

1 modular arithmetic

Solution of $a^b \% c$ for large a and b:

if(a, c) coprime:

$$a^b \% c = a^{(b \% \phi(c))} \% c$$

else if($b \geq \phi(c)$)

$$a^b \% c = a^{(b \% \phi(c) + \phi(c))} \% c$$

else $a^b \% c = a^b \% c$

mod inverse: $a^{m-2} \bmod m$