Math 437 – Homework 3

Due 10:15am on Thursday, February 2, 2017

Please indicate any sources you used for a given problem on the solution to that problem. For example, if you worked with another student to get the solution to a problem, please indicate who. You are welcome to work together in small groups, but please try the problems on your own first.

Problem 1. Let $a = x^6 + x^2 + 1$ and $b = x^4 + x^3 + x^2 + x + 1$ in $\mathbb{Z}_2[x]$.

(a) Find the greatest common divisor of a and b.
(b) Find polynomials $c, d \in \mathbb{Z}_2[x]$ so that $ac + bd = \gcd(a, b)$.

Problem 2.

(a) Let F be a field and $f(x) \in F[x]$ be a polynomial of degree 2 or 3. Show that f is irreducible if and only if $f(x)$ does not have any roots in F
(b) Find all irreducible polynomials of degree 1, 2, and 3 in $\mathbb{Z}_2[x]$.
(c) Give an example of a reducible polynomial of degree 4 in $\mathbb{Z}_2[x]$ with no roots in $\mathbb{Z}_2$.

Problem 3. Let F be the field $\mathbb{Z}_2[x]/(f)$ where $f = x^3 + x^2 + 1$.

(a) How many elements are in F and F^*?
(b) For each $1 \leq k \leq 7$, find a polynomial of degree ≤ 2 in $\mathbb{Z}_2[x]$ that equals $x^k \bmod (f)$. Is f primitive?
(c) Find a multiplicative inverse for $x^2 + x + 1$ in F.