Math 3527 (Number Theory 1)

Lecture #25

Finite Fields:

- Construction of Finite Fields
- Factorization of $x^p - x$ and $x^{p^n} - x$ in $\mathbb{F}_p[x]$
- Counting Irreducible Polynomials in $\mathbb{F}_p[x]$

This material represents §4.3.2 from the course notes.

Finite Fields, I

Recall from the previous lectures that if $q(x)$ is an irreducible polynomial in $R = F[x]$, then R/qR is a field. In the special case where $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we see that R/qR is a finite field:

Theorem (Constructing Finite Fields)

If $q(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree d, then the ring R/qR is a finite field with p^d elements.

Finite Fields, I

Recall from the previous lectures that if $q(x)$ is an irreducible polynomial in $R = F[x]$, then R/qR is a field. In the special case where $F = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, we see that R/qR is a finite field:

Theorem (Constructing Finite Fields)

If $q(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree d, then the ring R/qR is a finite field with p^d elements.

Proof:

- Since $q(x)$ is irreducible, R/qR is a field.
- The residue classes in the ring R/qR are represented uniquely by the polynomials in $\mathbb{F}_p[x]$ of degree $\leq d-1$.
- These polynomials are $a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$, for $a_i \in \mathbb{F}_p$.
- There are p choices for each of the d coefficients $a_0, \ldots, a_{d-1}$, so there are p^d such polynomials.

Finite Fields, II

Example: Show that the ring R/qR, where $R = \mathbb{F}_2[x]$ and $q(x) = x^2 + x + 1$, is a field with 4 elements.

Finite Fields, II

Example: Show that the ring R/qR, where $R = \mathbb{F}_2[x]$ and $q(x) = x^2 + x + 1$, is a field with 4 elements.

- Observe that $q(x) = x^2 + x + 1$ has no roots modulo 2, since $q(0) = q(1) = 1$.
- Therefore, since it is a polynomial of degree 2, it is irreducible.
- Thus by our results, we know that R/qR is a field, and since q has degree 2, R/qR has $2^2 = 4$ elements.
- We actually encountered this field before and wrote down its multiplication table (which clearly shows it is a field!):

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Finite Fields, III

Example: Show that the ring R/qR, where $R = \mathbb{F}_3[x]$ and $q(x) = x^2 + 1$, is a field with 9 elements.

Finite Fields, III

Example: Show that the ring R/qR, where $R = \mathbb{F}_3[x]$ and $q(x) = x^2 + 1$, is a field with 9 elements.

- Observe that $q(x) = x^2 + 1$ has no roots modulo 3, since $q(0) = 1$ and $q(1) = q(2) = 2$.
- Therefore, since it is a polynomial of degree 2, it is irreducible.
- Thus by our results, we know that R/qR is a field, and since q has degree 2, R/qR has $3^2 = 9$ elements.

Finite Fields, IV

Example: Give an explicit construction for a finite field with exactly 121 elements.

Finite Fields, IV

Example: Give an explicit construction for a finite field with exactly 121 elements.

- Note that $121 = 11^2$. Therefore, we can construct a finite field with 121 elements as R/qR where $R = \mathbb{F}_{11}[x]$ and $q(x)$ is an irreducible polynomial of degree 2.
- There are (as we will show later) quite a few possible choices.
- Since we want a polynomial of degree 2, it is enough to see that it has no roots.
- The polynomial $q(x) = x^2$ is obviously not irreducible, so let's try $q(x) = x^2 + 1$. In fact we see $q(0) = 1$, $q(\pm 1) = 2$, $q(\pm 2) = 5$, $q(\pm 3) = 10$, $q(\pm 4) = 6$, and $q(\pm 5) = 4$.
- Since these values represent every residue class modulo 11, we see that q has no roots and is therefore irreducible.
- Thus, R/qR for $R = \mathbb{F}_{11}[x]$ and $q(x) = x^2 + 1$ gives a finite field with 121 elements.

Finite Fields, V

Example: Give an explicit construction for a finite field with exactly 8 elements.

Finite Fields, V

Example: Give an explicit construction for a finite field with exactly 8 elements.

- From our discussion, since $8 = 2^3$, such a field can be obtained as R/qR where $R = \mathbb{F}_2[x]$ and q is an irreducible polynomial in R of degree 3.
- Again, since q has degree 3, to show that it is irreducible requires only establishing that it has no roots.
- The polynomials x^3, $x^3 + 1$, $x^3 + x$ all have roots (respectively, $x = 0, 1, 0$).
- However, $q(x) = x^3 + x + 1$ does not, since $q(0) = q(1) = 0$.
- Thus, for $q(x) = x^3 + x + 1$ in $R = \mathbb{F}_2[x]$, R/qR is a finite field with 8 elements.

Factorization of $x^p - x$, I

We now discuss a pair of very important polynomials in $\mathbb{F}_p[x]$ that will give us important information about factorizations; namely, $x^p - x$ and $x^{p^n} - x$.

Proposition (Factorization of $x^p - x$)

The factorization of $x^p - x$ in $\mathbb{F}_p[x]$ is $x^p - x = \prod_{a \in \mathbb{F}_p}(x - a)$.

Factorization of $x^p - x$, I

We now discuss a pair of very important polynomials in $\mathbb{F}_p[x]$ that will give us important information about factorizations; namely, $x^p - x$ and $x^{p^n} - x$.

Proposition (Factorization of $x^p - x$)

The factorization of $x^p - x$ in $\mathbb{F}_p[x]$ is $x^p - x = \prod_{a \in \mathbb{F}_p}(x - a)$.

Proof:

- First, by Fermat's Little Theorem in $\mathbb{F}_p$, we see that $a^p - a = 0$ for every $a \in \mathbb{F}_p$.
- Thus, for $q(x) = x^p - x$, we have $q(a) = 0$ for all $a \in \mathbb{F}_p$.
- This means $x - a$ is a divisor of $q(x)$ for all $a \in \mathbb{F}_p$.
- However, because this polynomial has at most p roots, and we have exhibited p roots, the factorization of $q(x)$ must be $q(x) = \prod_{a \in \mathbb{F}_p}(x - a)$, since the leading terms agree.

Factorization of $x^p - x$, II

Here is one interesting consequence of this factorization $x^p - x = \prod_{a \in \mathbb{F}_p} (x - a)$:

- By dividing through by x, we see that $x^{p-1} - 1 = \prod_{a \in \mathbb{F}_p, a \neq 0} (x - a)$.
- Now examine the constant term of the product: it is $(-1)^{p-1} \prod_{a \in \mathbb{F}_p, a \neq 0} (a) = (-1)^{p-1} \cdot (p-1)!$
- Also, the constant term on the left-hand side is equal to -1.
- So by comparing the coefficients as elements of $\mathbb{F}_p$, we deduce $(p-1)! \equiv (-1)^{p-2} \equiv -1 \pmod{p}$.
- Thus, by examining this factorization, we obtain an easy (and totally different) proof of Wilson's Theorem!

Factorization of $x^{p^n} - x$, I

Let us now study the factorization of $x^{p^n} - x$ in $\mathbb{F}_p[x]$. Examples:

- For $n = 2$ and $p = 2$, we find the factorization $x^4 - x = x(x+1)(x^2+x+1)$.
- For $n = 3$ and $p = 2$, we find the factorization $x^8 - x = x(x+1)(x^3+x^2+1)(x^3+x+1)$.
- For $n = 4$ and $p = 2$, we find the factorization $x^{16} - x = x(x+1)(x^2+x+1)(x^4+x^3+1)(x^4+x+1)(x^4+x^3+x^2+x+1)$.
- For $n = 2$ and $p = 3$, we find the factorization $x^9 - x = x(x+1)(x+2)(x^2+2)(x^2+x+2)(x^2+2x+2)$.
- For $n = 2$ and $p = 5$, we find the factorization $x^{25} - x = x(x+1)(x+2)(x+3)(x+4)(x^2+2)(x^2+3)(x^2+x+1)(x^2+x+2)(x^2+2x+3)(x^2+2x+4)(x^2+3x+3)(x^2+3x+4)(x^2+4x+1)(x^2+4x+1)$.

Factorization of $x^{p^n} - x$, II

We notice (especially in the $p = 5$ example) that the irreducible factors all appear to be of small degree, and that there are no repeated factors.

In fact, looking more closely, it seems that the factorization of $x^{p^n} - x$ over $\mathbb{F}_p$ contains all of the irreducible polynomials of degree n, or of degree dividing n.

Here is one more example that will confirm this suspicion:

- For $n = 5$ and $p = 2$, we find the factorization
$$x^{32} - x = x(x+1)(x^5 + x^2 + 1)(x^5 + x^3 + 1)$$
$$(x^5 + x^3 + x^2 + x + 1)(x^5 + x^4 + x^2 + x + 1)$$
$$(x^5 + x^4 + x^3 + x + 1)(x^5 + x^4 + x^3 + x^2 + 1).$$

Notice here that all the irreducible terms have degree 1 or degree 5.

Factorization of $x^{p^n} - x$, III

We now prove that our observation is correct:

Theorem (Factorization of $x^{p^n} - x$)

The polynomial $x^{p^n} - x$ factors in $\mathbb{F}_p[x]$ as the product of all monic irreducible polynomials over $\mathbb{F}_p$ of degree dividing n.

The proof of this result will be in several steps:

- First, we show that $q(x) = x^{p^n} - x$ has no repeated factors.
- Second, we show that every irreducible polynomial of degree dividing n divides $q(x)$.
- Finally, we show that no other irreducible polynomial can divide $q(x)$.

Factorization of $x^{p^n} - x$, IV

Part 1: $q(x) = x^{p^n} - x$ has no repeated factors.

- We proved last lecture that a polynomial has no repeated factors if and only if it is relatively prime to its derivative.
- We compute $q'(x) = p^n x^{p^n - 1} - 1 = -1$.
- So, clearly, $q(x)$ and $q'(x)$ are relatively prime, since the derivative $q'(x)$ is actually just a constant.
- Hence, $q(x)$ has no repeated irreducible factors.

Factorization of $x^{p^n} - x$, V

For the next two parts, we will need the following Lemma:

Lemma

If p is a prime number, then the greatest common divisor of $p^n - 1$ and $p^d - 1$ is $p^{\gcd(n,d)} - 1$.

Proof of Lemma:

- Use the division algorithm to write $n = qd + r$, and let $a = p^r(p^{(q-1)d} + p^{(q-2)d} + \cdots + p^d + 1)$.
- Then it is not hard to see by expanding the products that $p^n - 1 = (p^d - 1)a + (p^r - 1)$.
- So by properties of gcds, we see that $\gcd(p^n - 1, p^d - 1) = \gcd(p^d - 1, p^r - 1)$.
- This means we can perform the Euclidean algorithm on the exponents without changing the gcd.
- The end result is $p^{\gcd(n,d)} - 1$, so this is the desired gcd.

Factorization of $x^{p^n} - x$, VI

Part 2: Every irreducible poly. of degree dividing n divides $q(x)$.

- Suppose that $s(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree d dividing n, so that $n = ad$.
- Since s is irreducible, we know that R/sR is a finite field F having p^d elements.
- Therefore, by invoking Euler's theorem in F on the element x, we see that $x^{p^d-1} \equiv 1 \pmod{s}$.
- But, by the Lemma, $p^d - 1$ divides $p^n - 1$, so raising to the appropriate power modulo s shows $x^{p^n-1} \equiv 1 \pmod{s}$. We conclude that s divides $x^{p^n} - x$, as desired.

Factorization of $x^{p^n} - x$, VII

Part 3: No other irreducible polynomials divide $q(x)$.

- Suppose $s(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial that divides $x^{p^n} - x$ and has degree d not dividing n.
- Clearly $s(x) \neq x$, so we can assume s divides $x^{p^n-1} - 1$.
- As before, R/sR is a finite field F having p^d elements.
- Thus, Euler's theorem in F implies $a^{p^d-1} \equiv 1 \pmod{s}$ for all nonzero $a \in F$. Also, $a^{p^n-1} \equiv 1 \pmod{s}$ holds for every nonzero $a \in F$ by the above assumptions.
- Thus the order of every nonzero element in F divides both $p^d - 1$ and $p^n - 1$ and hence also their gcd $p^{\gcd(d,n)} - 1$.
- This means $a^{p^{\gcd(d,n)}-1} \equiv 1 \pmod{s}$ for all nonzero $a \in F$.
- This is impossible, because then $q(t) = t^{p^{\gcd(d,n)}-1} - 1$ is a polynomial of degree $p^{\gcd(d,n)} - 1$ having $p^d - 1$ roots.

Counting Irreducible Polynomials, I

As a corollary, the above theorem allows us to count the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of any particular degree n:

- Let $f_p(n)$ be the number of monic irreducible polynomials of exact degree n in $\mathbb{F}_p[x]$.
- By counting degrees on both sides of our factorization of $x^{p^n} - x$, we obtain a recursive formula $p^n = \sum_{d|n} d f_p(d)$.

Counting Irreducible Polynomials, I

As a corollary, the above theorem allows us to count the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of any particular degree n:

- Let $f_p(n)$ be the number of monic irreducible polynomials of exact degree n in $\mathbb{F}_p[x]$.
- By counting degrees on both sides of our factorization of $x^{p^n} - x$, we obtain a recursive formula $p^n = \sum_{d|n} d f_p(d)$.

We can use this formula to calculate the values $f_n(p)$:

- $n = 1$: the formula says $p = f_1(p)$ so $f_1(p) = p$.
- $n = 2$: formula says $p^2 = f_1(p) + 2f_2(p)$ so $f_2(p) = \dfrac{p^2 - p}{2}$.
- $n = 3$: formula says $p^3 = f_1(p) + 3f_3(p)$ so $f_3(p) = \dfrac{p^3 - p}{3}$.
- $n = 4$: $p^4 = f_1(p) + 2f_2(p) + 4f_4(p)$ so $f_4(p) = \dfrac{p^4 - p^2}{4}$.

Counting Irreducible Polynomials, II

Using this recursion, we can compute a few more values:

n	1	2	3	4	5
$f_p(n)$	p	$\frac{1}{2}(p^2-p)$	$\frac{1}{3}(p^3-p)$	$\frac{1}{4}(p^4-p^2)$	$\frac{1}{5}(p^5-p)$

n	6	7	8	9
$f_p(n)$	$\frac{1}{6}(p^6-p^3-p^2+p)$	$\frac{1}{7}(p^7-p)$	$\frac{1}{8}(p^8-p^4)$	$\frac{1}{9}(p^9-p^3)$

Counting Irreducible Polynomials, II

Using this recursion, we can compute a few more values:

n	1	2	3	4	5
$f_p(n)$	p	$\frac{1}{2}(p^2-p)$	$\frac{1}{3}(p^3-p)$	$\frac{1}{4}(p^4-p^2)$	$\frac{1}{5}(p^5-p)$

n	6	7	8	9
$f_p(n)$	$\frac{1}{6}(p^6-p^3-p^2+p)$	$\frac{1}{7}(p^7-p)$	$\frac{1}{8}(p^8-p^4)$	$\frac{1}{9}(p^9-p^3)$

Example: Find the number of monic irreducible polynomials of degree 3 in $\mathbb{F}_2[x]$.

- This is the value of $f_3(2) = \frac{1}{3}(2^3-2) = 2$.
- In fact, it is not hard to see that there are in fact exactly 2 such polynomials: x^3+x+1 and x^3+x^2+1.

Counting Irreducible Polynomials, III

Example: Find the number of monic irreducible polynomials of degree 5 in $\mathbb{F}_2[x]$.

- This is the value of $f_5(2) = \frac{1}{5}(2^5 - 2^1) = 6$.
- In fact, we calculated these six polynomials earlier in our factorization of $x^{32} - x$.

Counting Irreducible Polynomials, III

Example: Find the number of monic irreducible polynomials of degree 5 in $\mathbb{F}_2[x]$.

- This is the value of $f_5(2) = \frac{1}{5}(2^5 - 2^1) = 6$.
- In fact, we calculated these six polynomials earlier in our factorization of $x^{32} - x$.

Example: Find the number of monic irreducible polynomials of degree 6 in $\mathbb{F}_3[x]$.

- This is the value of $f_6(3) = \frac{1}{6}(3^6 - 3^3 - 3^2 + 3^1) = 116$.

Counting Irreducible Polynomials, III

Example: Find the number of monic irreducible polynomials of degree 5 in $\mathbb{F}_2[x]$.

- This is the value of $f_5(2) = \frac{1}{5}(2^5 - 2^1) = 6$.
- In fact, we calculated these six polynomials earlier in our factorization of $x^{32} - x$.

Example: Find the number of monic irreducible polynomials of degree 6 in $\mathbb{F}_3[x]$.

- This is the value of $f_6(3) = \frac{1}{6}(3^6 - 3^3 - 3^2 + 3^1) = 116$.

Example: Find the number of monic irreducible polynomials of degree 8 in $\mathbb{F}_5[x]$.

- This is the value of $f_8(5) = \frac{1}{8}(5^8 - 5^4) = 48750$.

Counting Irreducible Polynomials, IV

Looking at the formulas $f_n(p)$ for various small values of n suggests that there might be a nice formula for the general value. In fact, we can describe it using a technique known as Möbius inversion:

Definition

The Möbius function is defined as

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by the square of any prime} \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \end{cases}.$$

In particular, $\mu(1) = 1$.

Counting Irreducible Polynomials, IV

Looking at the formulas $f_n(p)$ for various small values of n suggests that there might be a nice formula for the general value. In fact, we can describe it using a technique known as Möbius inversion:

Definition

The Möbius function is defined as

$$\mu(n) = \begin{cases} 0 & \text{if } n \text{ is divisible by the square of any prime} \\ (-1)^k & \text{if } n \text{ is the product of } k \text{ distinct primes} \end{cases}.$$

In particular, $\mu(1) = 1$.

Examples:

- Since 19 is prime, we have $\mu(19) = -1$.
- Since $6 = 2 \cdot 3$, we have $\mu(6) = 1$.
- Since $8 = 2^3$, we have $\mu(8) = 0$.
- Since $30 = 2 \cdot 3 \cdot 5$, we have $\mu(30) = -1$.

Counting Irreducible Polynomials, V

The (quite clever!) observation is that we can use the Möbius function to solve the recurrence relation for our values $f_n(p)$:

Proposition (Möbius Inversion)

If $A(n)$ is any sequence satisfying a recursive relation of the form $B(n) = \sum_{d|n} A(d)$, for some function $B(n)$, then $A(n) = \sum_{d|n} \mu(d)B(n/d)$.

We will omit the proof (it is in the notes, if you are curious, but it is just a strong induction argument).

Counting Irreducible Polynomials, VI

By applying Möbius inversion for the function $B(n) = p^n$ and $A(n) = nf_n(p)$, we obtain an explicit formula for $f_n(p)$:

Corollary

The number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is $f_p(n) = \frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}$.

Counting Irreducible Polynomials, VI

By applying Möbius inversion for the function $B(n) = p^n$ and $A(n) = nf_n(p)$, we obtain an explicit formula for $f_n(p)$:

Corollary

The number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is $f_p(n) = \frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}$.

Examples:

- We have $f_6(p) = \frac{1}{6}(\mu(1)p^6 + \mu(2)p^3 + \mu(3)p^2 + \mu(6)p) = \frac{1}{6}(p^6 - p^3 - p^2 + p)$, which agrees with our earlier results.
- We have $f_8(p) = \frac{1}{8}(\mu(1)p^8 + \mu(2)p^4 + \mu(4)p^2 + \mu(8)p) = \frac{1}{8}(p^8 - p^4)$, again as before.

Counting Irreducible Polynomials, VII

Corollary

The number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is $f_p(n) = \frac{1}{n}\sum_{d|n}\mu(d)p^{n/d}$.

From this corollary (repeated above for your convenience), we see

$$f_p(n) = \frac{1}{n}p^n + O(p^{n/2})$$

where the "big-O" notation means that the error is of size bounded above by a constant times $p^{n/2}$.

Counting Irreducible Polynomials, VIII: The Last Slide

The observation $f_p(n) = \frac{1}{n}p^n + O(p^{n/2})$ can be reinterpreted:

- Let X be the number of polynomials in $\mathbb{F}_p[x]$ of degree n.
- Clearly, $X = p^n$. Now we ask: of all these X polynomials, how many of them are "prime" (i.e., irreducible)?
- This is simply $f_p(n) = \frac{1}{n}p^n + O(p^{n/2}) = \frac{X}{\log_p(X)} + O(\sqrt{X})$.
- In other words: the number of "primes less than X" is equal to $\frac{X}{\log_p(X)}$, up to a bounded error term.

Notice how very similar this statement is to the statement of the Prime Number Theorem for the integers $\mathbb{Z}$!

This is not a coincidence: in fact, it is the analogue of the Prime Number Theorem for the ring $\mathbb{F}_p[x]$.

Counting Irreducible Polynomials, IX: That Was a Lie

It is also fairly easy to show using the formula that $f_p(n) > 0$ for every prime p and every integer $n \geq 1$.

- Explicitly, by the Möbius inversion formula, we see that $f_p(n) \geq p^n - p^{n-1} - \cdots - p - 1$.
- But p^n is bigger than $p^{n-1} + p^{n-2} + \cdots + p + 1 = \frac{p^n - 1}{p-1}$ by the geometric series formula. Hence $f_p(n)$ is always positive.

As we showed earlier, if $q(x)$ is an irreducible polynomial of degree n in $R = \mathbb{F}_p[x]$, then R/qR is a finite field of size p^n. Thus:

Corollary

For any prime p and any n, there is a finite field with p^n elements.

As one additional note: by a linear algebra argument, the number of elements in a finite field must be a prime power.

Summary

We described how to construct finite fields with p^d elements as the ring of residue classes R/qR where $R = \mathbb{F}_p[x]$ and $q(x)$ is an irreducible polynomial of degree d.

We studied the factorization of the polynomials $x^p - x$ and $x^{p^n} - x$ in $\mathbb{F}_p[x]$ and used the results to count irreducible polynomials of degree n in $\mathbb{F}_p[x]$.

We used Möbius inversion to give a formula for the number of monic irreducible polynomials in $\mathbb{F}_p[x]$, and established the analogue of the Prime Number Theorem.

Next lecture: Primitive roots.