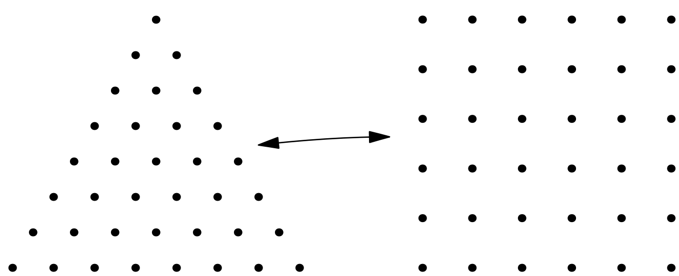
2 Pell's Equation

2.1 Square-triangular numbers and Convergents of Continued Fractions

Square-triangular numbers are integers which are simultaneously:

- Perfect squares: of the form n^2 for some $n \in \mathbb{N}$;
- Triangular: of the form $\sum_{k=1}^{m} k = \frac{1}{2}m(m+1)$ for some $m \in \mathbb{N}$.

For example, 36 is a square-triangular number:



To find all such, we need to solve the Diophantine equation $2n^2 = m(m+1)$. It can be seen that this is equivalent to solving the Diophantine equation

$$x^2 - 2y^2 = 1 \quad \text{where} \quad \begin{cases} x = 2m+1 \\ y = 2n \end{cases}$$

Here are the first few square-triangular numbers n^2, and the corresponding m, n, x, y:

n^2	m	n	x	y
1	1	1	3	2
36	8	6	17	12
1225	49	35	99	70
41616	288	204	577	408

You should notice something: the solutions (x, y) correspond to *some* of the convergents $\frac{p_n}{q_n}$ of the continued fraction representation of $\sqrt{2}$. Here is a table of the first ten convergents and the corresponding values of $p_n^2 - 2q_n^2$:

n	1	2	3	4	5	6	7	8	9	10
$\frac{p_n}{q_n}$	$\frac{1}{1}$	$\frac{3}{2}$	$\frac{7}{5}$	$\frac{17}{12}$	$\frac{41}{29}$	$\frac{99}{70}$	$\frac{239}{169}$	$\frac{577}{408}$	$\frac{1393}{985}$	$\frac{3363}{2378}$
$p_n^2 - 2q_n^2$	-1	1	-1	1	-1	1	-1	1	-1	1

It appears that exactly half the convergents of $\sqrt{2}$ yield to a solution of $x^2 - 2y^2 = 1$ and thus to a square-triangular number. This equation is the first in an important family:

Definition 2.1. A *Pell equation* is a Diophantine equation of the form $x^2 - dy^2 = 1$ where d is an integer which is *not* a perfect square. Among all solutions, the *fundamental solution* is the pair (a, b) where both are positive and a, b are minimal.

Recall we want only *integer* solutions (x, y). To keep the following treatment clean, we will only consider solutions where both x and y are *positive.* Clearly $(\pm x, \pm y)$ will also be solutions.

The above discussion suggests that solutions to Pell's equation should be some, but not all, of the convergents of $\sqrt{d}$. This is indeed the case. We shall show more: that Pell's equation has infinitely many solutions for any d and that these may be computed using a relatively simple procedure. It follows that there are infinitely many square-triangular numbers! For the present, we shall ignore the existence question and focus on how to find solutions. The first part of this is straightforward and follows from our discussion of Diophantine approximations.

Theorem 2.2. *If (x, y) is a solution to Pell's equation $x^2 - dy^2 = 1$, then $\frac{x}{y}$ is a convergent of $\sqrt{d}$.*

Proof. From our discussion of Hurwitz's Theorem, it is enough to show that any solution satisfies $\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{2y^2}$. This is straightforward by factorization: if $x^2 - dy^2 = 1$, then

$$\frac{x^2}{y^2} = d + \frac{1}{y^2} > d \implies \frac{x}{y} > \sqrt{d} > 1$$

from which

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y}\left|x - \sqrt{d}y\right| = \frac{\left|x^2 - dy^2\right|}{y\left|x + \sqrt{d}y\right|} = \frac{1}{y^2\left|\frac{x}{y} + \sqrt{d}\right|} < \frac{1}{2y^2\sqrt{d}} < \frac{1}{2y^2}$$

■

The Theorem says that we can find all solutions to Pell's equation by hunting through the list of convergents. This may take a while...

Examples 2.3. We've already seen that half of the convergents of $\sqrt{2}$ appear to yield solutions to $x^2 - 2y^2 = 1$. Here's what happens for the first few convergents of $\sqrt{7}$ and $\sqrt{13}$.

n	1	2	3	4	5	6	7	8	9	10
$\frac{p_n}{q_n}$	$\frac{2}{1}$	$\frac{3}{1}$	$\frac{5}{2}$	$\frac{8}{3}$	$\frac{37}{14}$	$\frac{45}{17}$	$\frac{82}{31}$	$\frac{127}{48}$	$\frac{590}{223}$	$\frac{717}{271}$
$p_n^2 - 7q_n^2$	-3	2	-3	1	-3	2	-3	1	-3	2
$\frac{p_n}{q_n}$	$\frac{3}{1}$	$\frac{4}{1}$	$\frac{7}{2}$	$\frac{11}{3}$	$\frac{18}{5}$	$\frac{119}{33}$	$\frac{137}{38}$	$\frac{256}{71}$	$\frac{393}{109}$	$\frac{649}{180}$
$p_n^2 - 13q_n^2$	-4	3	-3	4	-1	4	-3	3	-4	1

We had to go to the 10^{th} convergent before finding a solution to $x^2 - 13y^2 = 1$!

You should spot another pattern here: the values of $p_n^2 - dq_n^2$ are *eventually periodic.* This is a theorem, though we won't prove it: it relates to the eventual periodicity of the continued fraction of a quadratic irrational.

Exercises 1. A square lattice has 1189 dots on each side. If these dots are arranged into an equilateral triangular lattice, how many does are on each side of the triangle?

2. Check rigorously that the *integer* solutions to the Pell and square-triangular equations $x^2 - 2y^2 = 1$ and $2n^2 = m(m+1)$ correspond via $x = 2m+1$ and $y = 2n$.

3. (a) Create a table listing the fundamental solutions (x, y) to Pell's equation $x^2 - dy^2 = 1$ for each non-square $d \leq 15$.
(*No working is necessary*)

   (b) Write a computer program or learn how to use a computer algebra package to find a solution to the Pell equation $x^2 - 109y^2 = 1$.

2.2 New solutions from old

Thankfully there is an easier way to generate solutions to Pell's equation than calculating all the convergents and checking each. It still depends on knowing a solution, but once you have it the others are easy to find. Here is the process for the basic equation with $d = 2$.

- Start with the fundamental solution $(x, y) = (3, 2)$.
- Suppose that (x, y) also solves the equation. Consider

  $$(3 + 2\sqrt{2})(x + y\sqrt{2}) = (3x + 4y) + (2x + 3y)\sqrt{2}$$

  and observe that the coefficients give a *new solution* $(3x + 4y, 2x + 3y)$:

  $$\begin{aligned}(3x+4y)^2 - 2(2x+3y)^2 &= 9x^2 + 24xy + 16y^2 - 8x^2 - 24xy - 18y^2 \\ &= x^2 - 2y^2 = 1\end{aligned}$$

- By induction, if $x + y\sqrt{2} = (3 + 2\sqrt{2})^n$, then $x^2 - 2y^2 = 1$. Start computing:

  $$\begin{aligned}(3+2\sqrt{2})^2 &= 17 + 12\sqrt{2} \\ (3+2\sqrt{2})^3 &= 99 + 70\sqrt{2} \\ (3+2\sqrt{2})^4 &= 577 + 408\sqrt{2} \\ (3+2\sqrt{2})^5 &= 3363 + 2378\sqrt{2} \\ &\vdots\end{aligned}$$

  We seem to be obtaining all the solutions as powers of the fundamental solution $3 + 2\sqrt{2}$. Indeed this is the case:

Theorem 2.4. *(x, y) is a positive solution to Pell's equation $x^2 - 2y^2 = 1$ if and only*

$$x + y\sqrt{2} = (3 + 2\sqrt{2})^n \text{ for some } n \in \mathbb{N}$$

Proof. As seen above, if (x, y) is a solution, then $(3x + 4y, 2x + 3y)$ is another. We can think of this as a matrix equation: if (x_n, y_n) is a solution, then (x_{n+1}, y_{n+1}) is also a solution, where

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

The crucial observation is that the matrix has determinant 1, so we can reverse the process *in integers*:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} 3 & -4 \\ -2 & 3 \end{pmatrix} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 3x_{n+1} - 4y_{n+1} \\ -2x_{n+1} + 3y_{n+1} \end{pmatrix}$$

We wish to establish the following; if (x_{n+1}, y_{n+1}) is a positive solution with $x_{n+1} > 3$, then

(a) $x_n^2 - 2y_n^2 = 1$;

(b) x_n and y_n are positive;

(c) $x_n < x_{n+1}$.

The first is trivial: just calculate. For (b), first observe that

$$x_{n+1}^2 > 2y_{n+1}^2 \implies x_{n+1} > \sqrt{2}y_{n+1} \implies x_n = 3x_{n+1} - 4y_{n+1} > (3\sqrt{2} - 4)y_{n+1} > 0$$

Now observe that

$$y_n > 0 \iff \frac{2}{3}x_{n+1} < y_{n+1} \iff \frac{8}{9}x_{n+1}^2 < 2y_{n+1}^2 = x_{n+1}^2 - 1 \iff x_{n+1} > 3$$

For (c), the positivity of y_n guarantees

$$x_{n+1} = 3x_n + 4y_n > 3x_n > x_n$$

From (x_{n+1}, y_{n+1}) we can therefore produce a sequence of positive solutions where

$$x_{n+1} > x_n > x_{n-1} > x_{n-2} > \cdots$$

provided each x_k is always larger than 3. An infinite decreasing sequence of positive integers is an absurdity: eventually some solution must satisfy $1 \le x_1 \le 3$. Since the only solution with $x = 1, 2$ or 3 is the fundamental solution $(3, 2)$, the proof is complete. ∎

This type of proof is known as a *descent* argument, since one is repeatedly creating something smaller: these operate somewhat like a reverse induction and were popularized by Fermat. Nothing prevents us from continuing to descend from $(x, y) = (3, 2)$, except that the solutions will no longer be positive: indeed one obtains the sequence

$$(1, 0), \quad (3, -2), \quad (17, -12), (99, -70), (577, -408), \ldots$$

exactly the conjugates of the positive solutions.

The crucial thing that drives the argument is the presence of a matrix $\left(\begin{smallmatrix} 3 & 4 \\ 2 & 3 \end{smallmatrix}\right)$ with *integer entries and determinant 1.* Such matrices keep appearing in our discussions, and will continue to do so!

We can rephrase the result using matrix notation: first observe that the eigenvalues and eigenvectors[1] of $\left(\begin{smallmatrix}3&4\\2&3\end{smallmatrix}\right)$ are $3\pm 2\sqrt{2}$ and $\left(\begin{smallmatrix}\pm\sqrt{2}\\1\end{smallmatrix}\right)$. We can now diagonalize and easily exponentiate to obtain a simplified method of calculation:

$$\begin{aligned}\begin{pmatrix}x_n\\y_n\end{pmatrix} &= \begin{pmatrix}3&4\\2&3\end{pmatrix}^n\begin{pmatrix}1\\0\end{pmatrix}\\ &= \begin{pmatrix}\sqrt{2}&-\sqrt{2}\\1&1\end{pmatrix}\begin{pmatrix}(3+2\sqrt{2})^n&0\\0&(3-2\sqrt{2})^n\end{pmatrix}\begin{pmatrix}\sqrt{2}&-\sqrt{2}\\1&1\end{pmatrix}^{-1}\begin{pmatrix}1\\0\end{pmatrix}\\ &= \begin{pmatrix}\frac{1}{2}\Big((3+2\sqrt{2})^n+(3-2\sqrt{2})^n\Big)\\ \frac{1}{2\sqrt{2}}((3+2\sqrt{2})^n-(3-2\sqrt{2})^n)\end{pmatrix}\end{aligned}$$

Since $3-2\sqrt{2}\approx 0.1715$ is tiny, we can use the ceiling and floor functions to see that,

$$x_n = \left\lceil \frac{1}{2}(3+2\sqrt{2})^n \right\rceil \qquad y_n = \left\lfloor \frac{1}{2\sqrt{2}}(3+2\sqrt{2})^n \right\rfloor = \left\lfloor \frac{x_n}{\sqrt{2}} \right\rfloor$$

This can easily be entered into your calculator. For example $x_7 = 114243, y_7 = 80782$.

We have now proved that there are infinitely many solutions to the equation $x^2-2y^2=1$, and thus infinitely many square-triangular numbers. They get big rather quickly, indeed exponentially!

Can we apply the same trick with $x^2-3y^2=1$? It is easy to see that $(x,y)=(2,1)$ is the smallest solution. We'd therefore like to claim that the n^{th} positive solution (x_n,y_n) satisfies

$$x_n+\sqrt{3}y_n = (2+\sqrt{3})^n$$

Can we make this work in general? Indeed we can!

Theorem 2.5. *Suppose $d\in\mathbb{N}$ is not a perfect square. A pair (x,y) of positive integers solves the Pell equation $x^2-dy^2=1$ if and only if $\exists n\in\mathbb{N}$ such that*

$$x+y\sqrt{d} = \left(a+b\sqrt{d}\right)^n$$

where (a,b) is the fundamental solution. Moreover, such solutions may be computed using floors and ceilings:

$$x = \left\lceil \frac{1}{2}(a+b\sqrt{d})^n \right\rceil \qquad y = \left\lfloor \frac{1}{2\sqrt{d}}(a+b\sqrt{d})^n \right\rfloor = \left\lfloor \frac{x}{\sqrt{d}} \right\rfloor \tag{†}$$

We'll be able to give a very easy proof later in the term once we've developed some ring-theory. For now we give a sketch showing how to generalize the approach used for $d=2$. Note particularly that the matrix in step 2 again has determinant 1...

[1] $\left(\begin{smallmatrix}3&4\\2&3\end{smallmatrix}\right)\left(\begin{smallmatrix}\sqrt{2}\\1\end{smallmatrix}\right) = (3+2\sqrt{2})\left(\begin{smallmatrix}\sqrt{2}\\1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}3&4\\2&3\end{smallmatrix}\right)\left(\begin{smallmatrix}-\sqrt{2}\\1\end{smallmatrix}\right) = (3-2\sqrt{2})\left(\begin{smallmatrix}-\sqrt{2}\\1\end{smallmatrix}\right)$

Proof (Sketch). 1. If (x, y) solves $x^2 - dy^2 = 1$, then so does $(ax + dby, ay + bx)$. This follows from

$$(a + \sqrt{d}b)(x + \sqrt{d}y) = (ax + dby) + \sqrt{d}(ay + bx)$$

2. We therefore have a sequence (x_n, y_n) of solutions satisfying:

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{$*$}$$

3. To see that all solutions have this form, suppose that (x_{n+1}, y_{n+1}) is a solution with $x_{n+1} > a$, and reverse the process to define (x_n, y_n) via

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}^{-1} \begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} ax_{n+1} - bdy_{n+1} \\ ay_{n+1} - bx_{n+1} \end{pmatrix}$$

   Now check the following:

   (a) $x_n^2 - dy_n^2 = 1$;
   (b) $x_n, y_n \in \mathbb{N}$;
   (c) $x_n < x_{n+1}$.

4. By a descent argument, we must eventually produce the fundamental solution (a, b).

5. Diagonalizing the matrix in $(*)$ results in (†).

■

Exercises 1. (a) If (x_0, y_0) is an integer solution to $x^2 - dy^2 = -1$, show that $(x_0^2 + dy_0^2, 2x_0y_0)$ solves Pell's equation $x^2 - dy^2 = 1$.

   (b) Find a solution to $x^2 - 41y^2 = -1$ by plugging in $y = 1, 2, 3, \ldots$ until you find a value for which $41y^2 - 1$ is a perfect square. Use this to find a solution to $x^2 - 41y^2 = 1$.

2. If (x_0, y_0) is a solution to $x^2 - dy^2 = m$, and if (x_1, y_1) is a solution to $x^2 - dy^2 = 1$, show that $(x_0x_1 + dy_0y_1, x_0y_1 + y_0x_1)$ is also a solution to $x^2 - dy^2 = m$. Use this to find three solutions in positive integers to the equation $x^2 - 2y^2 = 7$.
   (*Hint: Guess your first solution* (x_1, y_1)*!*)

3. Consider the negative Pell equation $x^2 - dy^2 = -1$.

   (a) Prove that if this has a solution in integers, then d is not divisible by 4 or any prime congruent to 3 modulo 4.
   (*Hint: recall quadratic residues from a previous class*)

   (b) For each non-square integer $d \leq 15$, determine whether the negative Pell equation $x^2 - dy^2 = -1$ has a solution. What are the next three (non-square) integers d are for which $x^2 - dy^2 = -1$ has a solution? Find a solution in each case.

4. For each of the following equations, either find a solution (x, y) in positive integers, or explain why no solution can exist.

   (a) $x^2 - 11y^2 = 7$ (b) $x^2 - 11y^2 = 433$ (c) $x^2 - 11y^2 = 3$

5. Provide arguements for parts (a), (b) and (c) in the proof of Theorem 2.5. Also explain why the floor and ceiling formulæ are correct.

2.3 Existence of a Solution to Pell's Equation

We know (Theorem 2.2) that every solution (x, y) to $x^2 - dy^2 = 1$ yields a convergent $\frac{x}{y}$ of $\sqrt{d}$. We now see the converse:

Theorem 2.6. *Pell's equation $x^2 - dy^2 = 1$ has infinitely many solutions. More precisely,* at least one convergent *of $\sqrt{d}$ yields the fundamental solution, which generates all solutions by Theorem 2.5.*

Here is the strategy for the proof.

1. First hunt for two pairs $(x, y), (X, Y)$ for which $x^2 - dy^2 = X^2 - dY^2 = m$ gives the *same value.*
2. Divide one by the other:

$$\frac{x + \sqrt{d}y}{X + \sqrt{d}Y} = \frac{xX - dyY + \sqrt{d}(yX - xY)}{X^2 - dY^2} = \frac{xX - dyY + \sqrt{d}(yX - xY)}{m}$$

   whence

$$\left(\frac{xX - dyY}{m}\right)^2 - d\left(\frac{yX - xY}{m}\right)^2 = \frac{(x^2 - dy^2)(X^2 - dY^2)}{m^2} = 1$$

3. We therefore have an integer solution to Pell's equation if and only if

$$\frac{xX - dyY}{m}, \frac{yX - xY}{m} \in \mathbb{Z} \iff \begin{cases} xX \equiv dyY \pmod{|m|} \\ yX \equiv xY \pmod{|m|} \end{cases}$$

   Certainly if $x \equiv X$ and $y \equiv Y \pmod{|m|}$ then we're done.

Example 2.7. As a sanity check, recall that $45^2 - 7 \cdot 17^2 = 2 = 3^2 - 7 \cdot 1^2$ and that $45 \equiv 5$ and $17 \equiv 1 \pmod 2$. We check

$$\frac{45 + 17\sqrt{7}}{3 + \sqrt{7}} = \frac{45 \cdot 3 - 7 \cdot 17 + (17 \cdot 3 - 45)\sqrt{7}}{3^2 - 7} = \frac{16 + 6\sqrt{7}}{2} = 8 + 3\sqrt{7}$$

Indeed $(8, 3)$ is a solution: $8^2 - 7 \cdot 3^2 = 1$.

The hole in the strategy is step 1! We need to show the existence of pairs (x, y) and (X, Y) such that

$$x^2 - dy^2 = X^2 - dY^2$$

and for which $x \equiv X$ and $y \equiv Y$ modulo $m := x^2 - dy^2$. For this we'll invoke the box/pigeonhole principle by placing the infinite set of convergents into finitely many boxes: we first need to create the boxes...

Lemma 2.8. *If $\frac{x}{y}$ is a convergent of $\sqrt{d}$, then*

$$0 < x + y\sqrt{d} < 3y\sqrt{d} \quad \text{and so} \quad \left|x^2 - dy^2\right| < 3\sqrt{d}$$

The proof is a simple exercise. We're now in a position to complete the main result.

Proof of Theorem. If $\frac{x}{y}$ is a convergent of $\sqrt{d}$, the Lemma tells us that $x^2 - dy^2$ is one of the finitely many integers in the interval $(-3\sqrt{d}, 3\sqrt{d})$. Since there are infinitely many convergents, the box principle says that at least one such integer is attained infinitely many times: call this m.

We now have infinitely many pairs of solutions (x_i, y_i) to an equation $x^2 - dy^2 = m$. Modulo m, there are only m^2 distinct pairs of integers. A second application of the box principle says that there must be at least two pairs (indeed infinitely many!) which are mutually congruent.

By the above algebraic steps, we can find at least one solution to Pell's equation in positive integers. By well-ordering, there is a minimal such: this is the fundamental solution. ∎

The fundamental solution to Pell's equation can be pinned down more accurately. Recall that the sequence of quotients in the continued fraction for $\sqrt{d}$ is eventually periodic

$$\sqrt{d} = [c_1; \ldots, c_k, e_1, \ldots, e_l, e_1, \ldots, e_l, \ldots]$$

It can be shown that the convergent $\frac{p_n}{q_n}$ with $n = k + l - 1$ provides the fundamental solution to either $x^2 - dy^2 = \pm 1$. If the result is -1, then computing $(p_n + q_n\sqrt{d})^2$ in the usual way[2] solves $x^2 - dy^2 = 1$. The fundamental solution can therefore be very large when $\sqrt{d}$ has a long period.

Example 2.9. $\sqrt{73} = [8; 1, 1, 5, 5, 1, 1, 16, 1, 1, 5, 5, 1, 1, 16, \ldots]$ has $k + l - 1 = 1 + 7 - 1 = 7$. The seventh convergent is $\frac{1068}{125}$, but this produces

$$1068^2 - 73 \cdot 125^2 = -1$$

The fundamental solution to $x^2 - 73y^2 = 1$ comes from

$$x + \sqrt{73}y = (1068 + 125\sqrt{73})^2 = 2281249 + 267000\sqrt{73}$$

which corresponds to the $1 + 14 - 1 = 14^{\text{th}}$ convergent. Phew!

Exercises 1. Look at the table of convergents of $\sqrt{7}$ in Examples 2.3.

(a) For each of the pairs (p_n, q_n) in the table which produce $p_n^2 - 7q_n^2 = -3$, find their remainders modulo 3.

(b) Find the first two pairs in the table which are mutually congruent modulo 3. Labelling these (x, y) and (X, Y), compute

$$\frac{x + \sqrt{7}y}{X + \sqrt{7}Y}$$

where the numerator is the larger of the two. Which solution to Pell's equation do you obtain?

(c) Now try to be a bit sneakier: by allowing one or more of x, y, X, Y to be *negative*, see if you can produce the fundamental solution to Pell.

2. Prove Lemma 2.8.
(*Hint: recall that every convergent* $\frac{x}{y}$ *satisfies* $\left|\frac{x}{y} - \sqrt{d}\right| < \frac{1}{y^2}$)

[2] This is the $n = k + 2l - 1^{\text{th}}$ convergent.