Re: prime~.

Source: http://sci.tech−archive.net/Archive/sci.math/2004−10/1187.html

---

From: L.B. (*metafert_at_mail.ru*)
Date: 10/04/04

```
Date: 4 Oct 2004 06:53:25 −0700
```

"mina_world" <mina_world@hanmail.net> wrote in message news:<cjqd4r$c9u$1@news.hananet.net>...
> "Michael Lockhart" <ml1000@bellsouth.net> wrote in message
> news:X828d.227877$%n4.3977@bignews6.bellsouth.net...
> > "mina_world" <mina_world@hanmail.net> wrote in message
> > news:cjq9ds$a7o$1@news.hananet.net...
> > > hello......doctor~
> > >
> > > p is a prime.
> > > n is positive integer.
> > >
> > > show that
> > > p | (a^n) − 1 for some a in Z
> > > => (p^2) | (a^n) − 1
> >
> > That's not true.
> >
>
> oh......i'm sorry. my mistake.
>
> p is a prime.
>
> show that
> p | (a^p) − 1 for some a in Z
> => (p^2) | (a^p) − 1
>
> it's exact.
>
> Pardon me. sorry.

Let a^p=1 mod p. From other side a^(p−1)=1 mod p, Fermat's theoren.
So, we get a=1 mod p. Let a=1+p*b. Then

a^p−1=(1+p*b)^p−1=1+sum(binomial(p,i)*(p*b)^i, i=1..p) −1
=sum(binomial(p,i)*(p*b)^i, i=1..p). As is well know − binomial(p,i)=0
mod p and obviously (p*b)^i=0 mod p, sinse
a^p−1=sum(binomial(p,i)*(p*b)^i, i=1..p)=0 mod p^2