

Re: JSH: SF: Finally, surrogate factoring

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-06/msg01163.html>

- *From:* Rick Decker <rdecker@xxxxxxxxxxxxx>
 - *Date:* Wed, 07 Jun 2006 13:16:43 -0400
-

jstevh@xxxxxxx wrote:

Rick Decker wrote:

Rick Decker wrote:

Tim Peters wrote:

[added "JSH:" to subject, spared sci.crypt
and alt.math]

[jstevh@xxxxxxx]

...

And it has been posted in
this thread that I DID get it
wrong.

If you do it right, it shows a
dependency on the
factorization of T,
which is no good.

But what if you go the other
way, isolating y on the right
side,
instead of z?

Re: JSH: SF: Finally, surrogate factoring

So instead, you would complete the square twice isolating z on the left and with the second you would get y inside the square on the right.

The reason for wondering is that if you solve for z using the four linear equations, yup, it does solve in such a way that you can have a difference of factors of T, but y does not.

Long-shot.

... and a miss.

I got

$$(42*z + 10*y - 3*f_2 + 19*f_1)^2 = (4*y + 3*f_2 - 5*f_1)^2 + 84*T$$

then, but didn't care enough to double-check it.

That's what I got, too. Mathematica agrees.

(Responding to my own post...)

So completing the square w.r.t y first yields

$$(2*y + 10*z + 5*f_1 - f_2)^2 = (4*z + 3*f_1 - f_2)^2 + 4*T$$

Completing the square w.r.t. z first yields

$$(42*z + 10*y - 3*f_2 + 19*f_1)^2 = (4*y + 3*f_2 - 5*f_1)^2 + 84*T$$

The only problem I have with that is that you have too many solutions for y .

There is one explicit solution for y given by solving the 4 linear equations.

That solution is

$$y = (7g_1 - 3g_2 + 5f_1 - 3f_2)/4$$

which what you give covers, but you could have gotten that by working backwards FROM the explicit solution, and there is one problem.

If T has only two prime factors p_1 and p_2 , there are 8 possible values for y for a given f_1 and f_2 , which represent $g_1 = T, p_1, p_2$, or 1, and the negatives, and $g_2 = 1, p_2, p_1$, or 1, and the negatives.

But your solution has more than that because it gives

$$y = (5f_1 - 3f_2 + 21g_1 - g_2)/4$$

as a solution as well.

No. However, it would be interesting to see how you got this.

Ah. Perhaps you were working from $h_1 * h_2 = 21 * g_1 * g_2$, like this:

Let h_1 and h_2 be chosen so that $h_1 * h_2 = 21 * T$

$$h_1 + h_2 = 10*y + 42*z + 19*f_1 - 3*f_2 \quad [1]$$

$$h_2 - h_1 = 4*y - 5*f_1 + 3*f_2 \quad [2]$$

Then we can write

$$(10*y + 42*z + 19*f_1 - 3*f_2)^2 = (4*y - 5*f_1 + 3*f_2)^2 + 84*T$$

in the form

$$(h_1 + h_2)^2 = (h_1 - h_2)^2 + 4 * h_1 * h_2$$

Then, from [1] and [2] we solve for y to get

$$y = (5*f_1 - 3*f_2 + h_1 - h_2) / 4 \quad [3]$$

Then, since $h_1 * h_2 = 21 * T = 21 * g_1 * g_2$ we may as well pick $h_1 = 21 * g_1$ and $h_2 = g_2$ so [3] becomes

Re: JSH: SF: Finally, surrogate factoring

$$y = (5*f_1 - 3*f_2 + 21*g_1 - g_2) / 4$$

Right?

If that was your reasoning, it's wrong. You can't pick any old values for h_1 and h_2 . Watch:

Solving [1] and [2] for h_1 and h_2 we get

$$\begin{aligned} h_1 &= 7(y + 3 * z + f_1) \\ h_2 &= 3(y + 7 * z + 4 * f_1 - f_2) \end{aligned}$$

But from your original four linear equations we can derive

$$\begin{aligned} g_1 &= y + 3 * z + f_1 \\ g_2 &= y + 7 * z + 4 * f_1 - f_2 \end{aligned}$$

in other words, we are forced to choose

$$\begin{aligned} h_1 &= 7 * g_1 \\ h_2 &= 3 * g_2 \end{aligned}$$

and not your $h_1 = 21 * g_1$ and $h_2 = g_2$.

<snip>

It's why I decided after thinking that this method MUST lead to a surrogate factoring solution as the only way the algebra can avoid the contradiction is to use a surrogate factorization.

You claim otherwise with your post.

No. That was your (incorrect) deduction, as I show above.

Your claims mean that 4 linear equations can be wrong.

I wonder if you just lied.

You just can't resist, can you? Are you naturally boorish, or do you have to work at it?

Regards,

Rick

.

Re: JSH: SF: Finally, surrogate factoring