

Re: Counterexample to $t((c^n - a^n) \bmod b) \mid \phi(b)$

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-11/3741.html>

From: Daniel W. Johnson (panoptes_at_iquest.net)

Date: 11/18/04

Date: Thu, 18 Nov 2004 11:57:42 -0500

Doug Goncz <dgoncz@aol.com> wrote:

> >From: dgoncz@aol.com (Doug Goncz) (Me)
>
> > $\phi(6)=2$ (5 and 1 do not divide 6)
>
> Neither does 4.
>
> I just misspelled $\phi(b)=3$, it wasn't calculated correctly.
>
> So does the period of $(c^n - a^n) \bmod b$ divide $\phi(b)$ or doesn't it?
>
> I say it doesn't always divide $\phi(b)$.

I say you're wrong.

$c^{(n+\phi(b))} - c^n$ is a multiple of b (for sufficiently large n in the case that $\gcd(b,c) > 1$). The same is true of $a^{(n+\phi(b))} - a^n$.

Therefore $(c^{(n+\phi(b))} - a^{(n+\phi(b))}) - (c^n - a^n)$ is a multiple of b .

Therefore $(c^{(n+\phi(b))} - a^{(n+\phi(b))}) \bmod b = (c^n - a^n) \bmod b$

If that doesn't establish that the period of $(c^n - a^n) \bmod b$ is a factor of $\phi(b)$, what does?

--

Daniel W. Johnson
panoptes@iquest.net
<http://members.iquest.net/~panoptes/>
039 53 36 N / 086 11 55 W