

Re: $a^{(b^x)} \bmod n$?

Source: <http://sci.tech--archive.net/Archive/sci.math/2005-06/msg03927.html>

- *From:* "richard miller" <richard@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>
 - *Date:* Wed, 22 Jun 2005 19:00:09 +0100
-

<fredsaf_20055@xxxxxxxxxx> wrote in message
news:1119442304.187215.127240@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

> Given positive integers a,b,x,n is it possible to efficiently compute:
>
> $a^{(b^x)} \bmod n$?
>
> $\phi(n)$ is unknown and b^x is so large it can't be used directly.
>
> Or is it known this to be a hard problem?
>
> Thanks.
>
> --
> Fred
>

It can be done efficiently with a computer. You use the fact that

$$a^{(b^x)} = (a^{(b^{(x-1)})})^{b^1}$$

And work in reverse, i.e. start with $a^b \bmod n$ and keep raising to the b'th power, see further. Denoting

$$a_1 = a^b \bmod n,$$

then

$$a_2 = a_1^b \bmod n = a^{(b^2)}$$

$$a_3 = a_2^b \bmod n = a^{(b^3)}$$

and repeat x times to obtain

$$a_x = a_{x-1}^b \bmod n = a^{(b^x)}.$$

E.g. if x is 1000, then repeat 1000 times.

To raise a^b you use the binary method in the previous respondents reply.

RJM

-
- *Follow-Ups:*
 - ◆ [Re: \$a^{\(b^x\)} \bmod n\$?](#)
◇ From: fredsaf_20055@xxxxxxxxxx
 - ◆ [Re: \$a^{\(b^x\)} \bmod n\$?](#)
◇ From: Ioannis

 - *References:*
 - ◆ [a^{\(b^x\)} \bmod n?](#)
◇ From: fredsaf_20055

 - Prev by Date: [Re: Orlow cardinality question](#)
 - Next by Date: [Re: Orlow cardinality question](#)
 - Previous by thread: [Re: \$a^{\(b^x\)} \bmod n\$?](#)
 - Next by thread: [Re: \$a^{\(b^x\)} \bmod n\$?](#)
 - Index(es):
 - ◆ [Date](#)
 - ◆ [Thread](#)