

Re: generators be bound

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-10/2643.html>

From: Phil Carmody (*thefatphil_demunged_at_yahoo.co.uk*)

Date: 10/24/03

Date: 24 Oct 2003 17:52:39 +0300

"Tom St Denis" <tomstdenis@iahu.ca> writes:

> "Mok-Kong Shen" <mok-kong.shen@t-online.de> wrote in message
> news:3F988551.610D9516@t-online.de...
>>
>>
>> Tom St Denis wrote:
>>>
>>> [snip]
>>> So what should I have said to mean a generator of a sub-group of a
> given
>>> order?
>>
>> My math knowledge is poor and maybe I misunderstood you,
>> but, if you have a subgroup (of whatever order) of a cyclic
>> group, then it is also cyclic and there must be an element
>> of it that generates that subgroup and that element is by
>> definition a generator of that subgroup. Or am I missing
>> something?
>
> That's just my point. According to the folk here that's not a generator.
> Unless it generates the entire group it's just a ??? [blank]

Generator of a proper subgroup.

Generators always generate all of what they generate, by definition.

Subgroups are groups, by definition.

> What really happens is all generators are in fact primitive [to some
> sub-group]. Take $\mathbb{Z}/7\mathbb{Z}$ for instance. There will be sub-groups of order 2, 3
> and 6. Note that $\mathbb{Z}/7\mathbb{Z}$ actually has 7 elements so the group of order 6 must
> be a sub-group of it as well. There will be an element $[g=3]$ which
> generates an order 6 group but there are also elements which generate
> smaller sub-groups [e.g. $g=2$ generates a group of order 3].
>
> The point is w.r.t the 3 element sub group $\{2, 4, 1\}$ of $\mathbb{Z}/7\mathbb{Z}$ $g=2$ is
> primitive since it generates the entire group. w.r.t. $\mathbb{Z}/7\mathbb{Z}$ multiplicative
> sub-group $\{3,2,6,4,5,1\}$ $g=2$ is not primitive.

sci.crypt: Re: generators be bound

I think I'd avoid the use of the word primitive in those contexts. Primitive only makes sense if the group in which it's primitive is unambiguously specified. If you're juggling group G and subgroup S within a paragraph then you'd need to explicitly say which group was being talked about every time you want to use the word primitive.

Best of all, define your groups, subgroups and generators just once, clearly and unambiguously. After that hopefully all uses of them should be self explanatory, and you shouldn't need to keep mentioning the properties which were part of definitions.

- > *Not to abuse notation though. I agree that without further details*
- > *"generator" should therefore be w.r.t. the multiplicative group of maximal*
- > *order [as others stated].*

We've not said that. "the multiplicative group of maximal order" is meaningless.

- > *My point though is that it isn't invalid to say*
- > *"g=4 is a generator of prime order modulo a safe prime". It really does*
- > *generate such a sub-group.*

Yup, that's one way of describing it.

Phil

--

Unpatched IE vulnerability: protocol control chars
Description: Circumventing content filters
Reference: <http://badwebmasters.net/advisory/012/>
Exploit: <http://badwebmasters.net/advisory/012/test2.asp>