Probabilistic Aspects of the Integer-Polynomial Analogy

Kent E. Morrison
Department of Mathematics
California Polytechnic State University
San Luis Obispo, CA 93407
kmorriso@calpoly.edu

Zhou Dong *
Department of Mathematics
University of Illinois
Urbana, IL 61801
zhoudong@math.uiuc.edu

July 9, 2004

1 Introduction

Consider these remarkable facts about the integers:

1. The probability that an integer between 1 and n is prime is asymptotic to $1/\log n$.
2. The probability that two integers are relatively prime is $6/\pi^2$.
3. The probability that an integer is square-free is $6/\pi^2$.

These are classical results from the last quarter of the nineteenth century. The first, of course, is an informal statement of the Prime Number Theorem, which was proved independently in 1895 by Hadamard and de la Vallée Poussin. The second is due to Mertens in 1874 and the third is credited to Gegenbauer in 1885. In fact, Gegenbauer proved the more general result that the probability an integer is not divisible by an rth power, $r \geq 2$, is

*Partially supported by NSF Grant DMS-0097392

$1/\zeta(r)$. And, as is well known, thanks to Euler, $1/\zeta(2) = 6/\pi^2$. In 1900 D. N. Lehmer extended Mertens's result to show that the probability that r random integers are relatively prime is also $1/\zeta(r)$. The last word so far appears to be the theorem of Benkoski in 1976 that combines both threads by showing that the probability that k integers do not have a common rth power factor is $1/\zeta(kr)$.

For an account of the earlier results along with historical notes an excellent source is Hardy and Wright [5]. A short, accessible proof for the square-free probability is given by Nymann [10]. Lehmer's result appears in [8] and a more recent proof in Nymann [9]. Benkoski's unified generalization appears in [1].

In this paper we consider the analogues of these number theoretical results by replacing the ring of integers with the ring of polynomials over a finite field. Like the integers the polynomial ring is a principal ideal domain whose prime elements are the monic, irreducible polynomials. For simplicity we will refer to these polynomials as "prime." Since our focus will be on the analogues of the relatively prime and the square-free probabilities and their generalizations, we briefly mention the analogue of the Prime Number Theorem. Let q be a prime power and $\mathbf{F}_q$ the finite field of order q. Then the number of prime polynomials of degree n is given by

$$\frac{1}{n}\sum_{d|n}\mu(n/d)q^d,$$

where the sum is over divisors of n and μ is the Möbius function. This theorem was first proved by Gauss in the case q is prime. The probabilistic equivalent of our first classical result is that the probability that a monic polynomial of degree n is prime is asymptotic to $1/n$.

In the remainder of this article we consider the polynomial analogues of the other results. In section 2 we find the probability that r monic polynomials of degree n are relatively prime, and in section 3 we find the probability that a monic polynomial of degree n is not divisible by an rth power. In section 4 we unify both results into an analogue of Benkoski's theorem [1]. In section 5 we show that these probabilities are values of a zeta function for polynomials.

There are other problems and results from number theory with polynomial analogues that we do not examine in this paper. These include Goldbach's Conjecture, the twin-prime conjecture, The Waring problem, and the 3-primes theorem. The interested reader may consult Effinger and Hayes [4] for the polynomial analogues and Hardy and Wright [5] for the classical

results and history. Finally, we should mention that the probabilities for relatively prime integers and for square-free integers may also be considered for the Gaussian integers and for other rings of algebraic integers. In [2] Collins and Johnson determine the probability that two Gaussian integers are relatively prime in terms of a zeta function.

2 Relatively prime polynomials

Polynomials f and g in $\mathbf{F}_q[x]$ are **relatively prime** if they have no common factor of positive degree. Alternatively, the smallest ideal containing both f and g is all of $\mathbf{F}_q[x]$. Define the greatest common divisor of f and g, denoted $\gcd(f, g)$, to be the unique monic polynomial that generates the ideal generated by f and g. Extend these definitions to more than two polynomials. The greatest common divisor of $f_1, \ldots, f_r$ is the unique monic polynomial that generates the ideal generated by $f_1, \ldots, f_r$. (Such a unique polynomial exists because $\mathbf{F}_q[x]$ is a principal ideal domain.) It is no more difficult to count the relatively prime r-tuples than the relatively prime pairs.

Theorem 1 *Let a_n be the number of r-tuples of monic polynomials of degree n over the field $\mathbf{F}_q$ whose greatest common divisor is 1. Then for $n \geq 1$*

$$a_n = q^{rn} - q^{rn-r+1}.$$

Proof We partition the q^{rn} r-tuples of monic polynomials of degree n into subsets according to the degree k of their greatest common divisor. If $\gcd(f_1, \ldots, f_r) = h$ and $\deg h = k$, then $(f_1/h, \ldots, f_r/h)$ is a relatively prime tuple of polynomials of degree $n - k$. Thus, the number of tuples with a gcd of degree k is $q^k a_{n-k}$, the product of the number of monic polynomials of degree k and the number of relatively prime r-tuples of degree $n - k$. From this we obtain the recursion formula

$$q^{rn} = \sum_{k=0}^{n} q^k a_{n-k}.$$

We construct a generating function in order to solve this recursion. Multiply both sides by t^n and sum over n:

$$\begin{aligned}\sum_{n=0}^{\infty} q^{rn} t^n &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} q^k a_{n-k} t^n \\ &= \sum_{k=0}^{\infty} q^k t^k \sum_{m=0}^{\infty} a_m t^m \\ &= (1-qt)^{-1} \sum_{m=0}^{\infty} a_m t^m.\end{aligned}$$

Therefore,

$$\sum_{n=0}^{\infty} a_n t^n = (1-qt) \sum_{n=0}^{\infty} q^{rn} t^n. \tag{1}$$

Equating coefficients of t^n shows that

$$a_n = q^{rn} - q^{rn-r+1}.$$

□

Corollary 2 *The probability that r monic polynomials of degree n are relatively prime is $1 - 1/q^{r-1}$.*

Proof The probability is a_n/q^{rn}. □

Setting $r = 2$ gives the probability of $1-1/q$ that two monic polynomials of the same degree are relatively prime, which is the analogue of $6/\pi^2$ for integers.

Counting the number of relatively prime tuples of polynomials can be seen as an example in a more general setting of *prefabs*, which are combinatorial families in which each object uniquely decomposes into prime objects. In [3] this more general approach is worked out and the polynomials are given as one example. The authors remark that for polynomials over $\mathbf{F}_2$, there are just as many relatively prime pairs of degree n as non-relatively prime pairs, and they ask for a simple bijection to demonstrate that result. In [11] a bijection is given, although it is not especially simple.

3 Square-free polynomials, cube-free polynomials, and so on

A polynomial f is **square-free** if it is not divisible by the square of a polynomial of positive degree. Alternatively, the prime factorization of f has

no repeated factors. Generalizing this, we can fix a positive integer $r \geq 2$ and consider the polynomials not divisible by any rth power of a polynomial of positive degree. Alternatively, these are the polynomials whose prime factorization has no factors of multiplicity r or more.

Theorem 3 *Fix $r \geq 2$ and let b_n be the number of monic polynomials of degree n not divisible by an rth power. Then*

$$b_n = \begin{cases} q^n & 0 \leq n \leq r-1 \\ q^n - q^{n-r+1} & n \geq r \end{cases}$$

Proof Clearly, $b_n = q^n$ for $n = 0, 1, \ldots, r-1$ because the lowest degree of an rth power is r. For $n \geq r$ partition the q^n monic polynomials of degree n according to the degree k of their maximal factor that is an rth power. That is, factor f as $f = h^r f_0$, where $\deg h = k$ and f_0, which has degree $n - rk$, is not divisible by any rth power. From this partition we get the recursion

$$q^n = \sum_{k \geq 0} q^k b_{n-rk}.$$

Multiply both sides by t^n and sum over n. Then let $m = n - rk$ and change the order of summation:

$$\begin{aligned} \sum_{n=0}^{\infty} q^n t^n &= \sum_{n=0}^{\infty} \sum_{k \geq 0} q^k b_{n-rk} t^n \\ &= \sum_{k=0}^{\infty} q^k t^{rk} \sum_{m=0}^{\infty} b_m t^m \\ &= (1 - qt^r)^{-1} \sum_{m=0}^{\infty} b_m t^m \end{aligned}$$

Therefore,

$$\sum_{n=0}^{\infty} b_n t^n = (1 - qt^r) \sum_{n=0}^{\infty} q^n t^n \tag{2}$$

Comparing the coefficients of t^n gives the formula for b_n. □

Corollary 4 *The probability that a monic polynomial of degree $n \geq r$ is not divisible by an rth power is $1 - 1/q^{r-1}$.*

Proof The probability in question is b_n/q^n. □

Taking $r = 2$ we see that the probability that a polynomial is square-free is $1 - 1/q$. Furthermore, taking $q = 2$ we see that among the monic polynomials of degree n half of them are square-free and half of them are not. We wonder whether there is a natural bijection between the two sets.

4 m-tuples with no common rth power factors

Fix positive integers m and r. We will count the number of m-tuples of monic polynomials of degree n with no common rth power factor. When $r = 1$ we are counting m-tuples of relatively prime polynomials, and when $m = 1$ we are counting the polynomials not divisible by an rth power.

Theorem 5 *Let c_n be the number of m-tuples $(f_1, \ldots, f_m)$ of monic polynomials of degree n such that there is no common factor of the form h^r with $\deg h > 0$. Then*

$$c_n = \begin{cases} q^{mn} & 0 \le n \le r-1 \\ q^{mn} - q^{mn-mr+1} & n \ge r \end{cases}.$$

Proof Partition the q^{mn} m-tuples $(f_1, \ldots, f_m)$ into subsets according to the degree k of the monic polynomial h where h^r is the greatest common rth power divisor. Then $(f_1/h^r, \ldots, f_m/h^r)$ is a tuple with no common rth power divisors. There are c_{n-kr} such m-tuples. Therefore,

$$q^{mn} = \sum_{k \ge 0} q^k a_{n-kr}.$$

We construct the generating function and change indices by letting $j = n - kr$:

$$\begin{aligned} \sum_{n \ge 0} q^{mn} t^n &= \sum_{n \ge 0} \sum_{k \ge 0} q^k c_{n-kr} t^n \\ &= \sum_{n \ge 0} \sum_{k \ge 0} q^k t^{kr} c_{n-kr} t^{n-kr} \\ &= \sum_{j \ge 0} \sum_{k \ge 0} q^k t^{kr} c_j t^j \\ &= \sum_{j \ge 0} c_j t^j \sum_{k \ge 0} q^k t^{kr} \end{aligned}$$

From this we see that

$$\sum_{n \ge 0} c_n t^n = (1 - qt^r) \sum_{n \ge 0} q^{mn} t^n.$$

Comparing the coefficients of t^n gives the formula.

5 Zeta functions

The Riemann zeta function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

has a factorization over the primes

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

which can be seen by expanding each factor as a geometric series and using the Fundamental Theorem of Arithmetic to see that the term n^{-s} occurs exactly once.

Consider this heuristic derivation of the probability that two integers are relatively prime. For a fixed prime p the probability that an integer is divisible by p is $1/p$. Selecting two integers independently, the probability that both are divisible by p is $1/p^2$, and so the probability that p does not divide both is $1 - 1/p^2$. Now for integers to be relatively prime it must be that for all primes p, it is not the case that p divides both. Therefore, treating the events as independent for distinct primes, we conclude that the probability of being relatively prime is the product over all primes

$$\prod_p \left(1 - \frac{1}{p^2}\right),$$

which is $1/\zeta(2)$ using the product representation above. The same heuristic gives the probability that r integers are relatively prime as

$$\prod_p \left(1 - \frac{1}{p^r}\right) = \frac{1}{\zeta(r)}.$$

In a similar manner the probability that an integer is not divisible by p^r is $(1 - 1/p^r)$ and so the probability that an integer is not divisible by any rth power is the product over all primes of $(1 - 1/p^r)$, which is again $1/\zeta(r)$.

Now we apply the analogous heuristics to $\mathbf{F}_q[x]$. Let ϕ be a prime polynomial of degree d. Among the q^n monic polynomials of degree n, assuming $n \geq d$, there are q^{n-d} divisible by ϕ. Thus, the probability that a polynomial is divisible by ϕ is $1/q^d$, and the probability that a polynomial is not

divisible by ϕ is $1-1/q^d$. Then we would expect the probability that r polynomials are relatively prime, as well as the probability that a polynomial is not divisible by an rth power, is the product over all prime polynomials

$$\prod_{\phi}\left(1-\frac{1}{q^{r\deg\phi}}\right).$$

Now take the reciprocal of this product and expand each factor as a geometric series

$$\prod_{\phi}\left(1-\frac{1}{q^{r\deg\phi}}\right)^{-1}=\prod_{\phi}\left(1+\frac{1}{q^{r\deg\phi}}+\frac{1}{q^{2r\deg\phi}}+\cdots\right)$$

In the full expansion of the product, there is exactly one term of the form $1/q^{rn}$ for each monic polynomial of degree n because of unique factorization. Hence

$$\prod_{\phi}\left(1-\frac{1}{q^{r\deg\phi}}\right)^{-1}=\sum_{n=0}^{\infty}\frac{q^n}{q^{rn}}=\frac{1}{1-q^{1-r}}. \tag{3}$$

This function $1/(1-q^{1-r})$, then, is the analogue of the Riemann zeta function, but it has a compact closed form while the original one does not.

Make the substitution $t=q^{-r}$ in (3) to see that the ordinary generating function for the number of monic polynomials of degree n is

$$\frac{1}{1-qt}=\prod_{\phi}\left(1-t^{\deg\phi}\right)^{-1}. \tag{4}$$

Now we can use this to rediscover the generating function for the number of monic polynomials not divisible by an rth power. In (4) write each factor as a geometric series to see that

$$\frac{1}{1-qt}=\prod_{\phi}\left(1+t^{\deg\phi}+t^{2\deg\phi}+\cdots\right) \tag{5}$$

On the right side we eliminate all the terms of the form $t^{k\deg\phi}$, where $k\geq r$, so that when everything is multiplied we get only terms t^n corresponding to monic polynomials of degree n whose prime factors occur with multiplicity less than r. Let b_n be the number of such degree n monic polynomials. We have shown that

$$\sum_{n=0}^{\infty}b_nt^n=\prod_{\phi}\left(1+t^{\deg\phi}+t^{2\deg\phi}+\cdots+t^{(r-1)\deg\phi}\right).$$

Therefore,

$$\begin{aligned}\sum_{n=0}^{\infty} b_n t^n &= \prod_{\phi} \frac{1-t^{r\deg\phi}}{1-t^{\deg\phi}} \\ &= \frac{\prod_{\phi}(1-t^{r\deg\phi})}{\prod_{\phi}(1-t^{\deg\phi})}.\end{aligned}$$

Using (4) for both the numerator and the denominator we have

$$\sum_{n=0}^{\infty} b_n t^n = \frac{1-qt^r}{1-qt},$$

which is the generating function in (2).

From (1) we see that the closed form for the generating function for the number of relatively prime r-tuples is

$$\sum_{n=0}^{\infty} a_n t^n = \frac{1-qt}{1-q^r t}.$$

The generating function for the number of m-tuples with no common rth power factors is

$$\sum_{n\geq 0} c_n t^n = \frac{1-qt^r}{1-q^m t}.$$

References

[1] S. J. Benkoski, The probability that k positive integers are relatively r-prime, *J. Number Theory* **8** (1976) 218–223.

[2] G. E. Collins and J. R. Johnson, The probability of relative primality of Gaussian integers. Symbolic and algebraic computation (Rome, 1988), 252–258, Lecture Notes in Comput. Sci., **358**, Springer, Berlin, 1989.

[3] S. Corteel, C. D. Savage, H. S. Wilf, and D. Zeilberger, A pentagonal number sieve, *J. Combin. Theory Ser. A* **82** (1998) 186–192.

[4] G. W. Effinger and D. R. Hayes, *Additive Number Theory of Polynomials Over a Finite Field*. Oxford Univ. Press, Oxford, 1991.

[5] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition. Oxford Univ. Press, Oxford, 1979.

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

[7] M. Kac, *Statistical Independence in Probability, Analysis and Number Theory.* Carus Monographs, no. 12. Mathematical Association of America, Washington, D.C., 1959.

[8] D. N. Lehmer, Asymptotic evaluation of certain totient sums. *Amer. J. Math.* **22** (1900) 293–335.

[9] J. E. Nymann, On the probability that k positive integers are relatively prime. J. Number Theory **4** (1972) 469–473.

[10] J. E. Nymann, A note concerning the square-free integers. *Amer. Math. Monthly* **79** (1972) 63–65.

[11] A. Riefegerste, On an involution concerning pairs of polynomials over $\mathbf{F}_2$, *J. Combin. Theory Ser. A* **90** (2000) 216–220.