

Re: Periodicity of $a^n \bmod c$

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-09/6632.html>

From: Doug Goncz (dgoncz_at_aol.com)

Date: 09/27/04

Date: 27 Sep 2004 20:05:58 GMT

I have requested The Art of Computer Programming, Volume 2, Seminumerical Algorithms, from a nearby branch of my jurisdiction's public library, for pickup at my local branch.

>From: James Waldby j-waldby@pat7.com

>Doug Goncz wrote:

>> Who's Knuth and what's the name of his textbook?

><http://www-cs-faculty.stanford.edu/~knuth/taocp.html> has info

>re Donald E. Knuth and The Art of Computer Programming vol. 2

>Seminumerical Algorithms, Addison-Wesley, ISBN 0-201-89684-2

I have noticed that t , the period of $a^n \bmod c$, known to Marsaglia as the multiplicative order of a , with a coprime to c , is a factor of ϕ , as several here have reminded me.

Also N , the solution to $a^N \bmod c + b^N \bmod c = c$, is a factor of t .

I can't prove anything right now but I am lucky enough to have the time to study Knuth's exercise 20.

I have Marsaglia's article in my camera at fax resolution, using a home made copy stand. I believe this is not a copyright violation as it is for personal study.

Could any of you advise me on that copyright issue. Zaremba's publisher's copyright claim seems clear enough.

Yours,

Doug Goncz (<ftp://users.aol.com/DGoncz/incoming>)

Student member SAE for one year.

I love: Dona, Jeff, Kim, Mom, Neelix, Tasha, and Teri, alphabetically.

I drive: A double-step Thunderbolt with 657% range.