

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

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-11/3965.html>

From: Doug Goncz (dgoncz_at_aol.com)

Date: 11/19/04

Date: 19 Nov 2004 12:06:16 GMT

>*From:* Phil Carmody thefatphil_demunged@yahoo.co.uk

>*Don't just "say", prove.*

Good advice.

$a \ b \ c \ (c^n - a^n) \bmod b$

5 6 7 0 2 0 2 0 2...

period is two (2).

The totatives of $b=6$ are 1, 4, and 5. 1 has no factor and can have no factor in common with 6. $\phi(6) = 3$.

The period of the dual subtractive exponential generator with $\gcd(a,b,c)=1$ and $a < b < c < a+b$

$(c^n - a^n) \bmod b$

does not always divide the phi of its corresponding base.

I tolerance everything and tolerate everyone.

I love: Dona, Jeff, Kim, Kimmie, Mom, Neelix, Tasha, and Teri, alphabetically.

I drive: A double-step Thunderbolt with 657% range.

I fight terrorism by: Using less gasoline.