

Re: effective Method to calculate n–th power

Source: <http://sci.tech–archive.net/Archive/sci.math/2005–06/msg01226.html>

- *From:* Jyrki Lahtonen <lahtonen@xxxxxx>
 - *Date:* Wed, 08 Jun 2005 16:58:22 +0300
-

William Elliot wrote:

If q is the order of g^x , then the order of g^{x^n} can be calculated as I hinted in other post. That is different than the value of g^{x^n} which, knowing the order, can be 'simplified'.

How can you compute the order of g^{x^n} starting from the order of g^x alone??

E.g. consider the multiplicative group \mathbb{Z}_{17}^* of order 16. Assume that the other given data is $g^x=4$ and $n=3$.

Now we could have

- A) $g=2, x=2$, so the answer would be $g^{x^n}=2^8=1 \pmod{17}$, an element of order 1, or
- B) $g=4, x=1$, so the answer would be $g^{x^n}=4^1=4 \pmod{17}$, an element of order 4.

Do you now see that we are given insufficient information?

Cheers,

Jyrki

.