

Re: Generators of cyclic group

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/2930.html>

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

Date: 10/28/03

Date: Tue, 28 Oct 2003 23:03:28 +0100

Robin Lavall?e a écrit :

>

> *Hello,*

>

> *Given that $p = 2q + 1$ where p and q are odd prime. Prove that the
> generators of the group Z^*_p are $QR_p - \{-1\}$.*

>

> *Yes, this is an assignment question.*

>

> *1) I've been able to prove that QR_p cannot be generators.*

> *2) I've also been able to prove that -1 (i.e. $2q$) cannot be a*

> *generator either.*

> *3) However, I'm unable to prove that the rest of the group members are*

> *all generators.*

>

> *For (1):*

>

> *If g is a generator, then for all b , there exist an i such that $b =$*

> *g^i .*

> *However, we know that g is a quadratic residue, so $g = a^2$. Hence, $b =$*

> *$a^{2i} = a^{i^2}$. Hence, b must be a quadratic residue as well! So, g*

> *only generates other quadratic residue (not the whole group).*

>

> *For (2): This is rather trivial.*

>

> *(3) I'm not getting anywhere for that one. Any idea? (I would prefer a*

> *hint, not a complete solution).*

Notice that if x is not a quadratic residue then $x^q = -1$.

mm