

Revolutionary Mathematics: Physicists version

Source: <http://sci.tech-archive.net/Archive/sci.physics/2004-12/3659.html>

From: James Harris (jstevh_at_msn.com)

Date: 12/05/04

Date: 4 Dec 2004 16:17:34 -0800

For years at times there have been posts from me which you might have noticed seem to garner a lot of hostility, which talk about an error in the discipline of mathematics, and I've often heard questions about relevance to physicists.

Well, um, physicists USE mathematics, and in fact the problem does affect group theory, as the area of mathematics is the area from which group theory comes.

Here's a post I did earlier on some math newsgroups with some corrections.

The story actually is fascinating.

I'm an amateur mathematician who has found that using some simple ideas I can show a remarkable error in thinking which unfortunately underpins much of what's thought to be known in the discipline of algebraic number theory.

The mathematics which proves the problem is extrarodinary in that it is very simple, relying on some of the most basic concepts in algebra.

It is revolutionary in that it so upsets the status quo, changes the historical positions of so many mathematicians, and is just plain surprising in many ways.

Essentially what I do is relate one polynomial to a family of polynomials, using what I call a non-polynomial factorization, which I call that as the factoring of the primary polynomial is into factors that are themselves not polynomials.

For simplicity in explaining I don't initially give a tremendous amount of detail about where the polynomial comes from as years of experience talking about this on Usenet has shown me how easily posters can confuse people with detail of that sort, but I have no problem going into detail if real curiosity emerges.

So I say I use a polynomial. So let's see it.

$$P(x) = 14706125 x^3 - 900375 x^2 - 17640 x + 1078$$

where x is an integer.

It is, as you can see, a polynomial, and it's distinctive in an important way, as it has 49 as a multiple as

$$P(x) = 49(300125x^3 - 18375 x^2 - 360 x + 22)$$

and I'll relate it to a family of polynomials, where that multiple 49 is very important.

Now here's where a basic idea steps in, as years ago I discovered the idea of separating out a polynomial in a special way so that you can factor it as if it's a polynomial in a *different* variable from the polynomial variable itself.

Here that gives

$$P(x) = 49(2401 x^3 - 147 x^2 + 3x) (5^3) - 3(-1 + 49 x)(5)(7^2) + 7^3$$

where if you multiply it all out and simplify, you'll still get

$$P(x) = 49(300125x^3 - 18375 x^2 - 360 x + 22)$$

and the pattern I use next might not quite be visible, so I'll make a substitution using Y=5 and Z=7, to get

$$P(x) = 49(2401 x^3 - 147 x^2 + 3x) Y^3 - 3(-1 + 49 x) YZ^2 + Z^3$$

and you can hopefully see how that can factor as

$$P(x) = (Y a_1(x) + Z)(Y a_2(x) + Z)(Y a_3(x) + Z)$$

and going ahead and putting back in their values, as I used Y and Z just as a bit of help (a dangerous bit of help as sci.math posters have routinely jumped in at this point in the past to claim that actually x is not the polynomial variable at all!!!), I have

$$P(x) = (5a_1(x) + 7)(5a_2(x) + 7)(5a_3(x) + 7)$$

and the a's are easily determined by using

$$(5a_1(x) + 7)(5a_2(x) + 7)(5a_3(x) + 7) =$$

$$49(2401 x^3 - 147 x^2 + 3x) (5^3) - 3(-1 + 49 x)(5)(7^2) + 7^3$$

as you get three simultaneous equations, for instance,

$$a_1(x) a_2(x) a_3(x) = 49(2401 x^3 - 147 x^2 + 3x)$$

is one of the three.

Solving for the a's, you get a cubic, which is

$$a^3 + 3(-1 + 49x)a^2 - 49(2401 x^3 - 147 x^2 + 3x)$$

where the roots of that cubic are $a_1(x)$, $a_2(x)$, and $a_3(x)$, and that cubic is the family of polynomials that are related to $P(x)$, as for any given value of x , you get a polynomial.

Notice that the multiple of $P(x)$, 49 is locked into the family of cubics. But it's not a multiple of the cubic, as you have the term

$$3(-1 + 49x)$$

which is of course, coprime to 49.

That's important, as somehow with this technique of factoring $P(x)$ in a special way, I've related that factorization of a polynomial that has 49 as a multiple, to a family of polynomials that do not.

It's one of the most important relations in math history.

Why? Well, for $P(x)$, 49 is just a multiple, so I can divide it off.

That gives me

$$P(x)/49 = 300125x^3 - 18375 x^2 - 360 x + 22$$

and reasonably, dividing 49 from the factorization of $P(x)$, gets rid of it, without a trace, but that results in the factorization

$$P(x)/49 = (5a_1(x) + 7)(5a_2(x) + 7)(5a_3(x) + 7)/49$$

and so much arguing, over a period of years with this technique, settles on what happens next with such an example.

Before I go further though, let's stop to consider what I've done:

1. I have a polynomial $P(x)$ that has 49 as a multiple.
2. I factor that polynomial in a special way to get non-polynomial factors.
3. I solve for those factors giving me a cubic family of polynomials.
4. I now decide to divide 49 from $P(x)$, and am at the point of considering how that affects its factorization.

Here $P(x)$ is key. It has a multiple 49, and its factorization provides the relation to the cubic family that defines the a's. It is

a basic concept in algebra that a multiple can be divided off without problem, and necessarily that must be true, as consider, how can a factorization of

$$300125x^3 - 18375 x^2 - 360 x + 22$$

have some impact from the polynomial resulting from dividing off a multiple?

The equation has no memory. After all, if it did, why 49? Why not 3 or 11, or 83947397, or an infinity of other numbers?

I belabor that point as if you accept it, then what follows is obvious.

So I have

$$P(x)/49 = (5a_1(x) + 7)(5a_2(x) + 7)(5a_3(x) + 7)/49$$

and I want to know how the 49 divides through the factors of $P(x)$, while I already know that

$$P(x)/49 = 300125x^3 - 18375 x^2 - 360 x + 22$$

so 49 divides off of $P(x)$ itself, without a trace, which is not a surprise.

The simplest way to find out is to check directly. However, the a 's are rather complex being defined by the cubic

$$a^3 + 3(-1 + 49x)a^2 - 49(2401 x^3 - 147 x^2 + 3x)$$

and it might seem extraordinarily difficult to find out anything about them, so is the cause lost?

No, because I can simplify by focusing on the constant term of $P(x)$.

Why the constant term? Because unlike the other terms it is independent of x itself, and much of the complexity washes out.

The constant term of $P(x)$ is given by setting $x=0$, as that sets the terms that have x as a variable to 0, leaving just the constant term:

$$P(0) = 49(300125(0)^3 - 18375 (0)^2 - 360 (0) + 22) = 49(22).$$

Now what about the factors of $P(x)$? Well, they become a LOT easier to manage as well, as I then have

$$a^3 + 3(-1 + 49(0))a^2 - 49(2401 (0)^3 - 147 (0)^2 + 3(0))$$

which is

$$a^3 - 3a^2 = 0 \text{ and } a^3 - 3a^2 = 0, \text{ is } a^2(a - 3) = 0$$

so despite all the early complexity, I have now the simple result that two of the a's equal 0, at $x=0$, while one equals 3.

So I need to pick the a's to proceed, and my usual convention is to let

$$a_1(0) = 0, a_2(0) = 0, \text{ and } a_3(0) = 3$$

so with

$$P(0)/49 = (5a_1(0) + 7)(5a_2(0) + 7)(5a_3(0) + 7)/49$$

I have

$$P(0)/49 = (5(0) + 7)(5(0) + 7)(5(3) + 7)/49 = (7)(7)(22)/49 = 22$$

which is correct as we already found out earlier.

But wait, aren't I just checking at a *single* value, for something that's terribly complicated, where maybe things are different at a different value?

Well, sure, things are different for terms that have x as a factor, as that's how algebra works. As x varies, you get different things happening.

Well, yes, for terms that vary with x , that is correct. But if something is constant, then it doesn't vary.

Checking at $x=0$ clears out those terms that vary, leaving those that do not, revealing that for two of the terms, what's left over, is 7, while for one, what's left over is 22.

That's just a fact. It's such a simple fact that one of the more remarkable things over the years I've found is the ability of some people to argue around it.

If you accept that constants are not variable, and that 7 is just a number that does not change with x , and you accept that setting $x=0$ reveals constants by eliminating the terms that vary, then you should accept that the constants are constant without regard to the value of x .

So if I could look at the constants at $x=39473987$, then that'd be fine, but with that value, the terms with x get in the way, but at $x=0$, they do not.

But with $P(x)/49$, I already have that 49 is gone, without a trace.

So, if the constants for factors of $P(x)$ are 7, 7 and 49, who MUST the 49 divide through?

Like this

$$P(x)/49 = (5a_1(x)/7 + 1)(5a_2(x)/7 + 1)(5a_3(x) + 7)$$

with indices arbitrary, as remember, I picked the first two a's to be those that go to 0, when $x=0$.

So far, so good, and you may wonder how something so simple can be "revolutionary".

Well, remember I related the factorization of $P(x)$ to a *family* of cubics given by the roots of

$$a^3 + 3(-1 + 49x)a^2 - 49(2401x^3 - 147x^2 + 3x)$$

and now I've shown a result that indicates that two of the a's have 7 as a factor, without regard to the value of x .

That's HUGE as it turns out that a long time ago (like over a hundred years ago) mathematicians decided that you couldn't make such a determination if the roots of a polynomial were all irrational and didn't all have the same factor.

(Like $x^2 - 3$ has $\sqrt{3}$ and $-\sqrt{3}$ as roots.)

That belief is the basis for the modern usage of group theory including Galois Theory.

You've just seen a basic result showing it to be a false belief.

Like stick in $x=1$, and you have

$$S(a) = a^3 + 3(48)a^2 - 49(2257)$$

and without solving for the roots you know already that two of its roots should have 7 as a factor, but now there's another problem.

Over a hundred years ago, back in the late 1800's mathematicians studied polynomials special in that they had a leading coefficient of 1 or -1 , and integer coefficients. Polynomials with a leading coefficient of 1 or -1 are called monic, so more technically, they studied monic polynomials with integer coefficients.

They called the roots of these polynomials algebraic integers.

Those roots form a group of numbers called the ring of algebraic integers.

And it turns out that for

$$S(a) = a^3 + 3(48)a^2 - 49(2257)$$

if you take its roots, you can't find any that when divided by 7, give an algebraic integer.

It gets more complicated, as you can prove that with the factorization

$$P(x) = (5a_1(x) + 7)(5a_2(x) + 7)(5a_3(x) + 7)$$

its possible to find algebraic integers w_1 , w_2 , and w_3 , such that

$$w_1 w_2 w_3 = 49$$

where the w 's are the respective factors of

$$(5a_1(x) + 7), (5a_2(x) + 7), \text{ and } (5a_3(x) + 7)$$

when I just said that you can't get algebraic integers with $x=1$, and the roots of

$$a^3 + 3(48)a^2 - 49(2257)$$

where 7 is a factor of *any* of those roots, let alone two.

Hmmm...problem, right? Is it all lost? Does that mean everything before was wrong? Yuck, did I just waste your time with claims of revolutionary mathematics and all of that, when there's this weird result that seems to show it all must be wrong?

But wait, for my result I used some very basic concepts. Like I rely on 49 as a multiple just dividing off, without a trace. And I focused on constant terms because they are, well, constant, and simpler to work with than terms that include x , where all the complexity comes into the picture.

Well, there was that weird technique of factoring a polynomial some odd way.

But, sure, it's different, but all of the mathematical operations are valid ones.

So what gives?

Let's focus on the result again, as I said that with

$$P(x) = (5a_1(x) + 7)(5a_2(x) + 7)(5a_3(x) + 7)$$

you can have algebraic integers w_1 , w_2 , and w_3 that are factors of the factors of $P(x)$.

But I also showed that

$$P(x)/49 = (5a_1(x)/7 + 1)(5a_2(x)/7 + 1)(5a_3(x) + 7)$$

but that can't work with these numbers called algebraic integers!

Well, consider $u_1 u_2 u_3 = 1$, where multiplying through gives

$$P(x)/49 =$$

$$(5a_1(x)u_1/7 + u_1)(5a_2(x) u_2/7 + u_2)(5a_3(x) u_3 + 7u_3)$$

where now it all *does* work with algebraic integers.

That is, for some reason, while two of the a's do not have 7 as a factor in the ring of algebraic integers, they *do* have $7u_1$ and $7u_2$, respectively, as factors, where u_1 and u_2 are units, in that they are factors of 1.

But, here's where it's rather strange, as u_1 and u_2 are not algebraic integers i.e. roots of a monic polynomial with integer coefficients, while u_3 is.

So, for that reason, u_1 , u_2 , and u_3 are NOT units in the ring of algebraic integers.

Here's an example that I hope helps you see how it works.

In integers you can have

$$S(x) = (3x + 1)(x + 1) = 3x^2 + 4x + 1$$

but now consider

$$S'(x) = (3x + u_1)(x + u_2) = 3x^2 + kx + 1$$

where $u_1 u_2 = 1$, and k is an integer.

Here, u_1 CAN be an algebraic integer, but u_2 CANNOT be an algebraic integer.

So, in the ring of algebraic integers, u_1 cannot be a unit.

Well, maybe it's some kind of fraction, right? Well, yes, possibly, it is, and like, for $k=0$, you can see that it IS some kind of fraction. But, have you covered all the possibilities?

The answer is, no, you can't have and have it all be mathematically consistent.

So why all this talk about algebraic integers? They seem kind of messy at this point.

Like you get this nifty result with some basic concepts and a special factoring technique, where it was all rather straightforward, and then suddenly focusing on roots of monic polynomials with integer coefficients gives all kinds of head-scratching trouble!

Well, the reason for the focus is that mathematicians for over a hundred years focused on the ring of algebraic integers not understanding that it was, I'll say, quirky.

Actually it's worse than quirky, as not understanding the weirdness that can arise from focusing on the roots of monic polynomials with integer coefficients you can "prove" lots of things with the ring of algebraic integers that are in fact mathematically false.

It's a nasty little bug.

To give you some perspective, the tools used by Wiles in his work that purportedly proves the Taniyama–Shimura Conjecture, to most people, work that supposedly proves Fermat's Last Theorem, don't work.

They don't work because they're based on an improper understanding of the ring of algebraic integers. Works like Wiles's cannot be rescued from this bug.

So now maybe you understand the controversy!

Is my work actually complicated for a trained mathematician?

No. My guess is that a trained mathematician can go over the entire thing, and understand the implications in about an hour.

James Harris

<http://mathforprofit.blogspot.com/>