

Re: Congruence with division

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-08/msg06205.html>

- *From:* "scattered" <jcoleman@xxxxxxxxxxxxxxxx>
 - *Date:* 31 Aug 2005 06:17:58 -0700
-

Ulrich Sondermann wrote:

> I'm trying to break down a computing problem. I have a number to raise to a
> power and take the modulus of. If I can make the exponent a power of 2 then
> the mod problem is an easy one regardless of size. Here is a simple problem
> but in my case the numbers are quite large.
>
> $3^{13} = 3 \pmod{7}$, I would like to make this $(3^{16})/(3^3)$ Buy computing the
> numerator and denominator separately to simplify the problem.
>
> but $3^{16} = 4 \pmod{7}$ and $3^3 = 6 \pmod{7}$
>
> TIA
> Ulie

Greetings,

The idea of first exponentiating and then taking mods is deeply flawed. Instead, use a modular-exponentiation algorithm. Here is a recursive approach to define a function $\text{pow}(x,a,n)$ to compute $x^a \pmod{n}$:

$$\begin{aligned} \text{pow}(x,a,n) &= \{ 1 \text{ if } a = 0 \\ &x \text{ if } a = 1 \\ &(\text{pow}(x,k,n)*\text{pow}(x,k,n)) \pmod{n} \text{ if } a = 2k \\ &(\text{pow}(x,k,n)*\text{pow}(x,k,n)*x) \pmod{n} \text{ if } a = 2k+1 \end{aligned}$$

There are ways to put this in a loop (google "modular exponentiation"), but even a straightforward implementation of the above in Derive (not the fastest piece of software out there) will allow you to raise one hundred digit number by another hundred digit number mod a third hundred digit number in a small fraction of a second.

Hope that helps

–John Coleman

.

- **References:**
 - ◆ **Congruence with division**
 - ◇ *From:* Ulrich Sondermann
- Prev by Date: **Re: Congruence with division**
- Next by Date: **Re: infinity**
- Previous by thread: **Re: Congruence with division**
- Next by thread: **Multiplicative Seminorms**
- Index(es):
 - ◆ **Date**
 - ◆ **Thread**