

# Re: Order modulo $p^n$ (Number Theory)

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2008-09/msg01559.html>

---

- *From:* Angus Rodgers <[twirlip@xxxxxxxxxxx](mailto:twirlip@xxxxxxxxxxx)>
  - *Date:* Mon, 15 Sep 2008 14:15:37 +0100
- 

On Mon, 15 Sep 2008 04:09:53 -0700 (PDT),  
"dark.sorrow.mystery@xxxxxxxxx"  
<[dark.sorrow.mystery@xxxxxxxxx](mailto:dark.sorrow.mystery@xxxxxxxxx)> wrote:

On Sep 15, 2:21 am, Angus Rodgers <[twir...@xxxxxxxxxxx](mailto:twir...@xxxxxxxxxxx)> wrote:

On Sun, 14 Sep 2008 08:01:55 -0700 (PDT),  
"dark.sorrow.myst...@xxxxxxxxx"

<[dark.sorrow.myst...@xxxxxxxxx](mailto:dark.sorrow.myst...@xxxxxxxxx)> wrote:

On Sep 15, 12:37 am, Tonic <[Tonic...@xxxxxxxxx](mailto:Tonic...@xxxxxxxxx)> wrote:

On Sep 14, 3:56 pm,  
"dark.sorrow.myst...@xxxxxxxxx"  
<[dark.sorrow.myst...@xxxxxxxxx](mailto:dark.sorrow.myst...@xxxxxxxxx)> wrote:

Hello need some help with a  
question in number theory  
im attempting

Let  $p$  be an odd prime and  $n$   
> 1 an integer. Find the  
order of  $(1 + p)$   
modulo  $(p^n)$ .

Hints:

1.- Try with  $p = 3$ ,  $1 + p = 4$  and  $n = 1, 2, 3$ ,  
4, and then with  $p = 5$   
and  $1 + p = 6$ , and then even with  $p = 7$  and  
 $1 + p = 8$ ...

Re: Order modulo  $p^n$  (Number Theory)

2.– Now prove your guess or hunch: use Newton's binomial with

$(1 + p)^{p^{n-1}}$ ...you may want to show that the binomial

coefficient  $\binom{p^r}{r}$  is divisible by  $p$  iff  $r$  is a multiple of  $p$ ...

Cheers, thanks you for your help, I should of used the examples to find the order. Then try prove it. was trying to come up with the order via theorems and was getting know where. Thanks Tonio on the binomial, that really helped with the proof of the order.

Can you explain your proof?

My original "proof" was a load of dingo's kidneys (as I would have realised if I had typed it up neatly to post to sci.math). I think I've fixed it now, but I'm still reluctant to post it until you've shown your work.

well first through writing a few examples I saw that the order should be  $p^{n-1}$ . After that I used Newton's binomial and showed that  $p^n$  divides all the coefficients apart from when  $k=0$ . (lower bound on my sum) which gives a remainder 1, giving the required  $(1+p)^{p^{n-1}} \equiv 1 \pmod{p^n}$ . So either that is the order or the order divides  $p^{n-1}$ . Then I showed for any powers less than  $n-1$  the expansion doesn't give the remainder 1 and the coefficients are not divisible by  $p^n$ . :)

So your argument goes something like this?

Let  $m$  be any integer such that  $1 \leq m < n$ . Then (in a pseudo-LaTeX notation, which I hope is readable):

$$(1 + p)^{p^m} = 1 + p^{m+1} + \sum_{k=2}^{p^m} \binom{p^m}{k} (p^k)$$

## Re: Order modulo $p^n$ (Number Theory)

In the case  $m = n - 1$ , the argument is presumably that, for  $k = 2, 3, \dots, n - 1$ , the coefficient  $\binom{p^m}{k}$  is divisible by  $p^{n-k}$  – this being the weakest assumption needed to infer easily that the RHS is congruent to 1 (mod  $p^n$ ).

I'm not sure what the argument is supposed to be for  $m = 1, 2, \dots, n - 2$ , to show that the RHS is not congruent to 1 (mod  $p^n$ ). However, it is clearly enough to prove this for  $m = n - 2$  – which is fortunate, because the statement that  $p^{n-k}$  divides  $\binom{p^m}{k}$  isn't true for  $m < n - 2$ . (Take  $k = 2$ .)

I first tried arguing along these lines (having guessed the answer by numerical experiment like everyone else), but somehow I couldn't, and still can't, see how the argument is supposed to go\*. So I came up with a different proof, which I'm almost certain is valid – after correcting the rubbishy version of it I first came up with! – but I also have a strong feeling that it involves too messy a calculation.

So it looks as if I'm missing something that is obvious to everyone else. It's embarrassing to ask, but (before I give my own possibly unnecessary proof) would someone please explain in gory detail just how this one is supposed to go? 8-P

\*I expect it is true that  $p^{n-k}$  divides  $\binom{p^{n-2}}{k}$  for  $k = 2, 3, \dots, n - 2$ , but this just looks so fiddly to prove that I can hardly bring myself to look at it. So, what am I missing here? (The proof for  $m = n - 2$  is enough to give the required result, but that is starting to get on to my own proof.)

--

Angus Rodgers  
(twirlip@ eats spam; reply to angusrod@)  
Contains mild peril

.