Basic Algebra 1
Solutions to Assignment 3

Bahare Mirza

November 8, 2012

(1)

$$\begin{array}{rr}
 & 3x^2 - 5x + 8 \\ \cline{2-2}
x^2+x+1 \big) & 3x^4 - 2x^3 + 6x^2 \quad - x + 2 \\
 & -3x^4 - 3x^3 - 3x^2 \qquad\qquad \\ \cline{2-2}
 & -5x^3 + 3x^2 \quad - x \quad\;\; \\
 & 5x^3 + 5x^2 + 5x \quad\;\; \\ \cline{2-2}
 & 8x^2 + 4x + 2 \\
 & -8x^2 - 8x - 8 \\ \cline{2-2}
 & -4x - 6
\end{array}$$

So $q(x) = 3x^2 - 5x + 8$ and $r(x) = -4x - 6$.

(2)

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

And $-2x \equiv 0$ modulo 2. So we get

$$\begin{aligned}
(x^5 - x + 1) &\equiv (x^2 + x + 1)(x^3 - x^2 + 1) \quad mod \quad 2 \\
&\equiv (x^2 + x + 1)(x^3 + x^2 + 1) \quad mod \quad 2
\end{aligned}$$

(3) First note that the function $f : \mathbb{Z}[x] \to \mathbb{Z}$ assigns to each polynomial its value at 0, i.e. $f(p) = a_0 = p(0)$.
Now let $p_1, p_2 \in \mathbb{Z}[x]$, be given by $p_1(x) = a_0 + a_1x + ... + a_nx^n$ and $p_2(x) = b_0 + b_1x + ... + b_mx^m$, then

$$\begin{aligned} f(p_1 + p_2) &= (p_1 + p_2)(0) \\ &= p_1(0) + p_2(0) \\ &= f(p_1) + f(p_2). \end{aligned}$$

Similarly,

$$\begin{aligned} f(p_1 p_2) &= (p_1 p_2)(0) \\ &= p_1(0)p_2(0) \\ &= f(p_1)f(p_2). \end{aligned}$$

(4) We proceed using Euclidean Algorithm; in the first step we get

$$\begin{array}{rrrrrr}
 & & & x^2 & +3x & -1 \\
\cline{2-6}
x^2+1 \big) & x^4 & +3x^3 & & -2x & +4 \\
 & -x^4 & & -x^2 & & \\
\cline{2-4}
 & & 3x^3 & -x^2 & -2x & \\
 & & -3x^3 & & -3x & \\
\cline{3-5}
 & & & -x^2 & -5x & +4 \\
 & & & x^2 & & +1 \\
\cline{4-6}
 & & & & -5x & +5
\end{array}$$

But $-5x + 5 \equiv 0$ modulo 5, so we have

$$x^4 + 3x^3 - 2x + 4 = (x^2 + 1)(x^2 + 3x - 1),$$

hence $x^4 + 3x^3 - 2x + 4$ is divisible by $x^2 + 1$ modulo 5 and so we have

$$gcd(x^4 + 3x^3 - 2x + 4, x^2 + 1) = x^2 + 1.$$

(5) First we make the following claim:

Claim A polynomial of degree 3 in $F[x]$ is irreducible over F if and only if it has no roots in F.

Proof of the Claim If $f \in F[x]$ has a root t in F, then $(x - t)|f(x)$. So we have $f(x) = (x - t)g(x)$, for some $g \in F[x]$, of degree 2. As neither $x - t$ nor $g(x)$ are unit or equal to $f(x)$ (not having degree 0 or 3,) this gives a decomposition of f. so if f has a root then it is reducible. Conversely, assume f is reducible, say $f = gh$ for some $g, h \in F[x]$ with $0 < deg(g), deg(h)$. Then as $3 = deg(f) = deg(g) + deg(h)$, one of g and h should have degree 1 (and the other should be of degree 2.) So without loss of generality we can assume that $deg(g) = 1$; Let $g = rx + s$. Then we have $t = -s/r$ is a root of g and hence a root of f. This proves that if f is reducible then it has a root, or equivalently if f does not have a root, then it is irreducible.

Now going back to our problem; a monic polynomial of degree 3 in $\mathbb{Z}/2\mathbb{Z}$ is of the form

$$f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \{0, 1\}$(a complete set of representatives mod 2.)

By the claim we just proved, f is reducible iff it has a root in $\mathbb{Z}/2\mathbb{Z}$ i.e. either $f(0) = 0$ or $f(1) = 0$. But $f(0) = c$ and $f(1) = 1 + a + b + c$. So f is reducible if and only if

$$c = 0$$

or

$$c = 1 \quad and \quad a + b \equiv 1 + a + b + 1 \equiv 0 \quad mod \quad 2.$$

Note that the condition $a + b \equiv 0 \pmod 2$ is equivalent to $a = b$.

We conclude that f is irreducible if and only if

$$c \neq 0 \quad and \quad a \neq b.$$

So the only irreducible polynomials of degree three in $\mathbb{Z}/2\mathbb{Z}$ are

$$\begin{aligned} &x^3 + x^2 + 1 \\ &x^3 + x + 1. \end{aligned}$$

(6) If $p = 4m + 1$, then by Wilson's theorem we have $(4m)! \equiv -1$, in other words $(4m)! + 1 \equiv 0$. So if we prove $a^2 \equiv (4m)!$ modulo p then by the above congruence relation, we have shown that a is a root of the polynomial $x^2 + 1$ mod p.

Note first that $4m + 1 \equiv 0$ modulo p which implies $2m + i \equiv -2m + (i - 1) \pmod p = -(2m - (i - 1))$. So we have the following congruences mod p

$$\begin{aligned} &(2m+1)...(2m+(2m-1))(2m+2m) \\ &\qquad \equiv (-1)^{2m}(2m)...(2m-(2m-2))(2m-(2m-1)) \\ &\qquad \equiv (2m)(2m-1)...(2)(1) \\ &\qquad = (2m)!. \end{aligned}$$

Which gives

$$\begin{aligned} (4m)! &= (2m)!(2m+1)...(2m+2m) \\ &\equiv (2m)!(2m)! \\ &= (2m)!^2, \end{aligned}$$

as desired.

Now assume $p = 4m + 3$; any element $a \in \mathbb{Z}/p\mathbb{Z}$ satisfies $a^{4m+2} = a^{p-1} \equiv 1$ modulo p. If in adition, a is a root of $x^2 + 1$, then we can substitute a^2 in the first relation, by -1 to get

$$\begin{aligned} 1 &= a^{4m+2} \\ &= (a^2)^{2m+1} \\ &= (-1)^{2m+1} \\ &= -1, \end{aligned}$$

which is a contradiction. This shows that $x^2 + 1$ does not have a root in $\mathbb{Z}/p\mathbb{Z}$ for such p.

(7) First we consider the case of $p = 2, 3$ separately; we have

$$\begin{aligned} &0^2 + 0 + 1 = 1 \\ &1^2 + 1 + 1 = 3 \equiv 1 \quad mod \quad 2 \end{aligned}$$

So, modulo 2, this polynomial has no roots. On the other hand, 1 is a root of $x^2 + x + 1$ modulo 3.

Now any prime bigger than 3 is either of the form 6m+1 or 6m+5. Indeed any number of the form $6m$, $6m + 2$, $6m + 3$ and $6m + 4$ is divisible by either 2 or 3 and hence is composite.

Now note that a is a root of $x^2 + x + 1$ if and only if a is a root of $x^3 - 1$ that is not equal to 1; in fact, $x^3 - 1 = (x - 1)(x^2 + x + 1)$.

So in the following, we look at the roots of $f(x) = x^3 - 1$.

First we consider the case $p = 6m + 5$; any element $a \in \mathbb{Z}/p\mathbb{Z}$ satisfies $a^{6m+4} = a^{p-1} \equiv 1$ modulo p. If a is also a root of f then we have $a^3 = 1$, and so

$$\begin{aligned} 1 &\equiv a^{6m+4} \\ &\equiv (a^3)^{2m+1} a \\ &\equiv (1)^{2m+1} a \\ &\equiv a \end{aligned}$$

So the only root of f mosulo p is 1.

But if $p = 6m+1$, again any $a \in \mathbb{Z}/p\mathbb{Z}$ satisifies $a^{p-1} = a^{6m} = 1$. This shows that for any $a \in \mathbb{Z}/p\mathbb{Z}, a^{2m}$ is a root of f. So we only need to check whether we can find $a \in \mathbb{Z}/p\mathbb{Z}$ such that $a^{2m} \neq 1$. But the polynomial $x^{2m} - 1$ is a polynomial of degree $2m$ and hence has at most $2m$ roots over the field $\mathbb{Z}/p\mathbb{Z}$. Now if we take $a \in \mathbb{Z}/p\mathbb{Z}$ to be any element other than these $2m$ roots then $a^{2m} \neq 1$ and is a root of f. This shows that $x^2 + x + 1$ has a root modulo any prime of the form $6m + 1$.

Below we list all the primes modulo which $x^2 + x + 1$ has a root

$$\{3, 7, 13, 19, 31, 37, 43\}.$$

(8) We are looking for a polynomial of the form $f(x) = x^2 + Ax + B \in \mathbb{Z}/6\mathbb{Z}$ with four roots. We can do that by finding two different factorizations of f into linear factors

$$f(x) = (x - a)(x - b) = (x - c)(x - d).$$

But to have such factorizations we should have

$$x^2 - (a + b)x + ab = (x - a)(x - b) = (x - c)(x - d) = x^2 - (c + d)x + cd.$$

In other words, we want $a, b, c, d \in \mathbb{Z}/6\mathbb{Z}$ such that

$$a + b \equiv c + d \quad and \quad ab \equiv cd \quad mod \quad 6.$$

For example we can take $a = 2, b = 3, c = 0, d = -1 \equiv 5$, then $f(x) = (x - 2)(x - 3) = x^2 - 5x + 6 \equiv x^2 + x = x(x + 1)$.

Finally, his does not contradict the theorem mentioned, because the theorem is about polynomials in $F[x]$ for F a field. But since 6 is not a prime, $\mathbb{Z}/6\mathbb{Z}$ has zero divisors and is not a field.

(9) a. We use the Euclidean algorithm

$$\begin{aligned} x^4 - x^3 - x^2 + 1 &= \big(x^3 - 1\big) \cdot \big(x - 1\big) + \big(-x^2 + x\big). \\ x^3 - 1 &= \big(-x^2 + x\big) \cdot \big(-x - 1\big) + \big(x - 1\big) \\ -x^2 + x &= \big(x - 1\big) \cdot -x + 0 \end{aligned}$$

So we have

$$gcd(x^4 - x^3 - x^2 + 1, x^3 - 1) = x - 1.$$

And

$$\begin{aligned} x - 1 &= (x^3 - 1) + (x + 1)(-x^2 + x) \\ &= (x^3 - 1) + (x + 1)[(x^4 - x^3 - x^2 + 1) - (x - 1)(x^3 - 1)] \\ &= (x^3 - 1)(1 - (x^2 - 1)) + (x + 1)(x^4 - x^3 - x^2 + 1) \\ &= (x^3 - 1)(2 - x^2) + (x + 1)(x^4 - x^3 - x^2 + 1) \end{aligned}$$

c.

$$\begin{aligned} x^4 + 3x^3 + 2x + 4 &= (x^2 - 1)(x_2 + 3x + 1) + (5x + 5) \\ &\equiv (x^2 - 1)(x_2 + 3x + 1) \quad mod \quad 5. \end{aligned}$$

So $x^4 + 3x^3 + 2x + 4$ is divisible by $x^2 - 1$, and hence

$$gcd(x^4 + 3x^3 + 2x + 4, x^2 - 1) = x^2 - 1.$$

We have

$$x^2 - 1 = 0(x^4 + 3x^3 + 2x + 4) + 1(x^2 - 1).$$

e.

$$x^3 - \imath x^2 + 4x - 4\imath = (x^2 + 1)(x - \imath) + 3(x - \imath)$$
$$x^2 + 1 = (3x - 3\imath)(x/3 + \imath/3)$$

So

$$gcd(x^3 - \imath x^2 + 4x - 4\imath, x^2 + 1) = 3(x - \imath),$$

and

$$3(x - \imath) = (x^3 - \imath x^2 + 4x - 4\imath) - (x^2 + 1)(x - \imath).$$

f.

$$\begin{aligned} x^4 + x + 1 &= (x^2 + x + 1)(x^2 - x) + 2x + 1 \\ &\equiv (x^2 + x + 1)(x^2 - x) + 1 \quad mod \quad 2 \end{aligned}$$

So $x^4 + x + 1$ and $x^2 + x + 1$ are coprime and we have

$$gcd(x^4 + x^2 + 1, x^2 + x + 1) = 1.$$

Further

$$1 \equiv (x^4 + x + 1) - (x^2 + x + 1)(x^2 - x) \quad mod \quad 2.$$

(10) a. we know that for any field F and any polynomial $f(x) \in F[x]$ if $f(a) = 0$ for some $a \in F$ then $f(x) = (x - a)g(x)$ for some $g(x) \in F[x]$. In particular take $f(x) = x^p - x$ and $F = \mathbb{Z}/p\mathbb{Z}$. Note that by Fermat's Little Theorem, for every element $a \in \mathbb{Z}/p\mathbb{Z}$, we have $f(a) = 0$. Take $a = 0$ to get $g_0 \in F[x]$ such that

$$f(x) = (x - 0)g_0(x).$$

Now since $f(1) = 0$ and $(x - 0)(1) = 1 \neq 0$ we deduce that $g_0(1) = 0$, and so we have

$$g_0(x) = (x - 1)g_1(x),$$

and

$$f(x) = x(x - 1)g_1(x).$$

Proceeding inductively, if for $0 \leq n \leq p - 2$ we have $g_n(x) \in \mathbb{Z}/p\mathbb{Z}$ such that

$$f(x) = x(x - 1)...(x - n)g_n(x),$$

since $n+1$ is a root of f but not a root of $x(x-1)...(x-n)$, we deduce that $n+1$ is a root of g_n and hence $g_n(x) = (x - (n + 1))g_{n+1}(x)$, for some polynomial g_{n+1} over F. Continuing in this manner, we get

$$f(x) = x(x - 1)...(x - (p - 1))g_{p-1}(x).$$

But g_{p-1} has degree 0 and both f and $x(x-1)...(x-(p-1))$ are monic polynomials so $g_{p-1}=1$. This gives the factorization

$$x^p - x = x(x-1)...(x-(p-1)),$$

of f into $p-1$ linear factors.

b. $a \in F$ is a root of g if and only if $(x-a)$ divides g. But we know that $(x-a)$ divides f anyway! So a is in fact a root if and only if $(x-a)$ divides $gcd(f,g)$.

Now if $a, b \in F$ are different roots, then $(x-a)$ and $(x-b)$ are relatively prime, and so $(x-a)|g(x)$ and $(x-b)|g(x)$ implies $(x-a)(x-b)|g(x)$ and so again $(x-a)(x-b)|gcd(g(x), f(x))$.

This implies that if $a_1, ...a_d$ are distinct roots of g then

$$(x-a_1)...(x-a_d)|gcd(g(x), f(x)).$$

Conversely, if $x-a$ divides $gcd(g,f)$ it obviously divides g and so a is a root of g and so is included among $a_1, ...a_d$. Note also that since $gcd(g(x), f(x))|f(x)$ and f is factorizable into linear facors by (a), $gcd(g(x), f(x))$ is also factorizable to linear factors, sp by what we have seen it is factorizable to product of $(x-a)$'s where a is a root. So we have

$$gcd(g(x), f(x)) = (x-a_1)...(x-a_d).$$

c.The solution to this part of the question was discussed in detail in class, and so is not included here.