MATH/CSCI 4116: CRYPTOGRAPHY, WINTER 2019

Handout 1: Problems for Homework 1

Homework 1: Do the following problems from the textbook: 3.13 #1, 2, 4, 6, 7, 8. Also do the problems below.

Problem 1. In the ring $\mathbb{R}[x]$, let $a(x) = 2x^4 + 5x^3 + 7x^2 + 4x + 2$ and $b(x) = x^3 + 3x^2 + 4x + 2$.

(a) Find the quotient and remainder of dividing $a(x)$ by $b(x)$.

(b) Use Euclid's algorithm to find a greatest common divisor of $a(x)$ and $b(x)$.

Problem 2. In $\mathbb{Z}$, prove: if $a \equiv b (\mathrm{mod}\, c)$, then $\gcd(a, c) = \gcd(b, c)$.

Problem 3. In $\mathbb{Z}$, prove: if $\gcd(a, b) = c$, then $\gcd(a^2, b^2) = c^2$. Hint: consider prime factorizations.