

Re: JSH: Nearly done

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-01/8202.html>

From: Rick Decker (rdecker_at_hamilton.edu)

Date: 01/28/05

Date: Thu, 27 Jan 2005 20:58:52 -0500

Nora Baron wrote:

>

<snip>

>

> *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.*

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

$$a_1 x + b_1 = f_1$$

$$a_2 x + b_2 = f_2$$

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 . Doing a bit of high school algebra we derive

$$\begin{aligned} (b_2 z + (b_1 b_2 + 2m^2))^2 - (r/a_2)^2 &= \\ &= (b_1 b_2 + 2M^2)^2 - (b_1)^2 \end{aligned}$$

where $z = (a_1 / a_2)$. Simplify this by denoting

$$Q = b_1 b_2 + 2M^2 \text{ (which, BTW, equals } M + T)$$

and we get

$$(b_2 z + Q)^2 - (r/a_2)^2 = Q^2 - (b_1)^2 \quad [2]$$

Factor $Q^2 - (b_1)^2$ as $w * ((Q^2 - (b_1)^2) / g)$ so [2] can be decomposed as

$$\begin{aligned} b_2 z + Q + (r/a_1) &= ((Q^2 - (b_1)^2) / g) \\ b_2 z + Q - (r/a_1) &= g \end{aligned}$$

From this we see that

$$b_2 z + Q = (((Q^2 - (b_1)^2) / g) + g) / 2$$

so, eventually, we get that x will be a rational solution to [1] if we let

$$a_1 = a_2 ((Q - g)^2 - (b_1)^2) / 2gb_2 \quad [3]$$

from which we find the rational solutions to [1] to be

$$x = -b_2 (Q - b_1) / (a_2(Q - g - b_1))$$

and

$$x = b_2 g / (a_2(Q - g + b_1))$$

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

[It's amusing to try the "trivial" values of g , namely $g = 1$ and $g = Q + b_1$ and see what happens to x .]

I should mention in passing that I did my best to transcribe my notes accurately. If there are errors in what I've just written, I'm sure you can fix them. I am sure, though, that there are no deal-breakers: the end results are accurate, namely that there are values of the free variable that will give

any x you want.

- >
- > *Given a rational x , Harris will then look at its numerator*
- > *and try to find primes which divide M . Of course I would*
- > *think you need some assurance that such primes are not also*
- > *in the denominators of the things that x is multiplied by –*
- > *I would guess that is very unlikely in a real live problem*
- > *because those factors will be extremely large.*

Immaterial in light of what I've said above. Unless I've completely misinterpreted his results, all he's doing is obfuscated factorizing-by-trial-divisors.

- >
- > *Harris himself has declined to give the details that you have*
- > *given – it is interesting that your presentation is much*
- > *clearer than his – but he keeps referring to his Yahoo group*
- > *and the paper that is available. So I thought: I will just*
- > *join the Yahoo group and have a look at it. So I joined.*

Probably no need to join. Given James propensity for copy/paste, the "paper" is likely just what's in his post ""Checking with congruences" which you don't have to join to see.

<snip>

Regards,

Rick