Pell’s Equation

Pell’s equation is the Diophantine equation

\[(1) \quad x^2 - dy^2 = 1\]

where \(d\) is a fixed non-square positive integer. Our discussion of this topic follows the exposition of Chapter VII of Part One of *Elementary Number Theory* by Edmund Landau.

We begin by noting that for any positive integer \(d\), the number \(\sqrt{d}\) is either an integer, or else is irrational. For, if \(d\) is a perfect square, say \(d = s^2\) with \(s > 0\), then \(\sqrt{d} = s\). Conversely, if \(\sqrt{d}\) is rational, say \(\sqrt{d} = a/q\), then \(dq^2 = a^2\). Let

\[d = \prod_p p^{\delta_p}, \quad q = \prod_p p^{\kappa_p}, \quad a = \prod_p p^{\alpha_p}\]

be the canonical factorizations of \(d\), \(q\), and \(a\), respectively. By the unique factorization theorem we see that \(\delta_p + 2\kappa_p = 2\alpha_p\) for all primes \(p\). Thus every \(\delta_p\) is even, and hence \(d\) is a perfect square.

The equation (1) clearly has the two solutions \(x = \pm 1, y = 0\); our goal is to show that there are infinitely many other solutions. To this end we begin with a fundamental result of Dirichlet.

**Theorem 1.** For any real number \(\theta\) and any positive integer \(N\), there exists integers \(a\) and \(n\) such that \(1 \leq n \leq N\) and \(|n\theta - a| < 1/N\).

Our proof of the above (as well as many of the ensuing proofs) depends on the *pigeonhole principle*, which asserts that if \(M\) objects are placed in \(N\) boxes, and \(M > N\), then there is a box that contains at least 2 objects. While this may be intuitively clear, we can give a rigorous demonstration as follows: Let \(c_n\) denote the number of objects in the \(n^{\text{th}}\) box, let \(\mu_1\) denote the average of the \(c_n\), and let \(\mu_\infty\) denote the maximum of the \(c_n\). Since \(\sum_{n=1}^N c_n = M\), it follows that

\[\mu_1 = \frac{1}{N} \sum_{n=1}^N c_n = \frac{M}{N} > 1.\]
But $\mu_\infty \geq \mu_1$, and $\mu_\infty$ is an integer since each $c_n$ is an integer. Hence $\mu_\infty \geq 2$.

**Proof.** Let $\{\alpha\}$ denote the fractional part of $\alpha$, which is to say that $\{\alpha\} = \alpha - [\alpha]$. Thus $0 \leq \{\alpha\} < 1$ for every real number $\alpha$. We consider the $N+1$ numbers $\{0\theta\}, \{1\theta\}, \ldots, \{N\theta\}$. We partition the interval $[0, 1)$ into $N$ subintervals $[0, 1/N), [1/N, 2/N), \ldots, [(N-1)/N, 1)$. These are our boxes, and we have $M = N+1 > N$ numbers that lie in these intervals. Thus there is a subinterval that contains at least 2 of our numbers. Let us suppose that $(n-1)/N \leq \{j\theta\} < n/N$ and that $(n-1)/N \leq \{k\theta\} < n/N$ where $j$ and $k$ are distinct integers with $0 \leq j < N$ and $0 \leq k < N$. Let $r_j = [j\theta]$ and $r_k = [k\theta]$. Thus

\begin{align*}
&\frac{n-1}{N} \leq j\theta - r_j < \frac{n}{N}, \\
&\frac{n-1}{N} \leq k\theta - r_k < \frac{n}{N}.
\end{align*}

By exchanging $j$ and $k$ if necessary, we may suppose that $j > k$. If we multiply all members of (3) by $-1$ we obtain an equivalent form:

\begin{align*}
&-\frac{n}{N} < -k\theta + r_k \leq -\frac{n-1}{N}.
\end{align*}

By adding respective members of (2) and (4), we deduce that

\begin{align*}
&-\frac{1}{N} < (j - k)\theta - (r_j - r_k) < \frac{1}{N}.
\end{align*}

We obtain the stated result by taking $n = j - k$ and $a = r_j - r_k$. Note that $n \geq 1$ because $j > k$, and $n \leq N$ because $j \leq N$ and $k \geq 0$.

**Corollary 2.** If $\theta$ is irrational, then there exist infinitely many pairs $a, n$ of integers such that

$$|\theta - \frac{a}{n}| < \frac{1}{n^2}.$$ 

**Proof.** By multiplying $a$ and $n$ by $-1$, if necessary, we may assume that $n > 0$. By multiplying both sides by $n$ we see that the stated inequality asserts that $|n\theta - a| < 1/n$. A first solution of this can be found by taking $n = 1$ and $a$ to be the integer nearest $\theta$. Suppose that $R$ pairs $a_r, n_r$ have been found. Choose $N$ so large that $1/N < |n_r\theta - a_r|$ for all $r$, $1 \leq r \leq R$. Note that $|n_r\theta - a_r| > 0$ for all $r$, since $\theta$ is irrational. Thus such an $N$ exists. By Theorem 1 there exists a pair $a, n$ such that $|n\theta - a| < 1/N$. Here $n \leq N$, so $1/N \leq 1/n$, and hence $|n\theta - a| < 1/n$. Thus the pair $a, n$ is of the required type. Moreover, this pair is different from the earlier pairs, since $|n\theta - a| < 1/N < |n_r\theta - a_r|$ for all $r$, $1 \leq r \leq R$. Thus we may take $a_{R+1} = a$ and $n_{R+1} = n$, and by induction we deduce that we can construct an infinite sequence of such pairs.

**Example.** Suppose that $\theta = \pi$. We note that $\pi - 3 = 0.14159 \ldots$. Then $2\pi - 6 = 0.2831 \ldots$, $3\pi - 9 = 0.42477 \ldots$, $4\pi - 12 = 0.5663 \ldots$, $5\pi - 15 = 0.7079 \ldots$, $6\pi - 18 = 0.8495 \ldots$. 2
$7\pi - 22 = -0.008851\ldots$. Here we have an impressively good approximation. While Dirichlet’s theorem guarantees that there will be infinitely many $a, n$ for which $|\pi - a/n| < 1/n^2$, here we have $|\pi - 22/7| = 0.06/7^2$. The downside of this is that for the next many $n$ the quantity $n\pi$ is going to be very close to $22n/7$. Eventually the numbers $n\pi$ drift away from multiples of $1/7$. We suppress the details, as the calculation can be better done by using the theory of continued fractions, but the first improvement on $n = 7$ occurs with $106\pi - 333 = 0.008821\ldots$, which is only slightly better than $22/7$. Indeed, $\pi - 333/106 = 0.93/333^2$, so this rational approximation just barely qualifies to be counted in Corollary 2. The good news is that when an approximation is not remarkably good, a further good approximation will occur rather soon. In fact, the first improvement on $n = 106$ is $113\pi - 355 = 0.0000301$. This is even more remarkably good, since $355/113 = 0.0034 = 113/2$. In summary,

\[
\begin{align*}
\pi - 3 &= 0.14159\ldots = 0.14/1^2, \\
\pi - \frac{22}{7} &= -0.008851\ldots = -0.06196/7^2, \\
\pi - \frac{333}{106} &= 0.00088322\ldots = 0.93506/106^2, \\
\pi - \frac{355}{113} &= -0.0000026676\ldots = -0.0034/113^2.
\end{align*}
\]

A number of patterns are emerging here. For example, these record-breaking approximations alternate between being less than $\pi$ and greater than $\pi$. Also, the rational approximations are

\[
\begin{align*}
\frac{3}{1} \cdot 7 \cdot 3 + 1 &= \frac{22}{7} = 3.14159\ldots \\
\frac{15 \cdot 22 + 3}{7} &= \frac{333}{106} = \frac{1 \cdot 333 + 22}{1 \cdot 106 + 7} = \frac{355}{113}. 
\end{align*}
\]

Such patterns can be explained via the theory of continued fractions.

**Theorem 3.** Suppose that $d > 0$ is not a perfect square. Then there is an integer $m$ with $|m| < 1 + 2\sqrt{d}$ such that the equation $x^2 - dy^2 = m$ has infinitely many solutions.

**Proof.** Since $\sqrt{d}$ is irrational, there exist infinitely many pairs $a, n$ such that $|n\sqrt{d} - a| < 1/n$. For such a pair,

\[
|a^2 - dn^2| = |(a-n\sqrt{d})(a+n\sqrt{d})| = |(a-n\sqrt{d})(a-n\sqrt{d}+2n\sqrt{d})| < \frac{1}{n} \cdot \frac{1}{n} + 2n \cdot 1 = 1 + 2\sqrt{d}.
\]

Since there are only finitely many integers $m$ such that $|m| < 1 + 2\sqrt{d}$, one of them has to occur infinitely many times as the value of $a^2 - dn^2$.

**Theorem 4.** Pell’s equation (1) has at least one solution in integers with $y > 0$.

**Proof.** Let $m$ have the properties as in Theorem 3. For $x, y$ satisfying $x^2 - dy^2 = m$, we classify $x$ and $y$ according to the residue classes they fall in modulo $|m|$. There are $m^2$
possible pairs of residue classes, but there are infinitely many pairs \(x, y\), and hence there must be a pair of residue classes that occurs infinitely many times. Thus there will exist positive integers \(x_1, y_1\) and \(x_2, y_2\) such that \(x_1^2 - dy_1^2 = x_2^2 - dy_2^2 = m\), \(x_1 \equiv x_2 \pmod{|m|}\), \(y_1 \equiv y_2 \pmod{|m|}\), and \(0 < y_1 < y_2\). Put

\[
x = \frac{x_1x_2 - dy_1y_2}{m}, \quad y = \frac{x_1y_2 - x_2y_1}{m}.
\]

Since \(x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv 0 \pmod{|m|}\) and \(x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_2 \equiv 0 \pmod{|m|}\), we see that \(x\) and \(y\) are integers. Also,

\[
x^2 - dy^2 = \frac{1}{m^2}(x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2
\]

\[
= \frac{1}{m^2}(x_1^2x_2^2 - 2dx_1x_2y_1y_2 + d^2y_1^2y_2^2 - dx_1^2y_2^2 - dx_1y_1^2y_2^2 + 2dx_1y_2^2x_2y_1 - dx_2^2y_1^2)
\]

\[
= \frac{1}{m^2}(x_1^2x_2^2 - dx_1^2y_2^2 - dx_1y_1^2y_2^2 + d^2y_1^2y_2^2) - \frac{1}{m^2}(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = 1.
\]

Finally, if \(y = 0\), then it would follow that \(x = \pm 1\), and then we would have

\[
\pm y_2 = y_2x - x_2y = \frac{y_2(x_1x_2 - dy_1y_2) - x_2(x_1y_2 - x_2y_1)}{m} = \frac{y_1(x_2^2 - dy_2^2)}{m} = y_1.
\]

But \(0 < y_1 < y_2\), so this is impossible.

**Theorem 5.** Suppose that \(x_1, y_1\) and \(x_2, y_2\) both satisfy Pell’s equation (1), and put \(x_3 = x_1x_2 + dy_1y_2\), \(y_3 = x_1y_2 + x_2y_1\). Then \(x_3, y_3\) satisfies Pell’s equation.

**Proof.** We observe that

\[
(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = (x_1x_2 + dy_1y_2) + (x_1y_2 + x_2y_1)\sqrt{d} = x_3 + y_3\sqrt{d},
\]

and similarly that

\[
(x_1 - y_1\sqrt{d})(x_2 - y_2\sqrt{d}) = x_3 - y_3\sqrt{d}.
\]

By multiplying these two identities together we see that \((x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_3^2 - dy_3^2)\).

Thus we have the stated result.

**Theorem 6.** Suppose that \(x, y\) is a solution of (1) with \(y \neq 0\), and set \(\eta = x + y\sqrt{d}\). Then

\[
\eta > 1 \text{ if and only if } x > 0, y > 0;
\]

\[
0 < \eta < 1 \text{ if and only if } x > 0, y < 0;
\]

\[
-1 < \eta < 0 \text{ if and only if } x < 0, y > 0;
\]

\[
\eta < -1 \text{ if and only if } x < 0, y < 0.
\]

**Proof.** If \(x > 0\) and \(y > 0\), then \(\eta > y \geq 1\). Consequently, if \(x < 0\) and \(y < 0\), then \(\eta < -1\). If \(x > 0\) and \(y < 0\), then \(1 = (x + y\sqrt{d})(x - y\sqrt{d})\) and \(x - y\sqrt{d} > 1\), so \(0 < \eta < 1\). Consequently, if \(x < 0\) and \(y > 0\), then \(-1 < \eta < 0\). With these four implications established, the converses follow.
**Theorem 7.** Let $d$ be a positive non-square integer, and let $x_0, y_0$ be the solution of (1) with the least positive $y_0$ and with $x_0 > 0$. Then all solutions of (1) are given by

$$x + y\sqrt{d} = \pm(x_0 + y_0\sqrt{d})^n$$

where $n$ runs over all integers.

**Proof.** That such $x, y$ are solutions is evident from Theorem 5 if $n \geq 0$. For $n < 0$ it suffices to note that $(x_0 + y_0\sqrt{d})^{-1} = x_0 - y_0\sqrt{d}$.

Let $x_1, y_1$ and $x_2, y_2$ be two solutions of (1) in non-negative integers. Since $1 + dy^2$ is an increasing function of $y$, we deduce that if $y_1 < y_2$, then $x_1 < x_2$, and hence $x_1 + y - 1\sqrt{d} < x_2 + y_2\sqrt{d}$. Thus, among all solutions $x, y$ in positive integers, the quantity $x + y\sqrt{d}$ is minimized when $(x, y) = (x_0, y_0)$. Let $\varepsilon = x_0 + y_0\sqrt{d}$. Then by Theorem 6 we know that $\varepsilon > 1$. Let $x, y$ be an arbitrary solution in positive integers. Then $x + y\sqrt{d} < \varepsilon$ in view of the minimality of $x_0, y_0$. Thus there is a positive integer $n$ such that $\varepsilon^n \leq x + y\sqrt{d} < \varepsilon^{n+1}$. Let $x'$ and $y'$ be defined by the equation

$$x' + y'\sqrt{d} = (x + y\sqrt{d})/\varepsilon^n = (x + y\sqrt{d})(x_0 - y_0\sqrt{d})^n.$$

Thus $x', y'$ is a solution, by Theorem 5. Moreover, if $1 < x' + y'\sqrt{d}$, then by Theorem 6 it follows that $x'$ and $y'$ are positive. However, this contradicts the minimality of $\varepsilon$. Hence $x' + y'\sqrt{d} = 1$, and so $x' = 1, y' = 0$, and $x + y\sqrt{d} = \varepsilon^n$.

As a function of $d$, the fundamental solution of Pell’s equation may be quite large. For example, when $d = 166$, the fundamental solution is $x_0 = 1700902565, y_0 = 132015642$.

**Historical note.** Euler was familiar with the work of Lord Brouncker (1620–1684) on Pell’s equation, but erroneously attributed the results to John Pell (1611–1685).

**Exercises**

1. Suppose that the integer $d$ is not a perfect cube. Show that $d^{1/3}$ is irrational.

2. Suppose that $M$ objects are placed in $N$ boxes. Show that if $M > 2N$, then there is a box with at least 3 objects in it.

3. Our object here is to show that by taking a little more care, we can derive a slight strengthening of Theorem 1.

(a) Arrange the $N + 1$ numbers $\{0\theta\}, \{1\theta\}, \ldots, \{N\theta\}$ in increasing order, so that $0 = \{0\theta\} \leq \{j_0\theta\} \leq \{j_1\theta\} \leq \cdots \leq \{j_N\theta\} < 1$. For $1 \leq \nu \leq N$, let $g_\nu = \{j_\nu\theta\} - \{j_{\nu-1}\theta\}$ be the size of the gap between $\{j_{\nu-1}\theta\}$ and $\{j_\nu\theta\}$. In addition, let $g_{N+1} = 1 - \{j_N\theta\}$. Explain why

$$\sum_{\nu=1}^{N+1} g_\nu = 1.$$
(b) Note that average of the \( g_\nu \) is \( = 1/(N+1) \).
(c) Argue that the minimum of the \( g_\nu \) is \( \leq 1/(N+1) \).
(d) Let \( \nu \) be chosen so that \( g_\nu \) is minimal, set \( j = j_\nu \) and \( k = \nu - 1 \), so that

\[ 0 \leq \{j\theta\} = \{k\theta\} \leq \frac{1}{N+1}. \]

Continue as in the proof of Theorem 1 to show that there exist integers \( n \) and \( a \) with 
\( 1 \leq n \leq N \) such that \( |n\theta - a| \leq 1/(N+1) \).
(e) Note that equality is achieved in the above when \( \theta = 1/(N+1) \).

4. With reference to (5), express the following in reduced form:

(a) \( 3 + \frac{1}{7} \)
(b) \( 3 + \frac{1}{7 + \frac{1}{15}} \)
(c) \( 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}} \)

5. From the pattern evident in (5), one might infer that the next best approximation will 
arise from a fraction of the form

\[ f(k) = \frac{335k + 133}{113k + 106}. \]

(a) Find \( c \) such that

\[ f(k) = \frac{335}{113} + \frac{c}{113k + 106}. \]

(b) Deduce that \( f \) is increasing.

(c) Let \( K \) denote the least positive \( k \) such that \( f(k) > \pi \). Determine \( K \).
(d) For \( k = 1, 2, \ldots K \), which of the fractions \( f(k) \) deserve to be counted as acceptable in 
the context of Corollary 2?
(e) Use \( K \) to extend the table of Exercise 4.

6. Let \( \theta = (1 + \sqrt{5})/2 \) be the golden ratio.
(a) Find the first several record-breaking small values of \( n\theta - a \).
(b) Compute several expressions of the sort

\[ 1 + \frac{1}{1}, \quad 1 + \frac{1}{1 + \frac{1}{1}}, \quad 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}, \ldots \]

(c) Formulate a conjecture concerning the general record-breaking small values.
7. Let \( \theta = (1 + \sqrt{5})/2 \) be the golden ratio.
   (a) Show that \( \theta^2 - \theta - 1 = 0 \).
   (b) Show that if \( a \) and \( n \) are integers, not both zero, then \( |a^2 - an - n^2| \geq 1 \).
   (c) Write \( a^2 - an - n^2 = n^2(a/n - \theta)(a/n + 1/\theta) \), and note that if \( a/n \) is near \( \theta \), then \( a/n + 1/\theta \) is near \( \sqrt{5} \).
   (d) Deduce that if \( c < 1/\sqrt{5} \), then the inequality
   \[ |\theta - \frac{a}{n}| < \frac{c}{n^2} \]
   has at most finitely many solutions.

8. Suppose that \( d \) is positive and not a perfect square. Let \( n \) be a non-zero integer. Show that if \( x^2 - dy^2 = n \) has a solution, then it has infinitely many solutions.

9. Suppose that \( d \) is positive, not a perfect square, and that \( m \) is a positive integer. Show that there exist infinitely many solutions of \( x^2 - dy^2 = 1 \) with \( m|y \).

10. Suppose that

    \[ 1 + 2 + \cdots + n = m^2. \]

    (a) Deduce that \( (2n + 1)^2 - 8m^2 = 1 \).
    (b) Show that if \( x^2 - 8y^2 = 1 \), then \( x \) is odd.
    (c) Deduce that there are infinitely many pairs \( m, n \) that satisfy (6).
    (d) The first solution is \( m = n = 1 \) (not very exciting). Find the next solution.

The equation

\[ x^2 - dy^2 = -1 \]

is known as the *negative Pell equation*. For some \( d \), this equation has solutions, but for others it has none. This is explored in the following exercises.

11. Suppose that (7) holds. By arguing as in the proof of Theorem 6, show that if \( \eta = x + y\sqrt{d} \), then

    \[ \eta > 1 \text{ if and only if } x > 0, y > 0; \]
    \[ -1 < \eta < 0 \text{ if and only if } x > 0, y < 0; \]
    \[ 0 < \eta < 1 \text{ if and only if } x < 0, y > 0; \]
    \[ \eta < -1 \text{ if and only if } x < 0, y < 0. \]

12. Let \( x_0, y_0 \) be the fundamental solution of (1) in positive integers, and put \( \varepsilon = x_0 + y_0\sqrt{d} \).
    Suppose that (7) has a solution.
(a) Show that there is a solution \( u, v \) of (7) in positive integers with \( 1 < u + v\sqrt{d} < \varepsilon \).
(b) Show that \( u^2 + dv^2, 2uv \) is a solution of (1) with \( 1 < u^2 + dv^2 + 2uv\sqrt{d} < \varepsilon^2 \).
(c) Deduce that \( u^2 + dv^2 = x_0, 2uv = y_0 \).
(d) Conclude that all solutions of (7) occur with \( x + y\sqrt{d} = \pm(u + v\sqrt{d})^n \) with \( n \) odd, and all solutions of (1) occur similarly with \( n \) even.

13. (a) Find the fundamental solution of \( x^2 - 5y^2 = -1 \) in positive integers.
(b) Find the fundamental solution \( x_0, y_0 \) of \( x^2 - 11y^2 = 1 \) in positive integers. By examining \( y = 1, 2, \ldots, y_0 - 1 \), show that the equation \( x^2 - 11y^2 = -1 \) has no solution.

14. Suppose that \( d \equiv 3 \pmod{4} \). Show that the equation (7) has no solution because there is a modulus \( m \) such that (7) has no solution as a congruence modulo \( m \).

15. Show that if \( d \) is divisible by a prime \( p, p \equiv 3 \pmod{4} \), then (7) has no solution.

16. Suppose that \( p \equiv 1 \pmod{4} \).
   (a) Show that if \( x^2 - py^2 = 1 \), then \( x \) is odd and \( y \) is even.
   (b) Let \( x_0, y_0 \) be the fundamental solution of \( x^2 - py^2 = 1 \) in positive integers. Show that \( \gcd(x_0 + 1, x_0 - 1) = 2 \).
   (c) Deduce that one of two cases arise:
      Case 1. \( x_0 - 1 = 2pu^2, x_0 + 1 = 2v^2 \).
      Case 2. \( x_0 - 1 = 2u^2, x_0 + 1 = 2pv^2 \).
   Show that in Case 1, \( v^2 - pu^2 = 1 \) with \( |u| < y_0 \), which contradicts the minimality of \( y_0 \).
   (d) Show that in Case 2, \( u^2 - pv^2 = -1 \).
   (e) Conclude that if \( p \equiv 1 \pmod{4} \), then the equation \( x^2 - py^2 = -1 \) has solutions in integers.

17. (a) Show that the minimal solution of \( x^2 - 34y^2 = 1 \) in positive integers is \((35, 6)\).
   (b) By examining \( y = 1, 2, 3, 4, 5 \), show that \( x^2 - 34y^2 = -1 \) has no solution in integers.
   (c) Observe that the equation \( x^2 - 34y^2 = -1 \) has the rational solution \((5/3, 1/3)\). Deduce that the congruence \( x^2 - 34y^2 \equiv -1 \pmod{m} \) has a solution provided that \( 3 \nmid m \).
   (d) Observe that the equation \( x^2 - 34y^2 = -1 \) has the rational solution \((3/5, 1/5)\). Deduce that the congruence \( x^2 - 34y^2 \equiv -1 \pmod{m} \) has a solution provided that \( 5 \nmid m \).
   (e) Use the Chinese Remainder Theorem to show that the congruence \( x^2 - 34y^2 \equiv -1 \pmod{m} \) has a solution for all \( m \).