# 6.B. Generating solutions to Pell's equation

In the main notes for this unit we mentioned Brahmagupta's discovery that the existence of one solution to Pell's equation implies the existence of others. We shall prove a result along these lines.

**PROPOSITION.** *Let $p$ be a prime, and suppose that we are given a solution to Pell's equation $a^2 - pb^2 = 1$ where $a$ and $b$ are integers with $b \neq 0$. Then there are infinitely many distinct ordered pairs $(x, y)$ such that $x^2 - py^2 = 1$.*

**Proof.** Start with the given solution $a^2 - pb^2 = 1$ where $a$ and $b$ are integers with $b \neq 0$. We claim that $a$ must also be nonzero, for if it is not then $a^2 - pb^2$ is divisible by $p$.

One way of proving this result is to consider all numbers expressible in the form $x + y\sqrt{p}$, where $p$ is prime. It will be very helpful to know the following:

CLAIM 1. If $(x, y)$ and $(u, v)$ are distinct ordered pairs of integers, then $x + y\sqrt{p} \neq u + v\sqrt{p}$.

To see this suppose that $x + y\sqrt{p} = u + v\sqrt{p}$, so that $x - u = (v - y)\sqrt{p}$. If $x \neq u$ then the left hand side is nonzero, and therefore it follows that the right hand side is nonzero, so that $v - y$ is also nonzero and

$$\sqrt{p} \;=\; \frac{x - u}{v - y}\,.$$

Conversely, if $v - y$ is nonzero then so is $(x - u)/\sqrt{p}$ and hence $x - u$ is nonzero; in this case we also get the displayed formula for $\sqrt{p}$. However, since $p$ is prime we know that $\sqrt{p}$ is irrational, and hence there is no formula for $\sqrt{p}$ as a quotient of two nonzero integers. Therefore we must have $(x, y) = (u, v)$.

CLAIM 2. Let $p$ be prime again, and suppose that $(x, y)$ and $(u, v)$ are ordered pairs of integers. The product $(x + y\sqrt{p})(u + v\sqrt{p})$ has the form $r + s\sqrt{p}$ for suitable integers $(r, s)$.

In fact, the product is equal to $(xu + pyv) + (xv + yu)\sqrt{p}$.

CLAIM 3. In the setting above, define the norm $N(x + y\sqrt{p})$ of $x + y\sqrt{p}$ to be $x^2 - py^2$ (this is well-defined because $x$ and $y$ are uniquely determined). Then the norm of $(x + y\sqrt{p})(u + v\sqrt{p})$ is equal to $N(x + y\sqrt{p}) \cdot N(u + v\sqrt{p})$.

This is a straightforward verification and is left to the reader.

*Application to the proposition.* A solution of Pell's equation of the form $a^2 - b^2p = 1$ corresponds to a number of the form $a + b\sqrt{p}$ whose norm is equal to 1. We are assuming that we have a solution such that $b \neq 0$, and we have seen that $a \neq 0$ for every such solution. In fact, replacing $a + b\sqrt{p}$ with its negative if necessary, we can find a solution with $a > 0$ and $b \neq 0$.

CLAIM 4. Given a solution of Pell's equation as in the previous sentence, there is a second solution of the form $A + B\sqrt{p}$ such that $A > a$.

We can clearly iterate this procedure, and if we do so we obtain an infinite set of solutions to Pell's equation for the prime $p$.

Verification of Claim 4 is fairly simple. If $(a + b\sqrt{p})^2 = A + B\sqrt{p}$, then by the third claim the norm of $A + B\sqrt{p}$ is equal to the square of the norm of $(a + b\sqrt{p})$ and hence is equal to $1 \cdot 1 = 1$. But if we expand $(a + b\sqrt{p})^2$ we obtain

$$(a^2 + pb^2) \;+\; 2ab\sqrt{p}$$

so that $A = a^2 + pb^2$, which of course is greater than $p$ since $a$ and $b$ are both nonzero. This proves the statement in the conclusion of the proposition.