math −− values of f(x) (mod p)

Source: http://sci.tech−archive.net/Archive/sci.math/2008−04/msg02050.html

- *From*: quasi <quasi@xxxxxxxx>

- *Date*: Fri, 11 Apr 2008 00:31:01 −0500

Two conjectures ...

Conjecture (1):

If n is an odd positive integer, then for all sufficiently large primes p (depending on n), there does not exist f in Z_p[x], with deg(f) = n, such that for all r in Z_p, f(r) is a square in Z_p.

Conjecture (2):

If n is an even positive integer, then for all sufficiently large primes p (depending on n), if f in Z_p[x], with deg(f) = n, is such that for all r in Z_p, f(r) is a square in Z_p, then f = g^2 for some g in Z_p[x].

Remarks:

Conjecture (1) is trivially true for n = 1.

Conjecture (2) is true for n = 2, and can be proved as a corollary to the proposition I proved in the thread "quadratic quadratic non−residue".

For n = 3, 4, 5, 6, test data convincingly supports the conjectures, but of course, doesn't prove them.

Short of a general proof, a proof for n = 3 or n = 4 would be nice.

quasi
.