, $\gcd(u, v)$ and exactly one of u and v is odd.

Solution 2

If (a, b, c) is primitive, then we know that there exist u, v as required such that

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

Otherwise, (a, b, c) have a common divisor greater than 1. Let $d = \gcd(a, b, c)$. Then $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ is primitive, as any common divisor of two components would be a common divisor of the third, and hence must be 1. Thus, there exist u, v as required such that

$$\frac{a}{d} = (u^2 - v^2), \quad \frac{b}{d} = 2uv, \quad \frac{c}{d} = (u^2 + v^2)$$

as needed.

Exercise 3 *Hypotenuses of hypotenuses*

i) Show that, to any positive integer solution (a, b, c), with a, b, c pairwise coprime, to

$$x^2 + y^2 = z^4$$

we can associate a primitive Pythagorean triple (s, t, c).

ii) Hence, classify all such solutions to

$$x^2 + y^2 = z^4.$$

Solution 3

i) Given such a triple, (a, b, c^2) is a Pythagorean triple, which is primitive, as

$$\gcd(a, b) = \gcd(a, c^2) = \gcd(a, c) = \gcd(b, c^2) = \gcd(b, c) = 1$$

Hence, there exist $s, t \in \mathbb{N}$ such that $s > t$, $\gcd(s, t) = 1$, and exactly one of s and t is odd such that

$$s^2 + t^2 = c^2.$$

Thus (s, t, c) is a Pythagorean triple, that must be primitive. We know that $\gcd(s, t) = 1$, and if there existed a common factor of s and c (or t and c, it would have to be a common factor of s and t as well.

ii) Every such solution corresponds uniquely to a primitive Pythagorean triple (s, t, c). The conditions on s and t, up to reordering, are a consequence of primitivity. Every such Pythagorean triple is given by a pair $u, v \in \mathbb{N}$ such that $u > v$, $\gcd(u, v) = 1$ and exactly one of u and v is odd. Thus, every triple (a, b, c) of pairwise coprime integers such that

$$a^2 + b^2 = c^4$$

is given by (up to reordering a and b)

$$a = |u^4 - 6u^2v^2 + v^4|, \quad b = 4(u^2 - v^2)uv, \quad c = u^2 + v^2,$$

for integers $u, v \in \mathbb{N}$ such that $u > v$, $\gcd(u, v) = 1$ and exactly one of u and v is odd.

Exercise 4 *Odd numbers in Pythagorean triples*

i) Show that, if $t, n \in \mathbb{N}$ satisfy

$$t^2 + (n - 1)^2 = n^2$$

then $\gcd(t, n - 1) = \gcd(t, n) = 1$. Hence conclude that n is odd.

ii) Writing $n = 2s + 1$, determine for what positive integers s there exists t such that

$$t^2 + (2s)^2 = (2s + 1)^2$$

iii) Hence show that every odd number greater than 1 appears in a primitive Pythagorean triple.

Solution 4

i) Suppose $d|t$ and $d|(n-1)$. Then $d^2|n^2$ and hence $d|n$. Thus $d|\gcd(n, n-1) = 1$, and so $d = \pm 1$. Similarly, any common divisor of t and n is ± 1. Thus $\gcd(t, n-1) = \gcd(t, n) = \gcd(n-1, n) = 1$.

   This means that $(t, n-1, n)$ is a primitive Pythagorean triple, and hence we must have that n is odd.

ii) As $(t, 2s, 2s+1)$ is a primitive Pythagorean triple, we have that t is odd. We must also have that

$$t^2 = 4s + 1$$

   and so $s = \frac{t^2-1}{4}$, which is always an integer, as t is odd. Writing $t = 2k+1$ for some $k \geq 0$, we get $s = k^2 + k$. As s is positive, we must have $k \in \mathbb{N}$ Thus, for every for every s in the set

$$\{k^2 + k \mid k \in \mathbb{N}\}$$

   we can find a corresponding t.

iii) Given any $k \in \mathbb{N}$, we have a primitive Pythagorean triple

$$(2k + 1, 2k^2 + 2k, 2k^2 + 2k + 1).$$

   Every odd number greater than 1 appears as the first entry in this triple.

Exercise 5 *Areas of Pythagorean triangles*

You may freely use the results of Exercise 2 here.

i) Determine if there exists a right angled triangle with integer side lengths of area 35.

ii) Determine if there exists a right angled triangle with integer side lengths of area 546.

iii) Show that, for $n \geq 54$, there exists a right angled triangle with integer side lengths, and area between n and $2n$.

   Hint: Pick a primitive Pythagorean triple (a, b, c) and consider the right angled triangle with side lengths (ak, bk, ck) for $k \in \mathbb{N}$. Given $n \geq 54$, can we find k such that

$$\textit{Area}(ak, bk, ck) \leq n < \textit{Area}(a(k+1), b(k+1), c(k+1))\textit{?}$$

If so, how can we bound the second area by $2n$?

Remark: Integers that are the areas of right angled triangles with rational side lengths are called congruent numbers, and can be classified using special functions called modular forms, which also appear in the proof of Fermat's Last Theorem.

Solution 5

i) Suppose we have such a triangle, with side lengths (a, b, c). Then there exist $u, v, d \in \mathbb{N}$ as in Exercise 1, and hence we must have that

$$35 = \frac{1}{2}ab = d^2(u^2 - v^2)uv = d^2(u - v)(u + v)uv.$$

As $35 = 5 \times 7$ is not divisible by any squares, we must have $d = 1$. Since 5 and 7 are prime, we must have that 5 divides exactly one of the factors on the right hand side, and similarly for 7. All remaining factors must be 1. Since $u > v$, $u \neq 1$, and $u + v \neq 1$, that means that $u - v = v = 1$, and so $u = 2$, which is not a factor of 35. Therefore, no such right angled triangle can exist.

ii) Suppose we have such a triangle, with side lengths (a, b, c). Then there exist $u, v, d \in \mathbb{N}$ as in Exercise 1 such that

$$546 = \frac{1}{2}ab = d^2(u - v)(u + v)uv.$$

Factorising 546, we see that

$$546 = 2 \times 3 \times 7 \times 13.$$

This is not divisible by any squares, so we must have $d = 1$.

Since each prime factor appears exactly once, we just have to figure out how to distribute them among $v < u < u + v$ and $u - v$. As exactly one of u and v is odd, both $u + v$ and $u - v$ are odd, so 2 must divide one of u or v.

We note also that no pair of $\{2, 3, 7, 13\}$ sum to another element of the set, so we cannot have that each factor $u, v, u - v, u + v$ is equal to one of these primes. In particular, we must have that one of $u, v, u - v, u + v$ is equal to 1. The only possibilities are v or $u - v$.

If $v = 1$, then u is even. We cannot have $u = 2$, as then $u - v = 1$ and $u + v = 3$, which cannot occur given our list of primes, so we must have $u = 2k$ for some $k > 1$. Considering the possible values of u and $u + v = u + 1$, it is clear that this cannot occur: if $u + 1$ has more than one prime factor, it is too big compared to u, and if it has exactly one prime factor, then u has prime factors not in our list.

Thus, $u - v = 1$, so $u = v + 1$. Considering the possible values of v, we see that the only possibilities are

$$(u, v) \in \{(3, 2),\ (7, 6)\,(14, 13)\}.$$

Considering $u+v$ for each of these, we find that $(u, v) = (7, 6)$ is possible, and indeed, the right angled triangle with side lengths $(13, 84, 85)$ has area 546.

iii) Consider the triangle with side lengths $(3k, 4k, 5k)$. This has area $6k^2$. It would suffices to show that for every $n \geq 54$, there exists k such that

$$n \leq 6k^2 \leq 2n$$

Consider the largest $k \in \mathbb{N}$ such that

$$6k^2 \leq n$$

We must then have that $12k^2 \leq 2n$, and, by definition, that $6(k+1)^2 > n$. Thus, if we can show that

$$n < 6(k + 1)^2 \leq 12k^2 \leq 2n$$

we are done. The middle inequality holds if $6k^2 - 12k - 1 > 0$, which is true for all $k \geq 3$, as $6x^2 - 12x + 1$ is increasing for $x \geq 1$. Hence, for all $n \geq 6(3)^2 = 54$, we the claim holds.

Exercise 6 *Homogeneous equations and rational solutions*

Call a polynomial $F(x_1, x_2, \ldots, x_n)$ homogeneous if and only if there exists $d \geq 0$ such that

$$F(\lambda x_1, \ldots, \lambda x_n) = \lambda^d F(x_1, \ldots, x_n)$$

for all $\lambda \in \mathbb{R}$.

i) Show that $F(x_1, \ldots, x_n)$ has non-zero integer solutions if and only if it has non-zero rational solutions.

ii) Show that $F(x, y, z) = x^2 + y^2 - z^2$ is homogeneous.

iii) As $F(x, y, z)$ is homogeneous, every non-zero integer solution (a, b, c) to $F(x, y, z) = 0$ corresponds uniquely to a point on the circle

$$\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

with rational coordinates As such, it suffices to find all rational points on the circle to describe all Pythagorean triples.

Show that every point other than $(-1, 0)$ on the circle can be written in the form

$$\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

for a unique $t \in \mathbb{R}$

iv) Show that a point $(x, y) \neq (-1, 0)$ on the circle has rational coordinates $x, y \in \mathbb{Q}$ if and only if $t \in \mathbb{Q}$.

v) Hence recover our classification of primitive Pythagorean triples.

Hint: Let (a, b, c) be a primitive Pythagorean triple, and write $t = \frac{v}{u}$ where $\gcd u, v = 1$. Why must $u > v > 0$? Then note that if $\frac{a}{c} = \frac{A}{C}$, and $\gcd(a, c) = \gcd(A, C) = 1$, we must have $a = A$ and $c = C$.

Solution 6

i) If $F(x_1, \ldots, x_n)$ has a non-zero integer solution, that is a non-zero rational solution. Conversely, suppose $F(x_1, \ldots, x_n) = 0$ for some non-zero rational numbers $x_1, \ldots, x_n$, and let N be their least common denominator. Then

$$F(Nx_1, \ldots, Nx_n) = N^d F(x_1, \ldots, x_n) = 0$$

and $Nx_i \in \mathbb{Z}$ for each $1 \leq i \leq n$, so we get an integer solution.

ii)

$$(\lambda x)^2 + (\lambda y)^2 - (\lambda z)^2 = \lambda^2(x^2 + y^2 - z^2).$$

iii) We first note that

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

so these points are indeed on the circle. Clearly if

$$x^2 + y^2 = 1, \quad \text{and} \quad x = \frac{1-t^2}{1+t^2}$$

then we must have

$$y = \frac{2t}{1+t^2}$$

with positive t corresponding to the positive solution to $y^2 = 1 - x^2$, and negative t corresponding to the negative solution.

Now, given $x \in (-1, 1]$, we claim we can always find $t \in \mathbb{R}$ such that $x = \frac{1-t^2}{1+t^2}$. This is equivalent to solving

$$(1 + x)t^2 = 1 - x$$

for real t. Since $x \neq -1$, we can always find t satisfying this. Thus, given a pair (x, y) on the circle, we can determine t^2 from x, and the sign of t from the sign of y, giving unique t for every pair (x, y).

iv) Clearly if $t \in \mathbb{Q}$, then $x, y \in \mathbb{Q}$. Conversely, if $x, y \in \mathbb{Q}$, then $t^2 = \frac{1-x}{1+x} \in \mathbb{Q}$, so $1 + t^2 \in \mathbb{Q}$, and so

$$t = \frac{y(1+t^2)}{2} \in \mathbb{Q}.$$

v) A primitive Pythagorean triple (a, b, c), with a odd and b even corresponds to a point on the circle $(x, y) = (\frac{a}{c}, \frac{b}{c})$, and hence there exists rational t such that

$$fracac = \frac{1-t^2}{1+t^2}, \quad \frac{b}{c} = \frac{2t}{1+t^2}.$$

As $b > 0$, $t > 0$, and so there exist $u, v \in \mathbb{N}$ such that $\gcd(u, v) = 1$ and $t = \frac{v}{u}$. Thus

$$\frac{a}{c} = \frac{u^2 - v^2}{u^2 + v^2}, \quad \frac{b}{c} = \frac{2uv}{u^2 + v^2}.$$

This also implies that $u > v$ as $a > 0$, and the parity constraint similarly follows. As $\frac{a}{c}$ and $\frac{b}{c}$ are fully simplified, since $\gcd(a,c) = \gcd(b,c) = 1$, it suffices to show that

$$\gcd(u^2 - v^2, u^2 + v^2) = \gcd(2uv, u^2 + v^2) = 1$$

For the former, suppose that $p|u^2 - v^2$ and $p|u^2 + v^2$ for some prime p. Then $p|2u^2$ and $p|2v^2$. Since $\gcd(u,v) = 1$, we must have that $p|2$, i.e $p = 2$. Similarly, if $q|2uv$ and $q|u^2 + v^2$, then $q|(u+v)^2$ and $q|(u-v)^2$. For q a prime, this implies that $q|(u+v)$ and $q|(u-v)$, hence $q|2$ and $q = 2$. So the only way we have issues in either case is if u and v are both odd, as this is the only way to have $\gcd(u,v) = 1$, and u^2+v^2 even.

But if u, v are both odd, then $u^2 - v^2$ is divisible by 4, which $u^2 + v^2$ is only divisible by 2, not 4. Hence, when we simplify

$$\frac{u^2 - v^2}{u^2 + v^2} = \frac{a}{c}$$

we obtain an even numerator, but a is odd. Thus, we cannot have that $2|u^2+v^2$, and hence the fractions are fully simplified and we can conclude that

$$a = u^2 - v^2, \quad b = 2uv, \quad c = u^2 + v^2$$

Exercise 7 *Infinite descent times three*

Via the method of infinite descent, show that there are no triples of positive integers $a, b, c \in \mathbb{N}$ such that

$$9a^3 + 3b^3 + c^3 = 0$$

Unhelpful Hint: 3

Solution 7

Suppose we have a triple of positive integers satisfying the given equation, and in particular, one in which c is minimal among all possible triples.

Clearly $3|c^3$ and so $3|c$. Hence, there exists $c_1 \in \mathbb{N}$ such that $c = 3c_1$, and so

$$9a^3 + 3b^3 + 27c_1^3 = 0 \quad \Rightarrow 9c_1^3 + 3a^3 + b^3 = 0$$

and so we obtain another triple (c_1, a, b) satisfying the same equation. We can thus conclude that $3|b$ and so $b = 3b_1$ for some $b_1 \in \mathbb{N}$, and therefore

$$9b_1^3 + 3c_1^3 + a^3 = 0.$$

Similarly, we must have that $a = 3a_1$ for some $a_1 \in \mathbb{N}$, and so

$$9a_1^3 + 3b_1^3 + c_1^3 = 0.$$

But then (a_1, b_1, c_1) is a triple of positive integers satisfying the given equation, with $c_1 < c$. This contradicts the minimality of c, and hence so positive integer solutions can exist.

Exercise 8 *Infinite descent for rational solutions*

Consider again the equation

$$x^2 + y^2 + z^2 = 2xyz.$$

We have seen that it has no positive integer solutions. We will now show that it has no non-zero rational solutions

i) Show that there are no non-zero integer solutions, by considering what happening is one, two, or three of x, y, z are negative.

ii) Show that the existence of a rational solution is equivalent to the existence of a triple of rational numbers (x, y, r) such that

$$x^2y^2 - x^2 - y^2 = r^2.$$

iii) Show that the existence of a triple of such rational numbers is equivalent to the existence of a triple (a, b, c) of integers such that

$$a^2b^2 - a^2 - b^2 = c^2$$

Hint: take a common denominator and write $(x, y, r) = (\frac{a}{n}, \frac{b}{n}, \frac{q}{n})$

iv) By rewriting the equation as

$$(a^2 - 1)(b^2 - 1) - 1 = c^2$$

conclude that any integer solution (a, b, c) must have a, b, c all even.

v) Via the same formulation of the equation, show that if (a, b, c) satisfies

$$a^2b^2 - a^2 - b^2 = c^2$$

and $c = 0$, then $a = b = 0$.

Hint: What are the divisors of 1*?*

vi) Argue by infinite descent that no non-zero integer solution to

$$a^2b^2 - a^2 - b^2 = c^2$$

exists.

Hint: Let $a = 2r$*,* $b = 2s$*,* $c = 2t$*. What equation must* (r, s, t) *satisfy? What does that tell us about the parity of* r*,* s*, and* t*?*

vii) Hence conclude that no non-zero rational solution to

$$x^2 + y^2 + z^2 = 2xyz$$

exists.

Solution 8

i) As we saw in question 1, if one of x, y, z is zero, then they must all be 0. If one or three of them are negative, then $2xyz < 0$, while $x^2 + y^2 + z^2 > 0$, so we cannot have any such solutions. If two of them are negative, without loss of generality y and z, then $(x, -y, -z)$ is a positive integer solution, which cannot exist. Hence, there are no non-zero solutions.

ii) Considering

$$x^2 + y^2 + z^2 = 2xyz$$

as a quadratic equation in z, we find that

$$z = xy \pm \sqrt{x^2y^2 - x^2 - y^2}$$

via the standard formula. If

$$x^2y^2 - x^2 - y^2 = r^2$$

for a rational number r, we have that $z = xy \pm r \in \mathbb{Q}$ is rational and so we obtain a rational solution. Conversely, if $x, y, z \in \mathbb{Q}$, we have that

$$x^2y^2 - x^2 - y^2 = (z - xy)^2 = r^2$$

for a rational number $r = z - xy$.

iii) Suppose we have a triple of integers (a, b, c) such that

$$a^2b^2 - a^2 - b^2 = c^2$$

Then (a, b, c) is a triple of rational numbers satisfying the same equation. Conversely, if we have $(x, y, r) \in \mathbb{Q}^3$, such that

$$x^2y^2 - x^2 - y^2 = r^2,$$

then taking a common denominator and writing $(x, y, r) = (\frac{a}{n}, \frac{b}{n}, \frac{q}{n})$, we see that

$$\frac{a^2b^2}{n^4} - \frac{a^2}{n^2} - \frac{b^2}{n^2} = \frac{q^2}{n^2}$$

and so

$$a^2b^2 - a^2 - b^2 = (nq)^2 = c^2$$

for $c = nq$, giving a triple of integers satisfying the equation.

iv) The equation is equivalent to

$$(a^2 - 1)(b^2 - 1) - 1 \equiv c^2.$$

Considering this mod 4, we see that if a or b is odd, the left hand side will be congruent to $-1 \pmod 4$, which is not a square modulo 4, so there can be no solutions. If a is odd, then

$$(a^2 - 1)(b^2 - 1) - 1 \equiv (1 - 1)(b^2 - 1) - 1 \equiv -1 \pmod 4,$$

and similarly for b odd. Thus, a and b must be even. Then

$$(a^2 - 1)(b^2 - 1) - 1 \equiv (-1)^2 - 1 \equiv 0 \pmod 4$$

and so c must also be even.

v) If a rational solution to

$$x^2 + y^2 + z^2 = 2xyz$$

exists, then an integer solution to

$$a^2b^2 - a^2 - b^2 = c^2$$

exists. Without loss of generality, we can assume $a, b, c \geq 0$. Suppose we have a solution with $c > 0$. We must have that a, b, c are all even, and so there exist non-negative integers r, s, t such that $t > 0$ and

$$a = 2r, \quad b = 2s, \quad c = 2t.$$

We can quickly check that (r, s, t) satisfy

$$4r^2s^2 - r^2 - s^2 = t^2.$$

Considering this modulo 4, we see that we must have that all of r, s, and t are even. Defining $r_2 = \frac{r}{2}$, $s_2 = \frac{s}{2}$, $t_2 = \frac{t}{2}$, we see that (r_2, s_2, t_2) satisfies

$$4^2r_2^2s_2^2 - r_2^2 - s_2^2 = t_2^2.$$

More generally, given an integer solution (r_k, s_k, t_k) with $t_k > 0$ to

$$4^kx^2y^2 - x^2 - y^2 = z^2$$

we must have that r_k, s_k, t_k are all even, and hence we get an integer solution

$$(r_{k+1}, s_{k+1}, t_{k+1}) = (\frac{r_k}{2}, \frac{s_k}{2}, \frac{t_k}{2}$$

to

$$4^{k+1}x^2y^2 - x^2 - y^2 = z^2$$

satisfying $0 < t_{k+1} < t_k$. Thus, given an integer solution (a, b, c) to

$$x^2y^2 - x^2 - y^2 = z^2$$

with $c > 0$, we construct an infinite decreasing sequence of positive integers

$$c > t_1 > t_2 > \cdots > 0$$

which is impossible. Thus, any triple (a, b, c) such that

$$a^2b^2 - a^2 - b^2 = c^2$$

must have $c = 0$ and hence $a = b = 0$.

vi) If a non-zero rational solution to

$$x^2 + y^2 + z^2 = 2xyz$$

exists, writing

$$(x, y, r) = (\frac{a}{n}, \frac{b}{n}, \frac{q}{n})$$

we find that $(a, b, c = qn)$ is a non-zero integer solution to

$$a^2b^2 - a^2 - b^2 = c^2$$

which cannot exist. Therefore, no non-zero rational solutions to our original equation exist.