Math 75 NOTES 2 on finite fields

C. Pomerance

Let F be a finite field with q elements. We have just seen that the number $N_q(d)$ of monic irreducible polynomials of degree d in $F[x]$ that divide $x^{q^d} - x$ satisfies the formula

$$N_q(d) = \frac{1}{d} \sum_{j|d} \mu(d/j) q^j.$$

Here μ is the Möbius function from elementary number theory and combinatorics. We can use the fact that $\mu(n)$ is always ± 1 or 0 to get an estimate for $N_q(d)$. We see that the term in the sum with the biggest absolute value is when $j = d$; the term is $\mu(1)q^d = q^d$. Thus,

$$N_q(d) \geq \frac{1}{d} q^d - \frac{1}{d} \sum_{j=1}^{\lfloor d/2 \rfloor} q^j = \frac{1}{d} q^d - \frac{1}{d} \frac{q^{\lfloor d/2 \rfloor + 1} - q}{q - 1},$$

using the formula to sum a geometric series. It is easy to check that for every positive integer d, we have $\lfloor d/2 \rfloor + 1 \leq d$ (equality holds at $d = 1, 2$, and for $d \geq 3$ it is a strict inequality). Thus,

$$N_q(d) \geq \frac{1}{d} q^d - \frac{1}{d} \frac{q^d - q}{q - 1} \geq \frac{1}{d} q^d - \frac{1}{d}(q^d - q) > 0.$$

The conclusion: The polynomial $x^{q^d} - x$ in $F[x]$ has at least one irreducible factor of degree d.

A further conclusion: If F is a finite field of q elements and d is a positive integer, then there is a finite field of q^d elements that contains F as a subfield. Indeed, let $f \in F[x]$ be irreducible of degree d. The field $F[x]/(f)$ has q^d elements and it contains (an isomorphic copy of) F.

A still further conclusion: If p is a prime and d is any positive integer, there is a finite field of size p^d. This then is the converse of what we learned earlier, namely, that every finite field has a prime-power number of elements.

Here are some further consequences of our discussion. If F is a finite field of q elements and $f \in F[x]$ is irreducible of degree d, then $f(x) \mid x^{q^d} - x$. (So $N_q(d)$ counts the total number of monic irreducibles in $F[x]$ of degree d.) Here's why $f(x) \mid x^{q^d} - x$. Let $K = F[x]/(f)$, a finite field with q^d elements. Then the element x of K, call it α, satisfies $f(\alpha) = 0$, so f is the minimal polynomial for α in K. But every element in K is a root of $x^{q^d} - x$, so it follows that $f(x) \mid x^{q^d} - x$ in $F[x]$.

And: If L, F are finite fields with F a subfield of L of size q and $[L : F] = d$, then for each $j \mid d$, we have an intermediate field K with $[K : F] = j$ (which we have already seen is unique, provided it exists). Here's why. Let $f \in F[x]$ with $f \mid x^{q^d} - x$ irreducible of degree j. Since $x^{q^d} - x$ has q^d roots in L and splits into q^d distinct linear factors in $L[x]$, it follows that f has a root $\alpha \in L$. We've seen that $K = F[\alpha]$ is an intermediate field with $[K : F]$ being the degree of the minimal polynomial of α over F. But this polynomial is $f(x)$, which has degree j. In fact, $F[\alpha]$ is isomorphic to $F[x]/(f)$ and it is the unique intermediate field of size q^j. Done.

And finally: If F_1 and F_2 are finite fields of q elements each, then F_1 is isomorphic to F_2. Here's why. We know there is some positive integer d and prime p with $q = p^d$. We have just learned that for the field extension $\mathbb{Z}/(p) \subset F_1$, and for each $j \mid d$, there is some irreducible factor f_j of $x^{p^d} - x$ in $(\mathbb{Z}/(p))[x]$ with $(\mathbb{Z}/(p))[x]/(f_j)$ the unique intermediate field of size p^j. Let's apply this with $j = d$. So, F_1 is isomorphic to $(\mathbb{Z}/(p))[x]/(f_d)$, and the same for F_2. So they are isomorphic to each other.

Because of this last fact, for each prime power q, we have the notation $\mathbb{F}_q$ for the unique (up to isomorphism) finite field of size q. We shall see later that not all presentations of $\mathbb{F}_q$ are equally pleasant, and we may wish to distinguish between them, but the broad picture for now is that there is just one field of q elements.

Here's a proof of the formula

$$\sum_{j|n} \mu(j) = \begin{cases} 1, & n = 1, \\ 0, & n > 1. \end{cases}$$

From the definition of μ, we have for any positive integer n that

$$\sum_{j|n} \mu(j) = \sum_{\substack{j|n \\ j \text{ squarefree}}} \mu(j) = \sum_{j|m} \mu(j),$$

where m is the largest squarefree divisor of n. Thus, it suffices to prove the formula for squarefree numbers m. The formula is clearly correct for $m = 1$. Now assume it is true for m, and let p be a prime that does not divide m. The divisors of pm fall into two disjoint sets, those numbers j which divide m and those that don't. The latter divisors are of the form pj, where $j \mid m$. Thus, since $\mu(pj) = -\mu(j)$, we have

$$\sum_{j|pm} \mu(j) = \sum_{j|m} \mu(j) + \sum_{j|m} \mu(pj) = \sum_{j|m} \mu(j) - \sum_{j|m} \mu(j) = 0.$$

Thus, the formula follows by induction.