

Re: Surrogate factoring, update

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-07/2435.html>

From: James Harris (jstevh_at_msn.com)

Date: 07/10/04

Date: 10 Jul 2004 16:42:04 -0700

Jean-Luc Cooke <jlcooke@engsoc.org> wrote in message
news:<ccp66s\$73c\$1@driftwood.ccs.carleton.ca>...

> *James,*

>

> *Keep looking into this. You'll learn a lot. But honestly, this is just
> a variation of Fermat's Difference of Squares factorization:*

Actually in many ways it is. It's where it's different that things
get interesting.

> $pq = n$

>

> $M = \text{mean of } p \text{ and } q$

> $E = \text{error from mean}$

>

> $M = (p+q)/2$

> $p = M+E$

> $q = M-E$

>

> $n^2 = M^2 - E^2$

>

> *Using quadratic reciprocity you can eliminate many possible values, but*

> *then end result is no net improvement in factorization problem.*

That's just one side of what I gave in my original post.

What I've done is link the factorization of what you call n with
another variable that is dependent on the factorization of a number
other than n , which I call the surrogate.

I've found a way that links two different factorizations together.

> *Do yourself a favour – dont' give up on this untill you've quantified*

> *your results with equations and numbers (How many steps will be needed*

> *to use your technique compared to the one above? How much time will it*

> *take for each step?)*

Theoretically at its simplest you'd simply factor $T^2 - 1$, and take all of its factors in combinations where you get the difference to find a rational j .

You get a head start because $T^2 - 1 = (T-1)(T+1)$, and with T odd, both of those are even, and one is divisible by 3.

- >
- > *The $n^2 = M^2 - E^2$ can be re-written in a million different ways with even powers of n (as you did below). What are the advantages? Are there any? Quantify (nto qualify) your results.*
- >
- > JLC

No, I didn't just come up with the standard congruence of squares. Here are the equations pulled out:

$$(jk - Tk + T)(jk + Tk + T) = T^4$$

$$k = (-jT \pm T^2 \sqrt{j^2 - T^2 + 1}) / (j^2 - T^2)$$

and

$$j = (-T \pm T \sqrt{k^2 + T^2}) / k$$

where you'll notice that the second IS the standard congruence of squares while for the first you see something strange as you have $\sqrt{j^2 - T^2 + 1}$.

To get some appreciation for why this is different, let $k = d/c$, and substitute in the second to get

$$j = (-cT \pm T \sqrt{c^2 + T^2 d^2}) / d$$

and consider that if you get j by using the factors of $T^2 - 1$, and the very same congruence of squares that you brought up, then you get c and d , and may have just factored T , along with d as well, by congruence of squares.

Now **some** difference of factors of T WILL get picked no matter what, and at this point I don't know why, if T is not prime, half the time it wouldn't be non-trivial factors.

Note, the point again is that *SOME* factors of T will come out no matter what, and if for some reason they are always trivial, that is, for instance, T itself and 1, then this idea isn't that big of a deal.

But at this point there doesn't seem to be any mathematical reason why one factorization of T would be selected over another!!!

That's the scary thing which I'd like some answers on, as I think there will indeed be reasons why T itself as a factor tends to pop out, but even if non-trivial factors pop out a small percentage of the time, it still might be enough to affect public key encryption.

The problem now is a LOT of questions with few answers.

I'm just pushing the point that with such an idea, in such an area, that if mathematicians are who they say they are, then someone will either step forward and eliminate fears in this area by showing why this idea is not a threat, or there will be interest in understanding how it works.

Basically I found a linkage between factorizations, where if you factor $T^2 - 1$, you may factor T itself as well.

It's like maybe the math doesn't care *what* you factor, as long as you factor something.

So, if you factored T , you might get the factors of $T^2 - 1$, as well.

Mathematically, at this point, I don't see why the math would care.

And it certainly doesn't care that some people depend on the idea that T is hard to factor for their livelihoods!!!

If this idea does work well, and mathematicians sit back and ignore it, if things go badly then they can rightly be blamed by the world.

They are responsible here.

James Harris