

Random Polynomials over Finite Fields

Kent E. Morrison

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

November 9, 1999

1 Probability on Polynomials

Flip a coin to select a random polynomial over \mathbf{F}_2 . The sequence HTHHHTH, for example, corresponds to the sequence 1011101 or to the polynomial $1 + x^2 + x^3 + x^4 + x^6$. Do it again to get another random polynomial. What are the chances that the two polynomials are coprime?

We present some data. Consider sequences of length 3, which means polynomials of degree 2 or less. There are 64 pairs of such polynomials. Two polynomials f and g are coprime if and only if their greatest common divisor is 1, and we define the gcd of f and g to be the unique monic polynomial that generates the ideal generated by f and g . (Over \mathbf{F}_2 it is unnecessary to specify ‘monic.’). Thus, over \mathbf{F}_2 $\gcd(0, f) = f$ and so 0 is coprime only to 1 and to no other polynomial. In general the gcd of 0 and f is the unique monic polynomial that is a scalar multiple of f , and 0 is coprime to the non-zero constant polynomials. In the table below an asterisk means the corresponding pair is coprime.

	0	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
0		*						
1	*	*	*	*	*	*	*	*
x		*		*		*		*
$1+x$		*	*		*			*
x^2		*		*		*		*
$1+x^2$		*	*		*			*
$x+x^2$		*						*
$1+x+x^2$		*	*	*	*	*	*	

The table is symmetric with 16 coprime pairs above the diagonal, 16 below the diagonal, and 1 on the diagonal. The probability is $33/64$ that the pair is coprime.

In the article “ $6/\pi^2$ ” [1], Gareth Jones shows heuristically that $6/\pi^2$ is both the probability that two random positive integers are coprime and the probability that a positive integer is square-free. His point of view is that it is worthwhile to treat these questions

without complete rigor in a way that is accessible to students with a standard undergraduate course in algebra. In this article we first show that the same heuristics give an easy answer for the determination of the probabilities that two random polynomials over \mathbf{F}_q are coprime and that a random polynomial is square-free. Then we derive these probabilities by alternative and rigorous means.

For a set of polynomials $S \subset \mathbf{F}_q[x]$ we define $\hat{P}(S)$ to be the limit as n goes to infinity of the ratio of the number of polynomials in S of degree less than n to the number of all polynomials of degree less than n . (For a subset of positive integers the analagous limit is traditionally called the *density* of the subset.) However, this probability is not countably additive, meaning that for disjoint sets $S_1, S_2, \dots, S_k, \dots$ it is not always the case that

$$\hat{P}\left(\bigcup_k S_k\right) = \sum_k \hat{P}(S_k) \quad (1)$$

even though $\hat{P}(S_k)$ exists for all k . As a counter-example let S_k be the polynomials of degree k for $k \geq 0$. Then $\hat{P}(S_k) = 0$ but the union of the S_k is the entire space of polynomials and its probability is 1.

An important example is the probability of the ideal generated by h , denoted by (h) . Let $d = \deg h$ and suppose $n > d$. There are q^{n-d} polynomials of degree less than $n - d$. Multiplying each of these by h gives all the polynomials of degree less than n which are multiples of h . Thus,

$$\hat{P}(f \in (h)) = \lim_{n \rightarrow \infty} \frac{|(h) \cap \{f \mid \deg f < n\}|}{|\{f \mid \deg f < n\}|} \quad (2)$$

$$= \lim_{n \rightarrow \infty} \frac{q^{n-d}}{q^n} \quad (3)$$

$$= \frac{1}{q^d}. \quad (4)$$

We extend this definition of probability the Cartesian product of two or more copies of $\mathbf{F}_q[x]$ by counting the tuples of polynomials of degree less than n , forming the ratio compared to the number of tuples of all polynomials of degree less than n , taking the limit as $n \rightarrow \infty$.

Now our philosophy and that of Jones is to act as if our probability is countably additive. This allows us to add the probabilities of a countable number of disjoint events and to multiply the probabilities of a countable number of independent events.

2 Heuristic Derivation

Define $\alpha = \hat{P}(\gcd(f, g) = 1)$. We observe that

$$\gcd(f, g) = h \text{ if and only if } \begin{cases} f \in (h) \\ g \in (h) \\ \gcd(f/h, g/h) = 1 \end{cases} \quad (5)$$

The probability that f and g are both multiples of h is the product $(1/q^d)(1/q^d) = 1/q^{2d}$, since the events are independent. Therefore,

$$\hat{P}(\gcd(f, g) = h) = \frac{\alpha}{q^{2 \deg h}}. \quad (6)$$

Now we sum the probabilities over all monic polynomials h :

$$1 = \sum_{h \text{ monic}} \hat{P}(\gcd(f, g) = h) \quad (7)$$

$$= \sum_{h \text{ monic}} \frac{\alpha}{q^{2 \deg h}} \quad (8)$$

$$= \sum_{n \geq 0} q^n \frac{\alpha}{q^{2n}}. \quad (9)$$

For the last line we sum over the degree of h since there are q^n monic polynomials of degree n . From that we get that

$$\alpha = \left(\sum_{n \geq 0} \frac{1}{q^n} \right)^{-1} \quad (10)$$

$$= 1 - \frac{1}{q}. \quad (11)$$

In particular two random polynomials with binary coefficients have an equal chance of being relatively prime or not consistent with our data giving a value of 31/64.

As in [1] we consider the probability that a polynomial is square-free, that is, it is not divisible by the square of any non-constant polynomial. Let $\text{Sq}(f)$ denote the monic square factor of f of largest degree and define

$$\beta = \hat{P}(\text{Sq}(f) = 1), \quad (12)$$

the probability that a random polynomial is square-free. We observe that

$$\text{Sq}(f) = h \text{ if and only if } \begin{cases} f \in (h^2), \text{ and} \\ \text{Sq}(f/h^2) = 1. \end{cases} \quad (13)$$

From this we obtain

$$\hat{P}(\text{Sq}(f) = h) = \beta/q^{2 \deg h}. \quad (14)$$

Summing over all monic h we get

$$1 = \sum_{h \text{ monic}} \frac{\beta}{q^{2 \deg h}}. \quad (15)$$

This is exactly the same expression for β as we got for α in (8), and so it follows that $\beta = \alpha = 1 - 1/q$.

We end the heuristics with a second demonstration that α and β are equal—without actually finding their value—by showing that they can be written as the same infinite product.

Polynomials f and g are coprime if and only if no irreducible polynomial is a factor of both of them. That is, f and g are not both in the ideal generated by each irreducible monic polynomial ϕ . The probability that both are not in the ideal (ϕ) is

$$1 - \hat{\mathbb{P}}(f \in (\phi) \text{ and } g \in (\phi)) \quad (16)$$

which is

$$1 - \frac{1}{q^{2 \deg \phi}}. \quad (17)$$

Taking the product over all irreducible monic polynomials h it follows that

$$\hat{\mathbb{P}}(\gcd(f, g) = 1) = \prod_{\phi \text{ prime}} \left(1 - \frac{1}{q^{2 \deg \phi}}\right). \quad (18)$$

Likewise, we derive the same product formula for β by observing that f is square-free if and only if f is not in the ideal (ϕ^2) for any monic irreducible ϕ . The probability that f is in the ideal (ϕ^2) is $1/q^{2 \deg \phi}$, and so

$$\hat{\mathbb{P}}(f \notin (\phi^2)) = 1 - \frac{1}{q^{2 \deg \phi}}. \quad (19)$$

Taking the product over all irreducible monic polynomials ϕ gives us the same product for β :

$$\beta = \hat{\mathbb{P}}(f \text{ square-free}) = \prod_{\phi \text{ prime}} \left(1 - \frac{1}{q^{2 \deg \phi}}\right). \quad (20)$$

3 Explicit Count of Coprime Pairs

Let a_n be the number of coprime pairs of polynomials of degree at most n . We will show that $a_n = q^{2n+2} - q^{2n+1} + q - 1$. Since there are q^{n+1} polynomials of degree at most n , there are q^{2n+2} pairs of such polynomials, and the probability that two of them are coprime is

$$\frac{a_n}{q^{2n+2}} = 1 - \frac{1}{q} + \frac{1}{q^{2n+1}} - \frac{1}{q^{2n+1}}. \quad (21)$$

As $n \rightarrow \infty$ this probability has the limit $1 - 1/q$.

We count the pairs whose gcd has degree k . There are q^k monic polynomials that could be the gcd. Now consider the pair (f, g) with $h = \gcd(f, g)$ and $\deg h = k$. The pair $(f/h, g/h)$ is a coprime pair of degree at most $n - k$, and there are a_{n-k} of these pairs. Therefore, there are $q^k a_{n-k}$ pairs whose gcd has degree k for $k = 0, \dots, n$. We also have the special pair $(0, 0)$ which has not been counted in this way. All this gives us the recursion formula

$$q^{2n+2} = 1 + \sum_{k=0}^n q^k a_{n-k}. \quad (22)$$

We use a generating function approach in order to solve the recursion. Move the 1, multiply both sides by t^n , and sum over n :

$$\sum_{n=0}^{\infty} (q^{2n+2} - 1)t^n = \sum_{n=0}^{\infty} \sum_{k=0}^n q^k a_{n-k} t^n \quad (23)$$

$$= \sum_{k=0}^{\infty} q^k t^k \sum_{m=0}^{\infty} a_m t^m \quad (24)$$

$$= (1 - qt)^{-1} \sum_{m=0}^{\infty} a_m t^m \quad (25)$$

Therefore,

$$\sum_{n=0}^{\infty} a_n t^n = (1 - qt) \sum_{n=0}^{\infty} (q^{2n+2} - 1) t^n \quad (26)$$

Equating coefficients shows that

$$a_n = q^{2n+2} - q^{2n+1} + q - 1 \quad (27)$$

This gives us a rigorous proof that the probability is $1 - 1/q$ that two random polynomials are coprime. It gives even more in that we have not only the limiting probability but the probability for polynomials up to any degree.

4 Square-Free Polynomials

Let b_n be the number of non-zero polynomials of degree $\leq n$ having no square factor of positive degree. Then we partition the set $\{f \mid \deg f \leq n\}$, which has size q^{n+1} , according to the degree of $\text{Sq}(f)$. Then

$$q^{n+1} - 1 = \sum_{2k+m=n} q^k b_m \quad (28)$$

Multiply both sides by t^n and sum over n .

$$\sum_{n=0}^{\infty} (q^{n+1} - 1) t^n = \sum_{n=0}^{\infty} \sum_{2k+m=n} q^k b_m t^n \quad (29)$$

$$= \sum_{k=0}^{\infty} q^k t^{2k} \sum_{m=0}^{\infty} b_m t^m \quad (30)$$

$$= (1 - qt^2)^{-1} \sum_{m=0}^{\infty} b_m t^m \quad (31)$$

Therefore,

$$\sum_{n=0}^{\infty} b_n t^n = (1 - qt^2) \sum_{n=0}^{\infty} (q^{n+1} - 1) t^n \quad (32)$$

and so

$$b_0 = q - 1 \quad (33)$$

$$b_1 = q^2 - 1 \quad (34)$$

$$b_n = q^{n+1} - q^n + q - 1, \quad n \geq 2 \quad (35)$$

Finally, the probability that a random polynomial is square-free is

$$\lim_{n \rightarrow \infty} \frac{b_n}{q^{n+1}} = 1 - \frac{1}{q} \quad (36)$$

5 Independence

Let ϕ be a prime polynomial (recall that means ϕ is monic and irreducible) and let L be a subset of the natural numbers $\mathbf{N} = \{0, 1, 2, \dots\}$. Define the subset $\mathcal{E}(\phi, L)$ to be those f in $\mathbf{F}_q[x]$ containing ϕ^l in their prime factorization. In this section we will show that for any family of distinct primes ϕ_i , finite or countable, and for arbitrary subsets L_i of natural numbers, the sets $\mathcal{E}(\phi_i, L_i)$ are independent.

The generating function for the number of monic polynomials counted by degree is the geometric series

$$\frac{1}{1-qt} = \sum_{n=0}^{\infty} q^n t^n \quad (37)$$

The unique factorization of monic polynomials into products of prime powers is the explanation of the following fundamental product expansion for the geometric series

$$\frac{1}{1-qt} = \prod_{\phi \text{ prime}} (1 - t^{\deg \phi})^{-1} \quad (38)$$

The right side is the product over ϕ of the geometric series $\sum_j t^{j \deg \phi}$, and so the coefficient of t^n is the number of ways that n can be expressed as $n = j_1 \deg \phi_1 + \dots + j_s \deg \phi_s$. Such expressions for n are bijective with the monic polynomials in $\mathbf{F}_q[x]$ of degree n via the unique factorization into prime powers.

Now if we multiply by $(1 - t^{\deg \psi})$, then we eliminate all polynomials that contain a factor of ψ . If we also multiply by $\sum_{l \in L} t^{l \deg \psi}$, then we count the polynomials whose prime factorization includes ψ^l for $l \in L$. Thus,

$$\sum_{n=0}^{\infty} c_n t^n = \frac{1 - t^{\deg \psi}}{1 - qt} \sum_{l \in L} t^{l \deg \psi} \quad (39)$$

where c_n is the number of monic polynomials of degree n whose prime factorization includes ψ^l for $l \in L$. Substituting t/q for t results in

$$\sum_{n=0}^{\infty} \frac{c_n}{q^n} t^n = \frac{1 - \left(\frac{t}{q}\right)^{\deg \psi}}{1 - t} \sum_{l \in L} \left(\frac{t}{q}\right)^{l \deg \psi} \quad (40)$$

From this we see that

$$\lim_{n \rightarrow \infty} \frac{c_n}{q^n} = \left(1 - \frac{1}{q^{\deg \psi}}\right) \sum_{l \in L} \frac{1}{q^{l \deg \psi}} \quad (41)$$

(If $\sum_n a_n t^n = F(t)/(1-t)$, then $\lim_{n \rightarrow \infty} a_n = F(1)$.)

Since c_n counts just the monic polynomials of degree n , the number of non-zero polynomials of degree n in $\mathcal{E}(\psi, L)$ is $(q-1)c_n$, and the number of non-zero polynomials of degree not exceeding n is

$$(q-1)(c_0 + \dots + c_n) \quad (42)$$

Hence,

$$\hat{P}(\mathcal{E}(\psi, L)) = \lim_{n \rightarrow \infty} \frac{(q-1)(c_0 + \dots + c_n)}{q^{n+1}} \quad (43)$$

Now we will show that this limit is equal to $p = \lim_{n \rightarrow \infty} c_n/q^n$. Fix a positive integer i .

$$\lim_{n \rightarrow \infty} \frac{q-1}{q^{n+1}} \sum_{k=0}^n c_k = (q-1) \lim_{n \rightarrow \infty} \sum_{k=n-i+1}^n \frac{c_k}{q^{n+1}} + (q-1) \lim_{n \rightarrow \infty} \sum_{k=0}^{n-i} \frac{c_k}{q^{n+1}} \quad (44)$$

$$= (q-1) \sum_{k=0}^{i-1} \frac{c_{n-k}}{q^{n-k}} \frac{1}{q^{k+1}} + (q-1) \lim_{n \rightarrow \infty} \sum_{k=0}^{n-i} \frac{c_k}{q^{n+1}} \quad (45)$$

$$= (q-1) \sum_{k=0}^{n-i} \lim_{n \rightarrow \infty} \frac{p}{q^{k+1}} + (q-1) \lim_{n \rightarrow \infty} \sum_{k=0}^{n-i} \frac{c_k}{q^{n+1}} \quad (46)$$

$$= p \left(1 - \frac{1}{q^i}\right) + (q-1) \lim_{n \rightarrow \infty} \sum_{k=0}^{n-i} \frac{c_k}{q^{n+1}} \quad (47)$$

Since $c_k \leq q^k$, the second term is bounded by $\frac{1}{q^i(q-1)}$. Letting i go to infinity, we see that

$$\lim_{n \rightarrow \infty} \frac{q-1}{q^{n+1}} \sum_{k=0}^n c_k = p \quad (48)$$

This shows that

$$\hat{P}(\mathcal{E}(\psi, L)) = \left(1 - \frac{1}{q^{\deg \psi}}\right) \sum_{l \in L} \frac{1}{q^{l \deg \psi}} \quad (49)$$

Suppose that we specify a set of exponents L_ϕ for each prime ϕ . Let c_n be the number of monic polynomials of degree n such that in the prime factorization the exponent of ϕ is in L_ϕ for all primes ϕ . Going through the same algebraic computation as above we see that

$$\sum_{n=0}^{\infty} c_n t^n = \frac{1}{1-qt} \prod_{\phi} \left((1 - t^{\deg \phi}) \sum_{l \in L_\phi} t^{l \deg \phi} \right) \quad (50)$$

Replacing t by t/q to see that

$$\lim_{n \rightarrow \infty} \frac{c_n}{q^n} = \prod_{\phi} \left(\left(1 - \frac{1}{q^{\deg \phi}}\right) \sum_{l \in L_\phi} \frac{1}{q^{l \deg \phi}} \right) \quad (51)$$

but the product on the right is

$$\prod_{\phi} \hat{P}(\mathcal{E}(\phi, L_\phi)) \quad (52)$$

and the limit on the left is the probability that a monic polynomial is in the intersection of all the $\mathcal{E}(\phi, L_\phi)$ but that in turn is the probability that any polynomial is in that intersection. Thus, we have shown that the sets $\mathcal{E}(\phi, L_\phi)$ are independent, or as Kac wrote in [2] referring to the integers: “primes play a game of chance.” If we consider the multiplicity of ϕ in the prime factorization as a random variable, then these random variables are independent. By taking $L_\psi = \{l\}$ and all other $L_\phi = \mathbf{N}$, we see that the probability that multiplicity of ψ is equal to l is

$$\left(1 - \frac{1}{q^{\deg \psi}}\right) \frac{1}{q^{l \deg \psi}} \quad (53)$$

which is to say that the random variable has a geometric distribution.

As an example, the square-free polynomials are the intersection of $\mathcal{E}(\phi, L_\phi)$, where $L_\phi = \{0, 1\}$ for all primes ϕ . Thus, the probability of being square-free is

$$\prod_{\phi} \left(1 - \frac{1}{q^{\deg \phi}}\right) \left(1 + \frac{1}{q^{\deg \phi}}\right) = \prod_{\phi} \left(1 - \frac{1}{q^{2 \deg \phi}}\right) \quad (54)$$

This, of course, is the same product expansion we found in §2. Using (38) with $t = q^{-2}$, we see that

$$\prod_{\phi} \left(1 - \frac{1}{q^{2 \deg \phi}}\right) = 1 - \frac{1}{q} \quad (55)$$

will evaluate it in the next section on zeta functions.

6 Zeta Functions

For both the integers and the polynomials over a finite field, showing that the product formula for α and β is equal to the sum formula is a special case of the product expansion of a zeta function. For the integers, the zeta function is the classical Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (56)$$

defined for $\operatorname{Re} s > 1$ and extended by analytic continuation. The sum here is over positive integers n , which correspond bijectively to the non-zero ideals of \mathbf{Z} . Furthermore, the cardinality of the quotient ring $\mathbf{Z}/(n)$ is n . Thus, we see that the zeta function can be expressed as

$$\zeta(s) = \sum_I |\mathbf{Z}/I|^{-s} \quad (57)$$

where the sum is over non-zero ideals I .

Now we copy this definition to the ring of polynomials $\mathbf{F}_q[x]$. The non-zero ideals are bijective with the monic polynomials, since each non-zero ideal is uniquely of the form (h) for a monic h . The cardinality of $\mathbf{F}_q[x]/(h)$ is $q^{\deg h}$. Define the q -zeta function

$$\zeta_q(s) = \sum_I |\mathbf{F}_q[x]/I|^{-s} \quad (58)$$

where the sum is over the non-zero ideals of $\mathbf{F}_q[x]$. Then

$$\zeta_q(s) = \sum_{h \text{ monic}} q^{-s \deg h} \quad (59)$$

$$= \sum_{n=0}^{\infty} q^n q^{-sn} \quad (60)$$

since there are q^n monic polynomials of degree n . This geometric series sums (for $\operatorname{Re} s > 1$ to give

$$\zeta_q(s) = \frac{1}{1 - q^{1-s}}. \quad (61)$$

The product expansion for the Riemann zeta function is

$$\zeta(s) = \prod_{p \text{ prime}} (1 - p^{-s})^{-1} \quad (62)$$

which comes from expanding each factor as a geometric series in p^{-s} and then using the Fundamental Theorem of Arithmetic to see that each positive integer n appears exactly once in a product of the form $n^{-s} = p_1^{-e_1 s} \cdots p_r^{-e_r s}$. Likewise,

$$\zeta_q(s) = \prod_{\phi \text{ prime}} (1 - q^{-s \deg \phi})^{-1} \quad (63)$$

where the product is over the prime polynomials ϕ , by which we mean the monic irreducible polynomials. Again, to see that this product is the same as the definition of $\zeta_q(s)$ given by the sum we use the unique factorization of any monic polynomial h as a product of prime factors, $h = \phi_1^{e_1} \cdots \phi_r^{e_r}$.

In the situations of both the integers and the polynomials these factorizations can be seen as products over the non-zero prime ideals.

7 Several Coprime Polynomials

What we have seen is that the probability that two random polynomials are coprime is $1/\zeta_q(2)$ just as the probability that two integers are coprime is $1/\zeta(2)$. We can show that three random polynomials are coprime with probability $1/\zeta_q(3)$, in the sense that three polynomials are coprime if the ideal they generate is the entire ring. (We do not want to confuse this with the property of being pairwise coprime.) We will actually consider the more general case of r polynomials being coprime.

Let f_1, \dots, f_r be in $\mathbf{F}_q[x]$. They are not coprime if there is some monic irreducible polynomial ϕ that divides all of them. This means that each f_i is in the ideal (ϕ) . The probability of that happening is $1/q^{r \deg \phi}$ since the f_i are selected independently. Thus, the probability that they are coprime is the product

$$\prod_{\phi \text{ prime}} \left(1 - \frac{1}{q^{r \deg \phi}}\right) \quad (64)$$

which is the product expansion of $1/\zeta_q(r)$. Explicitly, this probability is $1 - q^{1-r}$.

Generalizing the property of being square-free to higher powers we can show that the probability that a random polynomial is not divisible by an r th power is also $1/\zeta_q(r)$. Incidentally, these results also hold for the integers using the Riemann zeta function.

8 Further Questions

Now the result for two polynomials being coprime can also be stated as: the probability that two random polynomials have a common factor is $1/q$. This suggests a natural question. Is there a more direct way to see that? We offer one possibility. The resultant of two polynomials over a field F is an element of F and it is 0 if and only if the polynomials

have a common factor. We consider the resultant as a random variable on the space of pairs (f, g) of polynomials in $\mathbf{F}_q[x]$. Is this random variable uniformly distributed? If so, then the probability is $1/q$ that the resultant is 0 and that the polynomials have a common factor.

For the probability of being square-free, consider the discriminant as a random variable on the space $\mathbf{F}_q[x]$. For a monic polynomial $f \in \mathbf{F}_q[x]$, there is factorization $f(x) = (x - \lambda_1) \cdots (x - \lambda_n)$ in some extension field over \mathbf{F}_q . The discriminant of f is $\prod_{i,j} (\lambda_i - \lambda_j)^2$, which lies in \mathbf{F}_q by basic Galois theory. The discriminant of f is 0 if and only if f has a multiple root, and that is equivalent to f being divisible by a square. If we could show that the probability distribution of the discriminant is uniform over \mathbf{F}_q , then we could conclude that the probability of not being square-free is $1/q$. We end with some problems.

Find the probability that r random polynomials are pairwise coprime.

Find the probability that r random integers are pairwise coprime.

Consider the problems in this paper for the ring of Gaussian integers $\mathbf{Z}[i] = \{a + bi \mid a, b \in \mathbf{Z}\}$.

References

- [1] G. A. Jones, $6/\pi^2$, *Mathematics Magazine* 66 (1993), 290-298.
- [2] M. Kac. *Statistical Independence in Probability, Analysis and Number Theory*. Carus Monographs, no. 12. Mathematical Association of America, Washington, D.C., 1959.