

## Re: Generators of cyclic group

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/2996.html>

---

**From:** Anton Stiglic (*stiglic\_at\_cs.mcgill.ca*)

**Date:** 10/29/03

Date: Wed, 29 Oct 2003 10:32:33 -0800

I think you can use a counting argument. You have already proved that quadratic residues mod  $p$  cannot be generators. You also proved that  $-1$  cannot be a generator. How many elements are left? And how many generators are there mod  $p$  where  $p = 2q + 1$  with  $q$  prime (Euler phi function will help out here...).

—Anton