

# Re: Prime lists and Computation

---

*Source:* <http://sci.tech--archive.net/Archive/sci.math/2005-07/msg02417.html>

---

- *From:* Phil Carmody <[thefatphil\\_demunged@xxxxxxxxxxxxx](mailto:thefatphil_demunged@xxxxxxxxxxxxx)>
  - *Date:* 16 Jul 2005 23:51:56 +0300
- 

"Dik T. Winter" <[Dik.Winter@xxxxxx](mailto:Dik.Winter@xxxxxx)> writes:

- > In article <[Xns968EA5FD9CF0Bcparkesactewaglnetau@xxxxxxxxxxxxx](mailto:Xns968EA5FD9CF0Bcparkesactewaglnetau@xxxxxxxxxxxxx)> Carl Parkes <[Carl\\_Parkes@xxxxxxxxxxxxx](mailto:Carl_Parkes@xxxxxxxxxxxxx)> 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, wat
    - > other information is generated?
    - > And here also the answer is nothing.

I hate to dive in and contradict, as the subtleties will probably confuse the OP, but it's entirely reasonable for information to be leaked by a succeeded compositeness test, for example. The total quantity of information leaked is most likely negligible, but typically non-zero. A lot depends on the compositeness test (or primality test) used. All /.\*PRP/ tests leak information, for a start.

- >> 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.

After a lengthy discussion on this subject several years ago, we concluded:  
Any sieve that's slower than a hard disk is insufficiently advanced.  
Any hard disk which is slower than a sieve is insufficiently advanced.

- >> Q4 What would be the expected time to factor a 1 MB file, if it was
- >> interpreted as a very [large] integer.
- >>
- > Argh. Currently factoring a 2048 bit number is already impossible in
- > real time.

I don't know about you, but I create my 1MB files from dd'ing /dev/zero not /dev/random! The insertion of 'arbitrary' would remove ambiguity.

## Re: Prime lists and Computation

Phil

—

If a religion is defined to be a system of ideas that contains unprovable statements, then Godel taught us that mathematics is not only a religion, it is the only religion that can prove itself to be one. — John Barrow

.

---

- *Follow-Ups:*

- ◆ *Re: Prime lists and Computation*

- ◇ *From:* Dik T. Winter

- *References:*

- ◆ *Prime li*