Irreducibility of $X^n - X - 1$

Peter Müller

August 18, 2015

In [Sel56] Selmer proved that $X^n - X - 1$ ($n \geq 2$) is irreducible over $\mathbb{Q}$. In [Lju60] Ljunggren developed a different technique to prove irreducibility of lacunary polynomials. His technique works particularly well for $f(X) = X^n - X - 1$:

For $g(X) \in \mathbb{Q}[X]$ of degree m let $\hat{g}(X) := X^m g(1/X)$ be the reciprocal polynomial.

Assume that $f(X)$ is reducible, so $X^n - X - 1 = u(X)v(X)$ with non-constant monic polynomials $u, v \in \mathbb{Z}[X]$. From $u(0)v(0) = -1$ we may assume that $u(0) = 1$, $v(0) = -1$. Set $g(X) = \hat{u}(X)v(X)$. So g is monic of degree n, and $g(0) = -1$. Write $g(X) = -1 + a_1 X + a_2 X^2 + \cdots + a_{n-1} + X^n$. Comparing the coefficients of X^n in

$$(X^n - X - 1)(-X^n - X^{n-1} + 1) = f(X)\hat{f}(X) = u(X)v(X)\hat{u}(X)\hat{v}(X) = g(X)\hat{g}(X)$$

yields

$$3 = 1 + a_1^2 + a_2^2 + \cdots + a_{n-1}^2 + 1,$$

hence

$$g(X) = X^n + \epsilon X^m - 1$$

for some $1 \leq m \leq n-1$ and $\epsilon \in \{-1, 1\}$.

Now comparing the coefficients of X in

$$(X^n - X - 1)(-X^n - X^{n-1} + 1) = g(X)\hat{g}(X) = (X^n + \epsilon X^m - 1)(-X^n + \epsilon X^{n-m} + 1)$$

shows that either $\epsilon = -1$, $m = 1$, or $\epsilon = 1$, $m = n-1$. In the former case we have $g = f$, hence $\hat{u} = u$. The latter case yields $g = -\hat{f}$, hence $\hat{v} = -v$.

Let $\zeta \in \mathbb{C}$ be a root of u if $\hat{u} = u$, or a root of v if $\hat{v} = -v$. Thus in either case, $f(\zeta) = 0 = -\hat{f}(\zeta)$. From

$$\zeta^n - \zeta - 1 = 0 = \zeta^n + \zeta^{n-1} - 1$$

we get $\zeta^{n-2} = -1$. So $0 = -f(\zeta) = -\zeta^2\zeta^{n-2} + \zeta + 1 = \zeta^2 + \zeta + 1$, and therefore $\zeta^3 = 1$.

Write $n = 3k + r$ with $r \in \{0, 1, 2\}$. So $0 = f(\zeta) = \zeta^r - \zeta - 1$, in conflict with $\zeta^2 + \zeta + 1 = 0$.

References

[Lju60] W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. (1960), **8**, 65–70.

[Sel56] E. S. Selmer, *On the irreducibility of certain trinomials*, Math. Scand. (1956), **4**, 287–302.

E-mail: `peter.mueller@mathematik.uni-wuerzburg.de`