

Re: surrogate factoring

Source: <http://sci.tech--archive.net/Archive/sci.math/2006-06/msg01212.html>

- *From:* "Tim Peters" <tim.one@xxxxxxxxxxx>
 - *Date:* Wed, 7 Jun 2006 18:54:45 -0400
-

[gjedwards@xxxxxxxx]

A previous poster was right – having anything to do with JH's posts is like rubbernecking a traffic accident. Sad but difficult to resist. Anyway ...

The bit I don't get (well one of the bits) is what specifically JH *thinks* is the point of surrogate factoring. I know it's total nonsense but does anyone have a clue *why* he thinks it's worthwhile? I guess I find the nature of the delusion somewhat puzzling and it's an amusing diversion to work out what he actually thinks.

I really should get out more.

Me too, but so long as we're both house-ridden today, and I've enjoyed more quality "SF time" than anyone other than James ...

First, "surrogate factoring" doesn't really mean anything specific. There are literally dozens of distinct methods James has _called_ "surrogate factoring" over the past two years. While they've all been wrong (in the sense that none have been efficient factoring methods, and for some it was a miracle if they ever found a factor), "total nonsense" is either overstatement or understatement :-)

The general idea is that you want to factor T, but factor some "related" integer S ("the surrogate") instead and hope to relate the factors of S to T's factors. That's perfectly sensible so far as it goes. For example, many methods try to factor $k \cdot T$ instead, and that can even be useful "by eyeball". Consider $T=817$. A tiny bit of thought shows it's not divisible by 2, 3, or 5, and then you might notice it's about a third of 2500. Indeed,

$3 \cdot T =$
 $3 \cdot 817 =$
 $2451 =$
 $2500 - 49 =$
 $50^2 - 7^2 =$
 $(50+7) \cdot (50-7) =$

Re: surrogate factoring

57*43

by inspection, so you can know almost at once that 43 and $57/3 = 19$ are factors of T, if only you think about $3*T$ instead of T.

More, variations on that can be turned into straightforward algorithms that always find factors (Google for "Fermat's method"). Some of them don't even need division, which may be surprising at first sight.

Alas, trial division is usually more efficient (if you suspected I put some care into picking the 817 example, you were right ;-)), and a few of James's SF attempts have been inefficient variations on this theme, excruciatingly obfuscated ways of trying to find integers I and J such that $I^2 - J^2 = k*T$, in which case $\gcd(I \pm J, T)$ has a good chance of revealing a non-trivial factor of T.

Most typica