On Taking Square Roots

On Taking Square Roots

Daniel W. Stroock

The traditional method for computing square roots is based on the identity

$$(a+b)^2 = a^2 + (2a+b)b.$$

For example, to compute $\sqrt{2}$, one uses the following procedure to construct a sequence $\{a_n : n \geq 0\} \subseteq \{0, \ldots, 9\}$ such that $0 \leq \sqrt{2} - r_n < 10^{-n}$, where $r_n = \sum_{m=0}^{n} a_m 10^{-m}$. One begins by finding the greatest integer $0 \leq a_0 < 10$ for which $a_0^2 \leq 2$, and then sets $r_0 = a_0$ and $E_0 = 2 - r_0^2$. Next, one finds the greatest integer $0 \leq a_1 < 10$ such that $(r_0 + a_1 10^{-1})^2 \leq 2$, or equivalently,

$$\left(2r_0 + a_{-1}10^{-1}\right) a_{-1}10^{-1} \leq E_0,$$

and then sets $r_1 = r_0 + a_1 10^{-1}$ and $E_1 = 2 - r_1^2$. More generally, if $n \geq 1$ and a_{n-1}, r_{n-1}, and E_{n-1} have been determined, then one takes a_n to be the greatest integer less than 10 such that

$$\left(2r_{n-1} + a_n 10^{-n}\right) a_n 10^{-n} \leq E_{n-1},$$

and sets $r_n = r_{n-1} + a_n 10^{-n}$ and

$$E_n = 2 - r_n^2 = E_{n-1} - \left(2r_{n-1} + a_n 10^{-n}\right) a_n 10^{-n}.$$

Using induction, one can show that $|\sqrt{2} - r_n| < 10^{-n}$ for all $n \geq 0$.

Applying this algorithm, one finds that

$$\begin{array}{lll} a_0 = 1, & r_0 = 1, & E_0 = 1, \\ a_1 = 0.4, & r_1 = 1.4, & E_1 = 0.04, \\ a_2 = 0.01, & r_2 = 1.41, & E_2 = 0.0119, \\ a_3 = 0.004, & r_3 = 1.414, & E_3 = 0.000604, \\ a_4 = 0.0002, & r_4 = 1.4142, & E_4 = 0.00003836, \\ a_5 = 0.00001, & r_5 = 1.41421, & E_5 = 0.00000952. \end{array}$$

Thus $\sqrt{2}$ is equal to 1.41421, apart from an error smaller than 10^{-5}. More generally, if $10^{2\ell} \leq N < 10^{2(\ell+1)}$ is not a square, then after n steps, this procedure will produce the decimal representation of the number r_n such that $0 \leq \sqrt{N} - r_n < 10^{\ell - n}$.

An Alternative Method

The traditional method is fine but somewhat tedious and—unless one keeps one's wits about one—subject to error. In addition, from a mathematical standpoint, it is not natural. To understand this latter objection, suppose that N is an integer that is not the square of an integer. Then $\sqrt{N}$ is an irrational number. Irrational numbers are hard to understand, and one way of getting a handle on them is to study how well they can be approximated by rational numbers. That is what decimal expansions do, but they restrict themselves to rational numbers whose

denominators are powers of 10. Other than the fact that most of us have ten fingers, there is nothing sacrosanct about the number 10 or its powers, and from a mathematical perspective, this restriction is arbitrary and foolish.

To see how removal of the restriction to powers of 10 can lead to alternative procedures for computing square roots, again consider $\sqrt{2}$. Obviously, the integer part $\lfloor\sqrt{2}\rfloor$ of $\sqrt{2}$ is 1, and so what we are interested in is $u = \sqrt{2} - 1$. It is easy to verify that $u = \frac{1}{u+2}$ and that

$$\frac{1}{y+2} - \frac{1}{x+2} = \frac{-(y-x)}{(x+2)(y+2)}.$$

Now define $r_0 = 0$ and $r_n = \frac{1}{r_{n-1}+2}$ for $n \geq 1$. Then

$$u - r_n = \frac{1}{u+2} - \frac{1}{r_{n-1}+2} = -\frac{u - r_{n-1}}{(r_{n-1}+2)(u+2)}.$$

Hence $|u - r_n| \leq u4^{-n}$. Writing r_n as $\frac{a_n}{b_n}$, one has that $a_0 = 1$, $b_0 = 2$, and $a_n = b_{n-1}$ and $b_n = a_{n-1} + 2b_{n-1}$ for $n \geq 1$. In particular, $r_7 = \frac{408}{985}$, whose denominator is much smaller than 10^5 and yet has a decimal expansion that begins 0.41421, which coincides with the first five places in the expression for $\sqrt{2} - 1$ as a decimal.

For a second example, set $u = \sqrt{11} - 3$, and observe that $u = \frac{u+6}{3u+19}$. In addition,

$$\frac{y+6}{3y+19} - \frac{x+6}{3x+19} = \frac{y-x}{(3y+19)(3x+19)}.$$

Hence if $r_0 = 0$ and $r_n = \frac{r_{n-1}+6}{3r_{n-1}+19}$ for $n \geq 1$, then $|u - r_n| \leq u(19)^{-2n}$. In particular, $r_2 = \frac{120}{379}$, whose decimal expansion begins 0.3166 and coincides with the first four places in the decimal expansion of $\sqrt{11} - 3$.

The preceding examples suggest that given any N that is not a square, one should set $u = \sqrt{N} - \lfloor\sqrt{N}\rfloor$ and look for a partial fraction $\frac{ax+b}{cx+d}$ with integer coefficients such that $u = \frac{au+b}{cu+d}$. There are, of course, infinitely many such partial fractions, but the virtue of those in our examples is that $ad - bc = \pm 1$, which guarantees that if $r_0 = 0$ and $r_n = \frac{ar_{n-1}+b}{cr_{n-1}+d}$ for $n \geq 1$, then $|u - r_n| \leq \frac{|u-r_{n-1}|}{d^2}$ and therefore that $|u - r_n| \leq ud^{-2n}$. Thus we want to look for integers a, b, c, d for which

$$u = \frac{au+b}{cu+d} \quad \text{and} \quad ad - bc = \pm 1. \tag{1}$$

It turns out that finding the coefficients a, b, c, d in (1) entails a good deal of interesting mathematics. In fact, it is not at all obvious that they will always exist. Assuming that they do, we have in the first place $c \neq 0$, since if c were equal to 0, then u would be rational. Secondly, consider the quadratic function $f(x) = cx^2 + (d-a)x - b$. Since $f(u) = 0$, we know that $f(x) = c(x-u)(x-r)$ for some real number r. Thus

$$d - a = -c(u+r) \quad \text{and} \quad b = -cur.$$

The first of these equations implies that $u + r$ is a rational number and therefore that $r = -\sqrt{N} + s$, where s is a rational number. After combining this with the second equation in the display above, we see that

$$-\frac{b}{c} = -N + \big(\lfloor\sqrt{N}\rfloor + s\big)\sqrt{N} - s\lfloor\sqrt{N}\rfloor,$$

which is possible only if $s = -\lfloor\sqrt{N}\rfloor$. Thus $b = c\big(N - \lfloor\sqrt{N}\rfloor^2\big)$ and $d = a + 2c\lfloor\sqrt{N}\rfloor$. After multiplying the second of these equations by a and combining the result with $ad = bc \pm 1$ and the first equation, we obtain

$$a^2 + 2ac\lfloor\sqrt{N}\rfloor = c^2\big(N - \lfloor\sqrt{N}\rfloor^2\big) \pm 1,$$

which means that $\big(a + c\lfloor\sqrt{N}\rfloor\big)^2 = c^2N \pm 1$. Hence $c^2N \pm 1$ is the square of an integer β and

$$a = -c\lfloor\sqrt{N}\rfloor + \beta, \quad b = c\big(N - \lfloor\sqrt{N}\rfloor^2\big), \quad d = c\lfloor\sqrt{N}\rfloor + \beta. \tag{2}$$

We now know that in order for (1) to hold, $\beta = \sqrt{c^2N \pm 1}$ must be an integer, in which case a, b, and d are given by (2). In the number theory literature, an equation of the form $\beta = \sqrt{c^2N \pm 1} \in \mathbb{Z}^+$ is called a *Pell equation.*[1] When $N = 2$, one choice is $c = 1$, since $1^2 \cdot 2 - 1 = 1^2$ and $\beta = 1$. When $N = 11$, one can take $c = 3$, in which case $3^2 \cdot 11 + 1 = 10^2$ and $\beta = 10$. However, finding a number c by hand can take a lot of time. For example, when $N = 19$, the smallest c is 39, and when $N = 67$, it is 5967 (see the section "Some Examples" below). Thus it is important to develop a systematic procedure for finding c.

A Brief Introduction to Continued Fractions

Although it will not be immediately apparent why, it turns out that continued fractions are needed to carry out the program outlined at the end of the previous section. For that reason, this section will give a quick summary of a few basic facts about continued fractions.

Given a set $\{a_m \colon m \geq 1\} \subseteq \mathbb{Z}^+$, define the *continued fraction*

$$[a_1, \ldots, a_n] = \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

Equivalently,

$$[a_n] = \frac{1}{a_n} \quad \text{and} \quad \frac{1}{[a_m, \ldots, a_n]} = a_m + [a_{m+1}, \ldots, a_n] \tag{3}$$

for $1 \leq m < n$. Determine p_n and q_n to be the relatively prime integers such that $\frac{p_n}{q_n} = [a_1, \ldots, a_n]$. The rational number $\frac{p_n}{q_n}$ is called the nth *convergent* for $\{a_m \colon m \geq 1\}$. Notice that if $\left\{\frac{p'_k}{q'_k} \colon k \geq 1\right\}$ are the convergents for $\{a_{1+m} : m \geq 1\}$, then for $m \geq 2$, equation (3) implies that

$$\frac{p_m}{q_m} = \frac{1}{a_m + \frac{p'_{m-1}}{q'_{m-1}}} = \frac{q'_{m-1}}{a_m q'_{m-1} + p'_{m-1}}.$$

[1] Here and elsewhere, we will use $\mathbb{Z}$ to denote the set of all integers, $\mathbb{Z}^+$ the set of positive integers, and $\mathbb{Q}$ the set of rational numbers.

Therefore, since q'_{m-1} and $a_m q'_{m-1}+p'_{m-1}$ are relatively prime, we have $p_m = q'_{m-1}$ and $q_m = a_m q'_{m-1} + p'_{m-1}$. Clearly, $p_1 = 1$ and $q_1 = a_1$, and let us define $p_0 = 0$ and $q_0 = 1$. Proceeding by induction on $n \geq 1$, one can use the preceding to see that

$$\begin{pmatrix} p_{n-1} & p_n \\ q_{n-1} & q_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} \tag{4}$$

and

$$\begin{pmatrix} p_n \\ q_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & a_1 \end{pmatrix} \cdots \begin{pmatrix} 0 & 1 \\ 1 & a_n \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} p_{n-2} & p_{n-1} \\ q_{n-2} & q_{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ a_n \end{pmatrix},$$

and so

$$p_n = a_n p_{n-1} + p_{n-2} \quad \text{and} \quad q_n = a_n q_{n-1} + q_{n-2} \text{ for } n \geq 2. \tag{5}$$

In addition, by taking the determinant of both sides of (4), one finds that

$$p_{n-1}q_n - p_n q_{n-1} = (-1)^n. \tag{6}$$

From (5) and (6), one has

$$\frac{p_{n-1}}{q_{n-1}} - \frac{p_n}{q_n} = \frac{(-1)^n}{q_{n-1}q_n} \quad \text{and} \quad \frac{p_{n-1}}{q_{n-1}} - \frac{p_{n+1}}{q_{n+1}} = \frac{(-1)^{n+1}a_{n+1}}{q_{n-1}q_{n+1}}. \tag{7}$$

Because $q_n \geq 2$ for $n \geq 2$, it follows from (7) that there exists $u \in (0,1)$ such that

$$\frac{p_{2n}}{q_{2n}} \nearrow u \quad \text{and} \quad \frac{p_{2n+1}}{q_{2n+1}} \searrow u.$$

We will use $[a_1, \ldots, a_n, \ldots]$ to denote this number u.

Finally, to connect these considerations with those in the preceding section, observe that (4) implies that

$$\begin{pmatrix} p_{m+n} \\ q_{m+n} \end{pmatrix} = \begin{pmatrix} p_{m-1} & p_m \\ q_{m-1} & q_m \end{pmatrix} \begin{pmatrix} p'_n \\ q'_n \end{pmatrix},$$

where $\frac{p'_n}{q'_n}$ is the nth convergent for $\{a_{m+k} : k \geq 1\}$. Hence

$$\frac{p_{m+n}}{q_{m+n}} = \frac{p_{m-1}p'_n + p_m q'_n}{q_{m-1}p'_n + q_m q'_n} = \frac{p_{m-1}\frac{p'_n}{q'_n} + p_m}{q_{m-1}\frac{p'_n}{q'_n} + q_m},$$

and therefore, on letting $n \to \infty$, we obtain

$$[a_1, \ldots, a_n, \ldots] = \frac{p_{m-1}[a_{m+1}, \ldots, a_{m+n}, \ldots] + p_m}{q_{m-1}[a_{m+1}, \ldots, a_{m+n}, \ldots] + q_m}.$$

In particular, if $[a_1, \ldots, a_n, \ldots] = [a_{m+1}, \ldots, a_{m+n}, \ldots]$, then

$$[a_1, \ldots, a_n, \ldots] = \frac{p_{m-1}[a_1, \ldots, a_n, \ldots] + p_m}{q_{m-1}[a_1, \ldots, a_n, \ldots] + q_m}, \tag{8}$$

which is exactly the sort of equation that appears in (1).

Constructing Continued Fractions

In order to apply the theory of continued fractions, we must learn how to expand an irrational number $u \in (0,1)$ as a continued fraction, and the key to doing so is the Gauss map $T : (0,1) \setminus \mathbb{Q} \longrightarrow (0,1) \setminus \mathbb{Q}$ given by

$$Tu = \frac{1}{u} - \left\lfloor \frac{1}{u} \right\rfloor .$$

The basic observation is that

$$u = [a_1, \ldots, a_n, \ldots] \implies T^{m-1}u = [a_m, \ldots, a_{m+n}, \ldots], \quad a_m = \left\lfloor \frac{1}{T^{m-1}u} \right\rfloor \tag{9}$$

for $m \geq 1$. To prove this, first note that because

$$\frac{1}{[a_1, \ldots, a_n, \ldots]} = a_1 + [a_2, \ldots, a_n, \ldots]$$

and $[a_2, \ldots, a_n, \ldots] \in (0,1)$, we have $a_1 = \lfloor \frac{1}{u} \rfloor$, from which (9) is clear when $m = 1$. Next, assume that (9) holds for m, and note that because

$$\frac{1}{[a_m, \ldots, a_{m+n}, \ldots]} = a_m + [a_{m+1}, \ldots, a_{m+1+n}, \ldots],$$

one finds first that

$$[a_{m+1}, \ldots, a_{m+1+n}, \ldots] = \frac{1}{T^{m-1}u} - \left\lfloor \frac{1}{T^{m-1}u} \right\rfloor = T^m u$$

and then, just as in the case $m = 1$, that $a_{m+1} = \lfloor \frac{1}{T^m u} \rfloor$.

We now know that if u admits a continued fraction expansion $[a_1, \ldots, a_n, \ldots]$, then the a_m are given by (9). To show that this prescription works, let $\left\{ \frac{p_n}{q_n} : n \geq 1 \right\}$ be the convergents for the $\{a_n : n \geq 1\}$ in (9). Because we know that these convergents converge, it suffices to show that $\frac{p_n}{q_n}$ is greater than or less than u depending on whether n is odd or even. Since $p_1 = 1$ and $q_1 = \lfloor \frac{1}{u} \rfloor$, this is clear when $n = 1$. Let $n \geq 1$, and assume that the required relationship holds for n and all $u \in (0,1) \setminus \mathbb{Q}$. Then

$$[a_2, \ldots, a_{n+1}] < Tu \quad \text{or} \quad [a_2, \ldots, a_{n+1}] > Tu,$$

depending on whether n is even or odd. Hence

$$\frac{1}{[a_1, \ldots, a_{n+1}]} = a_1 + [a_2, \ldots, a_{n+1}]$$

is greater than or less than $a_1 + Tu = \frac{1}{u}$ depending on whether n is even or odd, and so the required relationship holds for $n + 1$ and all $u \in (0,1) \setminus \mathbb{Q}$.

Back to Square Roots

Assume that $N \in \mathbb{Z}^+$ is not a square, and set $u = \sqrt{N} - \alpha_0$, where $\alpha_0 = \lfloor \sqrt{N} \rfloor$. If $\left\{ \frac{p_k}{q_k} : k \geq 1 \right\}$ are the convergents in the continued fraction expansion of u, then we know from (8) and (9) combined with (6) and (2) that $T^k u = u$ implies

$$\begin{aligned} \beta &= \sqrt{q_{k-1}^2 + (-1)^k} \in \mathbb{Z}^+, \quad p_{k-1} = -q_{k-1}\alpha_0 + \beta, \\ p_k &= q_{k-1}(N - \alpha_0^2), \qquad\qquad q_k = q_{k-1}\alpha_0 + \beta, \\ u &= \frac{p_{k-1}u + p_k}{q_{k-1}u + q_k}. \end{aligned}$$

In particular, we will know how to produce solutions to the Pell equation as well as coefficients a, b, c, d for which (1) holds once we show that there is always a k for which $T^k u = u$. In fact, once we know that such a k exists, we will know that for all $m \geq 1$, one has $T^{mk} u = u$, and therefore that q_{mk-1} is a solution to the Pell equation and p_{mk-1}, p_{mk}, q_{mk-1}, q_{mk} can be taken to be the coefficients a, b, c, d in (1).

Referring to the preceding, there are two steps in the proof that there is always a k for which $T^k u = u$. The first is to show that there exist $m \geq 0$ and $k \geq 1$ such that $T^{m+k} u = T^m u$. The second is to show that if $1 \leq m < n$ and $T^n u = T^m u$, then $T^{n-1} u = T^{m-1} u$. To carry out the first step, observe that $\frac{1}{u} = \frac{\sqrt{N}+\alpha_0}{N-\alpha_0^2}$ and therefore that $Tu = \frac{\sqrt{N}-\alpha_1}{\Delta_1}$, where

$$\Delta_1 = N - \alpha_0^2 \quad \text{and} \quad \alpha_1 = \left\lfloor \frac{\sqrt{N} + \alpha_0}{\Delta_1} \right\rfloor \Delta_1 - \alpha_0.$$

In particular, Δ_1 divides $N - \alpha_1^2$, and so $\frac{1}{Tu} = \frac{\sqrt{N}+\alpha_1}{\Delta_2}$ and $T^2 u = \frac{\sqrt{N}-\alpha_2}{\Delta_2}$, where

$$\Delta_2 = \frac{N - \alpha_1^2}{\Delta_1} \quad \text{and} \quad \alpha_2 = \left\lfloor \frac{\sqrt{N} + \alpha_1}{\Delta_2} \right\rfloor \Delta_1 - \alpha_1.$$

Again Δ_2 divides $N - \alpha_1^2$, and so $T^3 u = \frac{\sqrt{N}-\alpha_3}{\Delta_3}$, where

$$\Delta_3 = \frac{N - \alpha_2^2}{\Delta_2} \quad \text{and} \quad \alpha_3 = \left\lfloor \frac{\sqrt{N} + \alpha_2}{\Delta_3} \right\rfloor \Delta_3 - \alpha_2.$$

Proceeding by induction, one sees that $T^m u = \frac{\sqrt{N}-\alpha_m}{\Delta_m}$, where $\alpha_m < \sqrt{N}$ and Δ_m divides $N - \alpha_m^2$. Hence $T^m u$ can take only a finite number of values, and so two of them must eventually coincide.

To see that $T^n u = T^m u \implies T^{n-1} u = T^{m-1} u$, write $T^m u$ and $T^n u$ as $\frac{\sqrt{N}-\alpha_m}{\Delta_m}$ and $\frac{\sqrt{N}-\alpha_n}{\Delta_n}$, and check that $T^m u = T^n u \implies \frac{\alpha_m}{\Delta_m} = \frac{\alpha_n}{\Delta_n}$. Hence $T^n u = T^m u \implies \frac{\sqrt{N}+\alpha_m}{\Delta_m} = \frac{\sqrt{N}+\alpha_n}{\Delta_n}$. But for $\ell \geq 1$,

$$\frac{\sqrt{N} + \alpha_\ell}{\Delta_\ell} = \frac{\sqrt{N} - \alpha_{\ell-1}}{\Delta_\ell} + \frac{\alpha_\ell + \alpha_{\ell-1}}{\Delta_\ell} = \frac{\Delta_{\ell-1}}{\sqrt{N} + \alpha_{\ell-1}} + \left\lfloor \frac{1}{T^{\ell-1} u} \right\rfloor.$$

This shows that $\frac{\sqrt{N}+\alpha_\ell}{\Delta_\ell} > 1$ for $\ell \geq 1$, and clearly $\sqrt{N}+\alpha_0 > 1$. Therefore,

$$\left\lfloor \frac{\sqrt{N}+\alpha_\ell}{\Delta_\ell} \right\rfloor = \left\lfloor \frac{1}{T^{\ell-1}u} \right\rfloor,$$

and so

$$\frac{1}{T^{\ell-1}u} = \left\lfloor \frac{\sqrt{N}+\alpha_\ell}{\Delta_\ell} \right\rfloor + T^\ell u.$$

As a consequence, one sees that $T^n u = T^m u \implies T^{n-1}u = T^{m-1}u$.

To summarize, we have now proved all but the final part of the following theorem.

Theorem 1 *Given $N \in \mathbb{Z}^+$ that is not a square, set $u = \sqrt{N} - \lfloor \sqrt{N} \rfloor$. Then there exists $k \geq 1$ such that $T^k u = u$. Moreover, if $\left\{ \frac{p_m}{q_m} : m \geq 1 \right\}$ are the convergents for the continued fraction expansion of u, then*

$$\begin{aligned}
&\beta_k \equiv \sqrt{q_{k-1}^2 N + (-1)^k} \in \mathbb{Z}^+, \quad p_{k-1} = \beta_k - q_{k-1} \left\lfloor \sqrt{N} \right\rfloor, \\
&p_k = q_{k-1}\big(N - \left\lfloor \sqrt{N} \right\rfloor^2\big), \qquad\qquad q_k = \beta_k + q_{k-1} \left\lfloor \sqrt{N} \right\rfloor, \\
&u = \frac{p_{k-1}u + p_k}{q_{k-1}u + q_k}.
\end{aligned}$$

Further, if $k_0 = \min\{k \geq 1 : T^k u = u\}$, then for every $\ell \in \mathbb{Z}^+$, one has $T^\ell u = u \iff \ell = mk_0$.

Proof To prove the final assertion, note first that it is obvious that $T^{mk_0}u = u$ for all $m \in \mathbb{Z}^+$. Conversely, suppose that $T^\ell u = u$ for some $\ell \in \mathbb{Z}$, and write $\ell = mk_0 + r$, where $r < k_0$. Then $u = T^r \circ T^{mk_0} u = T^r u$, and so $r = 0$.

Although I have not proved it here, with a little more work, one can show that all solutions to the Pell equations $\beta = \sqrt{q^2 N \pm 1} \in \mathbb{Z}^+$ correspond to periods of the orbit of T acting on $\sqrt{N} - \lfloor \sqrt{N} \rfloor$. In particular, if k_0 is even, there are no solutions to $\sqrt{q^2 N - 1} \in \mathbb{Z}^+$. Hence there always exist infinitely many solutions to $\sqrt{q^2 N + 1} \in \mathbb{Z}^+$, and depending on whether k_0 is odd or even, there are either infinitely many solutions or no solutions to $\sqrt{q^2 N - 1} \in \mathbb{Z}^+$.

Some Examples

Example 1 If $N = m^2 + 1$ for some $m \geq 1$, then $u = \sqrt{N} - m$. Thus

$$\frac{1}{u} = \sqrt{N} + m, \quad a_1 = 2m, \quad Tu = u,$$

and so there are infinitely many solutions to both $\sqrt{q^2 N + 1} \in \mathbb{Z}^+$ and $\sqrt{q^2 N - 1} \in \mathbb{Z}^+$. In addition, $p_0 = 0$, $p_1 = 1$, $q_0 = 1$, $q_1 = 2m$, $\beta_1 = m$, and $u = \frac{1}{u+2m}$.

Example 2 If $N = m^2 + 2$, then $u = \sqrt{N} - m$. Thus

$$\begin{aligned} \frac{1}{u} &= \frac{\sqrt{N}+m}{2}, \quad a_1 = m, \qquad Tu = \frac{\sqrt{N}-m}{2}, \\ \frac{1}{Tu} &= \sqrt{N}+m, \quad a_2 = 2m, \quad T^2u = u. \end{aligned}$$

Hence, there are no solutions to $\sqrt{q^2N-1} \in \mathbb{Z}^+$, $p_1 = 1$, $p_2 = 2m$, $q_1 = m$, $q_2 = 2m^2+1$, $\beta_2 = m^2+1$, and

$$u = \frac{u+2m}{mu+2m^2+1}.$$

Example 3 If $m \geq 2$ and $N = m^2 + 4$, then $u = \sqrt{N} - m$.

(i) If $m = 2n$, then

$$\begin{aligned} \frac{1}{u} &= \frac{\sqrt{N}+m}{4}, \quad a_1 = n, \qquad Tu = \frac{\sqrt{N}-m}{4}, \\ \frac{1}{Tu} &= \sqrt{N}+m, \quad a_2 = 2m, \quad T^2u = u. \end{aligned}$$

Thus, there are no solutions to $\sqrt{q^2N-1} \in \mathbb{Z}^+$. Furthermore, $p_1 = 1$, $p_2 = 2m$, $q_1 = n$, $q_2 = m^2+1$, $\beta_2 = \frac{m^2+2}{2}$, and

$$u = \frac{u+2m}{nu+m^2+1}.$$

(ii) If $m = 2n+1$, then

$$\begin{aligned} \frac{1}{u} &= \frac{\sqrt{N}+m}{4}, \qquad a_1 = n, \qquad Tu = \frac{\sqrt{N}-(m-2)}{4}, \\ \frac{1}{Tu} &= \frac{\sqrt{N}+m-2}{m}, \quad a_2 = 1, \qquad T^2u = \frac{\sqrt{N}-2}{m}, \\ \frac{1}{T^2u} &= \frac{\sqrt{N}+2}{m}, \qquad a_3 = 1, \qquad T^3u = \frac{\sqrt{N}-(m-2)}{m}, \\ \frac{1}{T^3u} &= \frac{\sqrt{N}+m-2}{4}, \quad a_4 = n, \qquad T^4 = \frac{\sqrt{N}-m}{4}, \\ \frac{1}{T^4} &= \sqrt{N}+m, \qquad a_5 = 2m, \quad T^5u = u. \end{aligned}$$

Thus both $\sqrt{q^2N+1} \in \mathbb{Z}^+$ and $\sqrt{q^2N-1} \in \mathbb{Z}^+$ have infinitely many solutions, $p_4 = m$, $p_5 = 2(m^2+1)$, $q_4 = \frac{m^2+1}{2}$, $q_5 = m(m^2+2)$, $\beta_5 = \frac{m(m^2+3)}{2}$, and

$$u = \frac{2mu+4(m^2+1)}{(m^2+1)u+2m(m^2+1)}.$$

Example 4 If $N = m^2 + m$, then $u = \sqrt{N} - m$ and

$$\begin{aligned} \frac{1}{u} &= \frac{\sqrt{N}+m}{m}, \quad a_1 = 2, \qquad Tu = \frac{\sqrt{N}-m}{m} \\ \frac{1}{Tu} &= \sqrt{N}+m, \quad a_2 = 2m, \quad T^2u = u. \end{aligned}$$

Thus $\sqrt{q^2N-1} \in \mathbb{Z}^+$ has no solutions, $p_1 = 1$, $p_2 = 4m+2$, $q_1 = 2$, $q_2 = 2m$, $\beta_2 = 2m+1$, and

$$u = \frac{u+2m}{2u+4m+1}.$$

Example 5 If $N = m^2 + 3$ with $m \geq 2$, then $u = \sqrt{N} - m$.

(i) If $m = 3n$, then

$$\begin{aligned}
\frac{1}{u} &= \frac{\sqrt{N}+m}{3}, \quad a_1 = 2n, \qquad Tu = \frac{\sqrt{N}-m}{3}, \\
\frac{1}{Tu} &= \sqrt{N}+m, \quad a_2 = 2m, \quad T^2u = u.
\end{aligned}$$

Thus there are no solutions to $\sqrt{q^2N-1} \in \mathbb{Z}^+$, $p_1 = 1$, $p_2 = 2m$, $q_1 = 2n$, $q_2 = 4mn+1$, $\beta_2 = 2mn+1$, and

$$u = \frac{u+2m}{2nu+4mn+1}.$$

(ii) If $m \in \{2n+1, 2n+2\}$, the outcome depends on properties of n. For example, if $N = 19 = (3 \cdot 1 + 1)^2 + 3$, then

$$\begin{aligned}
\frac{1}{u} &= \frac{\sqrt{19}+4}{3}, \quad a_1 = 2, \qquad Tu = \frac{\sqrt{19}-2}{3}, \\
\frac{1}{Tu} &= \frac{\sqrt{19}+2}{5}, \quad a_2 = 1, \quad T^2u = \frac{\sqrt{19}-3}{5}, \\
\frac{1}{T^2u} &= \frac{\sqrt{19}+3}{2}, \quad a_3 = 3, \quad T^3u = \frac{\sqrt{19}-3}{2}, \\
\frac{1}{T^3u} &= \frac{\sqrt{19}+3}{5}, \quad a_4 = 1, \quad T^4u = \frac{\sqrt{19}-2}{5}, \\
\frac{1}{T^4u} &= \frac{\sqrt{19}+2}{3}, \quad a_5 = 2, \quad T^5u = \frac{\sqrt{19}-4}{3}, \\
\frac{1}{T^5u} &= \sqrt{19}+4, \quad a_6 = 8, \quad T^6u = u.
\end{aligned}$$

Thus there are no solutions to $\sqrt{19q^2-1} \in \mathbb{Z}^+$, $p_5 = 14$, $p_6 = 117$, $q_5 = 39$; $q_6 = 326$, and so $\beta_6 = 170$ and

$$u = \frac{14u+117}{39u+326}.$$

If $N = 52 = (3 \cdot 2 + 1)^2 + 3$, then

$$\begin{aligned}
\frac{1}{u} &= \frac{\sqrt{52}+7}{3}, \quad a_1 = 4, \qquad Tu = \frac{\sqrt{52}-5}{3}, \\
\frac{1}{Tu} &= \frac{\sqrt{52}+5}{9}, \quad a_2 = 1, \qquad T^2u = \frac{\sqrt{52}-4}{9}, \\
\frac{1}{T^2u} &= \frac{\sqrt{52}+4}{4}, \quad a_3 = 2, \qquad T^3u = \frac{\sqrt{52}-4}{4}, \\
\frac{1}{T^3u} &= \frac{\sqrt{52}+4}{9}, \quad a_4 = 1, \qquad T^4u = \frac{\sqrt{52}-5}{9}, \\
\frac{1}{T^4u} &= \frac{\sqrt{52}+5}{3}, \quad a_5 = 4, \qquad T^5u = \frac{\sqrt{52}-7}{3}, \\
\frac{1}{T^5u} &= \sqrt{52}-7, \quad a_6 = 14, \quad T^6u = u.
\end{aligned}$$

Thus, there are no solutions to $\sqrt{52q^2-1} \in \mathbb{Z}^+$, $p_5 = 19$, $p_6 = 270$, $q_5 = 90$, $q_6 = 1279$, $\beta_6 = 649$, and

$$u = \frac{19u+270}{90u+1279}.$$

If $N = 28 = (3 \cdot 1 + 2)^2 + 3$, then

$$\begin{aligned}
\frac{1}{u} &= \frac{\sqrt{28}+5}{3}, \quad a_1 = 3, \qquad Tu = \frac{\sqrt{28}-4}{3}, \\
\frac{1}{Tu} &= \frac{\sqrt{28}+4}{4}, \quad a_2 = 2, \qquad T^2u = \frac{\sqrt{28}-4}{4}, \\
\frac{1}{T^2u} &= \frac{\sqrt{28}+4}{3}, \quad a_3 = 3, \qquad T^3u = \frac{\sqrt{28}-5}{3}, \\
\frac{1}{T^3u} &= \sqrt{28}+5, \quad a_4 = 10, \quad T^4u = u.
\end{aligned}$$

Thus there no solutions to $\sqrt{q^2N-1} \in \mathbb{Z}^+$, $p_3 = 7$, $p_4 = 72$, $q_3 = 24$, $q_4 = 247$, $\beta_4 = 127$, and

$$u = \frac{7u+72}{24u+247}.$$

If $N = 67 = (3 \cdot 2 + 2)^2 + 3$, then

$$\begin{aligned}
\frac{1}{u} &= \frac{\sqrt{67}+8}{3}, \quad a_1 = 5, \qquad Tu = \frac{\sqrt{67}-7}{3}, \\
\frac{1}{Tu} &= \frac{\sqrt{67}+7}{6}, \quad a_2 = 2, \qquad T^2u = \frac{\sqrt{67}-5}{6}, \\
\frac{1}{T^2u} &= \frac{\sqrt{67}+5}{7}, \quad a_3 = 1, \qquad T^3u = \frac{\sqrt{67}-2}{7}, \\
\frac{1}{T^3u} &= \frac{\sqrt{67}+2}{9}, \quad a_4 = 1, \qquad T^4u = \frac{\sqrt{67}-7}{9}, \\
\frac{1}{T^4u} &= \frac{\sqrt{67}+7}{2}, \quad a_5 = 7, \qquad T^5u = \frac{\sqrt{67}-7}{2}, \\
\frac{1}{T^5u} &= \frac{\sqrt{67}+7}{9}, \quad a_6 = 1, \qquad T^6u = \frac{\sqrt{67}-2}{9}, \\
\frac{1}{T^6u} &= \frac{\sqrt{67}+2}{7}, \quad a_7 = 1, \qquad T^7u = \frac{\sqrt{67}-5}{7}, \\
\frac{1}{T^7u} &= \frac{\sqrt{67}+5}{6}, \quad a_8 = 2, \qquad T^8u = \frac{\sqrt{67}-7}{6}, \\
\frac{1}{T^8u} &= \frac{\sqrt{67}+7}{3}, \quad a_9 = 5, \qquad T^9u = \frac{\sqrt{67}-8}{3}, \\
\frac{1}{T^9u} &= \sqrt{67}+8, \quad a_{10} = 16, \quad T^{10}u = u.
\end{aligned}$$

Thus there no solutions to $\sqrt{67q^2-1} \in \mathbb{Z}^+$, $p_9 = 1106$, $p_{10} = 1709$, $q_9 = 5967$, $q_{10} = 96578$, $\beta_{10} = 48842$, and

$$u = \frac{1106u+1709}{5967u+96578}.$$

M.I.T., 2-380
Cambridge, MA 02139, USA
dws@math.mit.edu