Notes for RC6:

Correct two mistakes:

Homomorphism:

Start with notes: coset

Converse of Lagrange’s Theorem: zach p194

Modular Arithmetic:

Three notations (interpretation of each other)

Explain: :

Existence/uniqueness of modular inverse: by group theory or

Arithmetic Function:

Exercise: notation of

Example: calculate

Chinese Remainder Theorem: two methods

(mod 120)

Extra Topic:

Fundamental theorem of arithmetic: write the power of p

Binomial Coefficients

Estimation of the inequalities