Nontrivial Solutions of Pell's Equation

This document consists of a self-contained proof that Pell's equation

$$x^2 - dy^2 = 1$$

always has nontrivial integer solutions x, y when d is a fixed positive integer that is not a square. By a "nontrivial" solution, we mean $(x, y) \neq (\pm 1, 0)$.

For example, a nontrivial solution of $x^2 - 5y^2 = 1$ is $(x, y) = (\pm 9, \pm 4)$, and a nontrivial solution of $x^2 - 13y^2 = 1$ is $(x, y) = (\pm 649, \pm 180)$. How can we prove nontrivial solutions exist for all positive nonsquare d?

The methods in the proof are not original with me, and indeed date back to people like Lagrange and Dirichlet. I just think it's nice to have self-contained proofs of famous results, and in this case, the proof is a great introduction to both the algebraic and the analytic sides of number theory.

Fact. $\sqrt{d}$ is irrational. Proof: If $\sqrt{d} = a/b$, then $a^2 = db^2$, which says a square is equal to a nonsquare.

Definition. Let

$$\mathcal{R} \;=\; \{\alpha = x + y\sqrt{d} \;:\; x, y \in \mathbb{Z}\}.$$

From now on, the variables u, v, w, x, y, and their subscripted versions, will always denote integers.

Fact. $\mathcal{R}$ is closed under multiplication. Proof:

$$(x + y\sqrt{d})(u + v\sqrt{d}) = (xu + dyv) + (xv + yu)\sqrt{d}. \tag{1}$$

Fact. If $\alpha \in \mathcal{R}$, the representation of α as $x + y\sqrt{d}$ is unique.

Proof: If $x + y\sqrt{d} = x_1 + y_1\sqrt{d}$, then $(x - x_1) + (y - y_1)\sqrt{d} = 0$. If $y - y_1 = 0$, then $x - x_1 = 0$ and we are done. If $y - y_1 \neq 0$, then $(x - x_1)/(y - y_1) = -\sqrt{d}$, contradicting the irrationality of $\sqrt{d}$.

Definition. If $\alpha \in \mathcal{R}$, say $\alpha = x + y\sqrt{d}$, then the **conjugate** of α, denoted $\overline{\alpha}$, is defined by $\overline{\alpha} = x - y\sqrt{d}$.

Fact. For $\alpha, \beta \in \mathcal{R}$, we have $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$.

Proof: Suppose $\alpha = x + y\sqrt{d}$ and $\beta = u + v\sqrt{d}$. Then $\overline{\alpha} = x - y\sqrt{d}$ and $\overline{\beta} = u - v\sqrt{d}$. We then observe

$$\begin{aligned} & \alpha\beta = (xu + dyv) + (xv + yu)\sqrt{d} \qquad \text{using (1)} \\ \text{so} \qquad & \overline{\alpha\beta} = (xu + dyv) - (xv + yu)\sqrt{d}. \end{aligned}$$

But also, we have

$$\begin{aligned} \overline{\alpha} \cdot \overline{\beta} &= (x - y\sqrt{d})(u - v\sqrt{d}) \\ &= (xu + dyv) - (xv + yu)\sqrt{d}. \end{aligned}$$

Definition. If $\alpha \in \mathcal{R}$, say $\alpha = x + y\sqrt{d}$, then the **norm** of α, denoted $N(\alpha)$, is defined by

$$N(\alpha) = \alpha \cdot \overline{\alpha} = (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2.$$

Notice that $N(\alpha)$ is always an integer (positive, negative, or zero).

Notice also that we can now rephrase our goal as:

GOAL: Show that there exists $\alpha \in \mathcal{R}$ satisfying $N(\alpha) = 1$, other than $\alpha = \pm 1$.

Fact. For $\alpha, \beta \in \mathcal{R}$, we have $N(\alpha\beta) = N(\alpha)N(\beta)$. That is, the norm function is multiplicative.

Proof: $N(\alpha\beta) = \alpha\beta \cdot \overline{\alpha\beta} = \alpha \cdot \beta \cdot \overline{\alpha} \cdot \overline{\beta} = \alpha \cdot \overline{\alpha} \cdot \beta \cdot \overline{\beta} = N(\alpha)N(\beta)$.

Fact. The only $\alpha \in \mathcal{R}$ satisfying $N(\alpha) = 0$ is $\alpha = 0$.

Proof: Suppose $\alpha = x + y\sqrt{d}$ with $N(\alpha) = x^2 - dy^2 = 0$. If $y = 0$, then also $x = 0$ and we are done. If $y \neq 0$, then $x^2/y^2 = d$, contradicting the irrationality of $\sqrt{d}$.

How do we find nontrivial $\alpha \in \mathcal{R}$ whose norm is 1? Naively, we might try to "divide" two elements of the same norm. However, $\mathcal{R}$ need not be closed under division.

Suppose $\alpha, \beta \in \mathcal{R}$ with $\beta \neq 0$. Let $\alpha = x + y\sqrt{d}$ and $\beta = u + v\sqrt{d}$, so both $u + v\sqrt{d}$ and $u - v\sqrt{d}$ are nonzero. We then have

$$\frac{x + y\sqrt{d}}{u + v\sqrt{d}} = \frac{(x + y\sqrt{d})(u - v\sqrt{d})}{u^2 - dv^2} = \frac{(xu - dyv) + (yu - xv)\sqrt{d}}{u^2 - dv^2} = s + t\sqrt{d}$$

where $s = \dfrac{xu - dyv}{u^2 - dv^2}$ and $t = \dfrac{yu - xv}{u^2 - dv^2}$ are rational numbers.

We will have $s + t\sqrt{d} \in \mathcal{R}$ if both $xu - dyv$ and $yu - xv$ are divisible by $u^2 - dv^2$, or equivalently, congruent to 0 mod $u^2 - dv^2$. The following gives a sufficient condition that guarantees this.

Fact. Suppose $x \equiv u \pmod{u^2 - dv^2}$ and $y \equiv v \pmod{u^2 - dv^2}$. Then $s = \dfrac{xu - dyv}{u^2 - dv^2}$ and $t = \dfrac{yu - xv}{u^2 - dv^2}$ are both integers, so $\dfrac{x + y\sqrt{d}}{u + v\sqrt{d}} = s + t\sqrt{d}$ is an element of $\mathcal{R}$.

Proof: If $x \equiv u \pmod{u^2 - dv^2}$ and $y \equiv v \pmod{u^2 - dv^2}$ then, working mod $u^2 - dv^2$, we have

$$\begin{aligned} xu - dyv &\equiv uu - dvv = u^2 - dv^2 \equiv 0, \\ yu - xv &\equiv vu - uv = 0. \end{aligned}$$

Corollary. Suppose $\alpha = x + y\sqrt{d}$ and $\beta = u + v\sqrt{d}$ are elements of $\mathcal{R}$ with the same nonzero norm ($x^2 - dy^2 = u^2 - dv^2 \neq 0$), and suppose that $\alpha \neq \pm\beta$. Suppose further that $x \equiv u \pmod{u^2 - dv^2}$ and $y \equiv v \pmod{u^2 - dv^2}$. Then

$$\frac{x + y\sqrt{d}}{u + v\sqrt{d}} = s + t\sqrt{d} \in \mathcal{R} \qquad (s + t\sqrt{d} \neq \pm 1)$$

so $x + y\sqrt{d} = (s + t\sqrt{d})(u + v\sqrt{d})$ and $N(x + y\sqrt{d}) = N(s + t\sqrt{d})N(u + v\sqrt{d})$, and therefore $s + t\sqrt{d} \neq \pm 1$ is a nontrivial element of $\mathcal{R}$ with norm 1, and hence provides a nontrivial solution of Pell's equation.

So our goal becomes finding $\alpha = x + y\sqrt{d}, \beta = u + v\sqrt{d} \in \mathcal{R}$ with the same nonzero norm, such that $\alpha \neq \pm\beta$ and such that the ordered pairs (x, y) and (u, v) are congruent mod $u^2 - dv^2$ (defining congruence of ordered pairs in the natural way). How do we do this? We now switch from algebraic to analytic thinking.

Lemma. Let y be a positive integer and let $\xi > 0$ be an irrational number. (We will use $\xi = \sqrt{d}$.) Then there exist integers x', y' with $y' > y$ and $|x' - y'\xi| < \dfrac{1}{y'}$.

Proof: For each $k = 1, 2, 3, \ldots, y$, define a_k to be the nearest integer to $k\xi$, and define $\varepsilon_k = |a_k - k\xi|$. Then choose y_1 to be an integer satisfying

$$y_1 > \max\left\{\frac{1}{\varepsilon_1}, \frac{1}{\varepsilon_2}, \ldots, \frac{1}{\varepsilon_y}\right\},$$

so $1/y_1 < \varepsilon_k = |a_k - k\xi|$ for all $k \leq y$. Next, for each $m = 1, 2, \ldots, y_1$, we write $m\xi$ as

$$m\xi = \lfloor m\xi \rfloor + \{m\xi\}$$

where $\lfloor m\xi \rfloor$ is an integer and $0 < \{m\xi\} < 1$ (the usual "floor" and "fractional part" of $m\xi$). Now consider the y_1 numbers

$$\{\xi\}, \{2\xi\}, \{3\xi\}, \ldots, \{y_1\xi\}.$$

Those are irrational numbers in $(0, 1)$, and they are all distinct. (If we had $\{u\xi\} = \{v\xi\}$, then $u\xi - v\xi$ would be an integer, contradicting the irrationality of ξ.) Therefore, there must exist u, v with $1 \leq u < v \leq y_1$ such that

$$|\{u\xi\} - \{v\xi\}| < \frac{1}{y_1}.$$

We now consider

$$\begin{aligned} v\xi &= \lfloor v\xi \rfloor + \{v\xi\} \\ u\xi &= \lfloor u\xi \rfloor + \{u\xi\} \\ (v-u)\xi &= \lfloor v\xi \rfloor - \lfloor u\xi \rfloor + \{v\xi\} - \{u\xi\} \end{aligned}$$

Let x' be the integer $\lfloor v\xi \rfloor - \lfloor u\xi \rfloor$ and let y' be the positive integer $v - u < y_1$. We then have

$$\begin{aligned} x' - y'\xi &= \{u\xi\} - \{v\xi\} \\ |x' - y'\xi| &= |\{u\xi\} - \{v\xi\}| < \frac{1}{y_1} < \frac{1}{y'}. \end{aligned}$$

It remains to show that $y' > y$. If $y' = k \leq y$, then

$$|x' - y'\xi| = |x' - k\xi| \geq |a_k - k\xi| = \varepsilon_k > \frac{1}{y_1}$$

where a_k is the closest integer to $k\xi$. This contradicts $|x' - y'\xi| < 1/y_1$. Therefore $y' > y$, and the proof of the lemma is complete.

Now, we construct an infinite sequence of ordered pairs

$$\{(x_0, y_0), (x_1, y_1), (x_2, y_2), \ldots\}$$

in the following way. We let $y_0 = 1$ and let x_0 be the closest integer to $\sqrt{d}$. Then we have $|x_0 - y_0\sqrt{d}| < 1/y_0$. Next, if (x_n, y_n) is defined, we let x_{n+1}, y_{n+1} be the integers x', y' generated by applying the lemma to the situation where $y = y_n$ and $\xi = \sqrt{d}$. We then have

$$y_0 < y_1 < y_2 < \cdots$$

so all pairs (x_n, y_n) are distinct, and we have

$$\left|x_n - y_n\sqrt{d}\right| < \frac{1}{y_n} \qquad \text{for each } n.$$

We now consider the norms of the numbers $x_n + y_n\sqrt{d}$. The norm is always an integer, and we have

$$\left|N(x_n + y_n\sqrt{d})\right| = \left|x_n + y_n\sqrt{d}\right| \left|x_n - y_n\sqrt{d}\right|.$$

We now observe that

$$\begin{aligned} \left|x_n + y_n\sqrt{d}\right| &\leq \left|x_n - y_n\sqrt{d}\right| + \left|2y_n\sqrt{d}\right| \\ &\leq \frac{1}{y_n} + 2y_n\sqrt{d} \\ &\leq y_n + 2y_n\sqrt{d} = (2\sqrt{d} + 1)y_n. \end{aligned}$$

We therefore have

$$\left|N(x_n + y_n\sqrt{d})\right| \leq (2\sqrt{d} + 1)y_n \cdot \frac{1}{y_n} = 2\sqrt{d} + 1.$$

That is, $N(x_n+y_n\sqrt{d})$ is an integer between $-(2\sqrt{d}+1)$ and $2\sqrt{d}+1$. So we have infinitely many numbers $x_n+y_n\sqrt{d}$, but only finitely many possibilities for their norms. By the pigeonhole principle, there is an infinite subsequence

$$\{(x_{j_0}, y_{j_0}), (x_{j_1}, y_{j_1}), (x_{j_2}, y_{j_2}), \ldots\}$$

such that $N(x_{j_n}+y_{j_n}\sqrt{d}) = N(x_{j_0}+y_{j_0}\sqrt{d})$ for all n. Say $N(x_{j_0}+y_{j_0}\sqrt{d}) = u^2-dv^2$. Note that u^2-dv^2 is nonzero because none of the numbers $x_n+y_n\sqrt{d}$ are zero.

Next, we will apply the pigeonhole principle again. Consider $(u^2-dv^2)^2$ boxes, corresponding to pairs of integers (a,b) where $1 \le a \le u^2-dv^2$ and $1 \le b \le u^2-dv^2$. We put (x_{j_n}, y_{j_n}) in box (a,b) if we have $x_{j_n} \equiv a$ and $y_{j_n} \equiv b \bmod u^2-dv^2$.

There are infinitely many (x_{j_n}, y_{j_n}) but finitely many boxes. Therefore there exist $m < n$ such that (x_{j_m}, y_{j_m}) and (x_{j_n}, y_{j_n}) are in the same box. Define $\alpha = x_{j_m}+y_{j_m}\sqrt{d}$ and $\beta = x_{j_n}+y_{j_n}\sqrt{d}$. Note that $\beta \neq \pm\alpha$ because we have $y_{j_n} > y_{j_m} > 0$. Now α and β have the same nonzero norm u^2-dv^2, and they satisfy $x_{j_m} \equiv x_{j_n}$ and $y_{j_m} \equiv y_{j_n} \bmod u^2-dv^2$. We have achieved our goal.