Cyclotomic polynomial

In mathematics, more specifically in algebra, the ***n*th cyclotomic polynomial**, for any positive integer n, is the unique irreducible polynomial with integer coefficients that is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any $k < n$. Its roots are all nth primitive roots of unity $e^{2i\pi\frac{k}{n}}$, where k runs over the positive integers not greater than n and coprime to n. In other words, the ***n*th cyclotomic polynomial** is equal to

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ \gcd(k,n)=1}} \left(x - e^{2i\pi\frac{k}{n}}\right).$$

It may also be defined as the monic polynomial with integer coefficients that is the minimal polynomial over the field of the rational numbers of any primitive nth-root of unity ($e^{2i\pi/n}$ is an example of such a root).

An important relation linking cyclotomic polynomials and primitive roots of unity is

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

showing that x is a root of $x^n - 1$ if and only if it is a dth primitive roots of unity for some d that divides n.

Contents

Examples

If n is a prime number, then

$$\Phi_n(x) = 1 + x + x^2 + \cdots + x^{n-1} = \sum_{k=0}^{n-1} x^k.$$

If $n = 2p$ where p is an odd prime number, then

$$\Phi_{2p}(x) = 1 - x + x^2 - \cdots + x^{p-1} = \sum_{k=0}^{p-1} (-x)^k.$$

For n up to 30, the cyclotomic polynomials are:[1]

$$
\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1 \\
\Phi_7(x) &= x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_8(x) &= x^4 + 1 \\
\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 \\
\Phi_{13}(x) &= x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{14}(x) &= x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \\
\Phi_{15}(x) &= x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 \\
\Phi_{16}(x) &= x^8 + 1 \\
\Phi_{17}(x) &= x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{18}(x) &= x^6 - x^3 + 1 \\
\Phi_{19}(x) &= x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{20}(x) &= x^8 - x^6 + x^4 - x^2 + 1 \\
\Phi_{21}(x) &= x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1 \\
\Phi_{22}(x) &= x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \\
\Phi_{23}(x) &= x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} + x^{12} + x^{11} \\
&\quad + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{24}(x) &= x^8 - x^4 + 1 \\
\Phi_{25}(x) &= x^{20} + x^{15} + x^{10} + x^5 + 1 \\
\Phi_{26}(x) &= x^{12} - x^{11} + x^{10} - x^9 + x^8 - x^7 + x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 \\
\Phi_{27}(x) &= x^{18} + x^9 + 1 \\
\Phi_{28}(x) &= x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1 \\
\Phi_{29}(x) &= x^{28} + x^{27} + x^{26} + x^{25} + x^{24} + x^{23} + x^{22} + x^{21} + x^{20} + x^{19} + x^{18} + x^{17} + x^{16} + x^{15} + x^{14} \\
&\quad + x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \\
\Phi_{30}(x) &= x^8 + x^7 - x^5 - x^4 - x^3 + x + 1.
\end{aligned}
$$

The case of the 105th cyclotomic polynomial is interesting because 105 is the lowest integer that is the product of three distinct odd prime numbers and this polynomial is the first one that has a coefficient other than 1, 0, or −1:

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

Properties

Fundamental tools

The cyclotomic polynomials are monic polynomials with integer coefficients that are irreducible over the field of the rational numbers. Except for n equal to 1 or 2, they are palindromics of even degree.

The degree of Φ_n, or in other words the number of nth primitive roots of unity is $\varphi(n)$, where φ is Euler's totient function

The fact that Φ_n is an irreducible polynomial of degree $\varphi(n)$ in the ring $\mathbb{Z}[x]$ is a nontrivial result due to Gauss.[2] Depending on the chosen definition, it is either the value of the degree or the irreducibility which is a nontrivial result. The case of prime n is easier to prove than the general case, thanks to Eisenstein's criterion

A fundamental relation involving cyclotomic polynomials is

$$
x^n - 1 = \prod_{1 \leqslant k \leqslant n} \left(x - e^{2i\pi \frac{k}{n}} \right) = \prod_{d \mid n} \prod_{\substack{1 \leqslant k \leqslant n \\ \gcd(k,n) = d}} \left(x - e^{2i\pi \frac{k}{n}} \right) = \prod_{d \mid n} \Phi_{\frac{n}{d}}(x) = \prod_{d \mid n} \Phi_d(x).
$$

which means that each n-th root of unity is a primitive d-th root of unity for a unique d dividing n.

The Möbius inversion formula allows the expression of $\Phi_n(x)$ as an explicit rational fraction:

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

where μ is the Möbius function.

The Fourier transform of functions of the greatest common divisor together with the Möbius inversion formula gives:[3]

$$\Phi_n(x) = \prod_{k=1}^{n} \left(x^{\gcd(k,n)} - 1\right)^{\cos\left(\frac{2\pi k}{n}\right)}.$$

The cyclotomic polynomial $\Phi_n(x)$ may be computed by (exactly) dividing $x^n - 1$ by the cyclotomic polynomials of the proper divisors of n previously computed recursively by the same method:

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}$$

(Recall that $\Phi_1(x) = x - 1$.)

This formula allows computation of $\Phi_n(x)$ on a computer for any n, as soon as integer factorization and division of polynomials are available. Many computer algebra systems have a built in function to compute the cyclotomic polynomials. For example, this function is called by typing `cyclotomic_polynomial(n,x)` in SageMath, `numtheory[cyclotomic](n,x);` in Maple, and `Cyclotomic[n,x]` in Mathematica.

Easy cases for computation

As noted above, if n is a prime number, then

$$\Phi_n(x) = 1 + x + x^2 + \cdots + x^{n-1} = \sum_{i=0}^{n-1} x^i.$$

If n is an odd integer greater than one, then

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

In particular, if $n=2p$ is twice an odd prime, then (as noted above)

$$\Phi_n(x) = 1 - x + x^2 - \cdots + x^{p-1} = \sum_{i=0}^{p-1} (-x)^i.$$

If $n=p^m$ is a prime power (where p is prime), then

$$\Phi_n(x) = \Phi_p(x^{p^{m-1}}) = \sum_{i=0}^{p-1} x^{ip^{m-1}}.$$

More generally, if $n=p^m r$ with r relatively prime to p, then

$$\Phi_n(x) = \Phi_{pr}(x^{p^{m-1}}).$$

These formulas may be applied repeatedly to get a simple expression for any cyclotomic polynomial $\Phi_n(x)$ in term of a cyclotomic polynomial of square free index: If q is the product of the prime divisors of n (its radical), then[4]

$$\Phi_n(x) = \Phi_q(x^{n/q}).$$

This allows to give formulas for the nth cyclotomic polynomial when n has at most one odd prime factor: If p is an odd prime number, and h and k are positive integers, then:

$$\Phi_{2^h}(x) = x^{2^{h-1}} + 1$$

$$\Phi_{p^k}(x) = \sum_{i=0}^{p-1} x^{ip^{k-1}}$$

$$\Phi_{2^h p^k}(x) = \sum_{i=0}^{p-1} (-1)^i x^{i2^{h-1}p^{k-1}}$$

For the other values of n, the computation of the nth cyclotomic polynomial is similarly reduced to that of $\Phi_q(x)$, where q is the product of the distinct odd prime divisors of n. To deal with this case, one has that, for p prime and not dividing n,[5]

$$\Phi_{np}(x) = \Phi_n(x^p)/\Phi_n(x).$$

Integers appearing as coefficients

The problem of bounding the magnitude of the coefficients of the cyclotomic polynomials has been the object of a number of research papers.

If n has at most two distinct odd prime factors, then Migotti showed that the coefficients of Φ_n are all in the set {1, −1, 0}.[6]

The first cyclotomic polynomial for a product of three different odd prime factors is $\Phi_{105}(x)$; it has a coefficient −2 (see its expression above). The converse is not true: $\Phi_{231}(x) = \Phi_{3\times7\times11}(x)$ only has coefficients in {1, −1, 0}.

If n is a product of more different odd prime factors, the coefficients may increase to very high values. E.g., $\Phi_{15015}(x) = \Phi_{3\times5\times7\times11\times13}(x)$ has coefficients running from −22 to 22, $\Phi_{255255}(x) = \Phi_{3\times5\times7\times11\times13\times17}(x)$, the smallest n with 6 different odd primes, has coefficients up to ±532.

Let $A(n)$ denote the maximum absolute value of the coefficients of Φ_n. It is known that for any positive k, the number of n up to x with $A(n) > n^k$ is at least $c(k)\cdot x$ for a positive $c(k)$ depending on k and x sufficiently large. In the opposite direction, for any function $\psi(n)$ tending to infinity with n we have $A(n)$ bounded above by $n^{\psi(n)}$ for almost all n.[7]

Gauss's formula

Let n be odd, square-free, and greater than 3. Then:[8][9]

$$4\Phi_n(z) = A_n^2(z) - (-1)^{\frac{n-1}{2}} nz^2 B_n^2(z)$$

where both $A_n(z)$ and $B_n(z)$ have integer coefficients, $A_n(z)$ has degree $\varphi(n)/2$, and $B_n(z)$ has degree $\varphi(n)/2 - 2$. Furthermore, $A_n(z)$ is palindromic when its degree is even; if its degree is odd it is antipalindromic. Similarly, $B_n(z)$ is palindromic unless n is composite and ≡ 3 (mod 4), in which case it is antipalindromic.

The first few cases are

$$\begin{aligned}
4\Phi_5(z) &= 4(z^4 + z^3 + z^2 + z + 1) \\
&= (2z^2 + z + 2)^2 - 5z^2 \\
4\Phi_7(z) &= 4(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) \\
&= (2z^3 + z^2 - z - 2)^2 + 7z^2(z + 1)^2 \\
4\Phi_{11}(z) &= 4(z^{10} + z^9 + z^8 + z^7 + z^6 + z^5 + z^4 + z^3 + z^2 + z + 1) \\
&= (2z^5 + z^4 - 2z^3 + 2z^2 - z - 2)^2 + 11z^2(z^3 + 1)^2
\end{aligned}$$

Lucas's formula

Let n be odd, square-free and greater than 3. Then[10]

$$\Phi_n(z) = U_n^2(z) - (-1)^{\frac{n-1}{2}} nzV_n^2(z)$$

where both $U_n(z)$ and $V_n(z)$ have integer coefficients, $U_n(z)$ has degree $\varphi(n)/2$, and $V_n(z)$ has degree $\varphi(n)/2 - 1$. This can also be written

$$\Phi_n\left((-1)^{\frac{n-1}{2}} z\right) = C_n^2(z) - nzD_n^2(z).$$

If n is even, square-free and greater than 2 (this forces $n/2$ to be odd),

$$\Phi_{\frac{n}{2}}\left(-z^2\right) = \Phi_{2n}(z) = C_n^2(z) - nzD_n^2(z)$$

where both $C_n(z)$ and $D_n(z)$ have integer coefficients, $C_n(z)$ has degree $\varphi(n)$, and $D_n(z)$ has degree $\varphi(n) - 1$. $C_n(z)$ and $D_n(z)$ are both palindromic.

The first few cases are:

$$\begin{aligned}\Phi_3(-z) &= \Phi_6(z) = z^2 - z + 1 \\ &= (z+1)^2 - 3z\end{aligned}$$

$$\begin{aligned}\Phi_5(z) &= z^4 + z^3 + z^2 + z + 1 \\ &= (z^2 + 3z + 1)^2 - 5z(z+1)^2\end{aligned}$$

$$\begin{aligned}\Phi_{6/2}(-z^2) &= \Phi_{12}(z) = z^4 - z^2 + 1 \\ &= (z^2 + 3z + 1)^2 - 6z(z+1)^2\end{aligned}$$

Cyclotomic polynomials over Z_p

For any prime number p which does not divide n, the cyclotomic polynomial Φ_n is irreducible over $\mathbf{Z}_p$ if and only if p is a primitive root modulo n. That is, the p does not divide n, and its multiplicative order modulo n is $\varphi(n)$ (which is also the degree of Φ_n).

Polynomial values

If x takes any real value, then $\Phi_n(x) > 0$ for every $n \geq 3$ (this follows from the fact that the roots of a cyclotomic polynomial are all non-real, for $n \geq 3$).

For studying the values that a cyclotomic polynomial may take when x is given an integer value, it suffices to consider only the case $n \geq 3$, as the cases $n = 1$ and $n = 2$ are trivial (one has $\Phi_1(x) = x - 1$ and $\Phi_2(x) = x + 1$).

For $n \geq 2$, one has

$$\Phi_n(0) = 1,$$
$$\Phi_n(1) = 1 \text{ if } n \text{ is not a prime power},$$
$$\Phi_n(1) = p \text{ if } n = p^k \text{ is a prime power with } k \geq 1.$$

The values that a cyclotomic polynomial $\Phi_n(x)$ may take for other integer values of x is strongly related with the multiplicative order modulo a prime number

More precisely, given a prime number p and an integer b coprime with p, the multiplicative order of b modulo p, is the smallest positive integer n such that p is a divisor of $x^n - 1$. For $b > 1$, the multiplicative order of b modulo p is also the shortest period of the representation of $1/p$ in the numeral base b (see Unique prime; this explains the notation choice).

The definition of the multiplicative order implies that, if n is the multiplicative order of b modulo p, then p is a divisor of $\Phi_n(b)$. The converse is not true, but one has the following.

If $n > 0$ is a positive integer and $b > 1$ is an integer, then (see below for a proof)

$$\Phi_n(b) = 2^k gh,$$

where

- k is a non-negative integer, always equal to 0 when b is even. (In fact, if n is neither 1 nor 2, then k is either 0 or 1. Besides, if n is not a power of 2, then k is always equal to 0)
- g is 1 or the largest odd prime factor of n.
- h is odd, coprime with n, and its prime factors are exactly the odd primes p such that n is the multiplicative order of b modulo p.

This implies that, if p is an odd prime divisor of $\Phi_n(b)$, then either n is a divisor of $p - 1$ or p is a divisor of n. In the latter case p^2 does not divides $\Phi_n(b)$.

Zsigmondy's theorem implies that the only cases where $b > 1$ and $h = 1$ are

$$\begin{aligned}\Phi_1(2) &= 1 \\ \Phi_2\left(2^k - 1\right) &= 2^k \qquad k > 0 \\ \Phi_6(2) &= 3\end{aligned}$$

It follows from above factorization that the odd prime factors of

$$\frac{\Phi_n(b)}{\gcd(n, \Phi_n(b))}$$

are exactly the odd primes p such that n is the multiplicative order of b modulo p. This fraction may be even only when b is odd. In this case, the multiplicative order of b modulo 2 is always 1.

There are many pairs (n, b) with $b > 1$ such that $\Phi_n(b)$ is prime. In fact, Bunyakovsky conjecture implies that, for every n, there are infinitely many $b > 1$ such that $\Phi_n(b)$ is prime. See A085398 for the list of the smallest $b > 1$ such that $\Phi_n(b)$ is prime. See also A206864 for the list of the smallest primes of the form $\Phi_n(b)$ with $n > 2$ and $b > 1$, and, more generally, A206942, for the smallest positive integers of this form.

Proofs [show]

- *Values of* $\Phi_n(1)$. If $n = p^{k+1}$ is a prime power, then

$$\Phi_n(x) = 1 + x^{p^k} + x^{p^{2k}} + \cdots + x^{(p-1)p^k} \qquad \text{and} \qquad \Phi_n(1) = p.$$

  If n is not a prime power, let $P(x) = 1 + x + \cdots + x^{n-1}$, we have $P(1) = n$, and P is the product of the $\Phi_k(x)$ for k dividing n and different of 1. If p is a prime divisor of multiplicity m in n, then $\Phi_p(x), \Phi_{p^2}(x), \cdots, \Phi_{p^m}(x)$ divide $P(x)$, and their values at 1 are m factors equal to p of $n = P(1)$. As m is the multiplicity of p in n, p cannot divide the value at 1 of the other factors of $P(x)$. Thus there is no prime that divides $\Phi_n(1)$.

- *If n is the multiplicative order of b modulo p, then* $p \mid \Phi_n(b)$. By definition, $p \mid b^n - 1$. If $p \nmid \Phi_n(b)$, then p would divide another factor $\Phi_k(b)$ of $b^n - 1$, and would thus divide $b^k - 1$, showing that, if there would be the case, n would not be the multiplicative order of b modulo p.

- *The other prime divisors of* $\Phi_n(b)$ *are divisors of n*. Let p be a prime divisor of $\Phi_n(b)$ such that n is not be the multiplicative order of b modulo p. If k is the multiplicative order of b modulo p, then p divides both $\Phi_n(b)$ and $\Phi_k(b)$. The resultant of $\Phi_n(x)$ and $\Phi_k(x)$ may be written $P\Phi_k + Q\Phi_n$, where P and Q are polynomials. Thus p divides this resultant. As k divides n, and the resultant of two polynomials divides the discriminant of any common multiple of these polynomials, p divides also the discriminant n^n of $x^n - 1$. Thus p divides n.

- *g and h are coprime*. In other words, if p is a prime common divisor of n and $\Phi_n(b)$, then n is not the multiplicative order of b modulo p. By Fermat's little theorem, the multiplicative order of b is a divisor of $p - 1$, and thus smaller than n.

- *g is square-free*. In other words, if p is a prime common divisor of n and $\Phi_n(b)$, then p^2 does not divide $\Phi_n(b)$. Let $n = pm$. It suffices to prove that p^2 does not divides $S(b)$ for some polynomial $S(x)$, which is a multiple of $\Phi_n(x)$. We take

$$S(x) = \frac{x^n - 1}{x^m - 1} = 1 + x^m + x^{2m} + \cdots + x^{(p-1)m}.$$

  The multiplicative order of b modulo p divides $\gcd(n, p - 1)$, which is a divisor of $m = n/p$. Thus $c = b^m - 1$ is a multiple of p. Now,

$$S(b) = \frac{(1+c)^p - 1}{c} = p + \binom{p}{2}c + \cdots + \binom{p}{p}c^{p-1}.$$

  As p is prime and greater than 2, all the terms but the first one are multiples of p^2. This proves that $p^2 \nmid \Phi_n(b)$.

Applications

Using Φ_n, one can give an elementary proof for the infinitude of primes congruent to 1 modulo n,[11] which is a special case of Dirichlet's theorem on arithmetic progressions.

Suppose $p_1, p_2, \ldots, p_k$ are a finite list of primes congruent to 1 modulo n. Let $N = np_1p_2\cdots p_k$ and consider $\Phi_n(N)$. Let q be a prime factor of $\Phi_n(N)$ (to see that $\Phi_n(N) \neq \pm 1$ decompose it into linear factors and note that 1 is the closest root of unity to N). Since $\Phi_n(x) \equiv \pm 1 \bmod x$, we know that q is a new prime not in the list. We will show that $q \equiv 1 \bmod n$.

Let m be the order of N modulo q. Since $\Phi_n(N) \mid N^n - 1$ we have $N^n - 1 \equiv 0 \bmod q$. Thus $m \mid n$. We will show that $m = n$.

Assume for contradiction that $m < n$. Since

$$N^m - 1 \equiv \prod_{d \mid m} \Phi_d(N) \equiv 0 \bmod q$$

we have

$$\Phi_d(N) \equiv 0 \bmod q,$$

for some $d < n$. Then N is a double root of

$$\prod_{d|n} \Phi_d(x) \equiv x^n - 1 \bmod q.$$

Thus N must be a root of the derivative so

$$\left.\frac{d(x^n-1)}{dx}\right|_N \equiv nN^{n-1} \equiv 0 \bmod q.$$

But $q \nmid N$ and therefore $q \nmid n$. This is a contradiction so $m = n$. The order of $N \bmod q$, which is n, must divide $q-1$. Thus $q \equiv 1 \bmod n$.

See also

- Cyclotomic field
- Aurifeuillean factorization
- Root of unity

Notes

1. Sloane, N.J.A. (ed.). "Sequence A013595" (https://oeis.org/A013595) *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation.
2. Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics, **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR 1878556 (https://www.ams.org/mathscinet-getitem?mr=1878556)
3. Schramm, Wolfgang (2015). "Eine alternative Produktdarstellung für die Kreisteilungspolynome" (https://web.archive.org/web/20151222122149/https://www.ems-ph.org/journals/show_abstract.php?issn=0013-6018&vol=70&iss=4&rank=1) *Elemente der Mathematik*. Swiss Mathematical Society. **70** (4): 137–143. Archived from the original (https://www.ems-ph.org/journals/show_abstract.php?issn=0013-6018&vol=70&iss=4&rank=1) on 2015-12-22. Retrieved 2015-10-10.
4. Cox, David A. (2012), "Exercise 12", *Galois Theory* (2nd ed.), John Wiley & Sons, p. 237, doi:10.1002/9781118218457 (https://doi.org/10.1002/9781118218457), ISBN 978-1-118-07205-9
5. Weisstein, Eric W. "Cyclotomic Polynomial" (http://mathworld.wolfram.com/CyclotomicPolynomial.html). Retrieved 12 March 2014.
6. Isaacs, Martin (2009). *Algebra: A Graduate Course*. AMS Bookstore. p. 310. ISBN 978-0-8218-4799-2
7. Meier (2008)
8. Gauss, DA, Articles 356-357
9. Riesel, pp. 315-316, p. 436
10. Riesel, pp. 309-315, p. 443
11. S. Shirali. *Number Theory.* Orient Blackswan, 2004. p. 67. ISBN 81-7371-454-1

References

Gauss's book *Disquisitiones Arithmeticae* has been translated from Latin into English and German. The German edition includes all of his papers on number theory: all the proofs of quadratic reciprocity, the determination of the sign of the Gauss sum, the investigations into biquadratic reciprocity, and unpublished notes.

- Gauss, Carl Friedrich (1986) [1801]. *Disquisitiones Arithmeticae*. Translated into English by Clarke, Arthur A. (2nd corr. ed.). New York: Springer. ISBN 0387962549.
- Gauss, Carl Friedrich (1965) [1801]. *Untersuchungen uber hohere Arithmetik (Disquisitiones Arithmeticae & other papers on number theory)*. Translated into German by Maser, H. (2nd ed.). New York: Chelsea. ISBN 0-8284-0191-8.
- Lemmermeyer, Franz (2000). *Reciprocity Laws: from Euler to Eisenstein*. Berlin: Springer. doi:10.1007/978-3-662-12893-0. ISBN 978-3-642-08628-1.
- Maier, Helmut (2008), "Anatomy of integers and cyclotomic polynomials", in De Koninck, Jean-Marie; Granville, Andrew; Luca, Florian, *Anatomy of integers. Based on the CRM workshop, Montreal, Canada, March 13-17, 2006*, CRM Proceedings and Lecture Notes, **46**, Providence, RI: American Mathematical Society, pp. 89–95, ISBN 978-0-8218-4406-9, Zbl 1186.11010
- Riesel, Hans (1994). *Prime Numbers and Computer Methods for Factorization* (2nd ed.). Boston: Birkhäuser. ISBN 0-8176-3743-5.

External links

- Weisstein, Eric W. "Cyclotomic polynomial". *MathWorld*.
- Hazewinkel, Michiel, ed. (2001) [1994], "Cyclotomic polynomials", *Encyclopedia of Mathematics*, Springer Science+Business Media B.V. / Kluwer Academic Publishers, ISBN 978-1-55608-010-4
- OEIS sequence A013595 (Triangle of coefficients of cyclotomic polynomial Phi_n(x) (exponents in increasing order))
- OEIS sequence A013594 (Smallest order of cyclotomic polynomial containing n or −n as a coefficient)