CHAPTER 2

THE SCHÖNEMANN-EISENSTEIN CRITERION AND NEWTON POLYGONS

Gauss is reported to have said,

"There have been but three epoch-making mathematicians,

Archimedes, Newton, and Eisenstein."

– E. T. Bell

Men of Mathematics

2.1. In this chapter, we explore a certain criterion for the irreducibility of polynomials and its generalizations. The main result in this section, often referred to as Eisenstein's Criterion, is a classical one. It was first proved by Schönemann [1] in a slightly more general setting, and shortly afterwards Eisenstein [1] published the same result.

Theorem 5. *Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ where n is a positive integer. Suppose that there exists a prime p such that $p \nmid a_n$, $p | a_j$ for all $j < n$, and $p^2 \nmid a_0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Proof 1. By Theorem 2, it suffices to show that $f(x)$ cannot be written in the form $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbb{Z}[x]$, $\deg g(x) > 0$, and $\deg h(x) > 0$. Assume that $f(x)$ can be written in this form. Write $g(x)$ and $h(x)$ in the form $g(x) = \sum_{j=0}^{r} b_j x^j$ and

$h(x) = \sum_{j=0}^{s} c_j x^j$ where $r + s = n$. Define $b_j = 0$ for $j > r$, and define $c_j = 0$ for $j > s$. Let k be the minimal $j \in \{0, ..., r\}$ such that $p \nmid b_j$. Let ℓ be the minimal $j \in \{0, ..., s\}$ such that $p \nmid c_j$. These exist since $p \nmid a_n$ and $a_n = b_r c_s$ so that $p \nmid b_r$ and $p \nmid c_s$. The coefficient of $x^{k+\ell}$ in $g(x)h(x)$ is

$$b_0 c_{k+\ell} + b_1 c_{k+\ell-1} + \cdots + b_{k-1} c_{\ell+1} + b_k c_\ell + b_{k+1} c_{\ell-1} + \cdots + b_{k+\ell} c_0 \equiv b_k c_\ell \not\equiv 0 \pmod{p}.$$

On the other hand, all the coefficients of $f(x)$ except a_n are divisible by p. Thus, it must be the case that $k + \ell = n$ so that $k = r$ and $\ell = s$. By the definitions of k and ℓ, we now get that p divides both b_0 and c_0. But this contradicts that $a_0 = b_0 c_0$ is not divisible by p^2 and hence completes the proof. ■

Proof 2. Assume as before that $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbb{Z}[x]$, $r = \deg g(x) > 0$, and $s = \deg h(x) > 0$. Since

$$g(x)h(x) \equiv f(x) \equiv a_n x^n \pmod{p},$$

Theorem 3 (with $F = \mathbb{Z}_p$, the field of integers modulo p) implies that $g(x)$ and $h(x)$ are both constants times a power of x modulo p. Furthermore, the condition that $p \nmid a_n$ implies that the leading coefficient of $g(x)$ and the leading coefficient of $h(x)$ are not divisible by p. Hence, there exist integers b and c such that $g(x) \equiv bx^r \pmod{p}$ and $h(x) \equiv cx^s \pmod{p}$. Since $r > 0$ and $s > 0$, we get that p divides the constant terms of $g(x)$ and $h(x)$. This contradicts that $p^2 \nmid a_0$, completing the proof. ■

Example 1. Theorem 5 with $p = 3$ implies that $f(x) = 2x^6 + 6x^4 + 6$ is irreducible over $\mathbb{Q}$. Here, it is not the case that $f(x)$ is irreducible over $\mathbb{Z}$, so that Theorem 5 does not remain true if the words "over $\mathbb{Q}$" are omitted.

Example 2. The polynomial $f(x) = x^5 + 4x^2 + 2$ is irreducible. Note that Theorem 5 guarantees that $f(x)$ is irreducible over $\mathbb{Q}$. Theorem 1 then implies that $f(x)$ is irreducible over $\mathbb{Z}$.

Example 3. Theorem 5 with $p = 5$ and Problem (1.2) imply that the polynomial $f(x) = 5x^6 + 10x + 3$ is irreducible over $\mathbb{Q}$. Theorem 1 then implies that $f(x)$ is irreducible.

We note that the first proof of Theorem 5 very much resembles the proof given for the Lemma to Theorem 1. There are many possible generalizations of the Schönemann - Eisenstein Criterion; one example of such a generalization is given in Problem (2.9). Momentarily, we shall see how we can view the Schönemann - Eisenstein Criterion as being a simple consequence of a general theorem concerning Newton polygons. Many results similar to Theorem 5 can be obtained from the use of Newton polygons. Before discussing Newton polygons further, however, we explore the concept of Eisenstein polynomials.

2.2. We say that a polynomial $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is in Eisenstein form (with respect to the prime p) if there is a prime p such that $p \nmid a_n$, $p|a_j$ for $j < n$, and $p^2 \nmid a_0$. An Eisenstein polynomial is an $f(x) \in \mathbb{Z}[x]$ for which there is an integer a and a prime p such that $f(x+a)$ is in Eisenstein form with respect to the prime p. In other words, $f(x) \in \mathbb{Z}[x]$ is Eisenstein if there is an integer a and a prime p such that $f(x+a) = \sum_{j=0}^{n} a'_j x^j$ where $p \nmid a'_n$, $p|a'_j$ for $j < n$, and $p^2 \nmid a'_0$. More specifically, we say that such an $f(x)$ is Eisenstein with respect to the prime p. For example, since $f(x) = x^2 + x + 1$ is such that $f(x+1) = x^2 + 3x + 3$, the polynomial $f(x)$ is Eisenstein with respect to 3. It follows easily from Theorem 5 that if $f(x)$ is Eisenstein with respect to a prime p, then $f(x)$ is irreducible over $\mathbb{Q}$ (see Problem (1.1)).

Suppose one is given an $f(x) \in \mathbb{Z}[x]$ and wishes to decide whether $f(x)$ is Eisenstein with respect to some prime (which is not given). We assume $n = \deg f(x)$ is at least 2. One approach to making such a decision involves the use of discriminants or resultants. Our presentation here will be restricted to resultants. Let $f(x) = \sum_{j=0}^{n} a_j x^j$ and $g(x) = \sum_{j=0}^{r} b_j x^j$ be in $\mathbb{C}[x]$ with $a_n b_r \neq 0$. We define the resultant of $f(x)$ and $g(x)$ in terms of the Sylvester determinant $R(f,g)$ associated with $f(x)$ and $g(x)$. $R(f,g)$ is the determinant of an $(n+r) \times (n+r)$ matrix with the first r rows consisting of the coefficients of $f(x)$, where each of these rows contains one more leading 0 than its predecessor, and with the last n rows consisting of the coefficients of $g(x)$, where each of these rows contains one more leading 0 than its predecessor. Specifically, we may write*

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\ 0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}. \tag{2.1}$$

For example, if $f(x) = x^3 + x + 1$ and $g(x) = 2x^2 + x + 3$, then (2.1) becomes

$$R(f,g) = \begin{vmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 2 & 1 & 3 & 0 & 0 \\ 0 & 2 & 1 & 3 & 0 \\ 0 & 0 & 2 & 1 & 3 \end{vmatrix}.$$

Lemma. *Let $f(x)$ and $g(x) \in \mathbb{C}[x]$, and suppose that there is an α such that $f(\alpha) = g(\alpha) = 0$. Then $R(f,g) = 0$.*

Proof. Add to the ith row of the last column (the $(n+r)$th column) of the determinant on the right-hand side of (2.1) the product of the entry in the ith row and jth column with α^{n+r-j}. Then the first r entries in the last column become $\alpha^{r-1}f(\alpha), \alpha^{r-2}f(\alpha), \dots, f(\alpha)$ and the last n entries become $\alpha^{n-1}g(\alpha), \alpha^{n-2}g(\alpha), \dots, g(\alpha)$. By the conditions of the Lemma, these are all 0, and the result follows. ■

If $\alpha_1, \dots, \alpha_n$ are the roots of $f(x)$, one can show that

$$R(f,g) = a_n^r g(\alpha_1) \cdots g(\alpha_n). \tag{2.2}$$

The proof can be found in Uspensky [1]. We will use (2.2) to help deal with the possibility that $R(f,g) = 0$. (If 0 wasn't around, there wouldn't be nothing to worry about.) Observe that (2.2) implies the lemma and also the converse of the lemma. Thus, if $R(f,g) = 0$, then $f(x)$ and $g(x)$ have a root in common. We now show that the following algorithm works to determine whether a given polynomial $f(x)$ is Eisenstein.

---

*The appearance of the right-hand side of (2.1) is somewhat misleading. The entry a_0 in the first row, for example, is not necessarily in the same column as the entry b_0 in the first row consisting of the b_j's.

Algorithm. *Suppose that $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 2$. Calculate $R(f, f')$ (using the right-hand side of (2.1)). If $R(f, f') = 0$, then $f(x)$ is not Eisenstein with respect to any prime. If $R(f, f') \neq 0$, then factor it. For each prime p dividing $R(f, f')$, check to see if any of the translates $f(x+a)$, where $a \in \{0, 1, ..., p-1\}$, is in Eisenstein form with respect to the prime p. If such a prime p and such an a are such that $f(x+a)$ is in Eisenstein form with respect to p, then $f(x)$ is Eisenstein with respect to p. If no such prime p and no such a are such that $f(x+a)$ is in Eisenstein form with respect to p, then $f(x)$ is not Eisenstein with respect to any prime.*

In justifying the algorithm, we explain how one can use the resultant $R(f, f')$ to determine whether a polynomial $f(x)$ has a multiple factor (a factor which appears with multiplicity > 1) modulo some prime (which is unspecified). To see this, suppose that there is a prime p such that

$$f(x) \equiv g(x)^2 h(x) \pmod{p} \tag{2.3}$$

where $g(x)$ is of degree ≥ 1. Note that if for some integer a we have that $f(x+a)$ is in Eisenstein form with respect to the prime p, then $f(x) \equiv a_n(x-a)^n \pmod{p}$ so that one can take $g(x) = x - a$. Define $f_1(x) = g(x)^2 h(x)$ so that the coefficients of $f(x)$ and of $f'(x)$ are the same as the corresponding coefficients of $f_1(x)$ and $f_1'(x)$ all considered modulo p. In particular, $R(f, f') \equiv R(f_1, f_1') \pmod{p}$. Since

$$f_1'(x) = 2g(x)g'(x)h(x) + g(x)^2 h'(x) = g(x)\left(2g'(x)h(x) + g(x)h'(x)\right),$$

we get that each root of $g(x)$ is a root of $f_1(x)$ and of $f_1'(x)$. By the Lemma, we get that $R(f_1, f_1') = 0$. Hence, $R(f, f') \equiv 0 \pmod{p}$. Thus, p divides $R(f, f')$; and to determine if (2.3) holds for some prime p, we simply need to check whether it holds for each prime divisor p of $R(f, f')$. The fact that the algorithm works when $R(f, f') \neq 0$ is now fairly straight forward, but we need to justify that we can restrict our consideration of integers a to $a \in \{0, 1, \ldots, p-1\}$. For this purpose, we suppose that b is an integer for which $f(x+b)$ is in Eisenstein form with respect to some prime p and show that $f(x+a)$ is also for any

$a \equiv b \pmod{p}$. Since $f(x+b) \equiv f(x+a) \pmod{p}$, we simply need to justify that p^2 does not divide the constant term in $f(x+a)$. In other words, we want to show that $p^2 \nmid f(a)$. Writing $f(x+b) = \sum_{j=0}^{n} a'_j x^j$, we get that $p | a'_j$ for $j < n$ and $p^2 \nmid a'_0$. Writing $a = kp + b$ where k is an integer, we get that

$$f(a) \equiv f(kp+b) \equiv \sum_{j=0}^{n} a'_j k^j p^j \equiv kpa'_1 + a'_0 \equiv a'_0 \pmod{p^2}.$$

Thus, $f(a) \not\equiv 0 \pmod{p^2}$, completing what we set out to show (for the case $R(f,f') \neq 0$).

If $R(f,f') = 0$, the above all works except that every prime is a prime divisor of $R(f,f')$ so it is not reasonable to consider all the prime divisors of $R(f,f')$. But observe that (2.2) implies that $f(x)$ and $f'(x)$ have a root in common. Hence, in this case, $f(x)$ must have a multiple root (the reader should justify this) so that $f(x)$ is reducible over $\mathbb{Q}$ (see Problem (1.8)). In particular, by Theorem 5, we can conclude that $f(x)$ cannot be Eisenstein with respect to any prime.

Example. Consider $f(x) = x^4 + 2x - 1$, and suppose that we wish to find every prime p such that $f(x)$ is Eisenstein with respect to p. We first calculate $R(f,f')$ by using (2.1). To do this somewhat efficiently, we multiply below the first row by -4 and add it to the fourth row. Observe that we will get the same result in the fifth row with an extra leading 0 if we multiply the second row by -4 and add it to the fifth row. Similarly, we can obtain the same result in the sixth row (as the fourth row) with 2 extra leading 0's by considering the third row. We get that

$$R(f,f') = \begin{vmatrix} 1 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & -1 \\ 4 & 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 4 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 4 & 0 & 0 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 2 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 2 & -1 \\ 0 & 0 & 0 & -6 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & -6 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & -6 & 4 \\ 0 & 0 & 0 & 4 & 0 & 0 & 2 \end{vmatrix}.$$

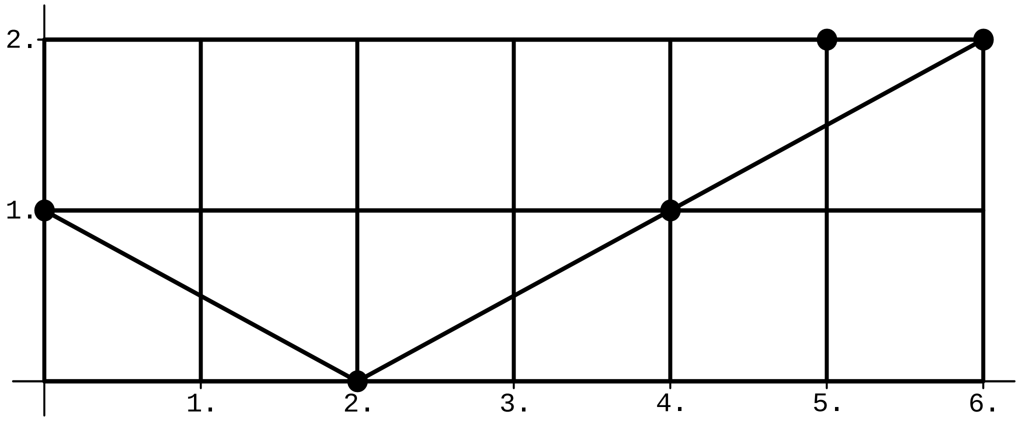
A direct computation now gives

$$R(f,f') = \begin{vmatrix} -6 & 4 & 0 & 0 \\ 0 & -6 & 4 & 0 \\ 0 & 0 & -6 & 4 \\ 4 & 0 & 0 & 2 \end{vmatrix} = -6 \times 72 - 4 \times 64 = -688.$$

Since $688 = 2^4 \times 43$, we only need to deal with the primes 2 and 43. We make use of exercise (2.2). Observe that 2 divides $f(1)$, and so we consider $f(x+1) = x^4 + 4x^3 + 6x^2 + 6x + 2$. Thus, $f(x)$ is Eisenstein with respect to the prime 2 (and, hence, $f(x)$ is irreducible). Observe that 43 divides $f(3)$ but that $f'(3) = 4 \times 27 + 2 = 110$ is not divisible by 43. Thus, $f(x)$ is not Eisenstein with respect to the prime 43. Hence, 2 is the only prime p such that $f(x)$ is Eisenstein with respect to p. Alternatively, we note that Problem (2.7) could have been used to determine that $f(x)$ is not Eisenstein with respect to 43.

In this section, we have considered the problem of determining whether a polynomial $f(x) \in \mathbb{Z}[x]$ can under a translation be shown to be irreducible over $\mathbb{Q}$ by the Schönemann - Eisenstein criterion. In general, if $f(x)$ and $g(x) \in \mathbb{Z}[x]$ and $f(g(x))$ is irreducible over $\mathbb{Q}$, then $f(x)$ is irreducible over $\mathbb{Q}$; hence, it is reasonable to attempt to determine whether a given $f(x)$ is irreducible by applying the Schönemann - Eisenstein criterion after composing $f(x)$ with another polynomial. We leave further consideration of this idea as an exercise (Problem (2.4)).

2.3. In this section, we explore the concept of Newton polygons. Some discussion of Newton polygons can be found in Dorwart [1], Weiss [1], and Chao [1]. Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_0 a_n \neq 0$. Let p be a prime. For $j \in \{0, \ldots, n\}$, we define $x_j = j$ and define $y_j \in \mathbb{Z}^+ \cup \{0\} \cup \{+\infty\}$ to be the exponent of p in the largest power of p dividing a_{n-j}. In other words, $p^{y_j} | a_{n-j}$ and $p^{y_j+1} \nmid a_{n-j}$ if $a_{n-j} \neq 0$ and $y_j = +\infty$ in the case that $a_{n-j} = 0$. Thus, we get a set of points $S = \{(x_0, y_0), \ldots, (x_n, y_n)\}$ in the extended plane. We consider the lower edges along the convex hull of these points. The left-most edge has one endpoint being (x_0, y_0) and the right-most edge has (x_n, y_n) as an endpoint. The endpoints of every edge belong to the set S. If (x_i, y_i) and (x_j, y_j) are the 2 endpoints of such an edge, then every point (x_u, y_u) with $i < u < j$ lies on or above the line passing through (x_i, y_i) and (x_j, y_j). The polygonal path formed by these edges is called the Newton polygon associated with $f(x)$. To clarify the dependence of this polygonal path on p, we will sometimes refer to it as the Newton polygon for $f(x)$ with respect to p. For example, if $f(x) = 2x^6 + x^4 + 2x^2 + 4x + 4$, then the Newton polygon for $f(x)$ with respect to the prime 2 consists of 2 edges, one from $(0, 1)$ to $(2, 0)$ and the other from $(2, 0)$ to $(6, 2)$.



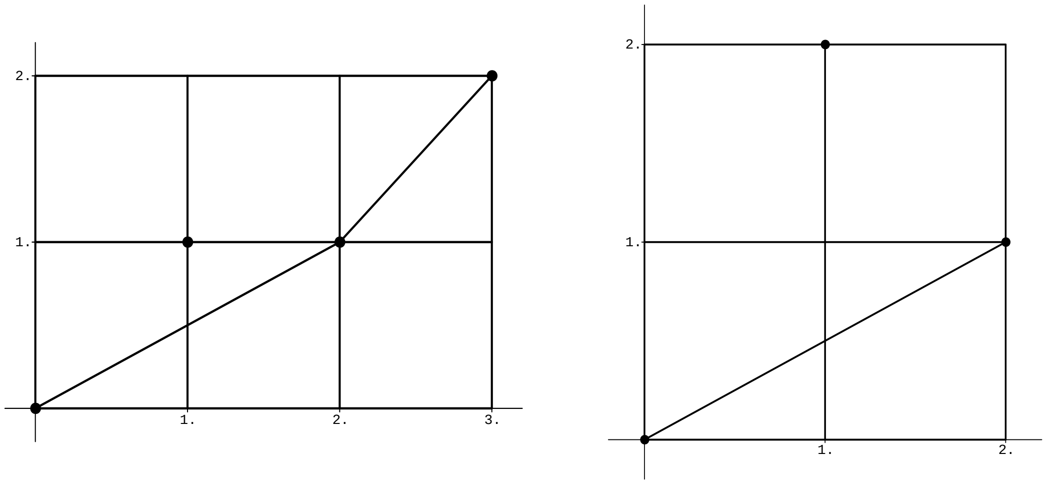
The Newton polygon for $f(x) = 2x^6 + x^4 + 2x^2 + 4x + 4$

Observe that the slope of the edges are always increasing when calculated from the left-most edge to the right-most edge. The following theorem is due to Dumas [1].

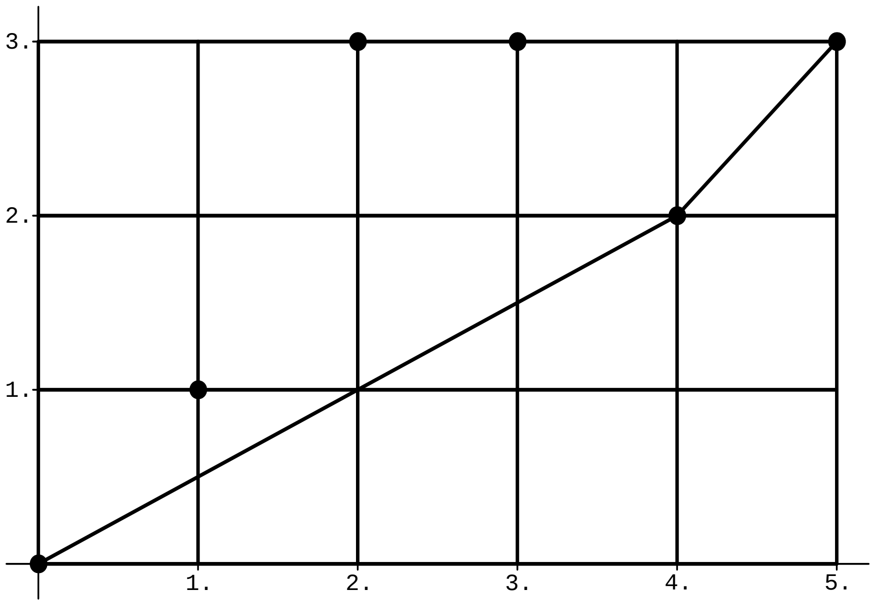
Theorem 6. *Let $g(x)$ and $h(x)$ be in $\mathbb{Z}[x]$ with $g(0)h(0) \neq 0$, and let p be a prime. Let k be a non-negative integer such that p^k divides the leading coefficient of $g(x)h(x)$ but p^{k+1} does not. Then the edges of the Newton polygon for $g(x)h(x)$ with respect to p can be formed by constructing a polygonal path beginning at $(0, k)$ and using translates of the edges in the Newton polygons for $g(x)$ and $h(x)$ with respect to the prime p, using exactly one translate for each edge of the Newton polygons for $g(x)$ and $h(x)$. Necessarily, the translated edges are translated in such a way as to form a polygonal path with the slopes of the edges increasing.*

To help explain the statement of the theorem, we consider a couple of examples. We take $p = 3$ and consider $g(x) = x^3 + 3x^2 + 12x + 9$ and $h(x) = 2x^2 + 9x + 3$. Then the Newton polygon for $g(x)$ consists of 2 edges, one with slope $1/2$ and the other with slope 1; the Newton polygon for $h(x)$ consists of 1 edge having slope $1/2$; and the Newton polygon for $g(x)h(x) = 2x^5 + 15x^4 + 54x^3 + 135x^2 + 117x + 27$ consists of 2 edges, one with slope $1/2$ and the other with slope 1. The translates of the edges of the Newton polygons for

$g(x)$ and $h(x)$ with slope $1/2$ have merged to form a single edge in the Newton polygon for $g(x)h(x)$. We emphasize that, for our purposes, when referring to the "edges" of a Newton polygon, we shall not allow 2 different edges to have the same slope.



The Newton polygons for $g(x) = x^3 + 3x^2 + 12x + 9$ and $h(x) = 2x^2 + 9x + 3$



The Newton polygon for $g(x)h(x) = 2x^5 + 15x^4 + 54x^3 + 135x^2 + 117x + 27$

As a second example, we consider a prime p and an $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ which is in Eisenstein form with respect to p (say with $a_n \neq 0$). Then in our description of the Newton polygon for $f(x)$ above, we get that $(x_0, y_0) = (0, 0)$, $(x_n, y_n) = (n, 1)$, and every other (x_j, y_j) lies on or above the line passing through (x_0, y_0) and (x_n, y_n). Observe that

Theorem 6 would imply that $f(x)$ is irreducible over $\mathbb{Q}$ since if $f(x) = g(x)h(x)$ with $g(x)$ and $h(x) \in \mathbb{Z}[x]$ and with $\deg g(x)$ and $\deg h(x) > 0$, then the Newton polygon for $f(x)$ with respect to p would be able to be represented as translates of 2 or more edges. The latter is impossible since the only lattice points (points with integral coordinates) on the Newton polygon for $f(x)$ are its endpoints (x_0, y_0) and (x_n, y_n). Thus, Theorem 6 can be viewed as a generalization of Theorem 5.

Proof of Theorem 6. We write $g(x) = \sum_{j=0}^{r} b_j x^j$ and $h(x) = \sum_{j=0}^{s} c_j x^j$ with $b_r \neq 0$ and $c_s \neq 0$ and $f(x) = g(x)h(x) = \sum_{j=0}^{n} a_j x^j$ where $a_n \neq 0$. Thus, $n = r + s$. For $j \in \{0, \dots, n\}$, we represent the exponent in the largest power of p (possibly $+\infty$) dividing a_{n-j} with y_j; for $j \in \{0, \dots, r\}$, we represent the exponent in the largest power of p dividing b_{r-j} with y'_j; and for $j \in \{0, \dots, s\}$, we represent the exponent in the largest power of p dividing c_{s-j} with y''_j. We consider an edge of the Newton polygon for $g(x)$ (with respect to the prime p). Let (k_1, u_1) and (k_2, u_2) denote the endpoints of such an edge with $k_2 > k_1$. Thus, $u_1 = y'_{k_1}$ and $u_2 = y'_{k_2}$. Observe that the equation of the line passing through (k_1, u_1) and (k_2, u_2) is

$$(u_2 - u_1)x - (k_2 - k_1)y = (u_2 - u_1)k_1 - (k_2 - k_1)u_1. \tag{2.4}$$

Since every point (i, y'_i) associated with a coefficient of $g(x)$ lies on or above this line, we get that

$$(u_2 - u_1)i - (k_2 - k_1)y'_i \leq (u_2 - u_1)k_1 - (k_2 - k_1)u_1 \quad \text{for } i \in \{0, \dots, r\}. \tag{2.5}$$

Furthermore, equality can occur in (2.5) only if $k_1 \leq i \leq k_2$. Consider the right-most edge (if such an edge exists) of the Newton polygon for $h(x)$ which has a slope which is $< (u_2 - u_1)/(k_2 - k_1)$, the slope of the line given by (2.4). Let (m_1, v_1) denote the right endpoint of that edge. If no such edge exists, then set $m_1 = 0$ and $v_1 = y''_0$. In any case, $v_1 = y''_{m_1}$. In the case that there is an edge on the Newton polygon for $h(x)$ which has (m_1, v_1) as its left endpoint, we set (m_2, v_2) to be the right endpoint of that edge. Thus, $m_2 > m_1$ (when m_2 is defined). Observe that if (m_2, v_2) is not defined or if the slope of the line passing through (m_1, v_1) and (m_2, v_2) is $> (u_2 - u_1)/(k_2 - k_1)$, then we need to show that the edge joining (k_1, u_1) and (k_2, u_2) on the Newton polygon for $g(x)$ can be translated to an edge of the Newton polygon for $f(x)$ with endpoints $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_1, u_2 + v_1)$. On the other hand, if (m_2, v_2) is defined and the slope of the line passing through (m_1, v_1) and (m_2, v_2) is equal to $(u_2 - u_1)/(k_2 - k_1)$, then we need to show that the edge joining (k_1, u_1) and (k_2, u_2) on the Newton polygon for $g(x)$ and the edge joining (m_1, v_1) and (m_2, v_2) on the Newton polygon for $h(x)$ can be translated to an edge of the Newton polygon for $f(x)$ with endpoints $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_2, u_2 + v_2)$.

Let $t \in \{0, \ldots, n\}$ and consider $i \in \{0, \ldots, r\}$ and $j \in \{0, \ldots, s\}$ such that $t = i + j$. The definition of (m_1, v_1) implies that point (j, y''_j) lies on or above the line passsing through (m_1, v_1) with slope $(u_2 - u_1)/(k_2 - k_1)$. In other words,

$$(u_2 - u_1)j - (k_2 - k_1)y''_j \leq (u_2 - u_1)m_1 - (k_2 - k_1)v_1. \tag{2.6}$$

Furthermore, equality can occur in (2.6) if and only if either (i) $(j, y''_j) = (m_1, v_1)$ or (ii) (m_2, v_2) exists, the line passing through (m_1, v_1) and (m_2, v_2) has slope equal to $(u_2 - u_1)/(k_2 - k_1)$, and (j, y''_j) is on the line segment joining (m_1, v_1) and (m_2, v_2). Combining (2.5) and (2.6), we get that

$$(u_2 - u_1)(i + j) - (k_2 - k_1)(y'_i + y''_j) \leq (u_2 - u_1)(k_1 + m_1) - (k_2 - k_1)(u_1 + v_1). \tag{2.7}$$

Recall that $t = i + j$. We view t as fixed and consider first the case that (m_2, v_2) is not defined or the slope of the line passing through (m_1, v_1) and (m_2, v_2) is $> (u_2 - u_1)/(k_2 - k_1)$. If equality holds in (2.7), then (i) must hold. For the moment, we consider $t = k_1 + m_1$. We get that equality holds in (2.7) if and only if $i = k_1$ and $j = m_1$. Since $t = i + j = k_1 + m_1$ is fixed, (2.7) implies that $y'_i + y''_j$ obtains its minimum when $i = k_1$ and $j = m_1$ and for no other values of i and j. Since $f(x) = g(x)h(x)$, we get that

$$a_{n-t} = \sum_{i+j=t} b_{r-i}c_{s-j}. \tag{2.8}$$

Each term $b_{r-i}c_{s-j}$ is divisible by $p^{y'_i + y''_j}$ (by the definition of y'_i and y''_j). Thus, the fact that the minimality of $y'_i + y''_j$ occurs when $i = k_1$ and $j = m_1$ implies that $p^{u_1+v_1}$ divides

a_{n-t}. Also, $p^{u_1+v_1+1}$ divides every term $b_{r-i}c_{s-j}$ in (2.8) except for the term $b_{r-k_1}c_{s-m_1}$. Thus, $p^{u_1+v_1}$ must exactly divide a_{n-t}. In other words,

$$y_{k_1+m_1} = u_1 + v_1 = y'_{k_1} + y''_{m_1}. \tag{2.9}$$

Now we consider $t = k_2 + m_1$. From (2.7), $y'_i + y''_j$ obtains its minimum precisely when $i = k_2$ and $j = m_1$. Instead of (2.9), we obtain that

$$y_{k_2+m_1} = u_2 + v_1 = y'_{k_2} + y''_{m_1}.$$

To show that the segment joining $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_1, u_2 + v_1)$ actually forms an edge of the Newton polygon for $f(x)$, it remains to show for $t \in \{0, \ldots, n\}$ that (t, y_t) is on or above the line passing through (k_1+m_1, u_1+v_1) and (k_2+m_1, u_2+v_1) and that if (t, y_t) is on the line, then $k_1 + m_1 \le t \le k_2 + m_1$. For $t \in \{0, \ldots, n\}$, observe that (2.8) implies that

$$y_t \ge \min_{i+j=t} \{y'_i + y''_j\}.$$

Fix $t \in \{0, \ldots, n\}$, and fix $i \in \{0, \ldots, r\}$ and $j \in \{0, \ldots, s\}$ so that $t = i+j$ and $y_t \ge y'_i+y''_j$. Then from (2.7), we get that

$$\begin{aligned}(u_2 - u_1)t - (k_2 - k_1)y_t &\le (u_2 - u_1)(i + j) - (k_2 - k_1)(y'_i + y''_j)\\ &\le (u_2 - u_1)(k_1 + m_1) - (k_2 - k_1)(u_1 + v_1).\end{aligned} \tag{2.10}$$

This implies that (t, y_t) is on or above the line passing through $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_1, u_2 + v_1)$. Recalling that (2.7) was a consequence of (2.5) and (2.6), we see that if equality occurs in (2.10), then $k_1 \le i \le k_2$ and $j = m_1$. In other words, if equality occurs in (2.10), then $k_1 + m_1 \le t \le k_2 + m_1$. This establishes what we set out to show for the case that (m_2, v_2) is not defined or the slope of the line passing through (m_1, v_1) and (m_2, v_2) is $> (u_2 - u_1)/(k_2 - k_1)$.

Suppose now that (m_2, v_2) exists and the slope of the line passing through (m_1, v_1) and (m_2, v_2) is equal to $(u_2 - u_1)/(k_2 - k_1)$. In this case, if equality holds in (2.6) or (2.7), then

$m_1 \leq j \leq m_2$. If equality holds in (2.7), we also have that $k_1 \leq i \leq k_2$. If $t = k_1 + m_1$, then either $i \leq k_1$ or $j \leq m_1$. Thus, we get that equality holds in (2.7) if and only if $i = k_1$ and $j = m_1$ as before, and (2.9) follows. If $t = k_2 + m_2$, then either $i \geq k_2$ or $j \geq m_2$. In this case, we get that equality holds in (2.7) if and only if $i = k_2$ and $j = m_2$. Thus, we obtain that

$$y_{k_2+m_2} = u_2 + v_2 = y'_{k_2} + y''_{m_2}.$$

As before, we get that (2.10) follows for every $t \in \{0, \ldots, n\}$. Here, if equality holds, then $k_1 \leq i \leq k_2$ and $m_1 \leq j \leq m_2$ so that $k_1 + m_1 \leq t \leq k_2 + m_2$. It follows that the segment joining $(k_1 + m_1, u_1 + v_1)$ and $(k_2 + m_2, u_2 + v_2)$ forms an edge of the Newton polygon for $f(x)$. This completes the proof. ■

The following corollary summarizes important information given by Theorem 6.

Corollary. *Let $f(x) \in \mathbb{Z}[x]$ be of degree n with $f(0) \neq 0$, and suppose that there are polynomials $g_1(x), \ldots, g_r(x) \in \mathbb{Z}[x]$ (not necessarily irreducible) such that $f(x) = g_1(x) \cdots g_r(x)$. Let p be a prime, and let $(x'_0, y'_0), (x'_1, y'_1), \ldots, (x'_k, y'_k)$, with $x'_0 = 0 < x'_1 < \cdots < x'_k = n$, be the complete list of lattice points on the Newton polygon for $f(x)$ with respect to p. For $j \in \{1, \ldots, k\}$, let $b_j = x'_j - x'_{j-1}$. Then there exist $\epsilon_{i,j} \in \{0, 1\}$, where $i \in \{1, \ldots, r\}$ and $j \in \{1, \ldots, k\}$, such that for each j, there is one and only one i for which $\epsilon_{i,j} = 1$, and such that for each i,*

$$\deg g_i(x) = \sum_{j=1}^{k} \epsilon_{i,j} b_j.$$

Example 1. Let p be a prime. Suppose that $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is such that $p \nmid a_n$, $p | a_j$ for $j \in \{0, \ldots, n-1\}$, and $p^2 \nmid a_1$. We show that either $f(x)$ is irreducible over $\mathbb{Q}$ or $f(x)$ factors as the product of a linear polynomial and an irreducible polynomial over $\mathbb{Q}$ of degree $n - 1$. If $p^2 \nmid a_0$, then we can apply the Schönemann - Eisenstein Criterion to conclude that $f(x)$ is irreducible over $\mathbb{Q}$. Hence, the result follows trivially in this case. Similarly, if $a_0 = 0$, then $f(x) = xg(x)$ and $g(x)$ is irreducible over $\mathbb{Q}$ by the Schönemann-Eisenstein Criterion so that the result holds. Suppose now that $p^2 | a_0$ and $a_0 \neq 0$. Then the

Newton polygon with respect to p contains exactly 2 segments, one from $(0,0)$ to $(n-1,1)$ and the other from $(n-1,1)$ to (n,m) where m is the largest power of p dividing a_0. Thus, Theorem 6 or its Corollary implies that either $f(x)$ is irreducible over $\mathbb{Q}$ or $f(x)$ factors as the product of a linear polynomial and an irreducible polynomial over $\mathbb{Q}$ of degree $n-1$, which is what we set out to show.

Example 2. We show that $f(x) = x^5 + 2x^3 + 2x + 4$ is irreducible. By Problem (1.9), the only possible rational roots of $f(x)$ are ± 1, ± 2, or ± 4. Clearly, $f(x)$ has no positive roots since all of its non-zero coefficients are positive. Also, $f(-1) \equiv 1 \pmod 2$ and $f(-4) \equiv 4 \pmod 8$ imply that -1 and -4 are not roots of $f(x)$. Finally, since $f(-2) = -32 - 16 - 4 + 4 \neq 0$, $f(x)$ has no rational roots. Using $p = 2$ in the previous example, we can conclude that $f(x)$ is irreducible.

We emphasize that the following strengthening of the Corollary is not true. (We do this partially to clear up a misprint which occurs in the literature in Grosswald [2, p. 107, Theorem A′].) Instead of considering every lattice point on the Newton polygon for $f(x)$ with respect to p, suppose that we only consider those lattice points (x'_j, y'_j) which correspond to the $(x_j, y_j) = (j, y_j)$ described at the beginning of this section in our construction of the Newton polygon for $f(x)$. The idea then is to hope for the same conclusion as in the Corollary with the new list of x'_j's and, hence, b_j's. Such a conclusion, however, does not hold. We have seen an example where this conclusion would not follow, namely when we considered the product of $g(x) = x^3+3x^2+12x+9$ and $h(x) = 2x^2+9x+3$ and the prime $p = 3$. Another easier example is given by $f(x) = x^2 + 4x + 4 = (x+2)^2$ with $p = 2$.

Theorem 6 is an important result which has found applications to some classical polynomials. We will explore some of these later. We observe that the theorem is limited by the fact that it derives all of its information from simply examining the primes dividing the non-zero coefficients of a given polynomial $f(x)$. Other important information is left untouched. We will see in the next chapter, for example, that examining the approximate location of the complex roots of $f(x)$ often aids in determining whether it is irreducible.

2.4. In this section, we show how Newton polygons can be used to establish the following result due to I. Schur [1].

Theorem 7. *Let n be a positive integer, and let $a_0, a_1, \ldots, a_n$ denote arbitrary integers with $|a_0| = |a_n| = 1$. Then*

$$a_n \frac{x^n}{n!} + a_{n-1} \frac{x^{n-1}}{(n-1)!} + \cdots + a_1 x + a_0$$

is irreducible over the rationals.

For convenience, we make use of the following p-adic notation. For p a prime (which will be clear form the context) and m a non-zero integer, we define $\nu(m)$ as the non-negative integer such that $p^{\nu(m)} | m$ and $p^{\nu(m)+1} \nmid m$. In the case that $m = 0$, we define $\nu(m)$ as $+\infty$. Also, we view $+\infty$ as being a quantitiy greater than any integer.

Our use of Newton polygons for obtaining Theorem 7 is summarized by the following Lemma.

Lemma 1. *Let k and ℓ be integers with $k > \ell \geq 0$. Suppose $g(x) = \sum_{j=0}^{n} b_j x^j \in \mathbb{Z}[x]$ and p is a prime such that $p \nmid b_n$, $p | b_j$ for all $j \in \{0, 1, \ldots, n-\ell-1\}$, and the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Then for any integers $a_0, a_1, \ldots, a_n$ with $|a_0| = |a_n| = 1$, the polynomial $f(x) = \sum_{j=0}^{n} a_j b_j x^j$ cannot have a factor with degree in the interval $[\ell + 1, k]$.*

Proof. We first consider the case that $a_j = 1$ for all $j \in \{0, 1, \ldots, n\}$ so that $f(x) = g(x)$. Assume $f(x)$ in this case has a factor with degree in $[\ell + 1, k]$. Then there exist $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ with $f(x) = u(x)v(x)$ and $\ell + 1 \leq \deg u(x) \leq k$. We consider the Newton polygon for $f(x) = g(x)$ with respect to p. Since the slopes of the edges of the Newton polygon for $f(x)$ increase from left to right, the conditions of the lemma imply that each edge has slope in $[0, 1/k)$. The left-most edge of the Newton polygon may have slope 0. For now, we consider an edge of the Newton polygon which does not have slope 0. Let

(a, b) and (c, d) be 2 lattice points on such an edge. Then the slope of the line passing through these points is the slope of the edge so that

$$\frac{1}{|c-a|} \leq \frac{|d-b|}{|c-a|} < \frac{1}{k}.$$

Hence, $|c-a| > k$. In other words, any 2 lattice points on an edge with non-zero slope of the Newton polygon for $f(x)$ with respect to p have their $x-$coordinates separated by a distance $> k$. Since $\deg u(x) \leq k$, we get that translates of the edges of the Newton polygon for $u(x)$ with respect to p cannot be found within those edges of the Newton polygon for $f(x)$ with respect to p which have non-zero slope. In other words, the left-most edge of the Newton polygon for $f(x)$ must have slope 0 and length $\geq \deg u(x)$. The conditions of the lemma imply that $\nu(b_{n-j}) \geq 1$ for $j \in \{\ell+1, \ell+2, \ldots, n\}$ so that if the left-most edge of the Newton polygon for $f(x)$ with respect to p has slope 0, then it has length $\leq \ell < \deg u(x)$, giving a contradiction.

Next, we consider the general case of arbitrary integers $a_0, a_1, \ldots, a_n$ with $a_0 = \pm 1$ and $a_n = \pm 1$. The conditions on a_0 and a_n imply that the left and right-most endpoints of the Newton polygon for $f(x)$ with respect to p are the same as the left and right-most endpoints of the Newton polygon for $g(x)$ with respect to p, respectively. Also, $p|a_j b_j$ for all $j \in \{0, 1, \ldots, n-\ell-1\}$. All the edges of the Newton polygon for $g(x)$ with respect to p lie above or on the line containing the right-most edge. The same statement holds for $f(x)$ in place of $g(x)$. Note that $\nu(a_j b_j) \geq \nu(b_j)$ for all $j \in \{0, 1, \ldots, n\}$. Hence, we also get that all the edges of the Newton polygon for $f(x)$ lie above or on the line containing the right-most edge of the Newton polygon for $g(x)$. Since the right-most endpoint for each of these 2 Newton polygons is the same, we deduce that the slope of the right-most edge of the Newton polygon for $f(x)$ is less than or equal to the slope of the right-most edge of the Newton polygon for $g(x)$. Therefore, the right-most edge of the Newton polygon for $f(x)$ must have slope $< 1/k$. Thus, $f(x)$ satisfies the same conditions imposed on $g(x)$ in the statement of the lemma so that by appealing to the first part of the proof, the lemma follows. ■

We will also need the following generalization due to Sylvester [1] of Bertrand's postulate that for every integer $m \geq 1$, there is a prime in the interval $(m, 2m]$ (take $k = m$ below). We do not give its proof here but note that an elementary argument has been obtained by Erdős [1].

Lemma 2. *Let m and k be positive integers with $m \geq k$. Then there is a prime $p \geq k+1$ which divides one of the numbers $m+1, m+2, \ldots, m+k$.*

Proof of Theorem 7. To make use of Lemma 1, we consider

$$g(x) = \sum_{j=0}^{n} \frac{n!}{j!} x^j \qquad \text{and} \qquad f(x) = \sum_{j=0}^{n} a_j \frac{n!}{j!} x^j.$$

It suffices to show that $f(x)$ is irreducible over the integers. Assume $f(x)$ is reducible. Let k be the smallest degree of an irreducible factor of $f(x)$. Necessarily, $k \leq n/2$. Thus, $n - k \geq k$ so that Lemma 2 implies there is a prime $p \geq k+1$ dividing $n - \ell$ for some $\ell \in \{0, 1, \ldots, k-1\}$. We consider the Newton polygon for $g(x)$ with respect to such a prime p. For $j \in \{0, 1, \ldots, n - \ell - 1\}$, we get that $n!/j!$ is divisible by $n - \ell$ and, hence, p. To obtain a contradiction and thereby prove the theorem, Lemma 1 implies that it suffices to show that the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$. Observe that the slope of the right-most edge can be determined by

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(n!) - \nu(n!/j!)}{j} \right\}.$$

Fix $j \in \{1, \ldots, n\}$. Note that $p^{\nu(n!) - \nu(n!/j!)}$ is the largest power of p which divides $j!$. Let r be the non-negative integer for which $p^r \leq n < p^{r+1}$. Then for $j \in \{1, \ldots, n\}$,

$$\nu(n!) - \nu(n!/j!) = \left[\frac{j}{p}\right] + \left[\frac{j}{p^2}\right] + \cdots + \left[\frac{j}{p^r}\right] \leq j\left(\frac{1}{p} + \cdots + \frac{1}{p^r}\right) = j\,\frac{p^r - 1}{p^r(p-1)}.$$

Therefore,

$$\max_{1 \leq j \leq n} \left\{ \frac{\nu(n!) - \nu(n!/j!)}{j} \right\} \leq \frac{p^r - 1}{p^r(p-1)} < \frac{1}{p-1}.$$

Recall that $p \geq k+1$. Hence, the right-most edge of the Newton polygon for $g(x)$ with respect to p has slope $< 1/k$, and the proof is complete. ■

PROBLEMS

(2.1) Using equation (2.1) or equation (2.2), show the following:

(i) If $f(x)$, $g_1(x)$, and $g_2(x)$ are non-zero polynomials in $\mathbb{C}[x]$, then $R(f, g_1g_2) = R(f, g_1)R(f, g_2)$. (Here, g_1g_2 means the product $g_1(x)g_2(x)$.)

(ii) If $f(x) \in \mathbb{C}[x]$ is of degree ≥ 1 and $g(x) = f(x + a)$ where $a \in \mathbb{C}$, then $R(f, f') = R(g, g')$.

(2.2) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_n \neq 0$ and $n \geq 2$, and let p be a prime. Suppose that there is an integer a such that $p|f(a)$. Prove the following:

(i) $f(x)$ is Eisenstein with respect to p if and only if $f(x+a)$ is in Eisenstein form with respect to p.

(ii) If $p^2|f(a)$, then $f(x)$ is not Eisenstein with respect to the prime p.

(iii) If $f(x)$ is Eisenstein with respect to the prime p, then $p|f^{(m)}(a)/m!$ for every $m \in \{1, \ldots, n-1\}$.

(2.3) For each of the following choices for $f(x)$, determine every prime p such that $f(x)$ is Eisenstein with respect to p.

(a) $f(x) = x^3 + x + 1$

(b) $f(x) = x^3 + x^2 - 2x - 1$

(c) $f(x) = x^3 + x^2 + x + 5$

(d) $f(x) = x^3 - x^2 + 4x + 2$

(2.4) Let $f(x) \in \mathbb{Z}[x]$. Suppose that there exists a $g(x) \in \mathbb{Z}[x]$ such that $f(g(x))$ is in Eisenstein form. Prove that $f(x)$ is Eisenstein. (Hint: Let $a = g(0)$ and prove that $f(x + a)$ is in Eisenstein form.)

(2.5) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $a_n \neq 0$ and $n \geq 2$. Let p be a prime which does not divide n. Suppose that a is an integer for which $f(x + a)$ is in Eisenstein form with respect to the prime p. Prove that $a \equiv -a_{n-1}(na_n)^{-1} \pmod{p}$.

(2.6) Suppose that $f(x) \in \mathbb{Z}[x]$ is Eisenstein with respect to a prime p. Prove that $f(x)$ has exactly one root modulo p.

(2.7) (a) Let $f(x) \in \mathbb{Z}[x]$ of degree $n \geq 1$. Suppose that $f(x)$ is Eisenstein with respect to a prime p. Using Problem (2.1) (ii), prove that $p^{n-1} | R(f, f')$.

(b) If in part (a) one also has that $p|n$, prove that $p^n | R(f, f')$.

(2.8) By considering Newton polygons with respect to 2 different primes, prove that $x^5 \pm 6x^4 \pm 6x^3 \pm 24x \pm 72$ is irreducible for any of the 16 combinations of the $\pm$ signs.

(2.9) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, and let p be a prime.

(a) Let k be an integer relatively prime to n. Suppose that $p \nmid a_n$, $p^k | a_j$ for $j \in \{0, 1, \ldots, n-1\}$, and $p^{k+1} \nmid a_0$. Prove that $f(x)$ is irreducible over $\mathbb{Q}$.

(b) Let k be such that $p^k | a_0$ and $p^{k+1} \nmid a_0$. Suppose that $p \nmid a_n$ and that for each $j \in \{1, 2, \ldots, n-1\}$ we have $p^{e(j)} | a_j$ for some positive integer $e(j)$ satisfying $ne(j) + kj \geq kn$. Prove that $f(x)$ factors in $\mathbb{Q}[x]$ as a product of irreducible polynomials each with degree a multiple of $n/\gcd(n, k)$.

(2.10) Prove that if $f(x)$ is Eisenstein with respect to a prime p, then $f(x)$ is irreducible modulo p^2. In other words, prove that if such an $f(x)$ is of degree n and $f(x) \equiv g(x)h(x) \pmod{p^2}$ for some $g(x)$ and $h(x)$ in $\mathbb{Z}[x]$ of degrees r and s, respectively, with $r + s = n$, then either $r = 0$ or $s = 0$.

(2.11) Show that we can deduce the irreducibility of

$$\frac{x^{19}}{20!} + \frac{x^{18}}{19!} + \frac{x^{17}}{18!} + \cdots + \frac{x^2}{3!} + \frac{x}{2!} + 1$$

over the rationals by multiplying the polynomial by 20! and considering its Newton polygons with respect to 19 and 5.

(2.12) For n an integer ≥ 2, define $f_n(x) = \left((x+1)^n - x^n - 1\right)/x$.

(a) Suppose α is a root of $f_n(x)$. Explain why $1/\alpha$ is a root of $f_n(x)$.

(b) Let $n = 2p$, where p is an odd prime. Consider the Newton polygon for $f_n(x)$ with respect to p and show that either $f_n(x)$ is irreducible over the rationals or $f_n(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ of degree $p-1$ which are irreducible over the rationals.

(c) Assume $f_n(x) = g(x)h(x)$ in part (b) (so $n = 2p$ and $g(x)$ and $h(x)$ are polynomials in $\mathbb{Z}[x]$ of degree $p-1$ which are irreducible over the rationals). We may suppose further that the leading coefficients of $g(x)$ and $h(x)$ are positive (why?). Show that the content of $g(x)$ and the content of $h(x)$ are both 1. Also, show that the constant terms of $g(x)$ and $h(x)$ are both positive.

(d) Assume $f_n(x) = g(x)h(x)$ in part (b). One can obtain a little more information from the Newton polygons considered in part (b). Show that if α is a root of $g(x)$, then $1/\alpha$ is NOT a root of $g(x)$.

(e) Again, assume $f_n(x) = g(x)h(x)$ in part (b). Show that $h(x) = x^{p-1}g(1/x)$.

(f) Show that if $n = 2p$ where p is an odd prime, then $f_n(x)$ is irreducible. In other words, show that the situation in part (e) cannot occur. (Hint: Let $x = 1$.)

(Comment: It may be the case that $f_n(x)$ is irreducible over the rationals for every even positive integer n.)