Algebra & Number Theory

Volume 11

2017

No. 5

Some sums over irreducible polynomials

David E. Speyer

ALGEBRA AND NUMBER THEORY 11:5 (2017)
dx.doi.org/10.2140/ant.2017.11.1231

Some sums over irreducible polynomials

David E. Speyer

We prove a number of conjectures due to Dinesh Thakur concerning sums of the form $\sum_P h(P)$ where the sum is over monic irreducible polynomials P in $\mathbb{F}_q[T]$, the function h is a rational function and the sum is considered in the T^{-1}-adic topology. As an example of our results, in $\mathbb{F}_2[T]$, the sum $\sum_P 1/(P^k-1)$ always converges to a rational function, and is 0 for $k=1$.

1. Introduction

Our goal is to explain some identities experimentally discovered by Dinesh Thakur, involving sums over irreducible polynomials in finite fields. We begin by stating the simplest of these identities: Let $\mathcal{P}$ be the set of irreducible polynomials in $\mathbb{F}_2[T]$. Then

$$\sum_{P\in\mathcal{P}} \frac{1}{P-1} = 0.$$

Here the sum must be interpreted as a sum of power series in T^{-1}. For example, the first five summands are

$$\begin{aligned}
\frac{1}{T-1} &= T^{-1}+T^{-2}+T^{-3}+\cdots \\
\frac{1}{(T+1)-1} &= T^{-1} \\
\frac{1}{(T^2+T+1)-1} &= \qquad\quad T^{-2}+T^{-3}+\cdots \\
\frac{1}{(T^3+T+1)-1} &= \qquad\qquad\qquad T^{-3}+\cdots \\
\frac{1}{(T^3+T^2+1)-1} &= \qquad\qquad\qquad T^{-3}+\cdots.
\end{aligned}$$

As the reader can see, only finitely many terms contribute to the coefficient of each power of T^{-1}, and the coefficient of T^{-j} is 0 for each j.

MSC2010: primary 11M38; secondary 05E05, 11M32.

Keywords: zeta function, special value, function field.

We now introduce the notation necessary to state our general results. To aid the reader's comprehension, we adopt the following conventions: Integers will always be denoted by lower case Roman letters (k, p, q, $\dots$); polynomials over finite fields will always be denoted by capital Roman letters (A, F, P, $\dots$), sets of such polynomials will always be denoted by calligraphic letters ($\mathcal{A}$, $\mathcal{P}$, $\mathcal{R}$, $\dots$), symmetric polynomials will be denoted by bold letters ($\boldsymbol{e}_k$, $\boldsymbol{p}_k$, $\dots$). Of course, there will be other sorts of mathematical objects as well, which we trust the reader to accommodate as they occur.

Let p be a prime and q a power of p. Let $\mathbb{F}_q$ be the field with q elements. Let $\mathcal{R}$ be the polynomial ring $\mathbb{F}_q[T]$. Let $\mathcal{K}$ be the fraction field $\mathbb{F}_q(T)$ and let $\widehat{\mathcal{K}}$ be the T^{-1}-adic completion of $\mathcal{K}$. All infinite sums will be understood in the T^{-1}-adic topology.

Let $\mathcal{P}$ be the set of irreducible polynomials in $\mathcal{R}$; let $\mathcal{P}_1$ be the set of monic irreducible polynomials. Here is our main result for the case $p = 2$.

Theorem 1.1. *If $p = 2$ then, for any positive integer $k \equiv 0 \bmod q-1$, the sum*

$$\sum_{P \in \mathcal{P}_1} \frac{1}{P^k - 1}$$

is in $\mathcal{K}$.

The reader may wonder what happens if we sum over all irreducible polynomials rather than monic ones; that is an easy corollary:

Corollary 1.2. *Let $p = 2$. For any positive integer k, the sum*

$$\sum_{P \in \mathcal{P}} \frac{1}{P^k - 1}$$

is in $\mathcal{K}$.

Proof. We rewrite the sum as $\sum_{P \in \mathcal{P}_1} \sum_{a \in \mathbb{F}_q^\times} 1/((aP)^k - 1)$. The corollary then follows from the identity

$$\sum_{a \in \mathbb{F}_q^\times} \frac{1}{(aX)^k - 1} = \frac{1}{X^{\mathrm{LCM}(k,q-1)} - 1}$$

in $\mathbb{F}_q(U)$. To prove this identity, write

$$\frac{1}{(aX)^k - 1} = \sum_{j=1}^{\infty} 1/(aX)^{kj}$$

and recall that

$$\sum_{a \in \mathbb{F}_q^\times} a^m = \begin{cases} 1, & m \equiv 0 \bmod q-1, \\ 0, & \text{otherwise.} \end{cases} \qquad \square$$

We now discuss the case of a general prime. Define the rational function $G_p(U)$ by

$$G_p(U) = \frac{(1-U^p)-(1-U)^p}{p(1-U)^p}.$$

When $p=2$, we have $G_2(U) = (2U-2U^2)/(2(1-U)^2) = U/(1-U)$, so $G_2(1/P) = 1/(P-1)$. When p is odd, we have the following alternate expressions for G_p:

Proposition 1.3. *If p is odd, then, as rational functions in $\mathbb{F}_p(U)$, we have*

$$G_p(U) = \frac{\sum_{j=1}^{p-1} U^j/j}{(1-U)^p} = \sum_{\substack{0\le j<\infty \\ j\not\equiv 0 \bmod p}} \frac{U^j}{j}.$$

Proof. If p is odd, then $(1-U^p)-(1-U)^p = \sum_{j=1}^{p-1}(-1)^{j-1}\binom{p}{j}U^j$. We have

$$\frac{(-1)^{j-1}}{p}\binom{p}{j} = \frac{(-1)^{j-1}(p-1)(p-2)\cdots(p-j+1)}{1\cdots 2\cdots (j-1)j} \equiv \frac{1}{j} \bmod p.$$

This proves the first equality, and the second is immediate. □

Theorem 1.4. *For any positive integer $k \equiv 0 \bmod q-1$, the sum*

$$\sum_{P\in\mathcal{P}_1} G_p(1/P^k)$$

is in $\mathcal{K}$.

As we noted, $G_2(1/X) = 1/(X-1)$, so Theorem 1.4 implies Theorem 1.1.

Remark 1.5. When $p=2$, we do *not* have $G_2(U) = \sum_{j\not\equiv 0 \bmod p} U^j/j$; the latter sum is $H(U) := U/(1-U^2)$. However, it is true that $\sum_{P\in\mathcal{P}_1} H(1/P^k)$ is in $\mathcal{K}$, because $H(U) = G(U) - G(U^2)$.

Once again, we have a trivial variant where we sum over $\mathcal{P}$:

Corollary 1.6. *For any positive integer k, the sum*

$$\sum_{P\in\mathcal{P}} G_p(1/P^k)$$

is in $\mathcal{K}$.

Proof. If $p=2$, we proved this in Corollary 1.2, so we may (and do) assume p is odd. As in the proof of Corollary 1.2, we rewrite the sum as $\sum_{P\in\mathcal{P}_1}\sum_{a\in\mathbb{F}_q^\times} G_p(1/(aP)^k)$. We now need the identity

$$\sum_{a\in\mathbb{F}_q^\times} G_p((aU)^k) = \mathrm{GCD}(q-1,k)G_p(U^{\mathrm{LCM}(q-1,k)})$$

in $\mathbb{F}_q(U)$. To prove this identity, we use the formula $G_p(U) = \sum_{j \not\equiv 0 \bmod p} U^j/j$ and the identity

$$\sum_{a \in \mathbb{F}_q^\times} a^m = \begin{cases} q-1, & m \equiv 0 \bmod q-1, \\ 0, & \text{otherwise.} \end{cases}$$

So

$$\sum_{a \in \mathbb{F}_q^\times} G_p(1/(aU)^k) = \sum_{j \not\equiv 0 \bmod p} \sum_{a \in \mathbb{F}_q^\times} \frac{1}{j(aU)^{kj}} = (q-1) \sum_{\substack{j \not\equiv 0 \bmod p \\ kj \equiv 0 \bmod q-1}} \frac{1}{jU^{kj}}.$$

Putting $kj = \mathrm{LCM}(q-1,k)\ell$, this is

$$\begin{aligned} (q-1) \sum_{\ell \not\equiv 0 \bmod p} & \frac{k}{\mathrm{LCM}(q-1,k)\ell\, U^{\mathrm{LCM}(q-1,k)\ell}} \\ &= \frac{k(q-1)}{\mathrm{LCM}(q-1,k)} G_p(U^{\mathrm{LCM}(q-1,k)}) \\ &= \mathrm{GCD}(q-1,k) G_p(U^{\mathrm{LCM}(q-1,k)}), \end{aligned}$$

as required. □

We also compute explicit values for the sum when k is not too large.

Theorem 1.7. *Let $k = (q-1)\ell$. If $1 \le \ell \le q/p$, then $\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = 0$. If $q/p + 1 < \ell \le 2q/p$, then*

$$\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = \ell \frac{(T^q - T)^{q+1}}{(T^{q^2} - T^q)(T^{q^2} - T)}.$$

In principle, our methods are capable of computing $\sum_{P \in \mathcal{P}_1} G_p(1/P^k)$ for any $k \equiv 0 \bmod q-1$, but they become impractical beyond $\ell = 2q/p$.

History of the problem. Dinesh Thakur suspected such relations should exist, based on heuristics concerning ζ deformation. He experimentally discovered most of the relations described above in characteristic two, and suspected there should be similar results in odd characteristic. Thakur [2015] published these computations in a preprint entitled "Surprising symmetries in distribution of prime polynomials". At Thakur's suggestion, Terence Tao [2015] promoted the problem in posts on his blog and on the Polymath blog. I am grateful to Thakur for finding such an elegant problem and to Tao for bringing it to my attention. My thanks also to all who participated in the discussion on the Polymath blog: Noam Elkies, Ian Finn, Ofir Gorodetsky, Jesse, Gil Kalai, David Lowry-Duda, Dustin G. Mixon, John Nicol, Partha Solapurkar, John Voight, Victor Wang, Qiaochu Yuan, Joshua Zelinsky, and additional thanks to Ofir Gorodetsky for suggesting several improvements to the manuscript.

The author is supported by NSF grant DMS-1600223.

2. The Carlitz exponential, and symmetric polynomials

The main tool in our proofs is the theory of the Carlitz exponential. Put

$$D_i = (T^{q^i} - T)(T^{q^i} - T^q)(T^{q^i} - T^{q^2}) \cdots (T^{q^i} - T^{q^{i-1}}).$$

Define

$$e_C(Z) = \sum_{j=0}^{\infty} \frac{Z^{q^j}}{D_j},$$

this sum is T^{-1}-adically convergent for any $Z \in \widehat{\mathcal{K}}$. We will make use of the product identity

$$\frac{e_C(\bar{\pi} Z)}{\bar{\pi} Z} = \prod_{A \in \mathcal{R} \setminus \{0\}} \left(1 + \frac{Z}{A}\right),$$

where $\bar{\pi} \in \widehat{\mathcal{K}}(\sqrt[q-1]{-T})$ is given by

$$\bar{\pi} = \frac{T \sqrt[q-1]{-T}}{\prod_{A \in \mathcal{R} \setminus \{0\}} (1 - (TA)^{-1})}.$$

See, for example, [Goss 1996, Theorem 3.2.8]. This identity should be thought of as similar to Euler's identity,

$$\frac{\sin(\pi z)}{\pi z} = \prod_{a \in \mathbb{Z} \setminus \{0\}} \left(1 + \frac{z}{a}\right).$$

We introduce the notations $\mathcal{A}$ for the nonzero polynomials of $\mathcal{R}$, and $\mathcal{A}_1$ for the monic polynomials.

Writing $\boldsymbol{e}_k$ for the elementary symmetric function of degree k, this implies

$$\boldsymbol{e}_k(1/A)_{A \in \mathcal{A}} = \begin{cases} \bar{\pi}^k / D_j, & k = q^j - 1, \\ 0, & \text{otherwise.} \end{cases}$$

Since the ring of symmetric polynomials is generated by the $\boldsymbol{e}_k$, we deduce:

Proposition 2.1. *If $\boldsymbol{f}$ is a homogenous symmetric polynomial of degree k, then $\boldsymbol{f}(1/A)_{A \in \mathcal{A}}$ is in $\bar{\pi}^k \mathcal{K}$.*

Here we note that $\boldsymbol{f}(1/A)_{A \in \mathcal{A}}$ is always defined, since only finitely many terms contribute to the coefficient of any particular power of T^{-1}.

The above considers symmetric polynomials in $\{1/A\}_{A \in \mathcal{A}}$, but we would rather restrict to the case of A monic. To this end, we have

Proposition 2.2.

$$\boldsymbol{e}_\ell(1/A^{q-1})_{A \in \mathcal{A}_1} = \begin{cases} (-1)^\ell \bar{\pi}^{\ell(q-1)} / D_j, & \ell = (q^j - 1)/(q - 1), \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. Grouping together scalar multiples of the same polynomial in the Carlitz product identity, we have

$$\frac{e_C(\bar{\pi} Z)}{\bar{\pi} Z} = \prod_{A \in \mathcal{A}_1} \Bigl(1 - \frac{Z^{q-1}}{A^{q-1}}\Bigr).$$

Equate coefficients of $Z^{\ell(q-1)}$ on both sides. □

Corollary 2.3. *If f is a homogenous symmetric polynomial of degree ℓ, then $f(1/A^{q-1})_{A \in \mathcal{A}_1}$ is in $\bar{\pi}^{\ell(q-1)}\mathcal{K}$.*

3. Proofs of rationality

We now have enough background to prove Theorem 1.4 and, hence, Theorem 1.1. Throughout, let $k \equiv 0 \bmod q-1$.

Consider the symmetric polynomial

$$g_p(X_1, X_2, \dots) := \frac{1}{p}\Bigl(\Bigl(\sum X_i\Bigr)^p - \sum X_i^p\Bigr).$$

The polynomial g_p has integer coefficients, so we may discuss plugging elements of $\mathcal{K}$ into it.

Let C be the cyclic group of order p, and let C act on $\mathcal{A}_1^p$ by rotating coordinates. Let Δ denote the diagonal: $\Delta := \{(A, A, \dots, A)\} \subset \mathcal{A}_1^p$. Then

$$g_p(1/A^k)_{A \in \mathcal{A}_1} = \sum_{(A_1, \dots, A_p) \in (\mathcal{A}_1^p \setminus \Delta)/C} \frac{1}{A_1^k A_2^k \cdots A_p^k}.$$

The sum is over cosets for the free action of C on $\mathcal{A}^p \setminus \Delta$.

Let

$$\Phi = \bigl\{(A_1, \dots, A_p) \in \mathcal{A}_1^p : \mathrm{GCD}(A_1, \dots, A_p) = 1\bigr\}.$$

Any $(A_1, \dots, A_p) \in \mathcal{A}_1^p$ can be uniquely factored as $A_i = DB_i$ for some $D \in \mathcal{A}_1$ and $(B_1, \dots, B_p) \in \Phi$. So we can factor the above sum as

$$g_p(1/A^k)_{A \in \mathcal{A}_1} = \Bigl(\sum_{D \in \mathcal{A}_1} \frac{1}{D^{kp}}\Bigr)\Bigl(\sum_{(B_1, \dots, B_p) \in (\Phi \setminus \{(1, \dots, 1)\})/C} \frac{1}{B_1^k B_2^k \cdots B_p^k}\Bigr).$$

Now, from Corollary 2.3, $g_p(1/A^k)_{A \in \mathcal{A}}$, is in $\bar{\pi}^{pk}\mathcal{K}$. Also from Corollary 2.3, $\sum_{D \in \mathcal{A}_1} 1/D^{kp}$ is in $\bar{\pi}^{pk}\mathcal{K}$, and a quick computation shows that this sum is 1 plus terms in $T^{-1}\mathbb{F}_q[\![T^{-1}]\!]$, so it is not zero. We deduce that

$$\sum_{(B_1, \dots, B_p) \in (\Phi \setminus (1, \dots, 1))/C} \frac{1}{B_1^k B_2^k \cdots B_p^k} \in \mathcal{K}.$$

For $B \in \mathcal{A}_1$, let $\Psi(B)$ be the set of p-tuples $(B_1, B_2, \dots, B_p)$ for which $\prod B_i = B$ and $\mathrm{GCD}(B_1, \dots, B_p) = 1$. Let $\psi(B) = \#\Psi(B)$. So we have shown that

$$\sum_{B \in \mathcal{A}_1 \setminus \{1\}} \frac{\psi(B)/p}{B^k} \in \mathcal{K}.$$

Here, to interpret the numerator, we must divide $\psi(B)$ by p as integers and only then consider the quotient in $\mathbb{F}_p$.

If $B = P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r}$ then there is an easy bijection between $\Psi(B)$ and $\Psi(P_1^{k_1}) \times \Psi(P_2^{k_2}) \times \cdots \times \Psi(P_r^{k_r})$, so $\psi(B) = \prod \psi(P_i^{k_i})$. If P is irreducible then $\psi(P^r)$ is divisible by p for any $r > 0$, since C acts freely on $\Psi(P^r)$. So, if B is divisible by two different irreducible polynomials, then $\psi(B)$ is divisible by p^2. So we can rewrite the sum as

$$\sum_{P \in \mathcal{P}_1} \sum_{r=1}^{\infty} \frac{\psi(P^r)/p}{P^{rk}}.$$

We now compute $\psi(P^r)$; which is the number of p-tuples $(P^{r_1}, \dots, P^{r_p})$ with $\prod P^{r_i} = P^r$ and $\mathrm{GCD}(P^{r_1}, \dots, P^{r_p}) = 1$. In other words, we must count $(r_1, \dots, r_p) \in \mathbb{Z}_{\geq 0}^p$ with $\sum r_i = r$ and $\min(r_1, \dots, r_p) = 0$. The number of $(r_1, \dots, r_p) \in \mathbb{Z}_{\geq 0}^p$ with $\sum r_i = r$ is the coefficient of U^r in $1/(1-U)^p$. In order to impose $\min(r_1, \dots, r_p) = 0$, we subtract off the terms with $\min(r_1, \dots, r_p) > 0$. These are in bijection with $(s_1, \dots, s_p) \in \mathbb{Z}_{\geq 0}^p$ with $p + \sum s_i = r$. So $\psi(P^r)$ is the coefficient of U^r in $1/(1-U)^p - U^p/(1-U)^p$. In other words, $\sum_{r=0}^{\infty} \psi(P^r) U^r = (1-U^p)/(1-U)^p$. So

$$\sum_{r=1}^{\infty} \frac{\psi(P^r)}{p} U^r = \frac{1}{p}\Big(\frac{1-U^p}{(1-U)^p} - 1\Big) = G_p(U).$$

We deduce that $\sum_{r=1}^{\infty} (\psi(P^r)/p)/P^{rk} = G_p(1/P^k)$. We have now shown that $\sum_{P \in \mathcal{P}_1} G_p(1/P^k) \in \mathcal{K}$, as claimed. □

We record the specific formula we have proved:

Proposition 3.1. *Let k be a positive integer. Then*

$$\sum_{P \in \mathcal{P}_1} G_p(1/P^k) = \frac{g_p(1/A^k)_{A \in \mathcal{A}_1}}{\sum_{A \in \mathcal{A}_1} 1/A^{pk}}.$$

We will rewrite this formula in various ways in Section 5. We remark that this formula is correct even if k is not divisible by $q-1$, although we have only shown the ratio is in $\mathcal{K}$ when $k \equiv 0 \bmod q-1$. The denominator of this formula is $\zeta(pk) = \zeta(k)^p$, where ζ is the Goss ζ-function [1979].

4. Vanishing

We will now prove the claim in Theorem 1.7 that the sum vanishes when $k = (q-1)\ell$ for $1 \leq \ell \leq q/p$. From Proposition 3.1, it is equivalent to show that $\boldsymbol{g}_p(1/A^{\ell(q-1)})_{A \in \mathcal{A}_1} = 0$. To this end, we must explicitly write $\boldsymbol{g}_p(1/A^{\ell(q-1)})$ as a polynomial in the $\boldsymbol{e}_k(1/A^{q-1})$.

The variables λ or μ will always denote partitions, meaning weakly decreasing sequences $(\lambda_1, \lambda_2, \dots, \lambda_r)$ of positive integers; sums over λ or μ implicitly contain the condition that the summation variable is a partition.

We define $\boldsymbol{e}_\lambda = \prod_s \boldsymbol{e}_{\lambda_s}$. The symmetric polynomials $\boldsymbol{e}_\lambda$ form an integer basis for the symmetric polynomials with integer coefficients.

Lemma 4.1. *Write*

$$\boldsymbol{g}_p(X_1^\ell, X_2^\ell, \dots) = \sum_{|\lambda| = p\ell} c_\lambda \boldsymbol{e}_\lambda(X_1, X_2, \dots)$$

for some integers c_λ. Then $c_{11\dots1} = 0$.

Proof. Note that $\boldsymbol{e}_{11\dots1}$ is the only $\boldsymbol{e}_\lambda$ with a nonzero coefficient of $X_1^{p\ell}$. The coefficient of $X_1^{p\ell}$ in $\boldsymbol{g}_p(X_1^\ell, X_2^\ell, \dots)$ is clearly 0. □

Now, suppose that $\ell \leq q/p$, so we have $p\ell < q+1$. So any partition $(\lambda_1, \dots, \lambda_r)$ of $p\ell$ other than $(1, 1, \dots, 1)$ contains a λ_i between 2 and q. By Proposition 2.2, $\boldsymbol{e}_m(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$ for $2 \leq m \leq q$, so $\boldsymbol{e}_\lambda(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$ whenever λ is a partition of $p\ell$ other than $(1, 1, \dots, 1)$. We deduce that $\boldsymbol{g}_p(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$ as desired. □

5. Computations for small *k*

In this section, we will discuss the computation of $\sum_{P \in \mathcal{P}_1} G_p(1/P^k)$ for $k \equiv 0 \bmod q-1$ and, in particular, prove the remaining half of Theorem 1.7. Our strategy is to combine Propositions 3.1 and 2.2. We must compute $\boldsymbol{g}_p(1/A^{\ell(q-1)})_{A \in \mathcal{A}_1}$ and $\sum_{A \in \mathcal{A}_1} 1/A^{pk}$. Note the latter is $(\boldsymbol{p}_\ell(1/A^{q-1})_{A \in \mathcal{A}_1})^p$, where $\boldsymbol{p}_d(X_1, X_2, \dots)$ is the power sum symmetric function $\sum X_i^d$. We write $k = (q-1)\ell$.

Put

$$\boldsymbol{g}_p(X_1^\ell, X_2^\ell, \dots) = \sum_{|\lambda| = \ell p} c_\lambda \boldsymbol{e}_\lambda(X_1, X_2, \dots),$$

$$\boldsymbol{p}_\ell(X_1, X_2, \dots) = \sum_{|\mu| = \ell} d_\mu \boldsymbol{e}_\mu(X_1, X_2, \dots).$$

Note that $\boldsymbol{e}_m(1/A^{q-1})_{A \in \mathcal{A}_1} = 0$ unless m is of the form $(q^j - 1)/(q-1)$. So we only need to sum over partitions where all the parts of λ are of the form $(q^j - 1)/(q-1)$.

From now on, we now impose that $q/p + 1 \leq \ell \leq 2q/p$. So $\ell < q+1$. Any partition of ℓ cannot contain any parts of size $(q^j - 1)/(q-1)$, for $j > 1$. Similarly,

$p\ell < 2q+2$, so a partition of $p\ell$ can contain at most one part of size $q+1 = (q^2-1)/(q-1)$ and no parts of size $(q^j-1)/(q-1)$ for $j > 2$. We deduce that the only terms which contribute to our final answer come from $\lambda = (1, 1, \dots, 1)$ or $\lambda = (q+1, 1, 1, \dots, 1)$ when computing $\boldsymbol{g}_p(1/A^{\ell(q-1)})_{A\in\mathcal{A}_1}$, and from $\mu = (1, 1, \dots, 1)$ in computing $(\boldsymbol{p}_\ell(1/A^{q-1})_{A\in\mathcal{A}_1})^p$. Moreover, from Lemma 4.1, the coefficient $c_{(1,1,\dots,1)}$ is zero.

We deduce that

$$\begin{aligned}\sum_{P\in\mathcal{P}_1} G_p(1/P^k) &= \frac{c_{(q+1,1^{p\ell-q-1})}\,\boldsymbol{e}_{(q+1,1^{p\ell-q-1})}(1/A^{q-1})_{A\in\mathcal{A}_1}}{(d_{1^\ell}\,\boldsymbol{e}_{1^\ell}\,(1/A^{q-1})_{A\in\mathcal{A}_1})^p}\\ &= \frac{c_{(q+1,1^{p\ell-q-1})}\,\boldsymbol{e}_{q+1}(1/A^{q-1})_{A\in\mathcal{A}_1}(\boldsymbol{e}_1(1/A^{q-1})_{A\in\mathcal{A}_1})^{p\ell-q-1}}{d_{1^\ell}\,(\boldsymbol{e}_1(1/A^{q-1})_{A\in\mathcal{A}_1})^{p\ell}}\\ &= \frac{c_{(q+1,1^{p\ell-q-1})}\,\boldsymbol{e}_{q+1}(1/A^{q-1})_{A\in\mathcal{A}_1}}{d_{1^\ell}\,(\boldsymbol{e}_1(1/A^{q-1})_{A\in\mathcal{A}_1})^{q+1}}.\end{aligned}$$

Here 1^r is shorthand for the partition with r parts equal to 1.

We now use Proposition 2.2. The powers of $\bar{\pi}$ and (-1) cancel to give

$$\sum_{P\in\mathcal{P}_1} G_p(1/P^k) = \frac{c_{(q+1,1^{p\ell-q-1})}}{d_{1^\ell}}\frac{D_1^{q+1}}{D_2} = \frac{c_{(q+1,1^{p\ell-q-1})}}{d_{1^\ell}}\frac{(T^q-T)^{q+1}}{(T^{q^2}-T^q)(T^{q^2}-T)}.$$

To finish the computation, we must find $c_{q+1,1^{ps-1}}$ and d_{1^ℓ}. The latter is easy: Comparing coefficients of X_1^ℓ on both sides of

$$\boldsymbol{p}_\ell(X_1, X_2, \dots) = \sum_{|\mu|=\ell} d_\mu \boldsymbol{e}_\mu(X_1, X_2, \dots),$$

we deduce that $d_{1^\ell} = 1$.

To compute $c_{(q+1,1^{p\ell-q-1})}$, we begin with the formula

$$\boldsymbol{g}_p(X_1^\ell, X_2^\ell, \dots) = \frac{1}{p}\big(\boldsymbol{p}_\ell(X_1, X_2, \dots,)^p - \boldsymbol{p}_{p\ell}(X_1, X_2, \dots)\big).$$

For brevity, we write $\boldsymbol{f}(X)$ to indicate that the inputs to a symmetric polynomial are $(X_1, X_2, \dots)$. Note that we are working with symmetric polynomials with integer coefficients, so it makes sense to divide by p.

We rewrite the right hand side of the previous equation as

$$\frac{1}{p}\Big(\big(\boldsymbol{e}_1(X)^\ell + \cdots\big)^p - \big(\boldsymbol{e}_1(X)^{p\ell} + d_{q+1,1^{p\ell-q-1}}\boldsymbol{e}_{q+1}(X)\boldsymbol{e}_1(X)^{p\ell-q-1} + \cdots\big)\Big).$$

Here the ellipses denote terms $\boldsymbol{e}_\lambda$ where λ has some part that is not of the form $(q^j-1)/(q-1)$. We deduce that

$$c_{q+1,1^{p\ell-q-1}} = -\frac{1}{p}d_{q+1,1^{p\ell-q-1}}.$$

Now, observe the identity

$$\sum_j \frac{(-1)^{j-1}\boldsymbol{p}_j(X)U^j}{j} = \sum_i \log(1+X_iU)$$
$$= \log\prod_i(1+X_iU) = \log\left(1+\sum_{m=1}^{\infty}\boldsymbol{e}_m(X)U^m\right).$$

The coefficient of $U^{p\ell}$ on the left is $((-1)^{p\ell}/p\ell)\boldsymbol{p}_{p\ell}$. Expanding the log on the right hand side as a Taylor series, only one term contributes to $U^{p\ell}\boldsymbol{e}_{q+1}\boldsymbol{e}_1^{p\ell-q-1}$. So we obtain

$$\frac{(-1)^{p\ell-1}}{p\ell}\boldsymbol{p}_{p\ell}(X) = \frac{(-1)^{p\ell-q-1}}{p\ell-q}\binom{p\ell-q}{1}\boldsymbol{e}_{q+1}(X)\boldsymbol{e}_1^{p\ell-q-1}(X)+\cdots,$$

where the ellipses denote a sum of $\boldsymbol{e}_\lambda$ other than $\boldsymbol{e}_{q+1}(X)\boldsymbol{e}_1^{p\ell-q-1}(X)$. So

$$d_{q+1,1^{p\ell-q-1}} = (-1)^q p\ell \quad \text{and} \quad c_{q+1,1^{ps-1}} = (-1)^{q-1}\ell.$$

Plugging into our previous formula, and using that $(-1)^{q-1} \equiv 1 \bmod p$,

$$\sum_{P\in\mathcal{P}_1} G_p(1/P^k) = \ell\frac{(T^q-T)^{q+1}}{(T^{q^2}-T^q)(T^{q^2}-T)}.$$

This concludes the proof of Theorem 1.7. □

We conclude by verifying one of Thakur's conjectures which goes beyond the range $\ell \le 2q/p$. Let $p=q=2$. Thakur conjectures

$$\sum_{P\in\mathcal{P}_1}\frac{1}{P^3-1} = \frac{1}{T^4+T^2}.$$

We begin by computing

$$\boldsymbol{p}_3(X) = \boldsymbol{e}_1(X)^3 + 3\boldsymbol{e}_3(X) - 3\boldsymbol{e}_2(X)\boldsymbol{e}_1(X),$$
$$\boldsymbol{p}_3(X)^2 = \boldsymbol{e}_1(X)^6 + 6\boldsymbol{e}_1(X)^3\boldsymbol{e}_3(X) + 9\boldsymbol{e}_3(X)^2 + \cdots.$$

Here and in the following equations, the ellipses denote $\boldsymbol{e}_\lambda$ terms where λ contains a part other than 1 and 3. (Note that $(2^3-1)/(2-1)=7$, too large to contribute to a symmetric polynomial of degree 6.) Similarly,

$$\boldsymbol{p}_6(X) = \boldsymbol{e}_1(X)^6 + 6\boldsymbol{e}_1(X)^3\boldsymbol{e}_3(X) + 3\boldsymbol{e}_3(X)^2 + \cdots.$$

So

$$\boldsymbol{g}_2(X_1^3, X_2^3, \ldots) = \tfrac{1}{2}\big(\boldsymbol{p}_3(X)^2 - \boldsymbol{p}_6(X)\big) = 3\boldsymbol{e}_3(X)^2 + \cdots$$

and (recall that we are working modulo 2)

$$\boldsymbol{g}_2(1/A^3)_{A\in\mathcal{A}_1} = (\boldsymbol{e}_3(1/A)_{A\in\mathcal{A}_1})^2 = \frac{\bar{\pi}^6}{D_2^2} = \frac{\bar{\pi}^6}{(T^4-T^2)^2(T^4-T)^2}.$$

Similarly,

$$\begin{aligned}\boldsymbol{p}_6(1/A)_{A\in\mathcal{A}_1} &= (\boldsymbol{e}_1(1/A)_{A\in\mathcal{A}_1})^6+(\boldsymbol{e}_3(1/A)_{A\in\mathcal{A}_1})^2\\ &= \Big(\frac{\bar{\pi}}{D_1}\Big)^6+\Big(\frac{\bar{\pi}^3}{D_2}\Big)^2\\ &= \bar{\pi}^6\Big(\Big(\frac{1}{T^2-T}\Big)^6+\Big(\frac{1}{(T^4-T^2)(T^4-T)}\Big)^2\Big).\end{aligned}$$

We verify Thakur's claim:

$$\sum_{P\in\mathcal{P}_1}\frac{1}{P^3-1}=\frac{1/\big((T^4-T^2)^2(T^4-T)^2\big)}{1/(T^2-T)^6+1/\big((T^4-T^2)^2(T^4-T)^2\big)}=\frac{1}{T^4+T^2}.$$

References

[Goss 1979] D. Goss, "v-adic zeta functions, L-series and measures for function fields", *Invent. Math.* **55**:2 (1979), 107–119. MR Zbl

[Goss 1996] D. Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik (3) **35**, Springer, 1996. MR Zbl

[Tao 2015] T. Tao, "Polymath proposal: explaining identities for irreducible polynomials", 2015, Available at https://polymathprojects.org/2015/12/28/.

[Thakur 2015] D. S. Thakur, "Surprising symmetries in distribution of prime polynomials", preprint, 2015. arXiv

Communicated by Kiran S. Kedlaya
Received 2016-10-17 Accepted 2017-04-03

speyer@umich.edu

Department of Mathematics, University of Michigan,
2844 East Hall, 530 Church Street,
Ann Arbor, MI 48109-1043, United States

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2017 is US $325/year for the electronic version, and $520/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 11 No. 5 2017

1937-0652(2017)11:5;1-G