SQUARE ROOTS,
FROM 1; 24, 51, 10
TO DAN SHANKS

Ezra Brown
BURNING QUESTIONS

WHOSE ANSWERS YOU’VE

ALWAYS WANTED TO KNOW:

- What does $1; 24, 51, 10$ have to do with square roots?

- How have square roots been approximated throughout history?

- How do you take square roots by hand?

- Who was Dan Shanks, and what does he have to do with square roots?

For the answers, stick around.
1; 24, 51, 10

From Tablet 7289 (Yale Collection), Mesopotamian (~ 1800 B.C.E.):
the inscription

1;24,51,10

This is base sixty:

\[ 1; 24, 51, 10 = 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3} \]

\[ = \frac{30547}{21600} \]

\[ = 1.41421296\ldots, \text{ and} \]

\[ (1; 24, 51, 10)^2 = 1; 59, 59, 59, 38, 1, 40 \]

\[ = 1.999998304\ldots \]

- How’d they find it?
**SUCCESSIVE APPROXIMATIONS**

... probably.

**Big Idea:** If $0 < a < \sqrt{2}$, then $\frac{2}{a} > \sqrt{2}$. If $a > \sqrt{2}$, then $0 < \frac{2}{a} < \sqrt{2}$. In both cases, $\frac{1}{2}(a + \frac{2}{a})$ is even closer to $\sqrt{2}$.

<table>
<thead>
<tr>
<th>Step</th>
<th>Approximation $a$</th>
<th>$\frac{2}{a}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\frac{3}{2} = 1; 30$</td>
<td>$\frac{4}{3}$</td>
</tr>
<tr>
<td>2</td>
<td>$\frac{17}{12} = 1; 24$</td>
<td>$\frac{24}{17}$</td>
</tr>
<tr>
<td>3</td>
<td>$\frac{577}{408} = 1; 24, 51, 10, 35, \ldots$</td>
<td></td>
</tr>
</tbody>
</table>
A BIGGER PICTURE:

HERON OF ALEXANDRIA’S METHOD

(FIRST CENTURY C.E.)

Theorem: Let $n$ and $\alpha$ be positive, let $d$ be a nonnegative integer, and define $h(\alpha) := (\alpha + n/\alpha)/2$. Then:

- $\sqrt{n}$ is between $\alpha$ and $n/\alpha$.
- If $\alpha > 0$, then $h(\alpha) > \sqrt{n}$.
- $|h(\alpha) - \sqrt{n}| = \frac{(\alpha - \sqrt{n})^2}{2\alpha}$
- If $|\alpha - \sqrt{n}| < 10^{-d}$, then
  $$|h(\alpha) - \sqrt{n}| < \min\{10^{-2d}, (\alpha - \sqrt{n})/2\}$$

Heron’s Square Root Algorithm: Define the sequence $\{\alpha_n\}$ by $\alpha_0 = \alpha$, $\alpha_1 = h(\alpha_0)$, \ldots, and $\alpha_{n+1} = h(\alpha_n)$ in general. Then $\{\alpha_n\}$ converges quadratically to $\sqrt{n}$.

Special Case $n = 2$, $\alpha_0 = 3/2$; then $\alpha_2 = 577/408 = 1; 24, 51, 10$

Newton’s Method (rediscovered 1674): Under favorable conditions, the sequence $(x_k)$, defined by $x_{k+1} = x_k - \frac{f(x_k)}{f'(x_k)}$ converges to a root of $f$.

Special Case $f(x) = x^2 - n$, $f'(x) = 2x$ and so

$$x_{k+1} = x_k - \frac{x_k^2 - n}{2x_k} = \frac{1}{2} \left( x_k + \frac{n}{x_k} \right),$$

which is Heron’s Algorithm.
ANOTHER WAY:

CONTINUED FRACTIONS

- **What are they?** A finite simple continued fraction (SCF) is an expression of the form

\[
a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ldots + \cfrac{1}{a_{k-1} + \cfrac{1}{a_k}}}}}
\]

:= \langle a_0, a_1, a_2, \ldots, a_k \rangle,

where the \(a_i\)'s are integers and \(a_i \geq 1\) for \(i \geq 1\).

- **Why are they important?** Notice that

\[577^2 - 2 \cdot 408^2 = 1.\]

SCF’s help with an old problem: Existence and construction of nonzero solutions to

\[x^2 - ny^2 = 1,\]

where \(n\) is a positive nonsquare integer.

- **Wait a minute!** Just what do they have to do with square roots?

Patience!
CONTINUED FRACTIONS
AND SQUARE ROOTS

A Few Facts:

- \(0 \leq x - a_0 < 1\), so \(a_0 = \lfloor x \rfloor\), the greatest integer \(\leq x\).

- If we set \(x_0 := x\), \(x_1 := \frac{1}{x_0 - a_0}\), and in general \(x_{k+1} := \frac{1}{x_k - a_k}\),
  then \(a_i = \lfloor x_i \rfloor\).

- If the \(a_i\)'s are real, \(a_i \geq 1\) for \(i \geq 1\) and we define \(s_k := \langle a_0, a_1, a_2, \ldots, a_k \rangle\), then \(\{s_k\}\) converges to a real number \(x\).

Try this on \(x = \sqrt{2}\):

\[
\begin{align*}
x_0 &= \sqrt{2}, a_0 = \lfloor x_0 \rfloor = 1 \\
x_1 &= \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1, a_1 = \lfloor x_1 \rfloor = 2 \\
x_2 &= \frac{1}{\sqrt{2} - 1} = \sqrt{2} + 1, a_2 = \lfloor x_2 \rfloor = 2 \\
\end{align*}
\]

\(\ldots\) hey, it repeats!

\[
\sqrt{2} = \langle 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, \ldots \rangle
\]

\(= \langle 1, \overline{2} \rangle\).

The part under the bar repeats.
The Heron Approximations to $\sqrt{2}$ and Continued Fractions

Notice that
\[
\frac{17}{12} = 1 + \frac{5}{12} = 1 + \frac{1}{\frac{12}{5}} = 1 + \frac{1}{2 + \frac{2}{5}} = 1 + \frac{1}{2 + \frac{1}{\frac{2+5}{2}}}
\]
\[
= 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2}}} = \langle 1, 2, 2, 2 \rangle.
\]

This is typical of the Heron approximations to $\sqrt{2}$:

\[
1 = \langle 1 \rangle,
\]
\[
3 = \langle 1, 2 \rangle,
\]
\[
\frac{17}{12} = \langle 1, 2, 2, 2 \rangle,
\]
\[
\frac{577}{408} = \langle 1, 2, 2, 2, 2, 2 \rangle,
\]
\[
\frac{665857}{470832} = \langle 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2 \rangle,
\]
\[
\frac{886731088897}{627013566048} = \langle 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2, 2 \rangle,
\]

that is, each iteration doubles the number of partial quotients.

**Theorem** If $a_1 = 3/2$ is the first Heron approximation to $\sqrt{2}$, then

\[
a_n = \langle 1, 2, 2, 2, \ldots, 2 \rangle (2^n - 1 \text{ 2's in all})
\]
**Burning Question:** The SCF for $\sqrt{n}$ begins with $[\sqrt{n}]$. How do you find $[\sqrt{n}]$ in the first place if, say, 

$$n = 3600277840830799482590179622558261311759349942860011?$$

**Answer:** Here’s a way:

**SQUARE ROOTS BY HAND**

**Theorem SRH** Let $a$ and $b$ be non-negative integers, with $a > 0$ and $b < 100$. If $c = [\sqrt{a}]$ and

$$d = \max\{j : j \text{ is a non-negative integer and } (20c+j)j \leq 100(a-c^2)+b\},$$

then $10c + d = [\sqrt{100a+b}]$.

**Key Step:** That $(20c+j)j \leq 100(a-c^2)+b$ business.

**Example:** Find $\sqrt{41897492}$.

\[
\begin{array}{cccc}
6 & 4 & 7 & 2 \\
\sqrt{41} & 89 & 74 & 92. \\
36 & \\
124 & 5 & 89 \\
\text{4 & 96} \\
1287 & 93 & 74 \\
\text{90 & 09} \\
1294\underline{2} & 3 & 65 & 92 \\
\text{2 & 58 & 84} \\
1 & 07 & 08
\end{array}
\]
\[ \sqrt{2} \text{ BY HAND} \]

\[ \sqrt{2}. \begin{array}{cccccc}
1. & 4 & 1 & 4 & 2 & 1 & 3 \\
\hline
& 00 & 00 & 00 & 00 & 00 & 00 \\
24 & 1 & 00 \\
96 & \\
281 & 4 & 00 \\
2 & 81 \\
2824 & 1 & 19 & 00 \\
1 & 12 & 96 \\
28282 & 6 & 04 & 00 \\
5 & 65 & 64 \\
282841 & 38 & 36 & 00 \\
28 & 28 & 41 \\
2828423 & 10 & 07 & 59 & 00 \\
8 & 48 & 52 & 69 \\
1 & 59 & 06 & 31 \\
\end{array} \]

\[ 1.414213^2 = 2 - 0.000001590631, \text{ and} \]

\[ 1.414214^2 = 2 + 0.000001237796. \]
**MODULAR SQUARE ROOTS**

- **Square Roots mod m:** For $x, a, m$ integers and $m > 0$, $x$ is a square root of $a$ mod $m$ provided $x^2 \equiv a \mod m$.

- **Dan Shanks’ observation about square roots mod $p$:**

  - ♠️ $p$ an odd prime $\Rightarrow p - 1 = s \cdot 2^e$ with $s$ odd and $e > 0$.

  - ♠️ $x = a^{(s+1)/2} \Rightarrow x^2 \equiv a^{s+1} \equiv a^s \cdot a \mod p$

  - ♠️ $a^{(s+1)/2}$ is almost the square root of $a \mod p$

  - ♠️ $a^s \equiv 1 \mod p \Rightarrow a^{(s+1)/2}$ is the square root of $a \mod p$ (two-thirds of the time, even!)

  - ♠️ $a^s \mod p$ is a $2^e$th root of unity $\mod p$

  - ♠️ $a^s \mod p$ is a fudge factor which can be updated.

- **The Shanks–Tonelli algorithm:** It updates both the initial guess $x$ and the fudge factor $a^s$ until the f.f. $\equiv 1 \mod p$. 
THE SHANKS–TONELLI ALGORITHM

1. BEGIN with an integer $a$ and a prime $p > 2$, relatively prime to $a$. Calculate $a^{(p-1)/2} \pmod{p}$. Now $a^{(p-1)/2} \equiv 1$ or $-1 \pmod{p}$.

2. IF $a^{(p-1)/2} \equiv -1 \pmod{p}$, then $a$ has no square root $\pmod{p}$. Say so, and EXIT quietly.

3. IF $a^{(p-1)/2} \equiv 1 \pmod{p}$, then we’re in business. Write $p - 1 = s \cdot 2^e$ with $s$ odd and $e$ positive.

4. FIND a number $n$ such that $n^{(p-1)/2} \equiv 1 \pmod{p}$—that is, a nonsquare $\pmod{p}$.

5. INITIALIZE these variables (all congruences are mod $p$):
   
   $x \equiv a^{(s+1)/2}$ (first guess at the square root)
   $b \equiv a^s$ (first guess at the fudge factor)
   $g \equiv n^s$ (powers of $g$ will update both $x$ and $b$)
   $r = e$ (exponent will decrease with each update of the algorithm).
   
   Note that $x^2 \equiv ba \pmod{p}$.

Now: WHILE $m > 0$

6. FIND the least integer $m$ such that $0 \leq m \leq r - 1$ and $b^{2^m} \equiv 1 \pmod{p}$. That is, find $m$ such that $\text{ord}_p(b) = 2^m$.

7. IF $m = 0$, we’re done. RETURN the value of $x$ and EXIT triumphantly.

8. IF $m > 0$, UPDATE the variables:
   
   replace $x$ by $x \cdot g^{2^r - m - 1}$
   replace $b$ by $b \cdot g^{2^r - m}$
   replace $g$ by $g^{2^r - m}$
   replace $r$ by $m$.

end WHILE
WHY DOES IT TERMINATE?

♡ Old value of $b$ satisfies $b^{2^m-1} \not\equiv 1 \pmod{p}$, but ...

♠ ... new value of $b$ satisfies $b^{2^m-1} \equiv 1 \pmod{p}$, so:

♡ The value of $m$ decreases with each update.

♡ Reason: for old $b$, $m$ minimal $\Rightarrow b^{2^m-1} \equiv -1 \pmod{p}$

♡ Also, $g^{2^r-1} \equiv -1 \pmod{p}$

♡ Hence, $(b \cdot g^{2^r-m})^{2^m-1} \equiv b^{2^m-1} g^{2^r-1} \equiv 1 \pmod{p}$

♡ But $b \cdot g^{2^r-m}$ is the new value of $b$ (see ♠)

♡ So, the new value of $m$ is less than the old value of $m$. 
AN EXAMPLE

THE SQUARE ROOT OF 2 MOD 113

SET UP: \( a = 2, p = 113, p - 1 = 7 \cdot 2^4, e = 4, s = 7, (p - 1)/2 = 56, (s + 1)/4 = 4 \)

BEGIN: \( 2^{56} \equiv 1 \pmod{113} \); we’re in business.

FIND \( n \): \( 3^{56} \equiv -1 \pmod{113} \), so \( n = 3 \).

INITIALIZE: \( x = a^{(s+1)/2} = 2^4 \equiv 16 \pmod{113} \); \( b = a^s = 2^7 \equiv 15 \pmod{113} \);
\[ g = n^s = 3^7 \equiv 40 \pmod{113} \]; \( r = e = 4 \).

FIND \( \text{ord}_p(b) = 2^m \): \( b^2 = 225 \equiv -1, b^4 \equiv 1 \pmod{113} \). Hence \( b^{2^2} \equiv 1 \pmod{113} \), and so \( m = 2 \).

\( m \neq 0 \), so UPDATE:
\[ x = x g^{2^{r-m-1}} = 16 \cdot 40^{2^{4-2-1}} = 16 \cdot 1600 \equiv 16 \cdot 18 \equiv 62 \pmod{113} \];
\[ b = b g^{2^{r-m}} = 15 \cdot 40^4 \equiv 15 \cdot (-15) \equiv 1 \pmod{113} \];
\[ g = g^{2^{r-m}} \equiv -15 \pmod{113} \];
\[ r = m = 2 \).

Since \( b = 1 \), \( \text{ord}_p(b) = 1 = 2^0 \); hence \( m = 0 \) and we’re done:
RETURN the current value of \( x \), namely 62. Sure enough, \( 62^2 = 3844 = 2 + 34 \cdot 113 \equiv 2 \pmod{113} \), and so 62 is a square root of 2 mod 113.