

Re: Another Quad. Residue question

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-05/msg00023.html>

- *From:* "Larry Hammick" <larryhammick@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Sun, 01 May 2005 07:41:49 GMT
-

"Nobody"

>> 1) Is there a good comprehensive source on
>> quadratic residues?

>> 2) Is it true that given a prime P , then there
>> there is between P and
>> $2P$ an (even?) integer for which P is not a
>> quadratic
>> residue?

>> 3) If 2) is true, can such an integer be
>> expressed as a function
>> of P .

>>

>> Thanks much for information.

>

> If $p \equiv 3 \pmod{4}$, we can pick $p+4$.

> (Pick $p+1$ if you want an even integer.)

>

> If $p \equiv 1 \pmod{4}$, we can pick $p+k$,

> where k is any quadratic non-residue mod p .

> (Pick an odd $q \cdot n - r$ if you want an even integer.)

He wants a quadratic *non*-residue. Alas there is no known algorithm of any value. Even the very elementary proof that nonsquares exist, and are one-to-one with the squares, is indirect: there are $(p-1)/2$ squares (omitting zero), and the rest are nonsquares. But how to find a nonsquare without effectively finding *all* the squares? Nobody knows.

LH

.

- *Follow-Ups:*

- ◆ *Re: Another Quad. Residue question*

- ◇ *From:* Nobody

- *References:*

Re: Another Quad. Residue question

◆ *Re: Another Quad. Residue question*

◇ *From:* Nobody

- Prev by Date: *Re: Dimensionality Reduction to a Circle*
- Next by Date: *calculating 3+ root with only a square root function*
- Previous by thread: *Re: Another Quad. Residue question*
- Next by thread: *Re: Another Quad. Residue question*
- Index(es):
 - ◆ *Date*
 - ◆ *Thread*