

LECTURE 1

**An Example Concerning
the Irreducibility of $x^n + g(x)$**

$$\begin{aligned}
&1 \\
&1 + x^3 \\
&1 + x^3 + x^{15} \\
&1 + x^3 + x^{15} + x^{16} \\
&1 + x^3 + x^{15} + x^{16} + x^{32} \\
&1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} \\
&1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} \\
&1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}
\end{aligned}$$

QUESTION 1: Let $f_0(x) = 1$. For $k \geq 1$, define $f_k(x)$ to be the *reducible* polynomial of the form $f_{k-1}(x) + x^n$ with n as small as possible and $n > \deg f_{k-1}$. Is the sequence $\{f_k(x)\}$ a finite sequence or an infinite sequence?

QUESTION 1: Let $f_0(x) = 1$. For $k \geq 1$, define $f_k(x)$ to be the *reducible* polynomial of the form $f_{k-1}(x) + x^n$ with n as small as possible and $n > \deg f_{k-1}$. Is the sequence $\{f_k(x)\}$ a finite sequence or an infinite sequence?

Answer: The sequence $\{f_k(x)\}$ is a finite sequence. The polynomial

$$1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}$$

is the last polynomial in the sequence.

Problem: Find a proof.

Definitions and Notation: Let $f(x) \in \mathbb{C}[x]$ with $f \neq 0$. Then

$\tilde{f}(x) = x^{\deg f} f(1/x)$ is the *reciprocal* of $f(x)$.

If $f = \pm \tilde{f}$, then we say that f is *reciprocal*.

Comment: If f is reciprocal and α is a root of f , then $1/\alpha$ is a root of f .

Two-Steps For Establishing $\{f_k(x)\}$ is Finite:

1. Handle reciprocal factors (there are none).
2. Handle non-reciprocal factors (there is no more than one).

STEP 1: HANDLE RECIPROCAL FACTORS

Let

$$g(x) = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}.$$

If f is an irreducible reciprocal factor of

$$F(x) = x^n + g(x),$$

then it divides

$$\tilde{F}(x) = \tilde{g}(x)x^{n-35} + 1.$$

So f divides

$$\begin{aligned} \tilde{g}(x)F(x) - x^{35}\tilde{F}(x) \\ = g(x)\tilde{g}(x) - x^{35}. \end{aligned}$$

$$g(x) = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}$$

$$f \text{ divides } g(x)\tilde{g}(x) - x^{35}$$

f is either

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

or

$$x^{64} + x^{61} - x^{60} + x^{54} - \dots - x^{43} + 2x^{42} \\ + x^{41} - \dots + x^{10} - x^4 + x^3 + 1.$$

f is either

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

or

$$x^{64} + x^{61} - x^{60} + x^{54} - \dots - x^{43} + 2x^{42} \\ + x^{41} - \dots + x^{10} - x^4 + x^3 + 1.$$

Thus, f divides $F(x) = x^n + g(x)$. If

$$f = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$

then f also divides $x^7 - 1$. If $n \geq 7$, then f must divide

$$x^{n-7} + g(x).$$

If $n \geq 14$, then f must divide

$$x^{n-14} + g(x).$$

If $n \equiv r \pmod{7}$, then f must divide $x^r + g(x)$.

If $n \equiv r \pmod{7}$, then f must divide $x^r + g(x)$.

Test if $f = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ divides $x^r + g(x)$ for $r \in \{0, 1, 2, 3, 4, 6\}$.

It doesn't.

Conclusion: $F(x) = x^n + g(x)$ is not divisible by $f = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ for any n .

If f is an irreducible reciprocal factor of F , then f is the polynomial

$$\begin{aligned} &x^{64} + x^{61} - x^{60} + x^{54} - \dots - x^{43} + 2x^{42} \\ &\quad + x^{41} - \dots + x^{10} - x^4 + x^3 + 1. \end{aligned}$$

Suppose f is

$$x^{64} + x^{61} - x^{60} + x^{54} - \dots - x^{43} + 2x^{42} \\ + x^{41} - \dots + x^{10} - x^4 + x^3 + 1.$$

Compute the roots of f . In particular, f has a root

$$\alpha \approx 0.58124854 - 0.96349774 i$$

with

$$1.125 < |\alpha| < 1.126.$$

$$|g(\alpha)| < g(1.126) < 231 < 1.125^{47} < |\alpha|^{47}$$

$$|F(\alpha)| \geq |\alpha|^n - |g(\alpha)| > 0 \text{ for } n \geq 47$$

f does not divide F for any $n \geq 0$

STEP 2: HANDLE NON-RECIPROCAL FACTORS

Lemma 1: If the non-reciprocal part of a polynomial $F(x) \in \mathbb{Z}[x]$ is reducible, then there exist non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $F(x) = u(x)v(x)$.

Proof. Let $a(x)$ be an irreducible non-reciprocal factor of $F(x)$.

CASE 1: $\tilde{a}(x)$ divides F

Write $F(x) = u(x)v(x)$ where

$$\tilde{a}(x) \nmid u(x) \quad \text{and} \quad a(x) \nmid v(x).$$

CASE 2: $\tilde{a}(x)$ does not divide F

Consider an irreducible non-reciprocal $b(x)$ such that $a(x)b(x)$ divides F . If $\tilde{b}(x)$ divides F , appeal to Case 1 with $b(x)$ in place of $a(x)$. If $\tilde{b}(x)$ does not divide F , write $F(x) = u(x)v(x)$ where

$$a(x) \mid u(x) \quad \text{and} \quad b(x) \mid v(x).$$

Lemma 1: If the non-reciprocal part of a polynomial $F(x) \in \mathbb{Z}[x]$ is reducible, then there exist non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $F(x) = u(x)v(x)$.

Comment: In the case that $F(x)$ has a positive leading coefficient, both $u(x)$ and $v(x)$ can be taken to have a positive leading coefficient.

Lemma 1: If the non-reciprocal part of a polynomial $F(x) \in \mathbb{Z}[x]$ is reducible, then there exist non-reciprocal polynomials $u(x)$ and $v(x)$ in $\mathbb{Z}[x]$ such that $F(x) = u(x)v(x)$.

Assume the non-reciprocal part $F(x)$ is reducible. Let $u(x)$ and $v(x)$ be as in Lemma 1.

Lemma. The polynomial $w(x) = u(x)\tilde{v}(x)$ has the following properties:

- (i) $w \neq \pm F$ and $w \neq \pm \tilde{F}$.
- (ii) $w\tilde{w} = F\tilde{F}$.
- (iii) $w(1) = F(1)$.
- (iv) $\|w\| = \|F\|$.
- (v) If F is a 0, 1-polynomial, then w is also and with the same number of non-zero terms as F .

$$F(x) = u(x)v(x), \quad w(x) = u(x)\tilde{v}(x)$$

$u(x)$ and $v(x)$ are non-reciprocal

(v) if F is a 0, 1-polynomial, then w is also and with the same number of non-zero terms as F

Proof.

$$F(x) = \sum_{j=1}^r a_j x^{d_j}, \quad w(x) = \sum_{j=1}^s b_j x^{e_j}$$

$$\begin{aligned} \left(\sum_{j=1}^s b_j \right)^2 &\leq \left(\sum_{j=1}^s b_j^2 \right)^2 = \left(\sum_{j=1}^s a_j^2 \right)^2 \\ &= \left(\sum_{j=1}^s a_j \right)^2 = \left(\sum_{j=1}^s b_j \right)^2 \end{aligned}$$

(v) follows

Assume (the non-reciprocal part of)

$$F(x) = x^n + g(x)$$

is reducible.

$$g(x) = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35}$$

Then there is a $w(x)$ satisfying:

- (i) $w \neq \pm F$ and $w \neq \pm \tilde{F}$
- (ii) $w\tilde{w} = F\tilde{F}$
- (iii) $w(1) = F(1)$
- (iv) $\|w\| = \|F\|$
- (v) w is a 0, 1-polynomial with the same number of non-zero terms as F

- (i) $w \neq \pm F$ and $w \neq \pm \tilde{F}$ (ii) $w\tilde{w} = F\tilde{F}$
 (iii) $w(1) = F(1)$ (iv) $\|w\| = \|F\|$
 (v) w is a 0, 1-polynomial with the same number of non-zero terms as F

If $n \geq 83$, then

$$F\tilde{F} = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35} + \dots$$

where all subsequent terms have degree ≥ 48 .

$$\begin{aligned} w(x) &= 1 + ??? + x^n \\ \tilde{w}(x) &= 1 + ??? + x^n \end{aligned}$$

$$\begin{aligned} w(x) &= 1 + x^3 + \dots + x^n \\ \tilde{w}(x) &= 1 + \dots + x^{n-3} + x^n \end{aligned}$$

- (i) $w \neq \pm F$ and $w \neq \pm \tilde{F}$ (ii) $w\tilde{w} = F\tilde{F}$
 (iii) $w(1) = F(1)$ (iv) $\|w\| = \|F\|$
 (v) w is a 0, 1-polynomial with the same number of non-zero terms as F

$$F\tilde{F} = 1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35} + \dots$$

$$w(x) = 1 + x^3 + \dots + x^n$$

$$\tilde{w}(x) = 1 + \dots + x^{n-3} + x^n$$

$$w(x) = 1 + x^3 + x^{15} + \dots + x^n$$

$$\tilde{w}(x) = 1 + \dots + x^{n-15} + x^{n-3} + x^n$$

$$w(x) = 1 + x^3 + x^{15} + x^{16} + \dots + x^n$$

$$\tilde{w}(x) = 1 + \dots + x^{n-16} + x^{n-15} + x^{n-3} + x^n$$

So $w = F!!$

Summary:

- I. $x^n + g(x)$ has no reciprocal irreducible factors
- II. the non-reciprocal part of $x^n + g(x)$ is irreducible

The first of these was shown for all $n \geq 0$, and the second of these was shown for $n \geq 83$. Checking directly for $35 < n \leq 83$, we deduce the original claim.

$$\begin{aligned} &1 \\ &1 + x^3 \\ &1 + x^3 + x^{15} \\ &1 + x^3 + x^{15} + x^{16} \\ &1 + x^3 + x^{15} + x^{16} + x^{32} \\ &1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} \\ &1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} \\ &1 + x^3 + x^{15} + x^{16} + x^{32} + x^{33} + x^{34} + x^{35} \end{aligned}$$

Theorem: Let $g(x)$ be a 0, 1-polynomial with the property that $g(x)$ is irreducible over the set of 0, 1-polynomials (that is, $g(x)$ is not the product of two 0, 1-polynomials of degree > 0). Then the non-reciprocal part of $F(x) = x^n + g(x)$ is irreducible if $n > 3 \deg g$.