

## Re: Amateur takes on Wiles's work

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2004-08/5374.html>

---

**From:** Andrzej Kolowski ([akolowski\\_at\\_hotmail.com](mailto:akolowski_at_hotmail.com))

**Date:** 08/30/04

Date: 29 Aug 2004 19:15:45 -0700

jstevh@msn.com (James Harris) wrote in message  
news:<3c65f87.0408290713.3a80d92c@posting.google.com>...

>Now I'm not a professional mathematician. I do post about math on  
>Usenet, but that's not an indication of expertise!  
>  
>I'm not beholdng to any mathematical interests though, so I feel no  
>compulsion to protect a favored Golden Calf of the modern math world,  
>which is an argument that supposedly proves something by one Andrew  
>Wiles, which I fear doesn't, and I'll say exactly why I say it  
>doesn't.  
>  
>It'll be up to others to answer the charge, dismiss it, or consider  
>that I might be right.  
>  
>First off despite the assertions of great complexity to the area what  
>mathematicians initially noticed isn't that complicated:  
>  
>They had these things they called modular forms, and these things they  
>called elliptic curves, which didn't seem at ALL related.  
>  
>But there are these 4 numbers that you can get from elliptic curves,  
>and find modular forms with the same 4 numbers. Those numbers are  
>kind of like a description.  
>  
>So there's some way that modular forms and elliptic curves could have  
>the same description!  
>  
>Mathematicians would check various elliptic curves and find they could  
>always find some modular form to associate with it.  
>  
>Taniyama and Shimura conjectured that there was a pattern here that  
>held, as in fact modular forms and elliptic curves WERE related in  
>some deep way, and that what mathematicians were noticing wasn't just  
>one of those intriguing coincidences.  
>  
>But you have the setup for a logical fallacy called Cum Hoc, Ergo  
>Propter Hoc, where people see what looks like a pattern, and leap to a

- >conclusion, though at this point mathematicians were ok, as it was
- >only a conjecture.
- >
- >It took Andrew Wiles coming in, with an attempt at proof by
- >association for the logical fallacy to fully take hold.
- >
- >The problem for many of you with such a charge is that it can seem
- >esoteric. I've had two posters on sci.math where I've discussed this
- >for a while actually come back to claim that Cum Hoc, Ergo Propter Hoc
- >is about time, so it can't apply to mathematics!!!
- >
- >But notice, it's actually about false implication, where you see a
- >pattern, and your mind plays a trick on you and tells you that the
- >pattern is proof of itself!!!
- >
- >To date, while mathematicians now apparently mostly believe the
- >Taniyama–Shimura Conjecture, they can't give you a reason why, or can
- >they?
- >
- >It turns out that if the charge of Cum Hoc, Ergo Propter Hoc is itself
- >challenged, the next proper step is to ask for a null test.
- >
- >What is a null test?
- >
- >A null test is to go through the argument under challenge with the
- >assumption that its conclusion is false, and find a contradiction with
- >that assumption!
- >
- >You see, math proofs begin with a truth and proceed by logical steps
- >to a conclusion which then **MUST BE TRUE**.
- >
- >But the conclusion follows from the previous steps in the proof, so
- >any challenge to the conclusion must contradict a previous logical
- >step, or the truth with which the proof begins.
- >
- >Math proofs are perfectly logical.
- >
- >There is no way for a math proof to fail a null test.
- >
- >It is just not logically possible.
- >
- >Therefore, any math proof can be challenged by assuming the opposite
- >of its conclusion, and tracing through it until you reach the logical
- >step where you end up with a contradiction.
- >
- >The resolution to the contradiction, if you have a proof, is that your
- >assumption is false and the conclusion **IS true!**
- >
- >It's neat. It's beautiful. It's just cool.
- >
- >Notice also that the null test, which can be requested whenever, and

- >not just when you have a case of *Cum Hoc, Ergo Propter Hoc*, is a great
- >way for someone who is not an expert in a particular field to find a
- >limited area to check.
- >
- >For instance, with my challenge to Wiles's work, someone should find a
- >single logical step where the assumption of a non-modular elliptic
- >curve will cause a contradiction, and be able to give the exact
- >section in his work where it occurs!!!
- >
- >Then they can explain why it occurs and despite the entire work being
- >hundreds of pages you have the ability to look at the crucial link
- >without going through the entire thing.
- >
- >You could call that logical step the keystone.
- >
- >I'm asking for someone to produce the keystone in Wiles's work, which
- >will ring out loud and clear if you assume the existence of a
- >non-modular elliptic curve.
- >
- >Let the full challenge--with witnesses now from *alt.math.recreational*
- >and others throughout the world through the Internet--begin.
- >
- >
- >James Harris

I like this idea of a "null test". Here is how I understand it.  
You take the conclusion of a given proof. You state its negation.  
You then go through the proof line by line to see if anything  
contradicts the negation.

If there is *\*no\** step that contradicts the negation, then the  
proof must be wrong.

If there *\*is\** a step that contradicts the negation, then it  
is still possible that the proof is wrong. You just have  
slight and nonconclusive evidence that it isn't.

So the "null test" is somewhat of a one-sided test, but  
still useful.

Applying it to Wiles' 100+ page long and very difficult proof is  
going to be pretty hard. Besides, you may get all the way  
to the end and then find that the concluding statement is  
the only one that contradicts the negation, and that would  
not tell you much of anything.

So I would like to try it with a shorter proof.

Below is a copy of the paper "Advanced Polynomial Factorization"  
by James Harris, exactly as it appeared in the Southwest  
Journal of Pure and Applied Mathematics:

[begin paper]

Electronic Journal: Southwest Journal of Pure and Applied Mathematics

Internet: <http://rattler.cameron.edu/swjpam.html>

ISSN 1083

Issue 2, December 2003, pp. 6--8.

Submitted: July 25, 2003. Published: December 31 2003.

#### ADVANCED POLYNOMIAL FACTORIZATION

James Harris

Email Address: [jstevh@msn.com](mailto:jstevh@msn.com)

**ABSTRACT.** Algebraic method for determining distribution of factors within a polynomial factorization, which breaks through what was seen as a barrier from overinterpretations of Galois Theory.

A.M.S. (MOS) Subject Classification Codes. 11R04,11R09

**KEY WORDS AND PHRASES.** Polynomial factorization, Galois theory, Factorization lemma, Ring of algebraic integers

#### ADVANCED POLYNOMIAL FACTORIZATION APPROACHED.

Determining the distribution of factors within irrational algebraic integers has long been considered impossible as it is not possible to do using Galois Theory. However a simple technique through the introduction of more variables makes it possible. To highlight the standard belief consider the algebraic integer roots of  $x^2 + x - 5$ .

While you know that the algebraic integer factors are themselves factors of 5, can either not have non unit factors of 5? How do you know?

In looking to consider distribution of algebraic integer factors within a factorization I'll be using a more complicated example than  $x^2 + x - 5$ .

This paper will show, using basic algebraic methods, that given the factorization, in the ring of algebraic integers,

$$65x^3 - 12x + 1 = (a_1x + 1)(a_2x + 1)(a_3x + 1)$$

one of the  $a$ 's is coprime to 5.

First I'll need a simple lemma to generalize beyond factors of a polynomial that are themselves polynomials.

#### FACTORIZATION LEMMA:

Given a factor  $g$  of a polynomial  $P(x)$ , further defined as a factor for all  $x$ , which means that the value of  $g$  for a value ' $a$ ' of  $x$  is a factor of  $P(a)$ , within the ring of algebraic integers, there exists  $r$  and  $c$  such that

$$g = r + c$$

where  $r=0$ , or varies as  $x$  varies, and  $c$  is a factor of the constant term  $P(0)$  and is itself constant.

Let  $x=0$ , then  $g$  must be a factor of  $P(0)$ , so at that point  $c = g$ .

If when  $x$  does not equal 0,  $g=c$ ,  $r=0$ . If when  $x$  does not equal 0,  $g \neq c$  there must exist  $r$  which varies with  $x$ . That is,  $r=g$ . []

As an example consider  $\sqrt{x+1}$  which is a non polynomial factor of  $x+1$ , and while there are an infinity of irrational solutions consider the rational solution at  $x=35$ .

Then I have  $\sqrt{35+1} = 6 = 5 + 1$ ; therefore when  $x=35$ ,  $g=6$ ,  $r=5$ , and  $c=1$ . But for different values of  $x$ ,  $g$  and  $r$  will vary, while  $c$  will not.

#### PRIMARY ARGUMENT.

Given

$$65x^3 - 12x + 1 = (a_1x + 1)(a_2x + 1)(a_3x + 1)$$

in the ring of algebraic integers. Let

$$P(m) = f^2 ((m^3 f^4 - 3m^2 f^2 + 3m)x^3 - 3(-1 + mf^2)xu^2 + u^3 f)$$

Here  $f$  is a non unit, non zero algebraic integer coprime to 3 and  $x$ , and  $u$  a non unit, non zero algebraic integer coprime to  $f$ . Note  $P(m)$  has a factor that is  $f^2$ .

That expression comes from expanding  $(v^3 + 1)x^3 - 3vxy^2 + y^3$ , using the substitutions  $v = -1 + mf^2$ , and  $y = uf$ , where additional variables provide an additional degree of freedom.

Now consider the factorization

$$P(m) = (a_1x + uf)(a_2x + uf)(a_3x + uf)$$

where multiplying out shows that

$$a_1 a_2 a_3 = m^3 f^6 - 3 m^2 f^4 + 3m f^2 = f^2 (m^3 f^4 - 3 m^2 f^2 + 3m)$$

so

$$a_1 a_2 a_3 = m f^2 (m^2 f^4 - 3 m f^2 + 3).$$

Therefore, at least one of the  $a$ 's cannot be coprime to  $m$ , and at least one of the  $a$ 's must equal 0 when  $m=0$ .

(Note: The  $a$ 's are roots of a monic polynomial with algebraic integer coefficients so they are algebraic integers.)

Notice that the constant term  $P(0)$  is given by  $P(0) = f^2 (3x u^2 + u^3 f)$  and also that  $P(0)/f^2 = 3x u^2 + u^3 f$ , which is coprime to  $f$ .

Then I have the factor of  $P(m)$ ,  $g_1$ , where  $g_1 = a_1 x + uf$ , where here I also have that  $a_1$  is not coprime to  $m$ .

From my factorization lemma, I have that, when  $m=0$

$$g_1 = c = uf$$

meaning  $f$  is a factor of the constant term.

Therefore, exactly two of the  $a$ 's equal 0, when  $m=0$ , to get the factor  $f^2$  in the constant term  $P(0)$ , while one must not equal 0, or  $f^3$  would be the factor.

Now as noted before in general  $P(m)$  has a factor that is  $f^2$ , and separating that factor off, gives a constant term coprime to  $f$ ; therefore, given  $g_1 = a_1 x + uf$  where with  $m = 0$ ,  $g_1$  gives a factor of  $f$  it must have that same factor in general, proving that two of the  $a$ 's have a factor that is  $f$ .

Therefore, one factor is coprime to  $f$ .

Now letting  $m=1$ ,  $f=\sqrt{5}$ , where I can let  $u=1$  as its value doesn't change the  $a$ 's, I have

$$(m^3 f^6 - 3m^2 f^4 + 3m)x^3 - 3(-1 + mf^2)xu^2 + u^3 = 65x^3 - 12x + 1$$

which may be more easily seen from using  $v = -1 + mf^2 = 4$ ,  $y=1$  with  $(v^3 + 1)x^3 - 3vxy^2 + y^3$ .

Therefore, with the factorization

$$65x^3 - 12x + 1 = (a_1x + 1)(a_2x + 1)(a_3x + 1)$$

one of the  $a$ 's is coprime to 5, which shows where some of the algebraic integer factors distribute despite the factors being irrational.

[end of paper]

---

So the conclusion of this paper is that if the following polynomial is factored as

$$65x^3 - 12x + 1 = (a_1x + 1)(a_2x + 1)(a_3x + 1)$$

where  $a_1$ ,  $a_2$ , and  $a_3$  are algebraic integers, then one of  $a_1$ ,  $a_2$ , or  $a_3$  is coprime to 5.

And the \*negation\* of this statement is that if the polynomial is factored as above, then EACH of  $a_1$ ,  $a_2$ , and  $a_3$  is NOT coprime to 5.

So that's your 'null test' statement.

Clearly it contradicts the conclusion of the paper. It was deliberately constructed to be the negation of the statement of the paper.

So evidently the paper basically passes this "null test": the negation of the conclusion is contradicted by a statement in the paper. I cannot conclude from this that the proof in the paper is wrong.

There is just one little problem.

The null test statement is *\*true\**.

You can prove it in at least 4 different ways.

Proofs have been given by Hall, Magidin, Winter, Decker, and Baron.

This means that a statement in the paper (namely, the conclusion) is contradicted by a *\*true\** statement.

Therefore that statement in the paper must be false.

Therefore the claimed "proof" in the paper is wrong!

Thanks for the null test idea! Works great!

Andrzej