The Coefficients of Cyclotomic Polynomials

GARY BROOKFIELD
California State University
Los Angeles CA 90032-8204
gbrookf@calstatela.edu

There is a remarkable amount of mathematics to be discovered just by factoring polynomials of the form $x^n - 1$ with $n \in \mathbb{N}$. To get started, consider

$$\begin{aligned} x - 1 &= x - 1 \\ x^2 - 1 &= (x+1)(x-1) \\ x^3 - 1 &= (x^2+x+1)(x-1) \\ x^4 - 1 &= (x^2+1)(x+1)(x-1) \\ x^5 - 1 &= (x^4+x^3+x^2+x+1)(x-1) \\ x^6 - 1 &= (x^2-x+1)(x^2+x+1)(x+1)(x-1). \end{aligned} \tag{1}$$

The polynomials appearing in such factorizations are called **cyclotomic polynomials**. The first few cyclotomic polynomials are

$$\begin{aligned} &\Phi_1(x) = x - 1 \qquad \Phi_2(x) = x + 1 \qquad \Phi_3(x) = x^2 + x + 1 \\ &\Phi_4(x) = x^2 + 1 \qquad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1 \\ &\Phi_6(x) = x^2 - x + 1 \qquad \Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ &\Phi_8(x) = x^4 + 1 \qquad \Phi_9(x) = x^6 + x^3 + 1 \\ &\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1 \\ &\Phi_{11}(x) = x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\ &\Phi_{12}(x) = x^4 - x^2 + 1. \end{aligned}$$

Before giving the official definition of cyclotomic polynomials, we point out some noteworthy patterns that are already apparent among the cyclotomic polynomials listed.

1. It seems that the factors of $x^n - 1$ are exactly those cyclotomic polynomials whose index divides n. For example,

$$x^6 - 1 = \Phi_6(x)\Phi_3(x)\Phi_2(x)\Phi_1(x).$$

2. Looking at $\Phi_2(x)$, $\Phi_3(x)$, $\Phi_5(x)$, $\Phi_7(x)$ and $\Phi_{11}(x)$, it appears that, for prime p,

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1.$$

3. We have $\Phi_4(x) = \Phi_2(x^2)$, $\Phi_8(x) = \Phi_4(x^2) = \Phi_2(x^4)$, $\Phi_9(x) = \Phi_3(x^3)$, and $\Phi_{12}(x) = \Phi_6(x^2)$. (But also $\Phi_6(x) \neq \Phi_3(x^2)$ and $\Phi_6(x) \neq \Phi_2(x^3)$.)

Math. Mag. **89** (2016) 179–188. doi:10.4169/math.mag.89.3.179. © Mathematical Association of America
MSC: Primary 12E10, Secondary 11C08; 13B25.

4. We have $\Phi_6(x) = \Phi_3(-x)$ and $\Phi_{10}(x) = \Phi_5(-x)$. (But also $\Phi_4(x) \neq \Phi_2(-x)$ and $\Phi_{12}(x) \neq \Phi_6(-x)$.)
5. The coefficients of $\Phi_{10}(x)$ put in decreasing degree order are

$$1, -1, \quad 1, -1, \quad 1.$$

Reversing the order of this list leaves it unchanged. Polynomials with this symmetry are called **reciprocal**, and, except for $\Phi_1(x)$, all of the cyclotomic polynomials listed have this property.

6. All coefficients of these cyclotomic polynomials are 0, 1 or -1.

Are these observations about the first 12 cyclotomic polynomials special cases of theorems about all cyclotomic polynomials? As we will see the answer is yes in most cases. Only the last observation (6) about the coefficients of cyclotomic polynomials is wrong in general. It is easy to imagine that the first mathematicians to study these polynomials thought that the coefficients of all cyclotomic polynomials are in $\{-1, 0, 1\}$ because that is indeed the case for $\Phi_n(x)$ with $n < 105$. Remarkably,

$$\begin{aligned}\Phi_{105}(x) = x^{48} &+ x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} \\ &+ x^{36} + x^{35} + x^{34} + x^{33} + x^{32} + x^{31} - x^{28} - x^{26} \\ &- x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} \\ &+ x^{12} - x^{9} - x^{8} - 2x^{7} - x^{6} - x^{5} + x^{2} + x + 1\end{aligned} \tag{2}$$

has terms with coefficient -2. This property of Φ_{105} was noted by Migotti [**15**] in 1883 who also proved that, if p and q are distinct odd primes, then the coefficients of Φ_{pq} are in $\{-1, 0, 1\}$ (see Theorem 15). This situation has motivated a large amount of research into the coefficients of cyclotomic polynomials.

Basic properties

To define and to understand cyclotomic polynomials, we need to discuss their zeros. And for that, a bit of group theory—at least the language of group theory—is useful.

The set of nonzero complex numbers, $\mathbb{C}^\times$, forms a group under multiplication. For $\omega \in \mathbb{C}^\times$, the set $\langle\omega\rangle = \{\omega^m \mid m \in \mathbb{Z}\}$ is the **subgroup generated by** ω. The number of elements in this subgroup is called the **order** of ω, which we write as $\operatorname{ord}\omega$. (The usual notation for the order of an element in a group, $|\omega|$, conflicts with the notation for the norm (or absolute value) of complex numbers.)

The connection to the zeros of polynomials of the form $x^n - 1$ is provided by the following group theoretic lemma whose proof can be found in any abstract algebra textbook, for example, [**8**] and [**9**].

Lemma 1. *A complex number $\omega \in \mathbb{C}^\times$ has finite order if and only if $\omega^k = 1$ for some $k \in \mathbb{N}$. If $\operatorname{ord}\omega = n$ is finite, then*

1. *n is the smallest natural number such that $\omega^n = 1$,*
2. $\langle\omega\rangle = \{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$,
3. *for all $m \in \mathbb{Z}$, $\omega^m = 1$ if and only if n divides m.*

There are a lot of easy and useful consequences of this lemma.

1. If $\omega \in \mathbb{C}^\times$ has finite order, then $\omega^{\operatorname{ord}\omega} = 1$.

2. For any $n \in \mathbb{N}$, the zeros of $x^n - 1$ are exactly the complex numbers whose orders divide n.
3. Every complex number of order $n \in \mathbb{N}$ is a zero of $x^n - 1$. So, for example, to find **all** complex numbers of order 4, we need only look among the zeros of $x^4 - 1 = (x^2 + 1)(x + 1)(x - 1)$, namely, 1, -1, i and $-i$. It is easy to check that i and $-i$ are the only complex numbers of order 4, whereas 1 and -1 have orders 1 and 2.

There is other language for describing the complex numbers of interest. For any natural number n, a complex number ω is called an n^{th} **root of unity** if ω is a zero of $x^n - 1$, that is, if $\omega^n = 1$, and ω is called a **primitive** n^{th} **root of unity** if $\operatorname{ord}\omega = n$, equivalently, if ω is a zero of $x^n - 1$ but is not a zero of $x^m - 1$ for any $m < n$.

The key property of the complex numbers is that $x^n - 1$ has exactly n complex zeros, and these can be expressed trigonometrically using De Moivre's theorem.

Lemma 2. *[**9**, p. 18] Let $n \in \mathbb{N}$ and $\omega_n = e^{2\pi i/n} \in \mathbb{C}^\times$. Then $x^n - 1$ has n simple zeros in $\mathbb{C}^\times$, namely,*

$$\omega_n^m = e^{2\pi i m/n} = \cos(2\pi m/n) + i \sin(2\pi m/n)$$

for $0 \leq m < n$. Consequently, $\langle \omega_n \rangle$ is the set of zeros of $x^n - 1$ and $\operatorname{ord}\omega_n = n$.

One useful consequence of Lemma 2 is that if two monic polynomials divide $x^n - 1$ for some $n \in \mathbb{N}$, then they are identical if and only if they have the same zeros.

The following lemma provides a formula for the order of ω^m in the case that $\operatorname{ord}\omega$ is known.

Lemma 3. *Suppose that $\omega \in \mathbb{C}^\times$ has finite order. Then, for all $m \in \mathbb{N}$,*

$$m \operatorname{ord}\omega^m = \operatorname{lcm}(m, \operatorname{ord}\omega).$$

Proof. Lemma 1(3) is used four times in this proof! Let $\operatorname{ord}\omega = n$. Because $\omega^{m \operatorname{ord}\omega^m} = (\omega^m)^{\operatorname{ord}\omega^m} = 1$, n divides $m \operatorname{ord}\omega^m$. This implies that $m \operatorname{ord}\omega^m$ is a common multiple of n and m and so $\operatorname{lcm}(m, n)$ divides $m \operatorname{ord}\omega^m$.

On the other hand, because both m and n divide $\operatorname{lcm}(m, n)$, it follows that $\operatorname{lcm}(m, n)/m \in \mathbb{N}$ as well as $(\omega^m)^{\operatorname{lcm}(m,n)/m} = \omega^{\operatorname{lcm}(m,n)} = 1$. Consequently, $\operatorname{ord}\omega^m$ divides $\operatorname{lcm}(m, n)/m$ and, equivalently, $m \operatorname{ord}\omega^m$ divides $\operatorname{lcm}(m, n)$.

Lemma 3 makes it possible to be precise about which complex numbers have finite order.

Lemma 4. *A complex number has order $n \in \mathbb{N}$ if and only if it has the form $\omega_n^m = e^{2\pi i m/n}$ with $0 \leq m < n$ and $\gcd(m, n) = 1$.*

Proof. If a complex number has order n, then, by Lemma 1, it is a zero of $x^n - 1$, and, by Lemma 2, has the form ω_n^m for some m such that $0 \leq m < n$. Because of Lemma 3, ω_n^m has order n if and only if $\operatorname{lcm}(m, n) = mn$, which is equivalent to $\gcd(m, n) = 1$.

For example, 1, 5, 7, and 11 are the only natural numbers that are less than 12 and relatively prime to 12, and so ω_{12}, ω_{12}^5, ω_{12}^7, and ω_{12}^{11} are the complex numbers of order 12. In general, the number of complex numbers of order n is given by Euler's phi function [**5**] defined by

$$\varphi(n) = \big|\{m \in \mathbb{N} \mid m < n \text{ and } \gcd(m, n) = 1\}\big|.$$

We should mention that all the above results are special cases of theorems that hold in any group. See, for example, [**9**, Section 6] and [**8**, Section 2.3].

We are finally ready to define cyclotomic polynomials.

Definition 5. *For $n \in \mathbb{N}$, the n^{th}* ***cyclotomic polynomial*** *is*

$$\Phi_n(x) = \prod_{\operatorname{ord}\omega = n} (x - \omega).$$

Thus, $\Phi_n(x)$ is the monic polynomial whose zeros are the complex numbers of order n.

For example, since 1 is the only the complex number of order 1 and -1 is the only the complex number of order 2 we have

$$\Phi_1(x) = x - 1 \qquad \Phi_2(x) = x + 1.$$

Also, since $\pm i$ are all the complex numbers of order 4 we have

$$\Phi_4(x) = (x - i)(x + i) = x^2 + 1.$$

By Lemma 1(3), the zeros of $x^4 - 1$ are exactly those complex numbers whose orders divide 4. Hence

$$\begin{aligned} x^4 - 1 &= \prod_{(\operatorname{ord}\omega)|4} (x - \omega) \\ &= \left(\prod_{\operatorname{ord}\omega=1} (x - \omega)\right)\left(\prod_{\operatorname{ord}\omega=2} (x - \omega)\right)\left(\prod_{\operatorname{ord}\omega=4} (x - \omega)\right) \\ &= \Phi_1(x)\Phi_2(x)\Phi_4(x). \end{aligned}$$

The argument made for $n = 4$ generalizes very easily to yield the following lemma.

Lemma 6. *For $n \in \mathbb{N}$, $x^n - 1 = \prod_{d|n} \Phi_d(x)$.*

Proof. Since $x^n - 1$ has exactly n simple zeros (Lemma 2), to prove the claim it suffices to check that the polynomials on the left and right of the equal sign have the same zeros. But that is exactly what Lemma 1(3) says.

Lemma 6 makes calculating cyclotomic polynomials much easier. For example, $\Phi_1(x) = x - 1$ and $x^5 - 1 = \Phi_5(x)\Phi_1(x)$, so,

$$\Phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1.$$

To calculate $\Phi_{10}(x)$, we use

$$x^{10} - 1 = \Phi_{10}(x)\Phi_5(x)\Phi_2(x)\Phi_1(x).$$

Dividing $x^{10} - 1$ by

$$\Phi_5(x)\Phi_2(x)\Phi_1(x) = (x^4 + x^3 + x^2 + x + 1)(x + 1)(x - 1) = x^6 + x^5 - x - 1$$

we get $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$. Note that $\Phi_{10}(x) = \Phi_5(-x)$, a relationship that we generalize in Lemma 11.

The fact that all cyclotomic polynomials have integer coefficients is not at all obvious from the definition and needs a proof:

Lemma 7. *For all $n \in \mathbb{N}$, $\Phi_n(x) \in \mathbb{Z}[x]$.*

Proof. We prove the claim by induction on $n \in \mathbb{N}$. Since $\Phi_1(x) = x - 1 \in \mathbb{Z}[x]$ the claim is true for $n = 1$.

Now suppose $n > 1$. By Lemma 6,

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x)g(x),$$

where $g(x)$ is the product of all the cyclotomic polynomials $\Phi_d(x)$ with d a proper positive factor of n. By the induction hypothesis, $\Phi_d(x) \in \mathbb{Z}[x]$ for all such cyclotomic polynomials and hence $g(x) \in \mathbb{Z}[x]$. Since cyclotomic polynomials are monic by construction, and products of monic polynomials are monic, $g(x)$ is also monic.

Then $\Phi_n(x)$ is the quotient of $x^n - 1 \in \mathbb{Z}[x]$ by the monic polynomial $g(x) \in \mathbb{Z}[x]$, so $\Phi_n(x)$ is also in $\mathbb{Z}[x]$.

A similar induction proof, left to the reader, shows that $\Phi_n(0) = 1$ for all $n > 1$.

Lemma 8. *For $m, n \in \mathbb{N}$,*

$$\Phi_n(x^m) = \prod_{d \in D} \Phi_d(x),$$

where $D = \{d \in \mathbb{N} \mid \operatorname{lcm}(m, d) = mn\}$.

Proof. Because $\Phi_n(x)$ divides $x^n - 1$, we see that $\Phi_n(x^m)$ divides $x^{mn} - 1$. And, if $d \in D$, then d divides $\operatorname{lcm}(m, d) = mn$ and so, by Lemma 6, the right side of the equation also divides $x^{mn} - 1$. The zeros of $x^{mn} - 1$ are distinct (Lemma 2), so to prove the claim it suffices to confirm that both sides of the equation have the same zeros. For this we just need Lemma 3:

A number $\omega \in \mathbb{C}$ is a zero of $\Phi_n(x^m)$ if and only if $\operatorname{ord} \omega^m = n$, if and only if $\operatorname{lcm}(m, \operatorname{ord} \omega) = mn$, if and only if $\operatorname{ord} \omega \in D$, if and only if ω is a zero of $\prod_{d \in D} \Phi_d(x)$.

For example, if $m = 2$ and $n = 3$, then

$$D = \{d \in \mathbb{N} \mid \operatorname{lcm}(2, d) = 6\} = \{3, 6\}$$

and so $\Phi_3(x^2) = \Phi_6(x)\Phi_3(x)$.

The condition $\operatorname{lcm}(m, d) = mn$ in the definition of D is rather obscure, so to make further use of Lemma 8, we derive a simpler description of D. (See [**5**] for the relevant facts on greatest common divisors and least common multiples.)

Suppose that $d \in D$, that is, $\operatorname{lcm}(m, d) = mn$. Set $k = m/\gcd(m, d)$ so, in particular, $k|m$. Because of the identity $\gcd(a, b) \operatorname{lcm}(a, b) = ab$ for all $a, b \in \mathbb{N}$, we get $n \gcd(d, m) = d$ and $dk = mn$. In addition, because of the identity $a \gcd(b, c) = \gcd(ab, ac)$ for all $a, b, c \in \mathbb{N}$, we have

$$d \gcd(n, k) = \gcd(dn, dk) = \gcd(dn, mn) = n \gcd(d, m) = d$$

and so $\gcd(n, k) = 1$.

Thus, if $d \in D$, then $d = mn/k$ for some $k \in \mathbb{N}$ such that $k|m$ and $\gcd(n, k) = 1$. The converse of this statement can be proved similarly giving

$$D = \left\{ \frac{mn}{k} \mid k \in \mathbb{N} \text{ and } k|m \text{ and } \gcd(n, k) = 1 \right\}. \tag{3}$$

Lemma 9. *If every prime divisor of $m \in \mathbb{N}$ is also a divisor of $n \in \mathbb{N}$, then $\Phi_{mn}(x) = \Phi_n(x^m)$.*

Proof. We use Lemma 8 with D as given by (3). If $d \in D$, then $d = mn/k$ for some $k \in \mathbb{N}$ such that $k|m$ and $\gcd(n, k) = 1$. If p is a prime divisor of k, then, because $k|m$,

p divides m, and then, by assumption, p divides n. But then p divides $\gcd(n, k)$, contradicting $\gcd(n, k) = 1$.

Thus, $k \in \mathbb{N}$ has no prime divisors, $k = 1$ and $d = mn$, $D = \{mn\}$ and $\Phi_n(x^m) = \Phi_{mn}(x)$.

This result enables us to calculate many new cyclotomic polynomials. For example, since $400 = 40 \cdot 10$ and every prime that divides 40 divides 10, we have

$$\Phi_{400}(x) = \Phi_{10}(x^{40}) = x^{160} - x^{120} + x^{80} - x^{40} + 1.$$

Note that $\Phi_{400}(x)$ and $\Phi_{10}(x)$ have the same coefficients.

Corollary 10. *Let n be the product of the prime numbers that divide $m \in \mathbb{N}$. Then $\Phi_m(x) = \Phi_n(x^{m/n})$ and, in particular, $\Phi_m(x)$ and $\Phi_n(x)$ have the same coefficients.*

Proof. Since every prime that divides m/n divides n, this follows directly from Lemma 9.

The main consequence of this corollary is that, for discussion of the coefficients of cyclotomic polynomials, we need only consider $\Phi_n(x)$ when n is a product of distinct prime numbers.

Lemma 11. *If $n \in \mathbb{N}$ is odd, then $\Phi_{2n}(x) = \Phi_n(-x)$.*

Proof. From Lemma 8, we find $\Phi_n(x^2) = \Phi_{2n}(x)\Phi_n(x)$. Replacing x by $-x$ in this equation gives

$$\Phi_{2n}(x)\Phi_n(x) = \Phi_{2n}(-x)\Phi_n(-x). \tag{4}$$

Since $\Phi_n(x^2)$ divides $x^{2n} - 1$, it has only simple zeros. So to prove the claim it suffices to match the zeros on both sides of (4).

If $\Phi_n(\omega) = 0$, then $\operatorname{ord} \omega = n$ so, in particular, $\omega^n = 1$. Since n is odd, $(-\omega)^n = -1$ and so $-\omega$ does not have order n. This means that $-\omega$ must be a zero of $\Phi_{2n}(x)$ and have order $2n$.

Similarly, if $\Phi_{2n}(\omega) = 0$, then $\omega^n \neq 1$ and $(\omega^n)^2 = 1$ and so $\omega^n = -1$. Consequently, $(-\omega)^n = 1$ and so $-\omega$ does not have order $2n$. This means that $-\omega$ has order n and is a zero of $\Phi_n(x)$.

Cyclotomic polynomials have the property that their coefficients are the same when read backward as forward. Such polynomials are called reciprocal polynomials. Specifically, if $f(x)$ is a polynomial of degree m, then $x^m f(1/x)$ is called the **reverse** of f, and f is a **reciprocal polynomial** if it is equal to its reverse, that is, if

$$f(x) = x^m f(1/x). \tag{5}$$

It is not hard to see that the reverse of f is the polynomial f with its coefficients in reverse order. For example, if $f(x) = x^4 + 2x^3 + 3x^2 + 4x + 5$, then

$$\begin{aligned} x^4 f(1/x) &= x^4 \left[(1/x)^4 + 2(1/x)^3 + 3(1/x)^2 + 4(1/x) + 5\right] \\ &= 1 + 2x + 3x^2 + 4x^3 + 5x^4 \\ &= 5x^4 + 4x^3 + 3x^2 + 2x + 1. \end{aligned}$$

So a polynomial is reciprocal if and only if the sequence of its coefficients is symmetric with respect to reversal of order. Because of this property, these polynomials are sometimes called **palindromic**.

Lemma 12. *If $n > 1$, then $\Phi_n(x)$ is a reciprocal polynomial.*

Proof. Directly from the definition, if $\omega \in \mathbb{C}^\times$, then $\langle \omega \rangle = \langle \omega^{-1} \rangle$ and so $\operatorname{ord} \omega = n$ if and only if $\operatorname{ord} \omega^{-1} = n$. This means that the function $\omega \mapsto \omega^{-1}$ is a permutation of the set of zeros of $\Phi_n(x)$. Thus, $x^m \Phi_n(1/x)$, with $m = \deg \Phi_n(x)$, has the same set of zeros as $\Phi_n(x)$. The leading coefficient of $x^m \Phi_n(1/x)$ is the constant term of $\Phi_n(x)$ which is 1 for $n > 1$ (see comment after Lemma 7). Thus, $x^m \Phi_n(1/x) = \Phi_n(x)$ for all $n > 1$.

One of the most important properties of cyclotomic polynomials is that they are irreducible over $\mathbb{Q}$. This means that they do not factor into lower-degree polynomials with rational coefficients. Proofs of this fact and its consequences are to be found in many algebra textbooks (which is why this article is focused on the coefficients). See, for example, [**8**, Section 13.6] and [**17**].

The main result

We are now in a position to prove that the coefficients of $\Phi_n(x)$ are in $\{-1, 0, 1\}$ for all $n < 105$. To start, we need some formulas for cyclotomic polynomials whose indices contain two or fewer primes.

Lemma 13. *Let p and q be distinct prime numbers.*

1. $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$
2. $\Phi_q(x^p) = \Phi_{pq}(x)\, \Phi_q(x)$
3. $(x^{pq} - 1)\, \Phi_{pq}(x) = \Phi_q(x^p)\, \Phi_p(x^q)\, (x - 1)$.

Proof. These equations could be obtained from Lemma 8, but it is just as easy to derive them from $\Phi_1(x) = x - 1$ and

$$x^p - 1 = \Phi_p(x)\Phi_1(x) \qquad x^q - 1 = \Phi_q(x)\Phi_1(x)$$
$$x^{pq} - 1 = \Phi_{pq}(x)\Phi_p(x)\Phi_q(x)\Phi_1(x),$$

which are obtained from Lemma 6.

1. $\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1$.
2. As well as the expression for $x^{pq} - 1$ above, we have

$$\begin{aligned} x^{pq} - 1 = (x^p)^q - 1 &= \Phi_q(x^p)\Phi_1(x^p) = \Phi_q(x^p)(x^p - 1) \\ &= \Phi_q(x^p)\Phi_p(x)\Phi_1(x). \end{aligned}$$

   Cancellation from the two expressions for $x^{pq} - 1$ gives $\Phi_q(x^p) = \Phi_{pq}(x)\, \Phi_q(x)$.

3. This follows from $\Phi_q(x^p) = \Phi_{pq}(x)\, \Phi_q(x)$, $\Phi_p(x^q) = \Phi_{pq}(x)\, \Phi_p(x)$ and the above expression for $x^{pq} - 1$.

We note for future reference that, from (2) or (3) of this lemma, the degree of $\Phi_{pq}(x)$ is $pq - p - q + 1 = (p - 1)(q - 1)$ and is strictly less than pq.

The following lemma is really a weak version of the Chinese remainder theorem [**5**, Theorem 4.8].

Lemma 14. *If p and q are distinct primes, then the coefficients of $\Phi_q(x^p)\, \Phi_p(x^q)$ are in $\{0, 1\}$.*

Proof. From Lemma 13(1), we get

$$\Phi_q(x^p)\,\Phi_p(x^q) = \big(1 + x^p + \cdots + x^{(q-1)p}\big)\big(1 + x^q + \cdots + x^{(p-1)q}\big) = \sum_{\substack{0 \le m < q \\ 0 \le n < p}} x^{mp+nq}.$$

To complete the proof, it suffices to show that each of the pq terms in this sum has distinct degree. Suppose, to the contrary, that $pm + qn = pm' + qn'$ with $0 \le m < m' < q$. Then $p(m - m') = q(n' - n)$, and, because p and q are distinct primes, q divides $m - m'$. But $0 < m - m' < q$, so this is not possible.

Theorem 15. *If p and q are distinct primes, then the coefficients of $\Phi_{pq}(x)$ are in* $\{-1, 0, 1\}$.

Proof. From Lemma 13(3), we have

$$(x^{pq} - 1)\,\Phi_{pq}(x) = \Phi_q(x^p)\,\Phi_p(x^q)\,(x - 1). \tag{6}$$

Consider the left side of this equation. Since the degree of Φ_{pq} is less than pq, all nonzero terms of $x^{pq}\Phi_{pq}(x)$ have greater degree than the nonzero terms of $\Phi_{pq}(x)$. Hence, the coefficients of $(x^{pq} - 1)\,\Phi_{pq}(x)$ are, up to sign, simply the coefficients of Φ_{pq}.

To complete the proof, it suffices to show that the coefficients on the right side of (6) are in $\{-1, 0, 1\}$. From Lemma 14, the coefficients of $x\Phi_q(x^p)\,\Phi_p(x^q)$ are in $\{0, 1\}$ and the coefficients of $-\Phi_q(x^p)\,\Phi_p(x^q)$ are in $\{0, -1\}$. Hence, the coefficients of the sum of these two polynomials, namely $\Phi_q(x^p)\,\Phi_p(x^q)\,(x - 1)$, are in $\{-1, 0, 1\}$, as claimed.

For another proof, see [**13**].

It is now easy to see that $\Phi_{105}(x)$ is the cyclotomic polynomial of least possible index whose coefficients may not be in $\{-1, 0, 1\}$.

Theorem 16. *If $n \in \mathbb{N}$ has at most two odd prime divisors, then the coefficients of $\Phi_n(x)$ are in* $\{-1, 0, 1\}$.

Proof. We consider several cases:

1. If $n = p$ is prime, then, by Lemma 13(1),

$$\Phi_n(x) = \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

2. If $n = pq$ for primes p and q, then Theorem 15 applies.
3. If $n = 2pq$ for odd primes p and q, then, by Lemma 11, $\Phi_n(x) = \Phi_{2(pq)}(x) = \Phi_{pq}(-x)$ and Theorem 15 applies again.

Thus, for all these cases, and, by Corollary 10, for all n that have at most two distinct odd prime factors, the coefficients of $\Phi_n(x)$ are in $\{-1, 0, 1\}$.

The smallest $n \in \mathbb{N}$ for which the argument of Theorem 16 fails is the the smallest number that has three distinct odd prime factors, namely $n = 3 \cdot 5 \cdot 7 = 105$. After $n = 105$, the next few numbers that have three or more odd prime factors are $3 \cdot 5 \cdot 11 = 165$, $3 \cdot 5 \cdot 13 = 195$, $2 \cdot 3 \cdot 5 \cdot 7 = 210$, $3 \cdot 7 \cdot 11 = 231$, $3 \cdot 5 \cdot 17 = 255$, $3 \cdot 7 \cdot 13 = 273$, and $3 \cdot 5 \cdot 19 = 285$. Except for $\Phi_{231}(x)$, all of the corresponding cyclotomic polynomials have coefficients that are not in $\{-1, 0, 1\}$.

Other results

Cyclotomic polynomials of the form $\Phi_{pqr}(x)$ with p, q and r odd primes are called ternary. The coefficients of these polynomials continue to be the subject of much research. To discuss this, suppose that $p < q < r$ and let $A(n)$ be the largest coefficient of $\Phi_n(x)$ in absolute value. So, for example, $A(105) = 2$. Then already in 1895, Bang [**3**] proved that $A(pqr) \le p - 1$. In 1968, Beiter [**4**] conjectured that $A(pqr) \le (p + 1)/2$ and proved this bound for $p = 3$ and $p = 5$. Much later, it was noticed that $A(17 \cdot 29 \cdot 41) = 10$ whereas, with $p = 17$, $(p + 1)/2 = 9$, and so Beiter's conjecture is false. In 2009, Gallot and Moree [**11**] proposed a corrected Beiter conjecture, $A(pqr) \le 2p/3$, that has now been proven by Zhao and Zhang [**18**].

In another direction, G. Bachman [**2**] showed that there are infinitely many ternary cyclotomic polynomials $\Phi_{pqr}(x)$ for which $A(pqr) = 1$. The smallest example of this is $\Phi_{231}(x) = \Phi_{3\cdot7\cdot11}(x)$. See also [**12**].

A recent discovery, due to Gallot and Moree [**10**], is that neighboring coefficients of ternary cyclotomic polynomials differ by at most one. This can be seen already in $\Phi_{105}(x)$ (2) whose coefficients, when put in degree order, are

$$1,1,1,0,0,-1,-1,-2,-1,-1,0,0,1,1,1,1,1,1,0,0,-1,0,-1,0,-1,$$
$$0,-1,0,-1,0,0,1,1,1,1,1,1,0,0,-1,-1,-2,-1,-1,0,0,1,1,1.$$

In particular, -2 in this list is preceded and followed by -1. See also [**6, 7**].

What about cyclotomic polynomials involving four or more primes? In 1931, I. Schur (see [**14, 16**]) showed that there is, in general, no bound on the size of the coefficients of cyclotomic polynomials, essentially because there is no bound on the number of prime numbers. If the goal is to find cyclotomic polynomials with large coefficients, then the obvious candidates are polynomials whose indices are products of many distinct odd primes.

For example, for the product of the first nine odd primes, we get [**1**]

$$A(3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29) = 2\,888\,582\,082\,500\,892\,851.$$

Another product of nine odd primes is

$$N = 13\,162\,764\,615 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 19 \cdot 29 \cdot 37 \cdot 43$$

and

$$A(N) = 5\,465\,808\,676\,670\,557\,863\,536\,977\,958\,031\,695\,430\,428\,633.$$

The degree of $\Phi_N(x)$ is 4 389 396 480, so it is easy to imagine the scale of the computation needed to find $A(N)$. Calculating $A(n)$ when n is a product of 10 distinct primes is still out of the reach of modern computers. For these computational results and much more, see [**1**].

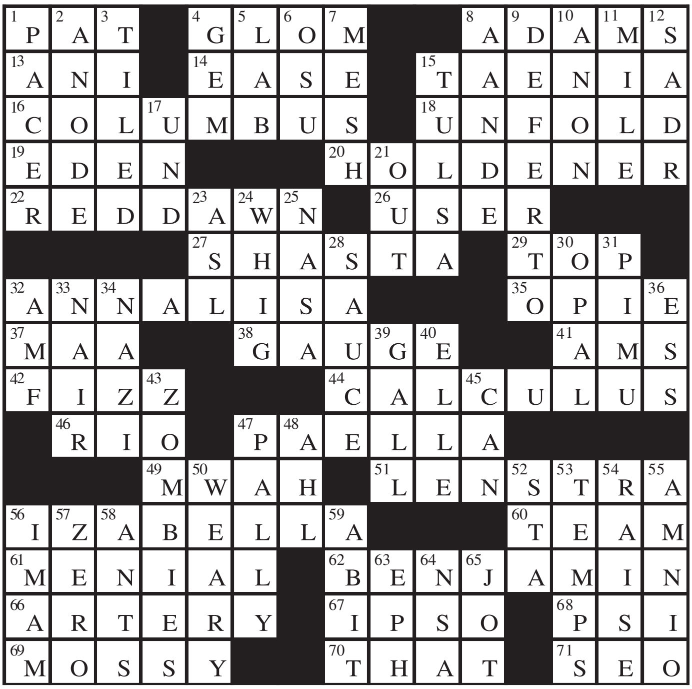
REFERENCES

1. A. Arnold, M. Monagan, Calculating cyclotomic polynomials, *Math. Comp.* **80** (2011) 2359–2379.
2. G. Bachman, Flat cyclotomic polynomials of order three, *Bull. London Math. Soc.* **38** (2006) 53–60.
3. A.S. Bang, Om Ligningen $\Phi_n(x) = 0$, *Nyt Tidsskrift for Mathematik (B)* **6** (1895) 6–12.
4. M. Beiter, Magnitude of the coefficients of the cyclotomic polynomial $F_{pqr}(x)$. *Amer. Math. Monthly* **75** (1968) 370–372.
5. D. Burton, *Elementary Number Theory.* Seventh edition. McGraw-Hill, New York, 2010.
6. B. Bzdęga, Bounds on ternary cyclotomic coefficients, *Acta Arith.* **144** (2010) 5–16.

7. B. Bzdęga, Jumps of ternary cyclotomic coefficients, *Acta Arith.* **163** (2014) 203–213.
8. D. Dummit, R. Foote, *Abstract Algebra.* Third edition. Wiley, Hoboken, 2003.
9. J. Fraleigh, *A First Course in Abstract Algebra.* Seventh edition. Pearson, Boston, 2002.
10. Y. Gallot, P. Moree, Neighboring ternary cyclotomic coefficients differ by at most one, *J. Ramanujan Math. Soc.* **24** (2009) 235–248.
11. Y. Gallot, P. Moree, Ternary cyclotomic polynomials having a large coefficient, *J. Reine Angew. Math.* **632** (2009) 105-125.
12. N. Kaplan. Flat cyclotomic polynomials of order three. *J. Number Theory* **127** (2007) 118–126.
13. T.Y. Lam, K.H. Leung, On the cyclotomic polynomial $\Phi_{pq}(X)$, *Amer. Math. Monthly* **103** (1996) 562–564.
14. E. Lehmer, On the magnitude of the coefficients of the cyclotomic polynomials, *Bull. Amer. Math Soc.* **42** (1936) 389–392.
15. A. Migotti, Zur Theorie der Kreisteilungsgleichung, *S.-B. der Math.-Naturwiss. Classe der Kaiser. Akad. der Wiss., Wien*, **87** (1883) 7–14.
16. J. Suzuki, On the coefficients of cyclotomic polynomials, *Proc. Japan Acad.* **63** Series A, (1987) 279–280.
17. S. Weintraub, Several proofs of the irreducibility of the cyclotomic polynomials, *Amer. Math. Monthly* **120** (2013) 537–545.
18. J. Zhao, X. Zhang, A proof of the corrected Beiter conjecture. arXiv:0910.2770

Summary. One of the most surprising properties of cyclotomic polynomials is that their coefficients are all 1, −1 or zero—at least that seems to be the case until one notices that the 105th cyclotomic polynomial has a coefficient of −2. This article serves as an introduction to these polynomials with a particular emphasis on their coefficients and proves that the coefficients of the first 104 cyclotomic polynomials are at most one in absolute value.

GARY BROOKFIELD (MR Author ID: 630431) got his Ph.D. at the University of California, Santa Barbara in 1997 and was a visiting professor at the University of Wisconsin, Madison, the University of Iowa, and the University of California, Riverside. He is currently a professor at California State University, Los Angeles. His interests include polynomials, forms, as well as the revival of the theory of invariants.



1 P	2 A	3 T	■	4 G	5 L	6 O	7 M	■	■	8 A	9 D	10 A	11 M	12 S
13 A	N	I	■	14 E	A	S	E	■	15 T	A	E	N	I	A
16 C	O	L	17 U	M	B	U	S	■	18 U	N	F	O	L	D
19 E	D	E	N	■	■	■	20 H	21 O	L	D	E	N	E	R
22 R	E	D	D	23 A	24 W	25 N	■	26 U	S	E	R	■	■	■
■	■	■	■	27 S	H	A	28 S	T	A	■	29 T	30 O	31 P	■
32 A	33 N	34 N	A	L	I	S	A	■	■	■	35 O	P	I	36 E
37 M	A	A	■	■	38 G	A	U	39 G	40 E	■	■	41 A	M	S
42 F	I	Z	43 Z	■	■	■	44 C	A	L	45 C	U	L	U	S
■	46 R	I	O	■	47 P	48 A	E	L	L	A	■	■	■	■
■	■	■	49 M	50 W	A	H	■	51 L	E	N	52 S	53 T	54 R	55 A
56 I	57 Z	58 A	B	E	L	L	59 A	■	■	■	60 T	E	A	M
61 M	E	N	I	A	L	■	62 B	63 E	64 N	65 J	A	M	I	N
66 A	R	T	E	R	Y	■	67 I	P	S	O	■	68 P	S	I
69 M	O	S	S	Y	■	■	70 T	H	A	T	■	71 S	E	O