NON-LINEAR DIOPHANTINE EQUATIONS.

Christian Haesemeyer

Introduction: A *diophantine equation* of degree d in n variables is an equation of the form $p(x_1, \ldots, x_n) = 0$ where $p(x_1, \ldots, x_n)$ is a polynomial with integer coefficients of (total) degree d. For example, a linear diophantine equation is a diophantine equation of degree one. Recall that linear diophantine equations can be studied using congruences and the Chinese remainder theorem. Equations of higher degrees are harder to deal with. We will start with quadratic equations.

A diophantine equation of degree d is called *homogeneous* if every term of the equation has total degree exactly d. For example, $x^2 + y^2 = 0$ is homogeneous, while $x^2 + y^2 = 1$ is not. Finally, two diophantine equations are called equivalent if one is an integer multiple of the other. By a *solution* of a diophantine equation $p(x_1, \ldots, x_n) = 0$ we mean an n-tuple of integers $x_1, \ldots, x_n$ such that the equation is satisfied.

Exercise 0. Show that for a given diophantine equation $p(x_1 \ldots, x_n) = 0$ there is a unique equivalent equation $q(x_1 \ldots, x_n) = 0$ such that the coefficients of q have no common divisor.

Exercise 1. In this exercise we study homogeneous quadratic equations in two variables.

(a) Let $ax^2 + by^2 + cxy = 0$ be a homogeneous quadratic diophantine equation. Show that this equation has an integer solution if and only if it has a rational solution.

(b) Show that there is a linear change of variables with rational coefficients $x = x(u, v)$ and $y = y(u, v)$ such that the resulting equation in (u, v) is equivalent to one of the form $ru^2 + sv^2 = 0$ for some relatively prime integers r, s. Hint: Writing $x = \alpha u + \beta v$ and $y = \gamma u + \delta v$, you can choose α and γ (as long as you choose one of those numbers non-zero) and then solve for β and δ. The resulting r and s might be rational numbers, how do you solve that problem?

(c) We have seen that to study homogeneous quadratic diophantine equations in two variables, it suffices to look at equations of the form $ax^2 + by^2 = 0$ with a and b relatively prime. Of course, all these equations can be solved by simply setting $x = y = 0$, but this is a "trivial" solution. Show that the equation above has a non-trivial solution if and only if $-a/b$ is a rational square, that is, the square of a rational number. Formulate and prove a statement about how to find all possible solutions once you have one solution.

(d) Let p be a prime number. Prove that $x^2 - py^2 = 0$ has no non-trivial solutions, or equivalently, that $\sqrt{p}$ is irrational.

Exercise 2. Non-homogeneous quadratic diophantine equations in two variables are much more varied. The most famous class, probably, are *Pell's equations.* This exercise is about them. A Pell equation is any diophantine equation of the form $x^2 - Dy^2 = 1$ for some fixed positive integer D that is not a perfect square. The equations are named after the mathematician John Pell - who never studied them. L. Euler mistakenly attributed someone else's work to him.

(a) Find at least two different solutions for the Pell equation $x^2 - 2y^2 = 1$. Are they related, and if so, how? Can you produce as many solutions as you'd like (that is, infinitely many)?

(b) Suppose we have a general Pell equation $x^2 - Dy^2 = 1$ and assume that (x_0, y_0) is a solution. Can you produce further solutions? Hint: Use the fact that $1^2 = 1$.

(c) Back to the equation $x^2 - 2y^2 = 1$. Starting with the smallest solution, does the method discovered in (b) produce all possible solutions? (We will return to the question later, so don't despair if you can't find the answer right now.)

Addendum: It is a theorem that every Pell equation has a solution in the integers.

We recall the parametrization of all Pythagorean triples - that is, solutions of the diophantine equation $a^2 + b^2 = c^2$.

Theorem: Let $s > t \geq 1$ be odd, relatively prime integers. Then $a = st$, $b = (s^2 - t^2)/2$ and $c = (s^2 + t^2)/2$ is a Pythagorean triple. Moreover, all Pythagorean triples such that a, b and c have no common factors and a is odd arise in this fashion. (Exercise: Check that these are, in fact, Pythagorean triples.)

Proof. Assume (a, b, c) is a Pythagorean triple with no common factors and such that a is odd. Re-arrange the equation $a^2 + b^2 = c^2$ to read $a^2 = (c + b)(c - b)$. Observe that $(c + b)$ and $(c - b)$ are relatively prime. Indeed, if d divides both, then d also divides $2c = (c+b)+(c-b)$ and $2b = (c+b)-(c-b)$. Since b and c are relatively prime, that would mean d is 2, which implies that $a^2 = (c + b)(c - b)$ is even, a contradiction.

Since the product $(c + b)(c - b)$ is a square, but the factors are relatively prime, each of $(c + b)$ and $(c - b)$ must be a square. Write $(c + b) = s^2$ and $(c - b) = t^2$ for appropriate positive integers s and t. (Exercise: why can't

$b = c$?) Solving for a, b and c gives the expression of the triple as asserted in the theorem. □

Exercise 3. In this exercise we will show that the quartic diophantine equation $x^4 + y^4 = z^4$ (the Fermat quartic) has no non-trivial solutions (that is, no solutions but the obvious ones). The method we will use is known as "infinite descent". We will only look for positive solutions (why?). Clearly, it suffices to show that the equation $x^4 + y^4 = z^2$ has no non-trivial solutions.

(a) Suppose there is a non-trivial solution of $x^4 + y^4 = z^2$ (that is, a solution such that $xyz \neq 0$). Then there is a solution with smallest z, say (x_0, y_0, z_0). Show first that x_0, y_0 and z_0 have no common factors.

(b) Next check that exactly one of x_0, y_0 is odd. We will assume that x_0 is odd and y_0 is even.

(c) Now observe that $a = x_0^2$, $b = y_0^2$ and $c = z_0$ form a Pythagorean triple of the form described in the parametrization theorem. Let $s > t \geq 1$ be appropriate parameters. Show that $s - t$ is divisible by 4.

(d) Using that $(s - t)(s + t) = 2y^2$, show that there are integers u and v with $s + t = 2u^2$ and $s - t = 4v^2$, and u and $2v$ are relatively prime. solving for s and t, verify that $x^2 + 4v^4 = u^4$.

(e) Let $A = x$, $B = 2v^2$ and $C = u^2$. This is another Pythagorean triple of the form described in the parametrization theorem. (Check this!) Arguing in a sdimilar fashion to (d), show that the parameters S and T satisfy $S + T = 2X^2$ and $S - T = 2Y^2$ for some positive integers X and Y.

(f) Solve for S and T and verify that $u^2 = X^4 + Y^4$. Finally show that $uXY \neq 0$ and that $0 < u < z$, leading to a contradiction.

Exercise 4. Try again to prove that all the solutions of the Pell equation $x^2 - 2y^2 = 1$ can be created from the smallest solution (that is, the non-trivial solution in positive integers with smallest value of x) by taking powers. Use infinite descent: Assuming the existence of a solution that can not be created from the smallest one by taking powers, produce a solution that is smaller than the smallest one - a contradiction.