Exercise 11.4: Prove the the only units in $\mathbb{Z}[x]$ are 1 and -1.

Suppose that $f(x)$ is a non-zero polynomial in $\mathbb{Z}[x]$ and is a unit. By definition, there exists some $g(x)$ in $\mathbb{Z}[x]$ such that $p(x)g(x) = 1$. Then, $deg(p(x)g(x)) = deg(p(x)) + deg(g(x)) = deg(1) = 0$. Therefore, $deg(p(x)) = deg(g(x)) = 0$ and so $p(x)$ is a constant polynomial of degree zero.

Since the units of $\mathbb{Z}[x]$ are the constant degree zero polynomials, we observe that every unit of $\mathbb{Z}[x]$ is contained in the subset of integers, $\mathbb{Z}$. Recall that the units of $\mathbb{Z}$ are 1 and -1. Since each of the units of $\mathbb{Z}[x]$ lie in $\mathbb{Z}$, the units of $\mathbb{Z}[x]$ are precisely the units of $\mathbb{Z}$: 1 and -1. Therefore the units of $\mathbb{Z}[x]$ are 1 and -1. $\square$

Exercise 11.8: Let n be an integer greater than 1 and suppose m is an odd integer.

In exercise 11.7, we show that $x^n - 2$ is irreducible in $\mathbb{Q}[x]$ by using contradiciton to show that $x^n - 2$ is impossible to factor as a product of two lower degree polynomials in $\mathbb{Z}[x]$. We will use a similar argument to show that $x^n - 2m$ does not factor as a product of two lower degree polynomials in $\mathbb{Z}[x]$, and therefore is irreducible in $\mathbb{Q}[x]$.

Suppose that $x^n - 2m = g(x)h(x)$ where $g(x)$ and $h(x)$ are polynomials of degrees k and l respectively in $\mathbb{Z}[x]$ such that $k < n$ and $l < n$. Let $g(x) = a_k x^k + a_{k-1}x^{k-1} + ... + a_2 x^2 + a_1 x + a_0$ and $h(x) = b_l x^l + b_{l-1}x^{l-1} + ... + b_2 x^2 + b_1 x + b_0$. Then, if we multiply $h(x)$ and $g(x)$ together we form a polynomial of degree n in terms of the coefficients a_i and b_i.

$$x^n - 2m =$$
$$(a_k x^k + a_{k-1}x^{k-1} + ... + a_2 x^2 + a_1 x + a_0)(b_l x^l + b_{l-1}x^{l-1} + ... + b_2 x^2 + b_1 x + b_0)$$
$$= (a_k b_l)x^n + ... + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_0 b_1 + a_1 b_0)x + (a_0 b_0)$$

Here we have two equivalent statements where the coefficients of the terms on the left side are equal to the coefficients of the terms on the right side. Since $2m$ divides the constant coefficient on left side of the equation, $2m$ must also divide the constant coefficient on the right side as well. We know that $2m$ divides $a_0 b_0$, in fact, because no other terms in the equation are purely constant, $2m = a_0 b_0$. Since 2 is a prime number, Euclids Lemma states that either $2|a_0$ or $2|b_0$, but it does not divide both terms because m is odd. Without loss of generality, we let 2 divide a_0.

Consider the degree-one term: $a_0 b_1 + a_1 b_0$. We know that $2m$ divides 0, the coefficient of the degree one term on the left side, so we may conclude that $2m|a_0 b_1 + a_1 b_0$, the coefficient on the right side. Because we have already established that $2|a_0$ it certainly follows that $2m|a_0 b_1$. If $2m$ divides $a_0 b_1$ and $2m$ divides $a_0 b_1 + a_1 b_0$, it is implied that $2m$ divides $a_1 b_0$ as well. We already know that $2 \nmid b_0$, so we may conclude by Euclids Lemma that $2|a_1$ as well. If we were to look at the coefficients of the degree two term on the right side, we would be able to say that $2m|a_0 b_2 + a_1 b_1 + a_2 b_0$ because $2m$ divides 0, the coefficient of the degree two term on the left side. Following a similar argument, we would see that $2m$ divides each of the terms individually because $2m|a_0 b_2$ and $2m|a_1 b_1$, so it would follow that $2m|a_2 b_0$. We already know that

$2 \nmid b_0$, so we find that $2|a_2$ as well.

Suppose we continue using this technique until we have completed the same process for the coefficient corrosponding to the $n-2$ term. The $n-2$ term is given by: $a_{k-2}b_l + a_{k-1}b_{l-1} + a_k b_{l-2}$ and so by the inductive process, starting with the knowledge that $2|a_{k-2}$ from the previous inductive steps, we can use the same logic to find that for all $0 \leq j \leq k$ and $0 \leq i \leq l$ that $2|a_j$ and $2 \nmid b_i$. By induction, we have shown that 2 divides all of the coefficients of $g(x)$, but not the coefficients of $h(x)$.

Now that we know that 2 divides each of the terms of $g(x)$, it would follow that $2|a_k b_l$, the leading coefficient. If we take a look back at the original equation above, $x^n - 2m = (a_k b_l)x^n + ... + (a_0 b_0)$, we see that the coefficients on the left side of the equation must be equal to the coefficients on the right side of the equation. Therefore, $a_k b_l = 1$. However, $2|a_k b_l$ and $a_k b_l = 1$ are two contradictory statements because $2 \nmid 1$. Therefore, we have arrived at a contradiction and we have now proved that it is impossible to factor $x^n - 2m$ into two lower degree polynomials in $\mathbb{Z}[x]$, and so $x^n - 2m$ is irreducible in $\mathbb{Z}[x]$. By Gauss's Lemma, it follows that for every positive integer n and every odd integer m, $x^n - 2m$ is irreducible in $\mathbb{Q}[x]$. In particular, we have now shown that for every positive integer n, there exist infinitely many monic irreducible polynomials in $\mathbb{Q}[x]$. $\square$

In the previous sections, we found that the only irreducible polynomials in $\mathbb{C}[x]$ are the degree one polynomials and the only irreducible polynomials in $\mathbb{R}[x]$ are the degree one polynomials and polynomials of degree two with negative discriminant. This exercise has helped us expand our idea of the irreducibles in $\mathbb{Q}[x]$ to the polynomials of positive degree n with odd integer m such that $x^n - 2m$ is now categorized to be irreducible in $\mathbb{Q}[x]$.

Exercise 11.12: Use Eisenstein's criterion to show that the following polynomials are irredicuble in $\mathbb{Z}[x]$.

For a polynomial $f(x)$ in $\mathbb{Z}[x]$ and a prime number p, there are three requirements for Eisenstein's criterion:

1. The leading coefficient is not divisible by p
2. Every other coefficient is divisible by p
3. The constant coefficient is not divisible by p^2

1. $x^{22} + 7x^3 + 7$
Let $p = 7$. Then $7 \nmid a_n = 1$, $7|a_1 = 7$ and $7|a_0 = 7$, but, $7^2 \nmid a_0 = 7$. By Eisenstein's criterion, $f(x) = x^{22} + 7x^3 + 7$ does not factor as a product of lower degree polynomials in $\mathbb{Z}[x]$, therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

2. $x^{35} + 35x^{15} - 90$
Let $p = 5$. Then $5 \nmid a_n = 1$, $5|a_1 = 35$ and $5|a_0 = 90$, but, $5^2 \nmid a_0 = 90$. By Eisenstein's criterion, $f(x) = x^{35} + 35x^{15} - 90$ does not factor as a product of lower degree polynomials in $\mathbb{Z}[x]$, therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

3. $1662x^{384} - 35x^{100} + 625x^{44} + 100x^{10} - 75x + 20$
Let $p = 5$. Then $5 \nmid a_n = 1662$, $5|a_4 = 35$, $5|a_3 = 625$, $5|a_2 = 100$, $5|a_1 = 75$, and $5|a_0 = 20$, but, $5^2 \nmid a_0 = 20$. By Eisenstein's criterion, $f(x) = 1662x^{384} - 35x^{100} + 625x^{44} + 100x^{10} - 75x + 20$ does not factor as a product of lower degree polynomials in $\mathbb{Z}[x]$, therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

4. $6x^{31} + 35x^{21} + 245x^{11} + 175$
Let $p = 7$. Then $7 \nmid a_n = 6$, $7|a_2 = 35$, $7|a_1 = 245$, and $7|a_0 = 175$, but, $7^2 \nmid a_0 = 175$. By Eisenstein's criterion, $f(x) = 6x^{31} + 35x^{21} + 245x^{11} + 175$ does not factor as a product of lower degree polynomials in $\mathbb{Z}[x]$, therefore, $f(x)$ is irreducible in $\mathbb{Q}[x]$.

Exercise 11.16: Suppose $f(x)$ is a polynomial of positive degree in $\mathbb{Z}[x]$ and p is a prime number that does not divide the highest degree coefficient of $f(x)$. If the reduction $[f](x)$ of $f(x)$ modulo p is irreducible in $\mathbb{F}_p[x]$, then $f(x)$ does not factor in $\mathbb{Z}[x]$ as a product of lower-degree polynomials.

We will prove the theorem above using the contrapositive. Suppose that $f(x)$ is a polynomial of positive degree in $\mathbb{Z}[x]$ that factors as a product of two lower degree polynomials $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ such that $f(x) = g(x)h(x)$, and p is a prime number that does not divide the highest degree coefficient. By theorem 11.8 in the textbook, the reductions of these polynomials modulo p satisfies $[f](x) = [g](x)[h](x)$ in $\mathbb{F}_p[x]$. Because p does not divide the highest degree coefficient, the degree of $f(x)$ and $[f](x)$ will be the same. Therefore, $[f](x)$ factors as a product of lower degree polynomials in $\mathbb{F}_p[x]$ and thus by the contrapositive, we have proven the theorem above. $\square$

Exercise 11.20: Prove Eisenstein's Criterion

Suppose $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ is a polynomial of positive degree in $\mathbb{Z}[x]$ and p is a prime number such that the following conditions are met: p does not divide the highest-degree coefficient a_n of $f(x)$, p does divide every other coefficient a_i, and p^2 does not divide a_0. Suppose that $f(x)$ factors as a product of two lower degree polynomials $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$ and have degrees m and l respectively.

Take reduction of $f(x)$ mod p. Then $[f](x) = [a_n]x^n$ because every a_i is divisible by p, so for each a_i, $0 \leq i < n$, $[a_i] = 0$. By Theorem 11.8, $[f](x) = [g](x)[h](x)$ where $[g](x) = [b_m]x^m + [b_{m-1}]x^{m-1} + ... + [b_1]x + [b_0]$ and $[h](x) = [c_l]x^l + [c_{l-1}]x^{l-1} + ... + [c_1]x + [c_0]$. By comparing the coefficients of $[f](x)$ to the coefficients of $[g](x)[h](x)$, we see that $[b_0][c_0] = 0$. Observe that $[b_0]$ and $[c_0]$ cannot both be 0, because this implies that $p|b_0$ and $p|c_0$, hence, $p^2|b_0c_0 = a_0$ which contradicts the statement that $p^2 \nmid a_0$, so either $[b_0] = 0$ or $[c_0] = 0$. Without loss of generality, suppose that $[b_0] \neq 0$ and $[c_0] = 0$. This means that $p|[c_0]$.

If we compare the coefficients of $[f](x)$ and $[g](x)[h](x)$, we see that the coefficient associated with the degree one term, which is equal to zero, must be divisible by p. Here, $p|[b_0][c_1] + [b_1][c_0]$. It follows that $p|[b_0][c_1]$, and since $p \nmid [b_0]$, we may conclude using Euclid's Lemma that $p|[c_1]$. By following the same argument used in Exercises 11.7 and 11.8, it is easy to show that p divides all of the $[c]$ terms, by first proving that $p|[c_0]$ and $p|[c_1]$ then using a generalized inductive step to prove that $p|[c_i]$ for $0 \leq i \leq l$.

Now that we know that $p|[c_l]$, it would follow that p divides the leading coefficient as well: $p|[b_m][c_l]$. However, because $[b_m][c_l] = [a_n]$, we arrive at a contradiction because $p \nmid [a_n]$ due the the fact that $p \nmid a_n$. Thus, $f(x)$ does not factor as a product of lower degree polynomials in $\mathbb{Z}[x]$ and therefore, we have shown that if $f(x)$ meets all the requirements of Eisenstein's criterion, $f(x)$ is irreducible in $\mathbb{Z}[x]$. $\square$

Problem 2.0: Factor $x^5 - 1$ into irreducibles

To factor $x^5 - 1 = 0$ into irreducibles, we should first observe that $x = 1$ is a root and $x^5 = 1$ is a fifth root of unity. We will begin the factorization in $\mathbb{C}[x]$. Using the formula for roots of unity in $\mathbb{C}[x]$, we choose two roots of unity: $cos(\frac{2\pi}{5}) \pm isin(\frac{2\pi}{5})$ and $cos(\frac{4\pi}{5}) \pm isin(\frac{4\pi}{5})$. Notation quickly becomes tedious, so we will convert to and from exponential form using Eulers Formula: $e^{\frac{\pm 2\pi i}{5}}$ and $e^{\frac{\pm 4\pi i}{5}}$.

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$$
$$x^5 - 1 = (x-1)(x - e^{\frac{2\pi i}{5}})(x - e^{-\frac{2\pi i}{5}})(x - e^{\frac{4\pi i}{5}})(x - e^{-\frac{4\pi i}{5}}) \text{ in } \mathbb{C}[x] \ \mathbf{(1)}$$

$$x^5 - 1 = (x-1)(x^2 - (e^{\frac{2\pi i}{5}} + e^{\frac{-2\pi i}{5}})x + 1)(x^2 - (e^{\frac{4\pi i}{5}} + e^{\frac{-4\pi i}{5}})x + 1)$$
$$x^5 - 1 = (x-1)(x^2 - 2cos(\tfrac{2\pi}{5})x + 1)(x^2 - 2cos(\tfrac{4\pi}{5})x + 1) \text{ in } \mathbb{R}[x] \ \mathbf{(2)}$$

To find the factorization of $x^5 - 1$ in $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$, we need to use the lemma provided in lecture: given $f(x) \in \mathbb{Q}[x]$, $f(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $f(x+1)$ is irreducible in $\mathbb{Q}[x]$. Suppose we take $x^4 + x^3 + x^2 + x + 1$ and substitute $x = x + 1$. We find that $f(x+1) = (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = x^4 + 5x^3 + 10x^2 + 10x + 5$. Using Eisenstein's criterion, if we let $p = 5$, we see that $p \nmid 1$, $p|5$, $p|10$, $p|10$, and $p|5$, but $p^2 = 25 \nmid 5$. Thus, Eisenstien's criterion has been met and so $f(x+1)$ is irreducible in both $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$. By the lemma, since $f(x+1)$ is irreducible, so is $f(x)$. Therefore,

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) \text{ in } \mathbb{Z}[x] \text{ and } \mathbb{Q}[x] \ \mathbf{(3)}$$

Using theorem 11.8 in the textbook, we know that $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$ in $\mathbb{Z}[x]$, so we can use the formula to find that $x^5 + (-1+2) = (x + (-1+2))(x^4 + x^3 + x^2 + x + 1)$ in $\mathbb{Z}_2[x]$. We can plug in the values $x = 0$ and $x = 1$ to see that $x^4 + x^3 + x^2 + x + 1$ does not have any roots. Although it has no roots, it could still be factorized into a product of two degree 2 polynomials. In Math 411 we found that the only irreducible polynomial of degree 2 in $F_2[x]$ was $x^2 + x + 1$. We can use long division to divide $x^2 + x + 1$ into $x^4 + x^3 + x^2 + x + 1$ and see that $x^2 + x + 1 \nmid x^4 + x^3 + x^2 + x + 1$. Therefore, $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$ and so

$$x^5 + 1 = (x+1)(x^4 + x^3 + x^2 + x + 1) \text{ in } \mathbb{Z}_2[x] \ \mathbf{(4)}$$

Similarly, $x^5 + 2 = (x+2)(x^4 + x^3 + x^2 + x + 1)$ in $\mathbb{Z}_3[x]$. We see using the values $x = 0$, $x = 1$, and $x = 2$ that $x^4 + x^3 + x^2 + x + 1$ has no roots in $\mathbb{F}_3[x]$. We can check to see if any of the irreducible degree two polynomials of $F_3[x]$ divide $x^4+x^3+x^2+x+1$: x^2+1, x^2+x+2, x^2+2x+2, $2x^2+x+1$, and $2x^2+2x+1$. Using long division, we see that none of these irreducibles divide $x^4 + x^3 + x^2 + x + 1$. Therefore, $x^4 + x^3 + x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$ and so

$$x^5 + 2 = (x+2)(x^4 + x^3 + x^2 + x + 1) \text{ in } \mathbb{Z}_3[x] \ \mathbf{(5)}$$

Finally, we will look at $x^5 - 1$ in $\mathbb{Z}_5[x]$. Using theorem 11.8, $x^5 + 4 = (x+4)(x^4 + x^3 + x^2 + x + 1)$ in $\mathbb{Z}_5[x]$. We can observe that $x = 1$ is a root of $x^4+x^3+x^2+x+1$, so we can long divide $x-1 = x+4$ into $x^4+x^3+x^2+x+1$ to see that $x^5 + 4 = (x+4)(x+4)(x^3 + 2x^2 + 3x + 4)$ in $\mathbb{Z}_5[x]$. Once again, we see that $x = 1$ is a root, so we can long divide $x+4$ into x^3+2x^2+3x+4 to see that $x^5 + 4 = (x+4)(x+4)(x+4)(x^2 + 3x + 1)$. Again, $x = 1$ is a root, so we can factor $x+4$ out: $x^5+4 = (x+4)(x+4)(x+4)(x+4)(x-1)$ and thus,

$$x^5 + 2 = (x+4)(x+4)(x+4)(x+4)(x+4)$$
$$x^5 + 4 = (x+4)^5 \text{ in } \mathbb{Z}_5[x] \ \mathbf{(6)}$$