# CHAPTER 7

# THE CYCLOTOMIC POLYNOMIALS

7.1. We define the $n^{\text{th}}$ cyclotomic polynomial, $\Phi_n(x)$, as the product of the monic irreducible factors of $x^n-1$ which are not factors of $x^k-1$ for $k \in \{1,...,n-1\}$. There are other ways one can define $\Phi_n(x)$. This particular definition seems to be the simplest in that it can be explained rather readily to a junior high school or high school student familiar with the rudiments of basic algebra. Observe that every irreducible factor of $x^n - 1$ in $\mathbb{Z}[x]$ necessarily has leading coefficient $\pm 1$. If $w(x)$ is such a factor, then so is $-w(x)$. We have restricted our attention to only the monic irreducible factors of $x^n - 1$ in defining $\Phi_n(x)$; thus, only one of $w(x)$ and $-w(x)$ is considered in the definition. The first 10 values of $\Phi_n(x)$ are:

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_4(x) = x^2 + 1,$$

$$\Phi_5(x) = x^4+x^3+x^2+x+1, \quad \Phi_6(x) = x^2-x+1, \quad \Phi_7(x) = x^6+x^5+x^4+x^3+x^2+x+1,$$

$$\Phi_8(x) = x^4 + 1, \quad \Phi_9(x) = x^6 + x^3 + 1, \quad \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1.$$

Our first theorem in this chapter shows that there is only one monic irreducible factor of $x^n - 1$ which is not a factor of $x^k - 1$ for some $k \in \{1, ..., n - 1\}$. In other words, $\Phi_n(x)$ is irreducible. This result is due to Kronecker [1]. Our proof will be based on a proof of Landau [1]. Note that when $n$ is a prime, the irreducibility of $\Phi_n(x)$ follows by Eisenstein's Criterion (see Problem (7.1)); Gauss [1] first established this particular case of the theorem.

**Theorem 23.** *$\Phi_n(x)$ is irreducible for all positive integers $n$.*

*Proof.* The roots of $x^n - 1$ are $e^{2\pi im/n}$ where $m \in \{0, 1, \ldots, n-1\}$. If $\gcd(m, n) = d > 1$, then there are integers $m'$ and $n'$ such that $m = dm'$ and $n = dn'$ so that $e^{2\pi im/n} = e^{2\pi im'/n'}$ is a root of $x^k - 1$ where $k = n' = n/d < n$. In this case, we get that $e^{2\pi im/n}$ is a root of $\gcd(x^n - 1, x^k - 1)$ and, hence, a root of an irreducible factor of $x^n - 1$ which is not among the irreducible factors defining $\Phi_n(x)$. Thus, the roots of $\Phi_n(x)$ are among the numbers of the form $e^{2\pi im/n}$ where $m \in \{0, 1, \ldots, n-1\}$ and $\gcd(m, n) = 1$. In particular, observe that $e^{2\pi i/n}$ is a root of $\Phi_n(x)$ since it is not a root of $x^k - 1$ for $k \in \{1, \ldots, n-1\}$.

Let $\zeta = e^{2\pi ij/n}$ with $j$ a non-negative integer. Let $f(x) \in \mathbb{Z}[x]$ such that $f(x)$ is monic and $f(\zeta) = 0$. By the above comments, it suffices to show that if $m \in \{0, 1, \ldots, n-1\}$ and $\gcd(m, n) = 1$, then $f(\zeta^m) = 0$ (and, in fact, we only need to establish this for $j = 1$). Since $\zeta$ is a root of $x^n - 1$, $\zeta$ is a root of a monic irreducible polynomial in $\mathbb{Z}[x]$. Let $d$ be the degree of this monic irreducible polynomial. By Problem (7.7), for each positive integer $k$, there is a unique element $R_k(x)$ of $\mathbb{Z}[x]$ which is $\equiv 0$ or of degree $< d$ such that $f(\zeta^k) = R_k(\zeta)$; furthermore, if $p$ is a prime, then every coefficient of $R_p(x)$ is divisible by $p$.

Since $\zeta^n = 1$, we get that for every positive integer $k$, $R_k(x) = R_{k+n}(x)$. Thus, the set of coefficients of the polynomials $R_1(x), R_2(x), \ldots$ is finite. Let $A$ denote the maximum of the absolute values of these coefficients. By the previous paragraph, if $p$ is a prime $> A$, then we must have that $R_p(x) \equiv 0$ so that $f(\zeta^p) = 0$ for every prime $p > A$. It suffices at this point to use Dirichlet's Theorem concerning primes in arithmetic progressions, but we will avoid the use of Dirichlet's Theorem as follows. The above all held with $\zeta = e^{2\pi ij/n}$ where $j$ is any non-negative integer. By applying the above observations several times while appropriately replacing $j$ by suitable multiples of $j$, one gets that $f(\zeta^w) = 0$ for every positive integer $w$ which has all of its prime factors $> A$. Let $m \in \{0, 1, \ldots, n-1\}$ such that $\gcd(m, n) = 1$. Since $\zeta^n = 1$, we get that $\zeta^m = \zeta^w$, where

$$w = m + n \prod_{\substack{p \text{ prime} \\ p \le A, p \nmid m}} p.$$

Since $\gcd(m,n)=1$, one gets that $w$ is not divisible by any prime $\leq A$. Hence, $f(\zeta^m)=f(\zeta^w)=0$. This completes the proof. ■

The following is an easy consequence of the above proof.

**Corollary.** *Let $n$ be a positive integer. Then*

$$\Phi_n(x)=\prod_{\substack{1\leq j\leq n\\ \gcd(j,n)=1}}\left(x-e^{2\pi ij/n}\right).$$

The Corollary implies that the degree of $\Phi_n(x)$ is the number of positive integers relatively prime to $n$ and $\leq n$. In other words,

$$\deg\Phi_n(x)=\phi(n),$$

where $\phi$ denotes Euler's $\phi-$function. A different formula for $\Phi_n(x)$ is often useful, and our next goal is to establish such a formula. We make use of Lemma 2 to Theorem 18 in Chapter 4.

**Theorem 24.** *Let $n$ be a positive integer. Then*

$$\Phi_n(x)=\prod_{d|n}\left(x^d-1\right)^{\mu(n/d)}.$$

*Proof.* Whenever $d$ divides $n$, the linear factors of $x^d-1$ in $\mathbb{C}[x]$ are all of the form $x-e^{2\pi ij/n}$ for some $j\in\{0,1,\ldots,n-1\}$. For a fixed $j\in\{0,1,\ldots,n-1\}$, $x-e^{2\pi ij/n}$ is a factor of $x^d-1$ if and only if $n/\gcd(j,n)$ divides $d$ or, in other words, if and only if $n/d$ divides $\gcd(j,n)$. Thus, the factor $x-e^{2\pi ij/n}$ appears on the right-hand side above with the exponent

$$\sum_{\substack{d|n\\ (n/d)|\gcd(j,n)}}\mu\left(\frac{n}{d}\right).$$

Observe that as $d$ runs over the divisors of $n$ so does $k=n/d$. Hence,

$$\sum_{\substack{d|n\\ (n/d)|\gcd(j,n)}}\mu\left(\frac{n}{d}\right)=\sum_{k|\gcd(j,n)}\mu(k).$$

By Lemma 2 to Theorem 18, $x - e^{2\pi ij/n}$ is a factor on the right-hand side above if and only if $\gcd(j, n) = 1$ and then $x - e^{2\pi ij/n}$ appears with the exponent 1. By the Corollary to Theorem 23, the result follows. ■

7.2. To illustrate an application of the cyclotomic polynomials, we give the next result first stated by Euler (cf. Dickson [2, Vol. I, p. 415]). It is an "easy" case of Dirichlet's Theorem that if $a$ and $b$ are relatively prime positive integers, then there exist infinitely many primes in the arithmetic progression $a + kb$.

**Theorem 25.** *Let $n$ be a positive integer. Then there are infinitely many primes $p$ such that $p \equiv 1 \pmod{n}$.*

*Proof.* By Problem (7.8), it suffices to show that if $p$ is a prime dividing $\Phi_n(a)$ for some integer $a$, then $p|n$ or $p \equiv 1 \pmod{n}$. Fix an integer $a$ and a prime $p$ dividing $\Phi_n(a)$ with $p \nmid n$. Note that $p$ cannot divide $a$ since otherwise the fact that $p|\Phi_n(a)$ would imply that $p$ divides the constant term in $\Phi_n(x)$; this is impossible since the constant term of $\Phi_n(x)$ divides the constant term of $x^n - 1$ and, hence, 1.

Next, we show that $a$ has order $n$ modulo $p$. Once this has been established, we will be through since the order of $a$ modulo $p$ must divide $p - 1$ which would imply that $n|(p-1)$ so that $p \equiv 1 \pmod{n}$.

Observe that since $p|\Phi_n(a)$ and $\Phi_n(a)$ divides $a^n - 1$, we have that $a^n \equiv 1 \pmod{p}$. Assume that there is a positive integer $k < n$ such that $a^k \equiv 1 \pmod{p}$. Let $d = \gcd(k, n)$. Then $d \leq k < n$. There are integers $u$ and $v$ such that $ku + nv = d$. Recalling that $p$ does not divide $a$ (so that $a$ and its powers have inverses modulo $p$), we get that

$$a^d = a^{ku+nv} = \left(a^k\right)^u \times (a^n)^v \equiv 1 \pmod{p}.$$

Since $d = \gcd(k, n)$ divides $n$, we get that $x^d - 1$ divides $x^n - 1$. By the definition of $\Phi_n(x)$,

$$\left(x^d - 1\right) \Phi_n(x) | \left(x^n - 1\right).$$

Since $a^d - 1 \equiv 0 \pmod{p}$ and $\Phi_n(a) \equiv 0 \pmod{p}$, we get that $(x-a)^2$ divides $x^n - 1$ modulo $p$. This contradicts that $a$ is non-zero modulo $p$ and

$$\frac{d}{d\,x}\,(x^n - 1) = nx^{n-1}$$

has 0 as its only root modulo $p$ (where here we have used that $p \nmid n$). Hence, $a$ has order $n$ modulo $p$, and the proof is complete. ■

Note that it is not difficult to modify the above proof to establish that $p$ is a prime with $p \equiv 1 \pmod{n}$ if and only if $p \nmid n$ and $p$ is a prime divisor of $\Phi_n(a)$ for some integer $a$.

7.3. In this section, we begin with the following result due to Kronecker [2].

**Theorem 26.** *If $f(x) \in \mathbb{Z}[x]$ is monic, is irreducible, and has all its roots on $\{z : |z| = 1\}$, then $f(x)$ is a cyclotomic polynomial.*

*Proof.* Let $\alpha$ be such that $f(\alpha) = 0$. If we can establish that $\alpha$ is a root of some cyclotomic polynomial, then since both cyclotomic polynomials and $f(x)$ are irreducible, $f(x)$ will be cyclotomic. Thus, it suffices to show that there exists a positive integer $m$ such that $\alpha^m = 1$.

Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the complete list of roots of $f(x)$ with $\alpha_1 = \alpha$. Using elementary symmetric functions (cf. Uspensky [1]), it is easy to deduce that $(x-\alpha_1^k)(x-\alpha_2^k)\cdots(x-\alpha_n^k)$ is in $\mathbb{Z}[x]$ for every positive integer $k$. We can avoid the use of elementary symmetric functions, however, by restricting consideration to polynomials of the form

$$f_k(x) = (x - \alpha_1^{2^k})(x - \alpha_2^{2^k})\cdots(x - \alpha_n^{2^k}).$$

Then one easily deduces that

$$f_1(x^2) = (-1)^n f(x) f(-x) \in \mathbb{Z}[x].$$

Since $f_1(x^2)$ is a polynomial in $x^2$ with integer coefficients, it follows that $f_1(x)$ has integer coefficients. An easy induction argument now implies that $f_k(x) \in \mathbb{Z}[x]$ for every positive integer $k$.

Since $f_k(x)$ is monic and each root of $f_k(x)$ has absolute value $\leq 1$, we conclude that the coefficient of $x^j$ in $f_k(x)$ is $\leq \binom{n}{j}$ (by observing, for example, that the coefficient of $x^j$ in $f_k(x)$ must be less than or equal to the coefficient of $x^j$ in $(x+1)^n$). Since $n$ is fixed, this implies that the set $\{f_k(x) : k \geq 1\}$ is finite. Let $F(x)$ denote the least common multiple of the elements of $\{f_k(x) : k \geq 1\}$. Since $\alpha^2, \alpha^4, \alpha^8, \ldots$ are all roots of $F(x)$, there exist integers $r$ and $s$ with $1 \leq r < s$ and $\alpha^{2^r} = \alpha^{2^s}$. Since $|\alpha| = 1 \neq 0$, we get that $\alpha^m = 1$ with $m = 2^s - 2^r$, completing the proof. ■

Before continuing, we make a comment about what Theorem 26 is *not* saying. Consider the polynomial $f(x) = x^4 - 2x^3 + x^2 - 2x + 1$. It is easy to verify that $f(x)$ is not divisible by a cyclotomic polynomial. Is it possible that $f(x)$ has roots with absolute value 1? Yes, and as we shall see, it does. Theorem 26 asserts that all of its roots cannot have absolute value 1. To see that $f(x)$ has roots on the unit circle in the complex plane, observe that $f(\alpha) = 0$ if and only if

$$\left(\alpha + \frac{1}{\alpha}\right)^2 - 2\left(\alpha + \frac{1}{\alpha}\right) - 1 = 0,$$

from which one can easily deduce that the roots of $f(x)$ are

$$\frac{1 + \sqrt{2} \pm \sqrt{2\sqrt{2} - 1}}{2} \quad \text{and} \quad \frac{1 - \sqrt{2} \pm i\sqrt{2\sqrt{2} + 1}}{2}.$$

The last two roots are imaginary, and a quick check indicates that they have absolute value 1.

There are a variety of results related to Theorem 26 (cf. Cassels [1], Smyth [1], and Lloyd-Smith [1]). In particular, we mention the following result of Dobrowolski [1].

**Theorem 27.** *Let $\epsilon > 0$, and let $n$ be a sufficiently large integer. If $f(x) \in \mathbb{Z}[x]$ is monic, non-cyclotomic, and irreducible of degree $n$, then there is a root $\alpha$ of $f(x)$ such that*

$$|\alpha| > 1 + \frac{2 - \epsilon}{n}\left(\frac{\log\log n}{\log n}\right)^3.$$

It has been conjectured by Schinzel and Zassenhaus [2] that the factor $(\log\log n/\log n)^3$ can be replaced by an absolute constant. We will establish

**Theorem 28.** *Let $n$ be a positive integer, and let $f(x) \in \mathbb{Z}[x]$ be monic, non-cyclotomic, and irreducible of degree $n$. Furthermore, suppose that $f(0) \neq 0$ and that $f(x)$ has no reciprocal roots (i.e., that $f(\alpha) = 0$ implies $f(1/\alpha) \neq 0$). Then there is a root $\alpha$ of $f(x)$ such that*

$$|\alpha| > 1 + \frac{1}{10n}.$$

In other words, the conjecture of Schinzel and Zassenhaus is true when $f(x)$ has no reciprocal roots. Theorem 28 was stated in such a way as to make its connection to Theorem 27 and the conjecture of Schinzel and Zassenhaus, but observe that the conditions that $f(x)$ is non-cyclotomic and that $f(x)$ is irreducible may be omitted from the theorem without changing the content of the result. Theorem 28 was established by Cassels [1] and is proven below. However, first we deal with some preliminaries.

**Lemma 1.** *Let $\delta \in (0, 1)$, and let $x_j$, for $j \in \{1, 2, \ldots, m\}$, be real numbers satisfying*

$$0 < x_j \leq 1 + \delta \quad \text{for } j \in \{1, 2, \ldots, m\} \tag{7.1}$$

*and*

$$\prod_{j=1}^{m} x_j = 1. \tag{7.2}$$

*Then*

$$\prod_{j=1}^{m} |x_j - 1| < (\delta e)^m. \tag{7.3}$$

*Proof.* Let $x_1, \ldots, x_m$ be real numbers satisfying (7.1) and (7.2), and assume that (7.3) is not true. For the time being, suppose that there are $i$ and $j \in \{1, 2, \ldots, m\}$ such that $x_i < 1$, $x_j < 1$, and $x_i \neq x_j$. For such an $i$ and $j$ fixed, consider

$$x'_k = \begin{cases} \sqrt{x_i x_j} & \text{if } k = i \text{ or } j \\ x_k & \text{otherwise.} \end{cases}$$

Then

$$0 < x'_k \leq 1 + \delta \quad \text{for } k \in \{1, 2, \ldots, m\},$$

and

$$\prod_{k=1}^{m} x'_k = \prod_{k=1}^{m} x_k = 1.$$

Observe that

$$|x_i - 1|\,|x_j - 1| = (1 - x_i)(1 - x_j) = 1 - (x_i + x_j) + x_i x_j$$

and

$$|x'_i - 1|\,|x'_j - 1| = (1 - \sqrt{x_i x_j})(1 - \sqrt{x_i x_j}) = 1 - 2\sqrt{x_i x_j} + x_i x_j.$$

Since $x_i \neq x_j$, we get that $x_i + x_j > 2\sqrt{x_i x_j}$. Therefore,

$$\prod_{k=1}^{m} |x_k - 1| < \prod_{k=1}^{m} |x'_k - 1|.$$

Since $x_1, \ldots, x_m$ do not satisfy (7.3), we get that $x'_1, \ldots, x'_m$ do not satisfy (7.3). By repeating the above several times if necessary, we get that we can replace the real numbers $x_1, \ldots, x_m$ by a new collection of $m$ real numbers satisfying (7.1) and (7.2) and not (7.3) and having the property that any two elements of the new collection of real numbers which are $< 1$ are equal. For notational reasons, we assume as we can that $x_1, \ldots, x_m$ already have the latter property.

Observe that if $x_j = 1$ for every $j \in \{1, \ldots, m\}$, then (7.3) would be true, giving a contradiction. Thus, since (7.1) and (7.2) hold, there must be an $i$ and $j \in \{1, \ldots, m\}$ such that

$$x_i < 1 < x_j \leq 1 + \delta.$$

Using an argument similar to the above, one can show that we can further assume that any such $x_j = 1 + \delta$. To do this, note that

$$((1 + \delta) - x_i)\,((1 + \delta) - x_j) > 0 \quad \text{if } x_j \neq 1 + \delta,$$

and set

$$x'_k = \begin{cases} 1 + \delta & \text{if } k = j \\ x_i x_j (1 + \delta)^{-1} & \text{if } k = i \\ x_k & \text{otherwise.} \end{cases}$$

By the above observations, there will be a certain number, say $m - s$, of the $x_j$ equal to $1 + \delta$ and the remaining $s$ will be equal to $1 - \eta$ where

$$(1 - \eta)^s (1 + \delta)^{m-s} = 1.$$

Then

$$-s \log(1 - \eta) \leq m \log(1 + \delta)$$

so that

$$s\eta < s\left(\eta + \frac{\eta^2}{2} + \frac{\eta^3}{3} + \cdots\right) \leq m\left(\delta - \frac{\delta^2}{2} + \frac{\delta^3}{3} - \cdots\right) < m\delta.$$

Thus, $\eta < m\delta/s$, and we get that

$$\prod_{k=1}^{m} |x_k - 1| = \eta^s \delta^{m-s} \leq \left(\frac{m}{s}\right)^s \delta^m.$$

Since $m/s > 1$, we get that

$$\frac{m}{s} < \left(\frac{m}{s}\right)^e \leq e^{m/s}$$

(see Problem (7.10)). Thus, $(m/s)^s < e^m$, and we get that

$$\prod_{k=1}^{m} |x_k - 1| < (e\delta)^m,$$

concluding the proof. ■

We will put off the proof of the next lemma for the moment and discuss first how to obtain a certain Corollary to the lemma and how to establish Theorem 28 from the Corollary.

**Lemma 2.** *Let $m$ be an integer $> 1$, and let $\rho$ be a real number $> 1$ satisfying*

$$\cos\left(\frac{\pi}{m}\right) < \frac{\rho^2}{\rho^4 + 1 - \rho^2}. \tag{7.4}$$

*Suppose that $z_1, \ldots, z_m \in \mathbb{C}$ and that*

$$|z_j| \leq \rho \quad \text{for all } j \in \{1, \ldots, m\}. \tag{7.5}$$

*Then*

$$\prod_{\substack{1 \leq j,k \leq m \\ j \neq k}} |z_j \overline{z_k} - 1| \leq \left(\frac{\rho^{2m} - 1}{\rho^2 - 1}\right)^m. \tag{7.6}$$

**Corollary.** *Let $m$ be an integer $> 1$, and let*

$$1 < \rho \leq 1 + \frac{1}{10m}. \tag{7.7}$$

*Suppose that $z_1, \ldots, z_m \in \mathbb{C}$ satisfying (7.5). Then*

$$\prod_{\substack{1 \leq j,k \leq m \\ j \neq k}} |z_j \overline{z_k} - 1| \leq m^m \rho^{2m(m-1)}. \tag{7.8}$$

*Proof (assuming Lemma 2).* One easily checks that for $x > 1$, $x^2 + x^{-2} - 1$ is increasing so that for $1 < x < 1 + (1/(10m))$, the value of $x^2 + x^{-2} - 1$ is at most

$$\begin{aligned}
&\left(1 + \frac{1}{10m}\right)^2 + \left(1 + \frac{1}{10m}\right)^{-2} - 1 \\
&\qquad = \left(1 + \frac{2}{10m} + \frac{1}{100m^2}\right) + \left(1 - \frac{2}{10m} + \frac{3}{100m^2} - \frac{4}{1000m^3} + \cdots\right) - 1 \\
&\qquad < 1 + \frac{4}{100m^2}.
\end{aligned}$$

Thus, the value of $1/(x^2 + x^{-2} - 1)$ is greater than

$$\frac{1}{1 + \dfrac{1}{25m^2}} > 1 - \frac{1}{25m^2} > 1 - \frac{\pi^2}{2m^2} + \frac{\pi^4}{24m^4} > \cos\left(\frac{\pi}{m}\right).$$

From (7.7), we get that

$$\cos\left(\frac{\pi}{m}\right) < \frac{1}{\rho^2 + \rho^{-2} - 1} = \frac{\rho^2}{\rho^4 + 1 - \rho^2}.$$

Thus, the conditions of Lemma 2 are satisfied. Hence,

$$\begin{aligned}
\prod_{\substack{1 \leq j,k \leq m \\ j \neq k}} |z_j \overline{z_k} - 1| &\leq \left(\frac{\rho^{2m} - 1}{\rho^2 - 1}\right)^m \\
&= \left(\rho^{2m-2} + \rho^{2m-4} + \cdots + \rho^2 + 1\right)^m \\
&\leq \left(\rho^{2m-2} m\right)^m = m^m \rho^{2m(m-1)},
\end{aligned}$$

establishing the corollary. ■

*Proof of Theorem 28 (assuming Lemma 2).* Let $w(x) = \sum_{j=0}^{m} a_j x^j$ with $a_0 \neq 0$ and $a_m = 1$, and suppose that the roots of $w(x)$ satisfy that

$$|\alpha_j| \leq 1 + \frac{1}{10m} \quad \forall j \in \{1, \ldots, m\}. \tag{7.9}$$

First, we show that $|a_0| = 1$. Assume that $|a_0| \geq 2$. Then observe that

$$\left(1 + \frac{1}{2m}\right)^m = 1 + \frac{1}{2} + \frac{m(m-1)}{2}\frac{1}{4m^2} + \cdots < 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 2.$$

Also,

$$\left|\prod_{j=1}^{m} \alpha_j\right| = |a_0| \geq 2.$$

Therefore, we get that there is a $j \in \{1, \ldots, m\}$ such that

$$|\alpha_j| \geq 2^{1/m} > 1 + \frac{1}{2m},$$

contradicting (7.9). Hence, $|a_0| = 1$. Thus,

$$\prod_{j=1}^{m} |\alpha_j| = 1. \tag{7.10}$$

Consider

$$P = \prod_{1 \leq i,j \leq m} (\alpha_i \alpha_j - 1).$$

If $P = 0$, then $w(x)$ has reciprocal roots, and we are through. We therefore assume $P \neq 0$. By the definition of $P$, $P$ is a symmetric function of the roots $\alpha_1, \ldots, \alpha_m$ of $w(x)$, and hence $P \in \mathbb{Z} - \{0\}$. Thus,

$$\prod_{1 \leq i,j \leq m} |\alpha_i \alpha_j - 1| \geq 1. \tag{7.11}$$

Observe that

$$\prod_{1 \leq i,j \leq m} |\alpha_i \alpha_j - 1| = \prod_{1 \leq i,j \leq m} |\alpha_i \overline{\alpha_j} - 1| = \Big( \prod_{1 \leq i \leq m} |\alpha_i \overline{\alpha_i} - 1| \Big) \Big( \prod_{\substack{1 \leq i,j \leq m \\ i \neq j}} |\alpha_i \overline{\alpha_j} - 1| \Big).$$

Also,

$$\alpha_i\overline{\alpha_i} = |\alpha_i|^2 \le \left(1+\frac{1}{10m}\right)^2 = 1+\frac{1}{5m}+\frac{1}{100m^2} \le 1+\frac{1}{4m}.$$

Therefore, by Lemma 1, with $\delta = 1/(4m)$, we get by (7.10) that

$$\prod_{1\le i\le m} |\alpha_i\overline{\alpha_i} - 1| \le \left(\frac{e}{4m}\right)^m.$$

Also, by the foregoing Corollary, we get that

$$\prod_{\substack{1\le i,j\le m\\ i\ne j}} |\alpha_i\overline{\alpha_j} - 1| \le m^m \left(1+\frac{1}{10m}\right)^{2m(m-1)}$$

$$= m^m \left(\left(1+\frac{1}{10m}\right)^{10m}\right)^{(m-1)/5} < m^m e^{m/5}.$$

Combining the above, we get that

$$\prod_{1\le i,j\le m} |\alpha_i\alpha_j - 1| < \left(\frac{e}{4m}\right)^m m^m e^{m/5} = \left(\frac{e^{6/5}}{4}\right)^m < 1.$$

This contradicts (7.11); hence, the assumption that $P \ne 0$ is invalid and the proof is complete. ■

To complete this section, we now proceed to prove Lemma 2. To do so, we first make some further preliminaries.

**Lemma 3.** *Let $r$, $\alpha$, and $\beta$ be real numbers, and set $\lambda = (\alpha+\beta)/2$. Suppose that*

$$r \ge 1, \quad \alpha \ge 0, \quad \beta \ge 0, \quad \lambda < 3\pi/2,$$

*and*

$$\cos(\lambda) < \frac{r}{r^2+1-r}.$$

*Then*

$$\left|re^{i\alpha}-1\right|\left|re^{i\beta}-1\right| \le \left|re^{i\lambda}-1\right|^2, \tag{7.12}$$

*with equality if and only if* $\alpha = \beta = \lambda$.

*Proof.* We suppose as we may that $\alpha \geq \beta$. Define $\mu = \alpha - \lambda$, and observe that

$$\alpha = \mu + \lambda \quad \text{and} \quad \beta = \lambda - \mu.$$

Let

$$L = \cos\lambda \quad \text{and} \quad M = \cos\mu.$$

Note that $\mu \geq 0$; and if $\mu = 0$, then $\alpha = \beta = \lambda$ and (7.12) holds. We need only show now that if $\mu > 0$, then (7.12) holds with strict inequality. Therefore, we suppose that $\mu > 0$. Observe that $\mu = \alpha - \lambda \leq \lambda < 3\pi/2$. Also, if $\lambda \geq 0$, then $0 \leq \lambda \leq \pi/2$. We get either

$$L < 0 \quad \text{and} \quad -1 \leq M < 1 \tag{7.13}$$

or

$$0 \leq L \leq M < 1 \quad \text{and} \quad L < \frac{r}{r^2 + 1 - r}. \tag{7.14}$$

Now, squaring the left-hand side of (7.12), we get that

$$\begin{aligned} \left|re^{i\alpha} - 1\right|^2 \left|re^{i\beta} - 1\right|^2 &= \left(re^{i\alpha} - 1\right)\left(re^{-i\alpha} - 1\right)\left(re^{i\beta} - 1\right)\left(re^{-i\beta} - 1\right) \\ &= \left((r^2+1) - 2r\cos(\alpha)\right)\left((r^2+1) - 2r\cos(\beta)\right). \end{aligned}$$

Using this together with

$$\begin{aligned} \cos(\alpha) + \cos(\beta) &= \cos(\lambda+\mu) + \cos(\lambda-\mu) \\ &= (\cos(\lambda)\cos(\mu) - \sin(\lambda)\sin(\mu)) + (\cos(\lambda)\cos(\mu) + \sin(\lambda)\sin(\mu)) \\ &= 2\cos(\lambda)\cos(\mu) = 2LM \end{aligned}$$

and

$$\begin{aligned} \cos(\alpha)\cos(\beta) &= (\cos(\lambda+\mu))(\cos(\lambda-\mu)) \\ &= \cos^2(\lambda)\cos^2(\mu) - \sin^2(\lambda)\sin^2(\mu) \\ &= \cos^2(\lambda)\cos^2(\mu) - \left(1 - \cos^2(\lambda)\right)\left(1 - \cos^2(\mu)\right) \\ &= \cos^2(\lambda) + \cos^2(\mu) - 1 = L^2 + M^2 - 1, \end{aligned}$$

we get that the square of the left-hand side of (7.12) is

$$\left(r^2+1\right)^2 - 4r\left(r^2+1\right)LM + 4r^2\left(L^2+M^2-1\right). \tag{7.15}$$

Observe that if we set $\alpha = \lambda$ and $\beta = \lambda$ in the above calculations of the square of the left-hand side of (7.12), we will obtain the square of the right-hand side of (7.12). In other words, we get the latter by setting $M = 1$ in (7.15). Thus, to finish the proof of the lemma, it suffices to show that

$$\left(r^2+1\right)^2 - 4r\left(r^2+1\right)LM + 4r^2\left(L^2+M^2-1\right) < \left(r^2+1\right)^2 - 4r\left(r^2+1\right)L + 4r^2\left(L^2\right).$$

This is the same as establishing that

$$4r^2\left(M^2-1\right) < 4r\left(r^2+1\right)L(M-1)$$

or, upon reducing and noting that $M - 1 < 0$,

$$r(M+1) > \left(r^2+1\right)L.$$

This is clear in the case that (7.13) holds. In the case that (7.14) holds, we rewrite the above as

$$r > \left(r^2+1\right)L - rM.$$

This inequality follows directly from

$$r > \left(r^2+1-r\right)L$$

and

$$\left(r^2+1-r\right)L \geq \left(r^2+1\right)L - rM,$$

completing the proof. ■

**Lemma 4.** *Let $m > 1$ be an integer, and let $\theta_1, \theta_2, \ldots, \theta_m$ be real numbers satisfying*

$$0 \le \theta_j \le 2\pi \quad \text{for } 1 \le j \le m.$$

*Let*

$$w = \frac{1}{2m}\left(\theta_1 + \cdots + \theta_m\right).$$

*Consider $r > 1$ such that*

$$|\cos(w)| < \frac{r}{r^2 + 1 - r}. \tag{7.16}$$

*Then*

$$\prod_{1 \le j \le m} \left|re^{i\theta_j} - 1\right| \le \left|re^{2iw} - 1\right|^m \tag{7.17}$$

*with equality if and only if $\theta_1 = \cdots = \theta_m = 2w$.*

*Proof.* Observe that if $r > 1$, then $r/(r^2 + 1 - r) < 1$. Hence, the lemma vacuously holds if $w = 0$ or $\pi$. Also, the lemma follows if $w = \pi/2$ since then we get that

$$\left|re^{i\theta_j} - 1\right| \le r + 1 = \left|re^{2iw} - 1\right|$$

with equality if and only if $\theta_j = \pi = 2w$. If $\pi/2 < w < \pi$, then replace $\theta_j$ with $2\pi - \theta_j$ and $w$ by $\pi - w$ to reduce the lemma to a case in which

$$0 < w < \pi/2.$$

Thus, we suppose as we may that the latter holds for $w$.

For fixed $w$, by continuity and compactness considerations, the left-hand side of (7.17) obtains its upper bound for some choice of $\theta_1, \ldots, \theta_m$ as in the lemma. We fix $\theta_1, \ldots, \theta_m$ so that this upper bound is obtained and note that now it suffices to prove (7.17) with the $\theta_j$ so chosen. If $\theta_1 = \cdots = \theta_m$, then we are through; thus, we suppose as we may that $\theta_1$ and $\theta_2$ satisfy

$$0 \le \theta_1 < 2w < \pi \quad \text{and} \quad 2w < \theta_2 \le 2\pi.$$

Set $\alpha = \theta_1$, $\beta = \theta_2$, and $\lambda = (\alpha + \beta)/2$. Then

$$\lambda = \frac{1}{2}(\theta_1 + \theta_2) < \frac{1}{2}(\pi + 2\pi) = \frac{3}{2}\pi$$

and either $\lambda \geq \pi/2$ so that

$$\cos(\lambda) \leq 0 < \frac{r}{r^2 + 1 - r}$$

or $0 < w < \theta_2/2 < \lambda < \pi/2$ so that from (7.16)

$$\cos(\lambda) \leq \cos(\theta_2/2) < \cos(w) < \frac{r}{r^2 + 1 - r}.$$

Thus, from Lemma 3, we get that

$$\left|re^{i\alpha} - 1\right| \left|re^{i\beta} - 1\right| < \left|re^{i\lambda} - 1\right|^2.$$

By considering $\theta_1' = \theta_2' = \lambda = (\theta_1 + \theta_2)/2$ and $\theta_j' = \theta_j$ for $j \in \{3, \ldots, m\}$, we get that the above inequality contradicts that $\theta_1, \ldots, \theta_m$ were chosen so that the left-hand side of (7.17) was maximal. Hence, for $\theta_1, \ldots, \theta_m$ so chosen, we must have that $\theta_1 = \cdots = \theta_m = 2w$ so that (7.17) holds with equality. This completes the proof. ■

**Lemma 5 (The Maximum Modulus Principle).** *Let $f(z) \in \mathbb{C}[z]$, and let $\rho \geq 0$. Then*

$$\max\{|f(z)| : |z| \leq \rho\} = \max\{|f(z)| : |z| = \rho\}.$$

*Proof.* Observe that the maximums exist above since $f(z)$ is continuous. Let $z_0$ be such that $|z_0| \leq \rho$ and

$$|f(z_0)| = \max\{|f(z)| : |z| \leq \rho\}.$$

Furthermore, suppose that $|z_0|$ is maximal with the above conditions (noting that this is in fact possible). If $|z_0| = \rho$, then we're done. Assume therefore that $|z_0| < \rho$. Let $r = \rho - |z_0|$. Then the average value of $|f(z)|^2$ on the circle $\{z : |z - z_0| = r\}$ is $< |f(z_0)|^2$.

Let $g(z) = f(z + z_0) = \sum_{j=0}^{n} b_j z^j$. Then the above implies that

$$\begin{aligned}\sum_{j=0}^{n} |b_j|^2 r^{2j} &= \frac{1}{2\pi} \int_0^{2\pi} \left( \sum_{j=0}^{n} b_j r^j e^{ji\theta} \right) \left( \sum_{j=0}^{n} \overline{b_j} r^j e^{-ji\theta} \right) d\theta \\ &= \frac{1}{2\pi} \int_0^{2\pi} g\left(re^{i\theta}\right) \overline{g\left(re^{i\theta}\right)}\, d\theta = \frac{1}{2\pi} \int_0^{2\pi} \left|g\left(re^{i\theta}\right)\right|^2 d\theta \\ &= \frac{1}{2\pi} \int_0^{2\pi} \left|f\left(z_0 + re^{i\theta}\right)\right|^2 d\theta < |f(z_0)|^2 = |g(0)|^2 = |b_0|^2,\end{aligned}$$

giving a contradiction. Thus, the result follows. ■

*Proof of Lemma 2.* Fix $j \in \{1, \ldots, m\}$ and complex numbers $z_1, \ldots, z_{j-1}, z_{j+1}, \ldots, z_m$ as in the lemma. Then

$$\begin{aligned}\prod_{\substack{1 \le t,k \le m \\ t \ne k}} |z_t \overline{z_k} - 1| &= \left( \prod_{\substack{1 \le t,k \le m \\ t \ne k, t \ne j, k \ne j}} |z_t \overline{z_k} - 1| \right) \prod_{\substack{1 \le k \le m \\ k \ne j}} \left( |z_j \overline{z_k} - 1| |\overline{z_j} z_k - 1| \right) \\ &= \left( \prod_{\substack{1 \le t,k \le m \\ t \ne k, t \ne j, k \ne j}} |z_t \overline{z_k} - 1| \right) \prod_{\substack{1 \le k \le m \\ k \ne j}} |z_j \overline{z_k} - 1|^2.\end{aligned}$$

Hence, we may view

$$\prod_{\substack{1 \le t,k \le m \\ t \ne k}} |z_t \overline{z_k} - 1| \tag{7.18}$$

as the absolute value of a polynomial in $z_j$. By Lemma 5, given that $|z_j| \le \rho$, we get that (7.18) obtains its maximum for some $z_j$ with $|z_j| = \rho$. Letting $j$ vary now, we see that to finish the proof, we need only consider the case when

$$|z_1| = |z_2| = \cdots = |z_m| = \rho.$$

By reordering the $z_j$'s if necessary, we suppose as we may that

$$z_j = \rho e^{i\phi_j} \quad \text{for } j \in \{1, \ldots, m\},$$

where

$$0 \le \phi_1 \le \phi_2 \le \cdots \le \phi_m < 2\pi.$$

Now, (7.18) becomes

$$\prod_{\substack{1\le t,k\le m\\ t\ne k}} |\rho^2 e^{i(\phi_t - \phi_k)} - 1| = \prod_{1\le s\le m-1} P_s,$$

where

$$P_s = \prod_{\substack{1\le t,k\le m\\ t\equiv k+s \pmod m}} |\rho^2 e^{i(\phi_t - \phi_k)} - 1|.$$

Observe that if $s$ and $t$ are known, then $k$ is uniquely determined by the conditions $1 \le k \le m$ and $t \equiv k + s \pmod m$. For fixed $s \in \{1, \ldots, m-1\}$ and fixed $t \in \{1, \ldots, m\}$, consider the uniquely determined $k$ as in the product above. Define

$$\theta_t = \theta_t(s) = \begin{cases} \phi_t - \phi_k & \text{if } t > k \\ \phi_t - \phi_k + 2\pi & \text{if } k > t \end{cases}$$

and note that $k > t$ in this definition if and only if $t \in \{1, \ldots, s\}$. Set

$$r = \rho^2$$

and

$$w = s\pi/m.$$

Then, for $s \in \{1, \ldots, m-1\}$,

$$\theta_1 + \cdots + \theta_m = 2\pi s = 2mw$$

and

$$|\cos(w)| = \left|\cos\left(\frac{s\pi}{m}\right)\right| \le \cos\left(\frac{\pi}{m}\right) < \frac{\rho^2}{\rho^4 + 1 - \rho^2} = \frac{r}{r^2 + 1 - r}.$$

Thus, we may apply Lemma 4 to get that

$$P_s \le \left|\rho^2 e^{2\pi i s/m} - 1\right|^m$$

so that (7.18) is bounded above by

$$\prod_{1\le s\le m-1}\left|\rho^2 e^{2\pi is/m}-1\right|^m=\left|\frac{\rho^{2m}-1}{\rho^2-1}\right|^m,$$

completing the proof. ■

7.4. In this section, we investigate the size of the coefficients of $\Phi_n(x)$. Recall the values of $\Phi_n(x)$ for $n\in\{1,2,\dots,10\}$ given at the beginning of the chapter. If we continue calculating up to $\Phi_{104}(x)$, the coefficients obtained will remain in the set $\{-1,0,1\}$ suggesting at the very least that the coefficients of $\Phi_n(x)$ do not get very large. This is in fact *not* the case, and it is the purpose of this section to mention two results in this direction. We shall only prove the first. It is a consequence of the second but seemingly much easier to establish. The proof given here is due to I. Schur (cf. E. Lehmer [1], her first mathematical publication).

**Theorem 29.** *Given $B$, there exists a positive integer $n$ such that $\Phi_n(x)$ has at least one coefficient with absolute value $> B$.*

*Proof.* Let $n=p_1p_2\dots p_k$, where $k$ is an odd positive integer and $p_1,p_2,\dots,p_k$ are primes satisfying

$$p_1<p_2<\cdots<p_k<p_1+p_2.$$

Note that there are infinitely many such $n$ for any given $k$ (see problem (AII.1)). To prove the theorem, it is sufficient to prove that the coefficient of $x^{p_k}$ in $\Phi_n(x)$ is $1-k$. Using Theorem 24 and calculating $\Phi_n(x)$ modulo $x^{p_k}+1$, we get that modulo $x^{p_k}+1$

$$\begin{aligned}\Phi_n(x)&\equiv\left(\prod_{j=1}^{k}\left(x^{p_j}-1\right)\right)/(x-1)\\&\equiv\left(x^{p_k-1}+x^{p_k-2}+\cdots+x+1\right)\left(x^{p_1}-1\right)\left(x^{p_2}-1\right)\cdots\left(x^{p_{k-1}}-1\right)\\&\equiv\left(x^{p_k-1}+x^{p_k-2}+\cdots+x+1\right)\left(-x^{p_{k-1}}-x^{p_{k-2}}-\cdots-x^{p_1}+1\right)\end{aligned}$$

The fact that the coefficient of $x^{p_k}$ in $\Phi_n(x)$ is $1-k$ follows, and the proof is complete. ■

The above proof shows that certain positive integers $n$ with sufficiently many distinct prime factors are such that $\Phi_n(x)$ has a coefficient whose absolute value exceeds $B$ for any preassigned $B$. Migotti (cf. E. Lehmer [1]) showed that if $n$ is the product of 2 primes, then the coefficients of $\Phi_n(x)$ are all from the set $\{0, \pm 1\}$. E. Lehmer [1] showed that as $n$ runs through the positive integers which are the product of 3 distinct primes, the coefficients of $\Phi_n(x)$ get arbitrarily large.

We end this section by stating what is undoubtedly one of the nicest result on the subject. Let $M_n$ denote the maximum of the absolute values of the coefficients of $\Phi_n(x)$. Erdős conjectured that for every constant $c$, one has that $M_n \geq c$ for almost all $n$. In other words, the number of $n \leq x$ for which $M_n < c$ is $o(x)$. The conjecture was first resolved by Maier [1] in a much stronger form. He showed the following:

**Theorem 30.** *Let $\epsilon(n)$ be any function defined for all positive integers and satisfying $\lim_{n\to\infty} \epsilon(n) = 0$. Then*

$$M_n \geq n^{\epsilon(n)}$$

*for almost all $n$.*

Thus, the conjecture follows by taking, for example, $\epsilon(n) = 1/\log\log n$. We note that the result of Maier [1] is in fact even stronger than that given by Theorem 30.

7.5. In this section, we discuss the factorization of $\Phi_n(x)$ modulo a prime. We will establish

**Theorem 31.** *Let $n$ be a positive integer, and let $p$ be a prime. Write $n = p^k m$ where $k$ is a non-negative integer and $\gcd(p, m) = 1$. Let $f$ be the least positive integer such that $p^f \equiv 1 \pmod{m}$. Then $\Phi_n(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo $p$ of degree $f$ each raised to the $\phi(p^k)$ power.*

Before presenting the proof of Theorem 31, we give two examples. Further examples can be found in the exercises as well as in the Corollaries following the proof.

*Example 1.* Consider $f(x) = \Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$. If $p = 2$, then $m = 5$ and $f = 4$ in Theorem 31 so that $f(x)$ is irreducible modulo 2. If $p = 5$, then $m = 2$ and $f = 1$ so that $f(x)$ factors as a linear polynomial raised to the 4th power modulo 5. In fact, we have

$$f(x)(x+1) \equiv x^5 + 1 \equiv (x+1)^5 \pmod{5}$$

so that by Theorem 3 (unique factorization in $\mathbb{Z}_5[x]$) we get that $f(x) \equiv (x+1)^4 \pmod{5}$. If $p$ is a prime $\equiv 1 \pmod{10}$, then $m = 10$ and $f = 1$ so that $f(x)$ factors as a product of 4 distinct linear polynomials modulo $p$. If $p$ is a prime $\equiv 3$ or $7 \pmod{10}$, then $m = 10$ and $f = 4$ so that $f(x)$ is irreducible modulo $p$. Finally, if $p$ is a prime $\equiv 9 \pmod{10}$, then $m = 10$ and $f = 2$ so that $f(x)$ factors as a product of 2 distinct irreducible quadratic polynomials modulo $p$.

*Example 2.* Consider $f(x) = \Phi_8(x) = x^4 + 1$. If $p = 2$, then $m = 1$ and $f = 1$ in Theorem 31 so that $f(x)$ factors as a linear polynomial raised to the 4th power modulo 2. Here we have

$$f(x) \equiv x^4 + 1 \equiv (x+1)^4 \pmod{2}.$$

If $p$ is a prime $\equiv 1 \pmod{8}$, then $m = 8$ and $f = 1$ so that $f(x)$ factors as a product of 4 distinct linear polynomials modulo $p$. If $p$ is a prime $\equiv 3$, 5, or $7 \pmod{8}$, then $m = 8$ and $f = 2$ so that $f(x)$ factors as a product of 2 distinct irreducible quadratic polynomials modulo $p$. Observe that this implies the result of Problem (4.1) that $x^4 + 1$ is reducible modulo every prime. (Also, see Corollary 1 below.)

These examples demonstrate what is apparent from the statement of the theorem, namely that the factorization of $\Phi_n(x)$ modulo a prime $p$ is completely determined by the residue class to which $p$ belongs modulo $n$. We also note that Theorem 31 can be used to give an alternative proof of Theorem 25. More specifically, Theorem 31 implies that if $p$ is a prime which does not divide $n$ and is such that $p|\Phi_n(a)$ for some integer $a$, then $p \equiv 1 \pmod{n}$.

*Proof of Theorem 31.* The main tool we use to obtain Theorem 31 is Theorem 17 of Chapter 4. We begin, however, by making use of Problem (7.3). If, in the statement of Theorem 31, $k \geq 1$, then Problem (7.3) (a) implies that

$$\Phi_n(x) = \Phi_{pm}\big(x^{p^{k-1}}\big),$$

and Problem (7.3) (b) implies that

$$\Phi_{pm}\big(x^{p^{k-1}}\big)\Phi_m\big(x^{p^{k-1}}\big) = \Phi_m\big(x^{p^k}\big).$$

On the other hand,

$$\Phi_m\big(x^{p^{k-1}}\big) \equiv \Phi_m\big(x\big)^{p^{k-1}} \pmod{p} \quad \text{and} \quad \Phi_m\big(x^{p^k}\big) \equiv \Phi_m\big(x\big)^{p^k} \pmod{p}.$$

Hence, we deduce that

$$\Phi_n(x) \equiv \Phi_m(x)^{\phi(p^k)} \pmod{p}.$$

We assumed above that $k \geq 1$, but we note that this last congruence is trivially true in the case that $k = 0$. To establish the theorem, then, it suffices to show $\Phi_m(x)$ factors modulo $p$ as a product of $\phi(m)/f$ incongruent irreducible polynomials of degree $f$.

By the definition of $f$, we see that $m$ divides $p^f - 1$. Hence, $x^m - 1$ divides $x^{p^f - 1} - 1$, and we obtain that $\Phi_m(x)$ divides $\big(x^{p^f - 1} - 1\big)x = x^{p^f} - x$. By Theorem 17, each irreducible factor $g(x)$ of $\Phi_m(x)$ modulo $p$ is such that its degree, say $r$, divides $f$. We show that for each such $g(x)$, $r = f$. Assume for some such $g(x)$, we have $r < f$. Then by Theorem 16 or Theorem 17, $g(x)$ divides $x^{p^r} - x$ modulo $p$. In fact, since $\Phi_m(x)$ divides $x^m - 1$, the constant term of $\Phi_m(x)$ is $\pm 1$ and so the constant term of $g(x)$ is non-zero modulo $p$. Thus, $g(x)$ is not a multiple of $x$ modulo $p$ and $g(x)$ divides $x^{p^r - 1} - 1$ modulo $p$. In particular, $x$ has an inverse (modd $p$, $g(x)$). The definition of $f$ implies that $m$ does not divide $p^r - 1$ so that $d = \gcd(m, p^r - 1) < m$. Let $u$ and $v$ be integers satisfying $mu + (p^r - 1)\, v = d$. Then

$$x^d - 1 \equiv x^{mu + (p^r - 1)\, v} - 1 \equiv (x^m)^u \left(x^{p^r - 1}\right)^v - 1 \equiv 0 \pmod{p,\ g(x)}.$$

Therefore, $g(x)$ divides $x^d - 1$ modulo $p$.

Observe that $d < m$ implies $\Phi_m(x)$ is by definition relatively prime to $x^d - 1$. Therefore, $\Phi_m(x)$ and $x^d - 1$ are relatively prime divisors of $x^{md} - 1$ in $\mathbb{Z}[x]$. Let $h_1(x) \in \mathbb{Z}[x]$ with $x^{md} - 1 = \Phi_m(x)\left(x^d - 1\right) h_1(x)$. Since $g(x)$ is a common divisor of $\Phi_m(x)$ and $x^d - 1$ modulo $p$, we get that for some $h_2(x) \in \mathbb{Z}[x]$

$$x^{md} - 1 \equiv \Phi_m(x)\left(x^d - 1\right) h_1(x) \equiv g(x)^2 h_2(x) \pmod{p}.$$

Since $d$ divides $p^r - 1$, $p$ does not divide $d$. The definition of $m$ implies that $p$ does not divide $m$. Hence, taking derivatives above, we deduce that $g(x)$ is an irreducible factor of $x^{md-1}$ modulo $p$ and yet $g(x)$ is not a multiple of $x$ modulo $p$. This is a contradiction which implies that $r = f$. Thus, every irreducible factor of $\Phi_m(x)$ modulo $p$ is of degree $f$.

Since $\deg \Phi_m(x) = \phi(m)$, it remains only to show that if $g(x)$ is an irreducible factor of $\Phi_m(x)$ modulo $p$, then $g(x)^2$ does not divide $\Phi_m(x)$ modulo $p$. Assume $g(x)^2$ divides $\Phi_m(x)$ modulo $p$. Then there is an $h(x) \in \mathbb{Z}[x]$ such that $x^m - 1 \equiv g(x)^2 h(x) \pmod{p}$. Following the argument above, we get in this case that $g(x)$ must be an irreducible factor of $x^{m-1}$ modulo $p$, resulting in a contradiction and, hence, completing the proof. ■

Let $n$ be a positive integer. Observe that if a prime $p$ does not have order $\phi(n)$ modulo $n$, then the above theorem implies $\Phi_n(x)$ is reducible modulo $p$. In particular, if there are no primitive roots modulo $n$ (i.e., no integers $a$ for which the order of $a$ is $\phi(n)$ modulo $n$), then $\Phi_n(x)$ is reducible modulo every prime. On the other hand, using the above theorem in conjunction with Dirichlet's Theorem on primes in arithmetic progression, one can easily deduce that if there exists a primitive root modulo $n$, then $\Phi_n(x)$ is irreducible modulo some prime. The $n$ for which a primitive root modulo $n$ exists are 1, 2, 4, and numbers of the form $p^k$ or $2p^k$ where $p$ is an odd prime and $k$ a positive integer; thus, we can summarize the comments here with

**Corollary 1.** *Let $n$ be a positive integer. Then $\Phi_n(x)$ is reducible modulo every prime $p$ if and only if $n$ is not among the numbers of the form 1, 2, 4, $p^k$, or $2p^k$ where $p$ denotes an odd prime and $k$ denotes a positive integer.*

We consider now the possibility that $\Phi_n(x)$ is Eisenstein with respect to some prime $p$. Then $\Phi_n(x)$ would factor modulo $p$ as a constant times a linear polynomial raised to the power $\phi(n)$. Using the notation of Theorem 31, we would necessarily have that $f = 1$ and $\phi(m) = 1$. Therefore, $m = 1$ or 2. This implies that either $n = p^k$ or $n = 2p^k$ for some prime $p$. In these cases, Theorem 31 can be used to establish that $\Phi_n(x)$ is Eisenstein with respect to $p$ (or see Problem (7.5) and Problem (7.6)). Hence, we get

**Corollary 2.** *Let $n$ be a positive integer. Then $\Phi_n(x)$ is Eisenstein with respect to a prime $p$ if and only if $n = p^k$ or $n = 2p^k$ for some positive integer $k$.*

7.6. There are numerous results concerning cyclotomic polynomials and it would be impossible in one chapter to give them a thorough treatment. In this section, we briefly mention a few other results without proofs. The results are classical and can be found in Narkiewicz [1].

The field $\mathbb{Q}(\zeta_n)$ is called a cyclotomic field. All the roots of $x^n - 1$ are in $\mathbb{Q}(\zeta_n)$. Thus, we can refer to the galois group $G = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ associated with the polynomial $\Phi_n(x)$. The galois group $G$ is isomorphic to $\mathbb{Z}_n^*$ (the multiplicative group of integers modulo $n$). The elements of $G$ can be described as follows. Let $j \in \{1, \ldots, n-1\}$ with $\gcd(j, n) = 1$. Define $\sigma_j$ as the automorphism of $\mathbb{Q}(\zeta_n)$ satisfying $\sigma_j(\zeta_n) = \zeta_n^j$ and $\sigma_j(u) = u$ for all $u \in \mathbb{Q}$. Then the $\sigma_j$'s are precisely the elements of $G$. Observe that in particular $|G| = \phi(n)$.

The ring of algebraic integers in $\mathbb{Q}(\zeta_n)$ clearly contains $\mathbb{Z}[\zeta_n]$. In fact, the ring of integers can be shown to be $\mathbb{Z}[\zeta_n]$. The units in $\mathbb{Z}[\zeta_n]$ are described in a convenient form by a result known as Kummer's Lemma (which Kummer used to establish his classical result that Fermat's Last Theorem holds for any "regular" prime exponent). It is

**Theorem 32.** *Every unit in $\mathbb{Z}[\zeta_n]$ can be written in the form $r\zeta_n^k$ where $r$ is real and $k$ is an integer.*

## Problems

(7.1) (a) What is the value of $\Phi_p(x)$ when $p$ is a prime?

(b) Expand $\Phi_p(x+1)$ as a polynomial in $x$, and deduce that $\Phi_p(x)$ is irreducible.

(7.2) Prove that if $\Phi_n(x)$ is Eisenstein with respect to $p$, then $p$ divides $n$. (Hint: First show that if $f(x)$ and $g(x)$ are in $\mathbb{Z}[x]$ and each does not have a multiple root, then $R(f,f')R(g,g')$ divides $R(fg,(fg)')$. Be sure to justify that $R(fg,(fg)')/(R(f,f')R(g,g'))$ is an integer.)

(7.3) Let $n$ be a positive integer, and let $p$ be a prime.

(a) Prove that if $p$ divides $n$, then $\Phi_{pn}(x) = \Phi_n(x^p)$.

(b) Prove that if $p$ does not divide $n$, then $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$.

(7.4) Prove that if $n$ is an odd integer $\geq 3$, then $\Phi_{2n}(x) = \Phi_n(-x)$.

(7.5) Without using any material after Section 7.1 except the problems above, prove that if $k$ is a positive integer and $p$ is a prime, then $\Phi_{p^k}(x)$ is Eisenstein with respect to $p$.

(7.6) Without using any material after Section 7.1 except the problems above, prove that if $k$ is a positive integer and $p$ is a prime, then $\Phi_{2p^k}(x)$ is Eisenstein with respect to $p$.

(7.7) Let $f(x)$ be a monic irreducible polynomial of degree n, and let $\alpha$ denote a root of $f(x)$.

(a) Prove that for every positive integer $k$, there is a unique polynomial $g(x) \in \mathbb{Z}[x]$ which is $\equiv 0$ or of degree $< n$ such that $f(\alpha^k) = g(\alpha)$.

(b) In (a), if $k = p$ where $p$ is a prime, then prove that every coefficient of $g(x)$ is divisible by $p$. (Hint: Consider $f(x^p) - f(x)^p$.)

(7.8) Let $f(x)$ be a non-constant polynomial with integer coefficients. Prove that there

are infinitely primes $p$ for which $p$ divides $f(m)$ for some integer $m$.

(7.9) Modify the proof of Kronecker's Theorem in Section 3 to give an easy proof that there is a positive function $\epsilon(n)$ such that if $f(x) \in \mathbb{Z}[x]$ is a monic irreducible polynomial of degree $n$ with all of its roots having absolute value $\leq 1 + \epsilon(n)$, then $f(x)$ is cyclotomic.

(7.10) Prove that if $x > 0$, then $x^e \leq e^x$ (a result used in the proof of Lemma 1 to Theorem 28).

(7.11) (a) Is it possible to load 2 dice in such a way that each face of each die has a rational probability of coming facing up on a roll and such that if both dice are rolled, then the sum of the 2 numbers rolled is equally likely to be each of $2, 3, \ldots, 12$?

(b) Do part (a) with each face of each die having a "real" probability of coming facing up on a roll.

(7.12) Let $n$ and $k$ be positive integers. Prove that $\Phi_n(x^k)$ is a product of distinct cyclotomic polynomials. (Note: The product may consist of just one factor.)

(7.13) Let $n$ and $k$ be positive integers. Prove that $\Phi_n(x^k)$ is irreducible if and only if every prime divisor of $k$ is a prime divisor of $n$.

(7.14) Prove that for each prime $p$, $\Phi_{200}(x)$ can be written as a product of at least 4 factors modulo $p$.