THE FACTORIZATION OF $X^{255} - 1$ IN $Z_2[X]$

Adrian ATANASIU [1*]
Bogdan GHIMIŞ [2]

ABSTRACT

AES (Rijndael) is considered the most prolific and widely used ([2]) encryption algorithm and it has deep roots in Galois field theory. The mathematical operations that occur are done in a special finite field – GF(2^8) that is obtained by factorizing $Z_2[X]$ over the polinomial $1 + X + X^3 + X^4 + X^8$. We have been wondering why that polynomial has been chosen and if there are some hidden proprieties of that polynomial that other's don't have. In this paper, we are going to look into the structure of GF(2^8) and try to find some answers regarding this choice made by the authors of AES.

1. INTRODUCTION

First we are going to present a short mathematical set of basic concepts; followed by the inner workings of AES by pointing out its computations using the GF(2^8) field. Finally will look into other papers published by the authors of AES and see how they solved another similar problem.

2. MATHEMATICAL PRELIMINARIES

2.1. Groups and Rings

Definition 2.1.1. A *group* (G, *) is defined by a set *G* and a binary operation * on the set, that obeys the following proprieties:

- the binary operation * is **closed** on S (taking any two elements x, y from G and applying the binary operation, the result is still an element from S)
- the binary operation * is **associative** (e. g. $(x * y) * z = x * (y * z)$)
- there exists an identity element in G (**1**) (e.g. $\exists\, \mathbf{1} \in G\ s.t. \mathbf{1} * x = x * \mathbf{1} = x\ \forall\, x \in G$)
- each element in G has an inverse (e.g. $\forall\, x \in G\ \exists\, x^{-1} \in G\ s.t.\ x * x^{-1} = x^{-1} * x = \mathbf{1}$)

Definition 2.1.2. An *abelian group* (G, *) is a group where the binary operation is also commutative.

[1*] corresponding author, Professor, PhD, University of Bucharest, aadrian@gmail.com
[2] University of Bucharest, bghimis@gmail.com

Definition 2.1.3. In a group (G, *), a subset S generates G if any element of G can be expressed as a combination of elements of S using the binary operation *.

Definition 2.1.4. A group (G, *) is called *cyclic* if it can be generated by a single element, which means that all the elements are actually "powers" of a single item α, called a generator ([5]).

Definition 2.1.5. A *ring* (R, +, *) is defined by a set R and two binary operations (additive and multiplicative), so that:

- (R, +) is an abelian group, with the identity element noted **0**
- (R, *) is an monoid, with the identity element noted **1**
- $x * (y + z) = x * y + x * z \ \wedge (x + y) * z = x * z + y * z \ \forall \ x, y, z \ \epsilon \ R$

Definition 2.1.5. A *commutative ring* is a ring in which the multiplicative operation is commutative.

2.2. Fields

Definition 2.2.1. A *field* (K, +, *) respects the following proprieties:

- (K, +, *) is a commutative ring
- $\forall x \epsilon K^* = K \backslash \{\mathbf{0}\} \ \exists x^{-1} \ \epsilon \ K \ s.t. \ x * x^{-1} = \ x^{-1} * x = \mathbf{1}$

Definition 2.2.2. A *finite field* is a field K with a finite number of elements. This number is called the *order* of K and denoted by *ord(K)*.

Theorem 2.2.3. If K is a finite field and $ord(K) \ = \ q$ then $q \ = \ p^n$, where *p* is a prime number and *n* is a positive integer. Usually we shall work with field $Z_2 = \{\mathbf{0}, \mathbf{1}\}$ where the addition is XOR, and the multiplication is defined $xy = \mathbf{1}$ iff $x = y = \mathbf{1}$.

Definition 2.2.4. A *polynomial ring* K[X] in variable X over a field K is the set of polynomials: $P \ = \ a_0 \ + \ a_1 \ * \ X \ + \ a_2 \ * \ X^2 \ + \ ... \ + \ a_n \ * \ X^n + \cdots \ (a_i \ \epsilon \ K)$ having as operations usual addition and multiplications with polynomials.

The *degree* (deg) of a polynomial represents the largest power of X for which the coefficient a_n is not null.

The fundamental result used here is the following: For every two polynomials P and Q, with Q $\neq$ 0, there are (unique) polynomials q (quotient) and r (remainder) so that:

- $P = q * Q + r$
- $deg(r) < deg(Q)$

Furthermore, we can define the greatest common divisor (gcd) and the least common multiple (lcm) for polynomials. We can calculate them using – first - the Euclid's algorithm (for *gcd*), then (for *lcm*) the relation

$$lcm(P, Q) = \frac{P * Q}{\gcd(P, \ Q)}.$$

Definition 2.2.5. An *irreducible polynomial* is polynomial that cannot be written as a product of nontrivial polynomials over the same field.

Definition 2.2.6. A *root* of a polynomial P is an element $r \in K$ so that $P(r) = 0$, where $P(r) = a_0 + a_1*r + a_2*r^2 + ... + a_n*r^n$.

Definition 2.2.7. A *minimal polynomial* of a value α is the polynomial m of lowest degree such that α is a root of m.

Definition 2.2.8. A *primitive polynomial* is a polynomial that generates all elements of an extension field.

In order to construct an *extension* of a field K, we will need

- the polynomial ring K[X],
- an irreducible polynomial f.

Then quotient ring $K[X] / f$ is defined as follows:

$$K[X] / f = \{r \mid \text{there is } P \in K[X] \text{ so that } P = q * f + r, \deg(r) < \deg(f)\}.$$

We say that $r = P$ (r equals P) modulo the irreductible polinomial f.

Therefore $K[X]/f$ will contain all polynomials of degrees less than $deg(f)$.

Theorem 2.2.9. Let $Z_p[X]$ be a ring of polynomials and $f \in Z_p[X]$ an irreducible polynomial. Then $(Z_p[X]/f, +, *)$ is a field, where the product is performed modulo the polinomial f.

In particular, for $p = 2$ and for $f \in Z_2[X]$ an irreducible polynomial of degree 8, we define $GF(2^8) = Z_2[X]/f$ as the set of bytes having a field structure that depends on the chosen polynomial f. We specify that the byte $a_0a_1a_2...a_7$ corresponds to the polynomial $a_0 + a_1X + a_2X^2 + \ldots + a_7X^7$.

The field $GF(2^8)=Z_2[X] / (1+X+X^3+X^4+X^8)$ has 2^8 elements, and the polynomial $1 + X$ (first row in Annex 2) can be chosen as generator for the multiplicative group $(GF(2^8)^*, *)$.

3. ADVANCED ENCRYPTION STANDARD

AES is a block cipher encryption symmetric algorithm with which one can partition the data into blocks, encrypt it and then send it through an insecure channel. Being a symmetric encryption algorithm, it uses the same encryption key for encrypting and decrypting the data.

Encryption steps:

- Key-Expansion step: (the symmetric key is used to derive Round-Keys)
- In the first round we execute AddRoundKey
- The next (9, 11 or 13) rounds the following operations take place:
  - SubBytes
  - ShiftRows
  - MixColumns
  - AddRoundKey
- In the final round, all operations will be performed except the last one:
  - SubBytes

- ShiftRows
- MixColumns

In the SubBytes step, a substitution box (S-box) is used in which each byte is swapped with another one in a deterministic fashion, using a lookup table. This lookup table was derived from the multiplicative inverse over GF(2^8), followed by a affine transformation. This is the only nonlinear step of the algorithm ([1]).

The MixColumns step ensures that if only one bit of the input text is modified, at least half of the output bits would change ([4]).

Most of the operations of this algorithm take place in a finite field GF(2^8) using the irreducible polynomial $1 + X + X^3 + X^4 + X^8$. All the irreducible polynomials of degree 8 over Z_2 are irreducible factors of $X^{255} - 1$ and it is because of that this factorization is particularly interesting.

4. ABOUT IRREDUCIBLE FACTORS OF $X^{255} - 1$

There are 30 irreducible polynomials of degree 8 over Z_2 that can be found in Annex 1. Each one of them could have been used for AES encryption system.

One possible reason for which the peculiar polynomial $1 + X + X^3 + X^4 + X^8$ has been chosen is the fact that it has only five terms, and it is the first polynomial in lexicographical order (among all irreducible polynomial of degree 8, this one has the smallest exponents).

We can also note that for polynomial $1 + X + X^3 + X^4 + X^8$, although irreducible, the polynomial X is not a generator of GF(2^8) (=$Z_2[X] / (1 + X + X^3 + X^4 + X^8)$), its period being 51.

One of AES's inventors, Vincent Rijmen, along with Paulo Barreto, has proposed a hash function WHIRLPOOL ([6]) which is based on AES.

This hash function uses the same Galois field GF(2^8), but uses $1 + X^2 + X^3 + X^4 + X^8$ as irreducible polynomial. It is specified by the authors that this polynomial was chosen because it was the first polynomial listed in Table C from [3], and for which the primitive polynomial X generates the whole GF(2^8).

Another possible reason for choosing the first polynomial for Rijndael is for processing speed for 8 and 32 bit processors. In the original specification of this algorithm, it is asserted that the operations that take place in this field can be very efficient both for 8-bit processors (smartcards) and for 32-bit processors (PCs) ([1]).

Moreover, the construction of S-boxes for AES was made in such a manner that the polynomials are simple, but there also exists an algebraic complexity, when working in GF(2^8)([1]).

Rijndael's authors have initially considered that the S-box should be the mapping $x \Rightarrow x^{-1}$ in GF(2^8), but the algebraic complexity was weak and some attacks (e.g. interpolation attack) can be performed. Because of that an affine transformation was added.

4.1. The factorization of $X^{255} - 1$

For the factorization of $X^{255} - 1$, we consider GF(2^8)=Z_2[X] / (1 + X^2 + X^3 + X^4 + X^8) using the first primitive polynomial listed in Annex 2.

Because $1 + X$ is a primitive polynomial, we can compute the factorization of $X^{255} - 1$. First of all, if α is a root of 1+X^2 + X^3 + X^4 + X^8 = 0, we shall compute the minimal polynomials of each power of α:

Minimal polynomial	Roots
$1 + X^2 + X^3 + X^4 + X^8$	$\alpha^1, \alpha^2, \alpha^4, \alpha^8, \alpha^{16}, \alpha^{32}, \alpha^{64}, \alpha^{128}$
$1 + X^1 + X^2 + X^4 + X^5 + X^6 + X^8$	$\alpha^3, \alpha^6, \alpha^{12}, \alpha^{24}, \alpha^{48}, \alpha^{96}, \alpha^{129}, \alpha^{192}$
$1 + X^1 + X^4 + X^5 + X^6 + X^7 + X^8$	$\alpha^5, \alpha^{10}, \alpha^{20}, \alpha^{40}, \alpha^{65}, \alpha^{80}, \alpha^{130}, \alpha^{160}$
$1 + X^3 + X^5 + X^6 + X^8$	$\alpha^7, \alpha^{14}, \alpha^{28}, \alpha^{56}, \alpha^{112}, \alpha^{131}, \alpha^{193}, \alpha^{224}$
$1 + X^2 + X^3 + X^4 + X^5 + X^7 + X^8$	$\alpha^9, \alpha^{18}, \alpha^{33}, \alpha^{36}, \alpha^{66}, \alpha^{72}, \alpha^{132}, \alpha^{144}$
$1 + X^1 + X^2 + X^5 + X^6 + X^7 + X^8$	$\alpha^{11}, \alpha^{22}, \alpha^{44}, \alpha^{88}, \alpha^{97}, \alpha^{133}, \alpha^{176}, \alpha^{194}$
$1 + X^1 + X^3 + X^5 + X^8$	$\alpha^{13}, \alpha^{26}, \alpha^{52}, \alpha^{67}, \alpha^{104}, \alpha^{134}, \alpha^{161}, \alpha^{208}$
$1 + X^1 + X^2 + X^4 + X^6 + X^7 + X^8$	$\alpha^{15}, \alpha^{30}, \alpha^{60}, \alpha^{120}, \alpha^{135}, \alpha^{195}, \alpha^{225}, \alpha^{240}$
$1 + X^1 + X^4$	$\alpha^{17}, \alpha^{34}, \alpha^{68}, \alpha^{136}$
$1 + X^2 + X^5 + X^6 + X^8$	$\alpha^{19}, \alpha^{38}, \alpha^{49}, \alpha^{76}, \alpha^{98}, \alpha^{137}, \alpha^{152}, \alpha^{196}$
$1 + X^1 + X^3 + X^7 + X^8$	$\alpha^{21}, \alpha^{42}, \alpha^{69}, \alpha^{81}, \alpha^{84}, \alpha^{138}, \alpha^{162}, \alpha^{168}$
$1 + X^1 + X^5 + X^6 + X^8$	$\alpha^{23}, \alpha^{46}, \alpha^{92}, \alpha^{113}, \alpha^{139}, \alpha^{184}, \alpha^{197}, \alpha^{226}$
$1 + X^1 + X^3 + X^4 + X^8$	$\alpha^{25}, \alpha^{35}, \alpha^{50}, \alpha^{70}, \alpha^{100}, \alpha^{140}, \alpha^{145}, \alpha^{200}$
$1 + X^1 + X^2 + X^3 + X^4 + X^5 + X^8$	$\alpha^{27}, \alpha^{54}, \alpha^{99}, \alpha^{108}, \alpha^{141}, \alpha^{177}, \alpha^{198}, \alpha^{216}$
$1 + X^2 + X^3 + X^7 + X^8$	$\alpha^{29}, \alpha^{58}, \alpha^{71}, \alpha^{116}, \alpha^{142}, \alpha^{163}, \alpha^{209}, \alpha^{232}$
$1 + X^2 + X^3 + X^5 + X^8$	$\alpha^{31}, \alpha^{62}, \alpha^{124}, \alpha^{143}, \alpha^{199}, \alpha^{227}, \alpha^{241}, \alpha^{248}$
$1 + X^1 + X^2 + X^3 + X^4 + X^6 + X^8$	$\alpha^{37}, \alpha^{41}, \alpha^{73}, \alpha^{74}, \alpha^{82}, \alpha^{146}, \alpha^{148}, \alpha^{164}$
$1 + X^3 + X^4 + X^5 + X^6 + X^7 + X^8$	$\alpha^{39}, \alpha^{57}, \alpha^{78}, \alpha^{114}, \alpha^{147}, \alpha^{156}, \alpha^{201}, \alpha^{228}$
$1 + X^1 + X^6 + X^7 + X^8$	$\alpha^{43}, \alpha^{86}, \alpha^{89}, \alpha^{101}, \alpha^{149}, \alpha^{172}, \alpha^{178}, \alpha^{202}$
$1 + X^3 + X^4 + X^5 + X^8$	$\alpha^{45}, \alpha^{75}, \alpha^{90}, \alpha^{105}, \alpha^{150}, \alpha^{165}, \alpha^{180}, \alpha^{210}$
$1 + X^3 + X^5 + X^7 + X^8$	$\alpha^{47}, \alpha^{94}, \alpha^{121}, \alpha^{151}, \alpha^{188}, \alpha^{203}, \alpha^{229}, \alpha^{242}$
$1 + X^1 + X^2 + X^3 + X^4$	$\alpha^{51}, \alpha^{102}, \alpha^{153}, \alpha^{204}$
$1 + X^1 + X^2 + X^7 + X^8$	$\alpha^{53}, \alpha^{77}, \alpha^{83}, \alpha^{106}, \alpha^{154}, \alpha^{166}, \alpha^{169}, \alpha^{212}$
$1 + X^4 + X^5 + X^7 + X^8$	$\alpha^{55}, \alpha^{110}, \alpha^{115}, \alpha^{155}, \alpha^{185}, \alpha^{205}, \alpha^{220}, \alpha^{230}$
$1 + X^2 + X^3 + X^6 + X^8$	$\alpha^{59}, \alpha^{103}, \alpha^{118}, \alpha^{157}, \alpha^{179}, \alpha^{206}, \alpha^{217}, \alpha^{236}$
$1 + X^1 + X^2 + X^3 + X^6 + X^7 + X^8$	$\alpha^{61}, \alpha^{79}, \alpha^{122}, \alpha^{158}, \alpha^{167}, \alpha^{211}, \alpha^{233}, \alpha^{244}$
$1 + X^2 + X^3 + X^4 + X^6 + X^7 + X^8$	$\alpha^{63}, \alpha^{126}, \alpha^{159}, \alpha^{207}, \alpha^{231}, \alpha^{243}, \alpha^{249}, \alpha^{252}$
$1 + X^1 + X^2$	$\alpha^{85}, \alpha^{170}$
$1 + X^1 + X^5 + X^7 + X^8$	$\alpha^{87}, \alpha^{93}, \alpha^{117}, \alpha^{171}, \alpha^{174}, \alpha^{186}, \alpha^{213}, \alpha^{234}$
$1 + X^2 + X^4 + X^5 + X^6 + X^7 + X^8$	$\alpha^{91}, \alpha^{107}, \alpha^{109}, \alpha^{173}, \alpha^{181}, \alpha^{182}, \alpha^{214}, \alpha^{218}$
$1 + X^1 + X^2 + X^3 + X^4 + X^7 + X^8$	$\alpha^{95}, \alpha^{125}, \alpha^{175}, \alpha^{190}, \alpha^{215}, \alpha^{235}, \alpha^{245}, \alpha^{250}$
$1 + X^1 + X^3 + X^4 + X^5 + X^6 + X^8$	$\alpha^{111}, \alpha^{123}, \alpha^{183}, \alpha^{189}, \alpha^{219}, \alpha^{222}, \alpha^{237}, \alpha^{246}$
$1 + X^3 + X^4$	$\alpha^{119}, \alpha^{187}, \alpha^{221}, \alpha^{238}$
$1 + X^4 + X^5 + X^6 + X^8$	$\alpha^{127}, \alpha^{191}, \alpha^{223}, \alpha^{239}, \alpha^{247}, \alpha^{251}, \alpha^{253}, \alpha^{254}$
$1 + X^1$	α^{255}

In order to compute the minimal polynomial m of a value α, we firstly compute its order k (i.e. for α^i we compute $\alpha^{2*i}, \alpha^{2^2*i}, \alpha^{2^3*i} \ldots, \alpha^{2^k*i} = \alpha^i$ (modulus 1 + X^2 + X^3 + X^4 + X^8)**.**

Because $m(\alpha^i) = 0$ and because $m = a_0 + a_1 * X + a_2X^2 + \ldots + a_{k-1}X^{k-1} + X^k$, we will solve the linear system $Ax = B$, where

$$A = \begin{bmatrix} 1 & {\alpha^i}_0 & \cdots & {\alpha^{(k-1)*i}}_0 \\ 0 & {\alpha^i}_1 & & {\alpha^{(k-1)*i}}_1 \\ \vdots & & \ddots & \vdots \\ 0 & {\alpha^i}_{n-1} & \cdots & {\alpha^{(k-1)*i}}_{n-2} \\ 0 & {\alpha^i}_{n-2} & & {\alpha^{(k-1)*i}}_{n-1} \end{bmatrix} B = - \begin{bmatrix} {\alpha^{k*i}}_0 \\ {\alpha^{k*i}}_1 \\ \vdots \\ {\alpha^{k*i}}_{n-2} \\ {\alpha^{k*i}}_{n-1} \end{bmatrix} x = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-2} \\ a_{k-1} \end{bmatrix}$$

These polynomials are all irreductible factors of $X^{255} - 1$. To verify that we will compute their least common multiple. Because $gcd = 1$ for any pair of polynomials, the lcm is directly their product, that is $1 + X^{255}$ (or $X^{255} - 1$ in the binary case).

BIBLIOGRAPHY

[1] Joan Daemen, Vincent Rijmen - The Rijndael Block Cipher - AES Proposal, https://csrc.nist.gov/csrc/media/projects/cryptographic-standards-and-guidelines/documents/aes-development/rijndael-ammended.pdf, 1999

[2] Mansoor Ebrahim, Shujaat Khan, Umer Bin Khalid - Symmetric Algorithm Survey: A Comparative Analysis - International Journal of Computer Applications (0975 - 8887), 2014

[3] Rudolf Lidl, Harald Niederreiter - Introduction to Finite Fields and their Applications - Cambridge University Press, 1986, pag. 378, Tabel C.

[4] Claude Shannon - A Mathematical Theory of Cryptography, 1945, part 3, pag. 92.

[5] https://en.wikipedia.org/wiki/Finite_field

[6] https://web.archive.org/web/20170817134205/ http://www.larc.usp.br:80/~pbarreto/WhirlpoolPage.html

Annex 1. All irreducible polynomials of degree 8 over Z_2:

$1 + X^2 + X^3 + X^7 + X^8$
$1 + X^1 + X^3 + X^5 + X^8$
$1 + X^1 + X^2 + X^3 + X^4 + X^5 + X^8$
$1 + X^1 + X^2 + X^4 + X^5 + X^6 + X^8$
$1 + X^1 + X^2 + X^4 + X^6 + X^7 + X^8$
$1 + X^2 + X^4 + X^5 + X^6 + X^7 + X^8$
$1 + X^2 + X^3 + X^4 + X^5 + X^7 + X^8$
$1 + X^3 + X^5 + X^7 + X^8$
$1 + X^1 + X^3 + X^4 + X^8$ **(AES)**
$1 + X^2 + X^3 + X^6 + X^8$
$1 + X^3 + X^4 + X^5 + X^6 + X^7 + X^8$
$1 + X^4 + X^5 + X^7 + X^8$
$1 + X^2 + X^5 + X^6 + X^8$
$1 + X^2 + X^3 + X^4 + X^6 + X^7 + X^8$
$1 + X^3 + X^5 + X^6 + X^8$

$1 + X^1 + X^2 + X^3 + X^6 + X^7 + X^8$
$1 + X^2 + X^3 + X^5 + X^8$
$1 + X^3 + X^4 + X^5 + X^8$
$1 + X^4 + X^5 + X^6 + X^8$
$1 + X^2 + X^3 + X^4 + X^8$ (**WHIRLPOOL**)
$1 + X^1 + X^3 + X^7 + X^8$
$1 + X^1 + X^2 + X^3 + X^4 + X^7 + X^8$
$1 + X^1 + X^5 + X^7 + X^8$
$1 + X^1 + X^2 + X^7 + X^8$
$1 + X^1 + X^4 + X^5 + X^6 + X^7 + X^8$
$1 + X^1 + X^2 + X^3 + X^4 + X^6 + X^8$
$1 + X^1 + X^5 + X^6 + X^8$
$1 + X^1 + X^6 + X^7 + X^8$
$1 + X^1 + X^2 + X^5 + X^6 + X^7 + X^8$
$1 + X^1 + X^3 + X^4 + X^5 + X^6 + X^8$

These polynomials were found in an incremental manner, starting from irreducible polynomials of degree less or equal to 2. The method used in finding the irreducible polynomials was to generate the set of all polynomials of higher degree and then subtract from that set the reducible ones. A reducible polynomial of degree n can be found by taking two polynomials, one of degree *p* and one of degree *q,* where $p > 0, q > 0, p + q = n$, and multiplying them together.

Annex 2. All primitive polynomials which can generate $GF(2^8)=Z_2[X] / (1 + X + X^3 + X^4 + X^8)$

The current number corresponds (in base 10) to the vector representation of the polynomial associated on its right. For example, for $1 + X^2 + X^3$ the vector representation is [0, 1, 1, 1, 0, 0, 0, 0], that is 1110 in binary and $(1110)_2 = (14)_{10}$.

3	$1 + X^1$	134	$X^1 + X^2 + X^7$
5	$1 + X^2$	135	$1 + X^1 + X^2 + X^7$
6	$X^1 + X^2$	136	$X^3 + X^7$
9	$1 + X^3$	138	$X^1 + X^3 + X^7$
11	$1 + X^1 + X^3$	142	$X^1 + X^2 + X^3 + X^7$
14	$X^1 + X^2 + X^3$	143	$1 + X^1 + X^2 + X^3 + X^7$
17	$1 + X^4$	144	$X^4 + X^7$
18	$X^1 + X^4$	147	$1 + X^1 + X^4 + X^7$
19	$1 + X^1 + X^4$	149	$1 + X^2 + X^4 + X^7$
20	$X^2 + X^4$	150	$X^1 + X^2 + X^4 + X^7$
23	$1 + X^1 + X^2 + X^4$	152	$X^3 + X^4 + X^7$
24	$X^3 + X^4$	153	$1 + X^3 + X^4 + X^7$
25	$1 + X^3 + X^4$	155	$1 + X^1 + X^3 + X^4 + X^7$
26	$X^1 + X^3 + X^4$	157	$1 + X^2 + X^3 + X^4 + X^7$
28	$X^2 + X^3 + X^4$	160	$X^5 + X^7$
30	$X^1 + X^2 + X^3 + X^4$	164	$X^2 + X^5 + X^7$
31	$1 + X^1 + X^2 + X^3 + X^4$	165	$1 + X^2 + X^5 + X^7$
33	$1 + X^5$	166	$X^1 + X^2 + X^5 + X^7$
34	$X^1 + X^5$	167	$1 + X^1 + X^2 + X^5 + X^7$
35	$1 + X^1 + X^5$	169	$1 + X^3 + X^5 + X^7$

39	$1 + X^1 + X^2 + X^5$	170	$X^1 + X^3 + X^5 + X^7$
40	$X^3 + X^5$	172	$X^2 + X^3 + X^5 + X^7$
42	$X^1 + X^3 + X^5$	173	$1 + X^2 + X^3 + X^5 + X^7$
44	$X^2 + X^3 + X^5$	178	$X^1 + X^4 + X^5 + X^7$
48	$X^4 + X^5$	180	$X^2 + X^4 + X^5 + X^7$
49	$1 + X^4 + X^5$	183	$1 + X^1 + X^2 + X^4 + X^5 + X^7$
60	$X^2 + X^3 + X^4 + X^5$	184	$X^3 + X^4 + X^5 + X^7$
62	$X^1 + X^2 + X^3 + X^4 + X^5$	185	$1 + X^3 + X^4 + X^5 + X^7$
63	$1 + X^1 + X^2 + X^3 + X^4 + X^5$	186	$X^1 + X^3 + X^4 + X^5 + X^7$
65	$1 + X^6$	190	$X^1 + X^2 + X^3 + X^4 + X^5 + X^7$
69	$1 + X^2 + X^6$	191	$1 + X^1 + X^2 + X^3 + X^4 + X^5 + X^7$
70	$X^1 + X^2 + X^6$	192	$X^6 + X^7$
71	$1 + X^1 + X^2 + X^6$	193	$1 + X^6 + X^7$
72	$X^3 + X^6$	196	$X^2 + X^6 + X^7$
73	$1 + X^3 + X^6$	200	$X^3 + X^6 + X^7$
75	$1 + X^1 + X^3 + X^6$	201	$1 + X^3 + X^6 + X^7$
76	$X^2 + X^3 + X^6$	206	$X^1 + X^2 + X^3 + X^6 + X^7$
78	$X^1 + X^2 + X^3 + X^6$	207	$1 + X^1 + X^2 + X^3 + X^6 + X^7$
79	$1 + X^1 + X^2 + X^3 + X^6$	208	$X^4 + X^6 + X^7$
82	$X^1 + X^4 + X^6$	214	$X^1 + X^2 + X^4 + X^6 + X^7$
84	$X^2 + X^4 + X^6$	215	$1 + X^1 + X^2 + X^4 + X^6 + X^7$
86	$X^1 + X^2 + X^4 + X^6$	218	$X^1 + X^3 + X^4 + X^6 + X^7$
87	$1 + X^1 + X^2 + X^4 + X^6$	220	$X^2 + X^3 + X^4 + X^6 + X^7$
88	$X^3 + X^4 + X^6$	221	$1 + X^2 + X^3 + X^4 + X^6 + X^7$
89	$1 + X^3 + X^4 + X^6$	222	$X^1 + X^2 + X^3 + X^4 + X^6 + X^7$
90	$X^1 + X^3 + X^4 + X^6$	226	$X^1 + X^5 + X^6 + X^7$
91	$1 + X^1 + X^3 + X^4 + X^6$	227	$1 + X^1 + X^5 + X^6 + X^7$
95	$1 + X^1 + X^2 + X^3 + X^4 + X^6$	229	$1 + X^2 + X^5 + X^6 + X^7$
100	$X^2 + X^5 + X^6$	230	$X^1 + X^2 + X^5 + X^6 + X^7$
101	$1 + X^2 + X^5 + X^6$	231	$1 + X^1 + X^2 + X^5 + X^6 + X^7$
104	$X^3 + X^5 + X^6$	233	$1 + X^3 + X^5 + X^6 + X^7$
105	$1 + X^3 + X^5 + X^6$	234	$X^1 + X^3 + X^5 + X^6 + X^7$
109	$1 + X^2 + X^3 + X^5 + X^6$	235	$1 + X^1 + X^3 + X^5 + X^6 + X^7$
110	$X^1 + X^2 + X^3 + X^5 + X^6$	238	$X^1 + X^2 + X^3 + X^5 + X^6 + X^7$
112	$X^4 + X^5 + X^6$	240	$X^4 + X^5 + X^6 + X^7$
113	$1 + X^4 + X^5 + X^6$	241	$1 + X^4 + X^5 + X^6 + X^7$
118	$X^1 + X^2 + X^4 + X^5 + X^6$	244	$X^2 + X^4 + X^5 + X^6 + X^7$
119	$1 + X^1 + X^2 + X^4 + X^5 + X^6$	245	$1 + X^2 + X^4 + X^5 + X^6 + X^7$
121	$1 + X^3 + X^4 + X^5 + X^6$	246	$X^1 + X^2 + X^4 + X^5 + X^6 + X^7$
122	$X^1 + X^3 + X^4 + X^5 + X^6$	248	$X^3 + X^4 + X^5 + X^6 + X^7$
123	$1 + X^1 + X^3 + X^4 + X^5 + X^6$	251	$1 + X^1 + X^3 + X^4 + X^5 + X^6 + X^7$
126	$X^1 + X^2 + X^3 + X^4 + X^5 + X^6$	253	$1 + X^2 + X^3 + X^4 + X^5 + X^6 + X^7$
129	$1 + X^7$	254	$X^1 + X^2 + X^3 + X^4 + X^5 + X^6 + X^7$
132	$X^2 + X^7$	255	$1 + X^1 + X^2 + X^3 + X^4 + X^5 + X^6 + X^7$

We remark that 50% from elements of GF(2^8) (128 from 256) are primitive and can generate the whole field.