Abstract Algebra Homework 11

Joe Loser

April 30, 2016

This problem set includes problems $3c, 4b, 24$, and an extra problem from section 17.4.

3) Use the division algorithm to find $q(x)$ and $r(x)$ such that $a(x) = q(x)b(x) + r(x)$ with $\deg r(x) < \deg b(x)$.

3c) $a(x) = 4x^5 - x^3 + x^2 + 4$ and $b(x) = x^3 - 2$ where $a(x), b(x) \in \mathbb{Z}_5[x]$.

Solution: Performing long division, we have

$$
\begin{array}{rl}
 & 4x^2 - 1 \\
\cline{2-2}
x^3 - 2 \big) & 4x^5 - x^3 \quad + x^2 + 4 \\
 & -4x^5 \qquad + 8x^2 \\
\cline{2-2}
 & -x^3 + 9x^2 + 4 \\
 & x^3 \qquad - 2 \\
\cline{2-2}
 & 9x^2 + 2
\end{array}
$$

Thus,

$$
\begin{aligned}
a(x) &= (4x^2 - 1) \cdot (x^3 - 2) + (9x^2 + 2) \\
&\equiv (4x^2 - 1) \cdot (x^3 - 2) + (4x^2 + 2).
\end{aligned}
$$

$\square$

4) Find the greatest common divisor of each of the following pairs $p(x)$ and $q(x)$ of polynomials. If $d(x) = \gcd(p(x), q(x))$, find two polynomials $a(x)$ and $b(x)$ such that $d(x) = a(x)p(x) + b(x)q(x)$.

4b) $p(x) = x^3 + x^2 - x + 1$ and $q(x) = x^3 + x - 1$ where $p(x), q(x) \in \mathbb{Z}_2[x]$.

Performing the first stage of long division, we have that

$$
\begin{array}{rl}
 & 1 \\
\cline{2-2}
x^3 + x^2 - x + 1 \big) & x^3 \qquad + x - 1 \\
 & -x^3 - x^2 \quad + x - 1 \\
\cline{2-2}
 & -x^2 + 2x - 2
\end{array}
$$

Note that in $\mathbb{Z}_2[x], -x^2 + 2x - 2 \equiv -x^2$. So

$$
x^3 + x - 1 = 1 \cdot (x^3 + x^2 - x + 1) + (-x^2). \tag{1}
$$

In the second stage of long division, we get

$$
\begin{array}{rl}
 & -x - 1 \\
\cline{2-2}
-x^2 \big) & x^3 + x^2 - x + 1 \\
 & -x^3 \\
\cline{2-2}
 & x^2 \\
 & -x^2 \\
\cline{2-2}
\end{array}
$$

So

$$x^3 + x^2 - x + 1 = (-x-1)\cdot(-x^2) + (-x+1). \tag{2}$$

In the third stage, we get

$$\begin{array}{rl} & x+1 \\ \cline{2-2} -x+1 \big) & -x^2 \\ & x^2 - x \\ \cline{2-2} & -x \\ & x-1 \\ \cline{2-2} & -1 \end{array}$$

So

$$-x^2 = (-x+1)\cdot(x+1) + (-1). \tag{3}$$

In the last stage of long division, we have

$$\begin{array}{rl} & x-1 \\ \cline{2-2} -1 \big) & -x+1 \\ & x \\ \cline{2-2} & 1 \\ & -1 \\ \cline{2-2} & 0 \end{array}$$

So

$$-x+1 = (-1)\cdot(x-1) + 0. \tag{4}$$

Thus $\gcd(p(x), q(x)) = -1$. Performing the back substitution, we have the following

finish back sub

$$\begin{aligned} -1 &= -x^2 - (x+1)(-x+1) \\ &= -x^2 - (x+1)\Big((x^3+x^2-x+1) - (-x-1)(-x^2)\Big) \\ &= (x^3+x-1) - (x^3+x^2-x+1) - (x+1)\Big[(x^3+x^2-x+1) - (-x-1)\Big((x^3+x-1) - (x^3+x^2-x+1)\Big)\Big] \end{aligned}$$

24) Show that $x^p - x$ has p distinct zeros in $\mathbb{Z}_p$ for any prime p. Conclude that

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

Proof: By Fermat's Little Theorem, for all $a \in \mathbb{Z}_p$ we have that $a^p = a$. So $a^p - a = 0$. Thus every $a \in \mathbb{Z}_p$ is a zero of the polynomial $x^p - x$. Note that the polynomial has degree p and p zeros in $\mathbb{Z}_p$. The numbers $0, 1, \cdots, p-1$ are the roots of the equation $x^p - x$, i.e. the p distinct roots. Hence it must split into p distinct linear factors in $\mathbb{Z}_p[x]$ as follows:

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

$\square$

E1) Construct a field with 8 elements.

Solution: Since $8 = 2^3$ we start with a field $\mathbb{Z}_2$ of characteristic 2 and look for an irreducible polynomial of degree 3 in $\mathbb{Z}_2[x]$. Such a polynomial is $p(x) = x^3 + x + 1$.

We will show that

$$K := \frac{\mathbb{Z}_2[x]}{< x^3 + x + 1 >}$$

is a field of 8 elements.

To see why $p(x)$ is irreducible in $\mathbb{Z}_2[x]$, since it of degree 3 or lower, we can look at all of the roots in $mathbbZ_2$. We have that $g(0) = 1$ and $g(1) = 3 \equiv 1$. So neither 0 or 1 are a root of $p(x)$. Hence we see that we $p(x)$ is irreducible over $\mathbb{Z}_2[x]$.

By