

Re: Prime factorization

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-09/6642.html>

From: Phil Carmody (*thefatphil_demunged_at_yahoo.co.uk*)

Date: 09/27/04

Date: 27 Sep 2004 23:28:48 +0300

willem@bermon-dot-net.no-spam.invalid (Wilhelm) writes:

[Erm, this bit is me:]

> > *let's say i use the 4! sieve i can generate candidates as follows*

> >

> *What does 4! give you that 6 doesn't?*

>

> ...

> > *The sieve will not find numbers $<n$ but these can be found when*

> > *creating the sieve. Anyway computations above 9! are memory hogs so*

> >

> *What does 9! give you that 210 doesn't?*

>

>

> *You're reinventing the wheel.*

[And this bit is Wilhelm:]

> *Well i certainly did not come here to get flamed or pushed into the*

> *ground. So my idea isn't going to work on 100digit big primes but*

> *it's doing quite nicely on big prime numbers and it does work nicely*

> *as a prime number generator.*

I admit to being blunt, perhaps unnecessarily so. However, please see things from our view – you appeared to do no research, not even a simple googling for factorisation methods, before you came here and asked your question. If you'd have done the research then

- 1) You'd find your answers without waiting for others to reply.
- 2) You'd not have annoy the grumpy regulars here
- 3) You'd find bucket-loads more information

I've already provided you with 3 references. The above also has a hidden pointer, that if you'd have done your research you'd have picked up on. What you've done is reinvented the "wheel", an essential part of most modern sieves. Basically you discard a proportion of the non-primes simply by not even looking at them, saving you time.

However, these are 'small factor' speed-ups, that permit you to look at problem sizes that are a little bit larger. They never let

sci.math: Re: Prime factorization

you extend more than just that small factor. And what's also most important to factorisation researchers is the growth of the expected work factor as the numbers get larger. If you've got $O(\sqrt{N})$ work, then a factor of 10 lets you factor numbers two digits longer. No big deal. If you've got an $O(N^{1/5})$ algorithm, then a factor of 10 lets you factor a number 5 digits longer. No great shakes there, either, but still better than just 2 digits. The biggest way to make an impact is to decrease the `_growth_` of the work-factor itself, and not simply scale it down by a constant factor. You might get little gain with small numbers, but you get larger gains at larger numbers by doing so. That's why you can get algorithms that are 10^{40} times faster at 100 digits than naive trial division.

> Anyway i learn't today that this forum doesn't have very much nice
> people like Phil with his fucked up comments, ever heard of
> productive commentary?. I did get a few comments i can use thank you
> to those people.

Hmmm, was the reference to Riesel fucked up, or the reference to Bressoud, or perhaps the reference to Crandall and Pomerance? Please let me know so that I can inform the authors of the utter uselessness of their books.

Oh no – I get it – it was a spelling flame! All three refs were fucked!

Riesel and Bressoud spell factorisation the US way – 'factorization'. And 'perspective' has a 't', and it's a colon not a comma in the name.

/Mea culpa/ – I shall beat myself over the head with Knuth for the rest of the evening.

> Also this forum keeps coming up with Error 500 which someone should
> look at.
>
> And for your information $9! = 362880$ and i made a boo-boo because $10!$
> is doable which is approx 3628800 *whateveryouusetostoreyournumbers
> of sieving data.
>
> And yes this is reinventing the wheel. What's wrong with that?

Your wheel's too big. Try again with 210 rather than 9! Try 210 rather than 10! too. Try 2310 after that, then 30030, then 510510.

Or don't. Your choice.

Phil

--

They no longer do my traditional winks tournament lunch - liver and bacon. It's just what you need during a winks tournament lunchtime to replace lost ... liver. -- Anthony Horton, 2004/08/27 at the Cambridge 'Long Vac.'

Re: Prime factorization