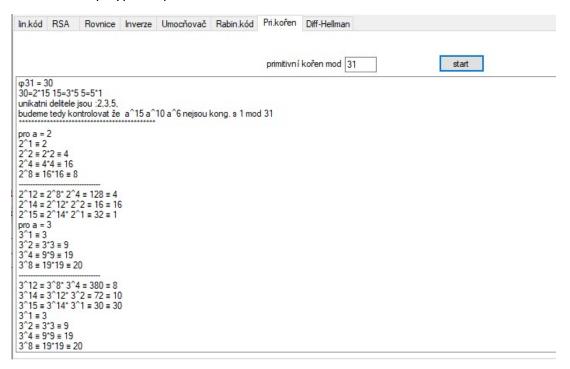
## Math engine

Step by step nástroj pro řešení algoritmických problémů v rozsahu předmětu diskrétní matematika pro potřeby zkoušek v distanční formě.

## Vybrané funkcionality:

Postup výpočtu primitivního kořene



Výpočet postupu alogoritmu pro bezpečnou výměnu klíčů v síti



• Postup výpočtu soustavy 2 rovnic lineárních kongruencí

lin.kód RSA Rovnice	Inverze Umocňovač	Rabin.kód Pri.kořen	Diff-Hellman	
c ≡ 8 mc	od 23 c ≡	24 mod 31		Start
31c = 8·31 = 248 23c = 24·23 = 552				
8c = 248 - (1·552) = -304 7c = 552 - (2·-304) = 1160 1c = -304 - (1·1160) = -146- c = -38 (mod 713) = 675(mo				