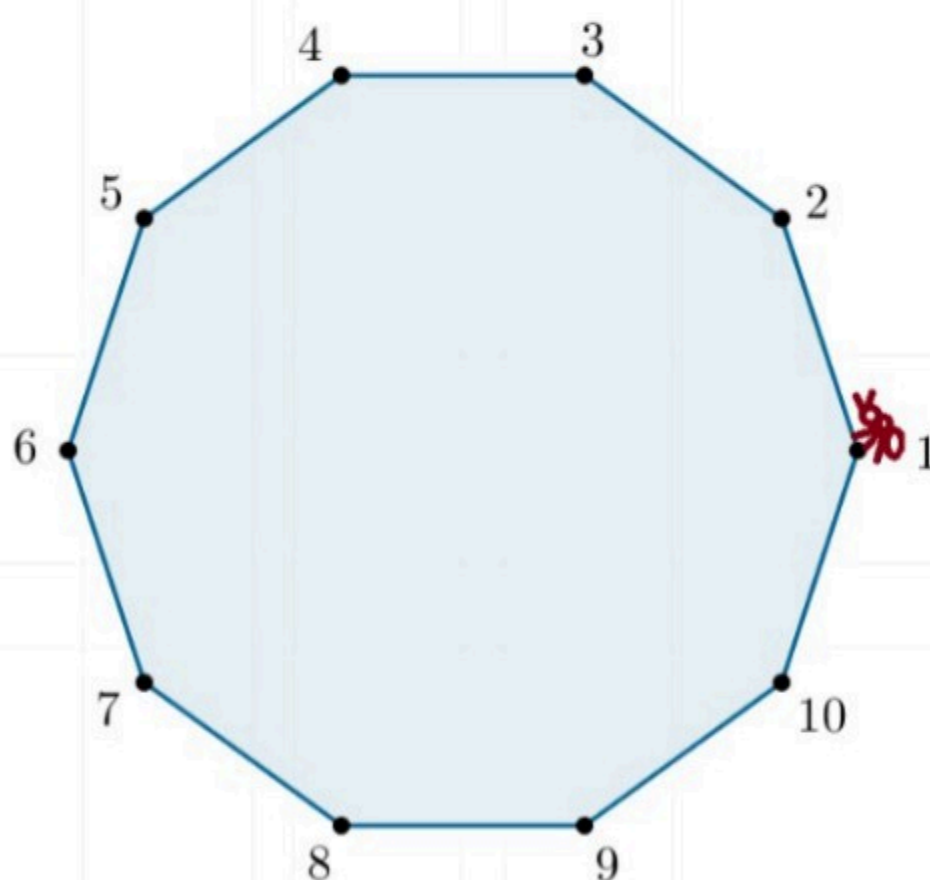




INFORMAL NOTES ON
MATHEMATICS
2022.07.23

今天学点 roots of unity. 理论上这是 7.23 的笔记但实际上开始写的时候已经 7.27 了。

Brilli the ant stands on vertex 1 of the **regular decagon** below.



- He starts by hopping 1 space at a time (from 1 to 2, then from 2 to 3, and so on). He performs 10 hops in this way.
- He then hops 2 spaces at a time (from 1 to 3, then from 3 to 5, and so on). He performs 10 hops in this way.
- He continues to increase the hop distance every 10 hops: hopping 3 spaces 10 times, then hopping 4 spaces 10 times, and so on.
- After Brilli has hopped 10 spaces 10 times, he ends his workout.

When Brilli has completed his workout, which vertex will he be standing on?

Answer: 1 obviously.

DEFINITION

For any positive integer n , the n^{th} roots of unity are the complex solutions to the equation $x^n = 1$, and there are n solutions to the equation.

(这是不是群论里的 order. 很好奇有多少结论能推广到群论)

THEOREM

If n is even, there will be 2 real solutions to the equation $x^n = 1$, which are 1 and -1 ; if n is odd, there will be 1 real solution, which is 1.

TRY IT YOURSELF

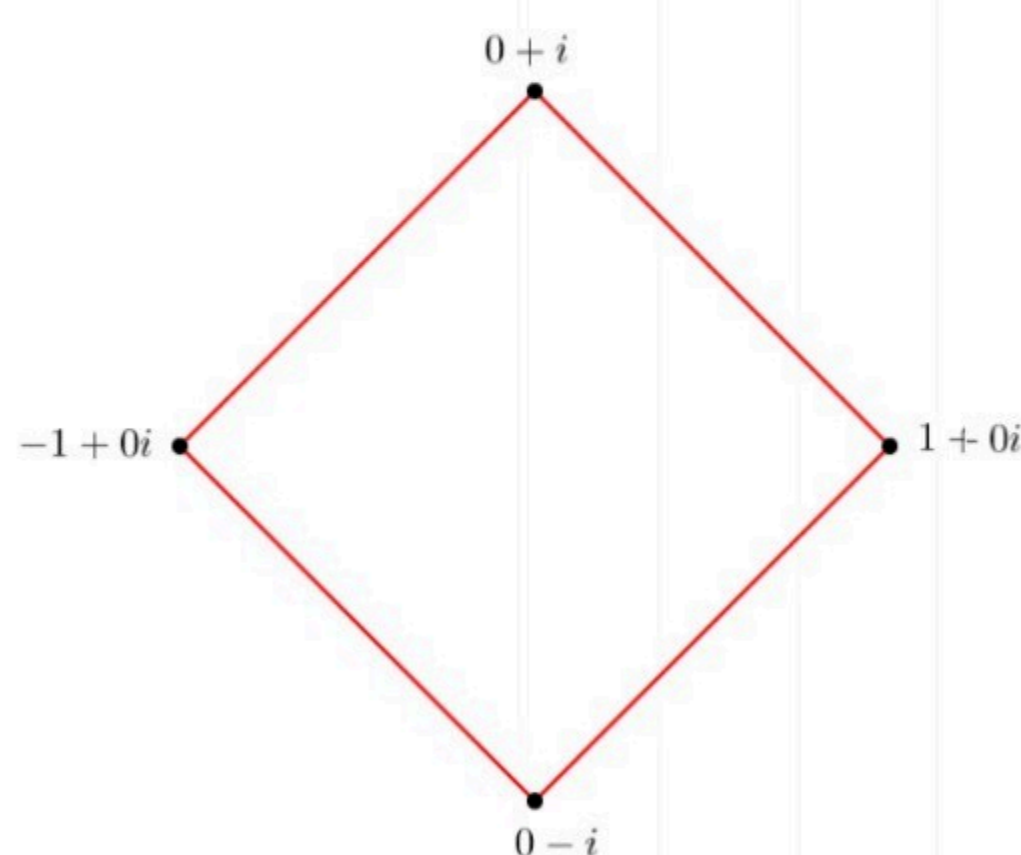
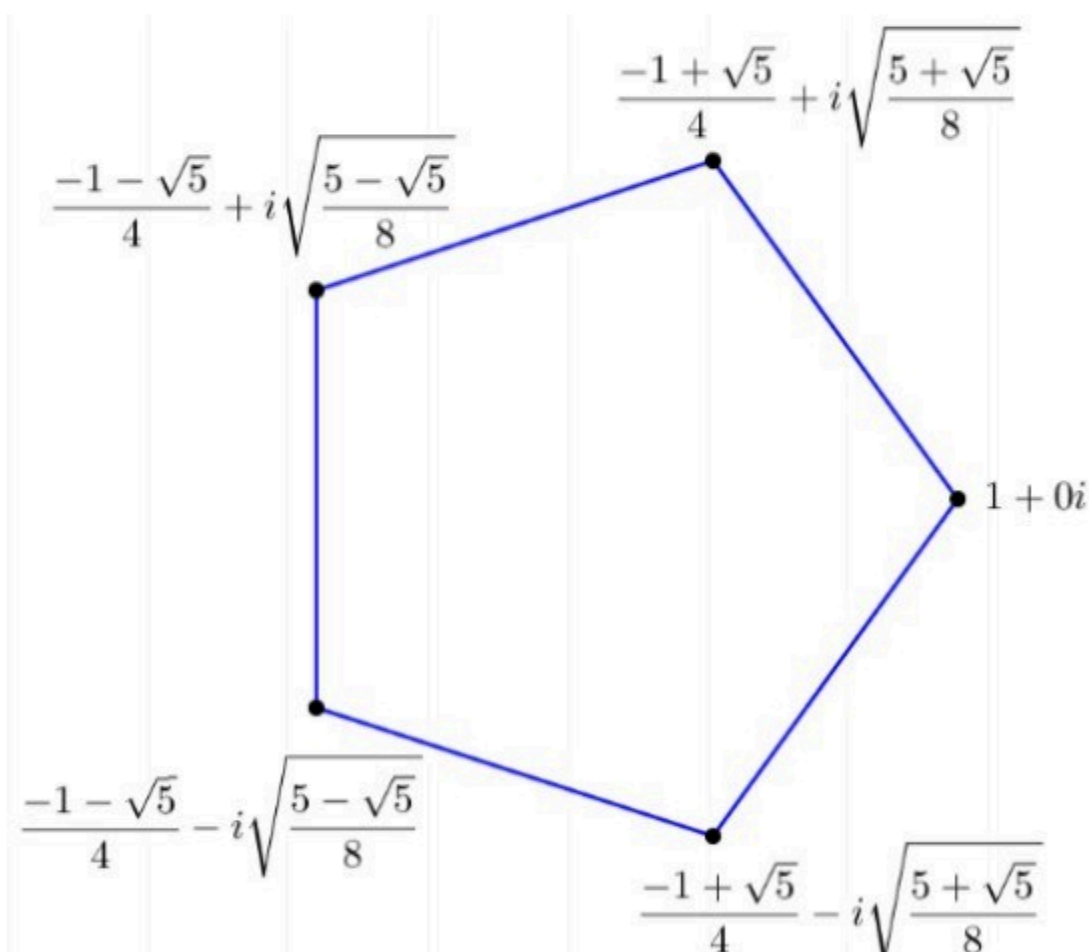
$$\left(\frac{-1 + i\sqrt{3}}{2} \right)^3 = ?$$

解 $\cos(\frac{2\pi}{3}) = -\frac{1}{2}$, $\sin(\frac{2\pi}{3}) = \frac{\sqrt{3}}{2}$ \therefore 原式 $= (\cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}))^3 = e^{3i\pi} = 1$

THEOREM

Let n be a positive integer and U_n be the set of all n^{th} roots of unity. Then

$$U_n = \left\{ e^{2k\pi i/n} \mid k \in \{1, 2, \dots, n\} \right\}.$$

The 4th roots of unityThe 5th roots of unity

How to prove that $x^{2n} + x^n + 1$ has a factor $x^2 + x + 1$ if and only if $n \not\equiv 0 \pmod{3}$?

Asked 2 days ago Modified today Viewed 92 times

2 Well, I don't know whether it is exactly correct. I get this result when I was dealing with a simple problem "find out the factors of $x^{10} + x^5 + 1$ ". I put different n into this polynomial and draw the roots in the complex plane by WolframAlpha: [n=4,7,9](#)

2 The distribution of these roots has certain rules: the red angle is half of the blue one, and one red angle comes after one blue angle and make up the whole circle in this way. By observing the pictures, we can easily get the result that is stated in the question.

2 The following question has been moved to another post: [How to prove that \$\sum_{i=0}^k x^{in}\$ have a same factor \$P\(x\)\$ if and only if \$n \not\equiv 0 \pmod{k+1}\$?](#)

[Also, for $x^{3n} + x^{2n} + x^n + 1$, I infer it has a factor $x^2 + 1$ if and only if $n \not\equiv 0 \pmod{4}$. Also see the pictures: [n=2,3,4,5](#)

My guess is: For polynomials $x^{kn} + x^{(k-1)n} + \dots + x^{2n} + x^n + 1, k \geq 2$, if $n \not\equiv 0 \pmod{k+1}$, they all have a certain factor $P(x)$.


Is that true? How do I find the factor $P(x)$? How to prove? (I think the method of Cotes' Theorem may be used for it. See T. Needham, *Visual Complex Analysis*, pp 46-47)]

[complex-analysis](#) [polynomials](#) [complex-numbers](#) [factoring](#)

Share Cite Follow

edited 2 days ago

asked 2 days ago

 **Дъартский**
35 4

 New contributor

Welcome to MSE. A question should be written in such a way that it can be understood even by someone who did not read its title. – [José Carlos Santos](#) 2 days ago

What is your question: That in the title or in your guess? – [Paul Frost](#) 2 days ago

Please do not ask multiple questions in one post. Here you are asking two questions:(1) about

$x^{2n} + x^n + 1$ and (2) about $\sum_{i=0}^k x^{in}$. Please make a separate question for one of these and keep the other question in this post. – [insipidintegrator](#) 2 days ago

@insipidintegrator ok i'll do it – [Дъартский](#) 2 days ago

- 1 Notice that $x^2 + x + 1 = \frac{x^3-1}{x-1}$, so working mod $x^2 + x + 1$ you can reduce all the exponents mod 3. – Qiaochu Yuan 2 days ago

Because of $\frac{-1 \pm \sqrt{-3}}{2}$ are roots of $x^2 + x + 1$ it is equivalent to prove that

$$\left(\frac{-1 \pm \sqrt{-3}}{2}\right)^{2n} + \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^n + 1 = 0$$

for the proposed values of n . In other words that

$$\left(\frac{-1 \pm \sqrt{-3}}{2}\right)^n = \left(\frac{-1 \pm \sqrt{-3}}{2}\right)^n$$

We are done. – Piquito 2 days ago

Have you learnt about cube roots of unity yet? – user1078285 2 days ago

2 Answers

Sorted by:

Highest score (default) ◆



Since $(x^2 + x + 1)(x - 1) = x^3 - 1$ the roots of $(x^2 + x + 1)$ are $\{\zeta, \zeta^2\}$ where ζ is a primitive cubic root of 1.

3



When $n \not\equiv 0 \pmod 3$ there is an equality of sets $\{\zeta^n, \zeta^{2n}\} = \{\zeta, \zeta^2\}$ which shows that ζ and ζ^2 are also roots of $x^{2n} + x^n + 1$, thus the divisibility of polynomials.



On the other hand when $n \equiv 0 \pmod 3$ we have $\zeta^n = \zeta^{2n} = 1$ so $\{\zeta, \zeta^2\}$ are not roots of $x^{2n} + x^n + 1$.



Share Cite Follow

answered 2 days ago



Andrea Mori

24.9k 1 41 76

This proof is nice, it seems that it isn't too much more to prove a more general statement this way for all cyclotomic polynomials that $\Phi_k(x^n)$ is divisible by $\Phi_k(x)$ iff $\gcd(k, n) = 1$, since otherwise we don't have a bijection of the set of roots. – Merosity 8 hours ago



We can also see this in terms of the factorizations themselves. The "template" would be

$$u^2 + u + 1 = \frac{u^3 - 1}{u - 1}, \quad u \neq 1.$$

As "base" examples, we have

1



$$\begin{aligned}
\mathbf{n} = \mathbf{2} : \quad & x^4 + x^2 + 1 \\
= & \frac{(x^2)^3 - 1}{x^2 - 1} = \frac{(x^3)^2 - 1}{x^2 - 1} \\
= & \frac{(x^3 - 1) \cdot (x^3 + 1)}{(x - 1) \cdot (x + 1)} \\
= & (x^2 + x + 1) \\
\cdot & (x^2 - x + 1), \quad x^2 \neq 1;
\end{aligned}$$

$$\begin{aligned}
\mathbf{n} = \mathbf{4} : \quad & x^8 + x^4 + 1 \\
= & \frac{(x^4)^3 - 1}{x^4 - 1} = \frac{(x^3)^4 - 1}{x^4 - 1} \\
= & \frac{([x^3]^2 - 1) \cdot ([x^3]^2 + 1)}{(x^2 - 1) \cdot (x^2 + 1)} \\
= & \frac{([x^3]^2 - 1) \cdot ([x^2]^3 + 1)}{(x - 1) \cdot (x + 1) \cdot (x^2 + 1)} \\
= & \frac{(x^3 - 1) \cdot (x^3 + 1) \cdot ([x^2]^3 + 1)}{(x - 1) \cdot (x + 1) \cdot (x^2 + 1)} \\
= & (x^2 + x + 1) \\
\cdot & (x^2 - x + 1) \\
\cdot & (x^4 - x^2 + 1), \quad x^4 \neq 1;
\end{aligned}$$

for these polynomials, we are able to write the numerator in each quotient as a "difference of two squares", *however*,

$$\begin{aligned}
\mathbf{n} = \mathbf{3} : \quad & x^6 + x^3 + 1 \\
= & \frac{(x^3)^3 - 1}{x^3 - 1}, \quad x^3 \neq 1, \\
= & \frac{(x^3 - 1) \cdot (x^6 + x^3 + 1)}{(x^3 - 1)}
\end{aligned}$$

since we are unable to use a "difference of two squares"; it is easily checked that this polynomial is irreducible over \mathbb{R} .

For the general cases, we actually need to consider the parity of n .

$$\begin{aligned}
\mathbf{n} = \mathbf{3m} \pm \mathbf{1} = \mathbf{2p}, \mathbf{2p'} : \\
& x^{4p} + x^{2p} + 1 \\
= & \frac{(x^{2p})^3 - 1}{x^{2p} - 1} = \frac{(x^{3p})^2 - 1}{x^{2p} - 1}
\end{aligned}$$

$$\begin{aligned}
&= \frac{(x^{3p} - 1) \cdot (x^{3p} + 1)}{(x^p - 1) \cdot (x^p + 1)} \\
&= \frac{((x^3)^p - 1) \cdot (x^{3p} + 1)}{(x^p - 1) \cdot (x^p + 1)} \\
&= \left(\frac{x^3 - 1}{x - 1} \right) \\
&\quad \cdot \frac{([x^3]^{p-1} + [x^3]^{p-2} + \dots + x^3 + 1) \cdot (x^{3p} + 1)}{(x^{p-1} + x^{p-2} + \dots + x + 1) \cdot (x^p + 1)} \\
&= (x^2 + x + 1) \\
&\quad \cdot \frac{([x^3]^{p-1} + [x^3]^{p-2} + \dots + x^3 + 1) \cdot (x^{3p} + 1)}{(x^{p-1} + x^{p-2} + \dots + x + 1) \cdot (x^p + 1)} , \\
&x^{2p} \neq 1 ,
\end{aligned}$$

and similarly for $2p'$,

$$\begin{aligned}
&\mathbf{n} = \mathbf{3m} \text{ [odd]} : \\
&x^{6m} + x^{3m} + 1 \\
&= \frac{(x^{3m})^3 - 1}{x^{3m} - 1} \\
&= \frac{(x^{3m} - 1) \cdot ([x^{3m}]^2 + x^{3m} + 1)}{x^{3m} - 1} \\
&= (x^{3m})^2 + x^{3m} \\
&+ 1 = x^{6m} + x^{3m} + 1 , \\
&x^{3m} \neq 1 ,
\end{aligned}$$

which simply returns our polynomial, which is biquadratic in $3m$ and irreducible over \mathbb{R} ;

$\mathbf{n} = \mathbf{3m} \pm \mathbf{1}$ [odd] :

$$\begin{aligned}
&x^{2n} + x^n + 1 \\
&= \frac{x^{3n} - 1}{x^n - 1} = \frac{(x^3)^n - 1}{x^n - 1} \\
&= \left(\frac{x^3 - 1}{x - 1} \right)
\end{aligned}$$

$$\begin{aligned}
& \cdot \frac{(x^3)^{n-1} + (x^3)^{n-2} + \dots + x^3 + 1}{x^{n-1} + x^{n-2} + \dots + x + 1} \\
& = (x^2 + x + 1) \\
& \cdot \frac{(x^3)^{n-1} + (x^3)^{n-2} + \dots + x^3 + 1}{x^{n-1} + x^{n-2} + \dots + x + 1} , \\
& x^n \neq 1 ,
\end{aligned}$$

n = 3m = 6q :

$$\begin{aligned}
& x^{12q} + x^{6q} + 1 \\
& = \frac{(x^{6q})^3 - 1}{x^{6q} - 1} \\
& = \frac{(x^{6q} - 1) \cdot ([x^{6q}]^2 + x^{6q} + 1)}{x^{6q} - 1} \\
& = x^{12q} + x^{6q} \\
& + 1 = (x^{6q} + x^{3q} + 1) \\
& \cdot (x^{6q} - x^{3q} + 1) , \quad x^{6q} \\
& \neq 1 ,
\end{aligned}$$

which returns irreducible biquadratic factors, none of which are $x^2 + x + 1$. A couple of examples of this latter case are

$$\begin{aligned}
\mathbf{n} = \mathbf{5} : & \quad x^{10} + x^5 + 1 \\
& = \frac{(x^5)^3 - 1}{x^5 - 1} = \left(\frac{x^3 - 1}{x - 1} \right) \\
& \cdot \frac{(x^3)^{5-1} + (x^3)^{5-2} + \dots + x^3 + 1}{x^{5-1} + x^{5-2} + \dots + x + 1} \\
& = (x^2 + x + 1) \\
& \cdot \frac{x^{12} + x^9 + x^6 + x^3 + 1}{x^4 + x^3 + x^2 + x + 1} , \\
& x^5 \neq 1 ,
\end{aligned}$$

$$\begin{aligned}
\mathbf{n} = \mathbf{6} : & \quad x^{12} + x^6 + 1 \\
& = (x^6 + x^3 + 1) \\
& \cdot (x^6 - x^3 + 1) , \quad x^6 \neq 1 .
\end{aligned}$$

Viewed in this way, the zeroes of $u^2 + u + 1$ are the three unit-modulus zeroes of $z^3 - 1$, $z_k = e^{i \cdot 2k\pi/3}$, $k = 0, 1, 2$, with $z_0 = 1$ "removed". Finding the zeroes of $w^{2n} + w^n + 1$ substitutes $u = w^n$, generating three "families" of n -th-roots,

$$\begin{aligned}
& \bullet \quad w^n = z_0 \quad \text{which are **excluded** by the condition } z^n \neq 1 ; \\
& \Rightarrow w_{0,j} = e^{i \cdot [0 + 2j\pi]/n} , \\
& \quad = e^{i \cdot 6j\pi/(3n)}
\end{aligned}$$

$$0 \leq j \leq n-1 ,$$

- $w^n = z_1$
 $\Rightarrow w_{1,j} = e^{i \cdot [(2\pi/3) + 2j]\pi/n}$
 $= e^{i \cdot (2+6j)\pi/(3n)} ,$
 $0 \leq j \leq n-1 ;$
- $w^n = z_2$
 $\Rightarrow w_{2,j} = e^{i \cdot [(4\pi/3) + 2j]\pi/n}$
 $= e^{i \cdot (4+6j)\pi/(3n)} ,$
 $0 \leq j \leq n-1 .$

This produces the $2n$ complex zeroes expected for the polynomial.

For $n = 3m \pm 1$, it is possible to find integer solutions for j in either
 $\frac{(2+6j) \cdot \pi}{3n} = \frac{2\pi}{3} , \frac{4\pi}{3} \Rightarrow j$ or $\frac{(4+6j) \cdot j}{3n} = \frac{2\pi}{3} , \frac{4\pi}{3} \Rightarrow j$, So the
 $= \frac{n-1}{3} , \frac{2n-1}{3} = \frac{n-2}{3} , \frac{2n-2}{3}$
 $0 \leq j \leq n-1 .$

zeroes of $z^2 + z + 1$ are found among those of $w^{2n} + w^n + 1$. But for
 $n = 3m$, the zeroes become $e^{i \cdot (2+6j)\pi/(9m)}$, and

$e^{i \cdot (4+6j)\pi/(9m)}$
 $j = \frac{18m-2}{6} , \frac{36m-2}{6}$, are no longer integers. Hence, the zeroes of $z^2 + z + 1$
 $\frac{18m-4}{6} , \frac{36m-4}{6}$
are *not* zeroes of $w^{6m} + w^{3m} + 1$.

Share Cite Follow

answered 9 hours ago



boojum

2,423

2

5

19

How to prove that $\sum_{i=0}^k x^{in}$ have a same factor $P(x)$ if and only if $n \not\equiv 0 \pmod{k+1}$?

Asked today Modified today Viewed 25 times



1



Please see the pre-content here: [How to prove that \$x^{2n} + x^n + 1\$ has a factor \$x^2 + x + 1\$ if and only if \$n \not\equiv 0 \pmod{3}\$?](#)

Well, I don't know whether it is exactly correct. I get this result ($x^{2n} + x^n + 1$ has a factor $x^2 + x + 1$ if and only if $n \not\equiv 0 \pmod{3}$) when I was dealing with a simple problem "find out the factors of $x^{10} + x^5 + 1$ ". I put different n into this polynomial and draw the roots in the complex plane by WolframAlpha: [n=4,7,9](#)

The distribution of these roots has certain rules: the red angle is half of the blue one, and one red angle comes after one blue angle and make up the whole circle in this way. By observing the pictures, we can easily get the result that is stated in the question.

Also, for $x^{3n} + x^{2n} + x^n + 1$, I infer it has a factor $x^2 + 1$ if and only if $n \not\equiv 0 \pmod{4}$. Also see the pictures: [n=2,3,4,5](#)

My guess is: For polynomials $x^{kn} + x^{(k-1)n} + \dots + x^{2n} + x^n + 1$, $k \geq 2$
 $n \not\equiv 0 \pmod{k+1}$, they all have a certain factor $P(x)$.

Is that true? How do I find the factor $P(x)$? How to prove? (I think the method of Cotes' Theorem may be used for it. See T. Needham, *Visual Complex Analysis*, pp 46-47)

complex-analysis

polynomials

complex-numbers

factoring

Share Cite Follow

asked 16 hours ago



Дъартский

35 4



New contributor

Sorted by:

Highest score (default)



1 Answer



1



If $P_k(x) = P(x) = x^k + x^{(k-1)} + \dots + x^2 + x + 1$, then with $Q_{k,n}(x) = Q(x) = x^{kn} + x^{(k-1)n} + \dots + x^{2n} + x^n + 1$ we have that $Q(y) = P(y^n)$.



Since the roots of P are precisely the $k + 1$ roots of unity distinct from 1, so $e^{2\pi im/(k+1)}, m = 1, \dots, k$ we get that the roots of Q are precisely



$$e^{2\pi ir/n} e^{2\pi im/(n(k+1))}, m = 1, \dots, k, r = 0, \dots, n - 1$$

Now if $(n, k + 1) = 1$ one can easily see that one can solve in $c = 1, \dots, k, r = 0, \dots, n - 1$ the equation $r(k + 1) - cn = m$ for every $m = 1, \dots, k$ as one first solves $r(k + 1) - cn = 1$ with $(c, k + 1) = 1$ and then one gets the solutions for $m = 2, \dots, k$ as $2c, \dots, kc$ (reducing them modulo $k + 1$) which are none divisible by $k + 1$ so are indeed in $1, \dots, k$ modulo $k + 1$

But this means that for all such n we have that $P_k / Q_{k,n}$ so indeed all $Q_{k,n}$ have that as a common subfactor.

If $(n, k + 1) = d > 1$ then we get as roots of Q only the nontrivial roots of unity of order $(k + 1)$ (and of course roots of unity of higher order involving n) that are of the form $e^{2\pi idm/(k+1)}, m = 1, \dots, (k + 1)/d$ so in general, there is no common factor.

Share Cite Follow

answered 10 hours ago



Conrad

21.1k

1

14

27