

Re: Prime lists and Computation

Source: <http://sci.tech--archive.net/Archive/sci.math/2005-07/msg01294.html>

- *From:* "Dik T. Winter" <Dik.Winter@xxxxxx>
 - *Date:* Sat, 9 Jul 2005 23:45:02 GMT
-

In article <Xns968EA5FD9CF0Bcparkesactewaglnetau@xxxxxxxxxxxxxx> Carl Parkes <Carl_Parkes@xxxxxxxxxxxxxx> writes:

- > Q1. Given a large integer $\{x\}$. If it is proved to be prime, what other information is generated?
- >
- > 1. Complete Prime list to $x^{(1/2)}$?
- > 2. The modulo residues?

None of those above. At the same time I will answer the following question:

Q1a. Given a large integer $\{x\}$. It is proved not to be prime, what other information is generated?

And here also the answer is nothing.

- > Q2 Is there a complete list of primes to X Published?
- > $X \sim 10^{20}$? $X \sim 10^{30}$. $X = 10^{??}$

Complete lists were published, but not until 10^{20} , there are 2220819602560918840 primes until that number. I do not think sufficient storage is available to store them all.

- > Q3 Storage: When does it become more efficient to store the prime list than to generate/calculate it.

As soon as you do not have sufficient storage available to store the primes. I think that with a 100 GB drive you might store all 12 digit primes (it might be reduced a bit if you store only differences). But there is no need to. Most algorithms that prove primality/non-primality use only short prime lists for trial division. Other algorithms are used for the remainder. E.g. in a program I use (that can be used to prove primality for numbers upto 300 digits), the list of primes used contains only the primes of 5 digits or less.

- > Q4 What would be the expected time to factor a 1 MB file, if it was interpreted as a very integer.

Argh. Currently factoring a 2048 bit number is already impossible in real time. With MPQS it was estimated that an increase of the number of digits by 3 would double the factoring time. Going from there to 4096 bits would increase the factoring time by a factor of 2^{682} , or

Re: Prime lists and Computation

a factor of:

20065826040452474621738395244141115820123061381619162977212070095324\
44822043258980603663076888118153086465060751410758099754116916726609\
75003349867654872163770874926419389518668810415568707379046298723287\
04

quite a lot I would say, and now we are only upto 4096 bits.

My estimate is that with current methods and current computers we would not yet have factored a number that large (unless it has some special properties) when we had started with the big bang.

—
dik t. winter, cwi, kruislaan 413, 1098 sj amsterdam, nederland, +31205924131
home: bovenover 215, 1025 jn amsterdam, nederland; <http://www.cwi.nl/~dik/>
.

- **Follow-Ups:**

- ◆ **Re: Prime lists and Computation**

- ◆ *From:* Phil Carmody

- **References:**

- ◆ **Prime lists and Computation**

- ◆ *From:* Carl Parkes

- Prev by Date: **Re: Is the set N of natural numbers well defined?**

- Next by Date: **Re: People are stupid**

- Previous by thread: **Re: Prime lists and Computation**

- Next by thread: **Re: Prime lists and Computation**

- Index(es):

- ◆ **Date**

- ◆ **Thread**