Math 75 notes, Lecture 9

P. Pollack and C. Pomerance

The number of monic irreducibles of degree d

Recall that if F is a field, we let $\mathcal{I}(F,d)$ denote the set of monic irreducible polynomials in $F[x]$ of degree d. Depending on the field, this set can be infinite, finite, or even empty. For example, if $F=\mathbb{C}$, the complex numbers, then $\mathcal{I}(F,d)$ is empty whenever $d>1$. (This is the Fundamental Theorem of Algebra.) A consequence is that $\mathcal{I}(\mathbb{R},d)$ is empty whenever $d>2$. On the other hand, $\mathcal{I}(\mathbb{Q},d)$ is infinite for each d, since x^d+p is irreducible in $\mathbb{Q}[x]$ for every prime p. (Do you know how to prove this?)

It is clear that if F is a finite field, then $\mathcal{I}(F,d)$ cannot be infinite, since if $\#F=q$, there are just q^d monic polynomials of degree d. Let $I(F,d)$ denote the number of elements of $\mathcal{I}(F,d)$. One of our goals with the past few lectures is, when F is a finite field, to get a formula for $I(F,d)$. We will do this via the irreducible factorization of $x^{q^d}-x$:

$$x^{q^d}-x=\prod_{j\mid d}\ \prod_{f(x)\in\mathcal{I}(F,j)} f(x) \quad (\text{when } \#F=q). \tag{1}$$

By comparing degrees of the left and right sides, we immediately have that

$$q^d=\sum_{j\mid d} jI(F,j). \tag{2}$$

As you have seen on homework, this formula can then be used to compute any $I(F,d)$.

So, what is the difficulty? We have already proved many results about $x^{q^d}-x$. In particular we know that each irreducible divisor of $x^{q^d}-x$ in $F[x]$ has its degree dividing d, and we know that every irreducible $f(x)\in F[x]$ of degree dividing d also divides $x^{q^d}-x$. Doesn't this then establish (1)? Almost, but not quite. This shows that in the irreducible factorization of $x^{q^d}-x$ in $F[x]$, we see appearing all of the members of the various $\mathcal{I}(F,j)$ for $j\mid d$ and no other irreducibles, but these irreducible factors might occur to an exponent higher than the first power. So, if we could prove that the irreducible factorization of $x^{q^d}-x$ is *squarefree* (that is, not divisible by the square of an irreducible polynomial), then we would be finished with the proof of (1) and (2).

If you've been following though, *we have already proved* that $x^{q^d}-x$ is squarefree! Well, almost. We did this under the additional assumption that there exists an irreducible polynomial of degree d. (Do you recall the proof?) Perhaps we can use this, and indeed we can. First note that there is absolutely no problem when $d=1$, since

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

is indeed squarefree (see Theorem 3 in Lectures 4&5). Now take d to be a prime number. If there is an irreducible polynomial in $F[x]$ of degree d, we would know that $x^{q^d}-x$ is squarefree, so assume such a polynomial does not exist. Since d is prime, it follows that in the irreducible factorization of $x^{q^d} - x$, we only see degree 1 factors, and at least one of them, say $x - a$ appears with an exponent at least 2. In particular, we have the factorization

$$x^{q^d} - x = (x - a)^2 g(x) \tag{3}$$

for some $g(x) \in F[x]$. Let us replace x with $x + a$ in this identity. Doing so on the right side We get $x^2 g(x + a)$. Doing so on the left side, we get

$$(x + a)^{q^d} - (x + a) = x^{q^d} + a^{q^d} - x - a,$$

where we have used Theorem 2 and Corollary 1 in Lectures 7&8. But by Theorem 3 in Lectures 4&5, we have $a^{q^d} = a$, so the last expression above simplifies to $x^{q^d} - x$. So replacing x with $x + a$ in (3) leads to

$$x^{q^d} - x = x^2 g(x + a).$$

But visibly the left side is not divisible by x^2, so this equation must be wrong. Thus, $x^{q^d} - x$ is in fact divisible by an irreducible polynomial of degree d, when d is prime, so it must be squarefree.

By way of mathematical induction, let $n \geq 2$ and suppose that we have shown that over any finite field, say with Q elements, and any positive integer d with less than n prime factors (counted with multiplicity), we have $x^{Q^d} - x$ squarefree. Now suppose that d has n prime factors and consider the polynomial $x^{q^d} - x$ over our field F of q elements. Let r be a prime factor of d. From the above paragraph we have seen that there is an irreducible polynomial $f(x) \in F[x]$ of degree r. Let $K = F[x]/(f)$, which is a finite field with $Q = q^r$ elements. Since d/r has fewer than n prime factors, by the induction hypothesis, we know that $x^{Q^{d/r}} - x$ is squarefree in its factorization in $K[x]$. But

$$Q^{d/r} = (q^r)^{d/r} = q^d,$$

so $x^{q^d} - x$ is squarefree in its factorization in $K[x]$. Now K contains F as a subfield, so the factorization in $K[x]$ being squarefree implies that the factorization in $F[x]$ is also squarefree. (If $g(x)^2 \mid x^{q^d} - x$ in $F[x]$, then if $h(x)$ is an irreducible factor of $g(x)$ in $K[x]$, then $h(x)^2 \mid x^{q^d} - x$ in $K[x]$.)

So, this does it. We have proved that $x^{q^d} - x$ is always squarefree, and so we have proved (1) and (2). We record this in the following theorem

Theorem 1. *If F is a finite field with q elements, we have* (1) *and* (2)*.*

We can use this result to get a very useful *approximate* formula for $I(F, d)$.

Corollary 1. *If F is a field with q elements, then for each positive integer d we have*

$$\frac{1}{d} q^d - \frac{2}{d} q^{d/2} < I(F, d) \leq \frac{1}{d} q^d.$$

Proof. One of the terms in the sum in (2) is $dI(F,d)$, and every other term that may exist in the sum is nonnegative, so we have $dI(F,d) \le q^d$, which gives the second inequality in the corollary. Since each $jI(F,j) \le q^j$ (just proved!), the identity (2) implies that

$$dI(F,d) \;=\; q^d - \sum_{\substack{j|d\\ j<d}} jI(F,j) \;\ge\; q^d - \sum_{\substack{j|d\\ j<d}} q^j \ge q^d - \sum_{j=1}^{\lfloor d/2 \rfloor} q^j, \tag{4}$$

where $\lfloor y \rfloor$ is the largest integer that is at most y (sometimes denoted $[y]$, but this might be confusing in our context). Let $m = \lfloor d/2 \rfloor$. Then, by the formula that sums a geometric progression,

$$\sum_{j=1}^{m} q^j \;=\; \frac{q^{m+1}-q}{q-1} \;<\; \frac{q^{m+1}}{q-1} \;=\; q^m \frac{q}{q-1} \;\le\; 2q^m.$$

Thus, (4) implies that

$$I(F,d) > \frac{1}{d}q^d - \frac{1}{d}2q^m,$$

which proves the first inequality of the corollary. $\square$

Before we leave this topic, we remark on a few things. First, the lower bound inequality in Corollary 1 implies that $I(F,d) > 0$. We record this as follows.

Corollary 2. *If F is a finite field and d is a positive integer, then there is at least one irreducible polynomial in $F[x]$ of degree d. In particular, if q is either a prime number or a power of a prime, then there is a finite field with q elements.*

We leave the details of the proof for a homework problem or test question.

Another remark concerning Corollary 1 is the main order of magnitude of $I(F,d)$, namely, it is about q^d/d. That is, about 1 in d polynomials in $F[x]$ of degree d are irreducible. Contrast this with $\mathbb{Q}[x]$. For example, take degree 2. For a quadratic polynomial to be irreducible in $\mathbb{Q}[x]$, it's discriminant must be a square. But square rationals are very sparsely distributed in the rationals, so the chance of choosing a "random" quadratic in $\mathbb{Q}[x]$ and having it be irreducible is close to 1, while in a finite field, the chance is close to 1/2.

Perhaps, it makes more sense to compare the distribution of irreducibles in $F[x]$ with the distribution of prime numbers in $\mathbb{Z}$. Up to a high number N, the number of primes is approximately $N/\log N$ in that the ratio of the count to this expression tends to 1 as $N \to \infty$; this is the celebrated Prime Number Theorem. (Note that log is the natural logarithm.) On the other hand, the number of monic irreducible polynomials in $F[x]$ of degree N is about q^N/N, which expression is exactly $q^N/\log_q(q^N)$, where $q = \#F$ and $\log_q$ is the base-q logarithm. Note that the Prime Number Theorem for $\mathbb{Z}$ is very hard to prove, so we should feel a sense of accomplishment that we have done the analogue for $F[x]$.