Math 75 notes, Lecture 6

P. Pollack and C. Pomerance

1 More on the factorization of $x^{q^d} - x$

Let's review where we were at the end of the last lecture. After a bout with some difficult notation, we had finished proving the following result:

Theorem 1. *Let F be a finite field with q elements, and let $f(x)$ be an irreducible polynomial in $F[x]$ of degree d. Then $f(x)$ divides $x^{q^d} - x$.*

Thus all irreducibles of degree d show up in the factorization of $x^{q^d} - x$. We now show that in fact the same is true for all irreducibles of degree j dividing d:

Theorem 2. *Let F be a finite field with q elements, and let $f(x)$ be an irreducible polynomial in $F[x]$ of degree j. If j divides d, then $f(x)$ divides $x^{q^d} - x$.*

Before we can prove this we need a few easy preliminary lemmas.

Lemma 1. *Let F be a field. If m and n are positive integers, then $x^m - 1$ divides $x^n - 1$ in $F[x]$ if and only if m divides n.*

Actually the 'if' part is all we need to prove Theorem 2, but we shall later require the 'only if' portion too, so we prove both of them here.

Proof. We work with congruences modulo $x^m - 1$ in the ring $F[x]$. Then, by our definition of congruence,

$$x^m \equiv 1 \pmod{x^m - 1}.$$

Suppose that m divides n, so that $n = mq$ for some positive integer q. Raising both sides of this congruence to the qth power we find

$$x^n = x^{mq} \equiv 1 \pmod{x^m - 1}.$$

But this says precisely that $x^m - 1$ divides $x^n - 1$.

The other direction is similar. Suppose $x^m - 1$ divides $x^n - 1$ and write $n = mq + r$, where $0 \le r < m$. Then working as above, we find

$$x^{mq} \equiv 1 \pmod{x^m - 1},$$

and so multiplying by x^r, we get

$$x^n = x^{mq+r} \equiv x^r \pmod{x^m - 1}.$$

But in this case we are supposing that $x^n \equiv 1 \pmod{x^m - 1}$. So we get that

$$1 \equiv x^r \pmod{x^m - 1},$$

so that $x^m - 1$ divides $x^r - 1$. But this forces r to be zero, since otherwise $x^r - 1$ would be a nonzero polynomial of smaller degree than $x^m - 1$. □

Lemma 2. *Let q be any integer with $q \geq 2$. Let m, n be positive integers. Then $q^m - 1$ divides $q^n - 1$ if and only if m divides n.*

Proof. We leave this as homework. The argument is almost exactly the same as above, except that instead of working modulo $x^m - 1$ in $F[x]$ one works modulo $q^m - 1$ in $\mathbb{Z}$. □

We can now prove Theorem 2.

Proof. Let $f(x) \in F[x]$ be an irreducible polynomial of degree j dividing d. By the last lemma, $q^j - 1$ divides $q^d - 1$. And so by Lemma 1,

$$x^{q^j - 1} - 1 \mid x^{q^d - 1} - 1 \quad \text{in } F[x].$$

Thus there is a $Q(x) \in F[x]$ with

$$x^{q^d - 1} - 1 = (x^{q^j - 1} - 1)Q(x),$$

and so, multiplying both sides by x,

$$x^{q^d} - x = (x^{q^j} - x)Q(x).$$

But we already know from Theorem 1 that $f(x)$ divides $x^{q^j} - x$, so that $f(x)$ is a factor of the right-hand side. Thus $f(x)$ must also be a factor of the left-hand side, which is what we wanted to show. □

It is natural to wonder how much of the truth is contained in Theorem 2. In other words, consider the factorization of $x^{q^d} - x$. We know from Theorem 1 that all primes of degree dividing d must show up. What are the exponents on these primes? And what other primes (if any?) show up in the factorization?

We can maybe get a feel for this by doing some computations. As an example we take $F = \mathbb{Z}/(3)$. Then in $F[x]$, we have

$$\begin{aligned}
x^3 - x &= x(x+1)(x+2), \\
x^{3^2} - x &= x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2), \\
x^{3^3} - x &= x(x+1)(x+2)(x^3+x^2+2x+1)(x^3+2x^2+x+1)(x^3+x^2+2)(x^3+2x^2+2x+2) \\
&\quad \cdot (x^3+2x+2)(x^3+2x^2+1)(x^3+2x+1)(x^3+x^2+x+2).
\end{aligned}$$

In these examples of factorizations of $x^{3^d} - x$ for $d = 1, 2, 3$, we have, as we must, all the irreducibles of degree dividing d. More noteworthy is that in these examples we have *only* these primes, and that all of these primes show up *exactly once* (there is no exponent > 1 on any of them). It is not hard, on a computer (say), to confirm that this pattern seems to continue for larger d.

Thus, we might well conjecture the following: Let $\mathcal{I}(F, d)$ be the set of irreducible polynomials of degree d over F (always understood to be *monic*).

Conjecture 1. *For every finite field F with q elements and any positive integer d, we have*

$$x^{q^d} - x = \prod_{j|d} \prod_{P \in \mathcal{I}(F,j)} P.$$

This conjecture turns out to be correct and to have a number of important applications. Unfortunately it will be a little while before we have the tools at our disposal to give the proof.

2 Groups, generators, and finite fields

We need a few more results from the theory of finite abelian groups. Let G be a finite abelian group. If $g \in G$, we define the *order* of the element g to be the smallest positive k for which

$$g \circ g \circ \cdots \circ g = e,$$

where e is the identity of the group and g appears on the left k times. This is a bit cumbersome to write, so we often abbreviate the left hand side to g^k.

It is convenient to also assign meaning to g^k when $k = 0$ or when k is negative. We can get started by remembering that we have already defined g^{-1} – it is just the inverse of g whose existence is guaranteed by the group axioms. We define g^{-2}, g^{-3}, etc., in terms of powers of g^{-1}, by setting, for $k < 0$,

$$g^k = (g^{-1})^{-k}.$$

Notice that if $k < 0$, then $-k > 0$, and so we already know what the right hand side means. We still have to define g^0, but that's easy; we let it be the identity element e of our group. With these definitions, it is easy to verify that the familiar laws of exponents hold: For every $g \in G$ and every pair of integers k, l, we have

$$g^k g^l = g^{k+l} \quad \text{and} \quad (g^k)^l = g^{kl}.$$

We say that the element $g \in G$ *generates* the group G (or that g is a *generator* of G) if every element of G can be written in the form g^k for some integer k. A group with a generator is called a *cyclic group*.

Lemma 3. *Let G be a finite abelian group and suppose g is an element of G of order m. Then the m elements g^r, for $r \in \{0, 1, 2, \ldots, m-1\}$, are all distinct. Moreover, every power of g has the form g^r for some $r \in \{0, 1, 2, \ldots, m-1\}$.*

Proof. If the elements g^r were not all distinct, then we would have

$$g^i = g^j \quad \text{for some } 0 \leq i < j < m.$$

Multiplying both sides by g^{-i} we find that

$$e = g^0 = g^j g^{-i} = g^{j-i}.$$

Let l be the integer $j - i$. Then $g^l = e$ and l is a positive integer smaller than m. But m was supposed to be the smallest positive integer for which $g^m = e$, so that we have a contradiction.

For the second half of the lemma, suppose k is any integer. We must show that $g^k = g^r$ for some $r \in \{0, 1, 2, \ldots, m-1\}$. By the division algorithm, we can write $k = mq + r$, where $r \in \{0, 1, 2, \ldots, m-1\}$. Then

$$g^k = g^{mq+r} = (g^m)^q g^r = g^r,$$

since $g^m = e$. □

Corollary 1. *Let G be an abelian group of order n. Then $g \in G$ generates G if and only if g has order n.*

Proof. If g has order n, then $g^0, \ldots, g^{n-1}$ are n different elements of G. But G only has n elements, so it must be that these are all the elements of G; thus g generates G. For the other half of the corollary, suppose that g generates G, and let m be the order of G. Since the powers of g have exhaust G, we must have $m \geq n$. But we can't have $m > n$, since otherwise we would have more than n distinct elements in a group of order n. □