Mersenne's challenge and square roots

With reference to Peter Shiu's fascinating article [1], and Mersenne's challenge to Fermat, it is possible that Fermat first tried square rooting a few multiples of $N = 100895598169$ when looking for factors. $\sqrt{N}$ apparently yields nothing special, but

$$\sqrt{2N} = \sqrt{201791196338} = 449211.74999\ldots \tag{1}$$

leading to

$$2N = (449211.75)^2 - (0.25)^2 = 449212 \times 449211.5$$

whence

$$N = 112303 \times 898423.$$

Mersenne may well have kept this approach 'up his sleeve' in case Fermat 'gave up'. It works, of course, because the larger factor is 8 times the smaller minus 1. You may say 'It's a very particular case', but it works here. Arguably, trying a few $\sqrt{aN}$, as noted in [1], has a place among other preliminary tests.

One extension is to seek a pair of factors whose ratio is nearly in small numbers, $a : b$, say.

Suppose

$$N = (aX + h)(bX + k) \tag{2}$$

where a, b, h, k are small compared with X, all integers. Then

$$abN = a^2b^2X^2 + abX(ak + bh) + abhk = \left(abX + \tfrac{1}{2}(ak + bh)\right)^2 - \left(\tfrac{1}{2}(ak - bh)\right)^2. \tag{3}$$

In the square root algorithm, instead of smaller and smaller place values in the scale of 10, consider powers of x, where x is to be small compared with 1. You get

$$\sqrt{1 + x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \ldots . \tag{4}$$

Expression (4) suggests that the contribution of the terms after $\frac{1}{2}x$ is small compared with $\frac{1}{2}x$, and that, for example, in $\sqrt{a^2 + e}$, where e is small compared with a^2, the error in

$$\sqrt{a^2 + e} = a\sqrt{1 + \frac{e}{a^2}} \approx a\left(1 + \frac{1}{2}\frac{e}{a^2}\right) = a + \frac{1}{2}\frac{e}{a} \tag{5}$$

is small compared with $\frac{1}{2}\frac{e}{a}$.

Thus (3) suggests that

$$\sqrt{abN} = abX + \tfrac{1}{2}(ak + bh) + e \tag{6}$$

where e is small compared with $\frac{1}{2}(ak + bh)$.

Now if a form (2) exists, $\frac{1}{2}(ak + bh)$ will be half an integer. So if we find the decimal part of $\sqrt{abN}$ is close to 0 or 0.5, it may be worth squaring the value but with exactly 0 or 0.5.

https://doi.org/10.1017/mag.2016.26 Published online by Cambridge University Press

Further, if ab has a squared factor, say $ab = c^2d$, we may reach a factorisation sooner, on square rooting dN. In Mersenne's case, $ab = 8$ but $d = 2$.

Dividing both sides of (6) by c,

$$\sqrt{dN} = \frac{abX}{c} + \frac{1}{2}\frac{ak + bh}{c}, \text{ approximately,}$$

where $\frac{abX}{c}$ is an integer.

If we find the decimal part of $\sqrt{dN}$ is close to some fraction in small numbers, it may be worth rounding the value found to this exact fraction and squaring.

For example, with

$$N = 3978254131$$

$$\sqrt{5N} = 141036.41605\ldots$$

where the decimal part is close to 5/12.

So $12 \times \sqrt{5N}$ is close to 1692437. Squaring the latter

$$1692437^2 = 2864342998969$$

and comparing, we get

$$720N = 1692437^2 - 24649 = 1692437^2 - 157^2 = 1692594 \times 1692280$$

and

$$N = 94033 \times 42307,$$

incidentally both prime factors, and whose ratio is nearly 20 : 9.

In a classroom

The Square Root Algorithm in our ordinary base 10 is one gateway to the heroic age of table-making in the 16 th and 17 th centuries. I think it best to work an example in integers, which excites curiosity, another across the decimal point with a zero digit somewhere in the root, and then explain you are simply completing and subtracting squares. Then, and only then, illustrate with the square root of, say, $a^2 + 2ab + b^2 + 2ac + 2bc + c^2$ (which involves commenting on place values). A bonus in (1) above is the pupils' 'aha!' as the trailing 9s appear.

After that, pupils begin to appreciate Henry Briggs's work in 'filling in the gaps' between $\log 1 = 0$ and $\log 10 = 1$. Starting with $\log \sqrt{10} = 0.5$, he continued to take the square root of the most recent number. After a while the logarithms become linear with respect to the numbers (why?) and the gaps easier to fill. Briggs worked to 35 places of decimals and the logarithms became linear after 54 extractions. (See, for example, [2].) Similarly, with trigonometrical tables, one can start with a 45° or 60° triangle and use the formulae for sine and cosine of half the angle.

https://doi.org/10.1017/mag.2016.26 Published online by Cambridge University Press

Why does (4) only 'suggest'? Can you be more precise? (Here, try multiplying the 'contribution' $\sqrt{1+x} - \left(1 + \frac{1}{2}x\right)$ by $\sqrt{1+x} + \left(1 + \frac{1}{2}x\right)$ and discussing the value of the multiplier.)

Mental arithmetic: what is $\sqrt{7.4}$ to 3 significant figures? (If you know your squares up to, say, $32^2 = 1024$, start with $740 = 27^2 + 11$.) What is the square root algorithm in binary?

Lastly, or as an appetiser, one can work out the formula for the distance of the horizon in Imperial measure, namely $\sqrt{\frac{3h}{2}}$ miles, where h is the height in feet. Why are the numbers so simple?

References

1. Peter Shiu, Fermat's method of factorisation, *Math. Gaz.* **99** (March 2015) pp. 97-103.
2. Charles Hutton, *Mathematical Tables*, London (1804) pp. 64-65.

doi:10.1017/mag.2016.26

JOHN B. CAMERON
21 Monks Way, Reading RG30 3DP

When is the sum of two triangular numbers triangular?

It was good to see Erick Gooding's 30 year involvement with *Mathematical Pie* celebrated in the June 2015 *MA News*. His *Pie Notes* are a constant source of inspirational ideas and the Summer 2015 issue was certainly no exception, providing the starting-point for this article. The item 'Sum of the squares become triangles' concerns triangular numbers, $T(n) = \frac{1}{2}n(n+1)$, satisfying the relationship

$$T(x) + T(y) = T(z) \qquad (*)$$

for whole numbers x, y, z.

Erick notes that an infinite set of solutions is provided by

$$T\big(T(n) - 1\big) + T(n) = T\big(T(n)\big)$$

and, for this set, $T(n) - 1$, n and $T(n)$ form the sides of an obtuse-angled triangle which becomes increasingly right-angled as $n \to \infty$. He also lists seven other solutions of $(*)$ which are not part of this set.

Our first result is that for *any* solution of $(*)$, the lengths x, y, z form the sides of an obtuse-angled triangle which is increasingly right-angled as the perimeter $x + y + z$ increases.

For if $T(x) + T(y) = T(z)$, then $\frac{1}{2}x(x+1) + \frac{1}{2}y(y+1) = \frac{1}{2}z(z+1)$ so that $x^2 + y^2 - z^2 = z - x - y$ or $(x+y)^2 - z^2 + x + y - z = 2xy$ whence $(x + y - z)(x + y + z + 1) = 2xy$.

It follows that $x + y > z$ giving the required triangle inequality; also

$$\cos Z = \frac{x^2 + y^2 - z^2}{2xy} = \frac{z - x - y}{2xy} = \frac{-1}{x + y + z + 1}.$$

https://doi.org/10.1017/mag.2016.26 Published online by Cambridge University Press