

Proof. Let $f(x) = x^n - x^{n-1} - \dots - x - 1$, $F(x) = (x-1)f(x) = x^{n+1} - 2x^n + 1$. Treat them as polynomials defined on complex plane \mathbf{C} .

Claim. Exactly one complex zero of f satisfies $|z| > 1$, and the other $n-1$ zeros of f satisfy $|z| < 1$.

Proof. It is equivalent to show that F has exactly one zero with $|z| = 1$, one with $|z| > 1$, and $n-1$ zeros with $|z| < 1$. Let's first prove that there is exactly one root of F with $|z| = 1$. If root z of F has absolute value 1, then we have that

$$2z^n = z^{n+1} + 1$$

thus

$$2 = 2|z^n| = |z^{n+1} + 1| \leq |z|^{n+1} + 1 = 2$$

This inequality only holds when $|z^{n+1} + 1| = |z|^{n+1} + 1$, in other words, $z^{n+1} = 1$. But since $F(z) = 0$, $z^n = \frac{z^{n+1} + 1}{2} = 1$. Dividing $z^{n+1} = 1$ by equation obtained just before, we get $z = 1$. So 1 is the only zero of F lies on the unit circle.

Let's denote with $\alpha_1, \alpha_2, \dots, \alpha_n$ be the zeros of F except 1. Since $|\alpha_1 \alpha_2 \dots \alpha_n| = 1$ and none of them lies on unit circle, it follows that at least one of the roots is larger than 1 in absolute value. Without loss of generality suppose $|\alpha_1| > 1$ and let

$$g(x) = x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0$$

be the polynomial with roots $1, \alpha_2, \alpha_3, \dots, \alpha_n$. Then,

$$\begin{aligned} F(x) &= (x - \alpha_1)g(x) \\ &= x^{n+1} + (b_{n-1} - \alpha_1)x^n + (b_{n-2} - b_{n-1}\alpha_1)x^{n-1} + \dots + (b_0 - b_1\alpha_1)x - b_0\alpha_1 \end{aligned}$$

Thus we get $b_{n-1} - \alpha_1 = -2$, $-b_0\alpha_1 = 1$, and $0 = b_{k-1} - b_k\alpha_1$ for $1 \leq k \leq n-1$. Then we have

$$\begin{aligned} |b_{n-1} - \alpha_1| &= 2 = 1 + 0 + \dots + 0 + 1 \\ &= 1 + |b_{n-2} - b_{n-1}\alpha_1| + |b_{n-3} - b_{n-2}\alpha_1| + \dots + |b_0\alpha_1| \\ &\geq 1 + |b_{n-1}||\alpha_1| - |b_{n-2}| + |b_{n-2}||\alpha_1| - |b_{n-3}| + \dots + |b_1||\alpha_1| - |b_0| + |b_0||\alpha_1| \\ &= 1 + |b_{n-1}| + (|\alpha_1| - 1)(|b_{n-1}| + \dots + |b_1| + |b_0|) \end{aligned}$$

On the other hand, $|b_{n-1} - \alpha_1| \leq |b_{n-1}| + |\alpha_1|$, so

$$|b_{n-1}| + |\alpha_1| \geq 1 + |b_{n-1}| + (|\alpha_1| - 1)(|b_{n-1}| + \dots + |b_1| + |b_0|)$$

and therefore

$$|b_{n-1}| + \dots + |b_1| + |b_0| \leq 1$$

Then, for any complex number α with $|\alpha| > 1$, we have

$$\begin{aligned} |g(\alpha)| &= |\alpha^n + b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + \dots + b_1\alpha + b_0| \\ &\geq |\alpha|^n - |b_{n-1}||\alpha|^{n-1} - |b_{n-2}||\alpha|^{n-2} - \dots - |b_1||\alpha| - |b_0| \\ &> |\alpha|^n - |\alpha|^n(|b_{n-1}| + \dots + |b_1| + |b_0|) \\ &= |\alpha|^n(1 - |b_{n-1}| - \dots - |b_1| - |b_0|) \geq 0 \end{aligned}$$

And so α cannot be a zero. It follows that all the zeros of g is not larger than one in absolute value. This completes the proof of the claim, because 1 is the only zero of g on unit circle, and the other $n - 1$ zeros of g are inside the unit circle. \square

Now, let's go back to our original problem and see how we can prove f is irreducible using this claim. Suppose that $f(x) = p(x)q(x)$, where p and q are integer polynomials. Since f has only one zero not in interior of the unit circle, one of the polynomials p, q has all its zeros strictly inside the unit circle. Suppose that z_1, \dots, z_k are the zeros of p , and $|z_1|, \dots, |z_k| < 1$. Since $f(0) = 1$, $p(0)$ is a nonzero integer, but $|p(0)| = |z_1 \cdots z_k| < 1$, which leads contradiction. Therefore f is irreducible over integers. Then f is irreducible over rationals by Gauss's lemma, which states that

If a polynomial with integer coefficients is irreducible over the integers, then it is also irreducible if it is considered as a polynomial over the rationals.

\square