Re: JSH: Contradictory behavior, issue of math fraud

Source: http://sci.tech−archive.net/Archive/sci.math/2007−09/msg00495.html

- *From*: rossum <rossum48@xxxxxxxxxxxx>
- *Date*: Mon, 03 Sep 2007 22:18:53 +0100

On Mon, 3 Sep 2007 15:09:16 −0500, "Mas Plak" <spamless@xxxxxxxxxxxx>
wrote:

> "JSH" <jstevh@xxxxxxxxx> wrote in message
> news:1188833147.062403.32640@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
>
>> On Sep 3, 1:42 am, rossum <rossu...@xxxxxxxxxxxx> wrote:
>>
>>> On Sun, 02 Sep 2007 10:19:32 −0700, JSH
>>> <jst...@xxxxxxxxx> wrote:
>>>
>>>> But if the idea turns out to be a brilliant one
>>>> which means factoring
>>>> is not a hard problem after all, then how can
>>>> mathematicians who not
>>>> only couldn't figure it out, but who ignored it
>>>> when presented with it
>>>> be considered to be true experts in the field?
>>>
>>> In its current version surrogate factoring is too slow to be
>>> considered "brilliant". Only when you have speeded it up
>>> sufficiently
>>
>> I asked, what if?
>
> Stick to reality, James, I know it can be hard for you, very hard, but
> accept the FACT that surrogate factoring is twice as slow as random
> guessing.
>
> TWICE AS SLOW AS RANDOM GUESSING.

Not always. Some of the iterations of James' method are better than random. For example, with k = 30, n = 7, 8, 9 ... and a suggestion by Tim Peters of using S = 27000 * (2*k^2 + n*T) then the results are:

Fermat average = 8.35 probes.
JSH average = 608.86 probes.
Probe ratio = 1 : 72.883
Trial average = 118.63 probes.
Reverse average = 12.70 probes.
Random average = 745.43 probes.
500 trials, 0 misfactors found.

Average n's tried per factorisation: 2.430
Average k's tried per n: 1.000

This version is better than random. Tim's reasoning for his suggestion was that by ensuring a lot of small factors in S, 27000 = (2 * 3 * 5)^3, each S will generate a lot more factor pairs and so is more likely to hit a factor of T. The results show that with Tim's suggestion fewer values of n have to be tried before hitting a factor.

Taking this further, I tried k = 30 with n = 12, 18, 24, 30, ... and I got James' method down to about 580 probes.

rossum

.