

Re: Another Quad. Residue question

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-05/msg00187.html>

- *From:* "Larry Hammick" <larryhammick@xxxxxxxxxxxxxxxxxxxx>
 - *Date:* Mon, 02 May 2005 11:51:20 GMT
-

"Nobody" <STBILLY@xxxxxxxxxxxx> wrote in message
<news:28135758.1114980680311.JavaMail.jakarta@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
>> "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
>>> P is not a quadratic
>>> residue?
>>> 3) If 2) is true, can such an integer be
>>> ger 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.
>
> I thought his question was : find an (even) integer
> n between p and $2p$ so that p is a $q \cdot n - r \pmod{n}$.
>
> Finding a $q \cdot n - r \pmod{p}$ (between p and $2p$)
> would be a different problem ...
>
>> 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

Re: Another Quad. Residue question

> > squares? Nobody knows.

> > LH

Yes, sorry, I saw "p" for "q" and vice versa. I suffer slightly from anno domini.

LH

• **References:**

◆ **[Re: Another Quad. Residue question](#)**

◇ *From:* Larry Hammick

◆ **[Re: Another Quad. Residue question](#)**

◇ *From:* Nobody

• Prev by Date: **[Re: abundance of irrationals!](#)**

• Next by Date: **[Re: abundance of irrationals!](#)**

• Previous by thread: **[Re: Another Quad. Residue question](#)**

• Next by thread: **[Relation on the zeta function](#)**

• Index(es):

◆ **[Date](#)**

◆ **[Thread](#)**