Hello!

I’ve been recently tinkering with the beginnings of a STARK VM and one of the things I’ve been considering is using Residue Numeral Systems to represent the numbers for it. RNS allows you to take an integer, represent it as a set of remainders modulo a set of moduli, letting you do cool things like carryless multiplication, addition, and subtraction, all over the field bounded by the product of the moduli.

However, the disadvantage of the system is that non-arithmetic operations like shifts and binary ops are very expensive. I’m currently doing them by converting to a ‘normal’ u256 and then converting back, although I have some ideas to implement with base extension that should improve efficiency.

I’m hoping to use RNS for my implementation, as I’ve already been getting decent performance benefits from it, but I’m not sure if the fact that it is over a field specified by the product of coprime moduli instead of a prime or binary field will have a security impact.

Any advice on things to watch out for while working on this?