

Re: Generators of cyclic group

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/3007.html>

From: Marcel Martin (mm_at_ellipsa.no.spam.net)

Date: 10/29/03

Date: Wed, 29 Oct 2003 21:48:50 +0100

Mok-Kong Shen a écrit :

>

> *Marcel Martin wrote:*

>>

> [snip]

>> *In short, if x is a NRQ different from -1 , we have $(x^2 \neq 1)$ and*

>> *$(x^q \neq 1)$ and $(x^{2q} = 1)$, which implies that x is a generator.*

>

> *Could you please explain a little bit why this is so?*

> *Thanks.*

If x is in $\text{QNR} - \{-1\}$ then the 3 conditions hold. If they hold, the order of x is $2q$, i.e., the order of x is equal to the group order, thus x is a generator.

mm