

Re: Proof factoring solution is closed form

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-02/3069.html>

From: KeithK (*me_at_nomail.com*)

Date: 02/09/05

Date: Wed, 9 Feb 2005 10:13:01 -0700

<jstevh@msn.com> wrote in message
news:1107951870.252176.91050@g14g2000cwa.googlegroups.com...
> *Rick Decker wrote:*
> > *jstevh@msn.com wrote:*
> > > *One of the most important points to make, which should end the*
> *debate*
> > > *and get someone to contact the US Government so that authorities*
> *can be*
> > > *informed is the closed form proof of surrogate factoring.*
> > >
> > > *By closed form I mean the proof that it is a complete solution*
> *which*
> > > *guarantees the factorization of a target number.*
> > >
> > > *However, after this point, the clock is really ticking, as anyone*
> *can*
> > > *use the information. You have your future in your hands. The*
> *start*
> > > *will be familiar. The closed form proof is short.*
> > >
> > > *Here we go.*
> > >
> > > *Take the two quadratics*
> > >
> > > $yx^2 + Ax - M^2 = 0$
> > >
> > > *and*
> > >
> > > $yz^2 + Az - j^2 = 0$
> > >
> > > *where A, j, and M are integers greater than 0 chosen, where M is*
> *the*
> > > *target to be factored, and you find that you can use T, where*
> > >
> > > $T = M^2 - j^2$
> > >
> > > *and substituting out y to solve for x and z gives*

sci.math: Re: Proof factoring solution is closed form

>>>
>>> $x = z(-Az \pm \sqrt{(Az - 2M^2)^2 - 4TM^2}) / (2j^2 - 2Az)$
>>>
>>> *and*
>>>
>>> $z = x(-Ax \pm \sqrt{(Ax + 2j^2)^2 - 4Tj^2}) / (2M^2 - 2Ax)$
>>>
>>> *and, let $A=1$, and the first equation gives you rational z 's where*
> *those*
>>> *are found by factoring TM^2 , as simply*
>>>
>>> $Az = f_1 + f_2 + 2M^2$
>>>
>>> *where $f_1 f_2 = TM^2$.*
>>>
>>> *Now then there must be some integer z , which factors M , and for*
> *that*
>>> *integer z , you will get a rational x that is probably a fraction,*
> *with*
>>> $A=1$.
>>>
>>> *BUT, if $x = x_{num}/x_{denum}$, where x_{num} and x_{denum} are integers,*
> *then*
>>>
>>> *let*
>>>
>>> $A = x_{denum}$
>>>
>>> *and you have*
>>>
>>> $\sqrt{(x_{denum} (x_{num}/x_{denum}) + 2j^2)^2 - 4Tj^2}$
>>>
>>> *which is just*
>>>
>>> $\sqrt{(x_{num} + 2j^2)^2 - 4Tj^2}$
>>>
>>> *as the A absorbed the x_{denum} .*
>>>
>>> *And notice that x_{num} is given by the integer factorization of*
> Tj^2 , *as*
>>> *you just have*
>>>
>>> $x_{num} = 2j^2 - g_1 - g_2$, *where $g_1 g_2 = Tj^2$, and are integers.*
>>>
>>> *Okay, more or less, down to here.*
>>>
>>> *The A can always pull factors from the denominator in this way, so*
> *the*
>>> *full solution is in fact given by the factorization of Tj^2 , which*
> *must*
>>> *give you an integer x_{num} , which will either be a factor of M or*

> can be
> > > used to get a z which must factor M .
> > >
> > That's an interesting avenue, using either x or z , but I don't see
> > why it must work.
> >
>
> Given any rational x that is a solution, if one exists, you can simply
> let A equal the value of its denominator, proving some other x' exists
> which IS an integer.
>
> > > It's a closed solution.
> > >
> > > What does that mean practically?
> > >
> > > It means that someone tonite can take some large target M , find a
> > > j ,
> > > and with that get a T , and then factor j and T , and use them to
> > > then
> > > get Tj^2 , and using combinations of factors of Tj^2 , guarantee
> > > themselves a factorization of their target M .
> >
> > There's a good chance that for M in the range of the RSA challenges
> > if someone started tonight, they would still be waiting for a
> > factorization when the universe ended, using your method. That's
> > not to say that your method is guaranteed to be impracticable,
> > but you certainly haven't convinced anyone so far.
>
> Well that's what you say, but where your proof?
>
> I've actually looked at the equations showing how many combinations you
> get by two for factorizations.
>
> If you have a number with only two prime factors, then you get 1
> combination by two's, so if j were a number with only two prime factors
> that's the number you'd have.
>
> But, it probably is not and you have T to factor as well, and it tends
> to have a lot of prime factors.
>
> Now I've actually calculated, while you appear to be trying to convince
> others to ignore my work without even bother to give mathematics, and
> my calculations show that if you form a number by multiplying the first
> one thousand primes together you get about 150 million combinations by
> two's.
>
Umm the number of combinations of $n = 1000$ things taken $k=2$ at a time is
 $n!/[k!(n-k)!] = 1000!/[2!(998)!] = 1000*999/2 = 499,500$.

KeithK

sci.math: Re: Proof factoring solution is closed form

> Now then Decker, how big of a number is formed by multiplying the first
> 1000 primes together?
>
> I dare you to reply to this post and answer at least that one question.
>
>>>
>>> Now for some large number the number of combinations would be huge,
> but
>>> they'd be certain of success if they cycled through them all.
>>
>> Not necessarily. As you should know, when trying to factor M there
>> are some values of j that give *no* useful factorizations. When that
>> happens, all one can do is start anew with a new j .
>
> Well then the theory must be wrong, as my analysis is that for any
> integer j greater than 1 it should work.
>
> If it doesn't, then I'm wrong, and I'd be very interested in seeing
> why!!!
>
> I have no interest in pushing wrong positions, but from what I've seen
> it should work.
>
> If I made a mistake in my analysis that mistake should be capable of
> being shown.
>
>>>
>>> And that's a polynomial time problem, as the equation defining how
> many
>>> combinations of those factors there are is a polynomial one.
>>>
>> That's not what we mean by a poly-time solution. In fact, one might
>> have to search for factors in a space that could be about as large as
> M
>> itself. If you're going to get a poly-time solution, you'll at least
>> have to cut down the search to $O((\log M)^k)$, for some fixed k .
>>
>
> Why?
>
> You aren't giving any information here, but just assertions without
> explanation.
>
> Why should I or anyone else just believe you?
>
>>> Now I'm using these examples because they're easier to explain
> with,
>>> but the full surrogate factorization theory shows that only a
>>> factorization of T is needed!
>>>
>> Even if that's so, it doesn't necessarily give you a good algorithm.

Re: Proof factoring solution is closed form

> > *Frankly, I'd love to see a proof that all one has to do is factor T.*
> >
>
> *It's not difficult. I've worked out the details on my Yahoo! site, but
> before moving to the more complicated mathematics, I'd like to get past
> the easy.*
>
> *For those thinking I'm dodging, my answer is that certain posters
> routinely try to move to the most complicated areas of my theories
> where it's easy, well, to lie and confuse people about what's
> mathematically true or not.*
>
> *So I've learned to try and keep it simple.*
>
> > > *So I'm at a primitive level with this discussion, as the full
> theory
> > > indicates that only a factorization of T is needed, which is what
> I've
> > > been trying to get to work.*
> > >
> > > *You can scoff at this if you want, but do the math. Trace it out.
> > > Understand how A can absorb factors.*
> > >
> > *The value of A unimportant, as long as it's not zero. "Move on,
> folks,
> there's nothing to see here."*
> >
>
> *Now you can see why. The poster is basically trying to deflect
> interest in my work.*
>
>
> >
> > *Regards,*
> >
> > *Rick*
>
> *Now Rick Decker has been at his game for years now, working to deflect
> interest in my work, no matter what it is.*
>
> *Now that's math society for real, not television or some movie, and I
> have to get past that first.*
>
> *The most important assertion Decker made in his post is that with
>
> $x = z(-Az \pm \sqrt{(Az - 2M^2)^2 - 4TM^2}) / (2j^2 - 2Az)$
>
> and
>
> $z = x(-Ax \pm \sqrt{(Ax + 2j^2)^2 - 4Tj^2}) / (2M^2 - 2Ax)$
>
>*

sci.math: Re: Proof factoring solution is closed form

- > *derived in my original post that given a full factorization of T_j^2 to*
- > *get x , you cannot get a factorization of M .*
- >
- > *If true then I'm wrong. It's math people. Either you're wrong, or*
- > *you're right.*
- >
- > *Now I'm curious to know if I'm wrong, and then I'll be curious about*
- > *why.*
- >
- > *That's called mathematical investigation.*
- >
- > *Now Decker will play his games and work for whatever reasons motivate*
- > *such a person to deflect people from my research, but what I can do, is*
- > *do what I enjoy and continue that research despite people like him.*
- >
- > *What you can do is pay attention to the facts.*
- >
- >
- > *James Harris*
- >