CHMC Advanced Group: Diophantine Equations

03/10/2018

1 Introduction

This worksheet explores Pell's equation, which itself is a kind of Diophantine equation. The study of Diophantine equations is a rich endeavour in itself, though here we'll stick to Pell's equation.

The second section gives a brief introduction to Diophantine equations, and motivates Pell's equation by trying to solve the equation $x^2 - 2y^2 = 0$. The third section introduces some other, seemingly unrelated, problems that also lead to Pell's equation. The final section explores the concept of quadratic surds, and shows how these objects can be used to solve many kinds of Pell's equation.

2 The basics and $\sqrt{2}$

A **Diophantine equation** is any polynomial, in any number of unknowns, for which we want to find integer solutions. We usually use the letters u, v, w, x, y, z, etc. for unknowns, and the letters a, b, c, d, k, l for known/given constants. For example, the following are all types of Diophantine equations:

$$\begin{aligned} ax + by &= 0, \quad a, b \text{ integers;} \\ x^2 - 2y^2 &= 0; \\ x^2 - dy^2 &= \pm 1, \quad d \text{ is a not a perfect square;} \\ x^2 + y^2 &= z^2; \\ nxz + nxy + nyz &= 4xyz, \quad n \text{ is an integer.} \end{aligned}$$

In each of these equations we want to find integers that, when substituted in for x, y, z, etc., result in an equality. The first equation should look familiar, especially when you divide everything by b (assuming b is non-zero):

$$\frac{a}{b}x + y = 0,$$

the equation of a line.

Exercise 2.1 What are conditions on a and b such that we can find integer solutions in x, y such that $ax + by = 0$?

The second equation can be rewritten to express the claim that $\sqrt{2}$ is a rational number. We will see in this first section that this equation naturally leads to the third equation above, namely $x^2 - 2y^2 = \pm 1$, which can be generalized to the form $x^2 - dy^2 = \pm 1$.

The fourth equation is related to the Pythagorean theorem, which can be used to show there exist integer solutions to $x^2 + y^2 = z^2$.

The fifth equation, which is more commonly written in the form

$$\frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z},$$

is still an open problem; we do not know whether or not there are integer solutions in x, y, z.

With these preliminary remarks aside, let's begin the actual investigation!

Exercise 2.2 Verify that

$$\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}}.$$

Use this to show that

$$\sqrt{2} = 1 + \frac{1}{1 + 1 + \frac{1}{1+\sqrt{2}}}.$$

Exercise 2.3 Show that

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2+\frac{1}{2+\cdots}}}.$$

You can assume the number on the right hand side is, in fact, a number.

The number in the last exercise can be interpreted as a limiting process. The next few exercises show that this process can be done, and does in fact lead to a finite number.

Exercise 2.4 Let $r_1 = 1$, and define

$$r_n = 1 + \frac{1}{1 + r_{n-1}}.$$

What are r_2, r_3, and r_4?

Exercise 2.5 Verify that, for every positive integer n, we have

$$r_{n+1} - r_n = -\frac{(r_n - r_{n-1})}{(1 + r_n)(1 + r_{n-1})}.$$

Exercise 2.6 Prove that we have the inequalities

$$1 \leq r_1 \leq r_3 \leq \cdots \leq r_{2k+1} \leq \cdots \leq r_{2l} \leq \cdots \leq r_4 \leq r_2 \leq \frac{3}{2}.$$

In other words, show that the r_l are increasing for odd l, and r_k are decreasing for even k, and that every r_l is less than or equal to r_k, for odd l and even k.

Exercise 2.7 Use the last two exercises to show that $|r_{n+1} - r_n| \leq \frac{1}{4}|r_n - r_{n-1}|$.

Exercise 2.8 Conclude that r_n tends to a number α as n goes to infinity that satisfies $\alpha = 1 + \frac{1}{1+\alpha}$. Use this last equality to show that α satisfies $\alpha^2 = 2$. Therefore, the r_n converge to $\sqrt{2}$.

Note that each r_n can be written as a rational number $\frac{a}{b}$, where a and b have no common factors. We define the numbers p_n and q_n to be such that $r_n = \frac{p_n}{q_n}$.

Exercise 2.9 What are p_n and q_n for $n = 1, 2, 3$, and 4?

Exercise 2.10 Prove that, for $n \geq 1$, we have

$$p_n = p_{n-1} + 2q_{n-1},$$
$$q_n = p_{n-1} + q_{n-1}.$$

Hint: use exercise 2.4.

Exercise 2.11 Prove, using induction[1], that

$$p_n^2 - 2q_n^2 = (-1)^n.$$

Use this to conclude that

$$r_n^2 - 2 = \frac{(-1)^n}{q_n^2},$$

and thus

$$r_n - \sqrt{2} = \frac{(-1)^n}{q_n^2(r_n + \sqrt{2})}.$$

Exercise 2.12 Conclude from the last exercise that the pair (p_{2k-1}, q_{2k-1}) is a solution to the equation $x^2 - 2y^2 = -1$, and that the pair (p_{2k}, q_{2k}) is a solution to the equation $x^2 - 2y^2 = 1$.

Exercise 2.13 Using exercise 2.11, conclude that r_n gets closer to $\sqrt{2}$ as n goes to infinity.

This section has produced a way of approximating $\sqrt{2}$ with rational numbers, to whatever desired accuracy we want. Moreover, we have seen that while the equation $x^2 - 2y^2 = 0$ does not have any integer solutions, the two equations $x^2 - 2y^2 = \pm 1$ have infinitely many solutions, and are closely related to $x^2 - 2y^2 = 0$.

[1] If you're not familiar with what induction is, don't hesitate to ask!

3 Some related Diophantine equations

In this section we explore some other Diophantine equations that are related to the equation $x^2 - 2y^2 = \pm 1$. The first few exercises explore Pythagorean triples, while the last exercise is a probability question that, surprisingly or not, leads to the same equation.

Exercise 3.1 Consider the Diophantine equation

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

Verify that, for any integers k, m, n, the triple $(k(m^2 - n^2), 2kmn, k(m^2 + n^2))$ is a solution.

Exercise 3.2 Given a solution (a, b, c) to the equation $x^2 + y^2 = z^2$, i.e. a solution where $x = a, y = b, z = c$, is it possible to find a triple k, m, n such that

$$a = k(m^2 - n^2), b = 2kmn, \text{ and } c = k(m^2 + n^2)?$$

Experiment with some specific solutions like $(3, 4, 5), (5, 12, 13)$, etc.

Exercise 3.3 Consider the case of a Pythagorean triple (a, b, c), where the two smallest entries a and b differ by 1. These entries must be of the form $m^2 - n^2$ and $2mn$ with difference equal to 1 or -1, for some integers m, n. Derive, in each case, a condition of the form $x^2 - 2y^2 = 1$, where x and y each depend on m and n.

Exercise 3.4 Recall that $(x, y) = (3, 2)$ satisfies the equation $x^2 - 2y^2 = 1$. Determine from this equation two possible corresponding values of the pair (m, n) and their Pythagorean triples.

This exercise is, as mentioned, an open ended exploration, and is intimately related to the Pythagorean triples explored above.

Exercise 3.5 What are integer pairs (m, n) such that $x^2 + mx + n$ and $x^2 + mx - n$ can both be factored into degree-one polynomials with integer coefficients? For example, $x^2 + 5x + 6 = (x + 2)(x + 3)$ and $x^2 + 5x - 6 = (x + 6)(x - 1)$, so $(5, 6)$ is one such integer pair.

This problem is unrelated to the last few, but still incorporates the equation $x^2 - 2y^2 = \pm 1$ in its solution.

Exercise 3.6 Suppose there are n marbles in a jar with r of them red and $n - r$ of them blue. Two marbles are drawn at random (without replacement). The probability that both have the same color is $\frac{1}{2}$. What are the possible values of n and r?

4 Pell's equation

Pell's equation is the Diophantine equation $x^2 - dy^2 = k$, where d and k are integers, and d is not a perfect square. In the last few sections, we explored Pell's equation with $d = 2$ and $k = \pm 1$.

A **quadratic surd** is a number of the form $a+\sqrt{d}b$, where a and b are integers. Quadratic surds turn out to be useful in the study of Pell's equation, together with the **surd conjugates** $a - \sqrt{d}b = \overline{a + \sqrt{d}b}$.

Exercise 4.1 What is the surd conjugate of $1 + 3\sqrt{2}$? What about of $2 - 5\sqrt{5}$?

When multiplying quadratic surds, we distribute everything and recombine like terms involving $\sqrt{d}$. For example,

$$\begin{aligned}(2 + 3\sqrt{3})(5 - \sqrt{3}) &= 2 \cdot 5 + 2 \cdot (-3\sqrt{3}) + (3\sqrt{3}) \cdot 5 + (3\sqrt{3}) \cdot (-\sqrt{3}) \\ &= 10 - 6\sqrt{3} + 15\sqrt{3} - 9 \\ &= 1 + 9\sqrt{3}.\end{aligned}$$

Exercise 4.2 Write the product of $2 + 7\sqrt{3}$ and $3 - 4\sqrt{3}$ in the form $a + b\sqrt{3}$, where a, b are integers.

We define the **norm** of a quadratic surd $a + \sqrt{d}b$ to be the number

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})\overline{(a + b\sqrt{d}} = a^2 - b^2 d.$$

Exercise 4.3 What are the norms of the quadratic surds $2 + 7\sqrt{3}$ and $2 - 5\sqrt{5}$?

Exercise 4.4 Let $c = a + b\sqrt{d}$ and $w = u + v\sqrt{d}$. Verify that

$$N(cw) = N(c)N(w), \quad \text{and } N(c + w) + N(c - w) = 2(N(c) + N(w)).$$

Exercise 4.5 Verify that Pell's equation $x^2 - dy^2 = k$ can be written in the form $N(x + y\sqrt{d}) = k$.

We now turn back to the general Pell's equation. Our first interesting result is that, given two different equations with the same d, and solutions to each equation, we can form a solution to the "product" of the two equations. This is made precise in the next exercise.

Exercise 4.6 Suppose that $x^2 - dy^2 = k$ and $u^2 - dv^2 = l$ are two integer equations. Define the integers m and n by the equation

$$m + n\sqrt{d} = (x + y\sqrt{d})(u + v\sqrt{d}).$$

Show that $m = xu + dyv, n = xv + yu$, and $m^2 - dn^2 = kl$.

The next few exercises show how, given one solution to Pell's equation, we can generate infinitely many.

Exercise 4.7 Suppose that $(x, y) = (x_1, y_1)$ is a solution to $x^2 - dy^2 = 1$. Define the integer pair (x_2, y_2) by the equation

$$x_2 + y_2\sqrt{d} = (x_1 + y_1\sqrt{d})^2.$$

Verify that $x_2 = x_1^2 + dy_1^2, y_2 = 2y_1x_1$, and that (x_2, y_2) is also a solution to the equation $x^2 - dy^2 = 1$.

Exercise 4.8 Suppose more generally that x_n, y_n are defined by

$$x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n \text{ for } n \geq 2.$$

Note that $x_n + y_n\sqrt{d} = (x_{n-1} + y_{n-1}\sqrt{d})(x_1 + y_1\sqrt{d}$, and deduce that

$$x_n = x_1x_{n-1} + dy_1y_{n-1}, y_n = x_1y_{n-1} + y_1x_{n-1}.$$

Prove that (x_n, y_n) is also a solution to the equation $x^2 - dy^2 = 1$.

Exercise 4.9 Using the last two exercises, conclude that if $x^2 - dy^2 = 1$ has any solution other than $(x, y) = (\pm 1, 0)$, then $x^2 - dy^2 = 1$ has infinitely many solutions.

Exercise 4.10 In the last exercise, what happens if $(x, y) = (\pm 1, 0)$ are our only solutions? Why don't we get infinitely many solutions?

Exercise 4.11 Given that $(x, y) = (3, 2)$ is a solution to $x^2 - 2y^2 = 1$ (check this), generate a sequence of solutions (infinitely many) that also solve $x^2 - 2y^2 = 1$.

Recall in exercise 4.6 that if we have two equations $x^2 - dy^2 = k$ and $x^2 - dy^2 = l$, we can combine the solutions of each equation to get solutions to the equation $x^2 - dy^2 = kl$.

Exercise 4.12 Given that $(x, y) = (1, 1)$ is a solution to $x^2 - 2y^2 = -1$ (check this), generate an infinite sequence of solutions to the equation $x^2 - dy^2 = -1$.

Exercise 4.13 Given that $(x, y) = (3, 1)$ is a solution to the equation $x^2 - 2y^2 = 7$, generate an infinite sequence of solutions to the equation $x^2 - 2y^2 = 7$.