Analytic Combinatorics Homework 7 Question and Answer

Eric Neyman

4/4/2017

(Note: the two paragraphs at the top are long-winded but necessary in case students are not familiar with polynomials over finite fields (most if not all students in the class are familiar with these, though). Perhaps it would be unfair to put this question on the exam, because it takes a bit of time to understand the first two paragraphs. However, I think it is a good question, so I decided to submit it.)

For any prime p, a *monic polynomial over* $\mathbb{F}_p$ *of degree* d is a polynomial of the form $x^d + a_{d-1}x^{d-1} + \cdots + a_1 d + a_0$, where all coefficients a_i are integers between 0 and $p-1$, inclusive. Such a polynomial P is called *reducible* if there exist two monic polynomials over $\mathbb{F}_p$ of degree greater than 0 such that $QR \equiv P \pmod{p}$, i.e. the coefficients of $Q \cdot R$ and the corresponding coefficients of P are congruent modulo p. Such a polynomial is called *irreducible* if it has positive degree and is not reducible.

An important result which you may use is that every monic polynomial over $\mathbb{F}_p$ can be factored uniquely into products of irreducible polynomials. (The polynomial 1 factors as the empty product.)

For this problem, let p be some prime.

(a) Explain why there are p^d monic polynomials over $\mathbb{F}_p$ of degree d.

(b) Let I be the class of all irreducible monic polynomials over $\mathbb{F}_p$ and P be the class of all monic polynomials over $\mathbb{F}_p$. Write down a construction involving I and P.

(c) Let $I(z)$ be the generating function for irreducible monic polynomials over $\mathbb{F}_p$ (where the size of a polynomial is its degree). Write down a generating function equation for $I(z)$.

(d) Let $I_d = [z^d]I(z)$. Use the above equation to prove that

$$\sum_{d|n} dI_d = p^n.$$

(a) There are p possible choices for each coefficient $a_0, \ldots, a_{d-1}$, so the total number of such polynomials is indeed p^d.

(b) A monic polynomial factors uniquely into irreducible monic polynomials. Thus we can think of each monic polynomial as a multiset of irreducible monic polynomials. We thus have

$$P = MSET(I).$$

(c) Let $P(z)$ be the generating function for all monic polynomials over $\mathbb{F}_p$. We have $P(z) = 1 + pz + p^2z^2 + \cdots = \frac{1}{1-pz}$, by part (a). This together with part (b) gives us

$$\exp\left(\sum_{k\geq 1} \frac{I(z^k)}{k}\right) = \frac{1}{1-pz}.$$

(d) Taking the log of both sides above, we have

$$\log\left(\frac{1}{1-pz}\right) = \sum_{k\geq 1} \frac{I(z^k)}{k}.$$

The left-hand side above can be written as $pz + \frac{(pz)^2}{2} + \frac{(pz)^3}{3} + \ldots$. The right-hand side can be written as

$$\sum_{k\geq 1} \frac{I(z^k)}{k} = \sum_{k\geq 1}\sum_{d\geq 1} \frac{I_d z^{kd}}{k} = \sum_{d\geq 1} I_d \sum_{k\geq 1} \frac{z^{kd}}{k}.$$

The coefficient of z^n here is the sum over all d dividing n of $\frac{I_d}{\frac{n}{d}}$. We know that this equals $\frac{p^n}{n}$ from earlier. Thus we have

$$\sum_{d|n} \frac{dI_d}{n} = \frac{p^n}{n}$$

$$\sum_{d|n} dI_d = p^n,$$

as desired.