

ECE 7670

Lecture 4 – Polynomials over Galois fields

Objective: To become acquainted with some basic algebraic concepts of polynomials.

1 The Euclidean algorithm

The Euclidean algorithm is perhaps the oldest algorithm in the world, being attributed to Euclid and appearing in his *Elements*. It applies on any Euclidean domain:

Definition 1 A **Euclidean domain** is a set D with operations $+$ and \cdot satisfying:

1. D forms an additive commutative ring with identity.
2. Multiplicative cancelation: if $ab = bc$ and $b \neq 0$ then $a = c$.
3. Every $a \in D$ has a metric $g(a)$ such that:
 - (a) $g(a) \leq g(ab)$ for $b \in D$, $b \neq 0$.
 - (b) For all $a, b \in D$ with $g(a) > g(b)$ there is a q (quotient) and r (remainder) such that

$$a = qb + r$$

with $g(r) < g(b)$ or $r = 0$. This is, for integers, the division algorithm.

□

Integers and polynomials form a Euclidean domain, where the metric for integers is simply the absolute value, and for polynomials it is the degree of the polynomial.

Before we get to Euclid's algorithm, we need one more fact about GCDs: For any integer x , $(a, b) = (b, a) = (a, -b) = (a, b + ax)$.

Euclid's algorithm finds the greatest common divisor of a pair elements in a Euclidean domain.

The Euclidean algorithm works by repeated division.

Example 1 Let $a = 168$ and $b = 166$, and find $(168, 166)$. We have

$$168 = 1 \cdot 166 + 2.$$

Divide again:

$$166 = 2 \cdot 83 + 0$$

Take the **last nonzero remainder**: $(168, 166) = 2$.

□

Example 2 Find $(336, 54)$. Divide:

$$336 = 54 \cdot 6 + 12$$

$$54 = 12 \cdot 4 + 6$$

$$12 = 6 \cdot 2 + 0$$

Take the last nonzero remainder: $(336, 54) = 6$.

□

This can be coded in nothing at all in MATLAB:

Algorithm 1 GCD program 1

```
function g = gcdint1(b,c)
% function g = gcdint1(b,c)
% Compute (only) the GCD (a,b) using the Euclidean algorithm
while(c)
  g = c;
  c = rem(b,c);
  b = g;
end
```

We can do more, however. It is a fact of number theory that

$$(a, b) = ax + by$$

for some integers x and y . We can use the Euclidean algorithm to determine x and y . In many of our applications, these will be the numbers that we need. (Another useful fact: if there is an x and y such that $ax + by = 1$, then $(a, b) = 1$.)

Example 3 Determine $(851, 966)$. By the division algorithm we can write

$$966 = 1 \cdot 851 + 115.$$

By the property stated above, we have

$$(966, 851) = (851, 966 - 1 \cdot 851) = (851, 115).$$

Thus the GCD problem has been reduced. Applying the division algorithm again we can write

$$851 = 7 \cdot 115 + 46$$

hence

$$(851, 115) = (115, 851 - 7 \cdot 115) = (115, 46).$$

Proceeding by application of the division algorithm and the property, we obtain successively

$$\begin{aligned} 115 &= 2 \cdot 46 + 23 \\ (115, 46) &= (46, 23) \\ 46 &= 2 \cdot 23 \\ (46, 23) &= 23. \end{aligned}$$

Chaining together the equalities we obtain

$$(966, 851) = 23.$$

We can find the x and y in the representation $(966, 851) = 966x + 851y$ by working the equations backwards:

$$\begin{aligned} 23 &= 115 - 2 \cdot 46 \\ &= 115 - 2 \cdot (851 - 7 \cdot 115) = -2 \cdot 851 + 15 \cdot 115 \\ &= -2 \cdot 851 + 15(966 - 1 \cdot 851) = 15 \cdot 966 - 17 \cdot 851, \end{aligned}$$

so $x = 15$ and $y = -17$. □

More formally, the algorithm may be stated in the following theorem, which also fixes some useful notation.

Theorem 1 (*The Euclidean algorithm*) Let b and c be integers > 0 . Then by repeated application of the division algorithm write

$$\begin{aligned} b &= cq_1 + r_1 & 0 < r_1 < c \\ c &= r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 &= r_2q_3 + r_3 & 0 < r_3 < r_2 \\ &\vdots \\ r_{j-2} &= r_{j-1}q_j + r_j & 0 < r_j < r_{j-1} \\ r_{j-1} &= r_jq_{j+1} + 0. \end{aligned}$$

Then $(b, c) = r_j$, the last nonzero remainder of the division process.

That the theorem stops after a finite number of steps follows since every remainder must be less than the preceding remainder.

If the GCD g and the coefficients x and y are desired such that

$$bx + cy = g,$$

a little more work is required. Observe that the recursion in the Euclidean algorithm may be expressed as

$$\begin{aligned} q_i &= \lfloor r_{i-2}/r_{i-1} \rfloor \\ r_i &= r_{i-2} - r_{i-1}q_i \end{aligned} \tag{1}$$

for $i = 1, 2, \dots$ (until termination) with $r_{-1} = b$ and $r_0 = c$. The values for x and y may be obtained by finding intermediate integers x_i and y_i satisfying

$$bx_i + cy_i = r_i$$

In conjunction with (1) we obtain

$$\begin{aligned} x_i &= x_{i-2} - q_i x_{i-1} \\ y_i &= y_{i-2} - q_i y_{i-1} \end{aligned} \tag{2}$$

for $i = 1, 2, \dots$ (until termination) with

$$\begin{aligned} x_{-1} &= 1 & x_0 &= 0 \\ y_{-1} &= 0 & y_0 &= 1 \end{aligned}$$

This algorithm applies as well to polynomials (over a field) as to integers. The following implementation is for polynomials.

Algorithm 2 GCD program 2 – polynomials

```
function [g,s,t] = gcdpoly(b,c,thresh)
% function [g,s,t] = gcdpoly(b,c)
% Compute the GCD g = (b,c) using the Euclidean algorithm
% and return s,t such that bs+ct = g, where b and c are polynomials
% with real coefficients
%
% thresh = (optional) threshold argument used to truncate small remainders

rm2 = b; rm1 = c;
sm2 = 1; sm1 = 0;
tm2 = 0; tm1 = 1;
while(any(rm1))
```

```

[q,tr] = polydiv(rm2,rm1);
if(nargin==3) tr(find(abs(tr) < thresh)) = 0; end; % truncate small
ts = polysub(sm2,polymult(q,sm1));
tt = polysub(tm2,polymult(q,tm1));
rm2 = rm1; sm2 = sm1; tm2 = tm1;
rm1 = tr; sm1 = ts; tm1 = tt;
end
lc = rm2(1); % make monic
g = rm2/lc;
s = sm2/lc;
t = tm2/lc;

```

As an example, we can try

```

>> [g,x,y] = gcdpoly([4 10 8 2],[8 14 7 1])
g =
    1.0000    1.5000    0.5000
x =
    0.3333
y =
   -0.1667

```

2 Minimal polynomials and conjugate elements

We begin with a reminder from polynomials over real. Suppose we are given a number $x_1 = (2+3j)$. Over the (extension) field \mathbb{C} , there is a polynomial $x - (2+3j)$ which has x_1 as a root. But suppose we are asked to find the polynomial of *smallest* degree with *real* coefficients that has x_1 as a root. We are well acquainted with the fact that the roots of real polynomials come in complex conjugate pairs, so we conclude immediately that there a real polynomial with root x_1 must also have a root $x_2 = (2 - 3j)$. We say that x_2 is a *conjugate* root to x_1 . A polynomial of *smallest degree* having these roots is

$$(x - (2 + 3j))(x - (2 - 3j)) = x^2 - 4x + 13.$$

We will apply the ideas of conjugate roots and polynomials having specified roots with coefficients in a given field now to finite fields.

Definition 2 Let $\alpha \in GF(q^m)$. The **minimal polynomial** of α with respect to $GF(q)$ is the smallest-degree nonzero polynomial $p(x) \in GF(q)[x]$ such that $p(\alpha) = 0$. \square

In our previous example, the polynomial we found would be a minimal polynomial for $2 + 3j$.

Some properties for minimal polynomials:

Theorem 2 For each $\alpha \in GF(q^m)$ there exists a unique monic polynomial $p(x)$ of minimal degree in $GF(q)[x]$ such that:

1. $p(\alpha) = 0$.
2. The degree of $p(x) \leq m$.
3. $f(\alpha) = 0$ means that $p(x) | f(x)$.
4. $p(x)$ is irreducible in $GF(q)[x]$.

Proof Write down the $(m + 1)$ elements $1, \alpha, \alpha^2, \dots, \alpha^m$ which are elements of $GF(q^m)$. Since $GF(q^m)$ is a vector space of dimension m over $GF(q)$, these $m + 1$ elements must be linearly dependent. Hence there exist coefficients such that

$$a_0 + a_1\alpha + \dots + a_m\alpha^m = 0;$$

these are the coefficients of the polynomial $p(x)$ which has α as the root.

To show uniqueness, suppose there are two minimal monic polynomials of α ; call them $f(x)$ and $g(x)$. These must both have the same degree. Then there must be a polynomial $r(x)$ such that

$$f(x) = g(x) + r(x),$$

where $\deg(r(x)) < \deg(f(x))$. Since α is a root, we get

$$0 = f(\alpha) = g(\alpha) + r(\alpha)$$

so that $r(\alpha) = 0$, which contradicts the minimality definition.

If there is an $f(x)$ s.t. $f(\alpha) = 0$, we write using the division algorithm

$$f(x) = p(x)q(r) + r(x)$$

where $\deg(r) < \deg(p)$. But then $r(\alpha) = 0$; again a contradiction of the minimality.

If $p(x)$ factors, so $p = fg$, then either $f(\alpha) = 0$ or $g(\alpha) = 0$, again a contradiction to the minimality. \square

We observe that: primitive polynomials are the minimal polynomials for primitive elements in a GF.

Definition 3 Let $\beta \in GF(q^m)$. The **conjugates** of β with respect to a subfield $GF(q)$ are $\beta, \beta^q, \beta^{q^2}, \beta^{q^3}, \dots$. \square

The conjugates of β with respect to $GF(q)$ form a set called the **conjugacy class** of β w.r.t. $GF(q)$.

Theorem 3 The conjugacy class of $\alpha \in GF(q^m)$ w.r.t. $GF(q)$ contains d elements, where

$$\alpha^{q^d} = \alpha.$$

Proof The elements

$$\alpha, \alpha^q, \alpha^{q^2}, \dots$$

has only a finite number of elements in it. The first number to repeat must be α . Otherwise, there is a number s such that

$$\alpha^{q^d} = \alpha^{q^s}$$

for some $s < d$. This means that

$$\alpha^{q^d - q^s} = 1.$$

But (by a previous result) we must have

$$\text{ord}(\alpha) | q^d - q^s = q^s(q^{d-s} - 1).$$

Recall that $\text{ord}(\alpha) | q^m - 1$. Since q^s is a power of prime (no factors in common with $q^{d-s} - 1$), we must have

$$\text{ord}(\alpha) | q^{(d-s)} - 1$$

so that $\alpha^{q^{(d-s)}} = \alpha$. \square

Example 4

1. In $GF(2^3)$, the conjugacy classes of α are

$$\beta = \alpha, \alpha^2, (\alpha^2)^2 = \alpha^4, (\alpha^2)^3 = \alpha$$

$$\beta = \alpha^3, (\alpha^3)^2 = \alpha^6, (\alpha^3)^{2^2} = \alpha^{12} = \alpha^5.$$

Note that each conjugacy class has the same number of elements in it, and that the number of elements divides m .

2. Let $\alpha \in GF(16)$ be an element such that $\text{ord}(\alpha) = 3$. (Check for consistency: since $3|15$, there are $\phi(3) = 2$ elements of order 3 in $GF(16)$.) The conjugacy class of α is

$$\alpha, \alpha^2, \alpha^{2^2} = \alpha^4 = \alpha.$$

So there are 2 elements in this conjugacy class.

□

Theorem 4 Let $\alpha \in GF(q^m)$, and let $p(x)$ be the minimal polynomial of α . The roots of $p(x)$ are exactly the conjugates of α w.r.t. $GF(q)$.

In other words, the minimal polynomial does just what we want it to, and the conjugates of α can be interpreted as we expect. Before proving this, we make the following observation:

$$(\alpha_1 + \alpha_2 + \cdots + \alpha_t)^{p^r} = \alpha_1^{p^r} + \alpha_2^{p^r} + \cdots + \alpha_t^{p^r}$$

for $r = 1, 2, 3, \dots$. In other words, we don't need to worry about the cross terms. Prove using two terms; recall that $p \mid \binom{p}{k}$. Also use

$$(\alpha + \beta)^{p^2} = ((\alpha + \beta)^p)^p = (\alpha^p + \beta^p)^p = (\alpha^{p^2} + \beta^{p^2})$$

Proof If $p(\alpha) = 0$, then, using the observation just made,

$$0 = (p(\alpha))^q = p(\alpha^q)$$

so α^q is a root of $p(x)$. Similarly

$$0 = (p(\alpha))^{q^r} = p(\alpha^{q^r})$$

The remaining step is to show that the polynomial with the conjugates of α as its roots has its coefficients in $GF(q)$. Let $f_\alpha(x)$ be this polynomial:

$$f_\alpha(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{d-1}}) = x^d + A_{d-1}x^{d-1} + \cdots + A_1x + A_0.$$

Then

$$(f_\alpha(x))^q = x^{qd} + A_{d-1}^q x^{q(d-1)} + \cdots + A_1^q x^q + A_0^q = f_\alpha(x^q).$$

(Start in product form; rearrange using uniqueness.) We therefore get

$$A_i = A_i^q$$

for $i = 0, 1, \dots, d-1$. Since every coefficient satisfies this, every coefficient is in $GF(q)$ (see thm 2-16). □

Lemma 5 All the roots of an irreducible polynomial have the same order.

Proof Let $p(x) \in GF(q)[x]$. By a previous result, the orders of the roots divide $q^m - 1$. Since the coefficients of $p(x)$ are in $GF(q)$, the roots must be conjugates, and are of the form $\{\beta, \beta^q, \beta^{q^2}, \dots\}$. We must have $q = p^u$ for some u . Thus q and its powers are relatively prime to $(q^m - 1)$ and all divisors of $q^m - 1$. We note that

$$\text{ord}(\beta^{q^k}) = \frac{\text{ord}(\beta)}{(q^k, \text{ord}(\beta))} = \text{ord}(\beta).$$

Since this is true for any k , root has the same order. \square

Example 5 Using the conjugacy classes we found before in $GF(8)$, we can write down the minimal polynomials:

$$\begin{array}{ll} \{0\} & x \\ \{1\} & x + 1 \\ \{\alpha, \alpha^2, \alpha^4\} & (x - \alpha)(x - \alpha^2)(x - \alpha^4) = x^3 + x + 1 \\ \{\alpha^3, \alpha^6, \alpha^5\} & x^3 + x^2 + 1. \end{array}$$

\square

3 Factoring $x^n - 1$

Recall that every element $\beta \in GF(q^m)$ has an order that divides $q^m - 1$; thus every element is a root of $x^{q^m - 1} - 1$. Put another way, the elements of $GF(q^m)$ are the $(q^m - 1)$ st roots of unity, and these are all the nonzero elements of the field.

Given a field, we divide it into conjugacy classes, taking the minimal polynomial from each. Then based on our observation, we must have $x^{q^m - 1}$ as a product of the minimal polynomials of the nonzero elements.

Example 6

$$x^7 - 1 = (x + 1)(x^3 + x + 1)(x^3 + x^2 + 1).$$

\square

We can now pursue a more general problem, roots of $x^n - 1$ for other values of n . These n roots of unity must exist in some field. We find the field, then find the minimal polynomials of the conjugacy classes in the field.

Suppose we have an element β of order n in some field $GF(p^m)$. Then β is a root of $x^n - 1$ in that field, and so are the elements $\beta^2, \beta^3, \dots, \beta^{n-1}$. We can find such a β if we form the field correctly.

Before doing so, it is interesting to pause a moment and suggest an application of this. Consider the DFT:

$$X[k] = \sum_{n=0}^{N-1} x[n] e^{-j2\pi nk/N}.$$

Note that the number $e^{-j2\pi/N}$ is an N th root of unity. We can define a Fourier transform in a finite field $GF(p^m)$ of length N , provided that we can find a field in which N th roots of unity exist.

Recall that if $n|p^m - 1$, then there are $\phi(n)$ elements of order n in $GF(p^m)$.

Definition 4 The smallest positive integer m such that $n|q^m - 1$ is called the **order of q modulo n** . \square

If m is the order of q modulo n , then $GF(q^m)$ is the smallest extension field of $GF(q)$ in which n th roots of unity exist.

Example 7 We are looking for an extension of $GF(2)$ in which 5th roots of unity exist:

$$\begin{aligned} 5 \nmid (2-1) \\ 5 \nmid (2^2-1) \\ 5 \nmid (2^3-1) \\ 5 \mid (2^4-1) = 15 \end{aligned}$$

So in $GF(16)$ there are primitive fifth roots of unity.

In $GF(16)$, let α be primitive; it has order 15. Then $\beta = \alpha^3$ has order 5, as needed. The conjugacy class for β is

We want 13th roots of unity in an extension of $GF(3)$. Note that

$$13 \mid 3^3 - 1$$

so they live in $GF(3^3)$. □

Example 8 We want to find a field $GF(2^m)$ which has 25th roots of unity. We need

$$25 \mid (2^m - 1)$$

For $m = 20$ this works. Now let us divide the roots of $2^{25} - 1$ into conjugacy classes. Let β be a primitive 25th root of unity.

$$\begin{aligned} & \{1\} \\ & \{\beta, \beta^2, \beta^4, \beta^8, \beta^{16}, \beta^7, \beta^{14}, \beta^3, \beta^6, \beta^{12}, \beta^{24}, \beta^{23}, \beta^{21}, \beta^{17}, \beta^9, \beta^{18}, \beta^{11}, \beta^{22}, \beta^{19}, \beta^{13}\} \\ & \{\beta^5, \beta^{10}, \beta^{20}, \beta^{15}\} \end{aligned}$$

So

$$x^{25} - 1 = p_1(x)p_4(x)p_{20}(x)$$

(where the subscript represents the degree). □

Example 9 Let us find a field $GF(7^m)$ in which $x^{15} - 1$ has roots. We need to find m such that

$$15 \mid 7^m - 1$$

$m = 4$ works. Let γ be a primitive 15th root of unity in $GF(7^4)$. The conjugacy classes with respect to $GF(4)$ of the roots of unity are:

$$\begin{aligned} & \{1\} \\ & \{\gamma, \gamma^7, \gamma^{49} = \gamma^4, \gamma^{7^3} = \gamma^{13}\} \\ & \{\gamma^2, \gamma^{14}, \gamma^8, \gamma^{11}\} \\ & \{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\} \\ & \{\gamma^5\} \\ & \{\gamma^{10}\} \end{aligned}$$

Thus $x^{15} - 1$ factors into six irreducible polynomials in $GF(7)$. □

If we list the exponents of the primitive roots of unity, we get what are called the *cyclotomic cosets*. For example, for the last example we have the following:

Conjugacy class	↔	Cyclotomic cosets
$\{1\}$	↔	$\{0\}$
$\{\gamma, \gamma^7, \gamma^4, \gamma^{13}\}$	↔	$\{1, 7, 4, 13\}$
$\{\gamma^2, \gamma^{14}, \gamma^8, \gamma^{11}\}$	↔	$\{2, 14, 8, 11\}$
$\{\gamma^3, \gamma^6, \gamma^{12}, \gamma^9\}$	↔	$\{3, 6, 12, 9\}$
$\{\gamma^5\}$	↔	$\{5\}$
$\{\gamma^{10}\}$	↔	$\{10\}$

The cyclotomic cosets modulo n with respect to $GF(q)$ contain the *exponents* of the n distinct powers of a primitive n th root of unity with respect to $GF(q)$, each coset corresponding to a conjugacy class. These cosets provide a shorthand representation for the conjugacy class.

4 Ideals in $GF(q)[x]/(x^n - 1)$

Review: we have seen that we can define a ring by operations on integers modulo an integer, e.g. $(\mathbb{Z}_6, +, \cdot)$. If the modulo number m is prime, we get a field. We can also do operations on *polynomials* modulo another polynomial. For example, the ring of polynomials $GF(q)[x]$ can be reduced modulo another polynomial $f(x)$. Notationally, we write $GF(q)[x]/f(x)$. If $f(x)$ is irreducible, then $GF(q)[x]/f(x)$ is a field; these are the Galois fields we have already seen. When $f(x)$ is reducible, then $GF(q)[x]/f(x)$ is a ring. A particular ring that will be of some importance to us is the ring

$$GF(q)[x]/(x^n - 1).$$

Example 10 Consider $GF(2)[x]/(x^3 + 1)$. The original ring $GF(2)[x]$ contains all polynomials with coefficients in $GF(2)$. When reduced modulo $x^3 + 1$, they divide into equivalence classes.

$$\begin{aligned} &\{0, x^3 + 1, x^4 + x, x^5 + x^2, x^6 + 1, \dots\} \\ &\{1, x^3, x^4 + x + 1, x^5 + x^x + 1, x^6, \dots\} \\ &\{x, x^3 + x + 1, x^4, x^5 + x^x + x, x^6 + 1 + x, \dots\} \\ &\{x^2, x^3 + x^2 + 1, x^4 + x^2 + x, x^5, x^6 + x^2 + 1, \dots\} \\ &\{x^2 + 1, x^3 + x^2, x^4 + x^x + x + 1, x^5 + 1, x^6 + x^2, \dots\} \\ &\{x^2 + x, x^3 + x^2 + x + 1, x^4 + x^2, x^5 + x, x^6 + x^2 + x, \dots\} \\ &\{x^2 + x + 1, x^3 + x^2 + x, x^4 + x^2 + 1, x^5 + x + 1, x^6 + x^2 + x, \dots\} \end{aligned}$$

There are thus 8 equivalence classes, which we can label by the smallest-degree element of each class (e.g., the first element listed above). □

We will denote $R_n = GF(2)[x]/(x^n + 1)$.

We now introduce a new algebraic concept.

Definition 5 Let R be a ring. A nonempty subset $I \subset R$ is an **ideal** if it satisfies the following:

1. I forms a group under addition.
2. For any $a \in I$ and any $r \in R$,

$$ar \in I.$$

In other words, elements outside the ideal fall back into the ideal under the multiplicative operation. □

Example 11 For any ring R , there are at least the two trivial ideals $\{0\}$ and R .

The set $I = \{0, x^4 + x^3 + x^2 + x + 1\}$ forms an ideal in R_5 . For example, take the element $x^4 + x + 1 \in R_5$. Then

$$(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1) = (x^8 + x^7 + x^6 + x^4 + 1) \equiv 0 \pmod{x^4 + x^3 + x^2 + x + 1} \in I$$

□

Definition 6 An ideal I in a ring R is said to be **principal** if there is a $g \in I$ such that every element $c \in I$ can be expressed as the product mg for some $m \in R$. The element g is said to be the **generator element** for the principle ideal, and the ideal generated by g is denoted $\langle g \rangle$. \square

Here's the lowdown for the rest of the course: **the codes we will be studying are ideals in a ring**. Since ideals will be so important to us, let us examine some properties of ideals.

Theorem 6 Let I be an ideal in $GF(q)[x]/(x^n - 1)$. Then

1. There is a unique monic polynomial $g(x) \in I$ of minimal degree.
2. I is principal with generator $g(x)$
3. $g(x)|(x^n - 1)$ in $GF(q)[x]$.

The latter fact accounts for our interest earlier in factors of $x^n - 1$.

Proof The ideal is not empty (since the entire ring is an ideal), and there is a lower bound on the degrees of polynomials. Hence there must be at least one polynomial in the ring of minimal degree, which may be normalized to be monic. Now to show uniqueness, let $g(x)$ and $f(x)$ be monic polynomials in I of minimal degree with $f \neq g$. Then $h(x) = g(x) - f(x)$ must be in I since I forms a group under addition, and $h(x)$ must be of lower degree, contradicting the minimality of the degree of g and f .

To show that I is principal, we assume (to the contrary) that there is an $f(x) \in I$ that is not a multiple of $g(x)$. Then by the division algorithm

$$f(x) = m(x)g(x) + r(x)$$

with $\deg(r) < \deg(g)$. But $m(x)g(x) \in I$ (definition of a ideal) and $r = f - mg \in I$ (definition of ideal), contradicting the minimality of the degree of g , unless $r = 0$.

To show that $g(x)|(x^n - 1)$, we assume to the contrary that $g(x) \nmid (x^n - 1)$. By the division algorithm

$$x^n - 1 = h(x)g(x) + r(x)$$

with $0 \leq \deg(r) < \deg(g)$. But $h(x)g(x) \in I$, and $r(x) = (x^n - 1) - h(x)g(x)$ is the additive inverse of $r(x) \in I$, and so is in I , contradicting the minimality of the degree of g . \square

When we deal with codes, we will pick a code length n , then find a generator g dividing $x^n + 1$ which will be our generator polynomial. All of our codewords will be multiples of $g(x)$.