§2.2 Eisenstein Polynomials

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 2.1.1 that if $f(x)$ is Eisenstein with respect to a prime p, then $f(x)$ is irreducible over $\mathbb{Q}$ (see Exercise (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 $n \geq 1$, $r \geq 1$ and $a_n b_r \neq 0$. We define the resultant of $f(x)$ and $g(x)$ in terms of the Sylvester determinant $R(f,g)$ associated with $f(x)$ and $g(x)$. The resultant $R(f,g)$ 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 have [1]

$$
R(f,g) = \begin{vmatrix}
a_n & a_{n-1} & a_{n-2} & \dots & a_0 & 0 & 0 & \dots & 0 \\
0 & a_n & a_{n-1} & \dots & a_1 & a_0 & 0 & \dots & 0 \\
0 & 0 & a_n & \dots & a_2 & a_1 & a_0 & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\
b_r & b_{r-1} & b_{r-2} & \dots & b_0 & 0 & 0 & \dots & 0 \\
0 & b_r & b_{r-1} & \dots & b_1 & b_0 & 0 & \dots & 0 \\
0 & 0 & b_r & \dots & b_2 & b_1 & b_0 & \dots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots
\end{vmatrix}. \tag{2.2.1}
$$

For example, if $f(x) = x^3 + x + 1$ and $g(x) = 2x^2 + x + 3$, then (2.2.1) becomes

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

[1] The appearance of the right-hand side of (2.2.1) 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.

Lemma 2.2.1. *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 (2.2.1) 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 $\alpha^{r-1}f(\alpha), \alpha^{r-2}f(\alpha), \ldots, f(\alpha)$ and the last n entries become $\alpha^{n-1}g(\alpha), \alpha^{n-2}g(\alpha), \ldots, g(\alpha)$. By the conditions of the lemma, these are all 0, and the result follows. ∎

Before continuing, it is of interest to point out that the above proof can be modified slightly to obtain another result of interest. We replace the role of α above with a variable x, adjusting the determinant in (2.2.1) so that the right-most column consists of the entries

$$x^{r-1}f(x), x^{r-2}f(x), \ldots, f(x), x^{n-1}g(x), x^{n-2}g(x), \ldots, g(x). \tag{2.2.2}$$

The other entries in (2.2.1) remain untouched and, hence, are coefficients of the polynomials $f(x)$ and $g(x)$. Call the $(n + r) \times (n + r)$ matrix associated with this determinant A. Expanding $\det A$ along the right-most column, we obtain

$$f(x)u(x) + g(x)v(x) = R(f, g), \tag{2.2.3}$$

for some polynomials $u(x)$ and $v(x)$ with $\deg u < \deg g$ and $\deg v < \deg f$. Of particular significance here is that if $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$, then (2.2.3) is a linear combination of $f(x)$ and $g(x)$ in the ring $\mathbb{Z}[x]$. In other words, in this case, $u(x)$ and $v(x)$ in (2.2.3) are in $\mathbb{Z}[x]$. The problem of finding the smallest positive integer d that can be so represented as a linear combination of two given relatively prime polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ is non-trivial. We will examine this in a later chapter in the special context of $f(x)$ and $g(x)$ being cyclotomic polynomials.

Of interest to us in (2.2.3) is the case that $f(x)$ and $g(x)$ are non-constant polynomials and $R(f, g) = 0$ over the field of rationals or over the field of arithmetic modulo a prime p. Denote the field by F. Our argument for (2.2.3) still holds over F except that we would like to know that $u(x)$ and $v(x)$ are not identically zero in our field. For this purpose, we observe that $R(f, g) = 0$ corresponds to $\det A = 0$ which corresponds to the rows of A being linearly dependent over F. Thus, if the jth row of A is the vector $\overrightarrow{v}_j$ consisting of $n+r$ components, then there are $c_j \in F$ not all zero such that

$$c_1\overrightarrow{v}_1 + c_2\overrightarrow{v}_2 + \cdots + c_{n+r}\overrightarrow{v}_{n+r} = \overrightarrow{0}.$$

In particular, recalling that the entries in the last column of A are given by (2.2.2), we see that (2.2.3) holds with

$$u(x) = c_1x^{r-1} + c_2x^{r-2} + \cdots + c_r$$

and

$$v(x) = c_{r+1}x^{n-1} + c_{r+2}x^{n-2} + \cdots + c_{r+n}.$$

Here, we have $u(x)$ and $v(x)$ are in $F[x]$, at least one of $u(x)$ and $v(x)$ is non-zero (hence, both are), $\deg u < \deg g$ and $\deg v < \deg f$. With such $u(x)$ and $v(x)$ in hand, we are now ready to show the following (but note the cautionary remark after the proof).

Lemma 2.2.2. *Let $f(x)$ and $g(x)$ be two non-constant polynomials in the field F of rational numbers or arithmetic modulo a prime p. If $R(f,g)$ is zero in F, then $f(x)$ and $g(x)$ have an irreducible factor in common in $F[x]$. If further $\deg g < \deg f$, then $f(x)$ is reducible over F.*

Proof. From (2.2.3) and $R(f,g) = 0$, we deduce $f(x)u(x) = -g(x)v(x)$ in $F[x]$. Since $v(x)$ is non-zero with degree less than the degree of $f(x)$, unique factorization in $F[x]$ implies the conclusions of the lemma. ∎

To clarify, the polynomials in Lemma 2.2.2 are to be viewed as polynomials in the field F. In particular, if one has polynomials $f(x)$ and $g(x)$ in $\mathbb{Z}[x]$ and wishes to apply the lemma modulo a prime p, then the polynomials should be reduced modulo p, possibly changing the degrees of the polynomials, before computing $R(f,g)$ with the Sylvester determinant and applying Lemma 2.2.2. By way of an example, consider

$$f(x) = 2x^3 + x^2 + x + 1 \quad \text{and} \quad g(x) = 2x^2 + x + 1.$$

In this case, one can check that $R(f,g) = 8 = 2^3$. Observe, however, that $f(x)$ and $g(x)$ do not have an irreducible factor in common modulo 2. Indeed, we have

$$f(x) \equiv x^2 + x + 1 \pmod 2, \quad g(x) \equiv x + 1 \pmod 2$$

and

$$R(x^2 + x + 1, x + 1) = 1.$$

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

$$R(f,g) = a_n^r g(\alpha_1) \cdots g(\alpha_n). \tag{2.2.4}$$

The proof can be found in Uspensky (1948). Observe that (2.2.4) implies Lemma 2.2.1 and also the converse of Lemma 2.2.1. Thus, if $R(f,g) = 0$, then $f(x)$ and $g(x)$ have a complex root in common. With the cautionary notes of the previous paragraph, we can view Lemma 2.2.2 as a consequence of (2.2.4).

We now show that the following algorithm works to determine whether a given polynomial $f(x)$ is Eisenstein.

Algorithm: *Suppose that $f(x) \in \mathbb{Z}[x]$ is of degree $n \geq 2$. Calculate $R(f,f')$ (using the right-hand side of (2.2.1)). 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

$$f(x) \equiv g(x)^2 h(x) \pmod{p} \tag{2.2.5}$$

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 Lemma 2.2.1, 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 (2.2.5) 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 $a \in \{0,1,\dots,p-1\}$. 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 (2.2.4) 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 (see Exercise (1.8)). Alternatively, Lemma 2.2.2

implies that $f(x)$ is reducible over $\mathbb{Q}$. In particular, by Theorem 2.1.1, 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 (2.2.1). 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 (2.6). 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 Exercise (2.13) 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 by the Schönemann-Eisenstein criterion. In general, if $f(x)$ and $g(x) \in \mathbb{Z}[x]$ and $f(g(x))$ is irreducible, then $f(x)$ is irreducible; 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 (Exercise (2.10)).