Canad. Math. Bull. Vol. 61 (2), 2018 pp. 346–352
http://dx.doi.org/10.4153/CMB-2017-013-4

Counting Separable Polynomials in $\mathbb{Z}/n[x]$

Jason K. C. Polak

Abstract. For a commutative ring R, a polynomial $f \in R[x]$ is called *separable* if $R[x]/f$ is a separable R-algebra. We derive formulae for the number of separable polynomials when $R = \mathbb{Z}/n$, extending a result of L. Carlitz. For instance, we show that the number of polynomials in $\mathbb{Z}/n[x]$ that are separable is $\phi(n)n^d \prod_i (1 - p_i^{-d})$, where $n = \prod p_i^{k_i}$ is the prime factorisation of n and ϕ is Euler's totient function.

1 Introduction

Suppose a, b, c are independently, uniformly randomly chosen elements of $\mathbb{Z}/11$. What is the probability that the element $a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2$ is nonzero in $\mathbb{Z}/11$? Answer: 10/11. This peculiar fact follows from a theorem of Carlitz [2, §6], who proved that the number of monic separable polynomials in $\mathbb{Z}/p[x]$ of degree d where $d \geq 2$ is $p^d - p^{d-1}$. Our aim is to extend his result to separable polynomials in $\mathbb{Z}/n[x]$. Now, most people are familiar with separable polynomials over fields, but just what is a separable polynomial over an arbitrary commutative ring? To understand separable polynomials, we will first have to look at separable algebras.

Let R be a commutative ring. If A is an R-algebra, we define A^{op} to be the ring with the same underlying abelian group as A and whose multiplication is given by $(a, b) \mapsto ba$. Then A can be made into a left $A \otimes_R A^{\mathrm{op}}$-module via the action $(a \otimes a')b = aba'$. An R-algebra A is called *separable* if A is projective as an $A \otimes_R A^{\mathrm{op}}$-module, the basic theory of which is contained in [1]. Examples include separable field extensions, full matrix rings over a commutative ring R, and group rings $k[G]$ when k is a field and G is a finite group whose order is invertible in k. On the other hand, $\mathbb{Z}[\sqrt{5}]$ is not a separable $\mathbb{Z}$-algebra.

A polynomial $f \in R[x]$ is called *separable* if $R[x]/f$ is separable as an R-algebra. A monic polynomial is separable if and only if the ideal (f, f') is all of $R[x]$ [4, §1.4, Proposition 1.1], and so for fields coincides with the usual definition. For example, $x - a$ for $a \in R$ is always separable. To state our results, recall Euler's *totient function*: for a positive integer n, the number $\phi(n)$ is the number of elements of the set $\{1, 2, \dots, n\}$ relatively prime to n. In other words, $\phi(n) = |(\mathbb{Z}/n)^\times|$. For example, $\phi(p^k) = p^k - p^{k-1}$. Our first theorem is on the number of monic separable polynomials in $\mathbb{Z}/p^k[x]$.

Received by the editors December 22, 2016.
Published electronically April 13, 2017.
This research was made possible by ARC Grant DP150103525.
AMS subject classification: **13H05**, 13B25, 13M10.
Keywords: separable algebra, separable polynomial.

Theorem 1.1 *Let p be a prime and $k \geq 1$ be an integer. The number of monic separable polynomials of degree d with $d \geq 2$ in $\mathbb{Z}/p^k[x]$ is $p^{kd-1}(p-1) = \phi(p^{kd})$. Equivalently, the proportion of monic polynomials of degree d with $d \geq 2$ that are separable in $\mathbb{Z}/p^k[x]$ is $(1-p^{-1})$.*

When $k = 1$, this result is Carlitz's theorem. For example, when $k = 1$ and $d = 2$, this result is easily computable. There are p^2 monic quadratic polynomials. Since $\mathbb{Z}/p$ is a perfect field, every irreducible quadratic is separable. Therefore, the only quadratic polynomials that are not separable are of the form $(x-a)^2$ for $a \in \mathbb{Z}/p$. Therefore, there are $p^2 - p$ separable quadratics. We note that in general, one must be careful with factorisation when $k > 1$, since then $\mathbb{Z}/p^k[x]$ is not a unique factorisation domain: for example, in $\mathbb{Z}/4[x]$, we have $x^2 = (x+2)^2$.

Example 1.2 If $k = 1$, then $\mathbb{Z}/p^k = \mathbb{Z}/p$ is a field, and every irreducible polynomial is also separable. This is not true if $k > 1$. For example, in $\mathbb{Z}/4[x]$, the polynomial x^2+1 is irreducible, but not separable. On the other hand, x^2+x+1 is separable and irreducible.

Next, we consider the general case of $\mathbb{Z}/n$.

Theorem 1.3 *Let n be an integer with $|n| > 1$ and let $n = p_1^{k_1} \cdots p_m^{k_m}$ be the prime factorisation of n. Then the number of monic separable polynomials of degree d with $d \geq 2$ in the ring $\mathbb{Z}/n[x]$ is $\phi(n^d)$. Equivalently, the proportion of monic polynomials of degree d with $d \geq 2$ that are separable in $\mathbb{Z}/n$ is equal to $\prod_{i=1}^m (1-p_i^{-1})$.*

Since there exist separable polynomials in $\mathbb{Z}/n[x]$ that are not monic and whose leading coefficient is not a unit, our ultimate aim is to count all separable polynomials in $\mathbb{Z}/n[x]$.

Theorem 1.4 *Let n be a positive integer with prime factorisation $n = p_1^{k_1} \cdots p_m^{k_m}$ and let $d \geq 1$. Then the number of separable polynomials f with $\deg(f) \leq d$ in $\mathbb{Z}/n[x]$ is*

$$\phi(n)n^d \prod_i (1+p_i^{-d}).$$

2 Monic Separable Polynomials in $\mathbb{Z}/n[x]$

Let R be a commutative ring. If A is a finitely generated projective R-module, then there exists elements $f_1, \dots, f_n \in \operatorname{Hom}_R(A, R)$ and $x_1, \dots, x_n \in A$ such that for all $x \in A$,

$$x = \sum_{i=1}^n f_i(x)x_i.$$

https://doi.org/10.4153/CMB-2017-013-4 Published online by Cambridge University Press

The elements $\{f_i, x_i\}_{i=1}^n$ are called a *dual basis* for A. If A is additionally an R-algebra, one can define the *trace map* to be

$$\begin{aligned} \mathrm{tr}\colon A &\longrightarrow R \\ x &\longmapsto \sum_{i=1}^n f_i(xx_i). \end{aligned}$$

It is easy to see that the trace map is independent of the chosen dual basis. If f is a monic polynomial in $R[x]$, then the algebra $R[x]/f$ is a finitely generated free R-module. One possible dual basis for $R[x]/f$ is $x_i = x^i$ with $f_i(g)$ being the coefficient of x^i in g, where $i = 1, \dots, n-1$ with $n = \deg(f)$. We can use part of [3, Theorem 4.4, Chapter III] to decide when a polynomial $f \in R[x]$ is separable.

Proposition 2.1 *Let R be a commutative ring with no nontrivial idempotents and let $f \in R[x]$ be a degree n monic polynomial. Let A be the matrix whose $(i+1, j+1)$-entry is $\mathrm{tr}(x^{i+j})$. Then f is separable if and only if $\mathrm{disc}(f) := \det(A) \in R$ is a unit.*

Example 2.2 Consider $f = x^2 + ax + b \in \mathbb{Z}/p[x]$. Then the matrix A in Theorem 2.1 is

$$A = \begin{pmatrix} 2 & -a \\ -a & a^2 - 2b \end{pmatrix}.$$

Its determinant is the familiar $a^2 - 4b$. If $f = x^3 + ax^2 + bx + c$, then

$$A = \begin{pmatrix} 3 & -a & a^2 - 2b \\ -a & a^2 - 2b & -a^3 + 3ab - 3c \\ a^2 - 2b & -a^3 + 3ab - 3c & a^4 - 4a^2b + 4ac + 2b^2 \end{pmatrix},$$

and its determinant is the less familiar $a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2$. This explains the relation of separable polynomials to the opening paragraph's bizarre question.

We now prove the following theorem.

Theorem 2.3 *Let p be a prime and $k \geq 1$ be an integer. The number of monic separable polynomials of degree d with $d \geq 2$ in $\mathbb{Z}/p^k[x]$ is $p^{kd-1}(p-1) = \phi(p^{kd})$. Equivalently, the proportion of monic polynomials of degree d with $d \geq 2$ that are separable in $\mathbb{Z}/p^k[x]$ is $(1 - p^{-1})$.*

Proof From Proposition 2.1, $f \in \mathbb{Z}/p^k[x]$ is separable if and only if its discriminant $\mathrm{disc}(f)$ is invertible in $\mathbb{Z}/p^k$. Since $\mathrm{disc}(f)$ is obtained from the coefficients of f through basic arithmetic operations of addition and multiplication, we see that f is separable if and only if its image in $\mathbb{Z}/p^k[x]/p\mathbb{Z}/p^k[x] \cong \mathbb{Z}/p[x]$ is separable. Hence, we have reduced the problem to Carlitz's theorem. ∎

Now that we have determined the number of separable polynomials in $\mathbb{Z}/p^k[x]$, we move on to the general case of $\mathbb{Z}/n$ for any integer n with $|n| > 1$. We will need the following result.

Proposition 2.4 ([3, Proposition II.2.1.13]) *Let R_1 and R_2 be commutative rings and let A_i be a commutative R_i algebra for $i = 1, 2$. Then $A_1 \times A_2$ is a separable $R_1 \times R_2$-algebra if and only if A_i is a separable R_i algebra for $i = 1, 2$.*

Theorem 2.5 *Let n be an integer with $|n| > 1$ and let $n = p_1^{k_1} \cdots p_m^{k_m}$ be the prime factorisation of n. Then the number of monic separable polynomials of degree d with $d \geq 2$ in the ring $\mathbb{Z}/n[x]$ is $\phi(n^d)$. Equivalently, the proportion of monic polynomials of degree d with $d \geq 2$ that are separable in $\mathbb{Z}/n$ is equal to $\prod_{i=1}^{m}(1 - p_i^{-1})$.*

Proof Factor $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$, where the p_i are the prime factors of n so that $\mathbb{Z}/n \cong \mathbb{Z}/p_1^{k_1} \times \cdots \times \mathbb{Z}/p_m^{k_m}$. Then we have

$$\mathbb{Z}/n[x] \cong \mathbb{Z}/p_1^{k_1}[x] \times \cdots \times \mathbb{Z}/p_m^{k_m}[x]. \tag{2.1}$$

An element $f \in \mathbb{Z}/n[x]$ corresponds to an element

$$(f_1, \ldots, f_m) \in \mathbb{Z}/p_1^{k_1}[x] \times \cdots \times \mathbb{Z}/p_m^{k_m}[x].$$

From Proposition 2.4, we see that f is separable if and only if f_i is a separable polynomial in $\mathbb{Z}/p_i^{k_i}$. Therefore, the number of monic polynomials over $\mathbb{Z}/n$ that are separable of degree d is equal to the number of tuples $(f_1, \ldots, f_m)$ such that f_i is a separable monic polynomial over $\mathbb{Z}/p_i^{k_i}$ for each i and $\deg(f_i) = d$. The result now follows from Theorem 1.1 and the fact that ϕ is multiplicative. ∎

Example 2.6 For $n = 614889782588491410$ (the product of the first fifteen primes) the proportion of monic polynomials over $\mathbb{Z}/n$ that are separable is 1605264998400/11573306655157, or about 0.138704092635850. The formula shows that as the number of prime factors of n increases to infinity, the proportion of separable polynomials goes to zero.

3 Arbitrary Polynomials and Separability

In the case of fields, it suffices to look at monic polynomials, since one can always multiply such a polynomial by a unit to make it monic, and this does not change the ideal it generates. For general rings, this is not so, and it is clear from the isomorphism in (2.1) that there are many polynomials that are separable are not monic and whose leading coefficient is not invertible.

Example 3.1 In the ring $\mathbb{Z}/6[x]$, the polynomial $f = 3x^2 + x + 5$ is separable and irreducible, but its leading coefficient is not a unit in $\mathbb{Z}/6$.

In this section we calculate the number of separable polynomials of at most degree d where $d \geq 1$, and whose leading coefficient is arbitrary. As before, this result depends on the result for polynomials in $\mathbb{Z}/p^k[x]$. We have already observed that a monic polynomial is separable in $\mathbb{Z}/p^k[x]$ if and only if its reduction modulo p is reducible in $\mathbb{Z}/p[x]$. To handle arbitrary polynomials, we use the following theorem.

https://doi.org/10.4153/CMB-2017-013-4 Published online by Cambridge University Press

Proposition 3.2 ([3, II.7.1]) *Let R be a commutative ring. For a finitely generated R-algebra A, the following are equivalent:*

(i) *A is a separable R-algebra;*
(ii) *A_m is a separable R_m algebra for every maximal ideal m of R;*
(iii) *A/mA is a separable R/m-algebra for every maximal ideal m of R.*

Since $\mathbb{Z}/p^k$ is a local ring with unique maximal ideal (p), we have the following corollary.

Corollary 3.3 *A polynomial $f \in \mathbb{Z}/p^k[x]$ is separable if and only if its reduction in $\mathbb{Z}/p[x]$ modulo p is separable.*

Example 3.4 Let $a \in \mathbb{Z}/p^k \subseteq \mathbb{Z}/p^k[x]$ be a constant polynomial. In $\mathbb{Z}/p[x]$, the zero polynomial is not separable, since $\mathbb{Z}/p[x]$ is not a separable $\mathbb{Z}/p$-algebra; indeed, a separable algebra over field must be finite-dimensional over that field [3, II.2.2.1]. Therefore, a is separable if and only if a is a unit in $\mathbb{Z}/p^k$. Thus, there are $\phi(p^k)$ separable polynomials in $\mathbb{Z}/p^k[x]$ of degree zero.

We can proceed inductively to calculate the number of separable polynomials of degree one. They are one of two types, according to Corollary 3.3:

(a) $ux + b$ where u is a unit,
(b) $ux + b$ where $u \neq 0$ is not a unit and b is a unit.

In the first case, we already know there are p^k monic separable linear polynomials, so there are $\phi(p^k)p^k$ polynomials whose leading coefficient is a unit. In the second case there are $(p^k - \phi(p^k) - 1)\phi(p^k)$ polynomials of the form $ux + b$ where $u \neq 0$ is not a unit but b is a unit. Adding these two together, we see that there are

$$\phi(p^k)\big(2p^k - \phi(p^k) - 1\big) = \phi(p^k)(p^k + p^{k-1} - 1)$$

linear separable polynomials in $\mathbb{Z}/p^k[x]$, and hence $\phi(p^k)(p^k + p^{k+1})$ separable polynomials of degree at most one.

Now we will derive a formula for the number of separable polynomials with arbitrary leading coefficient and degree at most d. But first, we will need the following elementary geometric sum.

Lemma 3.5 *Let $\beta = p^k$ and $\lambda = p^{k-1}$. Then*

$$\phi(\beta^d) + \lambda\phi(\beta^{d-1}) + \cdots + \lambda^{d-2}\phi(\beta^2) = p^{(k-1)d+1}(p^{d-1} - 1).$$

Proof We sum a geometric series

$$\begin{aligned}
&\phi(\beta^d) + \lambda\phi(\beta^{d-1}) + \cdots + \lambda^{d-2}\phi(\beta^2)\\
&\quad = p^{kd-1}(p-1)\Big[1 + \frac{\lambda}{p^k} + \Big(\frac{\lambda}{p^k}\Big)^2 + \cdots + \Big(\frac{\lambda}{p^k}\Big)^{d-2}\Big]\\
&\quad = p^{kd-1}(p-1)\big[1 + p^{-1} + p^{-2} + \cdots + p^{-(d-2)}\big]
\end{aligned}$$

$$= p^{kd-1}(p-1)\frac{1-p^{d-1}}{(1-p)p^{d-2}}$$
$$= p^{kd-1}\frac{p^{d-1}-1}{p^{d-2}} = p^{(k-1)d+1}(p^{d-1}-1). \blacksquare$$

Theorem 3.6 *For $d \geq 1$, the number of separable polynomials f such that* $\deg(f) \leq d$ *in $\mathbb{Z}/p^k[x]$ is*

$$\phi(p^k)p^{(k-1)d}(p^d+1) = \phi(p^k)p^{kd}(1+p^{-d}).$$

Proof Let a_d be the number of separable polynomials f in $\mathbb{Z}/p^k[x]$ with arbitrary leading coefficient and such that $\deg(f) \leq d$. We follow the calculation method in Example 3.4. A separable polynomial of degree d must either have unit leading coefficient, or else it must be of the form ux^d+g where $u \neq 0$ is not a unit and g is a separable polynomial of $\deg(g) < d$. We have already shown that the number of monic polynomials of degree $d \geq 2$ in $\mathbb{Z}/p^k[x]$ that are also separable is $\phi(p^{kd})$. Therefore, the number of separable polynomials with unit leading coefficient and of degree exactly d for $d \geq 2$ is $\phi(p^{kd})\phi(p^k)$. With our notation, the number $a_d - a_{d-1}$ is the number of separable polynomials of degree exactly d, and our reasoning shows that we have the recurrence relation

$$a_d - a_{d-1} = \phi(p^{kd})\phi(p^k) + (p^k - \phi(p^k) - 1)a_{d-1},$$

which simplifies to

$$a_d = \phi(p^{kd})\phi(p^k) + \left(p^k - \phi(p^k)\right)a_{d-1} = \phi(p^{kd})\phi(p^k) + p^{k-1}a_{d-1},$$

as long as $d \geq 2$. To simplify notation for intermediate computations, let us set $\beta = p^k$ and $\lambda = p^{k-1}$. Then $a_d = \phi(\beta^d)\phi(\beta) + \lambda a_{d-1}$. It is easy to see that

$$a_d = \phi(\beta)\left[\phi(\beta^d) + \lambda\phi(\beta^{d-1}) + \cdots + \lambda^{d-2}\phi(\beta^2)\right] + \lambda^{d-1}a_1.$$

Example 3.4 shows that $a_1 = \phi(p^k)(p^k + p^{k-1})$ so that $\lambda^{d-1}a_1 = \phi(p^k)p^{(k-1)d}(p+1)$. Now, using Lemma 3.5, we get

$$\begin{aligned} a_d &= \phi(p^k)\left[p^{(k-1)d+1}(p^{d-1}-1)\right] + \phi(p^k)p^{(k-1)d}(p+1) \\ &= \phi(p^k)p^{(k-1)d}\left[p(p^{d-1}-1)+p+1\right] = \phi(p^k)p^{(k-1)d}(p^d+1). \end{aligned}$$

This takes care of $d \geq 2$. Putting $d = 1$ into this last line shows that it is equal to a_1, so the formula is also valid for $d = 1$. $\blacksquare$

Theorem 3.7 *Let n be a positive integer with prime factorisation $n = p_1^{k_1}\cdots p_m^{k_m}$ and let $d \geq 1$. Then the number of separable polynomials f with* $\deg(f) \leq d$ *in $\mathbb{Z}/n[x]$ is*

$$\phi(n)n^d\prod_i(1+p_i^{-d}).$$

Proof This follows from Theorem 3.6 and the fact that Euler's totient function ϕ is a multiplicative arithmetic function in the sense that $\phi(mn) = \phi(m)\phi(n)$ whenever m and n are relatively prime. $\blacksquare$

Example 3.8 There are 65028096 separable polynomials in $\mathbb{Z}/120[x]$ of degree at most three. There are 1888 separable polynomials of degree exactly two in $\mathbb{Z}/15[x]$.

References

[1] M. Auslander and O. Goldman, *The Brauer group of a commutative ring.* Trans. Amer. Math. Soc. **97**(1960), no. 3, 367–409. http://dx.doi.org/10.1090/S0002-9947-1960-0121392-6

[2] L. Carlitz, *The arithmetic of polynomials in a Galois field.* Amer. J. Math. **54**(1932), no. 1, 39–50. http://dx.doi.org/10.2307/2371075

[3] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings.* Lecture Notes in Mathematics, 181, Springer-Verlag, Berlin-New York, 1971.

[4] A. R. Magid, *The separable Galois theory of commutative rings.* Second ed., Pure and Applied Mathematics, CRC Press, Boca Raton, FL, 2014. http://dx.doi.org/10.1201/b17145

School of Mathematics and Statistics, The University of Melbourne, Parkville, Victoria 3010, Australia
e-mail: jpolak@jpolak.org