What if?

Nigel Kalton

1 Pure versus applied mathematics

Research mathematics is frequently classified as either *pure* or *applied.* However all mathematicians, whether they consider themselves pure or applied, essentially adhere to the same structure in their work. The distinction seems to me to be mainly in the choice of problem. The applied mathematician selects a problem to work on which is motivated by some physical or practical situation, whereas the pure mathematician selects problems that seem natural in a mathematical context without regard to physical meaning. Once the problem is selected, there is really no difference between pure and applied mathematics: both pure and applied research are subject to the same standards of rigor, and can use very similar techniques.

Thus this whole division is only really philosophical. Even defiantly pure mathematicians can accidentally do applicable mathematics. Perhaps the *pure* of mathematicians, G.H. Hardy who is famous for the quote that "I have never done anything *useful* in my life" is also the co-author of the Hardy-Weinberg law in genetics. Equally hard-line applied mathematicians often do mathematics which has genuine appeal to those whose interests are exclusively pure.

So where does a pure mathematician find problems to work on and why? I said earlier that one looks for natural problems; but just what is *natural?* In this article I want to give a couple of examples to illustrate my belief that a mixture of curiousity and luck leads to the right problems. The pure mathematician is someone who is always prepared to ask the question *"What if?"* It is true that not every question that comes to mind is worthwhile or important; surely most questions that we ask turn out to lead nowhere. Just occasionally, however, a question which seems to come out of the blue is precisely the right one and generates a spark that eventually deepens our understanding of mathematics.

My two examples are different in character. The first is one of the classics of mathematics, while the second is an admittedly quite minor piece of research but has the advantage that I was personally involved and know the story very well. The message behind both is the same. Anyone interested in pure research needs to know first how to ask questions.

2 Fermat's Last Theorem

My first example is probably the most celebrated problem in mathematics, which has only recently been solved after nearly 400 years. Probably everyone knows the story but let me repeat it. Pierre de Fermat was a seventeenth century French lawyer who was an enthusiastic amateur mathematician. He conjectured (well, no, he actually claimed as a theorem) that if n is a natural number greater than 2 then it is impossible to find natural numbers, a, b, c so that

$$a^n + b^n = c^n.$$

Unfortunately he wrote this as a note in his copy of the work of the Greek mathematician Diophantus, and said that the margin was too small to contain his proof. Did he really prove it? Only the most romantic would now believe so, because the greatest minds in mathematics devoted themselves for centuries to establishing Fermat's throwaway remark. Only in the last year has Andrew Wiles of Princeton University finally proved that Fermat's theorem is a genuine theorem (and, perhaps it will be a few years yet before we are absolutely certain!).

I want to make the point that it is irrelevant whether Fermat could prove Fermat's theorem. It is enough, and even more significant, that he asked whether it was true. It is probably a gross exaggeration to claim that Fermat's question lauched all modern algebra, but I'll say that anyway!

So where did this problem come from? Fermat was reading the work of the ancient Greek mathematician Diophantus, and Diophantus was explaining how to give a complete list of *Pythagorean triples*. A Pythagorean triple is a triple of natural numbers $\{a, b, c\}$ satisfying

$$a^2 + b^2 = c^2.$$

Of course everyone schoolboy knows that

$$3^2 + 4^2 = 5^2$$

and maybe that

$$5^2 + 12^2 = 13^2.$$

The Greeks wanted to know solutions for what they considered very practical and applied reasons. The origin is of course Pythagoras's theorem on right-angled triangles (which may have been known for thousands of years before Pythagoras in both Egypt and China). Of course if you know Pythagoras's theorem you can make buildings with right-angled corners! The Greeks had another incentive: Pythagoras and his followers believed in a doctrine of commensurability which meant that only whole number solutions had meaning for them. So they worked out the complete answer. In fact if we assume $\{a, b, c\}$ have no common factors and say a is odd then there are natural numbers m, n, so that $a = m^2 - n^2$, $b = 2mn$ and $c = m^2 + n^2$.

This is an elegant but not very difficult piece of mathematics. Unfortunately time stood still for a couple of thousand years in the mathematical world between the Greeks and Fermat. There are many reasons, but at least in Europe Greek learning was almost lost in the

Dark Ages, until with the Renaissance finally scholars other than monks learned Greek and re-discovered Greek science. In reading Diophantus, I picture Fermat as being thrilled to discover the workings of mathematical minds from so long ago and restlessly asking questions himself. He was inspired to consider many variations of the ideas in Diophantus. For example he showed that every prime number p of the form $4m + 1$ can be expressed in the form $p = a^2 + b^2$; here his object was to decide when the hypotenuse of a Pythagorean triangle could be a prime number. Then he asked whether a and b could be squares themselves in a Pythagorean triple, i.e. can you solve

$$a^4 + b^4 = c^2.$$

The answer here (and Fermat *did* prove this) is no. So in particular you cannot solve

$$a^4 + b^4 = c^4.$$

At this point I think that Fermat began to wonder if he could replace the exponent 2 by *any* larger number. So we have Fermat's last theorem. There is no practical reason for any of this: Fermat simply speculated and asked the magic question *"What if $n > 2$?"*. The rest is history.

3 A personal example

Now we move from the sublime to the prosaic. I want to give an example from my own experience, where similar speculation led to a small, but, at least in my opinion, interesting piece of research.

The story begins in 1973 when I was teaching at the University of Wales in Swansea. A colleague of mine, Geoffrey Wood, was teaching elementary matrix algebra and assigned his class the following problem.

Let P and Q be idempotent matrices (i.e. $P^2 = P$, $Q^2 = Q$). Show that $P + Q$ is an idempotent if and only if $PQ = QP = 0$.

This is an exercise to illustrate that matrix multiplication does not commute. The solution is quite simple. Multiplying out gives

$$P + Q + PQ + QP = P + Q$$

and so $PQ + QP = 0$. Then left-multiplication by P gives $PQ + PQP = 0$ and right-multiplication by P gives $PQP + QP = 0$. Thus $PQ = QP = 0$ and we are done.

The hero of the story is an anonymous student who asked what happens if we replace 2 by 3. Thus if P and Q are idempotent matrices with $(P+Q)^3 = P+Q$ does $PQ = QP = 0$? This is a question of apparently idle curiousity, but for several of us on the faculty with nothing to do one afternoon it proved an amusing exercise. We covered the blackboard with calculations and after much effort we found that we could still obtain $PQ = QP = 0$ by multiplying out: it was just harder. I'll leave this as an exercise for the interested reader!

So what next? Of course we tackled $(P+Q)^4 = P+Q$. It still works, but this took a couple of days and several blackboards. Next came $(P+Q)^5 = P+Q$: but this was too much and we quit.

But the problem was a constant irritant: there must be a reason it worked for the cases of $n = 2, 3, 4$. Why should it fail when $n = 5$? A few months later I finally discovered a proof for all n. The argument was simple but depended on the notions of trace and rank for matrices. Let me explain it briefly. The equation $\lambda^n - \lambda = 0$ has only simple roots in the complex plane. So it follows that the matrix $P+Q$ satisfying this equation is diagonalizable i.e. is similar to a diagonal matrix. The eigenvalues must all be nth. roots of unity or zero. That means we have an inequality between the trace (sum of the eigenvalues), denoted by tr $(P+Q)$, and the rank (dimension of the range), denoted by rank $(P+Q)$, i.e. $|\text{tr}\,(P+Q)| \leq \text{rank}\,(P+Q)$. However we know $\text{rank}\,(P+Q) \leq \text{rank}\,P + \text{rank}\,Q = \text{tr}\,P + \text{tr}\,Q$ since P and Q are idempotents. Collecting together we see since $\text{tr}\,(P+Q) = \text{tr}\,P + \text{tr}\,Q$ that $\text{tr}\,(P+Q) = \text{rank}\,(P+Q)$ and every nonzero eigenvalue of $P+Q$ is equal to one. It is easy to see this means $(P+Q)^2 = P+Q$ and now we are back in the original question.

I kept this result in the back of my mind, because for some reason the argument appealed to me. I thought maybe it would be a good question to set on some future Ph.D. qualifying or comprehensive examination!

However, something continued to bother me. For $n = 2, 3, 4$ the proofs were pure algebraic manipulation, but for general n the proof required a lot more machinery; the general proof did require the notions of trace and rank which are only applicable to matrices. So for $n = 2, 3, 4$ the result was true in a general ring with only some mild assumptions but for larger n we need to have matrices. This resurfaced in 1981 when at a party I mentioned this to Mel Hochster of the University of Michigan (I was by now in the United States at the University of Missouri). He pointed out that for *most* rings one can make a reduction to the special case of matrices.

This is all at the level of amusement not research. But Hochster's remark lead me to wonder if I could relax the hypotheses further and ultimately lead to the following result published in a paper in the Canadian Mathematical Bulletin in 1988. I won't explain the concepts, but just say that it was motivated by the anonymous student's remark fifteen years before! I would simply never have dreamed of considering this problem without his *"What if?"* question from years before. The argument requires some quite delicate use of complex analysis and some combinatorial identities.

Theorem: Let A be a Banach algebra and some p, q are idempotents in A. Then $p+q$ is an idempotent if and only if $\sup_n \|(p+q)^n\| < \infty$.

So this piece of research is a direct result of *idle* speculation! It exists for no other reason. Yet the theorem is true and not absolutely trivial, so somehow the speculation was *right*.

Let me close by speculating further: why stop at *two* idempotents p, q? Why not three idempotents p, q and r? Actually this speculation is due to my colleague Mark Ashbaugh who pointed out that the corresponding matrix theorem is true for any finite number of idempotents not just two. You can simply rework the argument I gave if you assume $(P+Q+R)^n = P+Q+R$ with P, Q, R idempotent matrices. The question for Banach algebras as above is open, and apparently quite beyond the techniques I used in my 1988 paper. Maybe someone reading this article will see what to do. Ultimately it may not be earth-shaking for mathematics like Fermat's theorem, but I have the feeling a proof for more idempotents will involve some interesting mathematics.

Such is the way pure mathematics evolves!

araf

elektronik dil-düşünce dergisi

Nisan 1996, Sayı: 7

Matematik Özel Sayısı

İçindekiler