Diophantine Equations: A Guide

Daniel Liu

June 29, 2021

Introduction

When we think of the word *equation*, we often think of quadratics and polynomials where the solutions are complex expressions involving square roots and i. However, diophantine equations completely revise the above connotations that associate with the equal sign: they only involve integer solutions. This means that when looking at a diophantine equation, for example $x + y = 1$, would not be part of the solution set. In this guide, we will explore how to solve diophantine equations, their general solution forms, and their applications in the field of number theory.

Solving 2-Variable Diophantine Equations

Consider the equation $20x + 21y = 2021$. Typically when solving, we would simply set y equal to $\frac{2021 - 20x}{21}$ and graph the equation on a Cartesian plane. However, things get interesting when we only think about the *integer* solutions.

Geometrically speaking, the solution set would look like a group of individual, collinear points on a graph that can all be represented by integer coordinates. In fact, there are an infinite number of said points, and thus an infinite number of solutions.

Remark: A diophantine equation has an infinite number of solutions.

Now that we understand what a typical set of solutions to a 2-variable diophantine equation would look like, we get right into solving them.

The general protocols that one follows when solving these equations using the format $ax + by = c$ are:

1. Set $ax + by = 1$.
2. Find an integer pair (x, y) that satisfies the above equation.
3. Turn the equation into $ax + by = c$ by multiplying x and y by c.
4. Use the above solution pair to find a general form for the equation's solutions.

Needless to say, the four steps detailed above make very little sense without application. We will now look at some examples to develop better intuition for diophantine equations.

Example 1.1: Solve the diophantine equation $x + y = 1$.

We start off with an easy equation; step one of the above procedure has already been satisfied. Now, as per step 2, we find one solution. It is fairly obvious that we have a solution at $x = 1$ and $y = 0$. But is this the only solution?

There's no need to worry about step 3 since $(1, 0)$ is already a solution to the original equation (more on that in later problems). Looking at step 4, we are asked to find a *general form* for *all solutions* of the equation, meaning that the equation has more than one solution (an infinite amount to be exact, as noted previously).

So what's another solution? Playing around with numbers a bit, we come to the conclusion that $(2, -1)$ is also a solution. What about $(3, -2)$? Plugging the numbers in, we see that it is indeed valid. Now some may see a pattern at this point; can you name it?

The pattern here is that each new solution can be found by adding 1 to the x value and subtracting 1 from the y value of the preceding solution pair. Hence, we have $(2, -1)$ derived from adding 1 to 1 and subtracting 1 from 0 in the solution pair $(1, 0)$.

Thus far, we've exhibited this pattern for positive x-values. Naturally, this raises the question- does this pattern work for negative x-values as well? Well let's test some values.

Remark: When unsure if a pattern holds under particular conditions, it is always a good idea to make sure by testing values.

We find a "base case" involving a negative x-value to build off of by guess and check. $(-1, 2)$ is the solution pair with the largest x-value that is still negative, so we can use it as our base.

Applying our previously found rule of adding 1 to the x-value and subtracting 1 from the y-value, we can quickly see that x simply gets larger and larger until it becomes positive. Clearly, the above rule is quite useless. Does this mean the pattern we found is invalid for all negative x? Not necessarily.

If you've been reading closely, you may have already found the problem with our rule: It was formed under the pretense that x gets bigger and bigger and that y gets smaller and smaller. Therefore, we cannot use it to verify a case in which x is set to continuously decrease.

How can we transform it to encompass the fact that x decreases from our base case? One idea is to reverse our rule; that is, instead of having x increase by 1 and y decreases by 1 each time, we have x *decrease* by 1 and y *increase* by 1.

Does it work? Well the best thing to do here is to test cases. We started off with $(-1, 2)$. Now, we test $(-2, 3)$. Plugging these values in, it is easy to see that the original equation holds. What about $(-3, 4)$? Again, it works. From here, further testing of values shows that this new rule over the domain of negative integers holds.

We've found a pattern now -two actually- for both positive and negative integers. Back to step 4; how do we write these patterns algebraically? More importantly, how do we summarize them as *one* form? For now, let's just worry about the first pattern. It can be summarized as $(1 + n, 0 - n)$. This is true because, instead of comparing the case at hand to the previous case, we can compare the case at hand to the base case itself. That is, instead of comparing $(3, -2)$ to $(2, -1)$, we compare $(3 - 2)$ to our base case $(1, 0)$. From here we see that each time some

integer n is added to the x value, that same integer n is subtracted from the y value. Now what about the negative case?

Here's the part where we are saved by a bout of clever algebra: $(1+n, 0-n)$ includes all solutions involving a negative x because n doesn't have to be positive. If n is negative, it would imply the exact same rule that our rule for negative x's establishes. Thus, we have found the solution to the diophantine equation $x + y = 1$.

Example 1.2: Solve the diophantine equation $5x + 2y = 13$.

Now that we have a better understanding of the basics of solving these equations, we jump right to a typical problem.

By step 1, we set $5x + 2y = 1$.

Following step 2, we guess and check to find a solution for this case to use it as our base; $(-1, 3)$ works.

From here, we multiply the solution pair by 13 to get $(-13, 39)$ as step 3 instructs. Before moving on, we check to see if it still satisfies the equation: $5(-13) + 2(39) = 13$. It is valid.

We now begin step 4. For ease of computation, we can refer to the equation $5x + 2y = 1$ to find solutions and multiply them by 13 to satisfy our original equation. Aside from $(-1, 3)$, $(-3, 8)$ works as well after some guess-and-check. But wait.

We notice the difference between the x-coordinates of the two solutions is -2, and the difference between the y-coordinates is 5. Is this a coincidence? Our intuition gained from the previous problem tells us it might not be. But let's test just to make sure.

$(-5, 13)$ seems to work. And so does $(-7, 18)$.

The pattern does hold. And as the previous problem told us, the pattern will continue to hold regardless of positive or negative x-values.

But what happens when we multiply everything by 13? When we multiply $(-1, 3)$ and $(-3, 8)$ by each by 13, the difference in x-coordinates is now -26 and the difference in y-coordinates is now 65.

So is this the new rule, differing by -26 and 65, or does the old rule of -2 and 5 still hold?

Let's investigate. Our original case is now $(-13, 39)$, and $(-3, 8)$ becomes $(-39, 104)$. To get to $(-39, 104)$, we now subtract 26 from the x-coordinate and add 65 to the y-coordinate. What if we simply subtract 2 from the x-coordinate and add 5 to the y -coordinate? We then end up with $(-15, 44)$. Turns out, this still works!

Thus we have a general solution now: $(-13 - 2n, 39 + 5n)$.

Exercise 1.1: Solve the diophantine equation $x + y = 5$.

Exercise 1.2: Solve the diophantine equation $2x + 3y = 9$.

Exercise 1.3: Solve the diophantine equation $2x + 6y = 28$.

A Simplification

By now, you may be wondering why solving diophantine equations can be so tedious. Although it only technically involves 4 steps, step 4 is long and computation-heavy; easy to make errors on. So then the question becomes, is there an easier way?

The answer comes in the form of a theorem:

If a and b are relatively prime and (x_0, y_0) is a base case of the equation, then the diophantine equation $ax + by = c$ is given by

$$(x_0 + bt, y_0 - at)$$

for some, not necessarily positive integer t.

The proof of this theorem is actually a relatively simple one: We simply need to prove that $ax_0 + by_0 = a(x_0 + bt) + b(y_0 - at)$. This is true because, since $ax_0 + by_0$ is already equal to c, we can set the two equal to each other to prove that $a(x_0 + bt) + b(y_0 - at)$ equals c as well. The remainder of this proof will not be fully detailed for the sake of brevity, but direct expansion and cancellation of terms on the right hand side can easily verify this.

Theorem Application

We now know a much simpler way to solve diophantine equations. However, our understanding of this concept is still reasonably shallow.

Example 2.1: Solve the diophantine equation $5x + 2y = 13$.

This example will be a continuation of example 1.2. This time, we will instead use the theorem to solve it.

As found in 1.2, our base case is $(-13, 39)$. Directly using our theorem and substituting in values, our general solution is $(-13 + 2n, 39 - 5n)$, which, because n can be positive or negative, is the same thing as $(-13 - 2n, 39 + 5n)$.

Needless to say, this theorem vastly simplifies our original 4-step process, though still retaining its structure.

Remark: This is a great example of how theorems can be useful, time-saving tools in mathematics.

Exercise 2.1: Solve the diophantine equation $x + y = 5$ (using the theorem).

Exercise 2.2: Solve the diophantine equation $2x + 3y = 9$ (using the theorem).

Exercise 2.3: Solve the diophantine equation $2x + 6y = 28$ (using the theorem).

Exercise 2.4: Two farmers agree that pigs are worth 300 dollars and that goats are worth 210 dollars. When one farmer owes the other money, he pays the debt in pigs or goats, with "change" received in the form of goats or pigs as necessary. (For example, a 390 dollar debt could be paid with two pigs, with one goat received in change.) What is the amount of the smallest positive debt that can be resolved in this way (2006 AMC 12A Problem 14).

A More Complex Method

Now what if, instead of an easy base case, we get something like $243x + 79y = 1$? We can't really guess-and-check our way out of this one.

The procedure for these "complex" diophantine equations is outlined as follows:

1. Create two separate equations, one involving (x, y), and another involving (x_0, y_0).
2. Solve the equations using algebra to obtain a general form with no explicit base solution.
3. Use the Euclidean algorithm to obtain a base solution.

As we have done previously, we will now use $243x + 79y = 1$ as an example to gain intuition on the 3-step process above.

Step one: creating two separate equations.

- $243x + 79y = 1$
- $243x_0 + 79y_0 = 1$

That's all there is to it.

Step two: solving the equations for a non-specified base solution.

Subtract the equations to obtain:

$$243(x - x_0) + 79(y - y_0) = 0$$

Move one term to the other side:

$$243(x - x_0) = -79(y - y_0)$$

Use algebraic manipulations on the right hand side:

$$243(x - x_0) = 79(y_0 - y)$$

From here, observe that, since 79 and 243 are relatively prime,

$243|y_0 - y$ and $79|x - x_0$

This implies that

$y = y_0 - 243p$ and $x = x_0 + 79q$

Thus, we have the solution $(x_0 + 79q, y_0 - 243p)$. But to complete the problem, we must find an x_0 and an y_0. This is where the hard part comes in.

We apply the Euclidean algorithm repeatedly to get:

$243 = 79 * 3 + 6$

$79 = 6 * 13 + 1$

But then we must reverse this process:

$1 = 79 - 6 * 13$

$= 79 - 13 * (243 - 79 * 3)$

$= 40 * 79 - 13 * 243$

Thus, the general form of the solution is $(-13 + 79q, 40 - 243p)$.

However, note that this problem is a particularly easy one due to the fact that the Euclidean algorithm portion was not very extensive. Other "complex" diophantine equations will have far more computation involved.

This way of solving diophantine equations can be confusing and tedious, and is generally not recommended unless guess-and-check is *completely* out of the question.

Exercise 1.1: Solve the diophantine equation $101x + 33y = 1$.

Exercise 1.2: Solve the diophantine equation $101x + 33y = 26$.