Math 161 Final
Priya Malhotra

For my final I chose to prove the closed form equation of the number of irreducible monic polynomials of degree d, labelled as r_d, is $r_d = (1/d)\sum_{y|d}\mu(y)q^{(d/y)}$. There are three main steps to split this up into, as I outline below. This very closely mimics how I split up my main theorems in the Lean code, with some additional lemmas to reuse and make the work more readable. For this first draft, please find a write-up of question formulations and proofs for each of the three parts that directly build on previous parts to lead to a final answer.

Fix a prime number p. A polynomial $f(X) \in \mathbb{F}_p[X]$ is called *monic* if its leading coefficient is equal to one. Write a_d for the number of monic polynomials of degree d and write r_d for the number of irreducible monic polynomials of degree d. Our convention is that $a_0 = 1$.

1. Letting $A(x)$ denote the generating function for the sequence a_d, show that

$$A(x) = \frac{1}{1-px}.$$

. . . .

For a degree d monic polynomial

$$f(X) = X^d + c_{d-1}X^{d-1} + \cdots + c_0$$

in $\mathbb{F}_p[X]$, the vector of coefficients (except for the leading coefficient which is always the same) is $\langle c_{d-1}, \ldots, c_0\rangle \in \mathbb{F}_p^d$. Since each polynomial is uniquely determined by its vector of coefficients, the number of monic polynomials of degree d

$$\begin{aligned} a_d &= |\mathbb{F}_p^d| \\ &= |\mathbb{F}_p|^d \\ &= p^d, \end{aligned} \tag{1}$$

which is also consistent with the convention that $a_0 = 1$.

The power series expansion of

$$\frac{1}{1-z} = \sum_{i=0}^{\infty} z^i, \tag{2}$$

so

$$\begin{aligned} A(x) &= \frac{1}{1-px} \text{ as given} \\ &= \sum_{i=0}^{\infty}(px)^i \text{ by (2)} \\ &= \sum_{i=0}^{\infty} p^i x^i \\ &= \sum_{i=0}^{\infty} a_i x^i \text{ by (1).} \end{aligned}$$

$\square$

2. Using the fact that any polynomial can be uniquely factored into irreducible polynomials, prove that

$$A(x) = \prod_{d \geq 0} \left(\frac{1}{1 - x^d} \right)^{r_d}.$$

. . . .

$$\begin{aligned}
\prod_{d \geq 0} \left(\frac{1}{1 - x^d} \right)^{r_d} &= \prod_{d \geq 0} \left(\sum_{i=0}^{\infty} x^{id} \right)^{r_d} \quad \text{by (2)} \\
&= \prod_{d \geq 0} \prod_{j=1}^{r_d} \sum_{i=0}^{\infty} x^{id} \\
&= \prod_{\substack{f \in \mathbb{F}_p[X] \\ f \text{ monic} \\ f \text{ irreducible}}} \sum_{i=0}^{\infty} x^{i \deg f} \text{ by definition of } r_d \\
&= \prod_{\substack{f \in \mathbb{F}_p[X] \\ f \text{ monic} \\ f \text{ irreducible}}} \sum_{i=0}^{\infty} x^{\deg f^i} \\
&= \prod_{\substack{f \in \mathbb{F}_p[X] \\ f \text{ monic} \\ f \text{ irreducible}}} (1 + x^{\deg f} + x^{\deg f^2} + \cdots) \\
&= 1 \\
&\quad + \sum_{\substack{f \in \mathbb{F}_p[X] \\ f \text{ monic} \\ f \text{ irreducible}}} x^{\deg f} + \sum_{\substack{\{f,g\} \subset \mathbb{F}_p[X] \\ f,g \text{ monic} \\ f,g \text{ irreducible}}} x^{\deg f} x^{\deg g} + \cdots \\
&\quad + \sum_{\substack{f \in \mathbb{F}_p[X] \\ f \text{ monic} \\ f \text{ irreducible}}} x^{\deg f^2} \sum_{\substack{\{f,g\} \subset \mathbb{F}_p[X] \\ f,g \text{ monic} \\ f,g \text{ irreducible}}} x^{\deg f^2} x^{\deg g} + \cdots \\
&\quad + \cdots \\
&= 1 \\
&\quad + \sum_{\substack{f \in \mathbb{F}_p[X] \\ f \text{ monic} \\ f \text{ irreducible}}} x^{\deg f} + \sum_{\substack{\{f,g\} \subset \mathbb{F}_p[X] \\ f,g \text{ monic} \\ f,g \text{ irreducible}}} x^{\deg f + \deg g} + \cdots \\
&\quad + \sum_{\substack{f \in \mathbb{F}_p[X] \\ f \text{ monic} \\ f \text{ irreducible}}} x^{\deg f^2} \sum_{\substack{\{f,g\} \subset \mathbb{F}_p[X] \\ f,g \text{ monic} \\ f,g \text{ irreducible}}} x^{\deg f^2 + \deg g} + \cdots \\
&\quad + \cdots \\
&= 1
\end{aligned}$$

$$
\begin{aligned}
&+ \sum_{\substack{f\in\mathbb{F}_p[X]\\ f \text{ monic}\\ f \text{ irreducible}}} x^{\deg f} + \sum_{\substack{\{f,g\}\subset\mathbb{F}_p[X]\\ f,g \text{ monic}\\ f,g \text{ irreducible}}} x^{\deg fg} + \cdots \\
&+ \sum_{\substack{f\in\mathbb{F}_p[X]\\ f \text{ monic}\\ f \text{ irreducible}}} x^{\deg f^2} \sum_{\substack{\{f,g\}\subset\mathbb{F}_p[X]\\ f,g \text{ monic}\\ f,g \text{ irreducible}}} x^{\deg f^2 g} + \cdots \\
&+ \cdots
\end{aligned} \tag{3}
$$

Because any polynomial can be uniquely factored into irreducible polynomials, and (3) contains all possible combinations of all powers of the irreducible monic polynomials of $\mathbb{F}_p$, (3) is equal to

$$\sum_{\substack{f\in\mathbb{F}_p[X]\\ f \text{ monic}}} x^{\deg f}. \tag{4}$$

When indexed by degree, (4) is equal to

$$\sum_{d=0}^{\infty} a_d x^d, \tag{5}$$

which is $A(x)$ by definition. $\square$

3. By taking logarithmic derivative (i.e. computing $\frac{\mathrm{d}}{\mathrm{d}x}\log A(x) = \frac{A'(x)}{A'(x)}$ in two ways using above formulas for $A(x)$ and comparing the results) deduce that

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

Explain why this relation determines the numbers r_d uniquely.

. . . .

$$
\begin{aligned}
\frac{\mathrm{d}}{\mathrm{d}x}\log\frac{1}{1-px} &= \frac{\mathrm{d}}{\mathrm{d}x}\log\prod_{d\geq 0}\left(\frac{1}{1-x^d}\right)^{r_d} \\
\frac{\frac{\mathrm{d}}{\mathrm{d}x}\frac{1}{1-px}}{\frac{1}{1-px}} &= \frac{\mathrm{d}}{\mathrm{d}x}\log\prod_{d\geq 0}\left(\frac{1}{1-x^d}\right)^{r_d} \\
\frac{\frac{p}{(1-px)^2}}{\frac{1}{1-px}} &= \frac{\mathrm{d}}{\mathrm{d}x}\log\prod_{d\geq 0}\left(\frac{1}{1-x^d}\right)^{r_d} \\
\frac{p}{\frac{1}{1-px}} &= \frac{\mathrm{d}}{\mathrm{d}x}\log\prod_{d\geq 0}\left(\frac{1}{1-x^d}\right)^{r_d} \\
\frac{p}{\frac{1}{1-px}} &= \frac{\mathrm{d}}{\mathrm{d}x}\sum_{d\geq 0}\log\left(\frac{1}{1-x^d}\right)^{r_d} \\
\frac{p}{\frac{1}{1-px}} &= \frac{\mathrm{d}}{\mathrm{d}x}\sum_{d\geq 0} r_d\log\frac{1}{1-x^d}
\end{aligned}
$$

$$
\begin{aligned}
\frac{p}{\frac{1}{1-px}} &= \frac{\mathrm{d}}{\mathrm{d}x}\sum_{d\geq 0} r_d \log\frac{1}{1-x^d} \\
\frac{p}{\frac{1}{1-px}} &= \sum_{d\geq 0} r_d \frac{\mathrm{d}}{\mathrm{d}x}\log\frac{1}{1-x^d} \\
\frac{p}{\frac{1}{1-px}} &= \sum_{d\geq 0} r_d \frac{\frac{\mathrm{d}}{\mathrm{d}x}\frac{1}{1-x^d}}{\frac{1}{1-x^d}} \\
\frac{p}{\frac{1}{1-px}} &= \sum_{d\geq 0} r_d \frac{\frac{dx^{d-1}}{(1-x^d)^2}}{\frac{1}{1-x^d}} \\
\frac{p}{\frac{1}{1-px}} &= \sum_{d\geq 0} r_d \frac{dx^{d-1}}{1-x^d} \\
p\frac{1}{\frac{1}{1-px}} &= \sum_{d\geq 0} dr_d x^{d-1}\frac{1}{1-x^d} \\
p\sum_{n=0}^{\infty}(px)^n &= \sum_{d\geq 0} dr_d x^{d-1}\sum_{n=0}^{\infty} x^{nd} \text{ by (2)} \\
p\sum_{n=0}^{\infty}p^n x^n &= \sum_{d\geq 0} dr_d x^{d-1}\sum_{n=0}^{\infty} x^{nd} \\
\sum_{n=0}^{\infty}p^{n+1} x^n &= \sum_{d\geq 0} dr_d \sum_{n=0}^{\infty} x^{(n+1)d-1} \\
\sum_{n=1}^{\infty}p^{n} x^{n-1} &= \sum_{d\geq 0} dr_d \sum_{n=1}^{\infty} x^{nd-1} \\
x\sum_{n=1}^{\infty}p^{n} x^{n-1} &= x\sum_{d\geq 0} dr_d \sum_{n=1}^{\infty} x^{nd-1} \\
\sum_{n=1}^{\infty}p^{n} x^{n} &= \sum_{d\geq 0} dr_d x \sum_{n=1}^{\infty} x^{nd-1} \\
\sum_{n=1}^{\infty}p^{n} x^{n} &= \sum_{d\geq 0} dr_d \sum_{n=1}^{\infty} x^{nd} \\
px + p^2x^2 + \cdots &= \sum_{d\geq 0} dr_d (x^d + x^{2d} + \cdots) \\
px + p^2x^2 + \cdots &= \sum_{d\geq 0} (dr_d x^d + dr_d x^{2d} + \cdots) \qquad (6)
\end{aligned}
$$

For each term in the right-hand side of (6), dr_d is added to its coefficient if and only if the degree of the term is a multiple of d, because for each $d \geq 0$, dr_d is added to $x^d, x^{2d}, \ldots$

on the right-hand side. Therefore, we have:

$$
\begin{aligned}
px + p^2x^2 + \cdots &= \sum_{d|1} dr_d x + \sum_{d|2} dr_d x^2 + \cdots \\
\sum_{n=1}^{\infty} p^n x^n &= \sum_{n=1}^{\infty} \sum_{d|n} dr_d x^n \\
\sum_{n=1}^{\infty} p^n x^n &= \sum_{n=1}^{\infty} x^n \sum_{d|n} dr_d \\
p^n &= \sum_{d|n} dr_d \qquad (7)
\end{aligned}
$$

which allows r_d to be calculated recursively using only r_b with $b < d$. (The numbers r_d can also be calculated in closed form using Möbius inversion.) □

For my final draft, there will be many details included on my lean code.