

## Re: Simple answer, surrogate factoring

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2005-03/1807.html>

---

**From:** David Eather (*eather\_at\_tpg.com.au*)

**Date:** 03/05/05

Date: Sun, 6 Mar 2005 00:19:45 +1000

jstevh@msn.com wrote:

> *Nathan wrote:*

>> *jstevh@msn.com wrote:*

>>> *fiziwig wrote:*

>>>> *Could you take a reasonably small number, say 8 or 10*

>>>> *digits, and DEMONSTRATE, step by step how your method would be*

>>>> *applied to factoring that number. Can I see how you use it to*

>>>> *factor an easy number like 50,985,511 for example?*

>>

>>> *Why? It'd make as much sense to factor an easy number like 15.*

>>>

>>> *I'm more of a theoretical guy. I want to know why.*

>>

>> *So give a clear explanation of "how".*

>

> *I \*have\* posted algorithms.*

>

> *Even this thread contains an algorithm which should work perfectly.*

>

> *I'm just not interested in going through the effort of demonstrating*

> *the algorithm with a test number, especially when other posters have*

> *posted the algorithms in programmatic form, as has happened.*

>

> *I'm the theory guy.*

-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA1

I'm the theory guy? What sort of cop out is that? If you want to be "creative" then remember at the end of the process you have to \*create\* something – not just inconsistent gibberish but a solid result. % year old are "creative" – unfortunately all their space suits fail to work – perhaps you can aim a little higher and produce something real / testable

>

-----BEGIN PGP SIGNATURE-----

Version: PGP 8.1

sci.math: Re: Simple answer, surrogate factoring

iQA/AwUBQim/8ZS9Fk5okqe7EQIuPACgtia2cXVmOVDmVuwyzpGBuDAGhWsAn1zX  
N3k3ybTOwa2Zwvh+qX7ByG3

=mnWr

-----END PGP SIGNATURE-----

- > *Other people are the experimental people.*
- >
- > *It's how physics works, and I'm showing how it can be done with*
- > *mathematics.*
- >
- > *If you push me on details I get annoyed, as I'm the theory guy.*
- >
- > *I'm the theoretical amateur mathematician.*
- >
- >>
- >>> *So I give the mathematical basis for various ideas, and if you're*
- >>> *interested enough, you can play with it and test it out.*
- >>
- >> *The "basis" you've given so far isn't enough to really figure out*
- >> *what it is you mean.*
- >>
- >
- > *I know it is for some people, and that's important to me as more than*
- > *anything else I want to get to the bottom of this and understand it.*
- >
- > *To me people who can figure out what I'm doing are more valuable than*
- > *people who need extreme detail, as those people are more likely to be*
- > *able to test or critique.*
- >
- > *More than anything else I need people who are capable of pointing out*
- > *mistakes in my reasoning, or testing out the ideas themselves.*
- >
- > *Later I can address people who need more help, once the basic research*
- > *is done, and I'd fully intend to do that as I see it as an important*
- > *point.*
- >
- > *One of my BIG beefs with Wiles is that he disdained explaining his*
- > *work to a general audience claiming it was just beyond them.*
- >
- >>> *I don't like specific factorization requests though I have tried*
- >>> *some at times, as they don't serve a purpose.*
- >>
- >> *Okay, so you pick the number. Just show us, in \*complete\* detail.*
- >>
- >
- > *I explained above on that point.*
- >
- > *Yes, I can do it, and later I might, but for now, I need people who*
- > *can do it for themselves who feel motivated to do so, as hopefully*
- > *then, they may do more.*
- >

Re: Simple answer, surrogate factoring

sci.math: Re: Simple answer, surrogate factoring

>>> *If I factor the number, people will just put up bigger numbers, and*  
>>> *if I could factor RSA Challenge numbers I wouldn't be talking about*  
>>> *it on Usenet, but posters would keep putting up numbers until that*  
>>> *point and beyond, as that's how Usenet is.*  
>>  
>> *I think you misunderstood fziwig. I think he's just asking for a*  
>> *demonstration. That's something I would like to see, too.*  
>>  
>> *You get a lot of hostile, rhetorical questions, and you deserve that.*  
>> *But I read this as a genuine request.*  
>>  
>> *Do you really think you've explained "surrogate factoring" in enough*  
>> *detail for someone else to implement it? I don't think you have.*  
>  
> *People have implemented it.*  
>  
> *Given that the perfect algorithm is now out, I'm sure many more people*  
> *have implemented it, and that number will grow rapidly, which may be*  
> *unfortunate.*  
>  
> *I would like to address a more general audience later, but for now I*  
> *need people with expertise.*  
>  
> *People who can find holes in my reasoning or test out the ideas.*  
>  
> *I need experimental mathematicians.*  
>  
>  
> *James Harris*