

## Re: Why to call it pseudorandom?

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2004-08/5375.html>

---

**From:** John Morriss ([jmorriss\\_at\\_idirect.com](mailto:jmorriss_at_idirect.com))

**Date:** 08/30/04

Date: 29 Aug 2004 19:31:54 -0700

"Peter Webb" <[webbfamily@DIESPAMDIEoptusnet.com.au](mailto:webbfamily@DIESPAMDIEoptusnet.com.au)> wrote in message news:<41308afb\$0\$25605\$afc38c87@news.optusnet.com.au>...

> "David C. Ullrich" <[ullrich@math.okstate.edu](mailto:ullrich@math.okstate.edu)> wrote in message

> news:hl11j09t9o6cd9tvc9a6o32se65hhlofkq@4ax.com...

>> On 28 Aug 2004 05:55:20 -0700, [luiroto@yahoo.com](mailto:luiroto@yahoo.com) (Luis A. Rodriguez)

>> wrote:

>>

>>> If an algorithm produces a infinite sequence of digits that never

>>> falls into a loop and passes the most stringent statistical tests

>>> about its uniformity, why to call it pseudorandom?

>>

>>> maybe because the digits are not random? if they're produced by

>>> an algorithm then they're not unpredictable.

>>

>>> If genius discover a system of equations for the roulette, the

>>> old "random" experiments made with roulettes will appear at daybreak

>>> as pseudorandom?

>>

>>

>> \*\*\*\*\*

>>

>> David C. Ullrich

>>

>>> sorry about the inelegant formatting - typing

>>> one-handed for a few weeks...

>>

>>> And at a practical level, all computer rand() generators loop. They take a

>>> seed n and calculate f(n), then f(f(n)) etc.

>>> So they loop over whatever range n can take (at most). If n is a 32 bit

>>> integer - and it often is - it will loop over 4 billion numbers, probably

>>> enough to generate enough minesweeper boards and bridge hands to keep most

>>> people happy.

>>> Many rand() functions are however random according to all other statistical

>>> criteria.

I once took a look at the algorithm that MS used in writing the RND function for the Commodore 64 BASIC. A seed was multiplied by a fixed

sci.math: Re: Why to call it pseudorandom?

number, another fixed number was added, the four bytes of the result were reversed, and a little bit of cleansing up as done. This became the random number, and the new seed. As you said, the process would of necessity loop after some (hopefully large) number of cycles.

I found, quite by accident, a seed that looped in a ring of SIX (6) random numbers!!