

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

**Source:** <http://sci.tech-archive.net/Archive/sci.math/2004-09/5832.html>

---

**From:** James Waldby ([j-waldby\\_at\\_pat7.com](mailto:j-waldby_at_pat7.com))

**Date:** 09/25/04

Date: Fri, 24 Sep 2004 19:52:10 -0500

Doug Goncz wrote:

...

> >George Marsaglia directed me to his article "*The Structure of Linear  
> >Congruential Sequences*"

...

> -----  
> >*The period of an arbitrary sequence  $x_{n+1}=ax_n+b \bmod m$  is established  
> >in G. Marsaglia, "The structure of linear congruential sequences",  
> >{it Applications of Number Theory to Numerical Analysis}, Z. K. Zaremba,  
> >ed.,  
> >New York: Academic Press, pp249--285, (1972).  
> >It is summarized in exercise 20, section 3.2.1.2 of Knuth's Vol. 2.*  
> -----

...

> *Who's Knuth and what's the name of his textbook?*  
>  
> *I figure if I can work exercise 20 that will be progress.*

<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

The referenced problem is on page 22 (in 2nd ed.) and rated  
"M24" in difficulty, ie, about an hour of work for the  
mathematically inclined who have already absorbed the  
background material in pages 9 through 20.

-jiw