M246

Number Theory

Workbook 5 (without solutions)

Continued Fractions
(The Pay-Off)

Summer 2013

(originally written and devised by
Trevor Hawkes and Alyson Stibbard;
revised in 2010 by John Cremona)

Aims of these workbooks:

(a) To encourage you to teach yourself mathematics from written material,

(b) To help you develop the art of independent study — working either alone, or co-operatively with other students,

(c) To help you learn a mathematical topic, in this case Number Theory, through calculation and problem-solving.

Copies of this workbook, both with and without solutions, can be found on Mathstuff.

Icons in this Workbook

The 'Section Targets' box contains an idea of what you should aim to get out of the current section. Perhaps you might return to this at the end to evaluate your progress.

Reaching this icon in your journey through the workbook is an indication that an idea should be starting to emerge from the various examples you have seen.

Material here includes reference either to earlier workbooks, or to previous courses such as foundations/Sets and Groups.

A caution. Watch your step over issues involved here.

Are You Ready?

To understand the material and do the problems in each section of this workbook, you will need to be on good terms with:

Section 1: • The Quadratic Formula
Section 2: • Linear Dependence

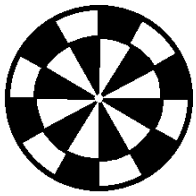
Note: You will need a pocket calculator for some of the questions in the workbooks, and are encouraged to use one for this purpose and to experiment with results and ideas in the course. Calculators are NOT needed and are NOT allowed in tests or in the examination.

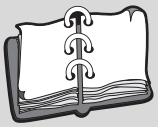
These workbooks were orginally written and devised by *Trevor Hawkes and and Alyson Stibbard*. *Ben Carr* designed the LaTeX template and *Rob Reid* converted their drafts into elegant print. Over the years, other lecturers and students have corrected a number of typos, mistakes and other infelicities. In 2010 *John Cremona* made some substantial revisions.

Send corrections, ask questions or make comments at the module forum. You can join the MA246 forum by going to `http://forums.warwick.ac.uk/wf/misc/welcome.jsp` and signing in, clicking the *browse* tab, and then following the path: Departments > Maths > Modules > MA2xx modules > MA246 Number Theory.

1 Periodic Continued Fractions - the dénouement

Section Targets We left the story of periodic continued fractions unfinished at the end of Workbook 4. At that stage we had perfectly described those CFs whose periodicity begins without delay – the *purely periodic* continued fractions, as we called them.
Our aim in this section is to characterise the real numbers that have general periodic continued fractions, delay included. The answer turns out to be very simple: they are just irrational roots of quadratic equations (*quadratic irrationals* as we will call them); with delay, the "reduced" requirement falls away.





Recall
We proved in Section 3 of Workbook 4 that a real number α has a purely periodic CF iff it is a reduced quadratic irrational, that is to say, an irrational root of a quadratic equation satisfying $\alpha > 1$ and $-1 < \alpha' < 0$ where α' is the conjugate of α.

(1.1) Questions on Quadratic Irrationals

(a) Let $\alpha = \frac{2+\sqrt{5}}{3}$. What is the conjugate α' of α?

(b) Find the rational numbers $\alpha + \alpha'$ and $\alpha\alpha'$.

(c) Write down a quadratic equation with integer coefficients satisfied by α.

(d) Find rational numbers R and S such that

$$\beta = \frac{1+6\alpha}{2-3\alpha} = R + S\sqrt{5}\,.$$

Hint: you can do this one directly, but a more general method would be to multiply top and bottom by $2 - 3\alpha'$ and use the previous part.

(e) Find a quadratic relation with integer coefficients which has β as a root.

The Quadratic Formula
The two roots of ax^2+bx+c are

$$\alpha, \alpha' = \frac{-b \pm \sqrt{b^2-4ac}}{2a}.$$

They satisfy $\alpha+\alpha' = -b/a$ and $\alpha\alpha' = c/a$.

Definition
A *quadratic irrational* is a number satisfying a quadratic equation with integer coefficients. Quadratic irrationals have the form

$$\frac{B \pm \sqrt{D}}{C}$$

where B is an integer, C and D are natural numbers and D is not a perfect square.

Observation
Since α is irrational, the real numbers 1 and α are linearly independent over $\mathbb{Q}$, and so are 1 and α'. Hence, for rational C, D,

$$\begin{aligned} C + D\alpha = 0 &\iff C = D = 0 \\ &\iff C + D\alpha' = 0. \end{aligned}$$

Answers to (1.1)

(a)

(b)

(c)

(d)

(e)

(1.2) Lemma *Let α be a quadratic irrational, and let A, B, C and D be rational numbers such that $AD \neq BC$ (in particular, C and D are not both zero). Then the real number*

$$\beta = \frac{A+B\alpha}{C+D\alpha}$$

is also a quadratic irrational.

Non-zero Denominator
The denominator of (1.a) is the product of two non-zero real numbers (see the previous side comment) and is therefore non-zero.

(1.3) Question on the proof of Lemma 1.2
Fill in the details of the following outline proof of Lemma 1.2.

(a) Show that $\alpha + \alpha'$ and $\alpha\alpha'$ are rational numbers.

(b) Multiply the numerator and denominator of β by the non-zero number $C + D\alpha'$ to get

$$\beta = \frac{(A + B\alpha)(C + D\alpha')}{(C + D\alpha)(C + D\alpha')}\,. \qquad (1.a)$$

and show that the denominator of (1.a) is a non-zero rational and that the numerator equals

$$AC+AD(\alpha+\alpha')+BD\alpha\alpha'+(BC-DA)\alpha = R+S\alpha$$

with $R, S \in \mathbb{Q}$ and $S \neq 0$.

(c) Deduce that $\beta = X+Y\sqrt{d}$ with $X, Y \in \mathbb{Q}$, $Y \neq 0$, and d equal to the discriminant of α.

Out in the Wash
Notice from this proof that α and β have the same discriminant D (up to a square factor). We will use this later.
In fact this proof shows that for any quadratic irrational α, the set

$$\mathbb{Q}(\alpha) = \{x + y\alpha \mid x, y \in \mathbb{Q}\}$$

is closed under all the arithmetic operations (except for division by zero, of course), so forms a *field*. Such a field is called a *real quadratic field*.

Answer to (1.3)

(a)

(b)

(c)

Bar Time
Don't forget the meaning of a bar over the periodic cycle of partial quotients. The notation is defined in Workbook 4.

(1.4) Corollary *Let β be a real number represented by a periodic continued fraction, say*

$$\beta = d_0, d_1, \ldots, d_r, \overline{q_0, q_1, \ldots, q_t}\,.$$

Then β is a quadratic irrational.

Proof. Set $\alpha = \overline{q_0, q_1, \ldots, q_t}$. Since α is purely periodic, it is a quadratic irrational by Theorem 3.10(a) in Workbook 4. Now

$$\beta = d_0 + \frac{1}{d_1 +} \cdots \frac{1}{d_r + \dfrac{1}{\alpha}} = \frac{[d_0, d_1, \ldots, d_r, \alpha]}{[d_1, d_2, \ldots, d_r, \alpha]} = \frac{A_r\alpha + A_{r-1}}{B_r\alpha + B_{r-1}}$$

where $\frac{A_{r-1}}{B_{r-1}}$ and $\frac{A_r}{B_r}$ are the convergents of $d_0 + \frac{1}{d_1+} \cdots \frac{1}{d_r+} \cdots$. By proposition 2.4 in Workbook 4 we have

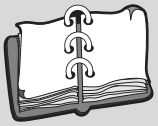
$$A_rB_{r-1} - A_{r-1}B_r = \pm 1$$

and so by Lemma 1.2 our β, like α, is a quadratic irrational. $\square$.

Thus far in this section we have shown that periodic CFs represent quadratic irrational numbers. To round off the story, it remains to show that all quadratic irrationals are represented by periodic CFs.

TAKE NOTE

For the rest of this section α will denote an arbitrary quadratic irrational number.



Reference
Equation (1.b) appears in Workbook 4 as Equation (2.h).

Carrying on
If we develop α as far as the complete quotient α_{n+1}, writing

$$\alpha = d_0 + \frac{1}{d_1+} \cdots \frac{1}{d_n+} \frac{1}{\alpha_{n+1}},$$

and then develop α_{n+1} as

$$\alpha_{n+1} = q_0 + \frac{1}{q_1+} \frac{1}{q_2+} \cdots,$$

we obtain the CF for α by joining the two bits together like this:

$$\alpha = d_0 + \frac{1}{d_1+} \cdots \frac{1}{d_n+} \frac{1}{q_0+} \frac{1}{q_1+} \cdots.$$

Using the recursive procedure

$$\begin{aligned} \alpha &= q_0 + \frac{1}{\alpha_1} \qquad (\alpha_1 > 1) \\ \alpha_1 &= q_1 + \frac{1}{\alpha_2} \qquad (\alpha_2 > 1) \\ \alpha_2 &= \ldots \end{aligned}$$

(repeatedly taking the integral part of α_i to find q_i and upending the fractional part to find α_{i+1}), we obtain the infinite sequence of complete quotients $\alpha_0(=\alpha), \alpha_1, \ldots, \alpha_{n+1}, \ldots$ related by the equation

$$\alpha = \frac{[q_0, q_1, \ldots, q_n, \alpha_{n+1}]}{[q_1, q_2, \ldots, q_n, \alpha_{n+1}]} = \frac{A_n \alpha_{n+1} + A_{n-1}}{B_n \alpha_{n+1} + B_{n-1}}. \quad (1.b)$$

This equation can be rearranged to make α_{n+1} the subject giving

$$\alpha_{n+1} = \frac{-B_{n-1}\alpha + A_{n-1}}{B_n \alpha - A_n}. \quad (1.c)$$

As we pointed out in the margin during the proof of Lemma (1.2), the complete quotient α_{n+1} is not only another quadratic irrational, but also has the same discriminant (D say) as α. Thus if we substitute $-\sqrt{D}$ wherever it appears in Equation (1.c) we obtain

$$\begin{aligned} \alpha'_{n+1} &= \frac{-B_{n-1}\alpha' + A_{n-1}}{B_n \alpha' - A_n} \\ &= -\frac{B_{n-1}}{B_n} \left(\frac{\alpha' - A_{n-1}/B_{n-1}}{\alpha' - A_n/B_n} \right). \end{aligned} \quad (1.d)$$

Our aim will be to find an n such that

$$-1 < \alpha'_{n+1} < 0 \quad (1.e)$$

for then α_{n+1} will be a *reduced* quadratic irrational and will have a purely periodic continued fraction, by Theorem 3.10. From this point on, the continued fraction development for α will then be periodic, which is what we want to show.
To see that (1.e) is eventually satisfied, it is just a matter of staring carefully at Equation (1.d). This equation can be rewritten:

$$\alpha'_{n+1} = -\frac{B_{n-1}}{B_n} \left(\frac{\alpha' - \alpha + (\alpha - A_{n-1}/B_{n-1})}{\alpha' - \alpha + (\alpha - A_n/B_n)} \right). \quad (1.f)$$

(1.5) Question to focus on Equation (1.f)

(a) Show that $\alpha - \alpha' \neq 0$.

(b) Find the chapter and verse in Workbook 4 for the following facts:

(i) $0 < B_1 < \ldots < B_{n-1} < B_n < \ldots$.

(ii) $\lim_{n\to\infty} \left(\alpha - \frac{A_n}{B_n}\right) = 0$.

(iii) $\alpha - \frac{A_n}{B_n}$ is positive when n is even and negative when n is odd.

Answers to (1.5)

(a)

(b)

(1.6) Questions leading to a proof that α_{n+1} is reduced for some n.

Suppose throughout that $\alpha' - \alpha > 0$.

(a) Show that there exists a natural number N such that both of the following conditions are satisfied:

(i) $0 > \alpha - \frac{A_{N-1}}{B_{N-1}} > -\frac{1}{2}(\alpha' - \alpha)$, and

(ii) $\alpha - \frac{A_N}{B_N} > 0$.

(b) Setting $\beta = \frac{\alpha' - \alpha + (\alpha - A_{N-1}/B_{N-1})}{\alpha' - \alpha + (\alpha - A_N/B_N)}$ show that $0 < \beta < 1$.

(c) Conclude that $-1 < \alpha'_{N+1} < 0$.

Answers to (1.6)

(a)

(b)

(c)

In your answer to (1.6) you have shown that α_{N+1} is reduced on the assumption that $\alpha' - \alpha > 0$. In the event that $\alpha - \alpha' > 0$, a similar argument applied to

$$\frac{\alpha - \alpha' + (-\alpha + A_{N-1}/B_{N-1})}{\alpha - \alpha' + (-\alpha + A_N/B_N)}$$

yields a value for N for which this expression lies between 0 and 1, and as before we conclude that

$$-1 < \alpha'_{N+1} < 0$$

for this value of N.
Thus we have proved that all quadratic irrationals eventually have a complete quotient that is reduced. Therefore they have periodic continued fractions. Putting this together with Corollary (1.4), we reach the stated goal of this section.

(1.7) Theorem *A real number has a periodic continued fraction if and only if it is an irrational root of a quadratic equation with integer coefficients.*

To practice the ideas of Section 1 you will find some concluding exercises below.

(1.8) Concluding Exercises

(a) If D is not a perfect square, set $q_0 = [\sqrt{D}]$. Show that $q_0 - \sqrt{D} \in (-1, 0)$ and deduce that $q_0 + \sqrt{D}$ has a purely periodic continued fraction.

(b) Prove that $\sqrt{D} = q_0, \overline{q_1, q_2, \ldots, q_t, 2q_0}$ for some t. [Hint: Use Part (a).] Show further that $q_t = q_1$, $q_{t-1} = q_2$, $q_{t-2} = q_3$, and so on. In other words, that the sequence $q_1, q_2, \ldots, q_t$ is unchanged when written in reverse order. [Hint: Consider Question 3.6 in Workbook 4.]

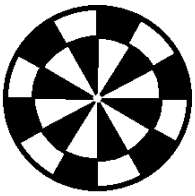
(c) Let n be a natural number. Prove that the continued fraction representation (i) for $\sqrt{n^2+1}$ is $n, \overline{2n}$; (ii) for $\sqrt{n^2+2}$ is $n, \overline{n, 2n}$; and (iii) for $\sqrt{n^2+2n}$ is $n, \overline{1, 2n}$.

(d) Use Part (c) to find a rational approximation to $\sqrt{15}$ that is accurate to four decimal places.

Summary of Section 1

Our main achievement was to characterise real numbers with periodic continued fractions as quadratic irrationals (QIs). To prove that periodic CFs represent QIs we needed the fact that if α is a QI, then so is $\frac{A\alpha+B}{C\alpha+D}$, provided $AD \neq BC$. In the reverse direction, we proved that eventually one of the complete quotients, α_n, of α has a conjugate in the interval $(-1, 0)$. This ensures that α_n is reduced and therefore has a purely periodic CF. The CF for α then becomes periodic from the nth partial quotient on.

2 Pell's Equation



Addition Impossible
What is

$$\left(\frac{1}{1+}\frac{1}{2+}\frac{1}{3}\right)+\left(\frac{1}{3+}\frac{1}{3}\right)?$$

Diophantine Equations
These are equations where the focus is on *integer* or *rational* solutions. They are named after Diophantine of Alexandria who lived in the third century AD and wrote a 13 volume work called *Arithmetica*, only six volumes of which survive. In these we find the first consistent use of mathematical notation and a systematic study of solutions of equations in integers. The most famous Diophantine Equation is

$$x^n + y^n = z^n$$

which Fermat claimed, in the margin of his copy of *Arithmetica*, has no solutions when $n \geq 3$. This was finally proved by Andrew Wiles (who subsequently received an honorary degree from Warwick!) in the 1990's.

Section Targets
We now ask: "What are continued fractions good for?" They are poor substitutes for decimal notation when it comes to basic arithmetic - try the sum on the left without reverting to standard rational or decimal notation, for example. However, continued fractions reveal important properties of numbers that are hidden in other representations, and they sometimes provide an explicit construction for the solution to a problem where other methods show at best merely the existence of a solution. One example of this is the famous Diophantine equation known (erroneously - see `http://en.wikipedia.org/wiki/Pell's_equation`) as Pell's Equation

$$x^2 - Dy^2 = 1 \qquad (2.a)$$

where D is a natural number which is not a perfect square. Our aim in this section is to show how to use continued fractions to construct infinitely many solutions to equation (2.a).

(2.1) Questions about Equation (2.a)

(a) Prove that if D is a perfect square then Equation (2.a) has no solutions with $x, y \in \mathbb{Z}$ and $y \neq 0$.

(b) By trial and error, find two positive integer solutions to Equation (2.a) when $D = 2$.

Answers to (2.1)

(a)

(b)

TAKE NOTE

The Pell Convention

In any discussion of Pell's Equation we make the unspoken assumption that the natural number D is *not* a perfect square.

The key to finding solutions to Pell's Equation (2.a) is to study the continued fraction for $\sqrt{D}$. We will show that one of its convergents

$$A_n/B_n$$

satisfies $A_n^2 - DB_n^2 = 1$. In fact, this holds for infinitely many of the convergents of $\sqrt{D}$, and each one of them yields a solution to Pell's Equation.

(2.2) Question on the CF for $\sqrt{D}$

(a) Let D be a natural number which is not a perfect square. Set $q_0 = \left[\sqrt{D}\right]$ the integer part of $\sqrt{D}$, and set $\alpha = q_0 + \sqrt{D}$. Show that α is a reduced quadratic irrational and therefore has a purely periodic continued fraction

$$\overline{2q_0, q_1, ..., q_t}\,.$$

(b) Deduce that $\sqrt{D} = q_0\,,\ \overline{q_1\,,\ \cdots\,,\ q_t\,,\ 2q_0}\,.$

Answer to (2.2)

(a)

(b)

Ring a Bell?
Compare Equation 2.b with Equation 3.d in Workbook 4.

From (2.2) we see that

$$\sqrt{D} = \alpha - q_0 = q_0 + \frac{1}{q_1+}....\frac{1}{q_t+}\frac{1}{\alpha}$$

and therefore

$$\sqrt{D} = \frac{\alpha A_t + A_{t-1}}{\alpha B_t + B_{t-1}} \qquad (2.b)$$

where $A_t = [q_0, q_1, ..., q_t]$, etc.

(2.3) Question on Equation 2.b. By multiplying through by $\alpha B_t + B_{t-1}$ and substituting $\alpha = q_0 + \sqrt{D}$, show that you can rewrite Equation (2.b) in the form $X + Y\sqrt{D} = 0$, where X and Y are the following rational numbers:

$$\begin{aligned} X &= B_t D - A_t q_0 - A_{t-1} \\ Y &= B_t q_0 + B_{t-1} - A_t \end{aligned} \qquad (2.c)$$

Answer to (2.3)

Familiar Argument

Since 1 and $\sqrt{D}$ are independent over $\mathbb{Q}$, the equation

$$X + Y\sqrt{D} = 0$$

implies $X = Y = 0$.

Since $\sqrt{D}$ is irrational, we conclude that $X = Y = 0$, and therefore

$$\begin{aligned} A_{t-1} &= B_t D - A_t q_0 \\ B_{t-1} &= A_t - B_t q_0 \end{aligned} \qquad (2.d)$$

We now substitute for A_{t-1} and B_{t-1} in Equation 2.d of Workbook 4 to obtain

$$\begin{aligned} (-1)^{t+1} &= A_t B_{t-1} - B_t A_{t-1} \\ &= A_t(A_t - B_t q_0) - B_t(B_t D - A_t q_0) \\ &= A_t^2 - D B_t^2 \end{aligned}$$

HEY PRESTO! If t is odd, then $(-1)^{t+1} = 1$, and we have found a solution

$$x = A_t\,, \qquad y = B_t$$

to Pell's Equation.

(2.4) Questions to test this claim

(a) Show that $3 + \sqrt{14} = \overline{6, 1, 2, 1}$. Deduce that $\sqrt{14} = 3, \overline{1, 2, 1, 6}$.

(b) For $0 \leq n \leq 3$ compute A_n, B_n, the convergent A_n/B_n and the value of $A_n^2 - 14B_n^2$. [Use the tabular layout as in Workbook 4.]

Answer to (2.4)

(a)

(b)

The Period of $\sqrt{D}$
The way we have labelled the CF for $\sqrt{D}$ as

$$q_0, \overline{q_1, \ldots, q_t, 2q_0}$$

means that the periodic cycle contains $t+1$ terms.

We still lack a solution when t is even. Fortunately, the same idea will work if we go one complete cycle further along the continued fraction for $\sqrt{D}$ thus:

$$\begin{aligned}\sqrt{D} &= q_0 + \frac{1}{q_1+} \cdots \frac{1}{q_t+} \frac{1}{2q_0+} \frac{1}{q_1+} \cdots \frac{1}{q_t+} \frac{1}{\alpha} \\ &= \frac{A_{2t+1}\alpha + A_{2t}}{B_{2t+1}\alpha + B_{2t}}.\end{aligned}$$

Starting from this equation rather than Equation 2.b, we can follow the same sequence of algebraic steps as before to conclude that

$$A_{2t+1}^2 - DB_{2t+1}^2 = (-1)^{2t+2} = 1$$

and once more we have found a solution for Pell's Equation, even when t is odd. We now summarise what we have proved.

Counting from zero
Since the first convergent A_0/B_0 for a continued fraction

$$q_0 + \frac{1}{q_1+} \frac{1}{q_2+} \cdots$$

is suffixed with a zero, the convergent A_n/B_n, although labelled with n, is in fact the $(n+1)$st on the list.

(2.5) Theorem *Let D be a natural number which is not a perfect square. Then*

$$\sqrt{D} = q_0\,,\ \overline{q_1\,,\ \cdots\,,\ q_t\,,\ 2q_0}$$

for some $t \geq 1$, and if A_n/B_n denotes the $(n+1)$st convergent of this periodic continued fraction, we obtain the following solutions to Pell's Equation $x^2 - Dy^2 = 1$:

$$\begin{aligned}(x, y) = (A_t, B_t) \quad &\text{if } t \text{ is odd;} \\ (x, y) = (A_{2t+1}, B_{2t+1}) \quad &\text{if } t \text{ is even.}\end{aligned}$$

(2.6) Questions to test this Theorem when t is even Recall from Workbook 4 Question (3.2)(d) that $\sqrt{13} = 3\,,\ \overline{1\,,\ 1\,,\ 1\,,\ 1\,,\ 6}$. Calculate A_n, B_n, and $A_n^2 - 13B_n^2$ for $n \leq 9$.

Pell in ancient Greece

Pell's Equation has a long history. *The Cattle Problem of Archimedes* (said to have been proposed by Archimedes as a challenge to Eratosthenes) involves 8 unknowns involving different kinds of cattle, together with two extra conditions that certain numbers are not perfect squares. The problem boils down to solving the equation

$$x^2 - 4729494y^2 = 1\,.$$

The least solution (given by Amthor in 1880) involves a number x with 41 digits. The existence of this problem raises the question whether Pell's Equation was known to the mathematicians of antiquity.

Answer to (2.6)

Mysterious -1

It is an unsolved problem to determine for exactly which natural numbers D there is a solution to the negative Pell equation!

(2.7) Turning a negative into a positive

(a) Verify the identity

$$(x^2 + Dy^2)^2 - D(2xy)^2 = (x^2 - Dy^2)^2.$$

(b) Deduce that if (x_0, y_0) give a solution to the "negative Pell equation"

$$x^2 - Dy^2 = -1$$

then $(x, y) = (x_0^2 + Dy_0^2, 2x_0y_0)$ is a solution to the usual Pell equation $x^2 - Dy^2 = +1$.

(c) Use this and the working of the previous question to solve the Pell equation with a lot less work.

Answers to (2.7)

(a)

(b)

(c)

(2.8) Negative practice Find the CF expansion of $\sqrt{10}$. By writing down the first few convergents (you will not need very many!) first solve the negative Pell equation $x^2 - 10y^2 = -1$ and then the Pell equation itself.

Answer to (2.8)

Large numbers

Notice that the solution you have obtained to Pell's Equation for $D = 13$ in Question 2.6 is already large relative to D (if your solution is between 500 and 1,000 you have found the smallest positive solution). The size of the smallest solution generally bears little relation to the size of D. For example, the smallest solution for $D = 60$ is $x = 31$ and $y = 4$. For $D = 61$ the smallest solution is $x = 17663319049$ and $y = 226153980$ while for $D = 62$ the smallest solution is $x = 63$ and $y = 8$.

There are two effective ways of generating infinitely many solutions. One is to use the trick we used to prove Theorem 2.5 in the case when t is even. The same argument shows that the convergents that correspond to the end of every periodic cycle yield solutions when t is odd, whereas the alternate ones yield solutions when t is even.

The second method is to use a known solution to generate new ones. In a way similar to the trick we used to turn negative solutions into positive ones, we can generate new positive solutions from a given one, as illustrated in the following question.

(2.9) Questions on new solutions for old

(a) Multiply out

$$(x_1 + y_1\sqrt{D})(x_2 + y_2\sqrt{D}),$$

giving the result in the form $x_3+y_3\sqrt{D}$ with x_3, y_3 expressed in terms of x_1, y_1, x_2, y_2 and D (with no square roots).

(b) Deduce that if (x_1, y_1) and (x_2, y_2) are both solutions to the Pell equation $x^2 - Dy^2 = 1$, then so is (x_3, y_3).

(c) Let $\alpha = x + y\sqrt{D}$, where (x, y) is a nontrivial solution to the Pell equation. By induction on n, show that for all $n \geq 1$,

$$\alpha^n = P_n + Q_n\sqrt{D}$$

where $P_n, Q_n \in \mathbb{Z}$ and $P_n^2 - DQ_n^2 = 1$. [So every (P_n, Q_n) is a solution to Pell.]

(d) What does this say about the number of solutions to the Pell equation?

Pell in India

Versions of his famous equation were known to mathematicians in India more than 1000 years before they reappeared in Europe. For instance, in the 7th century AD, Brahmagupta gave his definition of a mathematician as "someone who could solve

$$x^2 - 92y^2 = 1$$

within a year". If you would like to measure yourself against this yardstick, bear in mind that 7th century mathematicians did not have electronic calculators.

Answer to (2.9)

(a)

(b)

(c)

(d)

Pell was innocent

Pell actually had very little to do with his equation. Euler is responsible for the erroneous attribution; he came across Pell's name in Wallis's *Opera Mathematica* and mistakenly connected it with the famous equation.

(2.10) Proposition *Let D be a natural number which is not a perfect square. If A and B are natural numbers satisfying Pell's Equation $x^2 - Dy^2 = 1$, then the pairs (P_n, Q_n) defined by*

$$(A + B\sqrt{D})^n = P_n + Q_n\sqrt{D}$$

for $n \geq 1$ are further solutions to Pell's Equation, and are all distinct.

In fact one can show that if we start with the *minimal* solution in positive integers (A, B) then every nontrivial solution has the form $(\pm P_n, \pm Q_n)$ for some $n \geq 1$. And moreover, the continued fraction method will always find this minimal solution! So,

using CFs we have been able to completely solve Pell's Equation.

To establish these additional facts, it is probably better to use a slightly more highbrow viewpoint than we have been. The set of all numbers of the form $x+y\sqrt{D}$ with $x, y \in \mathbb{Z}$ is closed under addition and multiplication, so forms a *ring*, denoted $\mathbb{Z}[\sqrt{D}]$:

$$\mathbb{Z}[\sqrt{D}] = \{x + y\sqrt{D} \mid x, y \in \mathbb{Z}\}.$$

Solutions (x, y) to Pell's equation correspond to $\alpha = x+y\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ which are *units*, whose conjugate $\alpha' = x-y\sqrt{D}$ is also its inverse $1/\alpha$, since $\alpha\alpha' = (x+y\sqrt{D})(x-y\sqrt{D}) = x^2 - Dy^2 = 1$. So our proof that Pell's equation always has infinitely many solutions actually shows that the ring $\mathbb{Z}[\sqrt{D}]$ has infinitely many units. And the facts of the previous paragraph amount to saying that all these units have the form $\pm\alpha_0^n$ with $n \in \mathbb{Z}$, if we take $\alpha_0 = x_0 + y_0\sqrt{D}$ corresponding to the smallest solution to Pell's equation.

Who solved it?

Fermat may have had a general solution but if so he did not let on. He tantalised his contemporaries by issuing challenges to solve ever-more-difficult special cases. Two British mathematicians, John Wallis and his patron Lord Brouncker of Ireland, took up the gauntlet and solved, for instance, the equation

$$x^2 - 313y^2 = 1\,.$$

Subsequently Euler made progress on the general solution using the continued fraction development for $\sqrt{D}$. But it was Lagrange who finally settled the matter when in 1768 he published the first rigorous proof that the convergents of $\sqrt{D}$ provide all the positive solutions.

(2.11) Concluding Exercises

(a) Show that the solutions $x = P_n$ and $y = Q_n$ to Pell's Equation $x^2 - Dy^2 = 1$ described in Proposition 2.10 are strictly increasing in the sense that $A = P_1 < P_2 < P_3 < P_4 \ldots$ and $B = Q_1 < Q_2 < Q_3 < Q_4 \ldots$.

(b) Substitute $y = 1, 2, 3, \cdots$ successively into the expression Dy^2+1 until you reach a perfect square for (i) $D = 7$, (ii) $D = 19$, and (iii) $D = 39$. This is a slow but systematic method of finding the smallest positive integers x and y satisfying Pell's Equation.

(c) Use the previous question and Proposition 2.10 to find an integral solution to the equation $x^2 - 39y^2 = 1$ with $x \geq 10,000$.

(d) Let N be a natural number such that the equation

$$x^2 - Dy^2 = N \qquad (2.f)$$

has an integral solution (here, as usual, D is a natural number and not a perfect square). Use Proposition 2.10 to prove that Equation (2.f) then has infinitely many solutions.

Summary of Section 2

The thrust of this section was to find natural numbers x and y satisfying Pell's Equation $x^2 - Dy^2 = 1$, where D is a natural number which is not the square of another natural number. The key result is that a solution $x = A_n$ and $y = B_n$ can always be found among the first $2t+2$ convergents A_n/B_n of the periodic continued fraction for $\sqrt{D}$, where $t+1$ is the length of the period. For $n = 2, 3, \cdots$, any given solution $x = A$ and $y = B$ gives rise to new solutions $x = P$ and $y = Q$ when the power $\left(A + B\sqrt{D}\right)^n$ is expanded and arranged in the form $P + Q\sqrt{D}$ with P and Q natural numbers.