Exercise 11.11. Prove Eisenstein's criterion via the method indicated in the text.

Eisenstein's Criterion: Let $f(x)$ be a polynomial of degree $n > 1$ in $\mathbb{Z}[x]$. Suppose that $f(x) = \sum_{j=0}^{n} a_j x^j$. Further, suppose there is a prime number p satisfying the following three conditions:

(1) The coefficient a_n is not divisible by p;

(2) every coefficient a_i with $i < n$ is divisibly by p; and

(3) the constant coefficient a_0 is not divisibly by p^2.

Proof.

1. Suppose $f \in \mathbb{Z}[x]$ is such that $n := \deg(f) > 1$. Then $f(x) = \sum_{j=0}^{n} a_j x^j$ for some $\{a_j\}_{j=0}^{n} \subset \mathbb{Z}$. Suppose p is a prime satisfying the three conditions in Eisenstein's criterion.

In the spirit of contradiction, suppose that $f(x) = g(x)h(x)$ where $g(x) = \sum_{j=0}^{k} g_j x^j$ and $h(x) = \sum_{j=0}^{\ell} h_j x^j$ where $1 \le \ell, k < n$. Then,

$$f(x) = \sum_{j=0}^{n} a_j x^j = \sum_{j=0}^{n} x^j \left(\sum_{i+m=j} g_i h_m \right) \implies a_j = \sum_{i+m=j} g_i h_m \text{ for } j = 0, \dots, n. \tag{0.1}$$

2. By Equation (0.1) and condition (2) we observe that p divides $a_0 = g_0 h_0$ but by Equation (0.1) and condition (3) p^2 does not divide $a_0 = g_0 h_0$. Since p is prime, the first of these observations implies that

$$p \text{ divides } g_0 \text{ or } p \text{ divides } h_0. \tag{0.2}$$

The second observation, tells us that the "or" in Equation (0.2) is an exclusive or. So, without loss of generality, we assume that p divides g_0 but p does not divide h_0.

3. We have shown that p divides g_0 and does not divide h_0. Now, we make the inductive assumption that p divides g_j for all $j \le i - 1 < k$, for some $i \in \mathbb{N}$. Then, by Equation (0.1), since $i \le k < n$ it follows that

$$0 = a_i = \sum_{j+m=i} g_j h_m \implies g_i h_0 = - \sum_{\substack{j+m=i \\ m \neq 0}} g_j h_m.$$

Since each p divides g_j for all $j < i$, it follows that the right hand side, and hence the left hand side of the above equation is divisible by p. Since p does not divide h_0 and p is prime, this consequently shows that p divides g_i. Hence, induction holds, and p divides g_i for all $i \le k$.

4. One last time using Equation (0.1), we deduce that

$$a_n = \sum_{i+m=n} g_i h_m = g_k h_\ell.$$

By Part 3, it follows that p divides g_k and consequently p divides a_n, contradicting condition (1) of Eisenstein's criterion.

Hence, there do not exist polynomials $g, h \in \mathbb{Z}[x]$ with positive degree that divide f. ∎

Exercise 11.18. Use reduction modulo p to prove that $f(x) = x^5 + x^4 + 2x^3 + 2x + 2$ does not factor in $\mathbb{Z}[x]$ as a product of lower-degree polynomials.

Proof. We first note that if $f(x)$ can be factor, it can without loss of generality be factored into monic polynomials since it is itself monic.

Next, observe that 3 does not divide 1, so we consider $[f](x) = x^5 + x^4 + 2x^3 + 2x + 2 \in \mathbb{F}_3[x]$. Moreover, we recall from Exercise 11.13 that the only monic polynomials in $\mathbb{F}_3[x]$ of degree less than or equal to 2 are:

$$x^2 + 1, \quad x^2 + x + 2, \quad x^2 + 2x + 2. \tag{0.3}$$

Finally, we recall that if $g(x) \in K[x]$ is a polynomial of degree n, and there are no non-constant polynomials of degree less than or equal to $\frac{n}{2}$ in $K[x]$ that divide $g(x)$, then $g(x)$ is irreducible in $K[x]$.

Hence, it sufficies to show that none of the polynomials in (0.3) divides $[f](x) \in \mathbb{F}_3[x]$.

Indeed, by long division, we can check that the remainder of $[f](x)$ divided by $x^2 + 1$ is x, the remainder of $[f](x)$ divided byt x^2+x+2 is $2x+2$ and the remainded of $[f](x)$ divided by x^2+2x+2 is $2x$. Since none of these remainers are zero in $\mathbb{F}_3[x]$, the result follows: there are no divisors of $[f](x)$ in $\mathbb{F}_3[x]$ and therefore by Theorem 11. 9 there are no non-constant divisors of $f(x)$ in $\mathbb{Z}[x]$. ☐

Exercise 12.7. Prove Theorem 12.12.

Theorem 12.12. Let K be a field. Suppose that $a(x), b(x)$ are relatively prime polynomials in $K[x]$, and suppose that $c(x) \in K[x]$ is such that $a(x)$ divides $b(x)c(x)$ in $K[x]$. Then $a(x)$ divides $c(x)$ in $K[x]$.

Proof. Since $a(x), b(x)$ are relatively prime, Theorem 12.10 guarantees the existance of $r(x), s(x) \in K[x]$ such that

$$1 = r(x)a(x) + s(x)b(x).$$

Multiplying both sides by $c(x)$ yields

$$c(x) = r(x)\left(a(x)c(x)\right) + s(x)\left(b(x)c(x)\right).$$

Of course $a(x)$ divides $a(x)$. By assumption $a(x)$ divides $b(x)c(x)$. In particular, the right hand side of the above equation is divisible by $a(x)$ and consequently $a(x)$ divides $c(x)$ as desired. ☐

Exercise 13.4. Use Polar coordinates to prove that we can take square roots in $\mathbb{C}$.

Proof.

1. Fix $c \in \mathbb{C} \setminus \{0\}$ and write $c = a + bi$ for $a, b \in \mathbb{R}$. Let $|c|$ be the distance to the origin. Then $|c| = \sqrt{(a-0)^2 + (b-0)^2} = \sqrt{a^2 + b^2}$.
2. Show that every complex number c as above can be written as the product of a positive real number r and a complex number whose norm is 1.

We observe

$$c = \sqrt{a^2+b^2}\left(\frac{a}{\sqrt{a^2+b^2}} + \frac{bi}{\sqrt{a^2+b^2}}\right).$$

We note that

$$\left|\frac{a}{\sqrt{a^2+b^2}} + \frac{bi}{\sqrt{a^2+b^2}}\right| = \sqrt{\frac{a^2}{a^2+b^2} + \frac{b^2}{a^2+b^2}} = 1.$$

3. Suppose $|c| = 1$. Then, considering $[c] = (a, b)$ as a point in the cartesian plane corresponding to c in the complex plane, we know that $[c]$ must lie on the unit circle. The unit circle is parametrized by the set of points $\{(cos(\theta), \sin(\theta)) \mid \theta \in [0, 2\pi)\}$. In particular, since c is on the unit circle, there exists some particular θ_c such that $[c] = (\cos(\theta), \sin(\theta))$ and consequently $c = \cos(\theta) + i\sin(\theta)$ as desired.

4. Combining (2) and (3), we deduce that an arbitrary (non-zero) $c \in \mathbb{C}$ can be written as

$$c = |c|\left(\cos(\theta) + i\sin(\theta)\right), \text{ for some } \theta \in [0, 2\pi). \tag{0.4}$$

5. Now, we recall from Chapter 7 that $\left(\cos(x) + i\sin(x)\right)^n = \cos(nx) + i\sin(nx)$ for all $x \in \mathbb{R}$ and $n \in \mathbb{R}$. In particular:

$$\left(\pm\sqrt{r}\left(\cos(\frac{\theta}{2}) + i\sin(\frac{\theta}{2})\right)\right)^2 = r\left(\cos(\frac{\theta}{2}) + i\sin(\frac{\theta}{2})\right) = r\left(\cos(\theta) + i\sin(\theta)\right).$$

So, letting θ be as in (), it follows that

$$\pm\sqrt{|c|}\left(\cos(\theta/2) + i\sin(\theta/2)\right),$$

can both be the square root of c in $\mathbb{C}$. $\square$