Cyclotomic polynomial

From Wikipedia, the free encyclopedia

In algebra, the ***n*th cyclotomic polynomial**, for any positive integer n, is the unique irreducible polynomial with integer coefficients, which is a divisor of $x^n - 1$ and is not a divisor of $x^k - 1$ for any $k < n$. Its roots are the nth primitive roots of unity $e^{2i\pi\frac{k}{n}}$, where k runs over the integers lower 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, which is the minimal polynomial over the field of the rational numbers of any primitive nth-root of unity ($e^{2i\pi/n}$ is such a primitive root).

Contents

Examples

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=2p where p is an odd prime number then

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

For *n* up to 10 we have:

$$\Phi_0(x) = 1$$
$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$
$$\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$$
$$\Phi_6(x) = x^2 - x + 1$$
$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$
$$\Phi_8(x) = x^4 + 1$$
$$\Phi_9(x) = x^6 + x^3 + 1$$
$$\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$$

For *n* up to 30, the cyclotomic polynomials not covered by above formulas are:

$$\Phi_{12}(x) = x^4 - x^2 + 1$$
$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$
$$\Phi_{16}(x) = x^8 + 1$$
$$\Phi_{18}(x) = x^6 - x^3 + 1$$
$$\Phi_{20}(x) = x^8 - x^6 + x^4 - x^2 + 1$$
$$\Phi_{21}(x) = x^{12} - x^{11} + x^9 - x^8 + x^6 - x^4 + x^3 - x + 1$$
$$\Phi_{24}(x) = x^8 - x^4 + 1$$
$$\Phi_{25}(x) = x^{20} + x^{15} + x^{10} + x^5 + 1$$
$$\Phi_{27}(x) = x^{18} + x^9 + 1$$
$$\Phi_{28}(x) = x^{16} - x^{14} + x^{12} - x^{10} + x^8 - x^6 + x^4 - x^2 + 1$$
$$\Phi_{30}(x) = x^8 + x^7 - x^5 - x^4 - x^3 + x + 1$$

The case of 105 is interesting because it is the first integer that is the product of three distinct odd prime numbers and the 105th cyclotomic polynomial is the first one that has a coefficient of magnitude greater than 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 palindromic polynomials of even degree.

The degree of Φ_n, or in other words the number of *n*th 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.[1] 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

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

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:

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

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 to compute $\Phi_n(x)$ 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 in Maple, $\Phi_n(x)$ may be computed by typing "numtheory[cyclotomic](n,x);".

Easy cases for the 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

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

If *n* is an even integer, then

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

In particular, if *n*=2*p* 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 $n=q^m r$ with $m>1$ then

$$\Phi_n(x) = \Phi_{qr}(x^{q^{m-1}}).$$

This formula may be iterated to get a simple expression of 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

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

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 relatively prime to n,[2]

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

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 $\{1, -1, 0\}$.[3]

The first cyclotomic polynomial for a product of 3 different odd prime factors is $\Phi_{105}(x)$; it has a coefficient −2 (see its expression above). The converse isn't true: $\Phi_{231}(x) = \Phi_{3\times 7\times 11}(x)$ only has coefficients in $\{1, -1, 0\}$.

If n is a product of more odd different 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.[4]

Gauss's formula

Let n be odd, square-free, and greater than 3. Then[5][6]

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

where both $A_n(z)$ and $B_n(z)$ have integer coefficients, $A_n(z)$ has degree $\phi(n)/2$, and $B_n(z)$ has degree $\phi(n)/2 - 2$. 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 $\equiv 3 \pmod 4$, 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[7]

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

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

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

If n is even, square-free and greater than 2 (this forces n to be $\equiv 2 \pmod 4$),

$$\Phi_{n/2}(-z^2) = C_n^2(z) - n z D_n^2(z)$$

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

The first few cases are:

$$\begin{aligned}\Phi_3(-z) &= z^2 - z + 1 \\ &= (z+1)^2 - 3z \\ \Phi_5(z) &= z^4 + z^3 + z^2 + z + 1 \\ &= (z^2 + 3z + 1)^2 - 5z(z+1)^2 \\ \Phi_3(-z^2) &= z^4 - z^2 + 1 \\ &= (z^2 + 3z + 1)^2 - 6z(z+1)^2\end{aligned}$$

Prime Cyclotomic numbers

If $\Phi_n(b)$ is a prime, then the prime is a base-b unique prime. For example, if n=39, b=10, than $\Phi_n(b)$ = 900900900900990990990991 is a prime, so it is a base-10 unique prime, and if n=30, b=2, than $\Phi_n(b)$ = 331 is also a prime, so it is a base-2 unique prime.

The list is about the smallest natural number b>1 that $\Phi_n(b)$ is a prime. (sequence A085398 in OEIS)

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
min b	3	2	2	2	2	2	2	2	2	2	5	2	2	2	2	2	2	6	2	4
n	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
min b	3	2	10	2	22	2	2	4	6	2	2	2	2	2	14	3	61	2	10	2
n	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
min b	14	2	15	25	11	2	5	5	2	6	30	11	24	7	7	2	5	7	19	3
n	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
min b	2	2	3	30	2	9	46	85	2	3	3	3	11	16	59	7	2	2	22	2
n	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
min b	21	61	41	7	2	2	8	5	2	2	11	4	2	6	44	4	12	2	63	20
n	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120
min b	22	13	3	4	7	10	2	3	12	5	12	40	86	14	268	5	24	6	148	2
n	121	122	123	124	125	126	127	128	129	130	131	132	133	134	135	136	137	138	139	140
min b	43	2	12	6	127	2	2	102	2	3	7	3	2	5	33	56	13	8	11	4
n	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159	160
min b	5	46	3	6	2	18	13	4	5	2	29	9	14	3	62	4	56	2	189	20

In fact, if p is a prime, than $\Phi_p(b)$ is (b^p-1)/(b-1) and a base-b repunit number, $(111111...111111)_b$, so it is a list of the smallest b>1 which $\Phi_p(b)$ is a prime.

(sequence A066180 in OEIS)

The list is about the first 160 primes.

p	2	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53	59	61	67	71
min b	2	2	2	2	5	2	2	2	10	6	2	61	14	15	5	24	19	2	46	3
p	73	79	83	89	97	101	103	107	109	113	127	131	137	139	149	151	157	163	167	173
min b	11	22	41	2	12	22	3	2	12	86	2	7	13	11	5	29	56	30	44	60
p	179	181	191	193	197	199	211	223	227	229	233	239	241	251	257	263	269	271	277	281
min b	304	5	74	118	33	156	46	183	72	606	602	223	115	37	52	104	41	6	338	217
p	283	293	307	311	313	317	331	337	347	349	353	359	367	373	379	383	389	397	401	409
min b	13	136	220	162	35	10	218	19	26	39	12	22	67	120	195	48	54	463	38	41
p	419	421	431	433	439	443	449	457	461	463	467	479	487	491	499	503	509	521	523	541
min b	17	808	404	46	76	793	38	28	215	37	236	59	15	514	260	498	6	2	95	3
p	547	557	563	569	571	577	587	593	599	601	607	613	617	619	631	641	643	647	653	659
min b	473	417	123	30	89	88	236	76	124	2061	2	192	187	5	39	1267	190	321	24	79
p	661	673	677	683	691	701	709	719	727	733	739	743	751	757	761	769	773	787	797	809
min b	24	102	101	500	110	12	114	283	1004	566	75	398	40	62	70	61	1276	368	477	818
p	811	821	823	827	829	839	853	857	859	863	877	881	883	887	907	911	919	929	937	941
min b	342	217	168	119	202	55	430	22	438	1539	865	275	13	340	11	178	908	5	828	240

Applications

Using Φ_n, one can give an elementary proof for the infinitude of primes congruent to 1 modulo n,[8] which is a special case of Dirichlet's theorem on arithmetic progressions.

See also

- Cyclotomic field
- Aurifeuillean factorization

Notes

1. ^ Lang, Serge (2002), *Algebra*, Graduate Texts in Mathematics **211** (Revised third ed.), New York: Springer-Verlag, ISBN 978-0-387-95385-4, MR 1878556 (http://www.ams.org/mathscinet-getitem?mr=1878556)
2. ^ Weisstein, Eric W. "Cyclotomic Polynomial" (http://mathworld.wolfram.com/CyclotomicPolynomial.html). Retrieved 12 March 2014.
3. ^ Isaacs, Martin (2009). *Algebra: A Graduate Course*. AMS Bookstore. p. 310. ISBN 978-0-8218-4799-2.
4. ^ Meier (2008)
5. ^ Gauss, DA, Articles 356-357
6. ^ Riesel, pp. 315-316, p. 436
7. ^ Riesel, pp. 309-315, p. 443
8. ^ S. Shirali. *Number Theory*. Orient Blackswan, 2004. p. 67. ISBN 81-7371-454-1

References

The *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; Clarke, Arthur A. (translator into English) (1986), *Disquisitiones Arithemeticae (Second, corrected edition)*, New York: Springer, ISBN 0387962549
- Gauss, Carl Friedrich; Maser, H. (translator into German) (1965), *Untersuchungen uber hohere Arithmetik (Disquisitiones Arithemeticae & other papers on number theory) (Second edition)*, 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 (http://dx.doi.org/10.1007%2F978-3-662-12893-0), 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 (http://www.zentralblatt-math.org/zmath/en/search/?format=complete&q=an:1186.11010)
- Riesel, Hans (1994), *Prime Numbers and Computer Methods for Factorization (second edition)*, Boston: Birkhäuser, ISBN 0-8176-3743-5

External links

- Hazewinkel, Michiel, ed. (2001), "Cyclotomic polynomials" (http://www.encyclopediaofmath.org/index.php?title=p/c027580), *Encyclopedia of Mathematics*, Springer, ISBN 978-1-55608-010-4
- "Sloane's A013594 : Smallest order of cyclotomic polynomial containing n or −n as a coefficient (http://oeis.org/A013594)", *The On-Line Encyclopedia of Integer Sequences*. OEIS Foundation.