Lecture 1: Rational points on conics

Let’s first remember our strategy for finding the integer solutions to $a^2 + b^2 = c^2$, or (more-or-less) equivalently, the rational solutions to $x^2 + y^2 = 1$:

- We first find a single rational point $p$ on the circle $x^2 + y^2 = 1$.
- We take the line through $p$ with slope $t$ and, using a factoring technique, we find the other point of intersection $q_t$ of this line with the circle.
- As we vary over rational slopes $t$, the points $q_t$ fill out (almost) all the rational points on our circle.

Let’s try this strategy in some new situations. Suppose we are looking for all triples of integers $(a, b, c)$ such that $a^2 + 2b^2 = c^2$.

Note that the order matters, since the equation is not symmetric in $a$ and $b$. Some primitive examples are $(1, 2, 3)$ and $(7, 4, 9)$. It is not so easy to find more just by looking at the equation!

By dividing both sides of the equation by $c^2$, we see that finding primitive triples as above is the same as finding rational points on the ellipse $x^2 + 2y^2 = 1$.

We will fix the point $p = (-1, 0)$ on this ellipse.

1) Prove that the line through $(-1, 0)$ of slope $t$ will also meet the ellipse at the point

$$
\left( \frac{1 - 2t^2}{1 + 2t^2}, \frac{2t}{1 + 2t^2} \right)
$$
2) Conclude that we can generate all primitive triples solving our original equation by plugging in rational numbers $t$ to the parametric formula above and clearing denominators.

3) Find the rational points corresponding to the $t$-values $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, and $\frac{1}{4}$.

4) Find the $t$-values corresponding to the triples $(7, 30, 43)$ and $(41, 28, 57)$.

We can run the same argument for any conic. Once a (smooth) conic has a single rational point, it is guaranteed to have infinitely many of them and we can find them all by constructing a rational parametrization. Let’s try a few more.

5) Fix a positive integer $n$ and consider the triples of integers $(a, b, c)$ satisfying $a^2 + nb^2 = c^2$. Show that the rational parametrization of the ellipse $x^2 + ny^2 = 1$ which assigns to any point the slope of the line connecting it to $(-1, 0)$ is given by

$$\left(\frac{1 - nt^2}{1 + nt^2}, \frac{2t}{1 + nt^2}\right).$$

Use this to identify some integer solutions to the equation.

6) Find all the rational points on $x^2 + y^2 = 2$.

7) Show that there are no rational points on the circle $x^2 + y^2 = 3$. (Hint: first rescale to get an equation in integers $a^2 + b^2 = 3c^2$. Try looking at remainders mod 4 and doing a descent argument.)

8) Show that there are no rational points on the ellipse $2x^2 + 3y^2 = 1$.

9) The equation $2x^2 + 7y^2 = 1$ does have rational points; for example, the point $\left(\frac{-1}{3}, \frac{-1}{3}\right)$. Project away from the point $\left(\frac{-1}{3}, \frac{-1}{3}\right)$ to find all the rational points.

10) Pell’s equation has the form $x^2 - Dy^2 = 1$ where $D$ is an integer $> 1$. This equation always has the solution $(-1, 0)$, so we can find all the rational solutions using the techniques described earlier.

   a) Find all the rational solutions to Pell’s equation.

   b) Show that if $D$ is a perfect square, then the equation has no integer solutions besides the trivial ones $(\pm 1, 0)$.

It turns out that when $D$ is not a perfect square Pell’s equation has infinitely many integer solutions. (Can you see this from the rational parametrization?) Pell’s equation plays an important role in number theory due to its connections with $\sqrt{D}$. Note that for any integer solution $(x, y)$ the quotient $\frac{x}{y}$ is “very close” to $\sqrt{D}$. In
fact, using the theory of continued fractions one can show that such rational numbers $\frac{x}{y}$ are the “best approximations” to $\sqrt{D}$. One can also study Pell’s equation using techniques from algebraic number theory by factoring $x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y)$ inside of $\mathbb{Z}[\sqrt{D}]$. 