Primitive elements and irreducible polynomials of GF(256)

by Cody Planteen

https://codyplanteen.com/notes/rs

July 26, 2019

Intro

The finite field (also known as a Galois field) with 256 elements is sometimes written with the following notation $\mathbb{F}_{256}$ by mathematicians. Engineers and computer scientists often write GF(256) instead, which will be used for the rest of this paper. GF(256) is created by splitting the binary field GF(2) with a monic irreducible polynomial of degree 8 to form a field with 256 entries. A monic polynomial is a polynomial of a single variable with the coefficient of the highest degree being one.

Number of irreducible polynomials

The number of irreducible polynomials are given by Gauss's formula [Chebolu]:

$$\frac{1}{n}\left(\sum_{d|n}\mu(n/d)q^d\right)$$

The notation $d|n$ means the set of all positive divisors of n including 1 and n.

$\mu(x)$ is the Möbius function. This function is defined such that $\mu(1) = 1$.

For other values of x, it has the following properties:

$\mu(x) = 1$ if the prime factorization of x that is square-free (no prime factors with an exponent greater than one) and an even number of prime factors.

$\mu(x) = -1$ if the prime factorization of x that is square-free (no prime factors with an exponent greater than one) and an odd number of prime factors.

$\mu(x) = 0$ if the prime factorization of x has a squared prime factor (a prime factor with an exponent greater than one)

Using the above definitions:

$\mu(2) = -1$ since the prime factorization of 2 is 2 which is square-free with an odd number of factors

$\mu(4) = 0$ since the prime factorization of 4 is 2^2 has a squared prime factor

Number of irreducible polynomials in GF(256)

For GF(256) = GF(2^8), the number of irreducible polynomials with Gauss's formula q = 2 and n = 8:

$$\frac{1}{8}\left(\sum_{d|8}\mu(8/d)2^d\right)$$
$$=\frac{1}{8}\left(\sum_{d\in\{1,2,4,8\}}\mu(8/d)2^d\right)$$
$$=\frac{1}{8}\left(\mu(8/1)2^1+\mu(8/2)2^2+\mu(8/4)2^4+\mu(8/8)2^8\right)$$
$$=\frac{1}{8}\left(\mu(8)2^1+\mu(4)2^2+\mu(2)2^4+\mu(1)2^8\right)$$
$$=\frac{1}{8}\left(-2^4+2^8\right)$$
$$=\frac{1}{8}(240)$$
$$=30$$

So there are 30 irreducible polynomials splitting GF(2) into GF(256).

Minimum primitive element

Call α the minimum primitive element of GF(2^8). By raising α to successive powers, all non-zero elements of the field are generated: $\{\alpha^0, \alpha^1, \alpha^2, \ldots, \alpha^{254}\}$.

The below table gives all irreducible polynomials in GF(256) in algebraic, decimal, and hexadecimal format along with the minimum element α in algebraic and decimal format.

The irreducible polynomials were found using Wolfram Alpha by entering the expression `GF(256)` and expanding the "characteristic polynomial" view. Algorithms for finding irreducible polynomials are given by [Kerl]. The minimum primitive element was found by a C++ program which sequentially tested elements until finding one that generated the entire field.

Table 1: GF(256) irreducible polynomials

Irreducible polynomial	Poly (dec)	Poly (hex)	Min primitive element	Elem (dec)
$x^8+x^4+x^3+x+1$	283	0x11B	$x+1$	3
$x^8+x^4+x^3+x^2+1$	285	0x11D	x	2
$x^8+x^5+x^3+x+1$	299	0x12B	x	2
$x^8+x^5+x^3+x^2+1$	301	0x12D	x	2
$x^8+x^5+x^4+x^3+1$	313	0x139	$x+1$	3
$x^8+x^5+x^4+x^3+x^2+x+1$	319	0x13F	$x+1$	3
$x^8+x^6+x^3+x^2+1$	333	0x14D	x	2
$x^8+x^6+x^4+x^3+x^2+x+1$	351	0x15F	x	2
$x^8+x^6+x^5+x+1$	355	0x163	x	2
$x^8+x^6+x^5+x^2+1$	357	0x165	x	2
$x^8+x^6+x^5+x^3+1$	361	0x169	x	2
$x^8+x^6+x^5+x^4+1$	369	0x171	x	2
$x^8+x^6+x^5+x^4+x^2+x+1$	375	0x177	$x+1$	3
$x^8+x^6+x^5+x^4+x^3+x+1$	379	0x17B	x^3+1	9
$x^8+x^7+x^2+x+1$	391	0x187	x	2
$x^8+x^7+x^3+x+1$	395	0x18B	x^2+x	6
$x^8+x^7+x^3+x^2+1$	397	0x18D	x	2
$x^8+x^7+x^4+x^3+x^2+x+1$	415	0x19F	$x+1$	3
$x^8+x^7+x^5+x+1$	419	0x1A3	$x+1$	3
$x^8+x^7+x^5+x^3+1$	425	0x1A9	x	2
$x^8+x^7+x^5+x^4+1$	433	0x1B1	x^2+x	6
$x^8+x^7+x^5+x^4+x^3+x^2+1$	445	0x1BD	x^2+x+1	7
$x^8+x^7+x^6+x+1$	451	0x1C3	x	2
$x^8+x^7+x^6+x^3+x^2+x+1$	463	0x1CF	x	2
$x^8+x^7+x^6+x^4+x^2+x+1$	471	0x1D7	x^2+x+1	7
$x^8+x^7+x^6+x^4+x^3+x^2+1$	477	0x1DD	x^2+x	6
$x^8+x^7+x^6+x^5+x^2+x+1$	487	0x1E7	x	2
$x^8+x^7+x^6+x^5+x^4+x+1$	499	0x1F3	x^2+x	6
$x^8+x^7+x^6+x^5+x^4+x^2+1$	501	0x1F5	x	2
$x^8+x^7+x^6+x^5+x^4+x^3+1$	505	0x1F9	$x+1$	3

Number of primitive elements

Consider a term $\gamma = \alpha^n$. If γ raised to successive integer powers generates $\{\gamma^0, \gamma^1, \gamma^2, \ldots, \gamma^{254}\}$ all non-zero elements of the field, the γ is also a primitive element.

The number of primitive elements for GF(q) is given as $\phi(q-1)$ where ϕ is Euler's totient function [Kaliski].

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

where $p|n$ gives the distinct prime factors of n

For GF(256):

$\phi(256 - 1)$

$= \phi(255)$

$$= 255 \prod_{p|255} \left(1 - \frac{1}{p}\right)$$

$$= 255 \prod_{p \in \{3,5,17\}} \left(1 - \frac{1}{p}\right)$$

$$= 255 \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{17}\right)$$

$= 128$

There are 128 primitive elements of GF(256).

Table of primitive elements

This table of primitive elements was found by a C++ program which took the minimum primitive element for each of the 30 irreducible polynomails in GF(256) and tested each power greater than 0 to see if it generated each field element. The same values occur in all 30 irreducible polynomials.

Table 2: 128 primitive elements of GF(256)

α^{1}	α^{64}	α^{128}	α^{193}
α^{2}	α^{67}	α^{131}	α^{194}
α^{4}	α^{71}	α^{133}	α^{196}
α^{7}	α^{73}	α^{134}	α^{197}
α^{8}	α^{74}	α^{137}	α^{199}
α^{11}	α^{76}	α^{139}	α^{202}
α^{13}	α^{77}	α^{142}	α^{203}
α^{14}	α^{79}	α^{143}	α^{206}
α^{16}	α^{82}	α^{146}	α^{208}
α^{19}	α^{83}	α^{148}	α^{209}
α^{22}	α^{86}	α^{149}	α^{211}
α^{23}	α^{88}	α^{151}	α^{212}
α^{26}	α^{89}	α^{152}	α^{214}
α^{28}	α^{91}	α^{154}	α^{217}
α^{29}	α^{92}	α^{157}	α^{218}
α^{31}	α^{94}	α^{158}	α^{223}
α^{32}	α^{97}	α^{161}	α^{224}
α^{37}	α^{98}	α^{163}	α^{226}
α^{38}	α^{101}	α^{164}	α^{227}
α^{41}	α^{103}	α^{166}	α^{229}
α^{43}	α^{104}	α^{167}	α^{232}
α^{44}	α^{106}	α^{169}	α^{233}
α^{46}	α^{107}	α^{172}	α^{236}
α^{47}	α^{109}	α^{173}	α^{239}
α^{49}	α^{112}	α^{176}	α^{241}
α^{52}	α^{113}	α^{178}	α^{242}
α^{53}	α^{116}	α^{179}	α^{244}
α^{56}	α^{118}	α^{181}	α^{247}
α^{58}	α^{121}	α^{182}	α^{248}
α^{59}	α^{122}	α^{184}	α^{251}
α^{61}	α^{124}	α^{188}	α^{253}
α^{62}	α^{127}	α^{191}	α^{254}

Curiously, the sequence of exponent values $\{1, 2, 4, 7, 8, 11, 13, 14, 16, 19, 22, 23, 26, 28, 29, 31, \ldots\}$ are non-multiples of Fermat numbers. A Fermat number is of the form $2^{2^n} + 1$.
This corresponds to On-Line Encyclopedia of Integer Sequences (OEIS) entry

A080308 [Sloane].

References

S. K. Chebolu and J. Mináč, "Counting irreducible polynomials over finite fields using the inclusion-exclusion principle," Mathematics Magazine, vol. 84, no. 5, pp. 369–371, 2011. https://arxiv.org/pdf/1001.0409.pdf

Kaliski B., "Primitive Element", Encyclopedia of Cryptography and Security, 2005.

J. Kerl, "Computation in finite fields," published electronically at https://johnkerl.org/doc/ffcomp.pdf, July 2019.

N. J. A. Sloane, editor, "The On-Line Encyclopedia of Integer Sequences," published electronically at https://oeis.org/A080308, July 2019.