Modular Arithmetic

Moshe Rosenfeld

October 5, 2010

1 To help me prepare material for appliactions of number theory please let me kniow which of the following topics need to be covered in class.

1. Relatively prime
2. GCD (greatest common divisor)
3. Extended GCD
4. "Inverse Mod" ($a^{-1} \bmod b$)
5. Chinese remainder theorem.
6. Fermat's theorem.
7. Primality testing
8. Carmichael numbers
9. RSA (cryptosystems)
10. Quadratic residues.
11. Factoring integers