# HUNTERS AND FARMERS


## Clark Barwick


We have to start somewhere. It might as well be with three rational numbers $a$, $b$, and $c$ (with $a \neq 0$) and a quadratic equation

$$ax^2 + bx + c = 0.$$

A little trick[1] involving *completing the square* gives you a formula

$$x = \frac{1}{2a}\left(-b \pm \sqrt{b^2 - 4ac}\right).$$

[1] It's fun to remember how this goes: assume $a = 1$; now rewrite your equation as

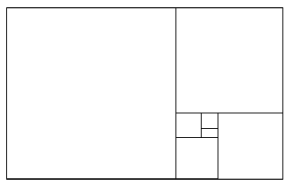
$$x^2 + bx + (b/2)^2 = (b/2)^2 - c,$$

and note that the left side is $(x + b/2)^2$.

This formula shows you a couple of things.

Right away, you now have a tool with which to get very precise answers to interesting questions. When the designers of a new tablet computer boast its *diagonal length of* 30 *centimetres, giving you a screen area of half a square metre!*, you get suspicious, and let $d$ be the diagonal and $A$ be the area. So its measurements are $x$ by $A/x$, where $x^2 + A^2/x^2 = d^2$. So your formula tells you that $x^2 = \frac{1}{2}(d^2 \pm \sqrt{d^4 - 4A^2})$, but since their numbers give $2A > d^2$, you're pretty sure that tablet isn't gonna live up to the hype.

And you read somewhere that ancient Greeks liked to use rectangles with the property that if you lop off a square with a single cut, what you'll be left with is a rectangle with the same proportions. *What are those proportions?* Well, if the short side has length 1, the long side will have length $x$, where



$$x = \frac{1}{x-1}.$$

Your formula tells you that

$$\begin{aligned} x &= \frac{1}{2}\left(1 + \sqrt{5}\right) \\ &= 1.6180339887498948482045868343656 \\ &\quad\ 38117720309179805762862135448 \\ &\quad\ 6227052604628189024497072072 04 \cdots . \end{aligned}$$

There's that rush of satisfaction at having a complete, tidy answer. You might feel a twinge of annoyance that $x$ is not a nice rational number – you didn't get to just shout *Six!* or *Five-twelfths!* and do a mic-drop – but still, that's the answer in a relatively neat package.

BUT THE REALISATION that $x$ is not rational shows you a second thing: the quest for a solution to your equation has forced you into to take on more numbers than you had to start with. After all, $a$, $b$, and $c$ were just rational numbers. The question *what is x?* certainly made perfect sense without knowing anything but rational numbers, but the answer doesn't – to understand it, you have to accept new numbers like $\sqrt{5}$.

In fact, now that you think of it, this isn't the first time a problem forced you contend with a new object: you learned to count with what we now call the set

$$\mathbf{N} \coloneqq \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \dots\}.$$

Then you realised you also had to quantify nothing[2], and after a sleepless night contemplating the void, you came to grips with the set

$$\mathbf{N}_0 \coloneqq \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, \dots\}.$$

[2] *The introduction of the cipher* 0 *or the group concept was general nonsense too, and mathematics was more or less stagnating for thousands of years because nobody was around to take such childish steps …* – A. Grothendieck

But then you found yourself trying to contemplate a number that when you add it to 3 gives you 2.

> — *But three is bigger than two!* — Yeah, but maybe it exists anyhow, like when you owe more money than you have, or when you're below sea level. — *But three is bigger than two!* — Yeah, but look: I can consider solutions to any equation $x + a = b$ with $a, b \in \mathbf{N}_0$ …

Thus your universe grew a little:

$$\mathbf{Z} \coloneqq \{\dots, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, \dots\}.$$

With that, your powers increased: now you can add, multiply, and *subtract*.[3]

[3] And not that impoverished subtraction where you only knew how to make $b - a$ when $b$ was at least as big as $a$.

And you found yourself trying to find a number that when you multiply it by two gives you three.

> — *But two doesn't go into three!* — Yeah, but when you put three equal line segments together end to end, there definitely *is* a place that's halfway between the ends. — *But two doesn't go into three!* — Yeah, but maybe it's a new number I could call 3/2, and it would be the solution to the equation $2x = 3$. In fact, for any $m, n \in \mathbf{Z}$, as long as $m \neq 0$, I can add solutions to $mx + n = 0$ …

Again your universe grew: $\mathbf{Q}$. Now you can add, multiply, subtract, and *divide*.

The quadratic formula fits nicely into this pattern of growth and mind-expansion. As long as you know how to form the square root of any rational number, you can use your formula to solve any equation $ax^2 + bx + c = 0$.

That means accepting a bunch of new numbers like $\sqrt{3}$ which at least are reasonable geometrical distances, but also a bunch of numbers like the two square roots of $-1$, neither of which could be the length of anything![4] If fact, as soon as you accept $\sqrt{d}$ for a squarefree[5] integer $d$, you earn the right to solve any quadratic equation $ax^2 + bx + c = 0$ with $a, b, c \in \mathbf{Q}$ and $b^2 - 4ac = q^2 d$ for some $q \in \mathbf{Q}$.

[4] — *But the square of any number is nonnegative!*

[5] An integer is *squarefree* if the only perfect square that divides it is 1.

That is, if you write $\mathbf{Q}(\sqrt{d})$ for the set of numbers of the form $s + t\sqrt{d}$ with $s, t \in \mathbf{Q}$, then $\mathbf{Q}(\sqrt{d})$ is a *field* in which you can solve a nice fat family of quadratic equations. Furthermore, you're permitted to continue expanding your mind:

$$\mathbf{Q} \subset \mathbf{Q}(\sqrt{-1}) \subset \mathbf{Q}(\sqrt{-1})(\sqrt{2}) \subset \mathbf{Q}(\sqrt{-1})(\sqrt{2})(\sqrt{3}) \subset \mathbf{Q}(\sqrt{-1})(\sqrt{2})(\sqrt{3})(\sqrt{5}) \subset \cdots$$

You can call the union of all these $K$, then you've built yourself a very big field in which you can find the roots of any quadratic polynomial with rational coefficients. The quadratic formula permits you build the whole tower just by adding a sequence of new square roots to $\mathbf{Q}$.

Let's pause the story and reflect. On one hand, we have a useful computational tool for giving definitive answers to particular questions. On the other hand, it is telling us something structural and conceptual about the collection of *all* solutions to a class of problem. Each of these perspectives is important, and each is emblematic of a kind of mathematician.

On one hand, there are folks who are good at using their knowledge to strike fast to find quick, clever, and sometimes unexpected solutions to narrowly-delineated problems. *The quadratic formula gives you a precise expression for the golden ratio as* $\frac{1}{2}(1 + \sqrt{5})$. These are HUNTERS – they patrol on the outside of a cluster of gazelles, waiting for the moment when one becomes isolated from the herd, so they can strike with their overwhelming power.

On the other hand, there are those who reflect on the patterns they observe, and they develop large programs and concepts to understand these patterns. They open up new avenues of research with the methodical development of ideas. *The quadratic formula shows us that we can enlarge the field of rational numbers to contain the roots of quadratic polynomials, just by adding in all the square roots of integers.* These are FARMERS – they plant seeds, water crops, watch the skies, spend time working with the soil, nurturing an idea to the eventual harvest.

There's been a lot of discussion of these two kinds of mathematicians, but perhaps not with these labels. Jean-Pierre Serre is a hunter, as is Sir Michael Atiyah. Alexander Grothendieck was a farmer, as was Daniel Kan.[6] My main point is:

[6] I too, am a pretty unmistakable farmer.

**Hunters and farmers are both necessary.**

These days especially, hunters are generally the ones to win the accolades and get papers in the best journals. They 'score' higher. This is not hard to understand: hunters speak directly to the limbic system, and solved problems – particularly at this point in history – are the coin of the realm. At the same time, however, the best farmers get to write for the ages and make an indelible mark on the community.

Farmers' work is expansive, quiet, and slow. We don't typically leave the farm unless we need to buy equipment. We need time: we don't catch a quick harvest between meetings. We work for a long time on a certain crop, harvest, and then plant a new crop, adapted to the soil left behind. When we aren't at work, we are asleep. That's not because we're rushed or bullied; it's simply because there's always something to do on the farm. You don't have to be fast to work on a farm, though a certain amount of physical strength is obviously helpful.

By contrast, hunting is a hell of a lot more exciting, at least from the outside. Hunters may work over vast domains, or they may confine themselves to relatively small areas where plenty of prey can be found. They spend plenty of time stalking their prey, but their jobs are completed in very short bursts. Speed and raw power are necessities, as are the right set of 'accidents' – just happening upon that herd of oryxes ...The stakes are higher: whereas harvests can vary by degree, a hunt is almost binary – either you solve the problem or you don't. As a hunter, there is a greater risk that you'll fail dramatically and go hungry.

You might be wondering – which are you?[7] Your habits of mind, the results and ideas that captivate you, the kinds of mathematical objects you find yourself wondering about and playing with – all of these will suggest a direction. But here are some principles:

[7] *Are you a hunter or a farmer? Take our online quiz and find out!*

- Don't deny yourself. There are a lot of hunters who try too hard to be farmers for part of their careers, and a lot of farmers who try too hard to be hunters for part of their careers.[8] Follow up on your natural predilections. Don't be afraid to love the mathematics you love.

[8] I've fallen into this trap myself.

- At the same time, don't try classify yourself too early. There's no need to get hung up on labels.[9] You'll even find that your attitudes may change as you age.
- Regardless of whether you're a hunter or a farmer, *you must read everything*. That paper on abstract widgets might provide a tool that a skilled hunter can deploy, and that masterstroke solution in that paper might be a special case of a general pattern that a skilled famer can cultivate.

[9] There are even a handful of people who have been successful both at hunting and farming, and they are amazing. Deligne's a good example.

Let's return to our story. It turns out that there's a *cubic formula* too.[10] If $a$, $b$, $c$, and $d$ are rational numbers (with $a \neq 0$), then the equation

$$ax^3 + bx^2 + cx + d = 0$$

can be solved, first by assuming $a = 1$ and performing the substitution $x = t - b/3$ to get it to the form

$$t^3 + pt + q = 0.$$

Then the formula says that the three solutions are all of the form

$$\left(-q/2 + \sqrt{(p/3)^3 + (q/2)^2}\right)^{1/3} + \left(-q/2 - \sqrt{(p/3)^3 + (q/2)^2}\right)^{1/3}.$$

One has to mumble something now about how to select the cube roots correctly, but it can be done. This formula shows you that the roots all lie in a field obtained by tacking on a square root and then a cube root:

$$\mathbf{Q} \subseteq \mathbf{Q}(\sqrt{r}) \subseteq \mathbf{Q}(\sqrt{r})(\alpha_1^{1/3}) \subseteq \mathbf{Q}(\sqrt{r})(\alpha_1^{1/3})(\alpha_2^{1/3}),$$

where $\alpha_1, \alpha_2 \in \mathbf{Q}(\sqrt{r})$.

There's a quartic equation too, discovered soon after by Ferrari. By dividing and substituting, you reduce to a monic without a 3rd degree term. Then some clever substitutions let you turn this into a combination of cubics and quadratics. The general formula is far too much for a mere mortal to remember, but gazing upon its intricacies leads you to ask yourself:

**What exactly are we achieving when we write these formulas?**

On one hand, there is a certain kind of fun and satisfaction at seeing these impressively enormous formulas – though maybe that satisfaction is waning

[10] This is usually credited to various Italian mantematicians from the 16th century – del Ferro and Tartaglia most particularly.

as these formulas get more involved. On the other, we are actually saying something conceptual about the roots of our polynomials: if $f$ a polynomial $a_n x^n + \cdots + a_0$. Expressing the roots of $f$ with radicals is really saying that the roots of $f$ all lie in a field $F \supseteq \mathbf{Q}$ that can be obtained via a sequence of field extensions

$$\mathbf{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

in which[11] $F_{i+1} = F_i(\alpha_i^{1/p_i})$.

[11] Here, the $p_i$'s are prime.

The next task, to generate a formula to solve the quintic, sat around unsolved for the next three centuries. It was Abel (following an incomplete proof by Ruffini) who was the first to show that for $n = 5$, there are quintic equations whose roots can't be expressed with radicals. In fact, here's one now:

$$x^5 - x - 1 = 0.$$

This has one real root and two distinct pairs of complex conjugate roots, but none of them can be expressed with radicals.

Abel's proof is the classic work of the hunter. It's a sequence of moves that are mostly simple, ingenious, and precisely adapted to the problem at hand. As you read his argument,[12] you get the strong impression of someone who isn't setting up a theory or establishing a general way of thinking about these objects – he's going in for the kill.

[12] Michael Rosen wrote an excellent exposition of the argument in the *American Mathematical Monthly* in 1995.

By contrast, Galois's proof, which is the one we now usually teach, has all the hallmarks of a farmer. Galois isn't telling you how to prove the unsolvability of the quintic; he's telling you how to think of *any* problem of this kind[13]. In keeping with his farmerly nature, his papers were rejected – a few times, it seems.

[13] and if you're lucky, solve it!

One thing I abhor is the stifling clouds of exaltation that settle in around some mathematicians who do good work. Galois's biography is most certainly romantic and entertaining, but too often you see an unsettling sort of idolatry emerge when one speaks of Galois. Excellent and underappreciated mathematician though he was, Galois was just another form of life. If he walked into the room now, we wouldn't have to avert our gaze. This unwarranted mystification is a terrible trap that mathematics finds itself in all too often. These people aren't magicians; they toiled for years with their ideas and computations.

In preparing this talk, I was tooling about on the Internet to learn a bit about how Galois understood his groups. I stumbled upon a messageboard where someone was educating themselves on some Galois theory, and asked a pretty reasonable question about how one connected two ideas they'd seen. I then saw the responses, which varied from the revoltingly elitist[14] to obfuscatingly worshipful.[15] There is no place for such nonsense in our subject.

[14] — *You can't learn Galois theory properly just from a book.* — Bollocks. This stuff isn't a secret; the books are excellent and clear; this stuff is out there for everyone.

[15] — *Only a genius like Galois could see this.* — Bollocks! This person wasn't even asking a hard question. Stop letting your idol (idle?) reverence get in the way of your comprehension.

**Standing in awe is an unsuitable posture for a mathematician.**

WE'VE ACCEPTED THAT expressing the roots of a polynomial $f$ with radicals is really saying that the roots $\theta_1, \ldots, \theta_n$ all lie in a field $F \supseteq \mathbf{Q}$ that can be obtained via a sequence of field extensions

$$\mathbf{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F$$

in which $F_{i+1} = F_i(\alpha_i^{1/p_i})$.

Note that at each stage, adding in one $p_i$-th root of $\alpha_i$ is meant to add in all the others as well. If you think about where the $p_i$-th roots of 1 sit inside $\mathbf{C}$, you'll notice that these roots can be permuted cyclically, but there's something fishy about other permutations – they aren't *algebraic*. To make that precise, we'll say that a permutation $\sigma$ of some finite collection of elements $r_1, \ldots, r_n$ in a field extension $E \supseteq E'$ is *E-algebraic* if, for any polynomial $F \in E[x_1, \ldots, x_n]$ in $n$ variables with coefficients in $E$, one has

$$F(r_1, \ldots, r_n) = 0 \text{ if and only if } F(r_{\sigma(1)}, \ldots, r_{\sigma(n)}) = 0.$$

That is, $E$-algebraic permutations are those that don't destroy algebraic relations among the elements with coefficients from $E$. When I look at the roots of a quadratic equation, for example, the fact that it's only a change in sign on the square root in the quadratic formula is basically ensuring that swapping them is an algebraic operation.

This is a key observation: the solutions of a linear equation are unique, but the solutions of a general polynomial equation $f(x) = 0$ have a *higher order unicity*; they aren't unique, but if $f$ is irreducible, then the algebraic permutations of the roots act transitively.

So when we look at a sequence of field extensions

$$\mathbf{Q} = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_n = F,$$

in which $F_{i+1} = F_i(\alpha_i^{1/p_i})$, we see a sequence of cyclic groups $C_{p_i}$, which are the groups of $F_i$-algebraic permutations of the $p_i$-th roots. Expressed differently, the field automorphisms of $F_{i+1}$ that fix $F_i$ form the group

$C_{p_i}$. Now, when we look at the group $G$ of field automorphisms of $F$, this filtration of fields produces a composition series of $G$ whose quotients are the cyclic groups $C_{p_i}$.

But now we discover an obstruction to our ability to express the roots of $x^5 - x - 1$ in terms of radicals: one can do this if and only if the $\mathbf{Q}$-algebraic permutations of the roots $\theta_1, \dots, \theta_5$ form a group with a composition series whose quotients are cyclic of prime order. However, one computes directly that *every* permutation of the roots of $x^5 - x - 1$ is $\mathbf{Q}$-algebraic. But the symmetric group $\Sigma_5$ has a short composition series: $1 \subset A_5 \subset \Sigma_5$, and $A_5$ is not cyclic.

Galois theory is a piece of 20th century mathematics that somehow slipped into the 19th century. Instead of contemplating objects – such as roots of polynomials – as isolated entities, Galois compels us to look at them *along with* the isomorphisms between them. This little idea turns out to be the gift that keeps on giving …