Diophantine equations essay sample

ASSIGN BUSTER

1. INTRODUCTION:

The mathematician Diophantus of Alexandria around 250A. D. started some kind of research on some equations involving more than one variables which would take only integer values. These equations are famously known as “ DIOPHANTINE EQUATION”, named due to Diophantus. The simplest type of Diophantine equations that we shall consider is the Linear Diophantine equations in two variables: ax+by= c, where a, b, c are integers and a, b are not both zero. We also have many kinds of Diophantine equations where our main goal is to find out its solutions in the set of integers. Interestingly we can see some good theoretical discussion in Euclid’s “ ELEMENTS” but no remark had been cited by Diophantus in his research works regarding this type of equations.

2. Whole Numbers:

In number theory, we are usually concerned with the properties of the integers, or whole numbers: Z = {. . . ,−3,−2,−1, 0, 1, 2, 3, . . .}. Let us begin with a very simple problem that should be familiar to anyone who has studied elementary algebra. • Suppose that dolls sell for 7 dollars each, and toy train sets sell for 18 dollars. A storesells 25 total dolls and train sets, and the total amount received is 208 dollars. How many of each were sold?

The standard solution is straight-forward: Let x be the number of dolls and y be the number of train sets. Then we have two equations and two unknowns:

x + y = 25

7x + 18y = 208

The equations above can be solved in many ways, but perhaps the easiest is

to note that the first one can be converted to: x = 25−y and then that value of x is substituted into the other equation and solved:

7(25 − y) + 18y = 208,

i. e. 175 − 7y + 18y = 208,

i. e.−7y + 18y = 208 − 175,

i. e. 11y = 33,

i. e. y = 3,

Then if we substitute y = 3 into either of the original equations, we obtain x = 22, and it is easy to check that those values satisfy the conditions in the original problem. Now let’s look at a more interesting problem:

• Suppose that dolls sell for 7 dollars each, and toy train sets sell for 18 dollars. A store sells only dolls and train sets, and the total amount received is 208 dollars. How many of each were theory

?

This time there is only one equation: 7x+18y = 208. We probably learned in algebra class that you need as many equations as unknowns to solve problems like this, so at first it seems hopeless, but there is one additional key piece of information: the number of dolls and the number of train sets must be non-negative whole numbers. With that in mind, let’s see what we can do, ignoring for the moment the fact that we already have a solution, namely: x = 22 and y = 3.

Again , the all other solutions will be of the form given below: X= 22+18c

Y= 3-7c , where c is any integer

If we want to have positive integral solutions then by an easy computation we observe that c= -1, 0, 1.

When an equation of this sort is solvable by this method, there is no limit to the number of steps that need to be taken to obtain the solution. In the example above, we needed to introduce integers a, b and c, but other equations might require more or fewer of these intermediate values.

3. Linear Diophantine Equations:

What we have just solved is known as a Diophantine equation – an equation whose roots are required to be integers. Probably the most famous Diophantine equation is the one representing Fermat's last theorem, finally proved hundreds of years after it was proposed by AndrewWiles:

If n > 2, there are no non-trivial1 solutions in integers to the equation: x n + y n = z n

There are many, many forms of Diophantine equations, but equations of the sort that we just solved are called " linear Diophantine equations": all the coefficients of the variables are integers. Let's look a little more closely at the equation we just solved: 7x + 18y = 208. If the only requirementwere that the roots be integers (not necessarily non-negative integers), then our solution: x = 22 + 18c and y = 3 − 7c represent an infinte set of solutions, where every different integer value of c generates another solution. A more geometric view of the problem is this: If we were to graph the equation 7x + 18y = 208, the solutions are places where the graph passes through points that have integer coordinates. In Figure 1 a portion of that line is plotted, and the points where the graph has integer coordinates are indicated and labeled. Figure 1: Graph of 7x + 18y = 208

Notice that all the points with integer coordinates are evenly spaced along the line. In fact, if we begin at any point and add 18 to the x-coordinate and at the same time subtract 7 from the y-coordinate, we arrive at another point on the graph with integer coordinates. A quick examination of the original equation should make it obvious why this is the case. The equation is:

$7x + 18y = 208.$

If we add 18 to the x value, we increase the left side by $7 \cdot 18$. If we subtract 7 from the y value, we decrease the left side by the same amount: $18 \cdot 7$. The net effect is to leave the left side unchanged.

Notice that this line has a negative slope and happens to cut through the first quadrant (quadrant I) and intersect some points with integer coordinates there. This may or may not be the case for the graphs of other linear Diophantine equations. Lines with positive slopes can have an infinite number of solutions where both are positive, and there are equations where there are none. It’s easy to construct such equations with whatever characteristics you wish.

Does every equation of the form:

$ax + by = c,$

where a, b and c are integers have a solution (x, y), where x and y are also integers? The answer is no. For example, what if a and b are even and c is odd? The left side must be even, and if the right side is odd, there is no possibility of a solution with integer values. Similarly, if a and b are both

multiples of 3 and c is not, the left side will be a multiple of 3 and the right side is not, so again, there are no possible integer solutions.

In fact, if the greatest common divisor (GCD) of a and b does not divide c, then there are no integer solutions. The amazing thing, however, is that if the GCD of a and b also divides c, then there are an infinite number of integer solutions, and we will see why that is the case later on.

Note also that another observation we made about our particular problem will also apply to a general linear Diophantine equation; namely, that if (x, y) is an integer solution to:

$ax + by = c$

then so will be $(x + bk, y - ak)$ where k is any integer. If we substitute $x + bk$ for x and $y - ak$ for y, we obtain:

$a(x + bk) + b(y - ak) = c$

$ax + abk + by - abk = c$

$ax + by = c,$

so if (x, y) is a solution, then so also is $(x + bk, y - ak)$. 4. Euclid’s Algorithm and Diophantine Equations:

Now let’s use the Euclidean algorithm on two of the numbers from the original Diophantine equation we solved in Section 1: $7x + 18y = 208$.

$18 = 7 \cdot 2 + 4$

$7 = 4 \cdot 1 + 3$

$4 = 3 \cdot 1 + 1$

$3 = 1 \cdot 3 + 0$

In this example, the final number is 1, so the GCD of 18 and 7 is 1 (in other

words, 18 and 7 are relatively prime), but the interesting thing to note is that the numbers in the GCD calculation: 18, 7, 4, 3, 1 are the same numbers that we got as denominators and as the coefficients of the variables in the numerators in the fractions when we were solving the Diophantine equation 7x + 18y = 208. The only oddball numbers were the constants in the numerators, and that’s not surprising: we never used the number 208 when we were using the Euclidean algorithm to find the GCD of 18 and 7. If you check the arithmetic calculations that are being done in each case, it will be clear why the numbers generated in both examples must be the same.

Suppose that the original Diophantine equation had had a 1 instead of the 208. To make sure you understand the technique we used to solve our Diophantine equation it would be a good exercise to solve the following equation by yourself before reading on: 7x + 18y = 1

The nice thing about the 1 in place of the 208 is that it remains constant throughout the calculation, whereas the 208 was reduced as various of the denominators divided it evenly. In this calculation, all the other coefficients are the same as the numbers generated in the straight-forward calculation of the GCD of 7 and 18. To complete the solution, we need to back-substitute the b = 1 − 3c and after a few steps we obtain: x = −5 + 18c and y = 2 − 7c, where c is an arbitrary integer. (Obviously this equation will have no solutions where both x and y are positive.) Thus when you do a GCD calculation of a and b, and that GCD turns out to be 1, you’ve done a lot of the work toward solving the Diophantine equation ax + by = 1.

So if we can do the Euclidean algorithm, we can find with almost no effort other than a little arithmetic the coefficients we need to solve a linear Diophantine equation of the form ax + by = 1. Of course we'd like to be able to solve equations where the 1 is replaced by an arbitrary number c, but that is actually not too difficult. As as example, let's find solutions for 7x + 18y = 208 assuming that we've solved 7x+ 18y = 1. The solutions for the latter equation are x = −5+18c and y = 2 −7c, where c is an arbitrary integer. An easy solution is simply to set c = 0 and obtain x = −5 and y = 2 as a particular solution. But if we multiply x and y by 208, then the left side will be increased by a factor of 208 so if we increase the right side by the same factor, we'll have an (x, y) pair that satisfies our original equation 7x + 18y = 208. Thus a solution is this: x = −5 · 208 = −1040 and y = 2 · 208 = 416. It's easy to plug these numbers in to check that they are valid.

But we also noticed that adding any multiple of 18 to x while at the same time adding that same multiple of −7 to y will yield the other solutions, so the general solution to our original problem is: x = −1040+18k and y = 416−7k. If k = 58, for example, this yields the solution x = 4 and y = 10.

We have seen that if we have any solution to one of these linear Diophantine equations, we can obtain all the others by adding constant multiples of the opposite coefficients to the given solution, all we really need is one solution.

In the previous examples, once we got to the point where we had b = 1−3c, we backsubstitutedand carefully kept track of the coefficient of c in the calculations. But since any solution will generate all the others, why not let c = 0? Then we just need to track a single number.

5. Putting It All Together:

Let’s use the techniques above, but in their most simplified form, to solve another Diophantine equation. So look at the problem stated below:

• In a pet shop, rats cost 5 dollars, guppies cost 3 dollars and crickets cost 10 cents. One hundred animals are sold, and the total receipts are 100 dollars. How many rats, guppies and crickets were sold?

If r, g and c represent the number of rats, guppies and crickets, respectively, we’ve got two equations (but three unknowns):

r + g + c = 100

5r + 3g + . 1c = 100

To turn the problem into a purely integer problem, multiply the second equation by 10: r + g + c = 100

50r + 30g + c = 1000

If we subtract the first equation from the second we obtain the familiar looking linear Diophantine equation in two variables:

49r + 29g = 900.

Luckily, the GCD for 49 and 29 is 1 which divides 900 so there will be solutions (although possibly not solutions where all the values are non-negative. (This problem is probably much easier to solve using “ guess and check” techniques: we know that the number of crickets must be a multiple of 10, so you could just try 0, 10, 20, …, 100 of them.), Let’s find the GCD of 49 and 29, using the Euclidean algorithm: 49 = 29 · 1 + 20

29 = 20 · 1 + 9

20 = 9 · 2 + 2

$9 = 2 \cdot 4 + 1$

$2 = 1 \cdot 2 + 0$

Thus we get two integers s & t such that 49s+29t= 1.

Then multiplying 900 to both the integers s&t would give a solution to the original problem.

NEXT WE SHALL PUT SOME LIGHT ON THE QUADRATIC DIOPHANTINE EQUATIONS LIKE AS:

1) (ax+by)(cx+dy)= e,

2) axy= bx+cy+d,

3) $ax^2 + by^2 = cx+dy+e$,

4) $ax^2 + by^2 = cz^2$

where a, b, c, d, e are all non-zero integers.

We can also have in our hand lots of Diophantine equations which can not be included in our discussion.

6. Quadratic Equations:

Next we will apply the Unique Factorization Theorem to the solution of the diophantine equation

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

in integers x, y, z are integers. Such triples of solutions are called Pythagorean triples. The most famous of these triples is of course (3, 4, 5). It is quite easy to give formulas for producing such triples: for example, take $x = 2mn$, $y = m^2 - n^2$

and z = m2 +n 2

(special cases were known to the Babylonians, the general case occurs in Euclid). It is less straightforward to verify that there are no other solutions (this was first done by the Arabs in the 10th century). Assume that (x, y, z) is a Pythagorean triple. If d divides two of these, it divides the third, and then (x/d, y/d, z/d) is another Pythagorean triple. We may therefore assume that x, y and z are pairwise coprime; such triples are called primitive. In particular, exactly one of them is even. Claim 1. The even integer must be one of x or y. In fact, if z is even, then x and y are odd. Writing x = 2X + 1, y = 2Y + 1 and z = 2Z, we find 4X 2

+ 4X + 4Y 2

+ 4Y + 2 = 4Z 2 : but the left hand side is not divisible by 4: contradiction. Exchanging x and y if necessary we may assume that x is even. Now we transfer the additive problem x 2 +y 2

= z 2

into a multiplicative one (if we are to

use unique factorization, we need products, not sums) by writing x 2 = z 2

−y 2

=

(z − y)(z + y).

Claim 2. gcd(z − y, z + y) = 2. In fact, put d = gcd(z − y, z + y). Then d divides z − y and z + y, hence their sum 2z and their difference 2y. Now gcd(2y, 2z) = 2 gcd(y, z) = 2, so d | 2; on the other hand, 2 | d since z − y and z + y are even since z and y are odd. Thus d = 2 as claimed. Some Properties:

1)Let a, b be two co- prime integers such that ab is a square. Then a and b are squares. 2) Let a, b be two positive integers with gcd(a, b) = d such that ab is a square. Then a/d and b/d are squares.

THEOREM: If (x, y, z) is a primitive Pythagorean triple with x even, then there exist co-prime integers m, n such that x = 2mn, y = m 2 − n 2

and

z = m2

+ n 2 .

Note that if y is even, then the general solution is given by x = m 2 − n 2 , y = 2mn and z = m2

+ n 2 . Moreover, if we drop the condition that the triples be primitive then the theorem continues to hold if we also drop the condition that the integers m, n be relatively prime.

Note that if y is even, then the general solution is given by x = m2 − n2, y = 2mn and z = m2 + n2. Moreover, if we drop the condition that the triples be primitive then the theorem continues to hold if we also drop the condition that the integers m, n be relatively prime.

Lagrange’s Trick

The same technique we used for solving x 2

+ y 2 = z 2

can be used to solve

equations of the type x 2

+ ay 2

= z 2 just write the equation in the form ay 2

=

(z − x)(z + x) and use unique factorization.

Equations like x 2 + y 2 = 2z 2

at first seem intractable using this approach

because we can’t produce a difference of squares. Lagrange, however, saw that in this case multiplication by 2 saves the day because (2z) 2 = 2×2

2

+ 2y 2

=

(x + y) 2

+ (x − y) 2 , hence (2z − x − y)(2z + x + y) = (x − y) 2 , and now the solution proceeds exactly as for Pythagorean triples.

Let us now show that we can do something similar for any equation of type

AX 2

+BY 2

= CZ 2

having at least one solution. First, multiplying through by

A shows that it is sufficient to consider equations X 2

+ aY 2 = bZ 2 . Assume

that (x, y, z) is a solution of this equation. Then

(bzZ) 2

= bz 2 X 2

+ abz 2 Y 2

= (x 2

+ ay 2)X2

+ (ax 2

+ a 2 y 2)Y 2

= (xX + ayY) 2 + a(yX − xY) 2 .

Thus a(yX − xY) 2 = (bzZ) 2

− (xX + ayY) 2

is a difference of squares, and we

can proceed as for Pythagoren triples. We have proved:

Theorem : If the equation ax 2

+ by 2

= cz 2

has a nontrivial solution

in integers, then this equation can be factored over the integers (possibly after multiplying through by a suitable integer).

Problem: Find out a rectangle with same area and perimeter, if exists.

Solution: Let a, b be the length and bredth of the rectangle, then we have by the following equation : 2(a+b)= ab

This is a Diophantine equation in a, b.

We can solve it by using Unique factorization property as follows: ab-2a-2b= 0,

i. e. a(b-2)-2(b-2)= 4,

i. e.(a-2)(b-2)= 4

implying that either a-2= 4, b-2= 1 or a-2= 1, b-2= 4 or a-2= 2, b-2= 2 i. e. either a= 6, b= 3 or a= 3, b= 6 or a= 4, b= 4.

Therefore we obtained two types of rectangles with the given property. Note that we can solve Diophantine equations using geometry, unique factorization property, inequalities and trial methods