

6.1 Polynomials Whose Roots Are Roots of Unity

WORKSHEET

The question

For any given positive integer n , a number a (which may be complex) is said to be a *primitive n th root of unity* if $a^n = 1$ and there is no integer m such that $0 < m < n$ and $a^m = 1$. Write down the two primitive 4th roots of unity.

Let $C_n(x)$ be the polynomial such that the roots of the equation $C_n(x) = 0$ are the primitive n th roots of unity, the coefficient of the highest power of x is one and the equation has no repeated roots. Show that $C_4(x) = x^2 + 1$.

- (i) Find $C_1(x)$, $C_2(x)$, $C_3(x)$, $C_5(x)$ and $C_6(x)$, giving your answers as unfactorised polynomials.
- (ii) Find the value of n for which $C_n(x) = x^4 + 1$.
- (iii) Given that p is prime, find an expression for $C_p(x)$, giving your answer as an unfactorised polynomial.
- (iv) Prove that there are no positive integers q , r and s such that $C_q(x) \equiv C_r(x) C_s(x)$.

Hints

Try the question on your own first. If you get stuck, read the hints *one at a time*, and go back to the question after each one. Hints marked *Pause and try* are the key steps.

- ?** **Ask yourself** Every n th root of unity satisfies $z^n = 1$. But the smallest positive power that gives 1 might be less than n . For each of the four 4th roots of unity, 1, i , -1 , $-i$, what is that smallest power?

STAGE 1 The first few

- ?** **Ask yourself** Which roots of unity have order 1, 2, 3, 5 and 6? (Draw the 6th roots of unity and sort them by order.)

STAGE 4 No cyclotomic polynomial is a product of two others

- 🔧** **Pause and try** Suppose $C_q = C_r C_s$. Take a root of C_r . What is its order? What does the identity say about its order? What does that force?

Try this next

- 1 Check the factorisation.** Verify that $(x-1)(x+1)(x^2+x+1)(x^2-x+1) = x^6-1$, and that $x^{12}-1$ factorises as in Figure 6.1.1 (in the full section online).
- 2 Twice a prime.** Show that if p is an odd prime then $C_{2p}(x) = C_p(-x)$. Check this for $p=3$.
- 3 Totients.** Show that $\varphi(p^k) = p^k - p^{k-1}$ for a prime p , and that $C_{p^k}(x) = C_p(x^{p^{k-1}})$. Use this to find C_9 .
- 4 A longer one.** **HARDER** Using $x^{15}-1 = C_1 C_3 C_5 C_{15}$, show that $C_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$.

Further reading

- **Ian Stewart, *Galois Theory*** (CRC Press). The standard undergraduate introduction; cyclotomic polynomials and the regular polygon appear early.
- **Harold Davenport, *The Higher Arithmetic*** (Cambridge University Press). Includes roots of unity and their arithmetic.
- **Marcus du Sautoy, *Finding Moonshine*** (Fourth Estate). A popular account of symmetry and group theory, including the story of Galois.

The full guided solution, and what the question leads to at university, is in Section 6.1:
https://keithmcnulty.github.io/step_book_mcnulty/ch06/cyclotomic.html