1 Consider the congruence ring $\mathbb{Q}[x]_{x^5-2}$

a) Explain why this is a field by describing the theorems you would apply and why their hypotheses are satisfied

We know that $x^5 - 2$ is irreducible in $\mathbb{Q}[x]$, since it is of the form $x^n - p$ for prime $p = 2$, arbitrary $n = 5$

We also know by Theorem 14.11 that if F is a field, and that $m(x)$ is a polynomial of positive degree in $F[x]$, the ring $F[x]_{m(x)}$ is a field if and only if $m(x)$ is irreducible.

So $\mathbb{Q}[x]_{x^5-2}$ must be a field.

Further, by theorem 14.12, it is a field extension

b) What is the multiplicative inverse of $x + 1$

We know that $f(x) \equiv g(x) mod x^5 - 2$ is the same as saying

$x^5 - 2 | f(x) - g(x)$, which is $(x^5 - 2)m(x) = f(x) - g(x)$

So find $x^5 - 2 = (x + 1)q(x) + r(x)$

Try to divide $\frac{x^5-2}{x+1}$ to get remainder

$x + 1\overline{)x^5 - 2} \rightarrow (x + 1)(x^4 - x^3 + x^2 - x + 1) - 3$

So $(x^5 - 2)(\frac{1}{3}) = (x + 1)(x^4 - x^3 + x^2 - x + 1) - 1$

So $gcd(x + 1, x^5 - 2) = 1$, and $(x + 1)[\frac{1}{3}(x^4 - x^3 + x^2 - x + 1)] \equiv 1 (mod x^5 - 2)$

Then the multiplicative inverse is $\frac{1}{3}(x^4 - x^3 + x^2 - x + 1)$

c) If we change the coefficient field to $\mathbb{R}$, is $\mathbb{R}[x]_{x^5-2}$ a field? Explain

$\mathbb{R}[x]$ is a field.

Again, using theorem 14.11, $\mathbb{R}[x]_{x^5-2}$ is a field if and only if $m(x) = x^5 - 2$ is irreducible in $\mathbb{R}[x]$

But we know by theorem 10.5 that all irreducibles in $\mathbb{R}[x]$ are of degree 1 or 2, so $x^5 - 2$ is degree 5, must not be irreducible.

So $\mathbb{R}[x]_{x^5-2}$ must not be a field.

d) If we change the coefficient field to $\mathbb{F}_3$, is $\mathbb{F}_3[x]_{x^5-2}$ a field? Explain

$\mathbb{F}_3$ is a field.

So by theorem 14.11, $\mathbb{F}_3[x]_{x^5-2}$ is a field iff $m(x) = x^5 - 2$ is irreducible in $\mathbb{F}_3[x]$

So we need to check if $x^5 - 2$ is irreducible.

If reducible, factors as one of $[1, 4], [2, 3]$

First, check if factors as $[1, 4]$, that is, has degree one factor. This corresponds to a root.

So check for roots in $\mathbb{F}_3$. These are $0, 1, 2$

$x = 0 : 1, x = 1 : 1, x = 2 : 30 = 0$

So it does have a root, $x = 2$, which corresponds to a degree one factor

So $x^5 - 2$ is reducible in $\mathbb{F}_3[x]$

So $\mathbb{F}_3[x]_{x^5-2}$ is not a field.

2 Consider the polynomial $x^2 + 3x + 1$. In each of the rings below, explain either why it is irreducible in that ring, or factor as a product of irreducible polynomials

a) $\mathbb{Q}[x]$

Reduce $[f(x)]$ in $\mathbb{F}_2[x]$

This is $[f(x)] = x^2 + x + 1$

Which is irreducible in $\mathbb{F}_2[x]$

But we know that if it is irreducible in reduced, then it is irreducible in $\mathbb{Z}[x]$, and irreducible in $\mathbb{Q}[x]$

So $x^2 + 3x + 1$ is irreducible

b) $\mathbb{R}[x]$

Use quadratic formula: $\frac{-3 \pm \sqrt{3^2 - 4*1*1}}{2*1}$

$\frac{-3}{2} \pm \frac{\sqrt{5}}{2}$

So it has roots $\frac{-3}{2} \pm \frac{\sqrt{5}}{2}$

Which correspond to degree one factors

$(x - [-1.5 + 0.5\sqrt{5}])(x - [-1.5 - 0.5\sqrt{5}]) = x^2 + 3x + 1$

c) $\mathbb{F}_{11}[x]$

Brute force guess and check:

Brute force ideas: We know that it should be +1 after modulo, these candidates are 12, 23, 34, 45, 56, 67, 78, 89, 100, 11

We know it has two factors for candidates, these factors, a,b must be such that $a + b$ modulo 11 is 3, and a, b must be in $\{0, 1, 2, ...10\}$

For 45, it has factors $5, 9$

$(x + 5)(x + 9) = x^2 + 14x + 45$

In $\mathbb{F}_{11}[x]$, this is $x^2 + 3x + 1$

So it does reduce, to factors $(x + 5)(x + 9)$

Second brute force idea: Finite number of elements

We know that if it does reduce, it has degree 1 factor that corresponds to roots

These are $\{0, 1, 2...10\}$

So plug in these values for x to see if it equals 0

It equals 0 for $x = 6$ and $x = 2$

So roots are $(x - 6)(x - 2)$

Which are $(x + 5)(x + 9)$ in $\mathbb{F}_{11}[x]$

3 In this problem, we will consider polynomials in $\mathbb{F}_3[x]$

a) Prove that the polynomial $x^3 - x - 1$ has no roots in $\mathbb{F}_3$. Using this, explain why $x^3 - x - 1$ is irreducible in $\mathbb{F}_3[x]$

If $x^3 - x - 1$ has roots in $\mathbb{F}_3$, then if we plug in $0, 1, 2$ for x, we get 0

For $x = 0, 2, x = 1, 2, x = 2, 2$

Then it has no roots in the ring

But we know that if it does factor nontrivially, it must be of polynomials $g(x), h(x)$ of strictly lower degree

These must be 1 and 2. But we know that $f(x)$ has no roots, which means it has no degree 1 factors in the ring.

So $f(x)$ must be irreducible

b) Construct a ring K that contains $\mathbb{F}_3$, has an element γ satisfying $\gamma^3 = \gamma + 1$, and has exactly 27 elements. Describe explicitly what the elements of K are, give a formula for the product of any two elements of K, and explain why K has 27 elements.

An element in K is of the form $a + b\gamma + c\gamma^2$ for $a, b, c \in \mathbb{F}_3$

The product $(a + b\gamma + c\gamma^2)(e + f\gamma + g\gamma^2)$

c) Using Bezout's theorem, prove that K is a field: that is, prove that each non-zero element of K has a multiplicative inverse in K

4 a) Let p be a prime integer. When (if ever) is $\mathbb{Z}_{p^2}$ (the integers modulo p^2 a field of order p^2

b) Find the gcd in $\mathbb{R}[x]$ of $x^3 - x - x - 2$ and $x^2 - x - 2$

Find gcd. Divide and find divisor for zero remainder

$x^2 - x - 2\overline{)x^3 - x^2 - x - 2} \rightarrow x^3 - x^2 - x - 2 = (x^2 - x - 2)(x) + (x - 2)$

$x - 2\overline{)x^2 - x - 2} \rightarrow x^2 - x - 2 = (x - 2)(x + 1) + 0$

So $(x - 2)$ is the gcd

c) How many elements in $\mathbb{F}_{41}$ are squares? Explain a systematic way to describe them all

d) Does $\mathbb{C}[x]$ have an irreducible polynomial of degree 100? Explain

No, because we know that all irreducibles in $\mathbb{C}[x]$ of positive degree are of degree 1

e) Does $\mathbb{R}[x]$ have an irreducible polynomial of degree 100? Explain

No, because we know that all irreducibles in $\mathbb{R}[x]$ of positive degree are of degree 1 or 2.

f) Does $\mathbb{Q}[x]$ have an irreducible polynomial of degree 100? Explain

No, since for $x^n - p$, with prime p, it is irreducible in $\mathbb{Q}[x]$

Example, $x^{100} - p$

g) Does $\mathbb{F}_{19}[x]$ have an irreducible polynomial of degree 100? Explain

Yes, because for prime p, 19 is prime, then in $\mathbb{F}_p[x]$, we know by a previous theorem that there are infinitely many irreducibles of arbitrary size

But we also know that there are finitely many number of elements, and finitely many number of irreducible elements under degree 100 from $\mathbb{F}_{19}[x]$

Then there must exist other irreducible polynomials of higher degree.

5 Let p be a prime number and suppose that a, b are integers such that $a^2 + b^2 = p$

a) Prove that the Gaussian integer $a + bi$ is irreducible in $\mathbb{Z}[i]$

This is theorem 16.1 and is proven in exercise 16.1

p prime

$r = a + bi$ such that $N(r) = p$

By contradiction. Assume r is reducible.

Let $r = st$ be a nontrivil factorization for $s, t \in \mathbb{Z}[i]$

Then $N(r) = N(s * t) = N(s)N(t) = p$

But we know p is prime, not irreducible

Without loss of generality, assume $N(s) = 1$

Then $s * t$ is a trivial factorization

But this contradicts that $r = s * t$ is a nontrivial factorization

Then r must be irreducible

b) Factor p in $\mathbb{Z}[i]$ as a product of irreducible Gaussian integers, and explain why the factors in your factorization are irreducible

$p = a^2 + b^2$

$p = (a + bi)(a - bi) = a^2 + b^2$

Irreducible because of the reasoning in part a)

In fact, there are 8 Gaussian integers (a, b) that satisfy $a^2 + b^2 = p$

$(\pm a, \pm b)$, and $(\pm b, \pm a)$

Take any one of these, and its conjugate multiplies to produce p

c) Let p be the prime number 1021, which happens to satisfy the equation $11^2 + 30^2 = 1021$. Describe 8 pairs of integers (a, b) that satisfy $a^2 + b^2 = 1021$

We know that these 8 pairs are $(\pm a, \pm b)$

and $(\pm b, \pm a)$

Then these are, for $a = 11, b = 30$

$(11, 30), (-11, 30), (11, -30), (-11, -30)$

$(30, 11), (30, -11), (-30, 11), (-30, -11)$

d) State what the unique factorization theorem for $\mathbb{Z}[i]$ says about the possible factorizations of 1021 for $\mathbb{Z}[i]$ as a product of irreducible Gaussian integers. Using this,

explain why there are exactly eight solutions (x, y) in the integers to the equation $x^2 + y^=1021$

The unqiue factorization theorem for $\mathbb{Z}[i]$ is theorem 15.20

Theorem 15.20: Suppose that $p_1p_2...p_m$ and $q_1q_2..q_n$ are two irreducible factorizations of a nonzero nonunit Gaussian integer a of R. Then $m = n$, and the order of the factors in the second factorization can be hcanged so that for each index j the elements p_j and q_2 either equal each other or differ from each other by multiplication by $-1, i, -i$

So for $11^2 + 30^2 = 1021$

So by unique factorization, we know that for prime $p = a^2 + b^2$

The solutions differ from $(a + bi)(a - bi)$ by multiplication $-1, i, -i$

So solutions are $(\pm a + \pm bi)$, or $(\pm b + \pm ai)$multiplied by its conjugate.

e) Now let p be the prime number 607. How many integer solutions are there to the equation $x^2 + y^2 = 607$

We know by theorem 16.16 that since $p \equiv 3(mod4)$

Then $x^2 + y^2 = p$ has no integer solutions

And p is irreducible in $\mathbb{Z}[i]$

6 Using the grid below, circle all of the irreducible Gaussian integers.

7 Form the congruence rings $R = \mathbb{F}_3[x]_{x^2+2x+2}$ and $S = F_3[x]_{x^2+x+1}$

a) Find the number of elements in each ring.

b) Are either of these rings fields? Explain

By theorem 14.11 we know $F[x]_{m(x)}$ is a field iff $m(x)$ is irreducible in $F[x]$

For $F[x] = \mathbb{F}_3, m(x) = x^2 + 2x + 2$

Check if it is reducible. That is, if it has degree 1 factors, which corresponds to roots

$x = 0 : 2, x = 1 : 2, x = 2 : 1$

So it has no degree 1 factors. So it is irreducible

So $\mathbb{F}_3[x]_{x^2+2x+2}$ is a field.

For $F[x] = \mathbb{F}_3, m(x) = x^2 + x + 1$

$x = 0 : 1, x = 1 : 0$

So $m(x) = x^2 + x + 1$ does have a root, which is a degree one factor

So $x^2 + x + 1$ is not irreducible

So $\mathbb{F}_3[x]_{x^2+x+1}$ is not a field.

c) Find the multiplicative inverse of $2x + 2$ in each of these rings

d) Calculate $(x + 2)(2x + 1)$ in each ring

$(x + 2)(2x + 1) = 2x^2 + x + 4x + 2$

$= 2x^2 + 5x + 2$

$= 2x^2 + 2x + 2$

For $m(x) = x^2 + 2x + 2$,

$x^2 + 2x + 2\overline{)2x^2 + 2x + 2} \rightarrow 2x^2 + 2x + 2 = (x^2 + 2x + 2)(2) + (-2x - 2)$

$2x^2 + 2x + 2 = (x^2 + 2x + 2)(2) + (x + 1)$

So $2x^2 + 2x + 2 \equiv x + 1(mod x^2 + 2x + 2)$

For $m(x) = x^2 + x + 1$,

$x^2 + x + 1\overline{)2x^2 + 2x + 2} \rightarrow 2x^2 + 2x + 2 = (x^2 + x + 1)(2) + 0$

So $2x^2 + 2x + 2 \equiv 0(mod x^2 + x + 1)$

8 Explain what it means for an element of $\mathbb{C}$ to be algebraic over $\mathbb{Q}$. Then prove from scratch that the numbers $\sqrt{3}$ and $\frac{1}{2} + i$ are both algebraic over $\mathbb{Q}$

If an element is algebraic over $\mathbb{Q}$, then that element is a root in $\mathbb{Q}[x]$

$\sqrt{3}$ is algebraic over $\mathbb{Q}[x]$

$x^2 + 3 \in \mathbb{Q}[x]$ irreducible, but reducible to $(x + \sqrt{3})(x - \sqrt{3}) \in \mathbb{C}[x]$

So $\sqrt{3}$ is a root, and is algebraic

$\frac{1}{2} + i$ is algebraic over $\mathbb{Q}[x]$

let $a = 0.5 + i$

Then $a - 0.5 = i$

Then $(a - 0.5)^2 = i^2 = -1$

Then $a^2 - a + 0.25 = -1$

Then $a^2 - a + 1.25 = 0$

Then $x^2 - x + 1.25 = 0 \in \mathbb{Q}[x]$, with root $0.5 + i$

9 For this quesiton, we work in the finite field $\mathbb{F}_3$. You may assume that 2 is a primitive 12th root of unity.

a) List all nonzero elements of $\mathbb{F}_{13}$ that are squares. List elements as numbers in the set $\{0, 1, ...12\}$

b) Determine if the polynomial $x^2 + x + 6$ is irreducible in $\mathbb{F}_{13}[x]$. If so, explain. If not, full factor as a product of irreducibles.

c) Determine whether the polynomial $x^2 + x + 8$ is irreducible in $\mathbb{F}_{13}[x]$. If so explain. If not, fully factor as a product of irreducibles.

10 In this quesiton, we work in the Gaussian integers $\mathbb{Z}[i]$ with the norm $N(a+bi) = a^2+b^2$

a) Let r be an irreducible in $\mathbb{Z}[i]$. Prove that $N(r) = p$ or $N(r) = p^2$ for some prime integer p (I want you to be able to explain the steps in exercise 16.3

b) Give an example of an irreducible r of each of the types in part a

$N(1+i) = 1+1 = 2$

$N(4+3i) = 16+9 = 25 = 5^2$

c) Factor $x = 30$ as a product of irreducible Gaussian integers

$x = 30 = 5 * 3 * 2 = (2+i)(2-i)(3)(1+i)(1-i)$

d) In the ring of Gaussian integers, let $b = 3+2i, a = 1+i$. Find $q, r \in \mathbb{Z}[i]$ so that $b = aq + r$ and $N(r) < N(a)$. Justify your answer. Are your answers for q, r unique? Explain

e) How many Gaussian integers have the norm $1, 2, 3, 11, 13$?

$N(r) = 1 : r \in \{1, -1, i, -i\}$

$N(r) = 2 : r \in \{1+i, 1-i, -1+i, -1-i\}$

$N(r) = 3 :$ None

$N(r) = 11 : r$ in the form $(\pm a, \pm bi)$ or $(\pm b, \pm ai)$ for $a, b \in \{1, 3\}$

$N(r) = 13 : r$ in the form $(\pm a, \pm bi)$ or $(\pm b, \pm ai)$ for $a, b \in \{2, 3\}$

11 If $b = 1+8i, a = 2-4i$, find Gaussian integers q, r so that $b = aq + r, N(r) \leq \frac{1}{2}N(a)$. There are two correct answers.

$b = 1+8i, N(b) = 65$

$a = 2-4i, N(a) = 20$

Need $b = aq + r$, for $N(r) \leq \frac{1}{2}N(a) = 10$

So find $\frac{1+8}{2-4i}$

Multiply top and bottom by conjugate of $2-4i$ to clear denominator of i

$\frac{(1+8i)(2+4i)}{(2-4i)(2+4i)} = \frac{(1+8i)(2-4i)}{20}$

$= \frac{-30+20i}{20} = -1.5 + i$

Since $1.5 \notin \mathbb{Z}$, we need to round for approximation

Since it is exactly 0.5, we can either round up or down

These are $r = -1+i, N(r) = 2$

and $r = -2+i, N(r) = 5$

12 Consider the polynomial $f(x) = x^2 + bx + 1$ in $\mathbb{F}_{11}[x]$, where $b \in \mathbb{F}_{11}$ is a fixed constant. Determine all b (if any) so that the qudratic is reducible. In the reducible cases, factor the quadratic.

13 Is $f(x) = x^2 + 1$ irreducible in $\mathbb{F}_{101}[x]$? Explain

We know by theorem 16.15 that for $p \equiv 3 \bmod 4$, then x^2+1 factors nontrivially in $\mathbb{F}_p$

We also know by theorem 16.16 that for $p \equiv 1$ most 4, then x^2+1 is irreducible in $\mathbb{F}_p$

Then for $101 \equiv 1 \bmod 4$, x^2+1 is irreducible in $\mathbb{F}_{101}[x]$

14 Prove from scratch that the elements of third smallest norm in $\mathbb{Z}[i]$ are irreducible and list all such elements.

15 List all elements of the polynomial congruence ring $\mathbb{F}_2[x]_{x^2+x+1}$. Obtain a formula for the congruence class $[x+1]^n$ for a positive integer n.