

# IRREDUCIBILITY OF $x^n - x - 1$

KEITH CONRAD

## 1. INTRODUCTION

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

**Theorem 1.1** (Selmer). *For all  $n \geq 2$ , the polynomial  $x^n - x - 1$  is irreducible in  $\mathbf{Q}[x]$ .*

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  $\mathbf{Q}[x]$ . More generally, if  $a$  is an integer not divisible by  $p$  then  $x^p - x - a$  is irreducible in  $\mathbf{Q}[x]$  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  $x^{p^m} - x - 1$  when  $m \geq 2$ , since this polynomial is generally reducible mod  $p$ .

**Example 1.2.** 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  $x^{p^m} - x - 1$ :

$$\alpha^p = \alpha + \frac{1}{m} \implies \alpha^{p^k} = \alpha + \frac{k}{m} \text{ in characteristic } p$$

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

## 2. PROOF OF IRREDUCIBILITY

Selmer's original proof of Theorem 1.1 involves studying the distribution of the roots of  $x^n - x - 1$  in  $\mathbf{C}$ , 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  $\tilde{\tilde{f}} = f$ ,
- if  $f = gh$  then  $\tilde{f} = \tilde{g}\tilde{h}$ ,
- for every nonzero constant  $c$ ,  $\tilde{cf} = c\tilde{f}$ ,

- 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  $a_0^2 + a_1^2 + \dots + a_n^2$ .

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

$$(2.1) \quad \alpha^n = \alpha + 1 \text{ and } \alpha^n = -\alpha^{n-1} + 1,$$

so  $-\alpha^{n-1} = \alpha$ . Thus  $\alpha^n = -\alpha^2$ . Substituting this into either equation in (2.1) 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 (2.1) 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 (2.1) 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  $f(x) \in \mathbf{Z}[x]$ , 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  $\mathbf{Z}[x]$ , then there is a  $k(x)$  in  $\mathbf{Z}[x]$  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  $kk = (gh)(\tilde{g}\tilde{h}) = (gh)(\tilde{g}\tilde{h}) = ff$ . If  $k$  and  $f$  are equal up to sign then  $gh$  and  $\tilde{g}\tilde{h}$  are equal up to sign, so  $\tilde{h}$  and  $h$  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  $\tilde{f} = \tilde{g}\tilde{h}$ , 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  $(ff)(0) = f(0)(\text{lead } f) = \pm 1$  so also  $(kk)(0) = \pm 1$ , or  $k(0)(\text{lead } k) = \pm 1$ . This is in  $\mathbf{Z}$ , so  $k(0)$  and lead  $k$  are  $\pm 1$  (maybe not equal). Replacing  $k$  with  $-k$  doesn't change  $\deg k$  or  $kk$ , 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  $\mathbf{Q}[x]$ .

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  $\mathbf{Q}[x]$  then it factors into a product of two nonconstant polynomials in  $\mathbf{Z}[x]$ . Set  $f(x) = x^n - x - 1$ . By Steps 1 and 2,  $ff = kk$  for some monic  $k \in \mathbf{Z}[x]$  of degree  $n$  with  $k(0) = \pm 1$  and  $k$  is not  $\pm f$  or  $\pm \tilde{f}$ . Write  $k(x) = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0$ , so  $b_n = 1$  and  $b_0 = \pm 1$ . Comparing the coefficients of  $x^n$  in both  $ff$  and  $kk$ ,

$$1^2 + (-1)^2 + (-1)^2 = b_0^2 + b_1^2 + \dots + b_n^2.$$

Since  $b_n = 1$  and  $b_0 = \pm 1$ , we get  $b_1^2 + \dots + b_{n-1}^2 = 1$  in  $\mathbf{Z}$ , so exactly one of  $b_1, \dots, b_{n-1}$  is  $\pm 1$  and the rest are 0:  $k(x) = x^n + b_i x^i + b_0$  with  $1 \leq i \leq n-1$  and  $b_i = \pm 1$ . Let's look at the terms of  $ff$  and  $kk$  in degrees above  $n$ :

$$ff = (x^n - x - 1)(-x^n - x^{n-1} + 1) = -x^{2n} - x^{2n-1} + x^{n+1} + \dots$$

and

$$\tilde{k}\tilde{k} = (x^n + b_i x^i + b_0)(b_0 x^n + b_i x^{n-i} + 1) = b_0 x^{2n} + b_i x^{2n-i} + b_0 b_i x^{n+i} + \dots$$

where  $\dots$  means terms of degree  $n$  or less. From the leading terms  $b_0 = -1$ , so

$$-x^{2n} - x^{2n-1} + x^{n+1} + \dots = -x^{2n} + b_i x^{2n-i} - b_i x^{n+i} + \dots.$$

The terms on the left have distinct degrees since  $2n > 2n-1 > n+1$  (the last inequality uses  $n > 2$ ), so there are three terms with degree greater than  $n$ . Therefore on the right side  $2n-i \neq n+i$  (otherwise the right side would have just one term with degree above  $n$ ). 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  $\pm f$  or  $\pm \tilde{f}$ , we have reached a contradiction.  $\square$

In the appendix we apply this method to more trinomials  $x^n \pm x^m \pm 1$ . For a further application of this method, see <https://mathoverflow.net/questions/404106>.

**Remark 2.1.** Before Selmer's work on  $x^n - x - 1$ , Perron [1] had proved irreducibility of  $x^n + ax \pm 1$  in  $\mathbf{Q}[x]$  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 A.1.** *For  $1 < m < n$  with  $m \neq n/2$ , and  $\delta$  and  $\varepsilon$  equal to  $\pm 1$ , the polynomial  $x^n + \delta x^m + \varepsilon$  is irreducible in  $\mathbf{Q}[x]$  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  $\tilde{f}(x) = \varepsilon x^n + \delta x^{n-m} + 1 = \varepsilon(x^n + \varepsilon \delta x^{n-m} + \varepsilon)$ . 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  $\mathbf{Q}[x]$  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 1.1 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.  $\square$

Concretely, 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  $x^n + \varepsilon \delta x^{n-m} + \varepsilon$ .

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

$$\begin{aligned} x^5 + x + 1 &= (x^2 + x + 1)(x^3 - x^2 + 1), \\ x^8 + x + 1 &= (x^2 + x + 1)(x^6 - x^5 + x^3 - x^2 + 1), \\ x^{11} + x + 1 &= (x^2 + x + 1)(x^9 - x^8 + x^6 - x^5 + x^3 - x^2 + 1). \end{aligned}$$

To prove  $x^2 + x + 1$  is a factor of  $x^n + x + 1$  if  $n \equiv 2 \pmod{3}$ , work in  $\mathbf{Q}[x]/(x^2 + x + 1)$ :  $x^2 \equiv -x - 1$  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  $\mathbf{Q}[x]$  then  $n \equiv 2 \pmod{3}$ . By Theorem A.1, reducibility implies  $x^n + x + 1$  and its reciprocal polynomial  $x^n + x^{n-1} + 1$  have a common root, say  $\alpha$ :

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

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  $n \equiv 2 \pmod{3}$ .

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

The polynomials  $x^n - x + 1$  and  $x^n + x - 1$  have properties similar to Example A.2: in each case there is a congruence condition on  $n \pmod{6}$  that gives the polynomial an automatic low-degree factor, which is  $x^2 - x + 1$ :

- $x^n - x + 1$  is irreducible unless  $n \equiv 2 \pmod{6}$  with  $n > 2$  (e.g.,  $n = 8, 14, 20$ ), when  $x^2 - x + 1$  is a factor,
- $x^n + x - 1$  is irreducible unless  $n \equiv 5 \pmod{6}$  (e.g.,  $n = 5, 11, 17$ ), when  $x^2 - x + 1$  is a factor.

For  $x^n - x + 1$  and  $x^n + x - 1$ , the congruence condition on  $n \pmod{6}$  above is equivalent to the polynomial having a common root with its reciprocal polynomial, so by Theorem A.1 the congruence condition is equivalent to reducibility when  $n > 2$ .

Theorem A.1 avoids the case  $m = n/2$ . What happens in that case?

**Corollary A.3.** *For all  $m \geq 1$  and  $\delta = \pm 1$ , the polynomial  $x^{2m} + \delta x^m - 1$  is irreducible in  $\mathbf{Q}[x]$ .*

*Proof.* The proof of Theorem 1.1 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.  $\square$

All that remains is  $x^{2m} + \delta x^m + 1$ , with constant term 1 and  $\delta = \pm 1$ . Examples generated by a computer suggest irreducibility is far less common than reducibility, as codified in the following theorem.

**Theorem A.4.** *For  $m \geq 1$ ,  $x^{2m} + x^m + 1$  is irreducible over  $\mathbf{Q}$  if and only if  $m$  is a power of 3 and  $x^{2m} - x^m + 1$  is irreducible over  $\mathbf{Q}$  if and only if  $m = 2^i 3^j$  for some nonnegative integers  $i$  and  $j$ .*

*Proof.* I learned the following argument from Dmitry Krachun.

There are two key points to keep in mind:

- (1)  $x^2 + x + 1$  is the minimal polynomial of primitive 3rd roots of unity and  $x^2 - x + 1$  is the minimal polynomial of primitive 6th roots of unity. In the notation of cyclotomic polynomials,  $x^2 + x + 1 = \Phi_3(x)$  and  $x^2 - x + 1 = \Phi_6(x)$ .
- (2) If  $f(x) \in \mathbf{Q}[x]$  and  $f(x^m)$  is irreducible then  $f(x^d)$  is irreducible when  $d$  is a (positive) factor of  $m$ . Indeed, arguing with the contrapositive, if  $f(x^d) = g(x)h(x)$  for nonconstant  $g(x)$  and  $h(x)$  in  $\mathbf{Q}[x]$ , then  $f(x^m) = g(x^{m/d})h(x^{m/d})$  and the polynomials on the right side are nonconstant. We will use this when  $d = p$  is a prime number: if  $f(x^m)$  is irreducible over  $\mathbf{Q}$  then so is  $f(x^p)$  for prime factors  $p$  of  $m$ .

First we will show

$$x^{2m} + x^m + 1 \text{ is irreducible over } \mathbf{Q} \implies m \text{ is a power of 3.}$$

Set  $f(x) = x^2 + x + 1$ , so  $x^{2m} + x^m + 1 = f(x^m)$ . If  $f(x^m)$  is irreducible over  $\mathbf{Q}$  then we will show  $m$  is a power of 3 by showing for each prime  $p \neq 3$  that  $f(x^p)$  is reducible, so the only possible prime factor of  $m$  is 3. (See the second key point above.)

Let  $\alpha$  be a root of  $x^2 + x + 1$ . The other root of  $x^2 + x + 1$  is  $\alpha^{-1}$  and  $\alpha^3 = 1$ , so powers  $\alpha^k$  only depend on  $k$  modulo 3. For each prime  $p \neq 3$ ,  $p \equiv \pm 1 \pmod{3}$ , so  $\alpha^p = \alpha^{\pm 1}$ . Therefore  $f(\alpha^p) = f(\alpha^{\pm 1}) = 0$ , so  $f(x^p)$  is divisible by the minimal polynomial of  $\alpha$  over  $\mathbf{Q}$ , which is  $x^2 + x + 1$ . That makes  $f(x^p)$  reducible since its degree  $2p$  is greater than 2.

Next we will show

$$x^{2m} - x^m + 1 \text{ is irreducible over } \mathbf{Q} \implies m = 2^i 3^j \text{ for some } i, j \geq 0.$$

Now set  $f(x) = x^2 - x + 1$ , so to prove  $f(x^m) = x^{2m} - x^m + 1$  can be irreducible only when the prime factors of  $m$  are 2 or 3, it suffices by the reasoning used above to show  $f(x^p)$  is reducible for each prime  $p > 3$ .

Let  $\beta$  be a root of  $x^2 - x + 1$ , so the other root is  $\beta^{-1}$  and  $\beta^6 = 1$ , so  $\beta^k$  only depends on  $k$  modulo 6. For prime  $p > 3$ ,  $p \equiv \pm 1 \pmod{6}$ , so  $f(\beta^p) = f(\beta^{\pm 1}) = 0$ . Thus  $f(x^p)$  is divisible by  $x^2 + x + 1$ , which makes  $f(x^p)$  reducible since its degree is greater than 2.

It remains to show

$$m \text{ is a power of 3} \implies \Phi_3(x^m) = x^{2m} + x^m + 1 \text{ is irreducible over } \mathbf{Q}$$

and

$$m = 2^i 3^j \implies \Phi_6(x^m) = x^{2m} - x^m + 1 \text{ is irreducible over } \mathbf{Q}.$$

These are both special cases of the following property of *all* cyclotomic polynomials  $\Phi_n(x)$ : if  $m$  is a positive integer whose prime factors all divide  $n$ , then  $\Phi_n(x^m) = \Phi_{mn}(x)$ . This polynomial identity is a consequence of both sides being monic of the same degree ( $m\varphi(n) = \varphi(mn)$  when all prime factors of  $m$  divide  $n$ ), the right side being the minimal polynomial over  $\mathbf{Q}$  of all roots of unity of order  $mn$ , and the left side vanishing at all roots of unity of order  $mn$ .<sup>1</sup>  $\square$

## REFERENCES

- [1] O. Perron, Neue Kriterien für die Irreduzibilität algebraischer Gleichungen, *J. reine angew. Math.* **132** (1907), 288–307. Online at <https://eudml.org/doc/149269>.
- [2] E. Selmer, On the Irreducibility of Certain Trinomials, *Math. Scand.* **4** (1956), 287–302. Online at <https://eudml.org/doc/165635>.

---

<sup>1</sup>In fact, for all positive integers  $m$  and  $n$ ,  $\Phi_n(x^m)$  is irreducible over  $\mathbf{Q}$  if and only if each prime factor of  $m$  is a factor of  $n$ . This becomes Theorem A.4 when  $n$  is 3 and 6.