Reading:

On the factorization of $x^n - 1$

According to Theorem 11 of Chapter 1 of DoA, because it is a monic polynomial with integer coefficients, the only possible rational roots of $x^n - 1$, are $+1$ and -1 because these are the only integer factors of -1. Our goal is to factor $x^n - 1$ into a product of polynomials $x^n - 1 = p_1 p_2 \cdots p_k$ so that each p_j is either $x - 1$ or $x + 1$ or a polynomial with no rational roots.

If m is a positive integer, the polynomial $x^m - 1$ has 1 as a root, so $x - 1$ is a factor of $x^m - 1$. Indeed,

$$x^m - 1 = (x - 1)(x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1)$$

To see this, we can find the product of the factors on the right

$$\begin{aligned}(x-1)(x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1) &= x(x^{m-1} + x^{m-2} + x^{m-3} + \cdots + x + 1) \\ &\quad -1(x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1) \\ &= x^m + x^{m-1} + x^{m-2} + \cdots + x^2 + x \\ &\quad - x^{m-1} - x^{m-2} - \cdots - x^2 - x - 1 \\ &= x^m - 1\end{aligned}$$

because of all the cancellation.

In the same way, we can see that if m is an odd positive integer, the polynomial $x^m + 1$ has -1 as a root (because $(-1)^m + 1 = -1 + 1 = 0$ when m is odd), so $x + 1$ is a factor of $x^m + 1$. Indeed,

$$x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + x^{m-3} - \cdots + x^2 - x + 1)$$

To see this, we can find the product of the factors on the right

$$\begin{aligned}(x+1)(x^{m-1} - x^{m-2} + \cdots + x^2 - x + 1) &= x(x^{m-1} - x^{k-2} + x^{k-3} - \cdots - x + 1) \\ &\quad +1(x^{m-1} - x^{m-2} + \cdots + x^2 - x + 1) \\ &= x^m - x^{m-1} + x^{m-2} + \cdots - x^2 + x \\ &\quad + x^{m-1} - x^{m-2} - \cdots + x^2 - x + 1 \\ &= x^m + 1\end{aligned}$$

because of all the cancellation. By the theorem mentioned above, the second factor, $(x^{m-1} - x^{m-2} + x^{m-3} - \cdots + x^2 - x + 1)$, does not have any rational roots because 1 is not a root

$$1^{m-1} - 1^{m-2} + 1^{m-3} - \cdots + 1^2 - 1 + 1 = 1 \neq 0$$

and -1 is not a root

$$(-1)^{m-1} - 1^{m-2} + (-1)^{m-3} - \cdots + (-1)^2 - (-1) + 1 = m \neq 0$$

If m is a positive even integer, $x^m + 1$ does not have any rational roots because neither 1 nor -1 is a root of $x^m + 1$.

Now, suppose n is an even positive integer, say $n = 2m$ for the positive integer m. Then

$$x^n - 1 = x^{2m} - 1 = (x^m)^2 - 1 = (x^m - 1)(x^m + 1)$$

The first factor on the right, $x^m - 1$, is another polynomial of the sort that we are considering, so we may use these ideas to factor it as well. The factorization of the second factor on the right was considered in the paragraph above and factored to the extent we are interested.

Finally, suppose n is an odd positive integer. Since n is odd, 2 does not divide n, and the prime factorization of n includes only odd primes. Let p be the smallest prime factor of n, and suppose $n = pm$ for some positive odd integer m. Then

$$x^n - 1 = x^{mp} - 1 = (x^m)^p - 1 = (x^m - 1)[(x^m)^{p-1} + (x^m)^{p-2} + \cdots + (x^m)^2 + x^m + 1]$$

The first factor on the right, $x^m - 1$, is another polynomial of the sort that we are considering, so we may use these ideas to factor it as well. The second factor on the right,

$$(x^m)^{p-1} + (x^m)^{p-2} + \cdots + (x^m)^2 + x^m + 1$$

does not have any rational roots. To see this, we note that the theorem noted above shows the only possible rational roots are $+1$ and -1. Clearly, 1 is not a root because

$$(1^m)^{p-1} + (1^m)^{p-2} + \cdots + (1^m)^2 + 1^m + 1 = p \neq 0$$

Further, -1 is not a root because m is odd and

$$\begin{aligned}((-1)^m)^{p-1} + ((-1)^m)^{p-2} + \cdots + ((-1)^m)^2 + (-1)^m + 1 \\ &= (-1)^{p-1} + (-1)^{p-2} + \cdots + (-1)^2 - 1 + 1 \\ &= 1 \neq 0\end{aligned}$$

To summarize, to factor $x^n - 1$ into factors of the desired form, begin by finding the canonical factorization of n into primes. Use the factorizations above, successively, starting with the smallest prime factors, removing one factor in each step, until all the factors have been used and the only polynomial of the form $x^j - 1$ in the final factorization has $j = 1$.

Note: This technique does *not* always find the complete factorization of the polynomial $x^n - 1$ into factors with integer coefficients, even though it *does* accomplish the goals we set for ourselves of factoring the polynomial into factors with no rational roots. For example, $x^6 + 1 = (x^2 + 1)(x^4 - x^2 + 1)$ even though we would be, from the above, content to stop at $x^6 + 1$. If you take courses in *modern algebra*, such as Math 453, Math 505, or Math 553, you may learn more about factorization and especially learn when you have completely factored a polynomial.

1. Factor $x^8 - 1$ as in the Reading.

2. Factor $x^{27} - 1$ as in the Reading.

3. Factor $x^{60} - 1$ as in the Reading.