NOTES ON THE PRIME POLYNOMIAL THEOREM COURSE NOTES, 2015

Z. RUDNICK

0.1. **Basics.** Let $\mathbb{F}_q$ be a finite field of q elements, and $\mathbb{F}_q[t]$ the ring of polynomials with coefficients in $\mathbb{F}_q$. The units (invertible elements) are the scalars $\mathbb{F}_q^\times$, and any nonzero polynomial may be uniquely written as $cf(t)$ with $c \in \mathbb{F}_q^\times$ and $f(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_0$ a *monic* polynomial. We denote by M_n the set of monic polynomials, whose cardinality is

$$\#M_n = q^n$$

The ring $\mathbb{F}_q[t]$ is a Euclidean ring: Given $A, B \neq 0$ in $\mathbb{F}_q[t]$, there are $Q, R \in \mathbb{F}_q[t]$ so that

$$A = QB + R$$

and $R = 0$ (in which case $B \mid A$) or $\deg R < \deg B$.

A standard consequence of this property is that irreducible polynomials are *prime*, that is if $P \mid AB$ then either $P \mid A$ or $P \mid B$. Moreover the Fundamental Theorem of Arithmetic holds: Any polynomial of positive degree is "uniquely" a product of irreducible polynomials, that is up to ordering and multiplication by scalars.

Let $\pi_q(n)$ be the number of monic irreducibles $P \in \mathbb{F}_q[x]$ of degree n. Our goal is to prove the Prime Polynomial Theorem (PPT):

Theorem 0.1 (PPT)**.** *As* $q^n \to \infty$,

$$\pi_q(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n}) \ .$$

Moreover for all n we have an inequality

$$\pi_q(n) \leq \frac{q^n}{n} \ .$$

This is an analogue of the Prime Number Theorem (PNT), which states that the number $\pi(x)$ of primes $p \leq x$ is asymptotically equal to

$$\pi(x) \sim \mathrm{Li}(x) := \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x} \ .$$

Exercise 1. Compute $\pi_q(n)$ for $n = 2, 3, 4, 5, 6$.

Date: April 13, 2015.

1. The zeta function

The proof we give goes via the zeta function for $\mathbb{F}_q[t]$, which is defined as

$$\zeta_q(s) := \sum_{\substack{0\neq f\in\mathbb{F}_q[t]\\ f \text{ monic}}} \frac{1}{|f|^s}, \quad \Re(s)>1$$

Here the norm of a nonzero polynomial is defined as

$$|f| := \#\mathbb{F}_q[t]/(f),$$

the number of residue classes modulo f. The norm depends only on the degree of f:

$$|f| = q^{\deg f}\ .$$

As we shall see below, the series converges absolutely in the half-plane $\Re(s)>1$, and uniformly in every closed half-plane $\Re(s)\geq 1+\delta$, $\delta>0$, and hence defines an anlytic function in $\Re(s)>1$.

1.1. **Analytic continuation.**

Proposition 1.1. *$\zeta_q(s)$ is absolutely convergent for $\Re(s)>1$, and has an analytic continuation for all $s\in\mathbb{C}$, save for simple poles where $q^s=q$, that is at $s=1+\frac{2\pi\sqrt{-1}}{\log q}n$, $n\in\mathbb{Z}$, in fact*

$$\zeta_q(s) = \frac{1}{1-q^{1-s}}\ . \tag{1.1}$$

Proof. We rearrange the series (which is allowed because we have absolute convergence):

$$\begin{aligned}\sum_{\substack{0\neq f\in\mathbb{F}_q[x]\\ f \text{ monic}}} \frac{1}{|f|^s} &= \sum_{n=0}^\infty \Big(\sum_{\substack{\deg f=n\\ f\text{ monic}}}\frac{1}{|f|^s}\Big)\\ &= \sum_{n=0}^\infty \frac{1}{q^{ns}}\#\{f\in\mathbb{F}_q[x],\ \text{monic },\deg f=n\}\\ &= \sum_{n=0}^\infty \frac{1}{q^{ns}}q^n\end{aligned}$$

since the number of monic polynomials of degree n is q^n.

Thus we find that for $\Re(s)>1$,

$$\zeta_q(s) = \sum_{n=0}^\infty (q^{1-s})^n = \frac{1}{1-q^{1-s}}$$

since when $\Re(s)>1$, we have $|q^{1-s}| = q^{1-\Re(s)}<1$. The right-hand side of (1.1) now defines the required analytic continuation of $\zeta_q(s)$ to the entire complex plane, with the exception of simple poles at $q^s=q^1$, that is at $s=1+\frac{2\pi\sqrt{-1}}{\log q}n$, $n=0\pm1,\pm2,\dots$. □

Exercise 2. Compute the residue at $s = 1$ of ζ_q.

1.2. **The Euler product.** We next show that $\zeta_q(s)$ admits an Euler product representation

Theorem 1.2. *For* $\mathrm{Re}(s) > 1$,

$$\zeta(s) = \prod_{P \text{ prime}} (1 - |P|^{-s})^{-1}$$

Here the infinite product means the limit of the finite subproducts as follows: For $M > 0$ define

$$\zeta^{(M)}(s) := \prod_{\deg P \le M} (1 - |P|^{-s})^{-1}$$

to be the partial Euler product; this is a finite product. The infinite product is defined as the limit $\lim_{M\to\infty} \zeta^{(M)}(s)$ (assuming it exists).

Proof. We will show that for $\mathrm{Re}(s) > 1$,

$$\lim_{M\to\infty} \zeta^{(M)}(s) = \zeta_q(s)$$

(in fact uniformly for any $\mathrm{Re}(s) \ge 1 + \delta$, $\delta > 0$), which is the meaning of the claim.

We expand

$$\frac{1}{1 - |P|^{-s}} = \sum_{k=0}^{\infty} \frac{1}{|P|^{ks}} = \sum_{k=0}^{\infty} \frac{1}{|P^k|^s}$$

and so obtain

$$\zeta^{(M)}(s) = \prod_{\deg P \le M} \sum_{k=0}^{\infty} \frac{1}{|P^k|^s} = \sum_{\substack{\deg P_j \le M \\ k_j \ge 0}} \frac{1}{|\prod_j P_j^{k_j}|^s}$$

The sum here goes over all monic f for which all prime factors have degree $\le M$, and each such f appears exactly once by the Fundamental Theorem of Arithmetic in $\mathbb{F}_q[t]$ (unique factorization into primes).

Hence the difference $\zeta - \zeta^{(M)}$ is the sum over all monic f which have at least one prime factor of degree $> M$:

$$\zeta_q(s) - \zeta^{(M)}(s) = \sum_{\substack{f \ s.t. \exists P | f \\ \deg P > M}} \frac{1}{|f|^s}$$

Taking absolute values and using the triangle inequality (recall $|A^s| = A^{\mathrm{Re}(s)}$) gives

$$\left| \zeta_q(s) - \zeta^{(M)}(s) \right| \le \sum_{\substack{f \ s.t. \exists P | f \\ \deg P > M}} \frac{1}{|f|^{\mathrm{Re}\, s}}$$

We note that each f appearing above has degree $> M$, hence if we replace the sum by the sum over all f of degree $> M$, we will increase the result because we are adding positive terms. Hence

$$\left|\zeta_q(s) - \zeta^{(M)}(s)\right| \leq \sum_{\deg f > M} \frac{1}{|f|^{\mathrm{Re}(s)}}$$

The sum on the RHS tends to zero as $M \to \infty$ (we should have seen this by now) because

$$\begin{aligned}\sum_{\deg f > M} \frac{1}{|f|^{\mathrm{Re}(s)}} &= \sum_{n=M+1}^{\infty} \sum_{\deg f = n} \frac{1}{|f|^s} \\ &= \sum_{n=M+1}^{\infty} \frac{1}{q^{ns}} \#\{\deg f = n, \mathrm{monic}\} \\ &= \sum_{n=M+1}^{\infty} \frac{q^n}{q^{ns}} = \frac{q^{M(1-\mathrm{Re}(s))}}{1-q^{1-s}}\end{aligned}$$

which for any fixed $\mathrm{Re}(s) > 1$ tends to zero as $M \to \infty$, □

1.3. **The Explicit Formula.** The von Mangoldt function is defined as $\Lambda(f) = \deg P$, if $f = cP^k$ is a power of a prime P ($k \geq 1$), and is zero otherwise.

Exercise 3. Show that

$$\sum_{d|f} \Lambda(f) = \deg f \ .$$

Define

$$\Psi(n) := \sum_{\substack{\deg f = n \\ f \text{ monic}}} \Lambda(f)$$

which counts prime powers weighted by the degree of the corresponding prime.

From the definition it is easy to see that

Lemma 1.3.

$$\Psi(n) = \sum_{d|n} d\pi_q(d) \ .$$

The fundamental fact is that for $\mathbb{F}_q[t]$, there is a closed-form expression for $\Psi(n)$:

Proposition 1.4 (The "Explicit Formula")**.**

$$\Psi(n) = q^n$$

Proof. Setting

$$u := q^{-s}$$

so that the half-plane $\Re(s) > 1$ is mapped to the disk $|u| < q^{-1}$, we define

$$Z(u) := \zeta_q(s) = \sum_{\substack{0 \neq f \in \mathbb{F}_q[t] \\ f \text{ monic}}} u^{\deg f}$$

for which we have an Euler product representation

$$Z(u) = \prod_{P \text{ prime}} (1 - u^{\deg P})^{-1}, \quad |u| < q^{-1} \,. \tag{1.2}$$

The resummation (1.1) of $\zeta_q(s)$ is expressed as

$$Z(u) = \frac{1}{1 - qu} \,. \tag{1.3}$$

We compute the logarithmic derivative $u\frac{Z'}{Z} = u\frac{d}{du}\log Z$ of $Z(u)$ in two different ways:

a) From the Euler product (1.2) we obtain

$$\begin{aligned} u\frac{Z'}{Z}(u) &= \sum_{P \text{ prime}} \frac{\deg(P) \cdot u^{\deg P}}{1 - u^{\deg P}} \\ &= \sum_{P \text{ prime}} \deg(P) \sum_{m=1}^{\infty} u^{m \deg P} \\ &= \sum_{f \text{ monic}} \Lambda(f) u^{\deg f} \end{aligned}$$

by the definition of the von Mangoldt function. Thus

$$u\frac{Z'}{Z}(u) = \sum_{n=1}^{\infty} \Psi(n) u^n \,. \tag{1.4}$$

b) By the analytic continuation (1.3) of $Z(u)$ we obtain

$$u\frac{Z'}{Z}(u) = u\frac{d}{du}\log\frac{1}{1 - qu} = \sum_{n \geq 1} q^n u^n \,. \tag{1.5}$$

Comparing (1.4) and (1.5) gives the result. □

2. Proof of the PPT

We use Lemma 1.3 and the Explicit Formula to obtain

$$\sum_{d|n} d\pi_q(d) = \Psi(n) = q^n \,. \tag{2.1}$$

Hence we find that for all $m \geq 1$,

$$m\pi_q(m) \leq q^m \,. \tag{2.2}$$

Furthermore, from (2.1) we get

$$0 \le n\pi_q(n) - \Psi(n) = \sum_{\substack{d|n \\ d<n}} d\pi_q(d) \le \sum_{\substack{d|n \\ d<n}} q^d \tag{2.3}$$

the last step by (2.2).

The sum over divisors of n is hard to understand, so we convert it to a more tractable form by observing that a proper divisor $d \mid n$, $d < n$ is at most $n/2$, and then noting that throwing in some extra terms of the form q^d, which are non-negative, will only increase the result. Hence

$$\sum_{\substack{d|n \\ d<n}} q^d \le \sum_{d=1}^{n/2} q^d = \frac{q^{\lfloor n/2 \rfloor + 1} - q}{q-1} \le \frac{q^{\lfloor n/2 \rfloor}}{1 - \frac{1}{q}} \le 2q^{n/2}$$

Inserting in (2.3) gives

$$0 \le n\pi_q(n) - \Psi(n) \le 2q^{n/2}$$

and replacing $\Psi(n)$ by q^n and dividing by n gives

$$\pi_q(n) = \frac{q^n}{n} + O(\frac{q^{n/2}}{n})$$

which proves the Prime Polynomial Theorem. □