CHAPTER 3

FURTHER IRREDUCIBILITY CRITERIA

You can try with dogs and roosters.

You can try with goats and geese.

– Dr. Seuss

I Am Not Going To Get Up Today

3.1. The Schönemann - Eisenstein Criterion is one of many criteria for testing the irreducibility of a given polynomial $f(x) \in \mathbb{Z}[x]$. In this chapter, we explore several other criteria. We begin in this section with a criterion due to Perron [1]:

Theorem 8. *If* $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ *with* $n \geq 1$ *is such that* $a_n = 1$, $a_0 \neq 0$, *and* $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$, *then* $f(x)$ *is irreducible.*

For a generalization and related results see Lipka [1] and Parodi [1]. To prove Theorem 8, we will obtain information about the roots of the polynomials $f(x)$ which satisfy the conditions in the theorem. To obtain this information, we will make use of a simplified version of a classical result from Complex Analysis. The classical result is Rouché's Theorem (cf. Conway [1, p. 125]). Since we are only interested in a special case of it, we will be able to include its proof without requiring much background from the reader. The version of Rouché's Theorem we want is given as Lemma 2 below. Before discussing it further, we consider a general theorem which connects information about the roots of polynomials to irreducibility.

Lemma 1. *Let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ for which $f(0) \neq 0$. Suppose further that $f(x)$ has exactly 1 root α (with multiplicity 1) such that $|\alpha| \geq 1$. Then $f(x)$ is irreducible.*

Proof. Assume $f(x)$ is reducible. Since $f(x)$ is monic, its content is 1. Thus, we can write $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ have integer coefficients and are of degree ≥ 1. Furthermore, we may suppose that $g(x)$ and $h(x)$ are monic and that $h(\alpha) = 0$. The given information now implies that $g(0) \neq 0$ and the roots of $g(x)$, say $\beta_1, \ldots, \beta_r$, all have absolute value < 1. Observe that $g(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_r)$. Hence,

$$1 \leq |g(0)| = |\beta_1||\beta_2| \cdots |\beta_r| < 1,$$

giving a contradiction. Therefore, $f(x)$ is irreducible. ■

Lemma 2. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{C}[x]$, and let $\mathcal{C} = \{z \in \mathbb{C} : |z| = 1\}$. If the strict inequality $|f(z)+g(z)| < |f(z)|+|g(z)|$ holds for each $z \in \mathcal{C}$, then $f(x)$ and $g(x)$ have the same total number of zeroes (counting multiplicity) inside the circle $\mathcal{C}$ (i.e., in the interior of the region bounded by $\mathcal{C}$).*

Proof. Observe that the condition $|f(z)+g(z)| < |f(z)|+|g(z)|$ for z on the circle $\mathcal{C}$ implies that $f(z)$ and $g(z)$ cannot have zeroes on $\mathcal{C}$. In particular, each of $f(z)$ and $g(z)$ is not identically 0. Let k be the number of roots of $f(z)$ inside the circle $\mathcal{C}$, and let ℓ be the number of roots of $g(z)$ inside the circle $\mathcal{C}$. By the symmetry of the roles of $f(z)$ and $g(z)$ in the statement of Lemma 2, it suffices to show that $k \leq \ell$. Assume $k > \ell$. We will obtain a contradiction by showing that there is a $\theta \in [0, 2\pi)$ such that

$$|f(e^{i\theta}) + g(e^{i\theta})| = |f(e^{i\theta})| + |g(e^{i\theta})|.$$

It suffices to show that there is a $\theta \in [0, 2\pi)$ such that $\arg(f(e^{i\theta})) = \arg(g(e^{i\theta}))$, where for $z \in \mathbb{C}$, we take $\arg(z) \in (-\pi, \pi]$. For $\alpha \in \mathbb{C}$ with $|\alpha| \neq 1$, define $w(\alpha; 0) = \arg(1 - \alpha)$;

and for $\phi \in \mathbb{R} - \{0\}$, define $w(\alpha;\phi) = \arg(e^{i\phi} - \alpha) + 2s\pi$ where $s = s(\phi)$ is an integer chosen so that $w(\alpha;\phi)$ is continuous on $\mathbb{R}$. As ϕ varies over $\mathbb{R}$, the values of $e^{i\phi} - \alpha$ are on a circle of radius 1 centered at $-\alpha$. The circle has 0 in its interior if and only if $|\alpha| < 1$. Geometrically, it is easy to see that

$$w(\alpha;2\pi) - w(\alpha;0) = \begin{cases} 2\pi & \text{if } \alpha \text{ is inside the circle } \mathcal{C} \\ 0 & \text{otherwise.} \end{cases} \tag{3.1}$$

Let a be the leading coefficient of $f(z)$ and b be the leading coefficient of $g(z)$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $f(z)$ and $\beta_1, \beta_2, \ldots, \beta_r$ the roots of $g(z)$ (the roots appearing as many times as their multiplicity). Define

$$F(\phi) = \arg(a) + \sum_{j=1}^{n} w(\alpha_j;\phi) + 2u\pi,$$

where u is an integer chosen so that $F(0) \in (-2\pi, 0]$. Define

$$G(\phi) = \arg(b) + \sum_{j=1}^{r} w(\beta_j;\phi) + 2v\pi,$$

where v is an integer chosen so that $G(0) \in [F(0), F(0)+2\pi)$. Hence, $-2\pi < F(0) - G(0) \leq 0$. Also, $F(\phi)$ and $G(\phi)$ are continuous on $\mathbb{R}$. Since

$$\arg\left(f(e^{i\phi})\right) = \arg\left(a \prod_{j=1}^{n}\left(e^{i\phi} - \alpha_j\right)\right) \equiv \arg(a) + \sum_{j=1}^{n} \arg\left(e^{i\phi} - \alpha_j\right) \pmod{2\pi},$$

we get that

$$F(\phi) \equiv \arg\left(f(e^{i\phi})\right) \pmod{2\pi}. \tag{3.2}$$

Similarly,

$$G(\phi) \equiv \arg\left(g(e^{i\phi})\right) \pmod{2\pi}. \tag{3.3}$$

Furthermore, by (3.1),

$$F(2\pi) = F(0) + 2k\pi \quad \text{and} \quad G(2\pi) = G(0) + 2\ell\pi.$$

Let $H(\phi) = F(\phi) - G(\phi)$. Then $H(0) = F(0) - G(0) \leq 0$ and $H(2\pi) = F(2\pi) - G(2\pi) = 2(k - \ell)\pi + F(0) - G(0) > 0$. By the Intermediate Value Theorem, there is a $\theta \in [0, 2\pi)$ for which $H(\theta) = 0$. By (3.2) and (3.3), we now get that

$$\arg\left(f(e^{i\theta})\right) = \arg\left(g(e^{i\theta})\right),$$

completing the proof. ■

Proof of Theorem 8. By Lemma 1, we need only show that $f(x)$ has exactly 1 root with absolute value ≥ 1. Let $w(x) = -a_{n-1}x^{n-1}$. Let $z \in \mathcal{C}$. Then

$$\begin{aligned}
|f(z) + w(z)| &= \left| \left(\sum_{j=0}^{n} a_j z^j \right) - a_{n-1} z^{n-1} \right| \\
&= \left| \left(\sum_{j=0}^{n-2} a_j z^j \right) + a_n z^n \right| \\
&\leq \left(\sum_{j=0}^{n-2} |a_j||z^j| \right) + |a_n||z^n| \\
&= |a_0| + |a_1| + \cdots + |a_{n-2}| + 1 \\
&< |a_{n-1}| \\
&= |a_{n-1} z^{n-1}| \\
&\leq |f(z)| + |w(z)|.
\end{aligned}$$

By Lemma 2, $f(x)$ and $w(x)$ must have the same total number of zeroes in $\mathcal{C}$. Each polynomial will have $n - 1$ zeroes strictly inside $\mathcal{C}$ since $w(x) = -a_{n-1}x^{n-1}$ clearly does. Thus, $f(x)$ has exactly 1 root with absolute value ≥ 1, completing the proof. ■

3.2. In this section, we consider two theorems of Schur (cf. Pólya and Szegő [2, pp. 133, 326-327]).

Theorem 9. *Let n be a positive integer. If $a_1, \dots, a_n$ are distinct integers, then $(x - a_1) \cdots (x - a_n) - 1$ is irreducible.*

Proof. Assume the conclusion of the theorem is false. Let $g(x)$ and $h(x)$ be polynomials in $\mathbb{Z}[x]$ with $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and $(x-a_1)\cdots(x-a_n)-1 = g(x)h(x)$. For $j \in \{1, \dots, n\}$, we get that $g(a_j)h(a_j) = -1$ which implies that $g(a_j) = -h(a_j) = \pm 1$. Since $g(x) \not\equiv \pm 1$ and $h(x) \not\equiv \pm 1$, both $g(x)$ and $h(x)$ have degree ≥ 1 and both have degree $\leq n-1$. Thus, $g(x) + h(x)$ has degree $\leq n-1$. Since $g(a_j) = -h(a_j)$ for $j \in \{1, \dots, n\}$, we get that $g(x) + h(x)$ is a polynomial of degree $\leq n-1$ with $\geq n$ roots and so (by Theorem 4) $g(x) + h(x) \equiv 0$. Hence, $g(x) \equiv -h(x)$. Therefore,

$$(x - a_1) \cdots (x - a_n) - 1 \equiv - \left(g(x)\right)^2,$$

giving a contradiction since the leading coefficient on the left-hand side above is 1 and the leading coefficient on the right-hand side is negative. ■

Theorem 10. *Let n be a positive integer. Let $a_1, \dots, a_n$ be distinct integers. If $f(x) = (x - a_1) \cdots (x - a_n) + 1$ is reducible, then $f(x)$ is a translation of either $x(x-2)+1$ or $x(x-1)(x-2)(x-3)+1$.*

Proof. Suppose that $f(x)$ is reducible. By translating and relabelling the a_j if necessary, we may take $a_n = 0$, and $1 \leq a_1 < a_2 < \cdots < a_{n-1}$. In particular, $a_j \geq j$ for $j \in \{1, \dots, n-1\}$. Let $g(x)$ and $h(x)$ be polynomials in $\mathbb{Z}[x]$ with $g(x) \not\equiv \pm 1$, $h(x) \not\equiv \pm 1$, and

$$f(x) = x(x - a_1) \cdots (x - a_{n-1}) + 1 = g(x)h(x).$$

For $j \in \{1, \dots, n\}$, $g(a_j)h(a_j) = f(a_j) = 1$ so that $g(a_j) = h(a_j) \in \{-1, 1\}$. This implies that the degrees of $g(x)$ and $h(x)$ must be ≥ 1 and also $\leq n-1$. Now, $g(x) - h(x)$ has n roots and has degree $\leq n-1$ so that $g(x) - h(x) \equiv 0$. Hence, $g(x) \equiv h(x)$. Thus,

$$f(x) = g(x)^2.$$

This implies that the degree of $f(x)$ is even. Let $m \in \mathbb{Z}$ with $n = 2m$. Now, for $n \geq 6$,

$$
\begin{aligned}
f\left(\frac{1}{2}\right) &= \left(\frac{1}{2}\right)\left(\left(\frac{1}{2}\right) - a_1\right)\cdots\left(\left(\frac{1}{2}\right) - a_{n-1}\right) + 1 \\
&= 1 - (-1)^{n-1}\left(\frac{1}{2}\right)\left(\left(\frac{1}{2}\right) - a_1\right)\cdots\left(\left(\frac{1}{2}\right) - a_{n-1}\right) \\
&= 1 - \left(\frac{1}{2}\right)\left(a_1 - \left(\frac{1}{2}\right)\right)\cdots\left(a_{n-1} - \left(\frac{1}{2}\right)\right) \\
&= 1 - \left(\frac{1}{2}\right)\left(\left(2a_1 - 1\right)/2\right)\cdots\left(\left(2a_{n-1} - 1\right)/2\right) \\
&\leq 1 - \left(\frac{1}{2}\right)^n \cdot 1 \cdot 3 \cdot 5 \cdots (2n-3) < 0.
\end{aligned} \tag{3.4}
$$

This is a contradiction (for $n \geq 6$) since $f(1/2) = g(1/2)^2 \geq 0$. Thus, either $m = 1$ or $m = 2$.

Case 1: $m = 1$ (or $n = 2$).

Since $f(1/2) = g(1/2)^2 \geq 0$, we examine $f(1/2)$ as in (3.4) to obtain that

$$1 - (1/4)(2a_1 - 1) \geq 0.$$

Solving for a_1, we get that $a_1 \leq 5/2$. This implies that $a_1 = 1$ or $a_1 = 2$. We cannot have $a_1 = 1$, since then $f(x) = x(x-1) + 1 = x^2 - x + 1$ which is irreducible (and also not a square). Thus, $a_1 = 2$, and in this case, necessarily, $f(x) = x(x-2) + 1 = x^2 - 2x + 1 = (x-1)^2$.

Case 2: $m = 2$ (or $n = 4$).

Using that $a_j \geq j$ for $j \in \{1, \ldots, n-1\}$, we examine $f(1/2)$ as in (3.4) to obtain that

$$
\begin{aligned}
0 \leq f\left(\frac{1}{2}\right) &= 1 - (1/16)(2a_1 - 1)(2a_2 - 1)(2a_3 - 1) \\
&\leq 1 - (1/16)(2-1)(4-1)(2a_3 - 1) = (19 - 6a_3)/16.
\end{aligned}
$$

Thus, $a_3 \leq 19/6$. This can only happen if $a_1 = 1, a_2 = 2$, and $a_3 = 3$. Therefore, in this case,

$$f(x) = x(x-1)(x-2)(x-3) + 1 = x^4 - 6x^3 + 11x^2 - 6x + 1 = (x^2 - 3x + 1)^2,$$

completing the proof. ■

If in Theorem 9 and Theorem 10, one considers instead polynomials of the form $f(x) = a(x-a_1)\cdots(x-a_n)\pm 1$ where $a_1,\dots,a_n$ are distinct integers and a is an arbitrary positive integer, then in addition to the reducible polynomials which are given in Theorem 10, the only other class of reducible polynomials one gets are the translations of $4x(x-1)+1 = (2x-1)^2$. This result and other related material can be found in Dorwart and Ore [3]. A discussion of this more general situation can also be found in the next section and in the problems at the end of the chapter (see Problems (3.18), (3.19), and (3.20)).

The next result, similar to the results above, was first conjectured by Schur and proved by Seres [1]. Seres' proof made use of Capelli's Theorem which we will discuss in Chapter 9. There the reader can also find a proof of the next theorem in the case that 2 of the a_j differ by more than 4. For our present purposes we simply state the following result of Seres conjectured by Schur.

Theorem 11. *Let n and k be a positive integers. If $a_1,\dots,a_n$ are distinct integers, then*

$$(x-a_1)^{2^k}(x-a_2)^{2^k}\cdots(x-a_n)^{2^k}+1$$

is irreducible.

We note that Seres [1] actually proved a stronger version of Theorem 11. Other related results can be found in Pirgov [1,2] and Pirgov and Tokarev [3].

3.3. Sometimes it is possible to determine the irreducibility of a polynomial by considering prime values of the polynomial. Indeed, prime values of polynomials play a major role in the theory of irreducible polynomials. We begin this section with a simple result, and then discuss an improvement due to Ore [1].

Theorem 12. *Let $f(x) \in \mathbb{Z}[x]$ be of degree n. If there exist at least $2n+1$ distinct integers m such that $|f(m)|$ is prime, then $f(x)$ is irreducible.*

Proof. Suppose $f(x) \in \mathbb{Z}[x]$ is of degree n and is not irreducible. Clearly, $f(x)$ is not identically 0, 1, or -1. Therefore, $f(x) = g(x)h(x)$ where $g(x)$ and $h(x)$ are in $\mathbb{Z}[x]$, $g(x) \not\equiv \pm 1$, and $h(x) \not\equiv \pm 1$. Let $r = \deg g(x)$ and $s = \deg h(x)$. Note that $\deg f(x) = n = r + s$. Since $\deg g(x) = r$ and $g(x) \not\equiv \pm 1$, each of $g(x)+1$ and $g(x)-1$ has at most r roots. Thus, there are at most r integers m such that $g(m) = 1$ and at most r integers m such that $g(m) = -1$. Therefore, there are at most $2r$ integers m such that $g(m) = \pm 1$. Similarly, there are at most $2s$ integers m such that $h(m) = \pm 1$. If $|f(m)| = |g(m)||h(m)|$ is prime, then either $g(m) = \pm 1$ or $h(m) = \pm 1$. Hence, there are at most $2r + 2s = 2(r+s) = 2n$ integers m such that $|f(m)|$ is prime, establishing the contrapositive of the theorem and therefore the theorem itself. ∎

Ore's Theorem is the following:

Theorem 13. *Let $f(x) \in \mathbb{Z}[x]$ be of degree n. If there exist at least $n+5$ distinct integers m such that $|f(m)|$ is prime, then $f(x)$ is irreducible.*

In $n \leq 4$, then Theorem 13 follows from Theorem 12. We will make use of the following

Lemma. *If $g(x)$ is a polynomial in $\mathbb{Z}[x]$ of degree $r \geq 1$, then there exist $\leq r+2$ integers m such that $g(m) = \pm 1$.*

Observe that once this lemma has been established, Theorem 13 follows as in the proof of Theorem 12 by replacing $2r$ and $2s$ in that argument by $r+2$ and $s+2$, respectively. The proof of the lemma that we present here is based on the method described in Dorwart and Ore [3]. Before proceding, it is worth connecting the lemma to the results of the previous section. In the previous section, we considered

$$f(x) = a(x - a_1)(x - a_2)\cdots(x - a_n) \pm 1, \tag{3.5}$$

where $a_1, \ldots, a_n$ are distinct integers and where there we took $a = 1$. Here, we consider the irreducibility of $f(x)$ with a denoting an arbitrary positive integer. (There is no need to look at the case when $a < 0$ since then the irreducibility of $-f(x)$ could be considered instead.) If the last term in (3.5) is -1, then the argument for proving Theorem 9 applies directly to give that $f(x)$ is irreducible. So suppose the final term is $+1$. Using the argument for the proof of Theorem 10, we can deduce that $f(x) = g(x)^2$ so that we get immediately that $f(x)$ is irreducible if n is odd. If $r = \deg g(x)$, then $n = 2r$ and each of $g(a_1), g(a_2), \dots, g(a_n)$ is ± 1. Hence, by the lemma, $2r = n \le r + 2$ so that $r \le 2$ and $n \le 4$. We get the

Corollary. *Let $f(x)$ be as in (3.5) with a denoting a positive integer and $a_1, \dots, a_n$ denoting distinct integers. If n is odd or $n \ge 5$, then $f(x)$ is irreducible. If $n \in \{2, 4\}$ and $f(x)$ is reducible, then there is a $g(x) \in \mathbb{Z}[x]$ of degree r such that $f(x) = g(x)^2$.*

To prove the lemma, let $a_1, \dots, a_m$ be distinct integers such that $g(a_j) = 1$ for each $j \in \{1, \dots, m\}$, and let $a_{m+1}, \dots, a_{m+k}$ be distinct integers such that $g(a_j) = -1$ for each $j \in \{m+1, \dots, m+k\}$. By considering $-g(x)$ if necessary, we may suppose that $m \ge k$, so we do so. Suppose further that the a_j are ordered so that $a_1 < a_2 < \cdots < a_m$ and $a_{m+1} < a_{m+2} < \cdots < a_{m+k}$. To prove the lemma, we want to show that $m + k \le r + 2$. Observe that $m \le r$ and $k \le r$. Hence, if $m = 0$ or $k = 0$ (i.e., if there are no integers a such that $g(a) = 1$ or if there are no integers a such that $g(a) = -1$), then $m + k \le r$, and we are through. Therefore, we suppose that $m \ge 1$ and $k \ge 1$. Since $g(a_j) = 1$ for each $j \in \{1, \dots, m\}$, we get that $g(x) - 1$ is divisible by $(x - a_1) \cdots (x - a_m)$. In other words,

$$g(x) = (x - a_1) \cdots (x - a_m) h(x) + 1$$

for some $h(x) \in \mathbb{Z}[x]$. (To see this, use the final remarks of Section 1.2 to write $g(x) - 1$ in the form $(x - a_1) \cdots (x - a_m) h(x) + r(x)$ where $h(x)$ and $r(x)$ are in $\mathbb{Z}[x]$ and where $r(x)$ does not have degree $\ge m$ but necessarily satisfies $r(a_j) = 0$ for $j \in \{1, 2, \dots, m\}$. It follows that $r(x) \equiv 0$ implying the desired result). For each $i \in \{1, \dots, m\}$ and each $j \in \{m+1, \dots, m+k\}$, we get that

$$2 = |g(a_j) - g(a_i)| = |a_j - a_1| \cdots |a_j - a_m| |h(a_j)|.$$

Since $a_j - a_1, \dots, a_j - a_m$, and $h(a_j)$ are integers, they are all contained in $\{-1, 1, 2\}$ or all contained in $\{-2, -1, 1\}$. Since also $a_j - a_1, \dots, a_j - a_m$ are distinct, we get that $m \le 3$. If

$m = 3$, then either $a_1 = a_j - 1$, $a_2 = a_j + 1$, and $a_3 = a_j + 2$ or $a_1 = a_j - 2$, $a_2 = a_j - 1$, and $a_3 = a_j + 1$. Observe that for fixed a_1, a_2, and a_3, there is at most one such a_j (specifically, if such an a_j exists, then it is $a_1 + 1$ if $a_2 - a_1 = 2$ and it is $a_1 + 2$ if $a_2 - a_1 = 1$). Thus, if $m = 3$, then $k \leq 1$ and $m + k \leq 4$. Since $m \geq k$, we get that if $m \leq 2$, then $k \leq 2$ so that again $m + k \leq 4$. Thus, for $r \geq 2$, the lemma follows. The case $r = 1$ is trivial, and the lemma follows.

The above argument establishes a little more. We can replace $r + 2$ in the statement of the lemma with $\max\{4, r\}$. If there are integers m_1 and m_2 such that $g(m_1) = 1$ and $g(m_2) = -1$, then we can replace $r + 2$ with 4.

We note that in the statements of Theorem 12 and Theorem 13, one can replace "$|f(m)|$ is prime" with "$|f(m)| = 1$ or $|f(m)|$ is prime." Considerably more work has been done in the direction of Ore's Theorem. Prior to Ore's Theorem, Pólya [1] showed that if the degree of $f(x) \in \mathbb{Z}[x]$ is an odd integer $n \geq 17$ and if there are $\geq n$ integers m such that $|f(m)| = p$ for some fixed prime p, then $f(x)$ is irreducible. Ore [1] classified the reducible polynomials $f(x) \in \mathbb{Z}[x]$ for which there are $> \deg f(x)$ integers m for which $|f(m)|$ is prime. Theorem 13 followed as a consequence of Ore's work. As an example of further consequences, we note that Ore showed that if $f(x) \in \mathbb{Z}[x]$ is reducible and is such that there are $\deg(f(x)) + 4$ integers m for which $|f(m)|$ is prime, then $f(x)$ is of degree 4 and has the form $f(x) = g(x)h(x)$ where both $g(x)$ and $h(x)$ are translates of $x(x+1) - 1$. For example, he notes that

$$f(x) = ((x - 2)(x - 1) - 1)\,((x - 6)(x - 5) - 1)$$

is such that $|f(m)|$ is prime for $m \in \{0, 1, \ldots, 7\}$. For other results related to Ore's Theorem see Desimirova [1], Dorwart [2], and Schulz [1].

3.4. Observe that one can use Ore's Theorem or Theorem 12 to establish the irreducibility of a polynomial $f(x) \in \mathbb{Z}[x]$ by showing that $|f(m)|$ is prime for a sufficient number of integers m. The next results we discuss are special cases in which we can deduce the irreducibility of a polynomial $f(x) \in \mathbb{Z}[x]$ based on the fact that $f(m)$ is prime for a single value of m. The next theorem, due to A. Cohn and G. Pólya (Pólya and Szegő [2, pp. 133, 330]), is a particular case of this.

Theorem 14. *Let $d_n d_{n-1} \dots d_0$ be the decimal representation of a prime. Then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible.*

Thus, since 7776589 is prime, $f(x) = 7x^6 + 7x^5 + 7x^4 + 6x^3 + 5x^2 + 8x + 9$ is irreducible. Or to put it another way, we can deduce the irreducibility of $f(x)$ based on the fact that $f(10)$ is prime. For related results see Brillhart, Filaseta, and Odlyzko [1], Filaseta [1,3], and Alexander [1]. In particular, Brillhart, Filaseta, and Odlyzko have shown that if $(d_n d_{n-1} \dots d_0)_b$ is the base b representation of a prime where b is an integer ≥ 2, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible. Our next result is a consequence of the work by Filaseta [3] and improvements of the result can be found there and in Alexander [1]. In particular, the next result easily implies Theorem 14.

Theorem 15. *If $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ is such that $f(10)$ is prime and $0 \leq a_j \leq 10^{15} a_n$ for $j \in \{0, 1, \dots, n-1\}$, then $f(x)$ is irreducible.*

Lemma. *Let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv \pm 1$, and let m be an integer such that $|f(m)|$ is 1 or a prime and such that $f(x)$ has no zeroes in $\{z \in \mathbb{C} : |z - m| \leq 1\}$. Then $f(x)$ is irreducible.*

Proof. Assume $f(x) = g(x)h(x)$ where $g(x)$ and $h(x) \in \mathbb{Z}[x]$, with $g(x) \not\equiv \pm 1$ and $h(x) \not\equiv \pm 1$. We will obtain a contradiction by showing that $f(x)$ must have a root in $\{z \in \mathbb{C} : |z - m| \leq 1\}$. Since $|f(m)| = |g(m)||h(m)|$ is 1 or a prime, either $|g(m)| = 1$ or $|h(m)| = 1$. Without loss of generality, say $|g(m)| = 1$. Then $g(x)$ is not a constant function since $g(x) \not\equiv \pm 1$. Hence, we can write $g(x) = b \prod_{j=1}^{r} (x - \beta_j)$, where b is a non-zero integer, r is a positive integer, and $\beta_1, \dots, \beta_r$ are the roots of $g(x)$ (counted to their multiplicity).

Thus,

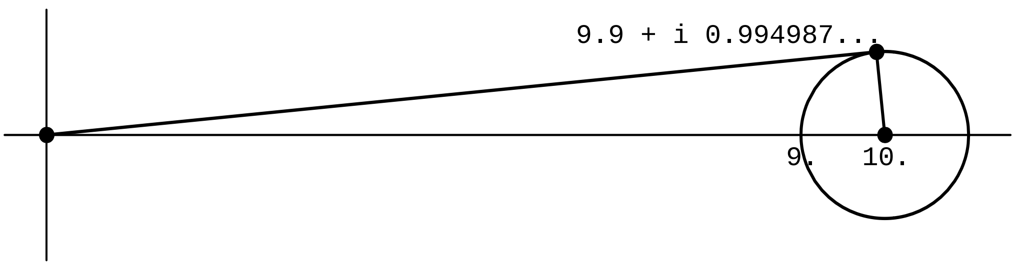
$$1 = |g(m)| = |b| \prod_{j=1}^{r} |m - \beta_j|.$$

Hence, there exists $k \in \{1, ..., r\}$ such that $|m - \beta_k| \leq 1$ and $f(\beta_k) = g(\beta_k)h(\beta_k) = 0$. Therefore, $f(x)$ has a root in $\{z \in \mathbb{C} : |z - m| \leq 1\}$, giving a contradiction and completing the proof. ■

Before continuing we note that the following Corollary is an immediate consequence of the above Lemma (with $m = 0$). The Corollary is due to Brillhart and Constantin [1]. We leave the details of its proof as an exercise (Problem (3.9)).

Corollary. *If $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$, $|a_0|$ is prime, and $|a_0| > |a_1| + |a_2| + \cdots + |a_n|$, then $f(x)$ is irreducible.*

Proof of Theorem 15. By the Lemma, it suffices to show that $f(x)$ has no zeroes in $D = \{z : |z - 10| \leq 1\}$. Let $z \in D$. Then $z = re^{i\theta}$ where $r \geq 9$ and $|\theta| \leq \text{Sin}^{-1}(1/10) = 5.739\ldots°$.



Since $|15\theta| < 90°$, we get that

$$\Re\left(z^{-1}\right) > 0, \Re\left(z^{-2}\right) > 0, \ldots, \Re\left(z^{-15}\right) > 0.$$

We may assume that $a_n \neq 0$ (so we do so). Thus,

$$\begin{aligned}
\left|\frac{f(z)}{z^n}\right| &= \left|a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_1}{z^{n-1}} + \frac{a_0}{z^n}\right| \\
&\geq \left|a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_{n-15}}{z^{15}}\right| - \sum_{j=16}^{n} \frac{|a_j|}{|z|^j} \\
&\geq \Re\left(a_n + \frac{a_{n-1}}{z} + \cdots + \frac{a_{n-15}}{z^{15}}\right) - \sum_{j=16}^{n} \frac{10^{15} a_n}{|z|^j} \\
&\geq a_n - 10^{15} \times \frac{1}{9^{16}} \times \frac{1}{1-(1/9)} \times a_n > 0.39 a_n > 0.
\end{aligned}$$

Thus, for $z \in D$, $f(z) \neq 0$, concluding the proof. ■

Before leaving this chapter, we note that there are many other irreducibility criteria in the literature. In particular, the interested reader may wish to read Dorwart [3] for a survey of some irreducibility results. Several irreducibility results also appear in Pólya and Szegő [2]; in particular, results related to deducing the irreducibility of a polynomial based on the size of non-zero values of the polynomial can be found there.

Problems

(3.1) Let $f(x) \in \mathbb{Z}[x]$. Prove that there are infinitely many integers k such that $f(x)+k$ is irreducible.

(3.2) Let $f(x) \in \mathbb{Z}[x]$. Prove that $x^2 f(x) + kx + 1$ is irreducible provided only that k is a sufficiently large integer. In other words, show that there is a number k_0, possibly depending on $f(x)$, such that if $k \geq k_0$, then $x^2 f(x) + kx + 1$ is irreducible.

(3.3) (a) Let $f(x) \in \mathbb{Z}[x]$, and let a be a non-zero integer. Prove that $f(x)$ is irreducible over the rationals if and only if $f(ax)$ is irreducible over the rationals.

(b) Note that (a) is no longer true if "over the rationals" is replaced by "over the integers." Give an example to justify this comment.

(c) Let $g(x) \in \mathbb{Z}[x]$. Use (a) and Problem (3.2) to show that if a is a fixed non-zero integer and k is a sufficiently large integer, then $f(x) = g(x)x^2 + kx + a$ is irreducible over the rationals.

(3.4) Let $f(x)$ be a quadratic polynomial with non-negative integer coefficients and non-zero constant term. Prove that if there is a positive integer m such that $f(m)$ is prime, then $f(x)$ is irreducible.

(3.5) Let $f(x)$ be a cubic polynomial with non-negative integer coefficients and non-zero constant term. Prove that if there is a positive integer m such that $f(m)$ is prime, then either $f(x)$ is irreducible or $f(x) = x^3 + 1$.

(3.6) Observe that $f(x) = x - 1$ is irreducible but $f(x^2) = x^2 - 1 = (x+1)(x-1)$ is reducible. Suppose that $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $n \geq 1$ is such that every coefficient of $f(x)$ is non-negative, $a_n = 1$, $a_0 \neq 0$, and $|a_{n-1}| > 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$. Then $f(x)$ is irreducible by Perron's Theorem. Prove that $f(x^2)$ is also irreducible.

(3.7) Let N be a positive integer, and let $f(x) \in \mathbb{Z}[x]$ such that the absolute value of each of its coefficients is $\leq N$. Prove that if there are at least $2N+4$ integers m such that $|f(m)|$ is prime, then $f(x)$ is irreducible.

(3.8) Suppose that $f(x)$ is a polynomial of degree 3 in $\mathbb{Z}[x]$, $f(m) = 1$ for 3 integers m, and $f(m) = -1$ for one integer m. Prove that $f(x)$ is a translate of $x(x-1)(x-3)+1$ or a translate of $-x(x-2)(x-3)+1$.

(3.9) Prove the Corollary to the Lemma for Theorem 15.

(3.10) Let n be a composite number > 1. Prove that there is an integer $b \geq 2$ such that if $n = \sum_{j=0}^{r} d_j b^j$, with $d_j \in \{0, 1, \ldots, b-1\}$, and $f(x) = \sum_{j=0}^{r} d_j x^j$, then $f(x)$ is a reducible polynomial of degree ≥ 2.

(3.11) Recall the remark after Theorem 14 that its analog for an arbitrary base $b \geq 2$ is true. Explain why this implies that if $f(x) \in \mathbb{Z}[x]$ has non-negative coefficients and if for some positive integer k one has that $f\left(f(k)\right)$ is prime, then $f(x)$ is irreducible.

(3.12) Let $f(x) \in \mathbb{Z}[x]$ of degree n. Suppose that $f(x)$ has non-negative coefficients and $f(10)$ is prime. Prove that if $n \leq 31$, then $f(x)$ is irreducible. (We note that the bound 31 in this problem cannot be replaced by 32.)

(3.13) Prove that if $d_n d_{n-1} \ldots d_0$ is the decimal representation of 5^k for some positive integer k, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible.

(3.14) Prove that if $d_n d_{n-1} \ldots d_0$ is the decimal representation of 16^k for some positive integer k, then $f(x) = \sum_{j=0}^{n} d_j x^j$ is irreducible.

(3.15) Show that the following more general version of Rouché's Theorem follows from Lemma 2 of Theorem 8.

Let R be a positive real number. Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{C}[x]$, and let $\mathcal{C} =$

$\{z : |z| = R\}$. If the strict inequality $|f(z) + g(z)| < |f(z)| + |g(z)|$ holds for each $z \in \mathcal{C}$, then $f(x)$ and $g(x)$ have the same total number of zeroes (counting multiplicity) inside the circle $\mathcal{C}$ (i.e., in the interior of the region bounded by $\mathcal{C}$).

(3.16) (a) Let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$. Prove that there is a B depending on $f(x)$ such that if b is an integer $\geq B$, then $f(x)(x-b)+1$ is irreducible. (Hint: Let $g(x) = -f(x)(x-b)$ and start by using the previous problem to show that for $b \geq B$, $f(x)(x-b)+1$ has at most one root with absolute value $\geq b/2$.)

(b) Let $f(x) \in \mathbb{Z}[x]$ with $f(x) \not\equiv 0$, and let c be an arbitrary non-zero integer. Prove that there is a B depending on $f(x)$ and c such that if b is an integer $\geq B$, then $f(x)(x-b)+c$ is irreducible over the rationals.

(3.17) For each positive integer n, prove that there is an irreducible $f(x) \in \mathbb{Z}[x]$ with n distinct real roots.

(3.18) Let $f(x)$ be as in equation (3.5) with $n = 2$, with a denoting a positive integer, and with a_1 and a_2 denoting distinct integers. Show that if $f(x)$ is reducible, then $f(x)$ is a translation of $x(x-2)+1$ or a translation of $4x(x-1)+1$.

(3.19) Let $f(x)$ be as in equation (3.5) with $n = 4$, with a denoting a positive integer, and with $a_1, \ldots, a_4$ denoting distinct integers. Show that if $f(x)$ is reducible, then $a = 1$ and $f(x)$ is a translation of $x(x-1)(x-2)(x-3)+1$.

(3.20) In this chapter, we have obtained irreducibility results for $f(x)$ as in equation (3.5) with a denoting a positive integer and with $a_1, \ldots, a_n$ denoting distinct integers. In this problem, we consider the possibility that $a_1, \ldots, a_n$ are not distinct.

(a) A squarefull number a is a positive integer which satisfies $p^2 | a$ for each prime divisor p of a. For example, the squares are squarefull as well as the numbers 72 and 108. Show that if a is squarefull, then $a = b^2 d^3$ for some positive integers b and d.

(b) Show that there are $O(\sqrt{x})$ squarefull numbers $\leq x$ (in other words, show that there is an absolute constant c such that the number of squarefull numbers $\leq x$ is $< c\sqrt{x}$ for every $x \geq 1$).

(c) Show that all but $O(\sqrt{t})$ positive integers $a \leq t$ satisfy the property that if $f(x)$ is of the form given in equation (3.5) where n is a positive integer and $a_1, \ldots, a_n$ are arbitrary integers, then $f(x)$ is irreducible.

(d) Show that all but $O(\sqrt{t})$ positive integers $a \leq t$ satisfy the property that if $f(x) = axg(x) \pm 1$ where $g(x)$ is an arbitrary monic polynomial in $\mathbb{Z}[x]$, then $f(x)$ is irreducible.

(3.21) Let S be an arbitrary finite set of integers. Show that there exists an N such that if $f(x)$ is a polynomial with integer coefficients of degree $n \geq N$, then there exist at most n integers m such that $f(m) \in S$.

(3.22) Prove that if $f(x) \in \mathbb{Z}[x]$ is reducible and is such that there are $\deg(f(x)) + 4$ integers m for which $|f(m)|$ is prime, then $f(x)$ is of degree 4 and has the form $f(x) = g(x)h(x)$ where both $g(x)$ and $h(x)$ are translates of $x(x+1) - 1$.

(3.23) Let $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ with $n \geq 1$, $a_n = 1$, and $a_0 \neq 0$. Suppose further that $|a_{n-1}| \geq 1 + |a_{n-2}| + |a_{n-3}| + \cdots + |a_0|$. Then it is possible for $f(x)$ to be reducible (for example, if $f(x) = x^2 - 2x + 1$ or $f(x) = x^2 + 2x + 1$). Show that if $f(1) \neq 0$ and $f(-1) \neq 0$, then $f(x)$ is irreducible. (Hint: Consider the proof of Theorem 8, and use that if $z_1, \ldots, z_n$ are complex numbers such that $|z_1 + \cdots + z_n| = |z_1| + \cdots + |z_n|$, then $z_1, \ldots, z_n$ are on the same ray emanating from the origin.)