Algebraic NT, L3 We prove Prop. 2, namely that $Z(S_{P(\bar{x})}/\mathbb{F}_q; x) \in \mathbb{Z}[[x]]$, even $\in \mathbb{N}_0[[x]]$

For that we need to recall several facts about finite fields. Consider an extension

$K = \mathbb{F}_q \subset \mathbb{F}_{q^s} = L$, $s \in \mathbb{N}$. then $L = K(\alpha)$ for some ~~algebr.~~ element $\alpha \in L$ that is algebr. over K and of degree s: $g(\alpha) = 0_L$ for some monic $g \in K[X]$, $g(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)$, every $\alpha_i \in L$. So ($\alpha_1 = \alpha$) (they are distinct) every $\beta \in L$ is of the (unique) form $\beta = a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{s-1}\alpha^{s-1}$ for some $a_i \in K$. The elements

$\beta_i = \sum_{j=0}^{s-1} a_j \alpha_i^j$, $i = 1, 2, \ldots, s$, ($\alpha_i \in L$) are the Conjugates of β.

Another fact on fin. fields we need is this:

the maps $\sigma_i : B \mapsto B_i$, $i = 1, \dots, s$) are field automorphisms of L. the fixed field of σ_i) $\{x \in L \mid \sigma_i(x) = x\}$, is a strict subfield of L.

Now back to the proof, as it is given in Koblitz's book. Let K be a finite extension of $\mathbb{F}_q$ and consider a K-point $B = (x_1, \dots, x_n)$ of the hypersurface $S_{p(F)}$. Let $s_0 \in \mathbb{N}$ be minimum with $\forall i \in [n]: x_i \in \mathbb{F}_{q^{s_0}}$. Let $B_j = (x_{1,j}, \dots, x_{n,j})$, $j = 1, \dots, s_0$, be the conjugates of B (where $B = B_1$) in $\mathbb{F}_{q^{s_0}}$. the B_j are all distinct for else we would get, by σ, a contradiction with the minimality of s_0.

We count contribution of $B_1, \dots, B_{s_0}$ to $Z(m)$. Each of these points is on $\mathbb{F}_{q^s} \iff \mathbb{F}_{q^s} \supset \mathbb{F}_{q^{s_0}} \iff$
$\iff s_0$ divides s (that's actually another property of fin. fields we use). these points therefore contribute by s_0 to each count $N_{s_0}, N_{2s_0}, N_{3s_0}, \dots$.

In terms of the zeta-function their contribution to $Z(u)$ is (or formal power series)

$$\exp\left(\sum_{j=1}^{\infty} s_0 T^{j s_0}/j s_0\right) = \exp(-\log(1-T^{s_0})) = \frac{1}{1-T^{s_0}} = \sum_{j=0}^{\infty} T^{j s_0}.$$

The $Z(u)$ is a product of series of this type, and so it has (infinite, formal, but formally converging) integral, even ≥ 0, coefficients. ☒

Let me mention a simple but very practical observation on the numbers

$$N_s := \#(S_p(\mathbb{F}_{q^s}))$$

appearing in $Z(S_p/\mathbb{F}_q; x) =$

$$= \prod_{s=1}^{\infty} \exp\left(\sum_{i=1}^{\infty} \frac{N_s x^s}{s}\right),$$

which is missing

in Koblitz's book. Namely,

$Z(x) = \exp\left(\sum_{s=1}^{\infty} \frac{N_s x^s}{s}\right)$ is rational

$\Rightarrow F(x) := \sum_{s=1}^{\infty} N_s x^s$ (the OGF of the numbers $N_s, s=1,2,\ldots$) is rational too. Indeed,

$Z(x) = \frac{a(x)}{b(x)} \in \mathbb{Z}(x)$ & $F(x) = x\frac{Z(x)'}{Z(x)} = x\frac{(a(x)/b(x))'}{a(x)/b(x)} \in \mathbb{Z}(x)$ (log-differentiation). Thus the fact that $(N_s)_{s\geq 1}$ is a LRS (linear recurrence sequence), satisfies a lin. recurrence with constant coefficients, is an immediate corollary of Dwork's theorem.

There is a whole book on the numbers N_s and their generalizations, namely

J.-P. Serre, Lectures on $N_X(p)$, Chapman & Hall/CRC Research Notes in Mathematics, 11. A K Peters, Ltd., Wellesley, MA, 2012; x+163 pp.

Here, in Serre's book, $N_X(p)$ is the number of $\mathbb{F}_p$-points on the variety X defined as the zero-set of finitely many polynomials in several variables. A preliminary version of this book is available on-line. Technically it is much more demanding than the book of Koblitz.

I conclude this lecture with an example from Koblitz's book. We compute the zeta-function of an affine line $L = \mathbb{S}_{x_1}$, i.e. S_p with $P(x_1, x_2) = x_1 \rightsquigarrow L = \{(0, x_2) \mid x_2 \in \mathbb{F}_{\bullet}\}$ and since $|\mathbb{F}_{q^s}| = q^s$, we have that $N_s = q^s$. Thus

$$Z(L/\mathbb{F}_q; x) = \exp\left(\sum_{s=1} q^s x^s / s\right) = e^{-\log(1-qx)} =$$

$$= \frac{1}{1-qx}.$$

• Jean-Pierre Serre (1926) – Fields medal in 1954

thank you for your attention (addressing an $\emptyset$ set), next time I will start with the proof in earnest.