CMSE491 Problem session 23.11.2020

1. GLR method: lattice, vector, matrix, linear combination, NTRU for integers lattice, vector norm, vector sum, difference, scalar product, angle between vectors, projection of one vector on another one, finding projection of a vector orthogonal to another vector, GLR iteration, GLR stop condition
2. NTRU for polynomials: polynomial, polynomial addition/subtraction, multiplication/division, quotient, remainder, finding of polynomials GCD, multiplicative inverse, polynomial rings $R, R\_{q}, R\_{p}$. Parameters of NTRU, constraints on NTRU parameters, secret keys $f\left(x\right), g(x)$ selection, public key $h(x)$ definition, NTRU encryption, decryption, center-lifting
3. NTRU for integers: constraints, secret keys, public key, encryption, decryption, finding of GCD and multiplicative inverse for restricted numbers