

## Re: A question about Probable Primes

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2006-01/msg03363.html>

---

- *From:* Phil Carmody <[thefatphil\\_demunged@xxxxxxxxxxxx](mailto:thefatphil_demunged@xxxxxxxxxxxx)>
  - *Date:* 22 Jan 2006 14:17:24 +0200
- 

Marc Bogaerts <[mar\\_c.bo\\_gaerts@xxxxxxxxxxxx](mailto:mar_c.bo_gaerts@xxxxxxxxxxxx)> writes:

- > If I recall correctly a probable prime is a number  $n$  that satisfies
- >  $a^n \equiv a \pmod n$ , and this for a limited series of values of  $a$ .
- >
- > In fact this only means that a set of numbers  $< n$  have multiplicative
- > order that is a divisor of  $(n-1)$ ;
- >
- > This is clearly not enough to prove that it is a prime number (does
- > anybody have some examples of a non prime satisfying this equation for
- > a non negligible set of  $a$ 's?).

Carmichael numbers satisfy all Fermat PRP tests. (By definition.)

Strong PRP tests have more interesting failure cases.

For small sets, Jaeschke.

For large sets, Arnault.

Both of the above have been improved upon by later computations.

- > On the other hand, the multiplicative group of the residues mod  $n$
- > forms a cyclic group of order  $\phi(n)$ , if one could explicitly
- > find a number  $a$  that is a generator of this group, would that prove  $n$
- > to be a prime?
- >
- > Example  $n=78965412325879886541233547894322017892532463949$
- >
- >  $n-1$  factors as 2, 2, 3, 53, 38431, 69661, 90731, 106273, 7320461,
- > 657039278116952161
- >
- > Take  $a=2$ , then for all the divisors  $d$  of  $(n-1)$  I calculate  $a^d$  and
- > this is only  $\equiv 1$  when  $d=(n-1)$ , so I conclude  $n$  is a prime number, is
- > this correct?

Yup. You've shown  $n-1 \mid \phi(n)$ , and you already know  $\phi(n) \leq n-1$ .

Phil

--

What is it: is man only a blunder of God, or God only a blunder of man?

-- Friedrich Nietzsche (1844-1900), *The Twilight of the Gods*

.

- **References:**

- ◆ *A question about Probable Primes*

- ◇ *From:* Marc Bogaerts

- Prev by Date: *Re: Cantorian pseudomathematics*

- Next by Date: *Re: An infinite number question*

- Previous by thread: *Re: A question about Probable Primes*

- Next by thread: *is  $f'$  continuous on this interval*

- Index(es):

- ◆ *Date*

- ◆ *Thread*