

Re: effective Method to calculate n–th power

Source: <http://sci.tech–archive.net/Archive/sci.math/2005–06/msg01225.html>

- *From:* William Elliot <marsh@xxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 8 Jun 2005 07:05:17 –0700
-

On Wed, 8 Jun 2005, Jyrki Lahtonen 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??

>

$$g^{x^n} = (g^x)^{x^{n-1}}$$
$$o(a^k) = o(a)/(k, o(a))$$

> E.g. consider the multiplicative group 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?

No, I often avoid eye strain, by not reading equations without spaces.

.

• *Follow-Ups:*

- ◆ **Re: effective Method to calculate n–th power**
◇ *From:* Jyrki Lahtonen

• *References:*

- ◆ **effective Method to calculate n–th power**
◇ *From:* Zsuzsanna Doncho
- ◆ **Re: effective Method to calculate n–th power**
◇ *From:* Mkajuma
- ◆ **Re: effective Method to calculate n–th power**
◇ *From:* Zsuzsanna Doncho
- ◆ **Re: effective Method to calculate n–th power**
◇ *From:* William Elliot

Re: effective Method to calculate n–th power

◆ ***Re: effective Method to calculate n–th power***

◇ *From:* Jyrki Lahtonen

- Prev by Date: ***Re: effective Method to calculate n–th power***
- Next by Date: ***Re: Rotated square in space***
- Previous by thread: ***Re: effective Method to calculate n–th power***
- Next by thread: ***Re: effective Method to calculate n–th power***
- Index(es):
 - ◆ ***Date***
 - ◆ ***Thread***