Brandon Chen
MATH 412
HW1

1 For u to be a unit in a ring R, it means that u has a multiplicative inverse in the ring.

2 Describe all of the units

a) $\mathbb{Z}$: $1, -1$

b) $\mathbb{Z}_p$, p prime integer: All nonzero elements in the ring

c) $\mathbb{Z}_9$: all elements in the ring relatively prime to 9: 2, 4, 5, 7, 8

d) $\mathbb{Z}[i]$: 1, -1, i, -i

e) $\mathbb{Q}$: all nonzero elements in the ring

f) $\mathbb{Q}[x]$: all polynomials of degree 0

g) $\mathbb{Z}_2[x]$ 1

h) $\mathbb{Z}_5[x]$ 1, 2, 3, 4

3 a) A polynomial in $\mathbb{F}$ is irreducible when there exists only a nontrivial factorization. That is, it cannot be written as the product of two polynomials of strictly lower degree.

b) There are always irreducible polynomials in $\mathbb{F}$ because constants and degree 1 polynomials are always irreducible.

4 a) Example irreducible degree 2 in $\mathbb{R}[X] : (x^2 + 1)$

b) Example reducible degree 2 in $\mathbb{R}[x] : (x^2)$

c) There is no irreducible of degree 3 in $\mathbb{R}$

We know that a polynomial of degree 3 in $\mathbb{R}$ is continous, so if we take x large enough positive, and x to be a large negative, one will be positive and the other negative.

We know by the intermediate value theorem that since it is continous, and 0 is in between both values, then there will be a value of x such that we get 0.

Then there exists a value of x that is a root, call it γ. So by thm 9.7, $(x - \gamma)$ divides the polynomial.

So the polynomial can be factored as $g(x)(x - \gamma)$, which are two polynomials of degree 2 and 1 respectively.

So a polynomial of degree 3 in $\mathbb{R}$ is always reducible.

5 a) For a polynomial of degree N in $\mathbb{Z}_p[x]$, the coefficient on x^N must be nonzero, so it has (p-1) possible values. For all other terms $x^n, 0 \leq n < N$, there are p possible values. There are N many of these terms.

So for a polynomials of degree N in the ring, there are $(p-1)(p)^N$ polynomials.

For polynomials of degree $N - 1$, there are $(p-1)(p)^{N-1}$ polynomials.

So for polynomaisl of degree $N - k, k \leq N$, there are $(p-1)(p)^{N-k}$ polynomials

Finally, there is the polynomial 0. There is only one of this.

So the total number of polynomials in the ring with degree less than or equal to N is the sum of $(p-1)(p)^N + (p-1)(p)^{N-1} + ...(p-1) + 1$

For $p = 2, N = 5$, this is $2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 + 1 = 64$

b) We know by part a) that there is a finite number of polynomials of degree less than or equal to any N in the ring.

So there are finitely many irreducible polynomials of degree less than or equal to N

But we know by thm 9.4 that there are infinitely many irreducible polynomials in the ring.

So there must be infinitely many irreducible polynomials of degree greater than any N.

6 $a(x) = x^2 + x + 1, b(x) = x^4 + x^2 + 1$, find $q(x), r(x)$ so that $b(x) = a(x)q(x) + r(x), q(x), r(x) \in \mathbb{Q}[x], deg[r(x)] < deg[a(x)]$

8 Determine all irreducibel polynomials of degree 4 in $\mathbb{Z}_2[x]$

For the polynomial of degree 4 to be irreducible, it must be in the form $ax^4 + bx^3 + cx^2 + dx + e$, with $a = 1, e = 1$, otherwise it either isnt degree 4, or can have an x factored out of each term.

So candidates for irreducible polynomials in the ring of degree 4 are:

$x^4 + 0x^3 + 0x^2 + 0x^1 + 1$

$x^4 + 0x^3 + 0x^2 + 1x^1 + 1$

$x^4 + 0x^3 + 1x^2 + 0x^1 + 1$

$x^4 + 0x^3 + 1x^2 + 1x^1 + 1$

$x^4 + 1x^3 + 0x^2 + 0x^1 + 1$

$x^4 + 1x^3 + 0x^2 + 1x^1 + 1$

$x^4 + 1x^3 + 1x^2 + 0x^1 + 1$

$x^4 + 1x^3 + 1x^2 + 1x^1 + 1$

Next, if it is irreducible, it must have no zeros in the ring. Plug in x = 0 and x = 1 for each to see if it has any zeros.

Our candidates are now

$x^4 + 0x^3 + 0x^2 + 1x^1 + 1$

$x^4 + 0x^3 + 1x^2 + 0x^1 + 1$, reduces to $(x^2 - x + 1)(x^2 + x + 1)$

$x^4 + 1x^3 + 0x^2 + 0x^1 + 1$

$x^4 + 1x^3 + 1x^2 + 1x^1 + 1$

So the irreducible polynomials of degree 4 in the ring are

$x^4 + 1x^1 + 1$

$x^4 + 1x^3 + 1$

$x^4 + 1x^3 + 1x^2 + 1x^1 + 1$