A Lemma on Polynomials Modulo p^m and Applications to Coding Theory

Richard M. Wilson
Department of Mathematics
California Institute of Technology
USA

The following lemma can be proved in a number of elementary ways: Let p be a prime, and e and m positive integers. Then there exists a polynomial

$$w(x) = c_0 + c_1 x + c_2 \binom{x}{2} + \ldots + c_d \binom{x}{d}$$

of degree $d \leq (m(p-1)+1)p^{e-1} - 1$ so that for all integers x

$$w(x) \equiv \begin{cases} 1 \pmod{p^m} & \text{if } x \equiv 0 \pmod{p^e}, \\ 0 \pmod{p^m} & \text{if } x \not\equiv 0 \pmod{p^e}. \end{cases}$$

The coefficients c_i are integers and, moreover,

$$c_i \equiv 0 \pmod{p^\ell}$$

whenever $i \geq (\ell(p-1)+1)p^{e-1}$. We give several applications of the lemma to coding theory. One is a quick proof of the fact that all codewords in the r-th order binary Reed-Muller code of length 2^n have weights divisible by $2^{\lfloor (n-1)/r \rfloor}$. The number of p-ary codewords with weights in one or several congruence classes modulo p^m is discussed. We give an extension of McEliece's theorem (on the power of p that divides the weights of all codewords in a cyclic code) to cyclic codes over the integers modulo p^e with respect to the Lee metric.