MATH 178 Homework #6

Tamir Enkhjargal

April 2019

FF

4.

Polynomials of Degree 3	Irreducible Form
$x^3 + 0x^2 + 0x + 0$	$x^2(x)$
$x^3 + 0x^2 + 0x + 1$	$(x^2 + x + 1)(x + 1)$
$x^3 + 0x^2 + x + 0$	$x(x^2 + 1)$
$x^3 + 0x^2 + x + 1$	Irreducible
$x^3 + x^2 + 0x + 0$	$x^2(x + 1)$
$x^3 + x^2 + 0x + 1$	Irreducible
$x^3 + x^2 + x + 0$	$x(x^2 + x + 1)$
$x^3 + x^2 + x + 1$	$(x^2 + 1)(x + 1)$

5.

Power of x^2	$\mod(x^3 + x + 1)$	Reduced Form
$(x^2)^1$	x^2	x^2
$(x^2)^2$	x^4	$x^2 + x$
$(x^2)^3$	x^6	$x^2 + 1$
$(x^2)^4$	x^8	x
$(x^2)^5$	x^{10}	$x + 1$
$(x^2)^6$	x^{12}	$x^2 + x + 1$
$(x^2)^7$	x^{14}	1

We see that x^2 is a generator in $\mathbb{F}_8^*$.

6.

(a)

$$x^3 + x + 1 \tag{1}$$
$$* \; x^3 + x^2 + 1 \tag{2}$$

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \tag{3}$$
$$x^6 = x^4 * x^2 = (x+1)x^2 = x^3 + x^2 \tag{4}$$
$$x^5 = x^4 * x = (x+1)x = x^2 + x \tag{5}$$
$$x^4 = x + 1 \tag{6}$$

$$x^2 + x \tag{7}$$

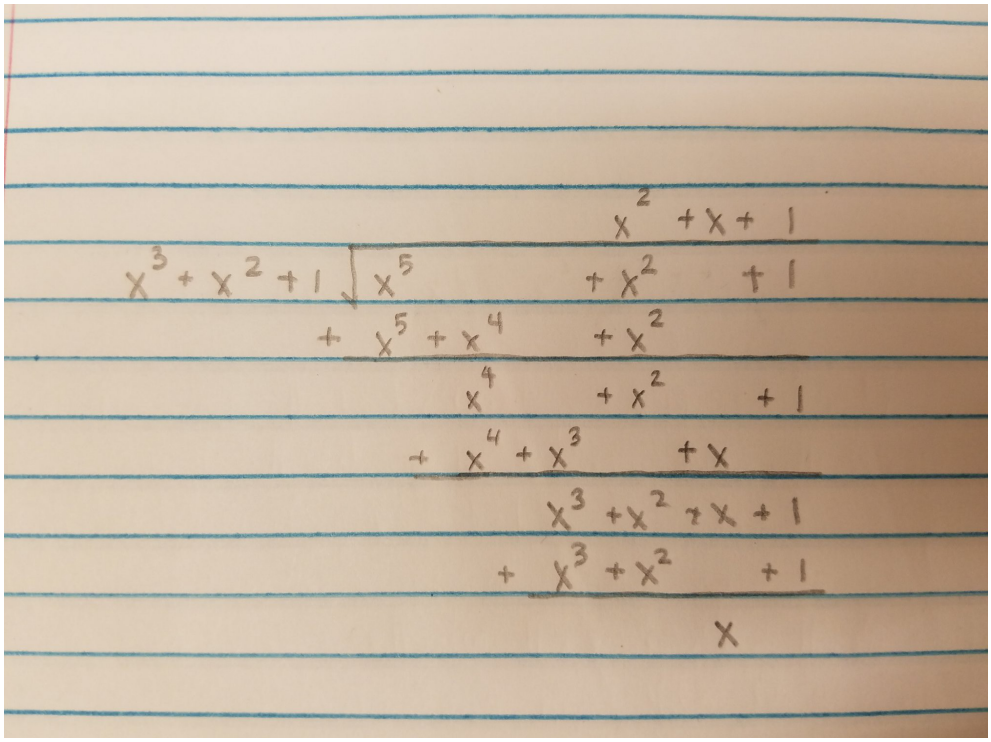
(b)

Power of x	Reduced mod$(x^4 + x + 1)$
x^1	x
x^2	x^2
x^3	x^3
x^4	$x + 1$
x^5	$x^2 + x$
x^6	$x^3 + x^2$
x^7	$x^3 + x + 1$
x^8	$x^2 + 1$
x^9	$x^3 + x$
x^{10}	$x^2 + x + 1$
x^{11}	$x^3 + x^2 + x$
x^{12}	$x^3 + x^2 + x + 1$
x^{13}	$x^3 + x^2 + 1$
x^{14}	$x^3 + 1$
x^{15}	1

(c) x^3 is not a generator of $\mathbb{F}_{16}^*$, because when x, which is a generator loops and repeats the pattern from x^{16} to x^{30} (and again x^{31} to x^{45}), the only numbers hit are the multiplies of 3, which will be $x^3, x^6, x^9, x^{12}, x^{15}$... The other elements of the set generating $\mathbb{F}_{16}^*$ never gets touched. One thing to note, is that the cardinality of $\mathbb{F}_{16}^*$ and the degree of x are not relatively prime, leading to this problem.

7.

In $\mathbb{F}_{32} = \mathbb{F}_2[x]/(x^5 + x^2 + 1)$, invert $x^3 + x^2 + 1$.



From the rest of the equation, we find that:

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

$$1 = (x^3 + x^2 + 1) + (x^2 + x)x \tag{1}$$
$$1 = (x^3 + x^2 + 1) + (x^2 + x)[(x^5 + x^2 + 1) + (x^2 + x + 1)(x^3 + x^2 + 1)] \tag{2}$$
$$1 = (x^3 + x^2 + 1) + (x^2 + x)(x^2 + x + 1)(x^3 + x^2 + 1) \tag{3}$$
$$1 = (x^3 + x^2 + 1) + (x^4 + x)(x^3 + x^2 + 1) \tag{4}$$
$$1 = (x^3 + x^2 + 1)(x^4 + x + 1) \tag{5}$$

$$(x^3 + x^2 + 1)(x^4 + x + 1) \equiv 1(\mathrm{mod}(x^5 + x^2 + 1)) \tag{1}$$

Therefore the inverse of $x^3 + x^2 + 1$ is $x^4 + x + 1$