CS 6001 Homework 3

Michael Catanzaro, Jacob Fischer, Christian Storer

October 21, 2016

1 Problem 1

$(9x^2 + 3x + 5)/(7x + 3)$

$$
\begin{array}{rlccc}
 & & \text{6x} & + 1 & \text{R } 2 \\
\cline{2-5}
\text{7x+3} &) & 9x^2 & + \text{3x} & + 5 \\
 & - & 9x^2 & + \text{7x} & \\
\cline{3-5}
 & & & \text{7x} & + 5 \\
 & & - & \text{7x} & + 3 \\
\cline{4-5}
 & & & & 2
\end{array}
$$

$(9x^2 + 3x + 5)/(7x + 3) = 6x + 1, \ R\ 2$

2 Problem 2

2.1 Addition

$(x^5 + x^3 + x^2 + x + 1) \ + \ (x^2 + x + 1)$
$= x^5 + x^3$

2.2 Subtraction

$(x^5 + x^3 + x^2 + x + 1) \ - \ (x^2 + x + 1)$
$= x^5 + x^3$

2.3 Multiplication

$(x^5 + x^3 + x^2 + x + 1) \ * \ (x^2 + x + 1)$

$$x^5 + x^3 + x^2 + x + 1 * x^2 = x^7 + x^5 + x^4 + x^3 + x^2$$
$$x^5 + x^3 + x^2 + x + 1 * x^2 = x^6 + x^4 + x^3 + x^2 + x$$
$$x^5 + x^3 + x^2 + x + 1 * 1 = x^5 + x^3 + x^2 + x + 1$$

$$
\begin{array}{llllllll}
x^7 & & + x^5 & + x^4 & + x^3 & + x^2 & & \\
& + x^6 & & + x^4 & + x^3 & + x^2 & + x & \\
& & + x^5 & & + x^3 & + x^2 & + x & + 1
\end{array}
$$

$= x^7 + x^6 + x^3 + x^2 + 1$

2.4 Division

$(x^5 + x^3 + x^2 + x + 1)\ /\ (x^2 + x + 1)$

$$
\begin{array}{lllllllll}
 & & x^3 & + x^2 & + \text{x} & + 1 & & \text{R x} \\
\cline{3-8}
x^2 + \text{x} + 1 &) & x^5 & & + x^3 & + x^2 & + \text{x} & + 1 \\
 & - & x^5 & + x^4 & + x^3 & & & \\
\cline{3-8}
 & & & x^4 & & + x^2 & + \text{x} & + 1 \\
 & & - & x^4 & + x^3 & + x^2 & & \\
\cline{4-8}
 & & & & x^3 & & + \text{x} & + 1 \\
 & & & - & x^3 & + x^2 & + \text{x} & \\
\cline{5-8}
 & & & & & x^2 & & + 1 \\
 & & & & - & x^2 & + \text{x} & + 1 \\
\cline{6-8}
 & & & & & & \text{x} &
\end{array}
$$

$= x^3 + x^2 + x + 1,\ R\ x$

3 Problem 3

Multiplicative inverse of 010=x with irreducible polynomial $x^3 + x + 1$:

$$
\begin{array}{llllll}
 & & x^2 & & +1 & +R\ 1 \\
\cline{2-5}
x &) & x^3 & +x & +1 & \\
 & & -x^3 & & & \\
\cline{3-5}
 & & & x & +1 & \\
 & & & -x & & \\
\cline{4-5}
 & & & & 1 &
\end{array}
$$

$(x)^{-1} = x^2 + 1$

Multiplicative inverse of 010=x with irreducible polynomial $x^3 + x^2 + 1$:

$$
\begin{array}{llllll}
 & & & x^2 & +x & +R\ 1 \\
\cline{2-5}
x &) & x^3 & +x^2 & +1 & \\
 & & -x^3 & & & \\
\cline{3-5}
 & & & x^2 & +1 & \\
 & & & -x^2 & & \\
\cline{4-5}
 & & & & 1 &
\end{array}
$$

$(x)^{-1} = x^2 + x$

4 Problem 4

Solved using program for Problem 6
With IP $x^3 + x + 1$

$$\begin{aligned}
(x^2+x+1)+(x^2+1) &= x \\
(x^2+x+1)-(x^2+1) &= x \\
(x^2+x+1)*(x^2+1) &= x^2+x \\
(x^2+x+1)/(x^2+1) &= (x^2+x+1)*(x^2+1)^{-1} \mod (x^3+x+1) \\
&= (x^2+x+1)*x \mod (x^3+x+1) \\
&= (x^3+x^2+x) \mod (x^3+x+1) \\
&= x^2+1
\end{aligned}$$

With IP $x^3 + x^2 + 1$

$$\begin{aligned}
(x^2+x+1)+(x^2+1) &= x \\
(x^2+x+1)-(x^2+1) &= x \\
(x^2+x+1)*(x^2+1) &= 1 \\
(x^2+x+1)/(x^2+1) &= (x^2+x+1)*(x^2+1)^{-1} \mod (x^3+x^2+1) \\
&= (x^2+x+1)*(x^2+x+1) \mod (x^3+x^2+1) \\
&= (x^4+x^2+1) \mod (x^3+x^2+1) \\
&= x
\end{aligned}$$

5 Problem 5

Solved with our program for Problem 6.

5.1 Binary Representations

$f(x) = 0xad = 1010\ 1101$
$g(x) = 0x0d = 0000\ 1101$

5.2 Multiplicative Inverses

MI of 0xad = 0xe7 = $x^7 + x^6 + x^5 + x^2 + x + 1$

MI of 0x0d = 0xe1 = $x^7 + x^6 + x^5 + 1$

6 Problem 6

See emailed code.