CHAPTER III: ALGEBRAIC EQUATIONS

Section 1: Diophantine Equations

As we have already seen in previous sections, many times we wish to solve equations and restrict our solutions to the integers. For example, when we find the greatest common divisor of two integers and then wish to write it as a linear combination, we solve an equation of the form $ax + by = \gcd(a,b)$. In this case, we have always been able to find integral solutions. These equations are part of a general class of equations called *diophantine equations*. Their defining characteristic is that they only admit integer solutions. These equations are named for the renowned Greek mathematician Diophantus of Alexandria. Very little is known about the life of Diophantus, but what is known has been passed down through the years in a mathematical puzzle that forms, appropriately, a diophantine equation. It goes like this:

> Diophantus lived $\frac{1}{6}$ of his life in childhood, $\frac{1}{12}$ in youth, and $\frac{1}{7}$ more as a bachelor. Five years after his marriage was born a son who died 4 years before his father and at half his father's final age.

Exercise 3.1.1 Find the linear equation described by the above puzzle, and solve it to find out how long Diophantus lived.

There are many different types of diophantine equations. Perhaps the most famous of all is $x^n + y^n = z^n$. In 1621, Pierre Fermat was reading about the equation $x^2 + y^2 = z^2$ in his copy of Diophantus' *Arithmetica*. In the margin he stated that $x^n + y^n = z^n$ has no integral solutions for $n > 2$. He claimed he had a proof but the margin he was writing in wasn't large enough to contain it. Since he died before he could ever prove this statement, it became known as ***Fermat's Last Theorem***. It is unlikely that he actually had such a proof. The theorem has since been proven true, but it took 375 years and the work of the greatest mathematical minds of the last four centuries.

We will focus most of our attention on *linear* diophantine equations, however before we do I would like to expose you to some rather interesting diophantine problems. In 1738, Euler showed that $x^2 - y^3 = 1$ has only one solution. It is also true that $x^3 - y^2 = 2$ has a unique solution. In 1932, Atle Selberg (of Prime Number Theorem fame) showed that $x^4 - y^3 = 1$ has no solutions. Finally, it has been shown that $1 + 2 + \ldots + n = 1^2 + 2^2 + \ldots + k^2$ has only four solutions. The most difficult of the four solutions is $n = 645$ and $k = 85$.

Exercise 3.1.2 Find the unique solutions to $x^2 - y^3 = 1$ and $x^3 - y^2 = 2$ and the three other solutions to $1 + 2 + \ldots + n = 1^2 + 2^2 + \ldots + k^2$.

The most common (and simplest) diophantine equations are of the form $ax + by = c$. These are the type we have already seen and we will generalize this in our present section.

Equations of this type can have no solutions (e.g. $2x+8y=111$) or many solutions (e.g. $2x+y=1$). So clearly, an interesting question is whether a given diophantine equation has solutions at all. The answer is surprisingly simple.

Theorem 3.1.3 Let $d=\gcd(a,b)$. The linear diophantine equation $ax+by=c$ has a solution in the integers if and only if $d \mid c$.

Proof: First suppose that $ax+by=c$ has a solution, say x_0, y_0 in the integers. Since $d=\gcd(a,b)$, there exists integers r and s such that $a=rd$ and $b=sd$. Then we have

$$c=ax_0+by_0=rdx_0+sdy_0=d(rx_0+sy_0),$$

so we see that $d \mid c$.

Conversely, suppose that $d \mid c$. This means there exists an integer t such that $c=td$. Now, we know from Theorem 1.2.3 of our notes that the equation $ax+by=d$ has a solution, call it x_0, y_0. Then clearly,

$$a(tx_0)+b(ty_0)=tax_0+tby_0=t(ax_0+by_0)=td=c$$

and the equation $ax+by=c$ has a solution as well. ■

Once we know we have solutions, how do we find them all? The answer follows the next two lemmas, which we will need for the proof.

Lemma 3.1.4 If $d=\gcd(a,b)$, then $\gcd(a/d, b/d)=1$.

Proof: Note that although a/d and b/d appear as fractions, they are both integers (since d is a divisor of both a and b). Now, from Theorem 1.2.3 again, we know there is a solution to the equation $ax+by=d$. Let's say $ax_0+by_0=d$ is that solution. Dividing by d, we get $(a/d)x_0+(b/d)y_0=1$. By the previous theorem, we know that the greatest common divisor of a/d and b/d must therefore divide 1. Hence $\gcd(a/d, b/d)=1$. ■

Lemma 3.1.5 Euclid's Lemma If $a \mid bc$ and $\gcd(a,b)=1$, then $a \mid c$.

Proof: Left as exercise.

Exercise 3.1.6 Prove Euclid's Lemma.

Now we are ready to state and prove the theorem that tells us how to find all solutions to $ax + by = c$.

Theorem 3.1.7 Let x_0, y_0 be a solution to the diophantine equation $ax + by = c$. All other solutions are given by $x = x_0 + (b/d)t$ and $y = y_0 - (a/d)t$, where t is an arbitrary integer.

Proof: Let x_0, y_0 be a known solution to the diophantine equation $ax + by = c$ and let x, y be any other solution. Then

$$ax_0 + by_0 = c = ax + by$$

which implies that $a(x - x_0) = b(y_0 - y)$. This can be rewritten as $r(x - x_0) = s(y_0 - y)$ for some r and s with $\gcd(r, s) = 1$. (WHY?) Hence $r \mid s(y_0 - y)$ and therefore $r \mid (y_0 - y)$. (WHY?) So there exists an integer, say t, such that $y_0 - y = rt$. This implies also that $x - x_0 = st$. (WHY?) Therefore, $x = x_0 + st$ and $y = y_0 - rt$. Amazingly enough, these formulae do not depend on the value of t. Notice that these values satisfy the diophantine equation regardless of what t is equal to.

$$\begin{aligned} ax + by &= a(x_0 + st) + b(y_0 - rt) \\ &= ax_0 + ast + by_0 - brt \\ &= c + t(as - br) \end{aligned}$$

But $as - br = 0$ so,

$$\begin{aligned} ax + by &= c + t(0) \\ &= c \end{aligned}$$

So there are infinitely many solutions to $ax + by = c$, one for each value of t. ■

Exercise 3.1.8 Answer the "WHY's" in the previous proof.

Example 3.1.9 Solve $56x + 72y = 40$.

The greatest common divisor of 56 and 72 (from the Euclidean Algorithm) is 8. Since this divides 40, we have solutions. To find the first solution, we must write 8 as a linear combination of 56 and 72 as such: $56(4) + 72(-3) = 8$. Multiplying through by 5 we obtain $56(20) + 72(-15) = 40$, so that $x_0 = 20$ and $y_0 = -15$ are our first solution. Then all solutions are expressed by $x = 20 + 9t$ and $y = -15 - 7t$ for some integer t.

Exercise 3.1.10 Solve $24x + 138y = 18$