

Re: JSH: Nearly done

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-01/8218.html>

From: Tim Peters (*tim.one_at_comcast.net*)

Date: 01/28/05

Date: Thu, 27 Jan 2005 23:57:21 -0500

[Nora Baron]

...

>> *Harris still seems to think that finding rational x might
>> be a problem. In your other post on this, the one in which
>> you used the Mighty Harris Method to factor $M = 15$, you noted that
>> it is possible, even easy, to find rational a_1 and a_2 , and from this
>> one easily gets rational x . I didn't see immediately how to
>> find such – perhaps it IS easy – I haven't put much effort into
>> it – but I wouldn't mind if you spelled it out.*

[Rick Decker]

> *Okay. Here goes.*

>

> *Let M be the number to be factored. Pick an integer j and
> factor $-j^2$ as the product $b_1 * b_2$. Factor $M^2 - j^2$ as
> the product $f_1 * f_2$.*

>

> *Just for the hell of it, consider the terms*

>

> *$a_1 x + b_1 = f_1$*

> *$a_2 x = b_2 = f_2$*

The first '=' on the line above should be '+'.
>

> *Multiply both sides to get the quadratic equation in x :*

>

> *$a_1 a_2 x^2 + (a_1 b_2 + a_2 b_1)x + b_1 b_2 = f_1 f_2$*

>

> *hence*

>

> *$a_1 a_2 x^2 + (a_1 b_2 + a_2 b_1)x - M^2 = 0$ [1]*

>

> *Thus, x will "factor" M^2 .*

>

> *We want a rational x , so the discriminant of [1],*

>

> *$(a_1 b_2 + a_2 b_1)^2 + 4M^2 a_1 a_2$*

>

> *must be a rational square, r^2 .*

It was all crystal clear to me up until this point, but not after, so I want to pause here. Aren't we really effectively done proving the point right after writing down

$$a_1 x + b_1 = f_1$$

$$a_2 x + b_2 = f_2$$

? Multiplying them together doesn't add any new **constraint**, it just obfuscates everything by mixing up the free choices in horridly complicated ways (a JSH specialty). If we pause right here, it's obvious we can pick any non-zero rational x *_right now_*, solve for a_1 and a_2 (the b_i and f_i are known), and then the quadratic must be satisfied by that $\langle x, a_1, a_2 \rangle$ triple, simply because the quadratic was derived from them to begin with.

Let me be concrete, harkening back to the example:

$$> T = 15^2 - 2^2 = (15 + 2)(15 - 2) = 17 * 13 = 221$$

>

> *Now factor T and $-j^2$. A good starting point is to use the factorization*> *above for T , namely $f_1 = 17, f_2 = 13$. Since j is small, we can factor*> *it easily, say as $b_1 * b_2$, where $b_1 = -4, b_2 = 1$.*

Then

$$a_1 x + b_1 = f_1$$

$$a_2 x + b_2 = f_2$$

is the same as

$$a_1 x - 4 = 17$$

$$a_2 x + 1 = 13$$

or

$$a_1 x = 21$$

$$a_2 x = 12$$

Now pick any non-zero rational x . I'll pick 1001 for the heck of it.

$$x = 1001$$

Then those equations trivially give

$$a_1 = 21/1001$$

$$a_2 = 12/1001$$

and the quadratic must be satisfied too by these values. Check:

$$\begin{aligned} a_1 a_2 x^2 + (a_1 b_2 + a_2 b_1)x &= \\ 21/1001 \ 12/1001 \ 1001^2 + (21/1001 (1) + 12/1001 (-4)) 1001 &= \\ 21*12 + 21 - 12*4 &= \\ 225 = M^2 \end{aligned}$$

Alas, $\gcd(1001, 15) = 1$, so it may not be the greatest discovery ever made in the field after all <wink>.

There was nothing special about the x I picked, nor anything else special about the example that I can see: so long as b_1 , b_2 , f_1 and f_2 are rational, then given any non-zero rational x , there exist rational a_1 and a_2 such that all the equations are satisfied.

> ... *[skipping over what seems to me now a too-complicated, and*
> ... *partly dubious, argument]*

> *Note that these solutions involve the free variable a_2 ,*
> *so since we have [3], we can get *any* rational value of*
> *x , given a suitable choice of a_2 .*

I agree with the conclusion, although if I understand it <wink>, it's a lot easier if you pick the x you want first. That forces a_1 and a_2 .

> *That kind of shoots down anything special about x as a "factor" of*
> *M , as far as I can see.*

Me too. It remains possible that the clear-as-mud details of how James works backward from the quadratic somehow favors finding an x having a common factor with T . I doubt it.

...

> *Unless I've completely misinterpreted his results, all he's doing*
> *is obfuscated factorizing-by-trial-divisors.*

Except that, despite picking trial divisors in a haphazard way, it runs in polynomial time <wink>.