Math 402 Homework 6

Alexandre Lipson

February 26, 2025

Problem 1. Show that $\sqrt{p}$ is irrational for all positive prime integers p.

Proof. We will consider all $p > 1$ because $1 = \sqrt{1}$ is a rational positive prime integer.

Consider the polynomial $x^2 - p$ which has roots $\pm\sqrt{p}$.

By the Rational Root Theorem, if $x^2 - p$ has a rational root q, then it must be $\pm p$ or ± 1.

But, $(\pm p)^2 - p \neq 0$ and $(\pm 1)^2 - p \neq 0$ for all $p > 1$.

So, $x^2 - p$ has no rational roots, hence its roots $\pm\sqrt{p}$ must not be rational. □

Problem 2. Show that there are infinitely many integers k such that $x^9 + 12x^5 - 21x + k$ is irreducible in $\mathbb{Q}[x]$.

Proof. We wish to satisfy Einstein's Criterion in order to show that the given polynomial is irreducible in $\mathbb{Q}[x]$.

We have that the leading coefficient of this polynomial is 1, which is coprime to all primes p.

Then, we must have $p \mid 12$, $p \mid 21$, and $p \mid k$. Since $(12, 21) = 3$, then $p = 3$.

We need $p \mid k$ but not $p^2 \mid k$. So, we must have $k = 3^{2n+1}$, $\forall n \in \mathbb{Z}_{\geq 0}$. This gives $3 \mid 3^{2n+1}$ but not $3^2 \mid 3^{2n+1}$ as desired.

Thus, f is irreducible over $\mathbb{Q}[x]$ by Einstein's Criterion, and there are infinitely many such k of the form $k = 3^{2n+1}$, $\forall n \in \mathbb{Z}_{\geq 0}$ which satisfy these conditions. □

Problem 3. Prove that for p prime, $f(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1$ is irreducible in $\mathbb{Q}[x]$.

Proposition 1. If $f(x + c)$ is irreducible over $F[x]$ $f(x)$, then so is $f(x)$.

Proof of Proposition. We will prove the contrapositive. $f(x)$ is reducible in $F[x]$ iff there is a root a of f such that $f(a) = 0$.

Then, for $x = a - c$, $f(a - c + c) = f(a) = 0$ is a root of $f(x + c)$.

Thus, $f(x+c)$ is reducible in $F[x]$ as well. □

Proof of Problem. Note that

$$(x-1)f(x) = x^p - 1 \implies f(x) = \frac{x^p-1}{x-1}.$$

We will consider

$$f(x+1) = \frac{(x+1)^p - 1}{x}.$$

By the binomial expansion, we have

$$(x+1)^p = \sum_0^p \binom{p}{k} x^k \cdot 1^{p-k} = \sum_0^p \binom{p}{k} x^k.$$

So,

$$f(x+1) = \frac{1}{x}\left(\sum_0^p \binom{p}{k} x^k - 1\right) = \sum_1^p \binom{p}{k} x^{k-1}.$$

For $k = p$, $\binom{p}{p} = 1$, so p is coprime with the leading coefficient.

Note that $\forall 0 < k < p$, $p \mid \binom{p}{k}$. So, p divides all the other coefficients.

Then, at $k = 1$, $\binom{p}{1} = p$ but $p^2 \nmid p$. So, the conditions of Einstein's Criterion are satisfied. Thus, $f(x+1)$ is irreducible in $\mathbb{Q}[x]$.

Hence, by the Proposition, $f(x)$ is irreducible in $\mathbb{Q}[x]$ as well. □

Problem 4. Factor each polynomial as a product of irreducibles in $\mathbb{Q}[x]$, $\mathbb{R}[x]$, and $\mathbb{C}[x]$.

a $x^4 - 2$.

$x^4 - 2$ is irreducible in $\mathbb{Q}[x]$ by the Rational Root Theorem.

Then, $x^4 - 2 = (x^2 + 2^{\frac{1}{2}})(x - 2^{\frac{1}{4}})(x + 2^{\frac{1}{4}}) \in \mathbb{R}[x]$, where the remaining quadratic term has a negative discriminant and is therefore irreducible in $\mathbb{R}[x]$.

However, in $\mathbb{C}[x]$, all irreducible polynomials are linear, so we must have

$$x^4 - 2 = (x - 2^{\frac{1}{4}}i)(x + 2^{\frac{1}{4}}i)(x - 2^{\frac{1}{4}})(x + 2^{\frac{1}{4}}) \in \mathbb{C}[x].$$

b $x^3 + 1$.

First, $x^3 + 1 = (x+1)(x^2 - x + 1)$. Since $x^2 - x + 1$ has a negative discriminant, then it is irreducible in both $\mathbb{Q}[x]$ and $\mathbb{R}[x]$.

So, the above is a product of irreducibles for $\mathbb{Q}[x]$ and $\mathbb{R}[x]$.

Then, we have

$$x^3 + 1 = (x + 1)\left(x - \left(\frac{1 \pm \sqrt{3}i}{2}\right)\right) \in \mathbb{C}[x]$$

by the quadratic formula, which is a product of linear and therefore irreducible polynomials in $\mathbb{C}[x]$.

c $x^3 - x^2 - 5x + 5$.

We have a root at $x = 1$, so $x - 1$ is a factor of this polynomial.

This gives $(x - 1)(x^2 - 5)$. Since $x^2 - 5$ is irreducible in $\mathbb{Q}[x]$, then the this is a product of irreducibles is $\mathbb{Q}[x]$.

But, in $\mathbb{R}[x]$, we have

$$x^3 - x^2 - 5x + 5 = (x - 1)(x - \sqrt{5})(x + \sqrt{5}) \in \mathbb{R}[x].$$

Since all of these factors are linear polynomials, then this factoring also holds in $\mathbb{C}[x]$.

Problem 5. Factor $x^2 + x + 1 + i$ in $\mathbb{C}[x]$.

We have a root at $x = -i$. Then,

$$(x + i)(x + (1 - i)) = x^2 + x - xi + xi + i - i^2 = x^2 + x + 1 + i.$$

Since these are linear factors, then they are irreducible.

Problem 6. Show that polynomials of odd degree with no multiple roots in $\mathbb{R}[x]$ must have an odd number of real roots.

Proof. By the Fundamental Theorem of Algebra, a polynomial of degree n must have n roots in $\mathbb{C}[x]$.

Since complex roots come in conjugate pairs for polynomials in $\mathbb{R}[x]$, then we must have an even number of such roots for the given polynomials.

The number of real roots is the number of total roots, which is odd, take the number of complex roots, which is even. Since odd - even = odd, then we must have an odd number of real roots. □

Problem 7. Let $f(x), g(x), p(x) \in F[x]$ with $p(x)$ nonzero. Determine whether $f(x)$ is congruent to $g(x)$ mod $p(x)$.

a) $f(x) = x^5 - 2x^4 + 4x^3 + x + 1$, $g(x) = 3x^4 + 2x^3 - 5x^2 - 9$, $p(x) = x^2 + 1$, and $F = \mathbb{Q}$.

We will check if p divides $f - g = x^5 - 5x^4 + 2x^3 + 5x^2 + x + 10$.

$$\begin{array}{r|l}
 & x^3 - 5x^2 + x + 10 \\
\hline
x^2 + 1 & x^5 - 5x^4 + 2x^3 + 5x^2 + x + 10 \\
 & -x^5 \quad\quad - x^3 \\
\hline
 & -5x^4 + x^3 + 5x^2 \\
 & 5x^4 \quad\quad + 5x^2 \\
\hline
 & x^3 + 10x^2 + x \\
 & -x^3 \quad\quad - x \\
\hline
 & 10x^2 + 10 \\
 & -10x^2 - 10 \\
\hline
 & 0
\end{array}$$

Since the remainder is zero, then $f \equiv g \mod p$ indeed.

b) $f(x) = x^4 + x < D - r > +x + 1$, $g(x) = x^4 + x^3 + x^2 + 1$, $p(x) = x^2 + x$, and $F = \mathbb{Q}$.

As before, $g - f = x^3 - x = x(x+1)(x-1) = (x^2 + x)(x-1)$. Since $x^2 + x \mid (x^2 + x)(x-1)$, then $p \mid g - f$, so $f \equiv g \mod p$.

c) $f(x) = 3x^5 + 4x^4 + 5x^3 - 6x^2 + 5x - 7$, $g(x) = 2x^2 + 6x^4 + x^3 + 2x^2 + 2x - 5$, $p(x) = x^3 - x^2 + x - 1$, and $F = \mathbb{R}$.

We have $f - g = x^5 - 2x^4 + 4x^3 - 8x^2 + 3x - 2$. Then,

$$\begin{array}{r|l}
 & x^2 - x + 2 \\
\hline
x^3 - x^2 + x - 1 & x^5 - 2x^4 + 4x^3 - 8x^2 + 3x - 2 \\
 & -x^5 + x^4 - x^3 + x^2 \\
\hline
 & -x^4 + 3x^3 - 7x^2 + 3x \\
 & x^4 - x^3 + x^2 - x \\
\hline
 & 2x^3 - 6x^2 + 2x - 2 \\
 & -2x^3 + 2x^2 - 2x + 2 \\
\hline
 & -4x^2
\end{array}$$

Since we have a nonzero remainder, then p does not divide $f - g$.
So $f(x)$ is not congruent to $g(x)$ mod $p(x)$.

Problem 8. List the distinct congruence classes of modulo $x^3 + x + 1$ in $\mathbb{Z}_2[x]$.

We need to find all possible remainders when dividing by $x^3 + x + 1$ in $\mathbb{Z}_2[x]$, these will have at most degree two.

There are $2^3 = 8$ such polynomials which will be the canonical representatives of the congruence classes: $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$.

Problem 9. Prove that if $p(x)$ is irreducible in $F[x]$ and $f(x)g(x) \equiv 0_F \mod p(x)$, then $f(x) \equiv 0_F \mod p(x)$ or $g(x) \equiv 0_F \mod p(x)$.

Proof. This is analogous to the fact that $\mathbb{Z}_p$ is field and therefore has no zero divisors when p is prime. So, we will show that the polynomial ring $F[x]$ is a field when $p(x)$ is irreducible.

Since $f(x)g(x) \equiv 0 \mod p(x)$, then $p(x) \mid f(x)g(x)$. By Theorem 4.12, $F[x]$ is a unique factorization

domain when $p(x)$ is irreducible; e.g., $p(x)$ irreducible and $p(x) \mid f(x)g(x)$ implies that $p(x)$ divides $f(x)$ or $p(x)$ divides $g(x)$. Thus, $f(x) \equiv 0 \mod p(x)$ or $g(x) \equiv 0 \mod p(x)$ and we are done. □

Problem 10. Prove that, when $f(x)$ and $p(x)$ are coprime in $F[x]$, then $f(x)$ is a unit in $F[x]/(p(x))$.

Proof. This is Theorem 5.9. We wish to show that there exists a $g(x) \in F[x]$ such that $f(x)g(x) \equiv 1_F \mod p(x)$.

By Theorem 4.8, since $(f(x), p(x)) = 1$, then there exist some $g(x), q(x) \in F[x]$ such that we have the linear combination $f(x)g(x) + p(x)q(x) = 1$.

Then, if we consider this equation in mod $p(x)$, we have that $f(x)g(x) \equiv 1 \mod p(x)$, so we are done. □

Problem 11. Write the addition and multiplication tables for the congruence class ring $F[x]/(p(x))$; in each case, is $F[x]/(p(x))$ a field?

i) $\mathbb{Z}_3[x]/(x^2+1)$.

The congruence classes are $3^2 = 9$ polynomials of degree 1: $0, 1, 2, x, 2x, x+2, x+2, 2x+1, 2x+1$.

Note that, in the following tables, we have omitted the brackets around each of the congruence classes, but this table holds for all members of each congruence class respectively.

$+$	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
0	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$2x+1$	$x+2$	x	$2x+2$	$2x$
2	2	0	1	$x+2$	$2x+2$	x	$x+1$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	0	$2x+1$	$2x+2$	1	2
$2x$	$2x$	$2x+1$	$2x+2$	0	x	1	2	$x+1$	$x+2$
$x+1$	$x+1$	$x+2$	x	$2x+1$	1	$2x+2$	$2x$	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	2	$2x$	$2x+1$	0	1
$2x+1$	$2x+1$	$2x+2$	$2x$	1	$x+1$	2	0	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	$x+2$	0	1	x	$x+1$

$\times$	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$2x$	$x+1$	$x+2$	$2x+1$	$2x+2$
2	0	2	1	$2x$	x	$2x+2$	$2x+1$	$x+2$	$x+1$
x	0	x	$2x$	2	1	$x+2$	$x+1$	$2x+2$	$2x+1$
$2x$	0	$2x$	x	1	2	$2x+1$	$2x+2$	$x+1$	$x+2$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x+1$	0	2	$2x$	1
$x+2$	0	$x+2$	$2x+1$	$x+1$	$2x+2$	1	0	2	$2x$
$2x+1$	0	$2x+1$	$x+2$	$2x+2$	$x+1$	$2x$	2	0	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	$x+2$	1	$2x$	1	0

Since we have zero entries in the multiplication table, then we have zero divisors, so $\mathbb{Z}_3[x]/(x^2+1)$ is not a field.

ii) $\mathbb{Z}_2[x]/(x^2+1)$.

We have the congruence classes of $0, 1, x, x+1$.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	1	$x+1$
$x+1$	0	$x+1$	$x+1$	0

Since x^2+1 is reducible in $Z_2[x]$ and its factor $x+1$ represents a congruence class, then $Z_2[x]/(x^2+1)$ has zero divisors and is thus not a field.