Chakravala - a modern Indian method

B.Sury

Indian Statistical Institute
Bangalore, India
sury@isibang.ac.in

IISER Pune, India
Lecture on October 18, 2010

Weil Unveiled

“What would have been Fermat’s astonishment if some missionary, just back from India, had told him that his problem had been successfully tackled there by native mathematicians almost six centuries earlier?” - André Weil.

Weil was talking about a 1657 challenge of Fermat “*to the English mathematicians and all others*”.
Writing to his friend Frenicle, he posed the problem of finding a solution of $x^2 - Ny^2 = 1$ “*pour ne vous donner pas trop de peine*” like $N = 61, 109$.

Cut back to 1150 A.D. when Bhaskara II gave the explicit solutions

$$1766319049^2 - 61(226153980)^2 = 1$$

$$158070671986249^2 - 109(15140424455100)^2 = 1!$$

Weil’s comment was because - unbeknownst to Fermat - the ancient Indians had not merely given a solution but they had gone all the way!

Brahmagupta, Jayadeva, Bhaskara

Jayadeva (11th century) and Bhaskara had given the finishing touches to a wonderful algorithm called the ‘Chakravala’ which finds all solutions to $x^2 - Ny^2 = \pm 1$ for any positive integer N!

Indeed, Brahmagupta (598-665) had already solved this equation in 628 A.D. for several values like $N = 83$ and $N = 92$.

Brahmagupta had remarked, “*a person who is able to solve these two cases within a year is truly a mathematician*”’!

Consider a natural number N which is not a perfect square. We are basically interested in integer solutions of the equations

$$x^2 - Ny^2 = 1, x^2 - Ny^2 = -1$$

More generally, suppose
(p, q) is a solution of $x^2 - Ny^2 = m$ and
(r, s) is a solution of $x^2 - Ny^2 = n$. Then

$$(p, q) * (r, s) := (pr + Nqs, ps + qr)$$

is a solution of $x^2 - Ny^2 = mn$.

This ‘composition law’ or ‘samasabhavana’ was discovered by Brahmagupta. This was one of the first instances of a group-theoretic argument.

Observe therefore that if $(p,q),(r,s)$ are positive solutions of $x^2 - Ny^2 = 1$, the Bhavana produces a "larger" solution. In this manner, starting with one nontrivial (that is, $\neq (1,0)$) solution, one obtains infinitely many solutions of this equation.

We shall describe a method known as the "chakravala" method due to Jayadeva, Bhaskara and Narayana from the 11th and 12th centuries which solve this equation. The amazing thing is that the chakravala method produces all solutions! This is what Weil was referring to.
As far as I know, the Indians did not state explicitly that the Chakravala method produces all solutions of the equations $x^2 - Ny^2 = 1$ although they might have even been convinced in their minds that it does. We shall find it convenient to use continued fractions to developed by Lagrange in the 1780's to prove that the Chakravala does give **all** *the solutions. Moreover, it is an algorithm which can easily be implemented on a computer. That is the reason we have called the Chakravala a modern method. Some of the references to consult for more information are :*
(i) 'History of Algebra' by V.S. Varadarajan in TRIM series,
(ii) 'Number theory from Hammurapi to Legendre' by A. Weil,
(iii) 'Theory of Numbers' by Hardy & Wright.

Brahmagupta's shortcuts

For finding a particular solution of $x^2 - Ny^2 = 1$, Brahmagupta devised some shortcuts of the following kind:

Write $(u,v;n)$ to mean $u^2 - Nv^2 = n$. Then,

$$(u,v;\pm 1) \Rightarrow (2u^2 \pm 1, 2uv; 1)$$

$$(u,v;\pm 2) \Rightarrow (u^2 \pm 1, uv; 1)$$

$$(2u,v;4) \Rightarrow (2u^2 - 1, uv; 1)$$

$$(2u+1,v;4) \Rightarrow ((2u+1)(2u^2+2u-1), 2u(u+1)v; 1)$$

$$(2u,v;-4) \Rightarrow (2u^2+1, v; 1)$$

$$(u,v;-4) \Rightarrow (p,q;1)$$

with u odd, $p = \frac{(u^2+2)((u^2+1)(u^2+3)-2)}{2}, q = \frac{uv(u^2+1)(u^2+3)}{2}$.

Examples

$N = 13$**.**
Observing that $11^2 - 13(3)^2 = 4$.
Then, $(11, 3; 4)$ and the 4th shortcut gives $(649, 180; 1)$.

$N = 61$**.**
Observe that $39^2 - 61(5)^2 = -4$.
The last shortcut gives a solution
$x = 1523\frac{(1522)(1524)-2}{2} = 1766319049$
and
$y = \frac{(39)(5)(1522)(1524)}{2} = 226153980$.
This happens to be the smallest solution!

Chakravala algorithm
Let us describe the Chakravala method roughly first. The basic idea is to start with the initial values $p_0 = [\sqrt{N}]$ and $q_0 = 1$ and look at them as solutions of the equation $x^2 = m_0 y^2 = 1$ where $m_0 = p_0^2 - N$. Taking an appropriate x_1 close to $\sqrt{N}$, one has a solution $(x_1, 1)$ of the second equation $x^2 - Ny^2 = x_1^2 - N$. Then, one uses Samasabhavana to get a solution of the equation $x^2 - Ny^2 = m_0(x_1^2 - N)$. Now, the key point is to make the choice of x_1 in such a manner that the resulting solution (p_1', q_1') of $x^2 - Ny^2 = m_0(x_1^2 - N)$ as well as the modulus $x_1^2 - N$ are all multiples of m_0 so that $(p_1'/m_0, q_1'/m_0)$ would be a solution of $x^2 - Ny^2 = m_1$ where $m_1 = (x_1^2 - N)/m_0$.
In this manner, recursively a suitable x_i is so chosen that a solution of a new equation $x^2 - Ny^2 = m_i$ is produced and the hope is that at some finite stage, the modulus $m_k = 1$ and we stop!
Let us describe this more precisely now.

- Start with $p_0 < \sqrt{N} < p_0 + 1$.

- Take $q_0 = 1$ and $m_0 = p_0^2 - N$ (note $m_0 < 0$).

Then, we have $(p_0, q_0; m_0)$.

- Choose $x_1 \equiv -p_0 \mod |m_0|$ and $x_1 < \sqrt{N} < x_1 + |m_0|$.

Note that in forming the solution
$(p_0, q_0) * (x_1, 1) = (p_0 x_1 + N, p_0 + x_1)$ of $(p_0 x_1 + N, p_0 + x_1; m_0(x_1^2 - N))$, the numbers $p_0 x_1 + N, p_0 + x_1, x_1^2 - N$ are all multiples of m_0 and $|x_1^2 - N|$ is as small as possible.

Indeed, $p_0 + x_1 \equiv 0 \bmod m_0$ and
$p_0 x_1 + N \equiv -p_0^2 + N = -m_0 \equiv 0 \bmod m_0$.
Of course, we also have $x_1^2 - N \equiv p_0^2 - N = m_0 \equiv 0 \bmod m_0$.
We have then $(p_1, q_1; m_1)$ where $p_1 = \frac{p_0 x_1 + N}{|m_0|}, q_1 = \frac{p_0 + x_1}{|m_0|}, m_1 = \frac{x_1^2 - N}{m_0}$.
Also $m_1 > 0$ as $x_1^2 - N < 0$ and $m_0 < 0$.
Knowing p_i, q_i, m_i, x_i we shall describe (in that order) $x_{i+1}, m_{i+1}, p_{i+1}, q_{i+1}$ such that $(p_{i+1}, q_{i+1}; m_{i+1})$ holds and stop when (and if!) we reach $m_k = 1$.

Recursive definition

- Suppose $(p_i, q_i; m_i)$ where we assume

$$p_i = \frac{p_{i-1} x_i + N q_{i-1}}{|m_{i-1}|}, q_i = \frac{p_{i-1} + x_i q_{i-1}}{|m_{i-1}|}, m_i = \frac{x_i^2 - N}{m_{i-1}}.$$

Define $x_{i+1} \equiv -x_i \bmod |m_i|$ with $x_{i+1} < \sqrt{N} < x_{i+1} + |m_i|$.
With this choice of x_{i+1},

$$(p'_{i+1}, q'_{i+1}) := (p_i, q_i) * (x_{i+1}, 1) = (p_i x_{i+1} + N q_i, p_i + q_i x_{i+1}).$$

The key point to note is that the choice of the congruence defining x_{i+1} ensures that m_i divides both p'_{i+1} and q'_{i+1} as well as $x_{i+1}^2 - N$:

Indeed
$q'_{i+1} = p_i + q_i x_{i+1} \equiv p_i - q_i x_i \quad mod \ |m_i|$

$$= \frac{p_{i-1} x_i + N q_{i-1} - p_{i-1} x_i - q_{i-1} x_i^2}{|m_{i-1}|} = \frac{q_{i-1}(N - x_i^2)}{|m_{i-1}|} = \pm q_{i-1} m_i.$$

That is, m_i divides q'_{i+1}.
Also, we get $p'_{i+1} \equiv \pm p_{i-1} m_i \equiv 0 \bmod m_i$.
The congruence $x_{i+1}^2 - N \equiv x_i^2 - N \bmod m_i$ ensures the divisibility of $x_{i+1}^2 - N$ by m_i as $m_i m_{i-1} = x_i^2 - N$.
Therefore, we can take $p_{i+1} = \frac{p'_{i+1}}{|m_i|}, q_{i+1} = \frac{q'_{i+1}}{|m_i|}, m_{i+1} = \frac{x_{i+1}^2 - N}{m_i}$.

The name Chakravala

We shall show that each $m_i \in (-2\sqrt{N}, 2\sqrt{N})$. The m_i's will repeat in cycles - hence called chakravala. However, it is not obvious as yet that some $m_k = 1$ but we will prove this later using continued fractions. Moreover, it is not even clear that the p_i, q_i are integers.
Later, we show using continued fractions that these assertions are true.

We now show simultaneously $|x_{i+1}| < \sqrt{N}, |m_i| < 2\sqrt{N}$.

$|m_0| = N - p_0^2 < 2\sqrt{N}$ and $x_1 < \sqrt{N} < x_1 + |m_0|$.
So, $x_1 > \sqrt{N} - |m_0| > \sqrt{N} - 2\sqrt{N} > -\sqrt{N}$.
Inductively, if $|m_i| < 2\sqrt{N}$, then $x_{i+1} < \sqrt{N} < x_{i+1} + |m_i|$ gives $|x_{i+1}| < \sqrt{N}$ as before, and

$$|m_{i+1}| = \frac{|x_{i+1}^2 - N|}{|m_i|} = |\sqrt{N} + x_{i+1}|\frac{|\sqrt{N} - x_{i+1}|}{|m_i|} < 2\sqrt{N}.$$

Formal algorithm summarized

$\boxed{p_0 < \sqrt{N} < p_0 + 1}$ $\boxed{q_0 = 1}$. $\boxed{m_0 = p_0^2 - N}$.
$\boxed{x_1 \equiv -p_0 \bmod |m_0|}$ $\boxed{x_1 < \sqrt{N} < x_1 + |m_0|}$.
$\boxed{p_1 = \frac{p_0x_1+N}{|m_0|}}$ $\boxed{q_1 = \frac{p_0+x_1}{|m_0|}}$ $\boxed{m_1 = \frac{x_1^2-N}{m_0}}$.
$\boxed{x_i \equiv -x_{i-1} \bmod |m_{i-1}|}$ $\boxed{x_i < \sqrt{N} < x_i + |m_{i-1}|}$
$\boxed{p_i = \frac{p_{i-1}x_i+Nq_{i-1}}{|m_{i-1}|}}$ $\boxed{q_i = \frac{p_{i-1}+x_iq_{i-1}}{|m_{i-1}|}}$ $\boxed{m_i = \frac{x_i^2-N}{m_{i-1}}}$.

Example $N = 13$

Then $p_0 = 3 < \sqrt{13} < 4$, $q_0 = 1, m_0 = p_0^2 - 13 = -4$.
Therefore $\boxed{(p_0, q_0; m_0) = (3, 1; -4)}$.
$x_1 \equiv -p_0 = -3(4)$ and $x_1 < \sqrt{13} < x_1 + 4$ gives $x_1 = 1$.
$p_1 = \frac{p_0x_1+13}{|m_0|} = 4, q_1 = \frac{p_0+x_1}{|m_0|} = 1, m_1 = \frac{x_1^2-13}{m_0} = 3$.
Therefore, $\boxed{(p_1, q_1; m_1) = (4, 1; 3)}$ and $\boxed{x_1 = 1}$.
Now $x_2 \equiv -4 \bmod 3$ and $x_2 < \sqrt{13} < x_2 + 3$ give $x_2 = 2$.
$x_2 = 2, p_1 = 4, q_1 = 1, m_1 = 3$.
So $p_2 = \frac{p_1x_2+13q_1}{|m_1|} = 7, q_2 = \frac{p_1+q_1x_2}{|m_1|} = 2, m_2 = \frac{x_2^2-13}{m_1} = -3$.
Therefore, $\boxed{(p_2, q_2; m_2) = (7, 2; -3)}$ and $\boxed{x_2 = 2}$.
Now $x_3 \equiv -2 \bmod 3$ and $x_3 < \sqrt{13} < x_3 + 3$ gives $x_3 = 1$.
So $p_3 = (7 + 26)/3 = 11, q_3 = (7 + 2)/3 = 3, m_3 = (1^2 - 13)/(-3) = 4$.
Therefore, $\boxed{(p_3, q_3; m_3) = (11, 3, 4)}$ and $\boxed{x_3 = 1}$.
$x_4 \equiv -1 \bmod 4$ and $x_4 < \sqrt{13} < x_4 + 4$ gives $x_4 = 3$.
So $p_4 = (33 + 39)/4 = 18, q_4 = (11 + 9)/4 = 5, m_4 = (3^2 - 13)/(4) = -1$.
Therefore, $\boxed{(p_4, q_4; m_4) = (18, 5; -1)}$ and $\boxed{x_4 = 3}$.
$x_5 \equiv -3 \bmod 1$ and $x_5 < \sqrt{13} < x_5 + 1$ gives $x_5 = 3$.

So $p_5 = (54+65)/1 = 119, q_5 = (18+15)/1 = 33, m_5 = (3^2-13)/(-1) = 4$.
Therefore, $\boxed{(p_5, q_5; m_5) = (119, 33; 4)}$ and $\boxed{x_5 = 3}$.
$x_6 \equiv -3 \bmod 4$ and $x_6 < \sqrt{13} < x_6 + 4$ gives $x_6 = 1$.
So $p_6 = (119+429)/4 = 137, q_6 = (119+33)/4 = 38, m_6 = (1^2-13)/4 = -3$.
Therefore, $\boxed{(p_6, q_6; m_6) = (137, 38; -3)}$ and $\boxed{x_6 = 1}$.
$x_7 \equiv -1 \bmod 3$ and $x_7 < \sqrt{13} < x_7 + 3$ gives $x_7 = 2$.
So $p_7 = (274+494)/3 = 256, q_7 = (137+76)/3 = 71, m_7 = (2^2-13)/(-3) = 3$.
Therefore, $\boxed{(p_7, q_7; m_7) = (256, 71; 3)}$ and $\boxed{x_7 = 2}$.
$x_8 \equiv -2 \bmod 3$ and $x_8 < \sqrt{13} < x_8 + 3$ gives $x_8 = 1$.
So $p_8 = (256+923)/3 = 393, q_8 = (256+71)/3 = 109, m_8 = (1^2-13)/3 = -4$.
Therefore, $\boxed{(p_8, q_8; m_8) = (393, 109; -4)}$ and $\boxed{x_8 = 1}$.
$x_9 \equiv -1 \bmod 4$ and $x_9 < \sqrt{13} < x_9 + 4$ gives $x_9 = 3$.
So $p_9 = (1179+1417)/4 = 649, q_9 = (393+327)/4 = 180, m_9 = (3^2-13)/(-4) = 1$.
Therefore, $\boxed{(p_9, q_9; m_9) = (649, 180; 1)}$ and $x_9 = 3$.
Voila!

(ii) $N = 67$.
$(48842, 5967; 1)$.

(iii) $N = 61$.
$(1766319049, 226153980; 1)$.

(iv) $N = 103$.
$(227528, 22419; 1)$.

(v) $N = 97$.
$(62809633, 6377352; 1)$.

Properties of the p_i's,q_i's

(I) $p_{i+1}q_i - q_{i+1}p_i = (-1)^i$.

(II) $0 < p_0 < p_1 < \cdots, 0 < q_1 < q_2 < \cdots$

(III) $a_{i+1} = \frac{x_{i+1}+x_i}{|m_i|}$ are positive integers satisfying

$$p_{i+1} = a_{i+1}p_i + p_{i-1}$$

$$q_{i+1} = a_{i+1}q_i + q_{i-1}$$

Proof of $p_{i+1}q_i - q_{i+1}p_i = (-1)^i$.
As $m_i m_{i+1} = x_{i+1}^2 - N < 0, m_0 < 0$, $\frac{m_i}{|m_i|} = (-1)^{i+1}$.

$$\begin{pmatrix} x_{i+1} & N \\ 1 & x_{i+1} \end{pmatrix} \begin{pmatrix} p_i \\ q_i \end{pmatrix} = \begin{pmatrix} p'_{i+1} \\ q'_{i+1} \end{pmatrix} = \begin{pmatrix} p_{i+1}|m_i| \\ q_{i+1}|m_i| \end{pmatrix}.$$

Multiplying on the left by $(q_i, -p_i)$, we get

$$\begin{pmatrix} q_i & -p_i \end{pmatrix} \begin{pmatrix} x_{i+1} & N \\ 1 & x_{i+1} \end{pmatrix} \begin{pmatrix} p_i \\ q_i \end{pmatrix}$$

$$= \begin{pmatrix} q_i & -p_i \end{pmatrix} \begin{pmatrix} p_{i+1}|m_i| \\ q_{i+1}|m_i| \end{pmatrix} = (q_i p_{i+1} - p_i q_{i+1})|m_i|.$$

The LHS $q_i^2 N - p_i^2 = -m_i$; so, $p_{i+1}q_i - q_{i+1}p_i = (-1)^i$.

Note that (II) follows from (III) inductively; the beginning inequalities $p_1 > p_0 > 0, q_1 > 0$ are accomplished as follows.
Recall $p_1 = \frac{p_0 x_1 + N}{|m_0|} = \frac{p_0 x_1 + p_0^2 + |m_0|}{|m_0|} = 1 + p_0 \frac{p_0 + x_1}{|m_0|} = 1 + p_0 q_1$.
If we show that $q_1 > 0$, then it would follow that $p_1 > p_0$.
As $x_1 > \sqrt{N} - |m_0|$ and $1 > \sqrt{N} - p_0$, we have

$$q_1 = \frac{p_0 + x_1}{|m_0|} > \frac{p_0 + \sqrt{N} - |m_0|}{|m_0|} = \frac{1}{\sqrt{N} - p_0} - 1 > 0$$

Proof of (III)
We leave the easy inductive proof of the fact that $a_{i+1} = \frac{x_{i+1} + x_i}{|m_i|}$ are integers satisfying

$$p_{i+1} = a_{i+1} p_i + p_{i-1}$$

$$q_{i+1} = a_{i+1} q_i + q_{i-1}$$

We prove that a_i's are positive as follows.
As $x_i < \sqrt{N} < x_i + |m_{i-1}|$, we have

$$|m_{i-1}| > \sqrt{N} - x_i = \frac{N - x_i^2}{\sqrt{N} + x_i} = \frac{-m_i m_{i-1}}{\sqrt{N} + x_i} = \frac{|m_i m_{i-1}|}{\sqrt{N} + x_i}.$$

Hence $\sqrt{N} + x_i > |m_i|$ and so,

$$a_{i+1} = \frac{x_i + x_{i+1}}{|m_i|} > \frac{|m_i| - \sqrt{N} + x_{i+1}}{|m_i|} > 0.$$

Continued fractions - a crash course

A simple continued fraction is
$l = a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots := \lim_{n\to\infty}(a_0 + \frac{1}{a_1+}\frac{1}{a_2+}\cdots\frac{1}{a_n})$
One writes symbolically as $l = [a_0; a_1, a_2, \cdots]$.
The successive quotients

$$\frac{p_0}{q_0} := \frac{a_0}{1}, \frac{p_1}{q_1} = \frac{a_0a_1+1}{a_1} = a_0 + \frac{1}{a_1}, \cdots$$

are called the convergents to the continued fraction. Note

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \cdots < l < \frac{p_1}{q_1} < \frac{p_3}{q_3} < \cdots$$

Inductively

$$p_{n+1} = a_{n+1}p_n + p_{n-1}$$

$$q_{n+1} = a_{n+1}q_n + q_{n-1}$$

To see these, note that p_{n+2}, q_{n+2} arise exactly like p_{n+1}, q_{n+1} but with a_{n+1} replaced by $a_{n+1} + \frac{1}{a_{n+2}}$ etc. So

$$\frac{p_{n+2}}{q_{n+2}} = \frac{(a_{n+1} + \frac{1}{a_{n+2}})p_n + p_{n-1}}{(a_{n+1} + \frac{1}{a_{n+2}})q_n + q_{n-1}}$$

$$= \frac{a_{n+2}(a_{n+1}p_n + p_{n-1}) + p_n}{a_{n+2}(a_{n+1}q_n + q_{n-1}) + q_n} = \frac{a_{n+2}p_{n+1} + p_n}{a_{n+2}q_{n+1} + q_n}$$

which proves the claim.

The above recursion is expressed better as :
$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}\begin{pmatrix} a_{n+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix}$.
But, $p_0 = a_0, q_0 = 1, p_1 = a_0a_1 + 1, q_1 = a_1$.
So $\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix}$.
Thus, the recursion is expressed neatly as:

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix}$$

Observe that immediately the determinants give

$$p_nq_{n-1} - p_{n-1}q_n = (-1)^{n-1}$$

So p_n, q_n are relatively prime and, from this, it can be shown that the limit defining the C.F. exists.

There is a simple way to recover l from any one of the so-called ‘complete quotients’ $l_n = a_n + \frac{1}{a_{n+1}+}\frac{1}{a_{n+2}+}\cdots$
Since $\frac{p_n}{q_n} = \frac{a_n p_{n-1}+p_{n-2}}{a_n q_{n-1}+q_{n-2}}$ and l is obtained when a_n above is replaced by l_n, we have

$$l = \frac{l_n p_{n-1} + p_{n-2}}{l_n q_{n-1} + q_{n-2}}.$$

C.F.s for rational numbers

It is elementary to observe that finding continued fractions for rational numbers p/q is not only equivalent to the Euclidean algorithm of finding the GCD of p and q but also equivalent to (very efficiently) solving the linear Diophantine equation $px - qy = (p, q)$.
Let us give an example.

Suppose we wish to solve $72x + 5^7y = 1$ in integers x, y. Look at the following division table:

14	72	78125	1085
2	2	5	2
	0	1	

Then $\frac{78125}{72} = [1085; 14, 2, 2]$.
The penultimate convergent $[1085; 14, 2] = 1085 + 1/(14 + \frac{1}{2}) = 1085 + \frac{2}{29} = \frac{31467}{29}$ provides us with a solution of $78125x - 72y = 1$; viz. $(x, y) = (29, 31467)$.
So, it is not surprising that finding the continued fractions of certain numbers may lead to solutions of some Diophantine equations.

How does one find the C.F. for an irrational number like $\sqrt{7}$?

$$\sqrt{7} = 2 + (\sqrt{7} - 2) = 2 + \frac{3}{\sqrt{7}+2} = 2 + \frac{1}{(\sqrt{7}+2)/3}.$$

$$\frac{\sqrt{7}+2}{3} = 1 + (\frac{\sqrt{7}+2}{3} - 1) = 1 + \frac{\sqrt{7}-1}{3}.$$

$$\sqrt{7} - 2 = \frac{1}{1+}\frac{\sqrt{7}-1}{3} = \frac{1}{1+}\frac{1}{(\sqrt{7}+1)/2} = \frac{1}{1+}\frac{1}{1+}\frac{\sqrt{7}-1}{2}$$

$$= \frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{\sqrt{7}+2} = \frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4+(\sqrt{7}-2)}.$$

Thus, we have a repetition and

$$\sqrt{7} - 2 = \frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4+}\frac{1}{1+}\frac{1}{1+}\frac{1}{1+}\frac{1}{4+}\cdots$$

So, $\sqrt{7} = [2; \overline{1, 1, 1, 4}]$.

Continued fraction of $\sqrt{N}$.

Let N be a square-free positive integer. How does the C.F. of $\sqrt{N}$ look?
Now, $\sqrt{N} = a_1 + (\sqrt{N} - a_1)$ with $a_1 = [\sqrt{N}]$.
Thus, $\sqrt{N} - a_1 = \frac{N-a_1^2}{\sqrt{N}+a_1} = \frac{r_1}{\sqrt{N}+a_1}$, say, where $r_1 = N = a_1^2$.
In other words, $\sqrt{N} = a_1 + \frac{r_1}{\sqrt{N}+a_1} = a_1 + \frac{1}{(\sqrt{N}+a_1)/r_1}$.
Write $[\frac{\sqrt{N}+a_1}{r_1}] = b_1$; then

$$\sqrt{N} + a_1 = b_1 r_1 + (\sqrt{N} - a_2)$$

where $a_2 = b_1 r_1 - a_1$.
So, $\sqrt{N} = a_1 + \frac{1}{b_1 + (\sqrt{N}-a_2)/r_1} = a_1 + \frac{1}{b_1+}\frac{1}{(\sqrt{N}+a_2)/r_2}$ where $r_1 r_2 = N - a_2^2$.

The C.F. is $\boxed{\sqrt{N} = b_0 + \frac{1}{b_1+}\frac{1}{b_2+}\cdots}$

$\boxed{b_0 = a_1 = [\sqrt{N}]}$ $\boxed{r_1 = N - a_1^2}$ $\boxed{b_1 = [\frac{\sqrt{N}+a_1}{r_1}]}$

$\boxed{a_n = b_{n-1} r_{n-1} - a_{n-1}}$ $\boxed{r_{n-1} r_n = N - a_n^2}$ $\boxed{b_n = [\frac{\sqrt{N}+a_n}{r_n}]}$.

The crucial point is that, at each stage if $b_n = [\frac{\sqrt{N}+a_n}{r_n}]$ is replaced by $l_n = \frac{\sqrt{N}+a_n}{r_n}$, then we get the exact value $\sqrt{N}$.

$$\sqrt{N} = \frac{l_{n+1} p_n + p_{n-1}}{l_{n+1} q_n + q_{n-1}} = \frac{(\frac{\sqrt{N}+a_{n+1}}{r_{n+1}}) p_n + p_{n-1}}{(\frac{\sqrt{N}+a_{n+1}}{r_{n+1}}) q_n + q_{n-1}}.$$

Comparing the terms with and without $\sqrt{N}$,

$$a_{n+1} p_n + r_{n+1} p_{n-1} = N q_n$$

$$a_{n+1} q_n + r_{n+1} q_{n-1} = p_n$$

Using $p_{n-1} q_n - p_n q_{n-1}) = (-1)^n$, we have

$$a_{n+1} (-1)^{n-1} = p_{n-1} p_n - N q_{n-1} q_n$$

$$r_{n+1}(-1)^{n-1} = p_n^2 - Nq_n^2$$

One may deduce from this $a_{n+1}, r_{n+1} > 0$.

Further, if we know some r_k (say r_{n+1}) equals 1, then

$$(-1)^{n-1} = p_n^2 - Nq_n^2$$

Comparing Chakravala with C.F.
Amazingy, the Chakravala method produces the same p_k's and q_k's as in the C.F. for $\sqrt{N}$.
Recall that in Chakravala method, we have

$$p'_{i+1} = a'_{i+1}p_i + p'_{i-1}$$

$$q'_{i+1} = a'_{i+1}q'_i + q'_{i-1}$$

where $a'_{i+1} = \frac{x_{i+1}+x_i}{|m_i|}$ with $a'_0 = p'_0 = [\sqrt{N}], x_i < \sqrt{N} < x_i + |m_{i-1}|$ and $m_i m_{i-1} = x_i^2 - N$.
We have written p'_i, q'_i, a'_i etc. to distinguish from the p_i, q_i, a_i in the C.F.
In view of the recursions, one can show that the b_i's in the C.F. of $\sqrt{N}$ are the same as the a'_i's here as follows.

Recalling the expression for complete quotient at any stage in the S.C.F. of $\sqrt{N}$, and recalling that

$$\sqrt{N} = \frac{l_{n+1}p_n + p_{n-1}}{l_{n+1}q_n + q_{n-1}}$$

we have $l_{n+1} = \frac{\sqrt{N}q_{n-1}-p_{n-1}}{p_n-\sqrt{N}q_n}$.
This gives the expression

$$b_{n+1} = [l_{n+1}] = [\frac{\sqrt{N}q_{n-1} - p_{n-1}}{p_n - \sqrt{N}q_n}].$$

Firstly, $a'_0 = p'_0 = [\sqrt{N}] = b_0$. Next,

$$a'_1 = q'_1 = \frac{p'_0 + x_1}{|m_0|} = \frac{b_0 + x_1}{|m_0|} = [\frac{b_0 + \sqrt{N}}{|m_0|}]$$

since $x_1 < \sqrt{N} < x_1 + |m_0|$.
Hence $a'_1 = [\frac{b_0+\sqrt{N}}{N-b_0^2}] = b_1$; that is,

$$a'_1 = q'_1 = b_1.$$

Also, $p'_1 = 1 + p'_0 q'_1 = 1 + b_0 b_1 = p_1$.
Thus, we have shown $a'_0 = b_0, p'_0 = p_0, q'_0 = q_0, p'_1 = p_1, q'_1 = q_1$.

We assume that $b_i = a'_i$ for all $i \leq n$; then $p'_i = p_i, q'_i = q_i$ for all $i \leq n$. We show $b_{n+1} = a'_{n+1}$.
Recall that

$$b_{n+1} = [\frac{\sqrt{N}q_{n-1} - p_{n-1}}{p_n - \sqrt{N}q_n}].$$

Hence, it suffices to show that

$$a'_{n+1} = [\frac{\sqrt{N}q'_{n-1} - p'_{n-1}}{p'_n - \sqrt{N}q'_n}] \cdots\cdots (\spadesuit)$$

Now, the Chakravala has

$$p'_i = \frac{p'_{i-1}x_i + Nq'_{i-1}}{|m_{i-1}|}, q'_i = \frac{p'_{i-1} + x_i q'_{i-1}}{|m_{i-1}|}$$

which gives

$$p'_n = \frac{p'_{n-1}x_n + \sqrt{N}q'_{n-1}}{|m_{n-1}|}, q'_n = \frac{p'_{n-1} + q'_{n-1}x_n}{|m_{n-1}|}.$$

Using these, the right hand side of $(\spadesuit)$ is

$$[\frac{\sqrt{N}q'_{n-1} - p'_{n-1}}{p'_n - \sqrt{N}q'_n}] = [\frac{|m_{n-1}|}{\sqrt{N} - x_n}] = [\frac{\sqrt{N} + x_n}{|m_n|}]$$

where we have used $m_n m_{n-1} = x_n^2 - N$.
Denote the integer $[\frac{\sqrt{N}+x_n}{|m_n|}]$ by t. Then, we have

$$t < \frac{\sqrt{N} + x_n}{|m_n|} < t + 1.$$

Hence $t|m_n| - x_n < \sqrt{N} < t|m_n| - x_n + |m_n|$.
As x_{n+1} is the unique integer satisfying $x_{n+1} < \sqrt{N} < x_{n+1} + |m_n|$ as we defined in the Chakravala, we have $x_{n+1} = t|m_n| - x_n$. This means $t = \frac{x_n + x_{n+1}}{|m_n|} = a'_{n+1}$. So $b_{n+1} = a'_{n+1}$. We have thus proved our assertion.

Recurrence of C.F. for $\sqrt{N}$

Let us start by proving the well-known fact that b_n's recur.
Now $0 < r_{n-1}r_n = N - a_n^2$ implies that $a_1 = [\sqrt{N}] \geq a_n \forall n$.

So, each a_n can only have the values $1, 2, \cdots, a_1 = [\sqrt{N}]$.
From $b_{n-1}r_{n-1} = a_n + a_{n-1} \leq 2a_1$, we have $r_{n-1} \leq 2a_1$ for all n.
This means that the complete quotients (these are $\frac{\sqrt{N}+a_n}{r_n}$) can take at the most $2a_1^2$ values; so they recur.
So $a_n = a_k, r_n = r_k, b_n = b_k$ for some $n < k$.
We shall show that $a_{n-1} = a_{k-1}, r_{n-1} = r_{k-1}, b_{n-1} = b_{l-1}$.
Now, $r_{k-1}r_k = N - a_k^2 = N - a_n^2 = r_{n-1}r_n$ gives $r_{k-1} = r_{n-1}$.
$a_{k-1} - a_{n-1} = (a_{k-1} + a_k) - (a_{n-1} + a_n) = (b_{k-1} - b_{n-1})r_{n-1}$.
We observe as follows that $a_1 < a_d + r_d$ for all d.

$$r_{d-1} \leq b_{d-1}r_{d-1} = a_{d-1} + a_d < \sqrt{N} + a_d = \frac{N - a_d^2}{\sqrt{N} - a_d} = \frac{r_{d-1}r_d}{\sqrt{N} - a_d}$$

So, it follows that $r_d > \sqrt{N} - a_d > a_1 - a_d$.
Thus, $(b_{k-1} - b_{n-1})r_{n-1} = a_{k-1} - a_{n-1}$
$= (a_1 - a_{n-1}) - (a_1 - a_{k-1}) < a_1 - a_{n-1} < r_{n-1}$;
we arrive at $b_{k-1} = b_{n-1}, a_{k-1} = a_{n-1}$.
Proceeding in this manner, there is n such that $a_{n+1} = a_1, r_{n+1} = r_1$. So

$$r_n r_1 = r_n r_{n+1} = N - a_{n+1}^2 = N - a_1^2 = r_1$$

which means $r_n = 1$.
So $r_n(-1)^n = (-1)^n = p_{n-1}^2 - Nq_{n-1}^2$.

Chakravala gives all

The Chakravala method does give solutions of $x^2 - Ny^2 = 1$.
Indeed, we know how to get a solution of $x^2 - Ny^2 = 1$ from one for $x^2 - Ny^2 = -1$. The remarkable fact that it gives all the solutions is contained in the theorem below:

Theorem.
Every solution of either of the equations $x^2 - Ny^2 = \pm 1$ is of the form (p_n, q_n) for some n.

Let us first observe that any solution of $x^2 - Ny^2 = \pm 1$ satisfies $|\frac{x}{y} - \sqrt{N}| < \frac{1}{2y^2}$.
We see this when $x^2 - Ny^2 = 1$, for $\frac{x}{y} - \sqrt{N} = \frac{x - y\sqrt{N}}{y} = \frac{1}{y(x+y\sqrt{N})} < \frac{1}{2y^2}$ since $x + y\sqrt{N} > 2y$.
When $x^2 - Ny^2 = -1$ and $x \geq y$, the same argument works.
When $x^2 - Ny^2 = -1$ with $x < y$, we have $-1 = x^2 - Ny^2 < y^2 - Ny^2 = (1 - N)y^2$ which means $(N - 1)y^2 < 1$, an impossibility.

The rest of the proof then follows from the more general statement:
If α is a real number which is irrational, and satisfies $|\alpha - \frac{r}{s}| < \frac{1}{2s^2}$ where $s > 0$, then r/s is a convergent to the continued fraction of α.

We skip the rest of the proof of the theorem which is an easy consequence of the fact that we can find ζ such that

$$\alpha = \frac{\zeta p_n + p_{n-1}}{\zeta q_n + q_{n-1}}$$

and the key observation (which we prove) where the so-called modular group plays a role:

Modular group comes in
If $\alpha = \frac{\zeta p + r}{\zeta q + s}$ where $\zeta > 1$ and $ps - qr = \pm 1$ and $q > s > 0$, then $p/q, r/s$ are consecutive convergents to the C.F. of α.

For the proof, write $\frac{p}{q} = [a_0; a_1, \cdots, a_n]$ with p_i/q_i the convergents (so $p_n/q_n = p/q$). Choose n so that

$$ps - qr = (-1)^{n-1} = p_n q_{n-1} - q_n p_{n-1}.$$

Note that we have used the easy observation that a rational number has two simple continued fractions - one of even length and the other of odd length. As p, q are relatively prime with $q > 0$ and $p/q = p_n/q_n$, it follows that $p = p_n, q = q_n$.
Thus, $(-1)^{n-1} = ps - qr = p_n s - q_n r = p_n q_{n-1} - q_n p_{n-1}$.
This gives $p_n(s - q_{n-1}) = q_n(r - p_{n-1})$ which means in view of coprimality of p_n, q_n that $q_n | (s - q_{n-1})$.
As $q_n = q > s$ (hypothesis) and $q_n \geq q_{n-1}$, we must have $s = q_{n-1}$ (and hence $r = p_{n-1}$). We are done.

Remarks.
It can be sown that if the continued fraction expansion of $\sqrt{N}$ looks like $[b_0; \overline{b_1, b_2, \cdots, b_r, 2b_0}]$ and, the penultimate convergent $[b_0; b_1, b_2, \cdots, b_r]$ gives a solution of $x^2 - Ny^2 = -1$ or of $x^2 - Ny^2 = 1$ according as to whether the period $r + 1$ above is odd or even.

Examples

$\sqrt{7} = [2; \overline{1, 1, 1, 4}, \cdots]$ gives the penultimate convergent before the period to be $[2; 1, 1, 1] = 8/3$. Then, $(8, 3)$ is a solution of $x^2 - 7y^2 = 1$ (as the period is of even length).
Note that $x^2 - 7y^2 = -1$ has no solution (look mod 4).

$\sqrt{13} = [3; \overline{1, 1, 1, 1, 6}, \cdots]$ gives the penultimate convergent before the period to be $[3; 1, 1, 1, 1] = 18/5$.
Then $(18, 5)$ is a solution of $x^2 - 13y^2 = -1$ (as the period is of odd length).
From this a solution for $x^2-13y^2 = 1$ can be obtained as $(18^2+13(5^2), 2(18)(5)) = (649, 180)$.