Reducible and Irreducible Polynomials

1. Brute Force

Sometimes we can show a polynomial is irreducible simply by showing that none of the polynomials that could possibly be factors are factors.

Show that $x^4 + x + 1$ is irreducible in $Z_2[x]$. Use an argument by contradiction. If $x^4 + x + 1$ is reducible, it has a factor of degree 1 or degree 2. Use long division or other arguments to show that none of these is actually a factor.

2. Checking all the possible roots.

If a polynomial with degree 2 or higher is irreducible in $F[x]$, then it has no roots in F.

If a polynomial with degree 2 or 3 is irreducible in F, then it has no roots in $F[x]$.

Show that $f(x) = 2x^2 + x + 1$ is irreducible in $Z_3[x]$ by showing that it has no roots.

Possible values of x are $0, 1, 2$. $f(0) = 1$, $f(1) = 4$, $f(2) = 11$.

So f(x) has no roots and is degree 2 so it is irreducible.

Consider the polynomial $f(x) = x^4 + 3x^3 + x^2 + 3$ in $Z_4[x]$. Possible values of x are $0, 1, 2, 3, 4$. Therefore $f(0) = 3$, $f(1) = 8$, $f(2) = 47$, $f(3) = 174$, $f(4) = 467$. So f(x) has no roots, however it is a degree 4 polynomial so we cannot conclude it is irreducible.

3. Using roots to factor.

Once we know a polynomial has a root $x = a$, we can factor $x - a$ out of the polynomial using long division. Then we can try to factor the quotient.

Given that $x = 3$ is a root of the polynomial $f(x) = 10x^3 + 3x^2 - 106x + 21$ in Q[x]. Factor the polynomial completely.

$$
\begin{array}{rrrrr}
10x^3 & 3x^2 & -106x & 21 & x-3 \\
-10x^3(x-3) & & & 10x^2 & \\
0 & 33x^2 & -106x & & \\
 & 33x(x-3) & & 33x & \\
 & 0 & -7x & 21 & \\
 & & -7(x-3) & & -7 \\
 & & 0 & &
\end{array}
$$

So $f(x) = 10x^3 + 3x^2 - 106x + 21 = (x-3)(10x^2 + 33x - 7)$.

Consider the polynomial $f(x) = 3x^3 + 8x^2 + 3x - 2 \in Q[x]$. Use the Rational Root Theorem to make a list of all the possible rational roots of this polynomial.

Rational Root Theorem

Consider the polynomial $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. With integer coefficients $a_i \in Z$ and $a_0, a_n \neq 0$. Solutions of the equation are also called roots or zeroes of the polynomial on the left side. The theorem states that each rational solution $x = \frac{p}{q}$ written in lowest terms so that p and q are relatively prime, satisfies:

1. p is an integer factor of the constant term a_0, and
2. q is an integer factor of the leading coefficient a_n.

In our polynomial f(x), $p = \pm 1, \pm 2$ and $q = \pm 1, \pm 3$. The possible roots are $\pm 1, \pm 2, \pm \frac{1}{3}, \pm \frac{2}{3}$.

So $f(1) = 12$, $f(-1) = 0$, $f(2) = 60$, $f(-2) = 0$, $f(\frac{1}{3}) = 0$, $f(\frac{-1}{3}) = \frac{-20}{9}$, $f(\frac{2}{3}) = \frac{40}{9}$, $f(\frac{-2}{3}) = \frac{-4}{3}$.

So the polynomial $f(x) = 3x^3 + 8x^2 + 3x - 2$ has factorisation $(x+1)(x-2)(x-\frac{1}{3})$, and has roots $x = -1$, $x = -2$, and $x = \frac{1}{3}$.

Now Consider the polynomial $f(x) = x^3 - x^2 + x - 6 \in Q[x]$. If $x = 3$ is a root then:

$$
\begin{array}{rrrrr}
x^3 & -x^2 & x & -6 & x-3 \\
-x^2(x-3) & & x^2 & & \\
0 & 2x^2 & x & & \\
 & 2x(x-3) & & 2x & \\
 & 0 & 7x & -6 & \\
 & & 7(x-3) & & 7 \\
 & & 15 & &
\end{array}
$$

This shows x=3 is not a root. Using the Rational root theorem the possible roots are $\pm 1, \pm 2, \pm 3, \pm 6$. In this case x=2 is a root.

$$
\begin{array}{rrrrr}
x^3 & -x^2 & x & -6 & x-2 \\
-x^2(x-2) & & x^2 & & \\
0 & x^2 & x & & \\
 & x(x-2) & & x & \\
 & 0 & 3x & -6 & \\
 & & 3(x-2) & & 3 \\
 & & 0 & &
\end{array}
$$

This $f(x) = x^3 - x^2 + x - 6 = (x-2)(x^2 + x + 3)$. So the polynomial is reducible over the rationals.

4. Eisenstein's Criterion

Eisenstein's Criterion is another method can be used to determine if a polynomial is irreducible. Note that if we can't find a prime to make Eisenstein's Criterion work, that does not tell us for certain that the polynomial is not irreducible.

Given a polynomial with integer coefficients $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots a_1 x + a_0$. If there exists a prime number p such that the following three conditions all apply: a. p divides $a_0, a_1, \ldots a_{n-1}$, b. p does not divide a_n, c. p^2 does not divide a_0.

Then f(x) is irreducible.

Is $f(x) = x^{10} + 50$ irreducible in Q[x]?

Pick $p = 5$. $p \nmid 1$, $p \mid 50$, and $p^2 = 25 \nmid 1$. THus f(x) is irreducible over Q by Eisentstein's Criterion with p=5. Could easily use p=2 as well.

Is $f(x) = 5x^{11} - 6x^4 + 12x^3 + 36x + 6 \in Q[x]$?

Pick $p = 2$, $p \nmid 5$, $p \mid -6$, $p \mid 12$, $p \mid 36$, $p \mid 6$, and $p^2 = 4 \nmid 6$. Thus f(x) is is irreducible over Q by Eisenstein's Criterion with p=2.

Reducing Mod p

The final method we have learned is reducing our polynomials mod a prime . If we reduce the polynomial mod and the result is reducible, then this doesn't tell us anything.

If f(x) is a polynomial with integer coefficients and p is a prime that does not divide the leading coefficient of f(x), then we can reduce the polynomial mod p. If the reduced polynomial is irreducible in $Z_p[x]$ then the original polynomial in Q[x] is irreducible.

Is $f(x) = 5x^2 + 10x + 4$ irreducible in Q[x]? Pick p = 3. $g(x) = 2x^2 + x + 1 \in Z_3[x]$. So are there any roots? g(0) = 1, g(1) = 1, g(2) = 2. There are no roots in $Z_3[x]$ and the degree is 2, so the polynomial g(x) is irreducible over $Z_3[x]$, therefore f(x) is irreducible over Q[x].

Is $f(x) = 3x^3 + 7x^2 + 10x - 5$ irreducible in Q[x]? Pick p = 2. Therefore $g(x) = x^3 + x^2 + 1 \in Z_2[x]$. So are there any roots? g(0) = 1, g(1) = 1. There are no roots in $Z_2[x]$ and the degree of g is 3, so g(x) is irreducible over $Z_2[x]$, therefore f(x) is irreducible over Q[x].

Is $f(x) = 9x^4 + 4x^2 - 3x + 7$ irreducible in Q[x]? Therefore pick p =2. Therefore $g(x) = x^4 + x + 1$. THus f(0) = 1, f(1) = 1. So f(x) has no roots, therefore it has no linear factors. This means the only possible factors are quadratic.

So $g(x) = x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$ or $(x^2 + ax - 1)(x^2 + bx - 1)$.

Thus $g(x) = x^4 + (a+b)x^3 + (2+ab)x^2 + (a+b)x + 1$, Equating terms $a + b = 0$ and $2 + ab = 0$ and $a + b = 1$. Thus we have an inconsistant system.

Similarly with $g(x) = x^4 + (a+b)x^3 + (-2+ab)x^2 - (a+b)x + 1$,

Therefore there are no quadratic roots, and hence the g(x) is irreducible in $Z_2[x]$ and therefore f(x) is irreducible in Q[x].

Problem Sheet 3: Question 1:

(a) Is $f(x) = x^3 + 2x^2 + 4x + 2 \in Q[x]$ irreducible?

If f(x) is reducible the only options are: i. Degree 1 polynomial x Degree 2 polynomial ii. or degree 2 polynomial x degree 1 polynomial.

If the polynomial is reducible one of the factors will be of form $(a_1 x + a_0)$. However since we are in Q[x] the brute force method is not something I am going to use.

If we use Eisenstein's criterion: p = 2. Therefore $p \nmid 1$, $p \mid 2$, $p \mid 4$, $p \mid 2$, and $p^2 = 4 \nmid 1$. Thus f(x) is irreducible over Q by Eisenstein's criteria with p =2.

If we use the Rational root theorem. The possible roots are ± 1, ± 2. So f(-1) = -1, f(1) = 9, f(-2) = -6, f(2) = 26. So non of the possible roots are roots. This means there are no linear factors of f(x) and so f(x) is irreducible.

If we use the Reducing Mod p method. So start with p = 2. Therefore f(x) becomes $g(x) = x^3 \in Z_2[x]$. The fact that g(x) is reducible Z_2 does not tell us any information about f(x)'s reducibility in Q.

Lets try with p = 3. therefore f(x) becomes $g(x) = x^3 + 2x^2 + x + 2 \in Z_3[x]$. So $f(0) = 2$, $f(1) = 6 = 0 mod 3$, $f(2) = 20 = 2 mod 3$. There x=1 is a root of g(x) in $Z_3[x]$. So (x-1) is a linear factor of g(x). Again fact that g(x) is reducible Z_3 does not tell us any information about f(x)'s reducibility in Q.

Lets try with p =5, therefore f(x) becomes $g(x) = x^3 + 2x^2 + 4x + 2 \in Z_5[x]$. So $f(0) = 2$, $f(1) = 9 mod 5 = 4$, $f(2) = 26 mod 5 = 1$, $f(3) = 68 mod 5 = 3$, $f(4) = 114 mod 5 = 4$. So there are no roots and therefore no linear factors in Z_5, and so g(x) is irreducible in $Z_5[x]$, and therefore f(x) is irreducible in Q[x].

(b) Is $f(x) = x^4 + 3x^3 + 15 \in Q[x]$ irreducible?.

Since f(x) has degree 4, we will not be able to infer from f(x) having no roots and therefore no linear factors that it is irreducible.

Just to be obstinant we will look for roots. Using the rational root theorem. Possible roots are ± 1, ± 15. Since non of these result in a root we have no linear factors. So the only possible factors are quadratic.

$$f(x) = (x^2 + ax + 1)(x^2 + bx + 15) \text{ or } (x^2 + ax - 1)(x^2 + bx - 15)$$

$$f(x) = x^4 + (a+b)x^3 + (16 + ab)x^2 + (15a + b)x + 15$$

So we have $(a + b) = 3$, $(16 + ab) = 0$, and $15a + b = 0$. This leads to an inconsistancy with a being equal to two different values. Thus f(x) has no quadratic factors. So f(x) is irreducible in Q[x]. A similar argument for the other quadratic pair.

A far easier approach is to use Eisensteins Criterion. Let us consider p = 3. We know $p \nmid 1$, $p \mid 3$, $p \mid 15$, $and\ p^2 = 9 \nmid 1$. So by Eisensteins criterion with p = 3, f(x) is irreducible in Q[x].

(c) Is $f(x) = x^3 + 6x^2 + 11x + 8 \in Q[x]$ irreducible?.

Since we have a cubic polynomial, if we can find a root then we know f(x) has a linear factor and is therefore reducible. To simplify our search for roots we will reduce mod p.

If p = 2, f(x) reduces to $g(x) = x^3 + x \in Z_2[x]$. Now g(x) is reducible over Z_2 but this doesn't tell us anything about its reducibility over Q.

If p = 3, f(x) reduces to $g(x) = x^3 + 2x + 2 \in Z_3[x]$. Now g(0) = 2, g(1) = 5 mod 3 = 2, g(2) = 14 mod 3 = 2. So g(x) has no roots in $Z_3[x]$ and hence it has no linear factors and is therefore irreducible in $Z_3[x]$, so we can say f(x) is irreducible in Q[x]

(d) Is $f(x) = x^4 + 3x^2 + x + 1 \in Q[x]$ irreducible?.

We have a degree 4 polynomial so having no roots just tells us there are no linear factors and hence only quadratic factors.

We can use the rational root test to confirm if there are any linear factors. The on roots are ± 1. Thus f(1) = 6, f(-1) = 4. Thus there are no linear factors of f(x). So we only have quadratic factors.

If we reduce f(x) mod p, let p = 3, thus $g(x) = x^4 + x + 1 \in Z_3[x]$.

$$\begin{aligned} g(x) &= (x^2 + ax + 1)(x^2 + bx + 1),\ a, b \in Z_3 \\ &= x^4 + (a+b)x^3 + (2+ab)x^2 + (a+b)x + 1 \\ &\therefore (a+b) = 0,\ (2+ab) = 2,\ (a+b) = 1 \end{aligned}$$

So we have an inconsistancy (a+b=0, and a+b =1), so these are not possible quadratic factors

There are no valid options for quadratic factors, and no linear factors so g(x) is irreducible in $Z_3[x]$, therefore f(x) is irreducible in Q[x].

(e) Is $f(x) = x^4 + x^2 + 1 \in Q[x]$ irreducible?.

Therefore pick p =2. Therefore $g(x) = x^4 + x + 1$. THus f(0) = 1, f(1) = 1. So f(x) has no roots, therefore it has no linear factors. This means the only possible factors are quadratic.

So $g(x) = x^4 + x + 1 = (x^2 + ax + 1)(x^2 + bx + 1)$.

Thus $g(x) = x^4 + (a+b)x^3 + (2+ab)x^2 + (a+b)x + 1$, Equating terms $a + b = 0$ and $2 + ab = 0$ and $a + b = 1$. Thus we have an inconsistant system.

Therefore there are no quadratic roots, and hence the g(x) is irreducible in $Z_2[x]$ and therefore f(x) is irreducible in Q[x].

Problem Sheet 3: Question 2:

Prove that $u^4 + 2u + 2$ is irreducible over Q. Let u be a root of this polynomial. Express u^4, $u^3 + u^5$, $and\ u^{-1}$ in terms of $u, u^2,\ and\ u^3$.

If we use Eisenstein's criterion with p = 2, $p \nmid 1$, $p \mid 2$, $p \mid 2$, $and\ p^2 = 4 \nmid 1$. Therefore by Eisenstein's criterion with p =2, f(x) is irreducible.

We are being asked to express $u^4, u^3 + u^5$, $and\ u^{-1}$ in the following form $a + bu + cu^2 + du^3$.

We know $f(u) = u^4 + 2u + 2 = 0$. Thus $u^4 = -2u - 2$.

$$\begin{aligned} u^4 + 2u + 2 &= 0 \\ u^4 &= -2u - 2 \\ u^5 &= u(u^4) = -2u^2 - 2u \\ u^6 &= u(u^5) = -2u^3 - 2u^2 \\ \therefore u^3 + u^6 &= -(2u^3 + 4u^2 + 2u) \\ u^{-1}(u^4 + 2u + 2) &= u^3 + 2 + 2u^{-1} = 0 \\ \therefore u^{-1} &= \frac{-1}{2}(u^3 + 2) \end{aligned}$$

Problem Sheet 3: Question 3:

Let $F = Z_{11}$, be the field of integers mod 11. Prove that $f(x) = x^3 + x + 4$ is irreducible over F. Show that $\frac{F[x]}{(x^3+x+4)}$ is a field having 121 elements.

We cannot use Eisenstein's criterion. So we will try to find all roots in F.

$$\begin{aligned} f(0) &= 4 mod 11 = 4 \\ f(1) &= 6 mod 11 = 6 \\ f(2) &= 10 mod 11 = 10 \\ f(3) &= 16 mod 11 = 5 \\ f(4) &= 24 mod 11 = 2 \\ f(5) &= 34 mod 11 = 1 \\ f(6) &= 46 mod 11 = 2 \\ f(7) &= 60 mod 11 = 5 \\ f(8) &= 76 mod 11 = 10 \\ f(9) &= 94 mod 11 = 6 \\ f(10) &= 114 mod 11 = 4 \end{aligned}$$

So there are no roots in F and hence no linear factors, since f(x) is a polynomial of degree 2, it is irreducible over F.

Thus from Theorem: Let F be a Field and p(x) be an irreducible polynomial over F. Then F[x]/(p(x)) is a field.

So since f(x) is an irreducible polynomial over F, F/<f(x)> is a field.

So we have:

$\frac{F[x]}{(x^3+x+4)} = \{a_0 + a_1 x + \ < x^3 + x + 4 > : a_i \in Z_{11}\}$

So the number of elements are $|\frac{F[x]}{(x^3+x+4)}| = 11^2 = 121$.

In [ ]: