Welcome back

We are all in this together and we will get through this together.

- Use a laptop or desktop with a large screen so you can read these words clearly.
- To conserve bandwidth, please turn off your camera.
- Please mute your microphone unless I call on you.
- Please have the chat window open to ask questions.
- Reading for today: 7.7, 8.1–8.2; for Wed: 8.3–8.4.
- PS08 due today; PS09 outline Wed, completed due Mon Apr 20. (But deadlines are elastic.)
- Exam 2 (tentatively) on Wed Apr 22; done on paper, submitted by Canvas, proctored by Zoom. (Exam submission rehearsal: Last 5 min of class today.)
- Today's DJ: Kyle.

Q: Would you rather have more weight on HW?
Compare: 25% HW, 20% Ex 1, 25% Ex 2, 30% Fin
vs. 35% HW, 20% Ex 1, 20% Ex 2, 25% Final

Every finite field has a primitive elt, case $\mathbf{F}_{11} = \mathbf{Z}/(11)$

Last: Found that 2 is a primitive element in $\mathbf{F}_{11}$.

Now: find the orders of all elements of $F_{11}^{\times}$.

$\#F_{11}^{\times} = \{1, 2^1, 2^2, \ldots, 2^9\}$

2^k	order	$2^{k'}$	order
$2^0 = 1$	1	$10 = 2^5$	2
2^1	10	$9 = 2^6$	5
$4 = 2^2$	5	$7 = 2^7$	10
$8 = 2^3$	10	$3 = 2^8$	5
$5 = 2^4$	5	$6 = 2^9$	10

If $n = \text{order}(\alpha)$

$\text{order}(\alpha^k) = \frac{n}{\gcd(n,k)}$

So if gcd (10,k)=1, order is 10.

If gcd(10,k)=2, order 5

$\text{order}(2) = 10$, ie $2^{10} = 1$ in F_{11},

$2^i \neq 1$ for $0 < i < 10$

Fact says $\text{order}(2^4) = \frac{10}{\gcd(4,10)} = 5$

$(2^4)^1 = 2^4 \neq 1$
$(2^4)^2 = 2^8 \neq 1$
} b/c order(2) = 10

wraparound

$(2^4)^3 = 2^{12} = 2^2 2^{10} = 2^2 \cdot 1 = 2^2 \neq 1$

$(2^4)^4 = 2^2 \cdot 2^4 = 2^6 \neq 1$

$(2^4)^5 = 2^6 \cdot 2^4 = 2^{10} = 1$ ✓

So 5 is the smallest power of 2^4 that gives you 1 (mod 11), which means that the order of 2^4 is 5 (in $\mathbb{F}_{11}^{\times}$).

Recall: Fact about finite fields is that if finite field has order q, multiplicative group (group of nonzero elements under multiplication) has order q-1.
Another fact about that: Order of any element of mult group must divide q-1.

For F_11, q-1=10. So every element of mult group must have order dividing 10: either 1, 2, 5, or 10.

We saw $2^1 \neq 1 \pmod{11}$

$2^2 \neq 1$

$2^5 \neq 1$

So order of 2 is not 1, 2, or 5, so it must be 10, and 2 is primitive.

(More brute force method: calc 2^1, 2^2, 2^3, ..., 2^9, see that all not equal to 1 (mod 11), but 2^10 = 1 (mod 11), so order is 10.)

The magic polynomial

Corollary

Let F be a field of order q. Then every α in F is a root of the polynomial $x^q - x \in F[x]$, and consequently,

$$x^q - x = \prod_{\alpha \in F} (x - \alpha). \tag{1}$$

Example: For $\mathbf{F}_{11} = \mathbf{Z}/(11)$, this means:

$$(x)(x-1)(x-2)\cdots(x-10) = x^{11} - x \pmod{11}$$

Proof: (Assuming previously stated facts about orders)

We saw that every nonzero element of F has order dividing q-1, say order n, where q-1=nd.
So if alpha is an elt of F, (alpha)^(q-1) = (alpha)^(nd) = ((alpha)^n)^d = 1^d = 1.

So $\alpha^{q-1} = 1 \Rightarrow \alpha^{q-1} - 1 = 0$ for all $\alpha \neq 0$ in F.

So α is a root of $x^{q-1} - 1 = 0$ for $\alpha \neq 0$.

$\Rightarrow$ All $\alpha \in F$, incl $\alpha = 0$, roots of

$$x(x^{q-1} - 1) = x^q - x.$$

α root of $x^q - x \Rightarrow (x - \alpha)$ divides $x^q - x$

The Factor Theorem from HS algebra!
(Generalized to polynomials over arbitrary fields.)

So $x^q - x$ factors as:

$$x^q - x = \prod_{\alpha \in F} (x - \alpha)$$

Details: We showed that RHS divides LHS, and degrees match and leading coefficient is 1, so RHS = LHS.

Deeper stuff about finite fields

You just have to know these facts; don't worry about their proofs:

Theorem All finite fields can be constructed as "mod (m(x))"

Let F be a finite field of characteristic p. Then F is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x) \in \mathbf{F}_p[x]$.

Theorem There exists a unique finite field of order p^e.

Let p be a prime, and let e be a positive integer.

1. *There exists at least one field of order p^e.*
2. *If F and K are both finite fields of order p^e, then F and K are isomorphic.*

We won't use this notation, but common in outside world (esp. in engineering).

Definition

Since any two fields of order p^e are isomorphic, algebraically we can think of them as being the same. For $q = p^e$ (p prime, $e \geq 1$), we may therefore define $\mathbf{F}_q$ to be "the" field of order q. This field is also sometimes known as the **Galois field of order** q, or $GF(q)$ for short.

Recap: Five Facts For Finite Fields

1. The characteristic of a finite field must be a prime p, and its order must be $q = p^e$ for some $e \geq 1$.
2. Every finite field has a primitive element.
3. If F is a field of order q, then every $\alpha \in F$ is a root of $x^q - x$, or in other words, $\alpha^q = \alpha$ for every $\alpha \in F$. Consequently, $x^q - x$ factors as the product of all $(x - \beta)$, where β runs over all elements of F (including $0 \in F$).
4. Every finite field of characteristic p is isomorphic to $\mathbf{F}_p[x]/(m(x))$ for some irreducible polynomial $m(x)$.

If deg(m(x))=e, order(F) = p^e.

5. For any prime p and $q = p^e$ $(e \geq 1)$, there exists a field $\mathbf{F}_q$ of order q that is unique up to isomorphism.

7.7: Worked examples

think of m(x) as modulus

Let $m(x) = x^4 + x^3 + 1$, an irreducible polynomial in $\mathbf{F}_2[x]$. We define $\mathbf{F}_{16}$ to be $\mathbf{F}_2[x]/(m(x))$, and we let β be a root of $m(x)$ in $\mathbf{F}_{16}$. (Or: "$\mathbf{F}_{16} = \mathbf{F}_2[\beta]$, where β is a root of $m(x)$.")

Elements of $\mathbf{F}_{16}$ are polynomials in β of degree ≤ 3 b/c deg $m(x) = 4$

Inverse of a random element of $\mathbf{F}_{16}$:

To pick a poly of degree <= 3, pick 4 coefficients each of which is 0 or 1 so there are 2^4 = 16 elts of field.

$\gamma = \beta + 1$

To find inverse of gamma, solve w/ Euc reduction:

$f(x)(x+1) + g(x)m(x) = 1$

(Then, mod $m(x)$, $f(\beta)) \cdot (\beta + 1) = 1$.)

So find gcd $(x+1, m(x))$.

$$
\begin{array}{r|l}
 & x^3 \\
\hline
x+1 & x^4+x^3 \quad +1 \\
 & x^4+x^3 \\
\hline
 & 1
\end{array}
$$

gcd → 1

So $x^4+x^3+1 = x^3(x+1)+1$ (char 2, $+=-$)

So $\underbrace{(x^3)}_{f(x)}(x+1)+\underbrace{(1)}_{g(x)}\underbrace{(x^4+x^3+1)}_{m(x)}=1$

Mod $m(x)$: $\beta^3(\beta+1)=1$

$(\beta+1)^{-1}=\beta^3$

More about $\mathbf{F}_{16}$

q=16, so order of any elt of mult group divides 15.

$\mathbf{F}_{16} = \mathbf{F}_2[\beta]$, where β is a root of $m(x) = x^4 + x^3 + 1$.

What are the possible orders of elements of $\mathbf{F}_{16}^{\times}$? 1, 3, 5, 15

Is β primitive?

$\beta^4 = \beta^3 + 1$

$\beta^5 = \beta^4 + \beta$

$= \beta^3 + \beta + 1$

Remember: Represent as polys of degree <= 3.

$\beta^1 = \beta \neq 1$ ✓

$\beta^3 = \beta^3 \neq 1$ ✓

$\beta^5 = \beta^3 + \beta + 1 \neq 1$ ✓

B/c beta^1, beta^3, beta^3 are not equal to 1, order of beta can't be 1, 3, 5, so it must be 15. So beta is primitive.
(So if you calculate, 1, beta, beta^2, beta^14, using reduction rules, you get every nonzero polynomial of deg <=3 in beta.)

Interlude: Prepare for exam upload rehearsal

Please log into Canvas now and get two pieces of paper ready.

8.1: Better codes

Recall: A binary linear $[n, k, d]$ code $\mathcal{C}$ has:

- Length n (i.e., $\mathcal{C}$ is a subspace of $\mathbf{F}_2^n$)
- Dimension k (think: amt of info in a codeword)
- Minimum distance d

Also recall: $\mathcal{C}$ can correct $\left\lfloor \frac{d-1}{2} \right\rfloor$ errors. Leads to:

Motivating Problem: Find $[n, k, d]$ codes where both k and d are as large as possible, given n.

Compare repetition and parity check:

Solution: Ideals!

8.2: Cyclic codes

Generalizing binary linear codes:

Definition

Let $q = p^r$ be a prime power, and let $\mathbf{F}_q$ be the (unique) field of order q. A **linear code $\mathcal{C}$ of length n over $\mathbf{F}_q$** is a subspace $\mathcal{C}$ of $\mathbf{F}_q^n$. Elements (vectors) of a linear code are still called **codewords**.

Definition

Let $\mathcal{C}$ be linear code, length n over $\mathbf{F}_q$. To say $\mathcal{C}$ **cyclic** means $\mathcal{C}$ closed under cyclic permutation of coordinates. So when $\mathcal{C}$ cyclic,

$$\text{if } \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ \vdots \\ c_{n-1} \end{bmatrix} \in \mathcal{C}, \text{ then } \begin{bmatrix} c_{n-1} \\ c_0 \\ c_1 \\ \vdots \\ c_{n-2} \end{bmatrix} \in \mathcal{C}, \begin{bmatrix} c_{n-2} \\ c_{n-1} \\ c_0 \\ \vdots \\ c_{n-3} \end{bmatrix} \in \mathcal{C}, \ldots.$$

Cyclic codes as ideals

Notation

The **polynomial notation** for vectors in $\mathbf{F}_q^n$ represents the vector $\begin{bmatrix} c_0 \\ \vdots \\ c_{n-1} \end{bmatrix}$ as the polynomial

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \tag{2}$$

in the ring $R = \mathbf{F}_q[x]/(x^n - 1)$ (i.e., setting $x^n \equiv 1$).

Why polynomial notation? Well, if

$$c(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_{n-1} x^{n-1} \tag{3}$$

then

$$xc(x) =$$

So $x^2 c(x)$ corresponds to:

And $x^k c(x)$ corresponds to:

Cyclic codes are ideals

Theorem

Let $\mathcal{C}$ be a linear code of length n over $\mathbf{F}_q$. In polynomial notation, $\mathcal{C}$ is cyclic if and only if it is an ideal of the ring $\mathbf{F}_q[x]/(x^n - 1)$.

Proof: Suppose $\mathcal{C}$ is an ideal of $\mathbf{F}_q[x]/(x^n - 1)$.

Exam upload rehearsal

- Prepare: Please turn on your cameras (phone cameras are fine) so I can see your workspace.
- At 11:40: Please download the exam text to your laptop, either from the Canvas quiz or from your email.
- Please do the exam and scan your answers to a single PDF file.
- Please submit the exam by 11:45am.