Math Club Notes: 2005 September 22

1 Spurious solutions

We discussed the phenomenon of spurious solutions. Ray gave an example something like this: find all solutions x of

$$\sqrt{5-x} = x+1$$

A typical solution:

$$\begin{aligned} \sqrt{5-x} &= x+1 \\ 5-x &= x^2+2x+1 \\ 0 &= x^2+3x-4 \\ 0 &= (x-1)(x+4) \end{aligned}$$

So $x = 1$ or $x = -4$. On testing these values in the original equation, we find that $x = -4$ is what they call a spurious solution.

The situation is made to seem more mysterious than it is by certain omissions in the problem above. In full, I'd write that solution as follows:

$$\begin{aligned} & \sqrt{5-x} = x+1 \\ \Rightarrow \quad & \{\text{square both sides}\} \\ & 5-x = x^2+2x+1 \\ \equiv \quad & \{\text{algebra}\} \\ & 0 = x^2+3x-4 \\ \equiv \quad & \{\text{factoring}\} \\ & 0 = (x-1)(x+4) \\ \equiv \quad & \{\mathbb{R} \text{ is an integral domain}\} \\ & x-1 = 0 \text{ or } x+4 = 0 \\ \equiv \quad & \{\text{algebra}\} \\ & x = 1 \text{ or } x = -4 \end{aligned}$$

The descriptions of each step are not so important here; what is important is that the first step is $\Rightarrow$, not $\equiv$ (that is, "implies", not "is equivalent to"). So what this derivation proves is

$$\forall x \in \mathbb{R}\colon \sqrt{5-x} = x+1 \Rightarrow x = 1 \text{ or } x = -4$$

We have not proved the converse, that is, we have not shown that if $x = 1$ or $x = -4$ then x solves the original equation. That's why we need to check.

Such methods as used in this solution, then, in general merely reduce the number of values we have to check, from all of $\mathbb{R}$ to some small, feasibly checkable set. (That's nothing to sneeze at, which is why such methods are taught.)

What if we abhor checking for spurious solutions for some reason? Can we solve the problem without any need to check? Yes, and the method is clear from the expanded derivation above. What we must do is strengthen that $\Rightarrow$ into $\equiv$.

Consider, then, the converse of that step:

$$\begin{aligned} & 5 - x = x^2 + 2x + 1 \\ \Rightarrow \quad & \{?\} \\ & \sqrt{5 - x} = x + 1 \end{aligned}$$

What operation are we performing here? We're taking square roots. Well, that's only allowable if both sides are at least zero. Fortunately, the right-hand side is a perfect square, hence at least zero, and if the left-hand side is equal to it, then it too is at least zero.

But there's something else wrong here. Observe the step in more detail:

$$\begin{aligned} & 5 - x = x^2 + 2x + 1 \\ \equiv \quad & \{\text{factoring}\} \\ & 5 - x = (x + 1)^2 \\ \Rightarrow \quad & \{\text{take square roots}\} \\ & \sqrt{5 - x} = \sqrt{(x + 1)^2} \\ \equiv \quad & \{\sqrt{a^2} = |a|\} \\ & \sqrt{5 - x} = |x + 1| \end{aligned}$$

So in order to end up with $x+1$, we need a reason for $|x+1|$ to be equal to $x+1$: we need $x + 1 \geq 0$. In full, then, the converse should be something like

$$\begin{aligned} & 5 - x = x^2 + 2x + 1 \text{ and } x + 1 \geq 0 \\ \Rightarrow \quad & \{\text{take square roots}\} \\ & \sqrt{5 - x} = x + 1 \end{aligned}$$

Now go back to the original proof, where we did the step whose converse this is trying to be. To strengthen that step into $\equiv$, we need this additional condition $x + 1 \geq 0$; and hey — we can infer that from the original equation. ($x + 1 \geq 0$ because it is equal to a square root.) So:

$$\begin{aligned} & \sqrt{5 - x} = x + 1 \\ \equiv \quad & \{\text{square both sides}\} \\ & 5 - x = x^2 + 2x + 1 \text{ and } x + 1 \geq 0 \end{aligned}$$

Now that this step is $\equiv$, we carry on with the derivation, preserving the additional condition as we go:

$$
\begin{aligned}
&\equiv \quad \{\text{algebra}\} \\
&\quad 0 = x^2 + 3x - 4 \text{ and } x \geq -1 \\
&\equiv \quad \{\text{factoring}\} \\
&\quad 0 = (x-1)(x+4) \text{ and } x \geq -1 \\
&\equiv \quad \{\mathbb{R} \text{ is an integral domain}\} \\
&\quad (x - 1 = 0 \text{ or } x + 4 = 0) \text{ and } x \geq -1 \\
&\equiv \quad \{\text{algebra}\} \\
&\quad (x = 1 \text{ or } x = -4) \text{ and } x \geq -1 \\
&\equiv \quad \{\text{logic}\} \\
&\quad x = 1
\end{aligned}
$$

In this version, every step is $\equiv$, so we can read off the solutions from the final result and check nothing: x satisfies the original equation if and only if it is 1.

(It's not clear that carrying extra conditions along like this actually pays for itself. But the fact that some steps — e.g., squaring both sides of an equation — yield implication, not equivalence, should, of course, be emphasized when elementary algebra is being taught. If I were teaching such material, I'd teach the meanings of $\Rightarrow$ and $\equiv$ and require students to write the appropriate symbol between steps.)

2 A calculus for the maximum function

I brought a photocopy of a few pages of an article by Feijen, in which he discusses a calculus of the maximum function.

(A note on words: when we say "calculus", we usually mean differential calculus and/or integral calculus. But there are other calculi (for example, predicate calculus). What the word actually means is a system for doing calculations symbolically. Differential and integral calculus are so called because they allow us to solve geometric problems (finding tangents and areas) by symbol manipulation rather than geometric argument.)

I won't describe this in much detail; you should read the article. Feijen uses the symbol $\uparrow$ for the maximum: $x{\uparrow}y$ is the maximum of x and y. Some algebraic facts about this operation: it is associative, that is,

$$x \uparrow (y \uparrow z) = (x \uparrow y) \uparrow z$$

(so we usually omit parentheses); it is commutative (or, as Feijen calls it, symmetric), that is,

$$x \uparrow y = y \uparrow x\,;$$

it is idempotent, that is,

$$x \uparrow x = x$$

(which three properties you might recall from my wee note on "half-lattices"); and addition distributes over it:

$$x + (y \uparrow z) = x + y \uparrow x + z\,.$$

(Note, in this last example, that $\uparrow$ has a lesser binding power than $+$, so the right-hand side means $(x + y) \uparrow (x + z)$.)

This makes for a very handy algebra; for example, if we define

$$|x| = x \uparrow -x$$

(as Feijen does), then we can prove the triangle inequality

$$|x + y| \leq |x| + |y|$$

by symbol manipulation alone. (Well, we also need some other facts;

$$x \leq x \uparrow y\,,$$

for example.) If you've ever seen the triangle inequality proven in a book, you'll know it's a hideous mess of cases. Feijen's calculational proof is fast, rigorous, direct, and has no case analysis at all.

3 Numbers congruent to their own squares

Problem 9 in the list of outstanding problems asks what can be said about the solutions of the congruence

$$k^2 \equiv k \pmod{n} .$$

Staring at a list of solutions for small n (see notes for Sep 11) led us to several conjectures.

There's a very noticeable diagonal line of solutions through the centre of the list; every fourth row has a pair of solutions on this line.

The solutions $(n, k) \in \{(6, 3), (12, 4), (20, 5), (30, 6)\}$ form a nice curve. Each is the leftmost in their row after the 0 and 1. (Note what $n + k$ is in each of these solutions. There are other curves of similar types.)

Each row is left-right symmetrical. Well, almost; you have to move the 0 from the beginning to the end.

If n is a prime power, then the only solutions k are 0 and 1.

The number of (distinct) solutions for a given n (i.e., the number of entries in each row) is always a power of 2. Eileen spotted that it is 2^λ, where λ is the number of distinct primes that divide n.

We have not yet looked at proofs of any of these; I encourage you to take a stab at them. (Proving the last one is rather complicated — at least, I don't have a simple proof — so you might want to warm up on the others first.)

(There was another conjecture, which I said I would check for larger n, but I forgot what it was.)