8. Conic sections

We can use Legendre's theorem, (7.1), to characterise all rational solutions of the general quadratic equation in two variables

$$ax^2 + bxy + cy^2 + dx + ey + ef = 0,$$

where a, b, c, d, e and f are rational numbers. The defines a conic section in $\mathbb{R}^2$ (a line, circle, parabola, ellipse or hyperbola, depending on the coefficients) and we want to locate all of the points with rational coordinates.

If $b = 0$ and $ac = 0$ then this means that the equation is linear in one variable (and we have either a line or a parabola). We can assign any value we want to the other variable and still find a rational solution.

If $b = 0$ and $ac \neq 0$ then we can complete the square in both x and y, so that we make the change of variables $x = x' + h$ and $y = y' + k$ and remove the linear terms in x and y. This reduces our equation down to

$$Ax^2 + By^2 + C = 0.$$

If $b \neq 0$ and $a = c = 0$ then consider the substitution

$$x = x' - y' \qquad \text{and} \qquad y = x' + y'.$$

As

$$\begin{aligned} xy &= (x' - y')(x' + y') \\ &= x'^2 - y'^2, \end{aligned}$$

we are reduced to the preceding case, when $b = 0$ and $ac \neq 0$.

If $b \neq 0$ and one of a and c is not zero then, possibly switching x and y, we may suppose that $a \neq 0$. In this case the substitution

$$x = x' - by'/2a \qquad \text{and} \qquad y' = y,$$

reduces us to the case $b = 0$.

Putting all of this together, we are reduced to considering the case

$$ax^2 + by^2 + c = 0.$$

The case when $abc = 0$ can be dealt with by hand (it turns on whether the ratio of the other two numbers is a square).

Clearing denominators we may assume that a, b and c are integers. If x and y are rational solutions of this equation then $x = X/Z$ and $y = Y/Z$ for some common denominator Z. Multiplying through by Z^2, we are reduced to considering integral solutions of the equation

$$aX^2 + bY^2 + cZ^2 = 0,$$

which we have already analysed.

Thus there is an algorithm to decide whether or not the conic C

$$ax^2 + bxy + cy^2 + dx + ey + ef = 0,$$

has a rational solution.

Note that once we are given one rational solution then in fact there are infinitely many and there is a simple way to describe all of them. Indeed, let $P_0 = (x_0, y_0)$ be a rational point on the curve C. Consider the line $L(m)$ through P_0 with slope m,

$$y - y_0 = m(x - x_0).$$

We suppose that $m \in \mathbb{Q}$. This line meets the conic at two points P_0 and an additional point $P_1(m)$. Suppose that $P_1(m)$ has coordinates (x_1, y_1). If we use the equation of the line to eliminate y from the equation for C, then we get a quadratic equation in x with rational coefficients. By assumption x_0 is one root of this equation. This implies that x_1 is also rational (for example, the sum $x_0 + x_1$ of the roots is minus the coefficient of x). Now using the equation of the line it follows that y_1 is rational as well.

Conversely, suppose that $P_1 = (x_1, y_1) \neq P_0$ is a rational point. Consider the line L connecting P_0 to P_1. This line has a slope m and contains P_0, so that $L = L(m)$. Thus we capture all rational points on C this way. Note that we consider the vertical line $x = x_0$ to have rational slope ∞.

It is fun and instructive to carry out this process for the unit circle

$$x^2 + y^2 = 1.$$

Let $P_0 = (-1, 0)$. The line $L(m)$ though P_0 with slope m is

$$y = m(x + 1).$$

Substituting this into the equation of the circle gives

$$x^2 + m^2(x + 1)^2 = 1,$$

so that

$$(1 + m^2)x^2 + 2m^2x + m^2 - 1 = 0.$$

Dividing through by $1 + m^2$, we get

$$x^2 + \frac{2m}{1 + m^2}x + \frac{m^2 - 1}{1 + m^2} = 0.$$

As one root x_0 is -1 and the product x_0x_1 of the roots is the constant term, we get

$$x_1 = \frac{1 - m^2}{1 + m^2}.$$

Thus

$$\begin{aligned} y_1 &= m(x_1+1) \\ &= \frac{2m}{1+m^2} \end{aligned}$$

It follows that the general rational point (x, y) on the circle $x^2+y^2 = 1$ is

$$x = \frac{1-m^2}{1+m^2} \qquad \text{and} \qquad y = \frac{2m}{1+m^2}.$$

Now if we put $m = a/b$, a and b integers, $(a, b) = 1$, we obtain every integral solution of the equation

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

We get

$$x = c(a^2 - b^2) \qquad y = 2abc \qquad \text{and} \qquad z = c(a^2 + b^2).$$

Note that as $z + x$ and $z - x$ are both integers, it follows that $2c \in \mathbb{Z}$.

If we have a primitive solution, that is, $(x, y) = 1$, then at most one of x and y is even. But if y is odd then a and b are both odd and $a^2 - b^2$ is divisible by 4, so that x is even and so precisely one of x and y is even.

Suppose that y is even. Then x is odd and so a and b have opposite parity. It follows that $c = \pm 1$. It is not hard to see these conditions are sufficient so that

Theorem 8.1. *Every primitive solution of the equation*

$$x^2 + y^2 = 1$$

with y even is given by

$$x = c(a^2 - b^2) \qquad y = 2abc \qquad \textit{and} \qquad z = c(a^2 + b^2)$$

with $c \pm 1$ and a unique pair a, $b \in \mathbb{Z}$ such that $(a, b) = 1$, and $a \not\equiv b \mod 2$, and vice-versa.

Every other solution for which a larger power of 2 divides y but not x is given by the same formula, with $c \neq \pm 1$ and a unique pair a, $b \in \mathbb{Z}$ such that $(a, b) = 1$, and $a \not\equiv b \mod 2$, and vice-versa.

It is interesting to consider the geometry of the zeroes of any polynomial $f(x, y)$ in x and y. We get a curve C in the plane defined by

$$f(x, y) = 0.$$

It turns out that there are polynomials of arbitrarily large degree d which can be reduced by a sequence of substitutions of rational functions with rational coefficients to conics, so that finding rational solutions to on the original curve is reduced to finding solutions on a conic.

In fact one can attach to any plane curve C a non-negative integer g called the **genus**. The genus is a birational invariant, which means that it is unchanged, even if we substitute for x and y rational functions (which don't necessarily have rational coefficients). Curves which can be reduced to conics have genus zero.

Unfortunately, even if a curve has genus zero, the birational transformations which turn it into a curve of genus zero need not have rational coefficients.

Let us consider an example. Consider the curve C given by the equation

$$2(x^2 + y^2)^2 = x^2 - y^2.$$

This looks like an infinity symbol and it is called a *lemniscate*.

It is not hard to check that this is a curve of genus zero. For example, the circle

$$x^2 + y^2 = t(x - y),$$

is tangent to the original curve C at the origin and meets C in one further point. Taking the second equation and plugging it into the first equation one gets

$$2t^2(x - y)^2 = x^2 - y^2.$$

It follows that

$$2t^2(x - y) = x + y.$$

Thus

$$y = \frac{2t^2 - 1}{2t^2 + 1}x.$$

Plugging this into the equation of the circle we get

$$x^2 \left(1 + \frac{(2t^2 - 1)^2}{(2t^2 + 1)^2}\right) = xt \left(1 - \frac{(2t^2 - 1)}{(2t^2 + 1)}\right),$$

so that

$$x^2 \left(\frac{(2t^2 - 1)^2 + (2t^2 + 1)^2}{(2t^2 + 1)^2}\right) = \frac{2xt}{(2t^2 + 1)}.$$

As expected $x = 0$ is a solution and the other solution is

$$x = \frac{t(2t^2 + 1)}{4t^4 + 1} \qquad \text{so that} \qquad y = \frac{t(2t^2 - 1)}{4t^4 + 1}.$$

This gives a rational parametrisation of C and if t is rational then we get rational values for x and y. However it is not so clear we get all rational values for x and y this way.

Instead, consider the change of variables

$$u = \frac{x}{x^2+y^2} \qquad \text{and} \qquad v = \frac{y}{x^2+y^2}.$$

On C we see that

$$\begin{aligned} u^2 - v^2 &= \frac{x^2}{(x^2+y^2)^2} - \frac{y^2}{(x^2+y^2)^2} \\ &= \frac{2(x^2-y^2)}{(x^2-y^2)} \\ &= 2. \end{aligned}$$

Conversely, since

$$\begin{aligned} u^2 + v^2 &= \frac{x^2}{(x^2+y^2)^2} + \frac{y^2}{(x^2+y^2)^2} \\ &= \frac{1}{x^2+y^2} \end{aligned}$$

we have the reciprocal relation

$$x = \frac{u}{u^2+v^2} \qquad \text{and} \qquad y = \frac{v}{u^2+v^2}.$$

Thus we get a birational transformation between the original curve and the hyperbola

$$u^2 - v^2 = 2.$$

This means u and v are rational functions of x and y and vice-versa. Now we can figure out the rational points of the hyperbola and use this to get the rational points of C. The birational map sets up a bijection between the rational points, away from the origin.