Diophantine Equations

Hugo Berg, Joakim Colpier, Lycka Drakengren, Kevin Haagensen Strömberg, Yuanqi Peng

Hvitfeldtska gymnasiet, Göteborg

June 7, 2020

Contents

1 Introduction

Diophantine equations are algebraic equations where we only seek the integer solutions. We might wish for a purely algebraic approach for solving these equations in general. That however is usually hard, for most Diophantine equations will require the use of number theory to be solved. Some tricks will be shown here, but as always the best teacher is you. Make sure to practice solving lots of problems.

Linear Diophantine equations will not be presented here, although they are the most fundamental type of Diophantine equations and are helpful in understanding modular arithmetic. The reader might be interested in reading the article about linear Diophantine equations on Brilliant Math & Science Wiki.[1]

2 Finding a Factorization

The word factorization denotes the writing of an expression as a product of two other expressions (two factors of the original expression, hence the name). For example, 6 can be factored as $2 \cdot 3$, and $x^2 + x$ as $x(x + 1)$. The *Fundamental Theorem of Arithmetic* states that every integer greater than 1 is either a prime or can be factored as a product of prime numbers in a unique way. As a result of the theorem, knowing the factorization of an expression provides a way of solving Diophantine equations. In a Diophantine equation, if we have a factored expression on one side and an integer on the other side, we can due to the *Fundamental Theorem of Arithmetic* determine all possible values of the factors by looking at the prime factorization of the integer. We will demonstrate how it works in later examples.

We will start by refreshing the reader's memory and giving some new useful identities to know. We encourage you to ascertain their validity by trying them out by yourself.

$$x^2 \pm 2xy + y^2 = (x \pm y)^2 \tag{1}$$

$$x^2 - y^2 = (x + y)(x - y) \tag{2}$$

$$x^3 \pm y^3 = (x \pm y)(x^2 \mp xy + y^2) \tag{3}$$

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - yz - xz) \tag{4}$$

Knowing these formulas can prove a useful skill, as they are very common and their simplicity makes them easy to handle.

Example 2.1. *For what integers a and b does the equality $a^2 - 4ab = -4b^2 + 9$ hold?*

[1] Linear Diophantine Equations (n.d.). On *Brilliant Math & Science Wiki.* Accessible at: `https://brilliant.org/wiki/linear-diophantine-equations-one-equation/`

Solution. From identity (1), we can see that $(x-y)^2 = x^2 - 2xy + y^2$. Also, we know that $a^2 - 4ab = -4b^2 + 9$ is equivalent to $a^2 - 2a(2b) + (2b)^2 = 9$, and can therefore conclude that $(a-2b)^2 = 9$. The number 9 can be factored as $9 \cdot 1$, $3 \cdot 3$, $(-9) \cdot (-1)$ and $(-3) \cdot (-3)$. Because the left side of the equation is the product of two identical integers $(a-2b)$, we can conclude that $a - 2b = \pm 3$, giving us $a = \pm 3 + 2b$. □

It is also worth noting that if a product of two factors is equal to the n:th power of an integer, and the factors have no common divisor greater than 1, the factors are also n:th powers of some integers. That is to say, if x and y are co-prime integers and $xy = z^n$ where z and n are integers with $n \geq 0$, then $x = a^n$ and $y = b^n$ for some integers a and b.

This can be verified by looking at the individual prime divisors of z, which occur in multiples of n. Since they cannot be split up between two co-prime factors, the prime power is either a factor in x or in y. As a result, both x and y will consist of prime factors with powers being multiples of n, which means that x and y in turn are n:th powers.

Remark. Two integers are said to be *relatively prime* (or *co-prime*) if their greatest common divisor is 1. The numbers (a, b, c) are *pairwise relatively prime* if (a, b), (b, c) and (c, a) are all pairs of relatively prime integers.

Example 2.2. *(Baltic Way 1995) The positive integers a, b, c are pairwise relatively prime, a and c are odd and the numbers satisfy the equation $a^2 + b^2 = c^2$. Prove that $b + c$ is a square of an integer.*

Solution. We can rewrite the equation in a more convenient form as $a^2 = c^2 - b^2$. Factoring the right hand side using identity (2) yields $a^2 = (c+b)(c-b)$. As previously explained, it is sufficient to prove that $b + c$ and $c - b$ are relatively prime for $b + c$ and $c - b$ to be squares. Let us assume the opposite, that $b + c$ and $c - b$ share a divisor $d > 1$. Let $b + c = dx$ and $c - b = dy$, where x and y are integers. Adding the equations together gives $2c = d(x + y)$, and subtracting them yields $2b = d(x - y)$. This means that either d divides both b and c, or 2 divides d. We can exclude the first case since b and c are relatively prime. If d were even, b and c would have had the same parity, which would in turn imply that a is even, which would be a contradiction. This means that we can exclude the second case as well. Hence $c + b$ and $c - b$ must be relatively prime, meaning that $b + c$ is the square of an integer (which is also true for $c - b$), which was to be proven. □

While an expression might remind you of a certain factorization, it might not always be possible to directly factorize it. In that case, it is often useful to add a term to make the factorization possible. A common strategy is to add an integer to both sides of a Diophantine equation, ending up with a factorizable expression on one side and an expression from which you can determine the factors on the other side.

Example 2.3 (Pythagoras Enigma 2019)**.** *Find all integer solutions to the equation $x^3 + y^3 - 3xy = 3$.*

Solution. Trying to immediately factor the expression in the left hand side will not lead to much progress. Nevertheless, the expression closely resembles the left hand side of identity (4), where z is replaced by 1. Comparing the expressions $x^3 + y^3 - 3xy$ and $x^3 + y^3 + z^3 - 3xyz$ where $z = 1$, we see that they only differ by the number 1. Therefore, we can add 1 to both sides of the equation $x^3 + y^3 - 3xy = 3$ to make the left hand side factorizable. Consequently, using identity (4), the obtained equation $x^3 + y^3 + 1 - 3xy = 4$ can be rewritten as

$$(x + y + 1)(x^2 + y^2 + 1 - xy - x - y) = 4. \tag{5}$$

There are six possible ways to split up the number 4 between the two factors, namely $(x+y+1, x^2+y^2+1-xy-x-y) = (1, 4)$, $(4, 1)$, $(2, 2)$, $(-1, -4)$, $(-4, -1)$ or $(-2, -2)$. For the first factor of the left hand side in equation (5) to be even, x and y must have different parity, making the second factor odd. Hence, we can exclude the alternatives $(2, 2)$ and $(-2, -2)$. The other alternatives, i.e. $(x + y + 1, x^2 + y^2 + 1 - xy - x - y) = (1, 4)$, $(4, 1)$, $(-1, -4)$ or $(-4, -1)$, lead to the systems of equations

$$\begin{cases} x + y = 0 \\ \quad xy = -1 \end{cases}, \quad \begin{cases} x + y = 3 \\ \quad xy = 2 \end{cases}, \quad \begin{cases} x + y = -2 \\ \ 3xy = 11 \end{cases}, \text{ and } \begin{cases} x + y = -5 \\ \ 3xy = 32 \end{cases},$$

respectively, which follows from rewriting the second factor as $(x + y)^2 + 1 - 3xy - (x + y)$. The two latter can be excluded, since 11 and 32 are not divisible by 3. The two first equations give, by substituting the upper equation into the lower, the solutions $(x, y) = (1, -1), (-1, 1), (1, 2)$ and $(2, 1)$. These are hence the integer solutions to the equation. □

2.1 Exercises for the reader

Exercise 2.1 (Baltic Way 2003). Let a and b be positive integers. Prove that if $a^3 + b^3$ is the square of an integer, then $a + b$ is not a product of two different prime numbers.

Exercise 2.2 (Baltic Way 1997). A rectangle can be divided into n equal squares. The same rectangle can also be divided into $n + 76$ equal squares. Find all possible values of n.

Exercise 2.3 (Skolornas matematiktävling 2009). Find all solutions in positive integers to the equation $\frac{1}{x} + \frac{1}{y} = \frac{1}{101}$.

3 Congruences

While often not containing many complicated terms or expressions, even quite normal-looking Diophantine equations can hide enormous amounts of complexity. Being able to reduce the mental complexity of some equation should therefore be very helpful, and as it turns out, using what is called modular arithmetic and congruences is one of the most powerful and fundamental tools at our disposal. The basic definition in this section is therefore the one of *congruence*.

Definition 3.1. Two integers a, b, are said to be congruent "modulo" another integer n if $n|a-b$, and we denote this by $a \equiv b \mod n$.

Remark. If (all mod some fixed positive integer n) $a \equiv a'$, and $b \equiv b'$ then $a+b \equiv a'+b'$ and $ab \equiv a'b'$. For example, since $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4 \equiv 0$, and $3^2 \equiv 9 \equiv 1 \mod 4$, this implies that integer squares can only be congruent to 0 or 1 $\mod 4$.

For instance, the 24-hour clock is an example of a system of integers mod 24. Another system you have used before is the fact that two odd numbers or two even numbers sum to an even number, and only the sum of one even and one odd number sum to an odd number; these are in fact statements about the integers mod 2.

We introduce below, an important and useful theorem in number theory and the study of Diophantine equations.

Theorem 3.1 (Fermat's little theorem). *Let p be a prime number, then for any integer a, we have*

$$a^p \equiv a \mod p$$

Moreover, if a is not divisible by p, we can get

$$a^{p-1} \equiv 1 \mod p$$

Example 3.1 (Baltic Way 2012). *Find all integer solutions a, b, c of*

$$a^2 + b^2 + c^2 = 20122012.$$

Solution. Let us first factorize the RHS. We immediately see that

$$20122012 = 10001 \cdot 2012 = 10001 \cdot 4 \cdot 503,$$

and we consider the equation $\mod 8$. As $10001 = 8 \cdot 1250 + 1$ and $503 = 480 + 23 = 8 \cdot 62 + 7$, we have that

$$20122012 \equiv 4 \cdot 7 \equiv 4 \mod 8.$$

Let us explore what n^2 can be congruent to $\mod 8$. As we can see from the table, since our sum of integer squares is congruent to 4 $\mod 8$, the only possible combinations of congruences for (a^2, b^2, c^2) are $(0,0,4)$ and $(4,4,4)$ (in any permutation). Thus the integers a, b, c, can only be even. Now let $a = 2 \cdot a'$, $b = 2 \cdot b'$, $c = 2 \cdot c'$ and we get

$n \mod 8$	0	1	2	3	4	5	6	7
$n^2 \mod 8$	0	1	4	1	0	1	4	1

$$4({a'}^2 + {b'}^2 + {c'}^2) = 20122012 = 4 \cdot 503 \cdot 10001,$$

which in turn gives

$$a'^2 + b'^2 + c'^2 = 503 \cdot 10001.$$

Now we combine the fact that $503 \cdot 10001 \equiv 7 \mod 8$ and look at our table once again, noting that no sum of three squares is congruent to $7 \mod 8$, and so no solutions to our original equation can exist. □

Example 3.2 (Andreescu et al.[2], 2010, p.224, modified). *Prove that the equation $8xy - x - y = 2z^4$ has no solution in positive integers.*

Solution. Assume there exists a positive integer solution. Multiplying by 8 and adding 1 gives us the equation $(8x-1)(8y-1) = 16z^4 + 1$. Suppose p is a prime divisor of $8x - 1$. Then p is also a divisor of $16z^4 + 1$, thus

$$16z^4 = (4z^2)^2 \equiv -1 \mod p.$$

Since p is not a divisor of z, Fermat's Little Theorem shows that $(4z^2)^{p-1} \equiv 1 \mod p$. We also know that p is odd, so

$$((4z^2)^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \equiv 1 \mod p$$

and $\frac{p-1}{2}$ must be even. As a result, $p \equiv 1 \mod 4$. Looking at the prime factorization of $8x - 1$, we can see that all factors are congruent to $1 \mod 4$, meaning that their product (i.e. $8x - 1$) is also congruent to $1 \mod 4$.

However, $8x - 1 \equiv -1 \mod 4$, which leads to a contradiction. This means that there are no solutions in positive integers to the equation. □

3.1 Exercises for the reader

Exercise 3.1 (Baltic Way 2016). For which integers n=1, 2 . . . 6 does the equation

$$a^n + b^n = c^n + n,$$

have a solution in integers?

Exercise 3.2 (USAMO 1979). Determine all non-negative integer solutions, apart from permutations, of the equation

$$n_1^4 + n_2^4 + n_3^4 + \ldots + n_{15}^4 = 1599.$$

Exercise 3.3 (AwesomeMath 2007). Find all non-negative integer solutions (a, b, c) of

$$4ab - a - b = c^2.$$

4 Inequalities

Discovering bounds on variables and expressions can be very useful in Diophantine equations since we don not have a continuous span of solutions but rather single points on the numberline. That means we easily can remove large quantities and get finitely many possibilities that can be tested in cases. We present three useful techniques for this endeavor.

[2] Andreescu et al. (2010). *Introduction to Diophantine Equations* Berlin: Springer

4.1 Creating extra equations

A common technique is to use the fact that squares of real numbers, and hence integers, are non-negative. We can with this technique limit the number of options for some variable and get a finite number of possible values. This works with $|x|$ or any other function that has a lower bound on its range.

Example 4.1. *Find all integral solutions to the following system of equations.*

$$\begin{cases} x+y+z=60, \\ (x-4y)^2+(y-2z)^2=2 \end{cases}$$

Solution. The integer squares in the second equation must be both 1 for their sum to be 2, since both squares are integers greater than or equal to zero. That gives:

$$\begin{cases} x=4y\pm 1 \\ y=2z\pm 1 \end{cases}.$$

We have reduced all infinitely many values to two possibilities for $x-4y$ and two for $y-2z$, which is four combinations in total. Now, if we express x and z in terms of y, we get when we plug into the first equation:

$$4y\pm 1+y+\frac{y}{2}\pm\frac{1}{2}=60,$$

which gives

$$11y\pm 2\pm 1=120.$$

Here the only way for $120\pm1\pm2$ to be a multiple of 11 is if $11y=120+2-1$ or $y=11$. Using our plus and minus choices we get $x=4\cdot 11-1=43$ and $11=2\cdot z-1$ which gives $z=6$. This solves the original equations, so we arrive at our answer of

$$x=43,\ y=11,\ z=6.$$

□

4.2 Using symmetry

Using symmetry is another useful technique which often allows us to eliminate one variable at once. We order the variables in the equation to use properties of the smallest or largest one.

Example 4.2 (Andreescu et al., 2010, p.14)**.** *Solve $\frac{1}{x}+\frac{1}{y}+\frac{1}{z}=\frac{3}{5}$ in positive integers.*

Solution. Without loss of generality let $x\leq y\leq z$ (sometimes we cannot order the variables and instead we can only choose which of the variables will be the smallest or largest one). This gives $\frac{3}{x} \geq \frac{3}{5}$ which gives $x \in \{1, 2, 3, 4, 5\}$. We can eliminate $x = 1$ since it is too large.

If $x = 2$ we get $\frac{1}{y} + \frac{1}{z} = \frac{1}{10} \rightarrow y = 10 + \frac{100}{z-10}$ so $z - 10|100$. Restricting ourselves to a finite amount of values for y and z, the solutions are easily found: $(2, 11, 110), (2, 12, 60), (2, 14, 35), (2, 15, 30), (2, 20, 20)$. Remember that the permutations of these solutions also work. The rest of the cases are left as an exercise to the reader. □

4.3 Minimization

Minimization is a technique taking advantage of the fact that, given some solutions in positive integers to an equation, one of them is the smallest one. Using this, we can disprove the existence of solutions through a proof by contradiction. We start by assuming that a solution to an equation exists. If that leads us to the existence of an infinite strictly decreasing sequence of positive integer solutions, we have arrived at a contradiction. In turn, we can deduce that there are no positive integer solutions to the equation. Of course, we will need to define what the smallest solution is for equations involving more than one variable. We can for instance do this by looking at the sum of the variables. For example: if (x, y) and (p, q) are solutions, then (x, y) is smaller than (p, q) if $x + y < p + q$.

Example 4.3 (Andreescu et al., 2010, p.49)**.** *Solve $x^3 + 2y^3 = 4z^3$ in positive integers.*

Solution. Let (a, b, c) be a solution minimized for $x+y+z$. In other words there is no solution (p, r, q) such that $p + r + q < a + b + c$. Because we seek positive values such a solution must exist. Notice that $a^3 = 4c^3 - 2b^3 = 2(2c^3 - b^3)$, or in other words a^3 and thus a is even. Letting $a = 2k$ where k is a positive integer gives

$$8k^3 + 2b^3 = 4c^3 \longrightarrow 4k^3 + b^3 = 2c^3 \longrightarrow b^3 = 2(c^3 - 2k^3),$$

so b is also even. Let $b = 2m$ where m is a positive integer.

From this we get

$$4m^3 = c^3 - 2k^3 \longrightarrow c^3 = 4m^3 + 2k^3 = 2(2m^3 + k^3),$$

so c is also even, and letting $c = 2n$, where n is a positive integer, gives another solution $x = k, y = m, z = n$ to the initial equation.

This means that our original solution is not minimized for $x + y + z$ since $k + m + n < a + b + c$, which is a contradiction, and thus no solutions exist. □

4.4 Exercises for the reader

Exercise 4.1. Prove that no solutions in integers exist for the equation $\frac{a}{b} = \sqrt{p}$ where p is a prime number.

Exercise 4.2. Finish all the cases in **Example 4.2**.

Exercise 4.3. Find all integer solutions to the equation $\sqrt{a} + \sqrt{b} = \sqrt{14}$.

5 Pythagorean Triples

You have probably encountered the equation $x^2+y^2=z^2$ from the *Pythagorean Theorem*, describing the relation between the side lengths x, y, z of a right angled triangle. If the side lengths are all positive integers, they form a so called *Pythagorean triple.* For instance, $(x, y, z) = (3, 4, 5)$ is a Pythagorean triple, and $(5, 12, 13)$ is another. Note that if we multiply the side lengths of a Pythagorean triangle with a positive factor k, the triangle still remains right angled since we have only scaled it. Hence, if (x, y, z) is a Pythagorean triple, all triples (kx, ky, kz), where k is a positive integer, are also Pythagorean. If we could find all Pythagorean triples (x, y, z) with x, y, z pairwise co-prime, we would know all positive integer solutions to the equation $x^2+y^2=z^2$ (indeed, two of the numbers x, y, z cannot share a common factor which is not a divisor in the third, a consequence of the condition $x^2+y^2=z^2$). Such triples are called *primitive Pythagorean triples.* As we can see in the following theorem, they are infinitely many.

Theorem 5.1. *Every primitive Pythagorean triple (x, y, z) with y even can be expressed in the form $x = m^2 - n^2$, $y = 2mn$, $z = m^2 + n^2$, where m and n are relatively prime integers of different parity with $m > n > 0$.*

Proof. Firstly, we can easily check that these indeed form a primitive Pythagorean triple. We have that $x^2 + y^2 = (m^2 - n^2)^2 + 4m^2n^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = z^2$. Also, any prime divisor of y (except 2) is a divisor of m or n, and hence not in $m^2 \pm n^2$ since it would then divide both m and n. A common prime divisor of x and z would divide both their sum and their difference, i.e. $2m^2$ and $2n^2$, and therefore also m and n (if not 2) which is not possible since m and n are co-prime. Neither do any pair of the numbers x, y, z share the factor 2, since if m and n have different parity, x and z are both odd. Hence, x, y, z are pairwise relatively prime. They are also positive integers due to the fact that $m > n > 0$.

We must also prove that there are no other primitive Pythagorean triples. Any primitive Pythagorean triple (x, y, z) satisfies $x^2 + y^2 = z^2$, where x, y, z are pairwise relatively prime. If both x and y were odd, we would have had z even and the right hand side divisible by 4. Since the square of an odd integer $2k + 1$ can be written as $4k^2 + 4k + 1$, which is congruent to 1 modulo 4 (see Section 3), the sum of two odd squares is therefore congruent to 2 modulo 4 and the left hand side can therefore not be divisible by 4. We can therefore assume that y is even, while x and z are odd.

Replacing a, b, c in Example 2.2 by (x, y, z), we can deduce that $y + z$ and $z - y$ are squares of integers. Write $y + z = s^2$ and $z - y = t^2$, where s and t are integers. Since y and z have different parity, s and t are odd, which means $s + t$ and $s - t$ are even. Hence, $s + t = 2m$ and $s - t = 2n$ for integers m and n. Since x, y and z are positive and $x^2 + y^2 = z^2$, z must be greater than y which makes s and t non-zero. Hence, we can assume s and t are positive. Also $s^2 - t^2 = 2z > 0$, so s is greater than t. This means that m and n also are positive integers. They are of different parity since otherwise $m + n$ is even and therefore $2(m+n)$ divisible by 4, making $(s+t)+(s-t)=2s$ divisible by 4 and s even, a contradiction. They are also relatively prime, since a common divisor of m and n divides both their sum and their difference, hence s and t, which are relatively prime. This again leads to a contradiction. Finally, $m > n$ since $2m = s+t > s-t = 2n$. Solving for s and t, we get $s = m+n$ and $t = m-n$, yielding $y+z=(m+n)^2$ and $z-y=(m-n)^2$. Solving for y and z, $y = 2mn$ and $z = m^2+n^2$. It follows that $x = \sqrt{z^2-y^2} = m^2-n^2$, and the proof is finished. $\square$

These convenient formulas for primitive Pythagorean triples provide a way for us to handle the condition $x^2+y^2=z^2$ in Diophantine equations.

Example 5.1. *Show that the equation $a^4+b^4=c^2$ has no solution in positive integers.*

Solution. We will assume there exist such solutions, and try to arrive at a contradiction. If a solution (a,b,c) exists, the numbers $x=a^2$, $y=b^2$ and $z=c$ satisfy the Pythagorean equation $x^2+y^2=z^2$. Common prime factors of any pair of the numbers (a,b,c) will be factors of the third as well. Noting that the exponent of the prime factors must be multiples of 4 in both sides of the equation, we can cancel them out without changing the equation. Hence, we can assume that a^2, b^2 and c are co-prime, thus forming a primitive Pythagorean triple. We can further assume that (a,b,c) is the solution with the smallest value of c.

We can without loss of generality assume that b^2 is even and write $a^2 = m^2-n^2$, $b^2=2mn$ and $c=m^2+n^2$ with m, n being co-prime integers of different parity, and $m>n>0$. Now, we directly see that (a,n,m) also form a primitive Pythagorean triple, since m and n are co-prime and can therefore not share a divisor with a for the Pythagorean equation to hold. This means we can again use the parametrization of primitive Pythagorean triples and write, since a is odd, $a=s^2-t^2$, $n=2st$ and $m=s^2+t^2$ with s, t being co-prime integers of different parity and $s>t>0$. Now, since $n=2st$, we have $b^2=2mn=4stm$. Since s, t are co-prime, the equation $m=s^2+t^2$ implies that s, t and m are pairwise relatively prime. This means that s, t and m all must be squares of positive integers for their product to equal $b^2/4$, which is a square (see Section 1).

We will hence write $s=u^2$, $t=v^2$ and $m=w^2$, where u, v and w are positive integers, pairwise co-prime. We can therefore rewrite the equation $m=s^2+t^2$ as $u^4+v^4=w^2$. We have thus obtained another solution to the initial equation, namely (u,v,w), where u, v and w are pairwise relatively prime. Since $c=m^2+n^2=w^4+n^2$ is strictly greater than w^4, which is in turn greater than or equal to w, we obtain the inequality $w<c$, contradicting the fact that c is minimal. Hence, there are no solutions in positive integers to the equation $a^4+b^4=c^2$ (See Section 4.3). $\square$

5.1 Exercises for the reader

Exercise 5.1. Find all solutions in positive integers to the system of equations

$$\begin{cases} a^2 + b^2 = c^2 \\ b^2 + c^2 = d^2 \end{cases}.$$