Solutions to Inhomogeneous Second Order Diophantine Equations

Eddie Revell

August 24, 2020

1 Introduction

I recently noticed that a selection of Project Euler problems can be boiled down to solving certain *Diophantine equations*. The method for solving linear Diophantine equations over the integers is well known and consists primarily of using Euclid's algorithm for finding the greatest common divisor of two integers. However, methods solving second order Diophantine equations, and in particular those that are *inhomogeneous*, are less well known. In this document, I will outline a particular method used for solving such equations.

2 Setup

We will study equations of the form:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0 \tag{2.1}$$

Where $(a, b, c, d, e, f) \in \mathbb{Z}^6$ is known and we wish to solve for $(x, y) \in \mathbb{Z}^2$. This equation is *second order* because the highest power occurring is 2 (so long as a, b, c are not all zero). It is called *inhomogeneous* if at least one of d, e, f is non-zero.

3 Method of Solution

3.1 Reducing to a Pell-like Equation

The first step to solving (2.1) is to reduce the problem to something more manageable. We begin by noting the identity:

$$\begin{gathered}(\underbrace{b^2 - 4ac}_{D})(\underbrace{2ax + by + d}_{Y})^2 = (Dy + \underbrace{bd - 2ae}_{E})^2 + D(\underbrace{d^2 - 4af}_{F})^2 - E^2 \\ \text{i.e.} \quad DY^2 = (Dy + E)^2 + DF - E^2\end{gathered} \tag{3.1}$$

If we then set $X = Dy + E$ and $N = E^2 - DF$ we have:

$$X^2 - DY^2 = N \tag{3.2}$$

We shall call this a *Pell-like* equation (because of it's similarity to Pell's equation: $x^2 - ny^2 = 1$). Observe that if $D \leq 0$ the equation will have at most finitely many solutions due to the convexity of the LHS in this case. We will be interested in the case $D > 0$.

Remark: Our goal will be to find integer solutions to (3.2), which will allow us to find integer solutions to (2.1). However, we should note that if (X, Y) solves (3.2), then the corresponding solution (x, y) to (2.1) is not necessarily a pair of integers. On the other hand, if $(x, y) \in \mathbb{Z}^2$ solves (2.1), then the corresponding solution (X, Y) to (3.2) is necessarily a pair of integers. *Hence we may solve (2.1) in its entirety by solving (3.2) in its entirety and discounting those solutions that do not give valid integer solutions of (2.1).*

3.2 Solving a Pell-like Equation

In this section we will follow the method provided by [1]. We will look for integer solutions (x, y) to:

$$Ax^2 - By^2 + C = 0 \qquad A, B \in \mathbb{N}^* \quad , \quad C \in \mathbb{Z}^* \tag{3.3}$$

Claim 3.1. If AB is a perfect square, then (3.3) has finitely many solutions.

Proof. Suppose AB is a perfect square, so $AB = k^2$ for $k \in \mathbb{N}$. Then by multiplying (3.3) through by A we see that $(Ax)^2 - k^2y^2 = -AC \iff (Ax - ky)(Ax + ky) = -AC$. So the problem reduces to finding integer factors of AC, of which there are finitely many. □

In light of the above claim, **we will now assume that $\boldsymbol{AB}$ is not a perfect square**.

Let us now assume that we can find a smallest positive integer solution to (3.3), (x_0, y_0), in the sense that if (x, y) is also a positive integer solution, then $x_0 \leq x$. From this solution, we will attempt to construct a sequence of solutions (x_n, y_n). Suppose that:

$$\begin{aligned} x_{n+1} &= \alpha x_n + \beta y_n \\ y_{n+1} &= \gamma x_n + \delta y_n \end{aligned} \tag{3.4}$$

Under the assumption that (x_{n+1}, y_{n+1}) and (x_n, y_n) are both solutions to (3.3), we have:

$$\begin{aligned} Ax_{n+1}^2 - By_{n+1}^2 + C = 0 &\iff A(\alpha x_n + \beta y_n)^2 - B(\gamma x_n + \delta y_n)^2 + C = 0 \\ &\iff (A\alpha^2 - B\gamma^2)x_n^2 + 2(A\alpha\beta - B\gamma\delta)x_n y_n + (A\beta^2 - B\delta^2)y_n^2 + C = 0 \\ &\implies (A\alpha^2 - B\gamma^2 - A)x_n^2 + 2(A\alpha\beta - B\gamma\delta)x_n y_n + (A\beta^2 - B\delta^2 + B)y_n^2 = 0 \end{aligned} \tag{3.5}$$

Where in the last line we used the fact (x_n, y_n) also satisfies (3.3) to eliminate C. Since this must be true in the general case, we can conclude that the coefficients of each of the three terms are zero (hmmm... this argument might need a little more thought). Therefore we have three simultaneous equations for the four unknowns $\alpha, \beta, \gamma, \delta$:

$$A\alpha\beta = B\gamma\delta \tag{3.6}$$

$$A\alpha^2 - B\gamma^2 = A \tag{3.7}$$

$$A\beta^2 - B\delta^2 = -B \tag{3.8}$$

By squaring equation (3.6) and using the other two equations to eliminate $A\alpha^2$ and $A\beta^2$, we have $(A + B\gamma^2)(B\delta^2 - B) = B^2\gamma^2\delta^2 \iff AB\delta^2 - AB - B^2\gamma^2 = 0 \iff A\delta^2 - B\gamma^2 = A$. Comparing this result to (3.7) we see that:

$$A\alpha^2 = A\delta^2 \implies \alpha = \pm\delta \tag{3.9}$$

This then tells us in (3.6):

$$\beta = \pm\frac{B}{A}\gamma \tag{3.10}$$

Therefore, so long as we can find α and γ satisfying (3.7), we can find δ and β by using (3.9) and (3.10). Let us now assume that (α_0, γ_0) is the smallest integer solution to (3.7) such that $\alpha_0\gamma_0 \neq 0$. We define the matrix A to be:

$$A = \begin{pmatrix} \alpha_0 & \frac{B}{A}\gamma_0 \\ \gamma_0 & \alpha_0 \end{pmatrix} \implies A^{-1} = \begin{pmatrix} \alpha_0 & -\frac{B}{A}\gamma_0 \\ -\gamma_0 & \alpha_0 \end{pmatrix} \tag{3.11}$$

Clearly A and A^{-1} have integer entries. Writing $\boldsymbol{x}_n = (x_n, y_n)^T$, we can then write the relations (3.4) more succinctly as:

$$\boldsymbol{x}_{n+1} = A\boldsymbol{x}_n \tag{3.12}$$

We may also use A^{-1} to find new solutions. In general, if $\boldsymbol{x}$ is an integer solution, so are $A\boldsymbol{x}$ and $A^{-1}\boldsymbol{x}$.

The value of $\boldsymbol{c}$ is very important in determining solutions. In general, the method for finding the sequence of solutions $(\boldsymbol{x}_n)_{n\in\mathbb{Z}}$ described above **will not find all integer solutions to the problem**. For the general case, we often have several "seeds" $\boldsymbol{x}_0$, $\boldsymbol{y}_0$, ..., $\boldsymbol{z}_0$, each of which generates there own independent sequence of solutions $(\boldsymbol{x}_n)_{n\in\mathbb{Z}}$, $(\boldsymbol{y}_n)_{n\in\mathbb{Z}}$, ..., $(\boldsymbol{z}_n)_{n\in\mathbb{Z}}$ by using the above recurrence relation. We shall call these "seeds" "primitive" (or "fundamental") solutions. Fortunately, there are always finitely many primitive solutions. Unfortunately, it is harder to determine if you have actually found them all - I haven't done enough reading in this field yet so this is something to add to this document at a later date.

Important fact: In the case $C = \pm 1$, there is at most one fundamental solution (there could be zero if the equation has no solutions, which is possible). This means the method above will give a complete list of solutions.

4 A Simple Example

We will solve over the integers:

$$2x^2 - 3y^2 = 5 \tag{4.1}$$

Applying the method outlined above, we begin by noting the smallest positive solution to $2\alpha^2 - 3\gamma^2 = 2$ such that $\alpha\gamma \neq 0$ is given by $(\alpha_0, \gamma_0) = (5, 4)$, and hence the matrix A is:

$$A = \begin{pmatrix} 5 & 6 \\ 4 & 5 \end{pmatrix} \iff A^{-1} = \begin{pmatrix} 5 & -6 \\ -4 & 5 \end{pmatrix} \tag{4.2}$$

We may find the eigenvalues and eigenvectors of A (A^{-1}) in order to make computing A^n (A^{-n}) easier. The result is:

$$A = P_1 D P_1^{-1} \qquad P_1 = \begin{pmatrix} \sqrt{6} & -\sqrt{6} \\ 2 & 2 \end{pmatrix} \quad , \quad D = \begin{pmatrix} 5+2\sqrt{6} & 0 \\ 0 & 5-2\sqrt{6} \end{pmatrix} \tag{4.3}$$

$$A^{-1} = P_{-1} D P_{-1}^{-1} \qquad P_{-1} = \begin{pmatrix} -\sqrt{6} & \sqrt{6} \\ 2 & 2 \end{pmatrix} \tag{4.4}$$

The smallest solution to the initial problem is easy to spot: it is simply $\boldsymbol{x}_0 = (x_0, y_0) = (2,1)$. **We assume that this is the only fundamental solution**. We therefore deduce that the set of solutions are:

$$P_1 D^n P_1^{-1} \boldsymbol{x}_0 \quad \text{and} \quad P_{-1} D^n P_{-1}^{-1} \boldsymbol{x}_0 \qquad \forall n \in \mathbb{N} \tag{4.5}$$

Which are unique up to choices of sign (i.e. $(-x_0, -y_0)$ is also a valid solution). I will not simplify this further, but it is done in [1].

5 Solution to Project Euler Problem 94

Problem: It is easily proved that no equilateral triangle exists with integral length sides and integral area. However, the almost equilateral triangle 5-5-6 has an area of 12 square units. We shall define an almost equilateral triangle to be a triangle for which two sides are equal and the third differs by no more than one unit. Find the sum of the perimeters of all almost equilateral triangles with integral side lengths and area and whose perimeters do not exceed one billion (1,000,000,000).

Solution: We simplify the problem as much as possible using our new found techniques. Then we write an algorithm to compute the sum.

Observe that there are two types of nearly equilateral triangles with integral side length: One has sides $n, n, n-1$ while the other has sides $n, n, n+1$ for n an integer greater than 1. We will call these triangles of type "short" and "long" respectively (should probably think of a better name here!). We use Heron's formula to find the area of both types of triangle in terms of n:

"Short" triangle: $A = \frac{1}{4}(n-1)\sqrt{(n+1)(3n-1)}$
"Long" triangle: $A = \frac{1}{4}(n+1)\sqrt{(3n+1)(n-1)}$

Therefore, to find triangles with integer areas we necessarily require that $3n^2 \pm 2n - 1 = m^2$ for some $m \in \mathbb{N}$, where the ± is for short and long triangles respectively. Notice that not all such solutions will give an integer area, because we would then require also that $(n \mp 1)m/4$ is an integer. Miraculously, both the long and short triangles boil down to solving the same Pell-like equation:

$$X^2 - 12Y^2 + 192 = 0 \tag{5.1}$$

While we find (n, m) for long and short triangles by:

"Short" triangle: $X = 12m$ and $6n + 2 = Y$
"Long" triangle: $X = 12m$ and $6n - 2 = Y$

Currently this equation is not amenable to the methods developed because there may be multiple fundamental solutions, the determination of which being tricky. Notice that $12|X^2$, and hence $6|X$. Writing $X = 6X', Y' = Y$, the problem becomes $3X'^2 - Y'^2 = -16$. Observing that squares modulo 16 are 0, 1, 4 and 9, we see that $X'^2 = Y'^2 = 0 \pmod{16}$ and we conclude that 2 divides both X' and Y'. So we write $X' = 2X''$ and $Y' = 2Y''$, and the equation we are interested in solving becomes $3X''^2 - Y''^2 = -4$. Finally, observing that squares modulo 4 are 0 and 1, we conclude that $X''^2 = Y''^2 = 0 \pmod 4$ which allows us to write $X'' = 2y$, $Y'' = 2x$, and so we are now interested in solving:

$$x^2 - 3y^2 - 1 = 0 \tag{5.2}$$

The relevant relations are now:

$$m = 2y \qquad \text{and} \qquad 3n \pm 1 = 2x \qquad (\pm \text{ for short/long resp}) \tag{5.3}$$

Following the method from the previous section, we must find the smallest solution to $\alpha^2 - 3\gamma^2 = 1$ with $\alpha\gamma \neq 0$, which is of course $(\alpha_0, \gamma_0) = (2, 1)$. This gives us the matrix:

$$A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix} \tag{5.4}$$

The eigenvalues of this matrix are $\lambda_\pm = 2 \pm \sqrt{3}$. This allows us to find the diagonal form of the matrix $A = PDP^{-1}$ with $D = \text{diag}(\lambda_+, \lambda_-)$ and:

$$P = \begin{pmatrix} \sqrt{3} & -\sqrt{3} \\ 1 & 1 \end{pmatrix} \iff P^{-1} = \frac{1}{2\sqrt{3}} \begin{pmatrix} 1 & \sqrt{3} \\ -1 & \sqrt{3} \end{pmatrix} \tag{5.5}$$

Taking the primitive solution to be $\boldsymbol{x}_0 = (1, 0)^T$ and computing $(x_k, y_k) = PDP^{-1}\boldsymbol{x}_0$ we find that:

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} \frac{1}{2}(\lambda_+^k + \lambda_-^k) \\ \frac{\sqrt{3}}{6}(\lambda_+^k - \lambda_-^k) \end{pmatrix} \tag{5.6}$$

As k becomes large, $\lambda_-^k \to 0$ because $0 < \lambda_- < 1$, so $x_k \sim \lambda_+^k/2$. This means we may terminate the algorithm when:

$$\lambda_+^k > \text{perimter limit} = 1000000000 \tag{5.7}$$

Which is easily inverted with a logarithm. We now have everything we need to code the solution! The code may be found on my GitHub, and the solution is found to be 518408346, computed in much less than one second.

References

[1] F. Smarandache, *Gaceta Matematica* **2004**, *1*, 151–157.