IRREDUCIBILITY OF $x^n - x - 1$

KEITH CONRAD

In 1956, Selmer [2] proved the following theorem.

**Theorem 1** (Selmer). For all $n \geq 2$, the polynomial $x^n - x - 1$ is irreducible in $\mathbb{Q}[x]$.

None of the standard irreducibility tests, such as reduction mod $p$ or the Eisenstein criterion, can be applied to $x^n - x - 1$ for general $n$. However, in a special case we can use one of these tests: if $n = p$ is prime then $x^p - x - 1$ is irreducible mod $p$ and therefore is irreducible in $\mathbb{Q}[x]$. More generally, if $a$ is an integer not divisible by $p$ then $x^p - x - a$ is irreducible in $\mathbb{Q}[x]$ because the polynomial is irreducible mod $p$; a proof of this is in many books on abstract algebra or field theory. Such a proof of irreducibility does not extend to $x^{pn} - x - 1$ when $m \geq 2$, since this polynomial is generally reducible mod $p$.

**Example 2.** If an integer $m > 1$ is not divisible by $p$ then a root of $x^p - x - 1/m$ in characteristic $p$ is a root of $x^{pn} - x - 1$:

$$a^p = \alpha + \frac{1}{m} \implies \alpha^m = \alpha + \frac{k}{m}$$

for all $k \geq 1$ by induction. Setting $k = m$ gives us $\alpha^m = \alpha + 1$. The polynomial $x^p - x - 1/m$ is irreducible in $\mathbb{F}_p[x]$, so $x^p - x - 1/m$ is a nontrivial factor of $x^{pn} - x - 1$ in $\mathbb{F}_p[x]$.

Selmer’s original proof of Theorem 1 involved studying the distribution of the roots of $x^n - x - 1$ in $\mathbb{C}$, relying at the end on the arithmetic–geometric mean inequality. The irreducibility proof that we give below is shorter and more algebraic. I learned it from David Rohrlich, who in turn learned it from Michael Filaseta.

**Proof.** For nonzero $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ of degree $n$, let $\tilde{f}(x)$ be its reciprocal polynomial:

$$\tilde{f}(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = x^{\deg f} f(1/x).$$

We call $\tilde{f}(x)$ the reciprocal polynomial because its roots are the reciprocals of the roots of $f(x)$. More precisely, if $f(x)$ has leading coefficient $a_0$ and $f(0) \neq 0$ then

$$f(x) = a_0(x - r_1) \cdots (x - r_n) \implies \tilde{f}(x) = f(0)(x - 1/r_1) \cdots (x - 1/r_n).$$

The following properties of this construction will be used below without comment:

- if $f(0) \neq 0$ then $\deg f = \deg \tilde{f}$ and $\tilde{f} = f$,
- if $f = gh$ then $\tilde{f} = \tilde{g} \tilde{h}$,
- for every nonzero constant $c$, $c \tilde{f} = c \tilde{f}$,
- if $f(x) = \sum_{i=0}^n a_i x^i$ has degree $n$ then the $x^n$-coefficient of $f(x) \tilde{f}(x)$ is $a_0^2 + a_1^2 + \cdots + a_n^2$.

Check all of these properties yourself. The last one is the most interesting.

The proof of the theorem will be presented in three steps.
Step 1: For \( n \geq 2 \), \( x^n - x - 1 \) and its reciprocal polynomial have no common root in characteristic 0.

The reciprocal polynomial is \(-x^n - x^{n-1} + 1\). If this shares a root with \( x^n - x - 1 \) in characteristic 0, say \( \alpha \), then
\[
\alpha^n = \alpha + 1 \quad \text{and} \quad \alpha^n = -\alpha^{n-1} + 1,
\]
so \(-\alpha^{n-1} = \alpha\). Thus \( \alpha^n = -\alpha^2 \). Substituting this into either equation in (1) gives us \(-\alpha^2 = \alpha + 1\), which implies \( \alpha^3 = 1 \), so every power of \( \alpha \) is either 1, \( \alpha \), or \( \alpha^2 \). If \( \alpha^n = 1 \) then the first equation in (1) becomes \( 1 = \alpha + 1 \), which is false since \( \alpha \neq 0 \). If \( \alpha^n = \alpha \) then \( \alpha = \alpha + 1 \), which is absurd. If \( \alpha^n = \alpha^2 \) then the two equations in (1) become \( \alpha^2 = \alpha + 1 \) and \( \alpha^2 = -\alpha + 1 \), so \( \alpha = -\alpha \), but \( \alpha \neq 0 \). Thus a common root \( \alpha \) in characteristic 0 doesn’t exist.

Step 2: For \( f(x) \in \mathbb{Z}[x] \), assume \( f(0) \neq 0 \) and \( f(x) \) and \( \tilde{f}(x) \) have no common roots in characteristic 0. If \( f(x) = g(x)h(x) \) for some nonconstant \( g(x) \) and \( h(x) \) in \( \mathbb{Z}[x] \), then there is a \( k(x) \) in \( \mathbb{Z}[x] \) with \( \deg k = \deg f \) such that \( ff = kk \) and \( k \neq \pm f \) or \( \pm \tilde{f} \). If \( f(x) \) is monic and \( f(0) = \pm 1 \) then we can choose \( k(x) \) to be monic with \( k(0) = \pm 1 \).

Since \( f(0) \neq 0 \), both \( g(0) \) and \( h(0) \) are not 0, so \( \deg \tilde{g} = \deg g \) and \( \deg \tilde{h} = \deg h \). Define
\[
k(x) = g(x)\tilde{h}(x).
\]
Then \( \deg k = \deg g + \deg \tilde{h} = \deg g + \deg h = \deg f \) and \( \tilde{g}h = (gh)(\tilde{h}) = (gh)(\tilde{h}) = \tilde{f}f \). If \( k \) and \( f \) are equal up to sign then \( \tilde{g}h \) and \( gh \) are equal up to sign, so \( h \) and \( \tilde{h} \) are equal up to sign, but then every root of \( h \) (it has roots since \( h \) is nonconstant) would be a common root of \( f = gh \) and \( \tilde{f} = g\tilde{h} \), which is a contradiction. The proof that \( k \) and \( \tilde{f} \) are not equal up to sign is similar with \( g \) in place of \( h \).

If \( f(x) \) is monic and \( f(0) = \pm 1 \) then \( (f\tilde{f})(0) = f(0)(\text{lead } f) = \pm 1 \) so also \( (k\tilde{k})(0) = \pm 1 \), or \( k(0)(\text{lead } k) = \pm 1 \). This is in \( \mathbb{Z} \), so \( k(0) \) and lead \( k \) are \( \pm 1 \) (maybe not equal). Replacing \( k \) with \(-k \) doesn’t change \( \deg k \) or \( \deg \tilde{k} \), so with a sign change we can make \( k \) monic.

Step 3: (We’re ready!) The polynomial \( x^n - x - 1 \), for \( n \geq 2 \), is irreducible in \( \mathbb{Q}[x] \).

We argue by contradiction, and can assume \( n > 2 \) since the case \( n = 2 \) can be checked directly. If \( x^n - x - 1 \) is reducible in \( \mathbb{Q}[x] \) then it factors into a product of two nonconstant polynomials in \( \mathbb{Z}[x] \). Set \( f(x) = x^n - x - 1 \). By Steps 1 and 2, \( ff = \tilde{k}k \) for some monic \( k \in \mathbb{Z}[x] \) of degree \( n \) with \( k(0) = \pm 1 \) and \( k \) is not \( \pm f \) or \( \pm \tilde{f} \). Write \( k(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \), so \( b_n \) is 1 and \( b_0 = \pm 1 \). Comparing the coefficients of \( x^n \) in both \( ff \) and \( kk \),
\[
1^2 + (-1)^2 + (-1)^2 = b_0^2 + b_1^2 + \cdots + b_n^2.
\]
Since \( b_n = 1 \) and \( b_0 = \pm 1 \), we get \( b_1^2 + \cdots + b_{n-1}^2 = 1 \) in \( \mathbb{Z} \), so exactly one of \( b_1, \ldots, b_{n-1} \) is \( \pm 1 \) and the rest are 0: \( k(x) = x^n + b_ix^i + b_0 \) with 1 \( \leq i \leq n-1 \) and \( b_i = \pm 1 \). Let’s look at the terms of \( \tilde{f}f \) and \( k\tilde{k} \) in degrees above \( n \):
\[
\tilde{f}f = (x^n - x - 1)(-x^n - x^{n-1} + 1) = -x^{2n} - x^{2n-1} + x^{n+1} + \cdots
\]
and
\[
k\tilde{k} = (x^n + b_ix^i + b_0)(b_0x^n + b_ix^{n-i} + 1) = b_0x^{2n} + b_ix^{n-i} + b_0b_ix^{n+i} + \cdots
\]
where \( \cdots \) means terms of degree \( n \) or less. From the leading terms \( b_0 = -1 \), so
\[
-x^{2n} - x^{2n-1} + x^{n+1} + \cdots = -x^{2n} + b_ix^{n-i} - b_ix^{n+i} + \cdots.
\]
The terms on the left have distinct degrees since $2n > 2n - 1 > n + 1$ (the last inequality uses $n > 2$), so on the right side $2n - i \neq n + i$. If $2n - i > n + i$ then $i = 1$ and $b_i = -1$, so $k = x^n - x - 1 = f$. If $n + i > 2n - i$ then $i = n - 1$ and $b_i = 1$, so $k = x^n + x^{n-1} - 1 = -\tilde{f}$. Recalling that $k$ is not ±$f$ or ±$\tilde{f}$, we have reached a contradiction. □

In the appendix we discuss how this proof applies to more trinomials $x^n \pm x^m \pm 1$.

**Remark 3.** Before Selmer’s work on $x^n - x - 1$, Perron [1] had proved irreducibility of $x^n + ax \pm 1$ in $\mathbb{Q}[x]$ for all integers $a$ such that $|a| \geq 3$, and also for $|a| = 2$ provided 1 or −1 are not roots (e.g., $x^n - 2x + 1$ has 1 as a root and $x^{2m} + 2x + 1$ has −1 as a root).

**Appendix A. More irreducible trinomials**

The irreducibility argument we gave for $x^n - x - 1$ can be applied to nearly all trinomials of the form $x^n \pm x^m \pm 1$, in the sense that it tells us exactly when they are irreducible.

**Theorem 4.** For $1 < m < n$ with $m \neq n/2$, and $\delta$ and $\varepsilon$ equal to ±1, the polynomial $x^n + \delta x^m + \varepsilon$ is irreducible in $\mathbb{Q}[x]$ if and only if it has no root in common with its reciprocal polynomial.

Proof. Let $f(x) = x^n + \delta x^m + \varepsilon$. Then $\tilde{f}(x) = \varepsilon x^n + \delta x^{m-n} + 1 = \varepsilon(x^n + \varepsilon \delta x^{m-n} + \varepsilon)$. Since $m \neq n/2$ the middle terms of $f(x)$ and $\tilde{f}(x)$ have different degrees, so $f(x)$ and $\tilde{f}(x)$ are not scalar multiples of each other. Therefore irreducibility of $f(x)$ in $\mathbb{Q}[x]$ implies $f(x)$ and $\tilde{f}(x)$ have no common root.

Conversely, if $f(x)$ and $\tilde{f}(x)$ have no common root then the proof of Theorem 1 goes through with $f(x)$ in place of $x^n - x - 1$. (As in that proof, the product $f(x)\tilde{f}(x)$ has three terms of degree above $n$ because $m \neq n/2$.) Details are left to the reader. □

In down-to-earth terms, if $m \neq n/2$ and $\delta, \varepsilon \in \{\pm 1\}$, then $x^n + \delta x^m + \varepsilon$ is irreducible except when it has a root in common with $x^n + \varepsilon \delta x^{m-n} + \varepsilon$.

**Example 5.** Let’s apply Theorem 4 to $x^n + x + 1$. Computer data suggest that $x^n + x + 1$ is reducible if and only if $n \equiv 2 \mod 3$ with $n > 2$, and in this case $x^2 + x + 1$ is a factor of $x^n + x + 1$. For example,

\[
\begin{align*}
x^5 + x + 1 &= (x^2 + x + 1)(x^3 - x^2 + 1), \\
x^8 + x + 1 &= (x^2 + x + 1)(x^6 - x^5 + x^3 - x^2 + 1), \\
x^{11} + x + 1 &= (x^2 + x + 1)(x^9 - x^8 + x^6 - x^5 + x^3 - x^2 + 1).
\end{align*}
\]

To prove $x^2 + x + 1$ is a factor of $x^n + x + 1$ if $n \equiv 2 \mod 3$, work in $\mathbb{Q}[x]/(x^2 + x + 1)$: $x^2 \equiv -x - 1$ and $x^3 \equiv 1$, so $x^{3j+2} + x + 1 \equiv x^2 + x + 1 \equiv 0$.

Next we will prove that if $x^n + x + 1$ is reducible in $\mathbb{Q}[x]$ then $n \equiv 2 \mod 3$. By Theorem 4, reducibility implies $x^n + x + 1$ and its reciprocal polynomial $x^n + x^{n-1} + 1$ have a common root, say $\alpha$:

$$\alpha^n + \alpha + 1 = 0 \quad \text{and} \quad \alpha^n + \alpha^{n-1} + 1 = 0.$$ 

Thus $\alpha = \alpha^{n-1}$, so $\alpha^n = \alpha^2$, which makes both of the equations above $\alpha^2 + \alpha + 1 = 0$. That implies $\alpha^3 = 1$, and definitely $\alpha \neq 1$, so from $\alpha^n = \alpha^2$ we must have $n \equiv 2 \mod 3$.

Selmer [2] showed that when $n \equiv 2 \mod 3$ and $n > 2$, so $x^n + x + 1 = (x^2 + x + 1)g_n(x)$, the polynomial $g_n(x)$ is irreducible over $\mathbb{Q}$.

The polynomials $x^n - x + 1$ and $x^n + x - 1$ have properties similar to Example 5: in each case there is a congruence condition on $n \mod 6$ that gives the polynomial an automatic
low-degree factor (discover it yourself by generating numerical data), and that congruence condition on \( n \) turns out to be equivalent to the polynomial having a common root with its reciprocal polynomial, so those \( n \) not fitting the congruence condition mod 6 lead to an irreducible polynomial.

Theorem 4 avoids the case \( m = n/2 \). What happens in that case?

**Corollary 6.** For all \( m \geq 1 \) and \( \delta = \pm 1 \), the polynomial \( x^{2m} + \delta x^m - 1 \) is irreducible in \( \mathbb{Q}[x] \).

**Proof.** The proof of Theorem 1 still works when it is applied to both \( x^{2m} + x^m - 1 \) and \( x^{2m} - x^m - 1 \) (here the degree \( n \) is \( 2m \)). Details are left to the reader. \( \square \)

The polynomials \( x^{2m} + \delta x^m + 1 \) with constant term 1 and \( \delta = \pm 1 \) are more subtle, with irreducibility being the exception rather than the norm. For \( m \geq 1 \), numerical evidence suggests that \( x^{2m} + x^m + 1 \) is irreducible over \( \mathbb{Q} \) if and only if \( m \) is a power of 3 and \( x^{2m} - x^m + 1 \) is irreducible over \( \mathbb{Q} \) if and only if \( m = 2^i 3^j \) for some \( i \) and \( j \).

**References**
