

GALOIS FIELD VECTOR-SPACE REPRESENTATIONS

<p>GF(8) $\rho(x) = x^3 + x + 1$ $\Rightarrow \alpha^3 + \alpha + 1 = 0$</p> <p>$x = a + b\alpha + c\alpha^2$</p> <p>$x \quad abc$ - ----</p> <p>0 100 1 010 2 001 3 110 4 011 5 111 6 101</p> <p>GF(16) $\rho(x) = x^4 + x + 1$</p> <p>0 1000 1 0100 2 0010 3 0001 4 1100 5 0110 6 0011 7 1101 8 1010 9 0101 10 1110 11 0111 12 1111</p>	<p>13 1011 14 1001</p> <p>GF(32) $\rho(x) = x^5 + x^2 + 1$</p> <p>0 10000 1 01000 2 00100 3 00010 4 00001 5 10100 6 01010 7 00101 8 10110 9 01011 10 10001 11 11100 12 01110 13 00111 14 10111 15 11111 16 11011 17 11001 18 11000 19 01100 20 00110 21 00011 22 10101 23 11110 24 01111 25 10011</p>	<p>26 11101 27 11010 28 01101 29 10010 30 01001</p> <p>GF(64) $\rho(x) = x^6 + x + 1$</p> <p>0 100000 1 010000 2 001000 3 000100 4 000010 5 000001 6 110000 7 011000 8 001100 9 000110 10 000011 11 110001 12 101000 13 010100 14 001010 15 000101 16 110010 17 011001 18 111100 19 011110 20 001111 21 110111 22 101011</p>	<p>23 100101 24 100010 25 010001 26 111000 27 011100 28 001110 29 000111 30 110011 31 101001 32 100100 33 010010 34 001001 35 110100 36 011010 37 001101 38 110110 39 011011 40 111101 41 101110 42 010111 43 111011 44 101101 45 100110 46 010011 47 111001 48 101100 49 010110 50 001011 51 110101 52 101010 53 010101 54 111010 55 011101</p> <p>56 111110 57 011111 58 111111 59 101111 60 100111 61 100011 62 100001</p>
--	--	---	---

MINIMAL POLYNOMIALS OF ELEMENTS OF $GF(2^m)$

<p>GF(4) 1 (0, 1, 2)</p>		<p>GF(64) 1 (0, 1, 6) 5 (0, 1, 2, 5, 6) 9 (0, 2, 3) 13 (0, 1, 3, 4, 6) 21 (0, 1, 2) 27 (0, 1, 3)</p>	<p>3 (0, 1, 2, 4, 6) 7 (0, 3, 6) 11 (0, 2, 3, 5, 6) 15 (0, 2, 4, 5, 6) 23 (0, 1, 4, 5, 6) 31 (0, 5, 6)</p>
<p>GF(8) 1 (0, 1, 3)</p>	<p>3 (0, 2, 3)</p>		
<p>GF(16) 1 (0, 1, 4) 5 (0, 1, 2)</p>	<p>3 (0, 1, 2, 3, 4) 7 (0, 3, 4)</p>		
<p>GF(32) 1 (0, 2, 5) 5 (0, 1, 2, 4, 5) 11 (0, 1, 3, 4, 5)</p>	<p>3 (0, 2, 3, 4, 5) 7 (0, 1, 2, 3, 5) 15 (0, 3, 5)</p>		