

Re: Order modulo p^n (Number Theory)

Source: <http://sci.tech-archive.net/Archive/sci.math/2008-09/msg01577.html>

- *From:* quasi <quasi@xxxxxxxx>
 - *Date:* Mon, 15 Sep 2008 11:28:25 -0400
-

On Mon, 15 Sep 2008 14:15:37 +0100, Angus Rodgers
<twirlip@xxxxxxxxxxxx> wrote:

would someone please explain in gory detail just
how this one is supposed to go?

Here's one version, essentially along the lines described by the OP,
but with more details included ...

proposition:

If p is an odd prime then $p+1$ has order $p^{(n-1)} \bmod p^n$.

proof:

First, a lemma:

If p is an odd prime and $p^r \parallel x$, where x in \mathbb{Z} and r in \mathbb{N} , then

$$p^{(r+1)} \parallel (x+1)^p - 1.$$

proof of the lemma:

Using the binomial theorem,

$$(x+1)^p - 1 = x^p + c_{-1} * x^{(p-1)} + \dots + c_{-(p-1)} * x$$

where $c_k = \binom{p}{k}$.

Claim each term on the RHS, except the last, is divisible by $p^{(r+2)}$,
and the last term is divisible by $p^{(r+1)}$ but not by $p^{(r+2)}$.

From this we would immediately get

$$p^{(r+1)} \parallel (x+1)^p - 1$$

Re: Order modulo p^n (Number Theory)

as required.

It remains to verify the claim.

First consider the leading term.

$$p^r \parallel x \Rightarrow p^{pr} \parallel x^k$$

Since $p \geq 3$ and $r \geq 1$,

$$p^{pr} \parallel x^k \Rightarrow p^{(3r)} \mid x^p \Rightarrow p^{(r+2)} \mid x^p$$

Next consider the other terms.

For $k = 1, \dots, (p-1)$

$$p^1 \parallel c_k$$

and

$$p^{((p-k)*r)} \parallel x^{(p-k)}$$

hence

$$p^{((p-k)*r+1)} \parallel c_k * x^{(p-k)}$$

For $k = 1, \dots, (p-2)$,

$$(p-k)*r+1 \geq 2*r+1 \geq r+2$$

$$\text{so } p^{(r+2)} \mid c_k * x^{(p-k)}$$

Finally, for $k = (p-1)$,

$$(p-k)*r+1 = r+1$$

$$\text{so } p^{(r+1)} \parallel c_{(p-1)} * x$$

which completes the verification of the claim, and completes the proof of the lemma.

corollary:

If p is an odd prime, and n in \mathbb{N} , then

$$p^n \parallel (p+1)^{(p^{(n-1)})} - 1$$

proof:

Proceed by induction.

Re: Order modulo p^n (Number Theory)

Re: Order modulo p^n (Number Theory)

The verification for $n=1$ is immediate.

Next, suppose the corollary is true for $n=m$, for some m in \mathbb{N} .

Thus, $p^m \parallel (p+1)^{p^{m-1}} - 1$.

Letting $x = (p+1)^{p^{m-1}} - 1$, and applying the lemma,

$$p^{m+1} \parallel (x+1)^p - 1$$

that is,

$$p^{m+1} \parallel (p+1)^{p^m} - 1$$

which completes the induction, and proves the corollary.

Returning to the proof of the proposition, let s be the order of $(p+1)$ mod p^n .

By the corollary,

$$p^n \mid (p+1)^{p^{n-1}} - 1$$

hence

$$(p+1)^{p^{n-1}} \equiv 1 \pmod{p^n}$$

It follows that $s \mid p^{n-1}$.

Applying the corollary again,

$$p^{n-1} \parallel (p+1)^{p^{n-2}} - 1$$

hence

$$p^n \text{ does not divide } (p+1)^{p^{n-2}} - 1$$

Equivalently

$$(p+1)^{p^{n-2}} \not\equiv 1 \pmod{p^n}$$

and hence, s does not divide p^{n-2} .

It follows that $s = p^{n-1}$, which completes the proof.

quasi

.