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 separable 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.