MITOCW | 9ocw-6-451_4-261-02mar2005-220k_512kb-mp4

PROFESSOR: So if you want to hand in your problem sets, we have three handouts. The old problem set solutions, the new problem set, and we're also handing out chapter eight today. Of course, these are all on the web.

Reminders of previously announced events. Next week I'm going to be away. Ralf Koetter will be a much-improved substitute. He'll be talking about Reed-Solomon codes and Reed-Solomon decoding. He's one of the world experts on these things. He's a great lecturer. So you're really lucky, I believe. I will, of course, look at the video afterwards and see how he did, but I'm sure he'll do it better than I would have done it.

And midterm is in two weeks. That's just a reminder. When I come back, we'll have a Monday class to go over anything that Ralf may have missed, or really anything in the whole course up through chapter eight. You can bring questions in to that. I don't know how much I feel I'll need to embellish and cover, so I don't know how much time there will be for questions. But that can be a fairly free form lecture. And then Ashish is going to run a review session on the Tuesday with exactly the same purpose.

So hopefully that'll put you in good shape for the midterm. We have to make up the midterm. No idea what's going to be on the midterm yet.

OK. Any questions about these things? Homework processes going OK? Office hours? Solutions? Everything seems to be all right so far? Good.

We're in chapter seven. I certainly plan to complete it today. I'm not going to cover all of chapter seven, but the key elements that I want you to know. You're responsible only for what's covered in class, by the way.

We've talked about a lot of algebraic objects. Our main emphasis has been to get the finite field, and at this point, we have prime fields. Fields with a prime number p of elements. And we find that we can construct such a field by taking the integers mod p. You can write that as z mod p z. You can equally well consider this as the equivalence classes of integers of the cosets of pz nz which are each identified by a remainder or residue r between 0 and p minus 1.

OK. So basically, the elements of the field are these remainders or these cosets. There are p of them. We do arithmetic by simply doing mod p addition and multiplication. So if you understand arithmetic mod p, you understand this field. Yes?

AUDIENCE: Is Fp and Zp isomorphic?

PROFESSOR: As an additive group, it's isomorphic to Zp. Zp we use that notation for the group. We use this notation for the field. And I write Zp is isomorphic to Z mod pZ as a quotient group. Here I've added in the multiplication operation mod p to make this a field. So this is somewhat more than just a quotient group.

Sorry. The notation is supposed to be more suggestive than precise. This is not a math class. I hope it's helpful rather than otherwise.

OK. So today, we're going to construct all the rest of the finite fields. By the way, we showed that these are the only fields with a prime number of elements. Today we're going to construct fields with a prime power number of elements in a very analogous way, and it will turn out -- although I'm not going to prove this -- that these are the only finite fields. Well, these are generalization of this, so all finite fields have a prime power number of elements and are basically isomorphic to one of these fields.

How do we construct this field? To give you a preview, very analogously to the way we constructed this field. You'll see that the character of the arguments is very much the same. And that's because there is a great algebraic similarity between the integers and the polynomials over a field. And we'll talk about that in a second.

Basically, they're both countably infinite rings, or infinite rings. Countably infinite if it's over a finite field. And they both have analogous factorization properties. They're both unique factorization domains, would be one characterization, algebraically.

All right. How do we construct this field? We're basically going to construct it by taking the set of all polynomials over Fp which is denoted by Fp square brackets x. And we're going to take that mod the set of all polynomials that are divisible by G of x, or G of x times the set of all polynomials. The set of all multiples of G of x. Or more simply, just mod G of x. Where we're going to take G of x to be a prime polynomial. And I guess I have to add that the degree of G of x is going to be equal to m.

So we basically need to find a prime polynomial degree m. Then we take the set of all polynomials modulo this prime polynomial. They're going to be exactly p to the m residue classes, or equivalence classes, or remainders modulo g of x. And we'll use the arithmetic operations from mod G of x arithmetic, addition mod G of x, multiplication mod G of x, and we'll find that the resulting object has satisfied the axioms of the field. OK?

So that's where we're going. You with me?

OK. So let's talk about factorization. And I think it makes it easy to understand polynomials if we understand the analogies to the integers. In particular where I'm headed is unique factorization. Both the integers and the polynomials have unique factorizations. The integers into product of integers, and any polynomial is uniquely factorizable into a product of polynomials.

Now I wasn't quite precise when I said that. We have to be a little bit more precise when we talk about factorization. In particular, we have a certain kind of trivial factorization that involves units. Units, if you remember, are the invertible elements. We're in a ring, so not every element has an inverse, but some of them do. And in the integers, what were the invertible integers under multiplication? Everything here is about multiplication, you know? A ring is something that satisfies all of the properties of the field, except that some of the elements don't have inverses, so that division is not necessarily well-defined, even for non-zero elements.

OK? Sorry. I think I said that before. But we're not emphasizing that these are rings, although they are. That's an informal definition.

So in the integers, of course 12 doesn't have a multiplicative inverse, but it's an integer. But which integers do have multiplicative inverses? Plus or minus 1. So if an integer is divisible by n, it's also divisible by minus n. All right? Trivially. These are the only ones in the integers.

And last time we actually talked, if I remember correctly, about the units and the polynomials. Which polynomials have inverses? Excuse me. The degree 0. Thank you.

The degree 0 polynomials have inverses because they are basically the non-zero elements of the field. OK? It's slight abuse of notation. We identify the field elements with the degree zero polynomials. These are polynomials just of the form F of x equals F_0 a constant, where the constant is non-zero.

OK. So similarly, we will have to have representatives of equivalence classes with respect to the units. So if both plus or minus n divide something, what we take as the representative is we take the positive integers. When we talk about divisibility, we talk only about divisibility by positive integers or factorization by positive integers. It's trivial that if something is divisible by n, it's also divisible by minus n.

Similarly for polynomials, the representatives are taken as mnemonic polynomials. And this means that the highest order term, Fm is equal to 1.

So we can take any polynomial, and by multiplying it by one of these invertible elements, basically by a non-zero constant in the ground field, we can make the highest order term equal to 1. Right? So if a polynomial is divisible by F of x, it's also divisible by alpha F of x, where alpha is any non-zero field element, right? And so we may as well fix the highest order coefficient equal to 1.

Actually, for some purposes in the literature, like you've probably seen this in filter design, or we always make the lowest order coefficient equal to one. F0 equal to 1. You could also adopt that convention, and say that that's going to be a mnemonic polynomial. Here we'll focus on the high order coefficient, but you could do it either way.

And these both have the nice property that the product of positive integers is a positive integer. The product of monic polynomials is a monic polynomial, right? The highest order term of the product is going to have a highest order term equal to 1. Or if you chose the lowest order one, that would work, too. The lowest order term of the product would be equal to 1.

All right. So having recognized this, when we talk about unique factorization, just as with the integers, what we really mean is factorization of a positive integer into a product of positive integers. It's unique up to units. We can always put units either on the integer that we're factoring or on any of the factors, and we can freely multiply any of these things by units, and it won't affect the factorization.

Similarly over here, when we talk about unique factorization, we mean unique up to units. We're basically going to talk about the factorization of monic polynomials into a product of monic polynomials.

Not getting a real positive feeling that everybody's following me. Would it help if I wrote down more things, or wrote some examples?

In F2 of x, for instance, we have -- well, this isn't a very good example. Let's write R of x. OK?

We're going to talk about factorizations like this. x squared minus 1 equals x minus 1 times x plus 1. That's a factorization of a monic polynomial into a product of monic polynomials of a lower degree. Happens in F2 of x. Since there is only one non-zero field element, then all polynomials are monic, except for the 0 polynomial. The only non-zero term we have play with is one. So the highest order non-zero term is always 1.

All right. OK. So that's what we're going to mean by unique factorization. Now, there's one other qualifier. There's some trivial factors. We took some care to use the standard mathematical terminology in the notes, so if it says trivial devisors, then that's what I mean. What would the trivial divisors of integer n be?

1 and n are always going to divide in. And we're really not interested in those when we talk about factorization.

Similarly, over here, the trivial divisor of a polynomial F of x are 1 and F of x. We're not interested in those.

So when we talk about unique factorization, we mean up to units and nontrivial factors. And for the integers, that means that we're going to talk about divisors d, let's say, such that d is between 1 and n.

And for polynomials, what this means is we're not interested in degree 0 factors. The only factor of degree the same as F of x is going to be F of x up to units. We're interested in divisors d of x such that the degree that 0 is less than the degree of the divisor less than the degree of what it's dividing into. Sorry. I'm not defining everything, but I hope that's clear. We're just interested in factors that have degree less than the polynomial that we're factoring, but we're not interested in degree 0 factors.

So that's what's meant by unique factorization. It also shows you the analogy in general. In the case of integers, the key thing in a divisor is that it have magnitude between 1 and n. The key thing in a polynomial is it have degree between 0 and the degree of F of x.

Basically, we want to factor something into smaller things here. And when we say smaller, we talk about magnitude. Here when we say smaller, we're talking about degrees. In general, we go between these two things. The concept of magnitude is replaced by the concept of degree, to say how big something is.

In both of these, the key to all proofs is the Euclidean division algorithm. Suppose we want to see if n is a divisor of m. I've forgotten what I put in the notes. Then we go through division, and we find that m is equal to q, some quotient times n, plus a remainder r.

This is standard grade school division. But it's really the key in the universe in talking about these two domains. And this is what we've used, really, to prove everything about the factorization properties of integers.

And how would you actually prove that everything can be written this way? There's an important caveat. That the remainder we can always choose to have to be in the range from 0 less than r less than or equal to n minus 1. And the remainder is what we call m mod n.

We divide and we get a remainder that's one of these n things, and that's the main thing we get out of this division, is m mod n, which is equal to the remainder r. And there are precisely n remainders.

Now, how do you actually prove this? You prove this, if you want, very easily, just by recursion. You take m, and you ask, is it already in this range? If it is, you're done. m is the remainder and q is zero.

If not, then you subtract n from m, thereby reducing the magnitude of m. You can use the magnitude as an indicator of how far you've gotten in this process. You reduce the magnitude, and then you ask, is the result in this range? OK. If it's in that range, fine, you finish this and q is 1. Otherwise, you continue. And in the recursion, you're continually reducing the magnitude, and it's easy to show that eventually, the magnitude has to fall into this range and be one of these n remainder numbers, and then you're done. OK?

So it's a descending chain where the chain has a bottom at 0. If you start with a positive integer, you can't go below 0. And this is the only way it can come out. Very easy to prove that.

All right. Similarly in polynomials, we get an analogous expression. If we want to take F of x and see if G of x is a divisor, we take F of x, and we can always write this as some quotient times G of x plus some remainder. Where the important thing here about the remainder is that the degree of the remainder is less than the degree of G of x. And here the remainder is called F of x mod G of x. Just as the remainder here is called m mod n.

And there's a unique remainder. And again, how would you prove this? You could just take any long division algorithm that you know for dividing G of x into F of x. Basically long division amounts to taking F of x. You can always choose some scalar multiple of G of x such that F of x minus alpha G of x has degree less than F of x. So you pick the top term to reduce the degree, all right?

Let's take G of x to be monic. We're only interested in monic polynomials. If the top term of F of x is -- well, we're only going to divide it into monic polynomials. But as we go along, we may get non-monic ones. So you take the top term, whatever it is over here, f(m). You multiply f(m) times g of x. You subtract f(m) g of x from f of x. You reduce the degree. OK?

AUDIENCE: [INAUDIBLE PHRASE].

PROFESSOR: Correct. Thank you very much. You need also a term x to whatever the difference in degrees is here to move the degree up to the top. When we're actually doing long division, we write f(m) f(m minus 1) down to f(0). We divide g(n) down to g(1). And the first term, g(n) is going to be equal to 1. We take f(m) up here. We implicitly move it over to get f(m) dot dot dot dot, down to f(m) alpha. We subtract, and we're down to something that only has degree m minus 1. That's what polynomial long division is shorthand for. So you all know how to do this.

OK. Again, similar kind of proof, that you must be able to get a remainder in this range, and furthermore, the remainder is unique. You basically can go through this process. You reduce the degree by at least one every time. Therefore, degree must eventually be reduced to where it's less than degree g of x.

At that point, you can't continue this process. You're stuck. And that's your remainder. There's no way of taking something of lesser degree of g of x and then subtracting some multiple from g of x from it to still further reduce the degree.

All right. So similar proof. Uniqueness is pretty obvious. So you get a unique remainder of lesser degree than g of x. And so you can reduce any f of x to some remainder r of x, which is called f of x mod g of x.

And if we do arithmetic, the way we do arithmetic over here for addition is we just, if we want to add two remainders mod n, we take the sum of them, and then if necessary, reduce them mod n. Similarly with multiplication. If we want to multiply them, we take the product of two remainders, and if necessary, reduce them again to a legitimate remainder which is in this range or to mod n.

It's the same over here. If we want to add two remainders, that's easy enough. We can do that and we won't increase the degree, so we automatically get something when we add two remainders that satisfies this degree property. We don't have to reduce mod g of x.

If we multiply, you do have to check that when you multiply two remainders, then all you need to do is reduce the mod g of x. And basically, the assertion is that -- let's see. r of x, s of x -- it's hard to write this without being tautological. r of x, s of x. Reduced mod n, I'm sorry, mod g of x. I'm sorry. This is not worth writing. r of x, s of x, mod g of x. Something like that.

Bah. It's a total tautology. Forget it. Said correctly in the notes.

I'd rather think of it as residue classes. If we, say, we talk about this as a coset, f of x plus r of x, and we want to multiply any element. This coset times any element of the coset f of x plus s of x. Then the result is just multiplying out symbolically the polynomials times the polynomials are the polynomials. Any polynomial times a polynomial is a polynomial. Plus r of x f of x. We could get some multiple of r of x, some polynomial multiple. We could get some polynomial multiple of s of x. Plus r of x s of x.

But this is a polynomial that's included in here. We don't need to say that again. Similarly here. And so this is equal to f of x. It's equal to the coset f of x plus r of x s of x.

But this is another polynomial that probably has higher degree. This is equal to the coset f of x plus r of x s of x mod g of x.

OK. So this tells us that to multiply cosets, coset with representative r of x times the coset with representative s of x, we're going to get something in the coset whose representative is r of x, s of x mod g of x.

So this is a sketch of a proof that basically mod g of x commutes with multiplication. To multiply r of x times s of x. All right. So --

AUDIENCE: [INAUDIBLE PHRASE].

PROFESSOR: Yeah. You're quite correct. What I mean is the cosets of g of x of f of x. So I now understand all the blank looks. Are we better off now?

We have a group consisting of the set of all multiples of g of x, which I write as g of x times all the polynomials. The cosets of the group are precisely -- there's one remainder of degree less than g of x in every coset. So this is the representative of the coset. This is a sketch of a proof that multiplication basically just amounts to multiplying the remainders. The representative of the product coset is the product of the representatives modulo g of x. I think I said it correctly for once.

Please read the notes if you are still confused, as I can see some of you are.

Maybe it would help to do an example. Let's take g of x to be equal to x squared plus x plus 1 in f2 of x. It's a binary polynomial. Then r of x. The remainders are equal to 0,1. This was degree minus infinity, this is degree 0. They're x or x plus one. OK? These are the possible remainders when I take any polynomial modulo g of x. Divide it by g of x, and I'm going to get a polynomial in f2 of x of degree less than or equal to 1, and those are all of the polynomials that are decisively for degree less than or equal to 1. All right?

So what's the addition table? Addition is pretty easy. 0 plus anything is itself. 1 plus 1 in F2 is simply 0. 1 plus x is 1 plus x, sorry, x plus 1 as I've written. And 1 plus x plus 1 is x. x, x plus 1. x plus x is what? Hello? 0. Thank you. x plus x plus 1? Thank you. x plus 1, x. x plus x plus 1, 1, and 0.

So that's what the addition table looks like. Actually you could think of these as being just written as binary pairs, 0 0, 0 1, 1 0, 1 1, where this pair is basically F1

F0. And then the addition table is precisely the same as the addition table for these binary 2-tuples. You just add, component-wise, the lowest order coefficient, the F1 coefficient.

So addition is just like addition in F2 squared. Or z2 squared, if you like.

OK. That's actually an additive group. Check it out. It's not z4 by the way. The other abelian group, or the other group of size four, sometimes called the Klein four-group, but it's really just the addition table for the set of all binary [UNINTELLIGIBLE] two-tuples. OK?

Multiplication. One very nice thing about finite fields is you can simply -- sorry. This was supposed to be addition, this was supposed to be multiplication. You know can simply write out what all the rules are in a finite space.

OK. So what's 0 times anything? What's 1 times anything? Itself. 1 is the multiplicative identity. But you know. You could formally do this by doing polynomial multiplication.

All right. Here's an interesting one. What's x times x? Do x times x. What is that going to be equal to? x plus 1. How did you do that? We did the modulo. First of all, we write that that's x squared. But then we have to do x squared modulo g of x. x squared plus x plus 1.

So we have to go through a little long division process. We have to subtract this out from that. And that gives us x plus 1.

So that's the key rule. Whenever we see something of degree two or higher, we can always reduce it by subtracting out some multiple of g of x down to something of lower degree. Right? So this is what I've been talking about.

So x times x is x plus 1. What's x times x plus 1? Equals what? Good. You can do that in your heads. And what's x plus 1 times x plus 1? Remember, we're doing mod-2 arithmetic in our base field here. So this equals what? x squared plus 1. We reduce that, we get x.

OK. Let me check right now. Is this a field? These four elements with these rules for addition and multiplication. Does that form a field? What do I have to check, apart from formalities like the distributive law? Which follows from the distributive law for polynomials. That's always going to hold through mod x arithmetic.

What do I have to check? What are my field axioms? Anybody? Closure under multiplication. That's getting towards a very crisp statement of the -- I'm looking for two group axioms. One has to do with something we have to check for addition. Something has to do with something we have to check for multiplication. Inverses?

AUDIENCE: [INAUDIBLE PHRASE].

PROFESSOR: OK. Between the two of you I heard the two answers that I want. We have to check that this forms an abelian group under addition. So we have to check that the addition table is the addition table of an abelian group. And under multiplication, we have to check that the non-zero elements form a billion group. So just this part of the table has to form an abelian group, and both these have to have an identity, of course. But the identity in mod g of x arithmetic is always going to be 0 for addition and it's always going to be 1 for multiplication.

All right. So I check this. Is this a group table? Basically, I just have to check whether every row and column is a permutation of the elements. And it is. And 0 acts as 0 should act. Has the additive identity. All right?

Here what I have to check is that the nonzero elements, these three, form an abelian group under multiplication. Well, there really is only one group of size three. It is isomorphic to Z3. If I replace -- let's remember what Z3 looks like under addition. This looks like 0 1 2, 0 1 2, 0 1 2, 0 1 2. It's mod-3. 1 plus 1 is 2, 1 plus 2 is 3, which is 0, 1 plus 2 is 3, which is 0, 2 plus 2 equals 1.

So gee whiz. This is isomorphic to that if I relabel 1 by 0, x by 1, and x plus 1 by 2. That's the only thing it could be. The only group table in which every row and column is a permutation of every other. OK?

So we verified that we now have a finite field with four elements. Prime power number of elements. Right? The elements of my field are these four remainders, or you can think of them as representatives for their cosets, modulo g of x. The addition rule is addition modulo g of x, and the multiplication rule is multiplication modulo g of x. And it satisfies the field axioms, therefore, it's a finite field. All right? I can add, subtract. Addition and subtraction basically looks like addition and subtraction of binary two-tuples, just component-wise. Multiplication is a little bit more mysterious right now, but it works.

Let me tell you where we're going to go on multiplication. In this case, I can write x plus 1 in a different way. I note that x plus 1 is equal to x squared. All right?

So let me write a little log table over here for multiplication purposes. I'm going to write x -- I'm going to call that alpha. And x plus 1 is equal to x squared, or it's alpha squared. What's alpha cubed? Alpha cubed is x times this again. Let me look in the table. x times x plus 1 is equal to 1. So 1 equals alpha cubed. Or I could write that as alpha to 0. If I multiply by x again, I just cycle. So I'm going to get a cyclic group here.

And now I'm going to write the multiplication table as follows. I'm going to write the elements of the group as 1, alpha, alpha squared, 0, 1, alpha, alpha squared. Again, 0 times anything is 0. We never have to worry about that. 1, alpha, alpha squared. Alpha times alpha is alpha squared. Alpha times alpha squared is alpha cubed. But that's equal to 1. Same here.

Alpha squared times alpha squared -- what's that? Alpha to the fourth, but what does alpha fourth equal to if alpha cubed is equal to 1? This has to be equal to alpha.

Point is, because of this relationship here, I can always reduce the exponents modulo 3. I've basically got a little multiplicative cyclic group of order three that's, of course, isomorphic to the additive group, Z3.

So there are two ways I can do multiplication. One is, I can do it by this mod g of x way. I can represent things by these which basically stand for polynomials of degree one or less. And I can multiply two of these by simply going through standard polynomial multiplication over the appropriate field. And then I'll likely get some powers of x squared or higher, and I reduce those to modulo x squared plus x plus 1. That's legitimate and that gives me this statement.

Well, the other thing I can do is for multiplication, I can have a different representation. This is basically just a log table. OK? For each, I would have in my little computer a separate table where I'd write that this corresponds to 0, 0 1 corresponds to 1, 1 0 corresponds to alpha, and 1 1 corresponds to alpha squared.

Or of course, I would just represent these by their exponents that have some special value for 0. And then all I have to do is add exponents modulo 3 for multiplication. So log of x is 1, log of x plus 1 is 2, log of 1 is 0, and then I just use this for my multiplication operation, or equivalently this cyclic multiplicative group. Then I go through some inverse log operation to get back to the other representation, if I wanted to.

And in fact, in finite field arithmetic, this is what's typically done. There's just a little table lookup such that you can go back and forth between this representation, which we use for addition, and this representation, which we use for multiplication. Yeah?

AUDIENCE: [INAUDIBLE PHRASE].

PROFESSOR: You have to represent it as being special in some way. So if, in fact, literally, I made log x equal to 1, log x plus 1 equal to 2, log 1 equal to 0 -- one thing I suggest in the notes, you can make log 0 equal to minus infinity. That will always work. If you ever multiply by 0, you'll be adding minus infinity. The result will be minus infinity, so the inverse log is 0. So that's one way you can do it.

Or you could do what you do in ordinary real and complex arithmetic. You could just, say, have some special routine for multiplication by 0 is always 0. Division by 0 is illegal. Put out some error message.

All right? So that's how you actually build a little finite field computer for this finite field.

OK. Now, I chose this advisedly. Suppose I have chosen g of x equal to x squared plus 1. OK? I can do mod g of x arithmetic for x squared plus 1. Again, my four field elements are going to be the four binary polynomials of degree 1 or less. The addition table is going to be exactly the same.

So let's just write the multiplication table over here. 0, 1, x, x plus 1, 0, 1, x, x plus 1. 0 times anything is 0 in ordinary polynomial multiplication, and therefore also in mod g of x for any g of x. 1 times anything is itself. No problem there. x, x plus 1.

So we again have to give a little bit care to x squared. What's that going to be equal to? 1. And x times x plus 1 is equal to what? x squared plus x is equal to what? Looks like there's a problem. x plus 1 times x squared x plus 1 is equal to x squared plus 1, what's that equal? 0. Yuck. Didn't work.

What's the essential problem here? Yeah. This clearly is not a group. It's not even closed under multiplication. Because x plus 1 times x plus 1 is equal to 0. The essential problem is that there are two polynomials of degree less than two whose product is x squared plus 1. In other words, this is factorizable. OK? In F2 of x.

All right? So whereas x squared plus x plus 1. Does that have any factors of degree 1 or less? Any nontrivial factors of degree 1 or less? Well, basically we proved that it didn't, when we wrote this multiplication table. We tried all products of degree 1 or less polynomials where they're both non-zero, and we never got 0.

So this will work if and only if g of x is irreducible, has no nontrivial factors, is a prime polynomial. These are all equivalent in F2 of x. There's this distinction in other fields that irreducible just means has no nontrivial factors. Prime means there's a monic polynomial with no non-trivial factors.

So that's what I said back here. That the way we're ultimately going to have to construct finite fields is take the polynomials in Fp, Fp of x -- we've been looking at F2 of x -- modulo a prime polynomial g of x. So what we're going to need to find is prime polynomials.

Let's see. Can I already prove that this is going to work for any prime polynomial? So I'm going to force the g of x to be equal to a prime polynomial in Fp of x of degree m. All right

For example, x squared plus x plus 1 is a prime polynomial. And I'm going to ask if the remainders mod g of x form a field under mod g of x arithmetic.

OK. Let's flow this out a little bit. Again, what are the remainders going to be of any polynomial of degree m? So this is basically going to be the polynomials of degree less than m in Fp of x.

How many of them are there, by the way? p to the m. So the size of this is p to the m. And one of the representations for these polynomials is just to write out F0, F1, up to m minus 1. So this just basically looks like the polynomial m-tuples. Set of F0, F1 up to F minus 1, for each of these an element of the field.

OK? I can make a one-to-one correspondence between the polynomials of degree less than m and the set of all coefficient m-tuples over Fp. These are just m-tuples over Fp. So there are p to the m of them.

And so it's a finite set, size p to the m. Does it form a field under mod g of x arithmetic?

AUDIENCE: [INAUDIBLE PHRASE].

PROFESSOR: Correct. And that's a homework problem. So I'm not going to do it in class, but I will sketch here how it's going to be done. But I'm glad that you instantly see that. Because again, we just model everything we do on what we did for integers. If you remember how we proved it for integers.

First of all, we really need to check two things. Addition. Just as we did for this specific example up here, we first have to check that the addition table is that of an abelian group, that these supposed field elements form an abelian group under addition.

And we've already observed several times that addition is just basically component-wise addition of these m-tuples. So it's just like vector addition. And vector addition, of course, has the group property. So addition is basically just like vector addition. Or I could write, perhaps more precisely, Zp over m. Distinction without a difference, really.

So it's just component-wise addition of the coefficients. That's how we do polynomial addition. And it will give us a remainder that has a degree of less than m, so we don't have to have ever reduce it. Modulo g of x, we just simply add component-wise.

OK. So that's easy to verify. The addition table is always going to be OK.

So what do we have to prove now? We have to -- what am I going to call these? Rg of x. The remainders mod g of x.

For multiplication, we have to prove that Rg of x star -- the non-zero polynomials form an abelian group, which, as I say, it's a homework problem. Let me sketch the proof. It's precisely analogous to the proof that we made for Zp star.

We basically have to check closure. If we multiply two non-zero polynomials, do we get another non-zero polynomial? Asking another way, is it possible to multiply two polynomials of degree less than m and get a result which is a multiple of g of x, which is either equal to g of x or a multiple of g of x?

And it's, I think, easy to convince yourself if this has no factors -- its only factors are itself and 1, no non-trivial factors -- then you can't multiply two lesser degree polynomials and get either g of x, of course, or any multiple of g of x. And it's an exercise for the student to write that proof out. OK? But it's just exactly analogous to the proof that you can't multiply two integers less than a prime p and get a multiple of p. So use that as a model, if you want to, in your proof.

That of course depends on this being prime. If this is factorizable, non-prime, then of course there are going to be two nontrivial factors, two remainders of degree less than m, whose product is equal to g of x itself, if it's factorizable. So you can't possibly get closure. So this is why non-prime polynomials don't work, just like non-prime integers don't work when we constructed Fp. Exactly analogous reasons.

All right. Second question is, when we go through this multiplication, suppose we take r of x times -- let's construct a multiplication table. Let's take a particular row. Let's take r of x times all the non-zero things. Can we possibly get any repeats? Can r of x times s of x equal r of x times t of x?

And again, it's easy to convince yourself that that's not possible. If that were possible, then r of x times s of x minus t of x would be equal to 0. And so we're back to where we were before -- mod g of x. And this is impossible. These are both degrees less than m. We can't multiply two things of lower degree together to get a multiple of g of x. So it can't equal 0.

That means there can't be any repeats. That means that each row is a permutation of every other row. Similarly for columns. If you want to do that, all you have to actually prove is one.

So every row or column is a permutations of every other one, if we just look at the non-zero polynomials, star. And therefore, this forms an abelian group whose identity is always one. Just as we proved up here. So this depends on irreducibility. Depends on no nontrivial factors of g of x.

OK. And that's all we have to check.

So I claim that by this process, I can, given a prime polynomial in Fp of x of degree m, I can construct a finite field with p to the m elements, that the addition and multiplication rules can be taken as mod g of x arithmetic, and they will satisfy the field axioms.

So you can now construct a finite field for any prime power p to the m, right?

There's actually still a hole in this.

AUDIENCE: [INAUDIBLE PHRASE].

PROFESSOR: Define prime polynomial? The term, or --

AUDIENCE: Define the [UNINTELLIGIBLE] of degree m.

PROFESSOR: Correct. Is there going to be a prime polynomial of every degree? I don't know. Suppose you want to define an irreducible polynomial over, say, F2 of x or F3 of x of degree 4. Could you do that?

AUDIENCE: [INAUDIBLE PHRASE].

PROFESSOR: Beautiful. I mean, that's an excellent suggestion.

So the question is, does there exist a prime polynomial in Fp of x of every degree? Or of a given degree?

And there are various ways of attacking this question. First of all, I'll tell you the answer is yes. For every p and every m, there does exist a prime polynomial. Which is fortunate. So from that, we conclude there is a finite field with p to the m elements for every prime p and every m greater than or equal to 1.

Now, how might we prove that? One is, look it up on Google. You can certainly formulate a question that will lead you to a webpage that will have a listing of all the prime polynomials of all degrees over any field that you're interested in. So perhaps that will suffice for you.

Two. What I'm going to talk about is the sieve method.

Three. You could do a bound on the number of polynomials of each degree in d, and show that it's greater than or equal to 1, always. And this is done in the notes. Section 7.9 I think.

Or four, you can do what Mr. Agarwal has suggested. You can actually do the closed form combinatoric formula, which -- I haven't done any number theory here. There's a little bit of elementary number theory in the notes. Euler numbers, this sort of thing. We get formulas for the number of integers degree d that -- well, number of integers that have multiplicative orders d mod n, and so forth. It's a lovely combinatoric field. There is a lovely closed form for this that you get from the Mobius inversion formula.

And it can be found in combinatoric books. I know it's in Berlekamp's *Algebraic Coding Theory* book. And it's extremely pretty.

And then of course, given the formula, you have to prove to all of the -- again, n of d is greater than or equal to 1. But there is a closed form expression for it that you get out of combinatorics. We're not going to do that here.

I'll be satisfied -- well, this is the real engineering solution here. This is the mathematical engineering solution.

And what do I mean by the sieve method? Again, take the analogy with the integers. One of the first mathematical accomplishments was Eratosthenes' sieve for finding prime numbers.

How does it work? You start to write down all the -- well. Imagine first writing down all the integers. All right? Cross off 1. Start with 2. All right. So the first prime is 2. Then you cross off all multiples of 2. 4,6,8, so forth. OK? So what's the next number that you haven't crossed off? It's 3, so that's the next prime. You cross off all the multiples of 3. 3,6,9. So forth. 15.

And thereby you continue. So the steps are, find the next integer on the list. That's going to be a prime, because it won't have been crossed off by any previous steps. It's not a multiple of any integer of lower degree. Then cross off all of its multiples, up to however long your scribe has written this on the tablet. And this way, you can find the primes up to any number you want. Gets kind of tedious after a while, but you can certainly find all the primes up to 100 in a few minutes doing this, right?

Well, it's the same for integers, and it's the same for polynomials. So let's, for instance, do a polynomial sieve. Of course, what we're most interested in is the polynomials with binary coefficients, F2 of x.

And how do we do it? Let's write down -- let's forget about 0 and 1. Those are not considered to be prime. Let's start with the degree 1 polynomials. What are the degree one polynomials? They're x, x plus 1.

Are these factorizable? Obviously their only factors are one and themselves. They have no nontrivial factors. So these are primes.

OK. So now let's write down all the polynomials of degree two. I'm sort of doing this in an interleaved manner. There are going to be two of degree 1, four of degree 2. All I'm going to do is -- well, the only polynomials are monic in F2 of x, so I don't have to make that qualification. All right. So here are the four of degree 2, right?

Now I go through with my sieve and we take out all multiples of x. Multiples of x are polynomials with 0 constant term, right? A lowest order term. So obviously this is a multiple of x, this is a multiple of x.

Multiples of x plus 1. How do you recognize those over the binary field? This is basically the polynomial whose root is 1. That means the mod-2 sum of the coefficients is equal to 0. So any polynomial that has an even number of non-zero coefficients is divisible by x plus 1.

Did you all get that? If not, try that at home. That's the easy way to recognize whether something is a multiple of x plus 1. It has an even number of non-zero coefficients.

So this is a multiple of x plus 1. We wrote it out explicitly. It's x plus 1 squared in F2 of x, and this is not. So there is only one prime polynomial over F2 of x that's degree 2. So this is our only possible choice if we want to construct a finite field with four elements, due to the two elements.

OK. So that might begin to get us scared. Is it possible that there are no prime polynomials of degree three? Well, we had two here, one here. Is it going down? Let's write down the polynomials of degree 3. x third, x third plus 1, x to the three plus x, to the three plus x plus 1, x to the three plus x squared, x to the three plus x squared plus 1, x to the three plus x squared plus x, x to the three plus x squared plus x plus 1.

Eight of them. So that's working in our favor. There's double the number of polynomials as we go up one in degree.

And again, let's go through the sieve. Which are multiples of x, non-zero constant term? Which are multiples of x plus 1, even number of non-zero coefficients? If you doubt that, write it out. Which are multiples of x squared plus x plus 1? Well, they're going to have to be x squared plus x plus 1 times x plus 1 or times x, so we've already got them. If we take this times itself, we're going to get a polynomial of degree 4. Not going to be on this list.

So we have to multiply this by these. We've already got those. So whew. We found two. We could use either of these to construct a finite field with eight elements.

And so forth. And it turns out as you go up to higher degrees, that the number now increases very nicely, and there's no problem finding a prime polynomial of each degree. And in fact, you could be cute about it and try to find one with only three non-zero terms, or has some other nice property that makes it easy to calculate with. And so forth.

So do you understand the sieve method? If you do, then I believe you could find a -- suppose you want to construct a field with 64 elements. What do you need? 64 is 2 to the sixth, so you're going to need a polynomial with p equals 2 and m equals 6. You're going to need a binary polynomial of degree 6 that is prime, irreducible. And again, in a few minutes by going through the sieve process, you can quickly find one, or you could look it up in Google, or in Peterson's book, or any algebraic coding theory book, or probably a lot of other places.

So this is a practical solution for the problem for any given p and m. Of course, it hardly proves that there's one of every degree, because they're kind of an infinite number of degrees. Yeah?

AUDIENCE: So there's two order 3 polynomials that are prime. Will it generate two separate fields, or are they going to be isomorphic to each other?

PROFESSOR: Great question. All fields with p to the m elements are isomorphic to each other. That's proved in the notes. I'm not going to do it in class. And the other thing that's proved in the notes is the analog to Zp. There are no other finite fields with other than p to the m number of elements. OK? So this is it.

Now, if you explicitly write out these two, and write out their -- well, the addition tables are always look the same, because it's always just binary three-tuples, in this case. But multiplication tables are going to look different. But there is some isomorphism. x and 1 may be equivalent to x squared plus 1 on the other one, or something. But if you go through that isomorphism, you'll find that the field tables are the same.

Actually, I guess I'm going to prove that, because I'm going to prove that the multiplication table is always cyclic. That the group to which it's isomorphic is z mod p to the m minus 1. Just as it was to Z3 here.

And I guess that's sufficient with the addition table isomorphism. I guess you have to prove they're equivalent. You saw it in a different way in the notes. But you're going to see that all the multiplication group is always a cyclic group, with p to the m minus 1 elements, and that goes a long way towards suggesting that these are always going to be isomorphic to each other. Yeah?

AUDIENCE: Identify roots, right?

PROFESSOR: Identify roots? If I understand what you're saying, that's basically the way it's done in the notes. You first show there's always going to be some primitive element that generates the cyclic group. Some single generator such that alpha alpha squared, so forth, is the entire non-zero set. You're going to show that alpha has some minimal polynomial, and the set of all linear combinations of powers of alpha is basically equal to the whole field. And so this allows you to establish the isomorphism. and I think that's what you're suggesting. So you're well equipped to read the notes, but I'm not going to do that in class.

Yeah. I'm very interested in your questions. Please ask more, as many questions as you like. What I'm getting from it is, you know, you all come from different backgrounds. Some of you have seen this in perhaps a math context, or some other context, or you've seen parts of it, or some of the words are familiar. And of course, there are many different ways to present this and to make the proofs and so forth.

So I'm trying to pick a line that works for the particular results that I want to get to. I don't think you would do anything much different if you wanted to develop finite fields. But the class has a very different set of backgrounds, and I'm trying to reach all of you.

Don't be alarmed if you've never seen anything like this before. You're not way behind everybody else, either. I think it's pretty easy to understand. Maybe it would take you a couple hours longer than somebody who has more background, but not more than that.

OK. So that's how we construct finite fields. You have an example of it.

Goodness. Is it really 11 o'clock? OK. So I'm not even -- so I've simply asserted, but not proved. You saw in this case that the multiplicative group was a cyclic group. And we could always, for multiplication, represent grouped elements by this log table. So I'd hoped to prove that in class. I'm not going to be able to prove that in class. And I'll simply ask you to read that, too.

This is important for working with finite fields, because it is the way, probably the preferred way, to implement multiplication. So you ought to be thinking of how you would program up a finite field multiplier. One way is polynomial multiplication. The other way is just use the fact that the multiplicative group is cyclic. And then it's easy. Just add exponents and reduce modulo q minus 1.

OK. I'm sorry not to have had a chance to go over that. Next time, Ralf Koetter will start to get into chapter eight, Reed-Solomon codes.