Re: mth powers in GF(p^n)

Source: http://sci.tech−archive.net/Archive/sci.math/2005−09/msg04651.html

- *From*: quasi <quasi@xxxxxxxx>
- *Date*: Thu, 29 Sep 2005 01:32:49 −0700

On Thu, 29 Sep 2005 15:24:42 +1000, Gerry Myerson
<gerry@xxxxxxxxxxxxxxxxxxxxxxxxx> wrote:

>In article <af6nj1dlr2f8t3n409h1ghsohjit5j398n@xxxxxxx>,
> quasi <quasi@xxxxxxxx> wrote:
>
>> On 28 Sep 2005 21:07:44 −0700, "Wolff" <daniel.wolff@xxxxxxxx> wrote:
>>
>> >Hello, any hints on showing that (p^n−1,m)=1 implies each member of
>> >GF(p^n) is an mth power?
>> >Thanks.
>> >DMW
>>
>> Hints:
>>
>> Consider the map f defined by f(x)=x^m. Can you verify that f is a
>> homomorphism from the multiplicative group of GF(p^n) to itself?
>>
>> What is the kernel of f?
>>
>> Note: The condition (p^(n−1),m)=1 is clearly equivalent to the much
>> simpler condition (p,m)=1, and probably should have been stated that
>> way. However if it had been stated as (p,m)=1, then you would need to
>> push it back up to (p^(n−1),m)=1 in order to compute the kernel of f.
>
>Maybe p^n−1 means (p^n) − 1, not p^(n − 1).

Yep −− p^n−1, thanks. After all, it's a field, so the multiplicative
group is all but 0.

So then ignore the "Note:" part of my reply −− sorry, but the hints
should still be ok.

quasi
.

- ***References***:

- ***mth powers in GF(p^n)***
  - *From:* Wolff
- ***Re: mth powers in GF(p^n)***
  - *From:* quasi
- ***Re: mth powers in GF(p^n)***
  - *From:* Gerry Myerson

- Prev by Date: ***Re: How to solve (2x + 3y)^3?***
- Next by Date: ***Re: Romanian math olympiad problem***
- Previous by thread: ***Re: mth powers in GF(p^n)***
- Next by thread: ***Re: mth powers in GF(p^n)***
- Index(es):
  - ***Date***
  - ***Thread***