PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 133, Number 10, Pages 2897–2902
S 0002-9939(05)08071-8
Article electronically published on April 25, 2005

THE POLYNOMIAL ANALOGUE OF A THEOREM OF RÉNYI

KENT E. MORRISON

(Communicated by David E. Rohrlich)

ABSTRACT. Rényi's result on the density of integers whose prime factorizations have excess multiplicity has an analogue for polynomials over a finite field.

Let $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the prime factorization of a positive integer n. Define the **excess** of n to be $(\alpha_1 - 1) + \cdots + (\alpha_r - 1)$, which is the difference between the total multiplicity $\alpha_1 + \cdots + \alpha_r$ and the number of distinct primes in the factorization. An integer with excess 0 is also said to be **square-free**. Let E_k denote the set of positive integers of excess k, $k = 0, 1, 2, \ldots$. Rényi proved that the set E_k has a density d_k and that the sequence $\{d_k\}$ has a generating function given by

$$\sum_{k \geq 0} d_k z^k = \prod_p \left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p - z}\right),$$

where the product extends over the primes. Recall that the density of a set of positive integers E is the limit (if it exists)

$$\lim_{n \to \infty} \frac{\#(E \cap \{1, 2, \ldots, n\})}{n},$$

which is the limiting probability that an integer from 1 to n is in E.

The set of square-free integers is E_0 and setting $z = 0$ in the generating function gives $d_0 = \prod_p (1 - 1/p^2)$, which is the well-known result that the density of square-free integers is $1/\zeta(2) = 6/\pi^2$. (This was first proved by Gegenbauer [2] in 1885. A clear, non-rigorous presentation is in [3].) By setting $z = 1$ one sees that $\sum_k d_k = 1$, so that the density is countably additive on the specific partition of $\mathbf{Z}^+$ given by the E_k. Rényi's proof appeared in [7], but an alternative proof was given by Kac in [4, pp. 64–71].

The aim of this paper is to derive an analogue of the generating function for polynomials in one variable over a finite field. Let $\mathbf{F}_q$ be the field with q elements and let $\mathbf{F}_q[x]$ be the polynomial ring. The prime elements of $\mathbf{F}_q[x]$ are the irreducible monic polynomials. Let f be a monic polynomial with prime factorization $f = \pi_1^{\alpha_1} \cdots \pi_r^{\alpha_r}$, and define the excess of f to be $(\alpha_1 - 1) + \cdots + (\alpha_r - 1)$, just as for an integer. Let $e_{n,k}$ be the number of monic polynomials of degree n and excess k. Define

$$d_{n,k} = \frac{e_{n,k}}{q^n},$$

Received by the editors June 9, 2004.
2000 *Mathematics Subject Classification.* Primary 11T06; Secondary 11T55, 05A16.

which is the probability that a monic polynomial of degree n has excess k. Note that $d_{0,k} = 0$ for $k > 0$. Then define the analogue of the density to be the limiting "probability" as the degree goes to infinity:

$$d_k = \lim_{n\to\infty} d_{n,k}.$$

Define $D(z) = \sum_{k\geq 0} d_k z^k$ to be the ordinary power series generating function of the sequence $\{d_k\}$. Let $\mathrm{N}f = q^{\deg f}$ be the norm of the polynomial f, which is the cardinality of the residue ring $\mathbf{F}_q[x]/(f)$. The main result of this paper is the following theorem concerning $D(z)$.

Theorem 1. *The generating function $D(z)$ has a factorization over the prime polynomials given by*

$$D(z) = \prod_{\pi} \left(1 - \frac{1}{\mathrm{N}\pi}\right)\left(1 + \frac{1}{\mathrm{N}\pi - z}\right).$$

Proof. We begin with the geometric series

$$\frac{1}{1-qt} = \sum_{n\geq 0} q^n t^n,$$

which is the generating function for the number of monic polynomials of degree n. Then unique factorization in $\mathbf{F}_q[x]$ allows us to factor the generating function formally:

$$\begin{aligned} \frac{1}{1-qt} &= \prod_{\pi}\sum_{j\geq 0} t^{j\deg\pi} \\ &= \prod_{\pi} \frac{1}{1-t^{\deg\pi}}. \end{aligned} \tag{1}$$

By grouping the primes of the same degree and letting ν_i denote the number of primes of degree i, we can rewrite the last line above as

$$\frac{1}{1-qt} = \prod_{i\geq 1}\left(\frac{1}{1-t^i}\right)^{\nu_i}.$$

From this it follows that

$$1 - qt = \prod_{i\geq 1}\left(1-t^i\right)^{\nu_i} \tag{2}$$

as a formal power series. In the product on the right there is a finite number of terms for each power of t so that the coefficients make sense. In fact, the coefficient of t^n is 0 except for $n = 0, 1$. However, considered as a function of a complex variable t, the product does not converge for all t. It does converges absolutely for $|t| < 1/q$. This follows from consideration of the series $\sum \nu_i t^i$ and the fact that ν_i is asymptotic to q^i/i.

Next we define the two-variable generating function

$$E(t,z) = \sum_{n,k} e_{n,k} t^n z^k.$$

Modifying the factorization in (1), we see that

$$E(t,z) = \prod_{\pi}(1 + t^{\deg\pi} + t^{2\deg\pi}z + \cdots + t^{j\deg\pi}z^{j-1} + \cdots).$$

Note that the variable z appears with a power that is equal to the excess multiplicity. That is, if $f = \pi_1^{\alpha_1} \cdots \pi_r^{\alpha_r}$, then the product expansion of $E(t,z)$ has a term of the form $t^{\alpha_1 \deg \pi_1} \cdots t^{\alpha_r \deg \pi_r} z^{\alpha_1 - 1} \cdots z^{\alpha_r - 1}$. Sum the geometric series in each factor to obtain the formal factorization

$$E(t,z) = \prod_{\pi} \left(1 + \frac{t^{\deg \pi}}{1 - t^{\deg \pi} z}\right).$$

Group the irreducibles by degree to get

$$E(t,z) = \prod_{i} \left(1 + \frac{t^i}{1 - t^i z}\right)^{\nu_i}. \tag{3}$$

Now the product on the right converges absolutely if and only if the series

$$\sum_{i \geq 1} \nu_i \left| \frac{t^i}{1 - t^i z} \right| \tag{4}$$

converges. We claim that (4) converges for $|t| < 1/q$ and $|z| < q$, because the denominators $|1 - t^i z|$ are bounded away from 0 and ν_i is asymptotic to q^i/i. (Actually, it suffices that $\nu_i < q^i$.)

From (2) and (3) we get

$$(1 - qt)E(t,z) = \prod_{i \geq 1} \left(1 - t^i\right)^{\nu_i} \prod_{i \geq 1} \left(1 + \frac{t^i}{1 - t^i z}\right)^{\nu_i}.$$

On the domain where both products converge absolutely, we can combine the factors for each i to get

$$(1 - qt)E(t,z) = \prod_{i \geq 1} \left(1 - t^i\right)^{\nu_i} \left(1 + \frac{t^i}{1 - t^i z}\right)^{\nu_i}. \tag{5}$$

By multiplying the factors together we can see that the absolute convergence of the infinite product depends on the convergence of the series

$$\sum_{i} \nu_i \left| \frac{t^{2i} z - t^{2i}}{1 - t^i z} \right|.$$

Then reasoning along the same lines as before, we see that this series converges for $|t^2| < q$ and $|z| < \sqrt{q}$. In particular, the product converges for $t = 1/q$, and so after carrying out the multiplication of the left side of (5) we arrive at

$$\sum_{n,k} (e_{n,k} - q e_{n-1,k}) t^n z^k = \prod_{i \geq 1} \left(1 - t^i\right)^{\nu_i} \left(1 + \frac{t^i}{1 - t^i z}\right)^{\nu_i}.$$

We evaluate this at $t = 1/q$ to get

$$\sum_{n,k} (e_{n,k} - q e_{n-1,k}) (1/q)^n z^k = \prod_{i \geq 1} \left(1 - (1/q)^i\right)^{\nu_i} \left(1 + \frac{(1/q)^i}{1 - (1/q)^i z}\right)^{\nu_i}.$$

The coefficient of z^k is the sum $\sum_{n \geq 1} (e_{n,k}/q^n - e_{n-1,k}/q^{n-1})$. This telescopes to give

$$\lim_{n \to \infty} \frac{e_{n,k}}{q^n} = \lim_{n \to \infty} d_{n,k},$$

which is the definition of d_k, and so we have

$$D(z) = \sum_k d_k z^k = \prod_{i\geq 1} \left(1-(1/q)^i\right)^{\nu_i} \left(1+\frac{(1/q)^i}{1-(1/q)^i z}\right)^{\nu_i}.$$

Finally, we write the product by indexing over the prime polynomials π and note that the norm of π is $\mathrm{N}\pi = q^{\deg \pi}$. With this we have the generating function for d_k in the form that is most directly analogous to Rényi's theorem:

$$\begin{aligned} D(z) &= \prod_\pi \left(1-(1/q)^{\deg \pi}\right)\left(1+\frac{(1/q)^{\deg \pi}}{1-(1/q)^{\deg \pi} z}\right) \\ &= \prod_\pi \left(1-\frac{1}{\mathrm{N}\pi}\right)\left(1+\frac{1}{\mathrm{N}\pi - z}\right). \end{aligned}$$

□

The coefficient d_0 is the limiting "probability" that a monic polynomial is square-free. To develop the analogy with the density of the square-free integers given by d_0 in Rényi's generating function, we use the zeta function of $\mathbf{F}_q[x]$ (i.e. the zeta function of the affine line over $\mathbf{F}_q$)

$$\zeta(s) = \frac{1}{1-q^{-s}},$$

which immediately comes from the definition

$$\zeta(s) = \sum_{\mathfrak{a}} \frac{1}{(\mathrm{N}\mathfrak{a})^s},$$

where the sum is over all ideals of $\mathbf{F}_q[x]$ and the norm $\mathrm{N}\mathfrak{a}$ is the cardinality of the residue ring $\mathbf{F}_q[x]/\mathfrak{a}$. It has a factorization over the prime ideals (i.e. irreducible polynomials)

$$\begin{aligned} \zeta(s) &= \prod_\pi \frac{1}{1-(\mathrm{N}\pi)^{-s}} \\ &= \prod_{i\geq 1} \left(\frac{1}{1-q^{-is}}\right)^{\nu_i}. \end{aligned}$$

Corollary 1. $d_0 = \frac{1}{\zeta(2)} = 1 - \frac{1}{q}$.

Proof. We have

$$d_0 = D(0) = \prod_{i\geq 1} \left(1-\frac{1}{q^{2i}}\right)^{\nu_i}.$$

Then in (2) we may let $t = 1/q^2$, because the product converges for $|t| < 1/q$, to obtain

$$1-\frac{1}{q} = \prod_{i\geq 1} \left(1-\frac{1}{q^{2i}}\right)^{\nu_i}.$$

Note that the product is $1/\zeta(2)$. □

Corollary 1 can be obtained as a special case of much more general results on square-free values of polynomials in one or more variables from the work of Ramsay [6] and Poonen [5]. It turns out that for $n \geq 2$, the value of $d_{n,0}$ is $1-1/q$. This can

be seen by finding the coefficients $e_{n,0}$, which count the number of monic, square-free polynomials of degree n. These polynomials can be counted directly; see, for example, [1].

Corollary 2. *The number of square-free monic polynomials of degree $n \geq 2$ is $q^n - q^{n-1}$.*

Proof. The generating function $\sum_{n\geq 0} e_{n,0}t^n = E(t,0)$. From (3) we see that

$$E(t,0) = \prod_{i\geq 1}(1+t^i)^{\nu_i}.$$

Using (2) we see that

$$\begin{aligned} E(t,0)(1-qt) &= \prod_{i\geq 1}(1+t^i)^{\nu_i}(1-t^i)^{\nu_i} \\ &= \prod_{i\geq 1}(1-t^{2i})^{\nu_i} \\ &= 1-qt^2. \end{aligned}$$

Therefore,

$$E(t,0) = \frac{1-qt^2}{1-qt},$$

from which it follows that $e_{n,0} = q^n - q^{n-1}$ for $n \geq 2$. □

From the expression

$$D(z) = \prod_{i\geq 1}\left(1-\frac{1}{q^i}\right)^{\nu_i}\left(1+\frac{1}{q^i-z}\right)^{\nu_i}$$

we can see that $D(z)$ has poles at $z = q^i$ of multiplicity ν_i. In particular the pole at $z = q$ has multiplicity $q-1$. Elementary analysis of the singularity there, along the lines of Kac [4] in his discussion of Rényi's result, enables us to describe the asymptotic behavior of the d_k as $k \to \infty$.

Corollary 3. *As k goes to infinity, d_k is asymptotic to*

$$A\frac{k^{q-2}}{q^k},$$

where the constant A is given by

$$A = \frac{1}{(q-2)!}\left(\frac{1}{q}-\frac{1}{q^2}\right)^{q-1}\prod_{i\geq 2}\left(1-\frac{1}{q^i}\right)^{\nu_i}\left(1-\frac{1}{q^i-q}\right)^{\nu_i}.$$

One may contrast this asymptotic result with the classical case of Rényi. Although the generating functions have clearly analogous form, the generating function for the number-theoretic version has only a simple pole $z = 2$, which is the pole of smallest absolute value. The asymptotic analysis shows that

$$d_k \sim \frac{\delta}{2^k},$$

where

$$\delta = \frac{1}{4}\prod_{p\geq 3}\frac{(p-1)^2}{p(p-2)}.$$

The referee has observed that Theorem 1 of this article can be extended naturally to function fields over finite fields by using S-zeta functions and their residues at $t = 1/q$. Let K be a function field over the constant field $\mathbf{F}_q$. Let S be a finite, non-empty set of places on K and let $\mathcal{O}_{K,S}$ denote the ring of S-integers of K. Then for every integer $k \geq 0$, the density $d_{k,S}$ of ideals in $\mathcal{O}_{K,S}$ with excess k exists, and the following analytic identity holds:

$$\sum_{k\geq 0} d_k z^k = \prod_{v\notin S}\left(1-\frac{1}{\mathrm{N}v}\right)\left(1+\frac{1}{\mathrm{N}v-z}\right),$$

where for each place v on K the norm $\mathrm{N}v = q^{\deg v}$ is the cardinality of the residue field at v.

Finally, the referee has pointed out that by generalizing Kac's proof of Rényi's theorem [4, pp. 64–71], there should also be an analogue of the theorem for the density of ideals with excess k in the ring of algebraic integers (or ring of S-integers) of any number field.

References

[1] L. Carlitz. An application of a theorem of Stickelberger, *Simon Stevin* **31** (1956) 27–30. MR0080696 (18:285g)

[2] L. Gegenbauer. Asymptotische Gesetze der Zahlentheorie, *Denkshcriften Akad. Wien* **49** (1885) 37–80.

[3] G. A. Jones. $6/\pi^2$, *Mathematics Magazine* **66** (1993) 290–298. MR1251442 (94m:11002)

[4] M. Kac. *Statistical Independence in Probability, Analysis and Number Theory.* Carus Monographs, no. 12. Mathematical Association of America, Washington, D.C., 1959. MR0110114 (22:996)

[5] B. Poonen. Squarefree values of multivariable polynomials, *Duke Math. J.* **118** (2003), no. 2, 353–373. MR1980998 (2004d:11094)

[6] K. Ramsay. Square-free values of polynomials in one variable over function fields, *Internat. Math. Res. Notices*, no. 4 (1992) 97–102. MR1159451 (93b:11115)

[7] A. Rényi. On the density of certain sequences of integers, *Acad. Serbe Sci. Publ. Inst. Math.* **8** (1955), 157–162. MR0076787 (17,944f)

Department of Mathematics, California Polytechnic State University, San Luis Obispo, California 93407

E-mail address: kmorriso@calpoly.edu